УСТРОЙСТВО ДЛЯ ОТСЛЕЖИВАНИЯ ВРЕДОНОСНОЙ И НЕЖЕЛАТЕЛЬНОЙ АКТИВНОСТИ В ПРОМЫШЛЕННЫХ СЕТЯХ MODBUS RTU

И.А. Тутов, ст. преподаватель,
Я.В. Калинкин, ст. группы 8Т8Б.
Томский политехнический университет.
E-mail: yvk36@tpu.ru

Введение

На сегодняшний день большинство предприятий переходит на автоматизированное производство, которое основано на осуществлении и контроле технологического процесса при помощи различных автоматических приборов и устройств. Данные устройства соединяются в сложные промышленные сети, связь между которыми организуется с помощью различных протоколов. Однако, несмотря на то, что физически устройства или документация о их структуре недоступна для внешнего влияния, возможно определенное вмешательство непосредственно в работу сети. Любое устройство в сети Интернет может подменить АРМ оператора. Несколько лет назад промышленные сети были изолированы от Интернет и в настоящее время не полностью разработаны механизмы защиты.

Целью нашей работы является создание устройства, способного определять нежелательную активность в сети Modbus RTU и уведомлять о ней.

Описание сети Modbus RTU

Modbus – открытый коммуникационный протокол, основанный на архитектуре «ведущий – ведомый» («master – slave») [1]. Данный протокол может использовать для передачи данных интерфейсы RS-485, RS-422, RS-232, а также Ethernet сети TCP/IP (протокол Modbus TCP).

В данной работе речь идет о протоколе Modbus RTU. Данная версия наиболее распространена и работает с интерфейсами RS-232, RS-422 и RS-485. Проводной интерфейс обеспечивает стабильную работу устройств на расстоянии до 1200 м и широко используется в промышленности. При использовании данного протокола передаваемые данные переводятся в двоичный вид и отправляются пакетами с определенными временными промежутками.

Таким образом, данный протокол прост в реализации, не требует установки дополнительного оборудования при разработке контроллеров и устройств, а также надежен и прост в отладке.

Однако данный протокол не предусматривает шифрование данных, а также принцип «ведущий – ведомый» ограничивает реактивность системы, поскольку все действия в сети инициируются ведущим устройством – контроллером, поэтому ведомые устройства не могут передавать данные, пока не будут опрошены ведущим.

Таким образом, если вмешаться в процесс передачи данных со стороны ведущего устройства, то можно получать данные с любого ведомого устройства без необходимости расшифровки данных и обхода каких-либо ограничений на получение или запись информации в ведомые устройства.

Следует также упомянуть, что изначально протокол Modbus разрабатывался для контроллеров Modicon, для которых характерна следующая структура [2]: 10001-19999 – дискретные входы (функция 02 – чтение группы регистров), 20001-29999 – дискретные выходы (01 – чтение группы регистров, 05 – запись одного регистра, 15 – запись группы регистров), 30001-39999 – 16-битные входы (04 – чтение группы регистров), 40001-49999 – 16-битные выходы (03 – чтение группы регистров, 06 – запись 1 регистра, 16 – запись группы регистров). Однако, данная адресация больше не является частью стандарта и конфигурации устройств могут различаться [3].

Структура сообщений Modbus RTU

Каждый тип протокола Modbus поддерживает собственный формат посылок ведущего ведомому, а также ответов ведомого ведущему. Структура сообщения ведущего ведомому имеет следующую структуру, приведенную на рисунке 1 [4].

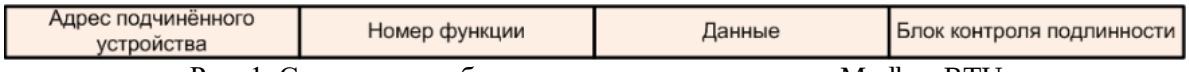

Рис. 1. Структура сообщения ведущего ведомому в Modbus RTU

Здесь поле «данные» содержит сведения о том, с какого регистра необходимо читать данные (или с какого необходимо записать) и какое количество регистров подлежит чтению/записи, номер функции

определяет назначение сообщения (запись/чтение), блок контроля подлинности содержит контрольную сумму для проверки целостности полученных данных. В основном контрольная сумма задается таблично [5].

Возможные сценарии утери информационной безопасности

Имея доступ к каналу связи между ведущим и ведомым устройством, злоумышленник извне может отправлять на ведомые устройства команды с целью чтения или записи информации в регистры.

Однако, как было указано выше, соответствие адресов, характерное для контроллеров Modicon, больше не является частью стандарта, поэтому адресация в отдельных сетях Modbus RTU может различаться. Таким образом, злоумышленнику может быть неизвестна реальная структура промышленной сети. В таком случае, имея доступ к каналу связи, злоумышленник может направлять команды на чтение последовательности регистров с целью выяснения конфигурации ведомого устройства.

Принцип работы разрабатываемого устройства

Поскольку конфигурация ведомых устройств некоторое время остается неизвестной для злоумышленника, то в ходе последовательного чтения регистров он может считать регистр, использование которого функционально не предполагается в ходе эксплуатации устройства, данный регистр может быть зарезервирован или вообще отсутствовать. Данные действия могут быть зафиксированы.

На основе микроконтроллера AVR создается и программируется устройство, которое связывается с внешней сетью Modbus. Поскольку внутри предприятия конфигурация устройств известна, возможно составить некоторую уставку, определяющую диапазон используемых в проекте регистров и применимых к ним команд.

Разрабатываемое устройство связывается с сетью Modbus RTU посредством универсального асинхронного интерфейса (UART). На этапе программирования в программу устройства закладывается указанная выше уставка. В ходе работы устройство принимает и анализирует сообщения Modbus и, если сообщение не удовлетворяет уставке, уведомляет штатного специалиста о несанкционированной активности или некорректной работе устройств. Информирование специалиста осуществляется по другому интерфейсу, например, с помощью LCD-дисплея.

Заключение

Описанная выше концепция позволяет создать универсальное, компактное и нетребовательное устройство для контроля информационной безопасности промышленной сети Modbus без использования таких средств, как существующие информационные диоды, обеспечивающие однонаправленную передачу информации как на физическом, так и на программном уровне. Устройство просто в эксплуатации и монтаже, не требует повышенного внимания и может быть использовано для контроля информационной безопасности предприятий различного рода.

Список использованных источников

1. Просто о протоколе Modbus RTU. [Электронный ресурс]. – URL: https://ipc2u.ru/articles/prostye-resheniya/modbus-rtu/ (дата обращения: 07.03.2021).
2. Как общаются машины: протокол Modbus. [Электронный ресурс]. – URL: https://habr.com/ru/company/advantech/blog/450234/?mobile=no (дата обращения: 07.03.2021).
3. Modbus. [Электронный ресурс]. – URL: https://ru.wikipedia.org/wiki/Modbus (дата обращения: 07.03.2021).
4. Промышленный протокол Modbus. [Электронный ресурс]. – URL: http://lazysmart.ru/osnovy-avtomatiki/promyshlenny-j-protokol-modbus/ (дата обращения: 07.03.2021).
5. Как посчитать контрольную сумму CRC32, CRC16, CRC8. [Электронный ресурс]. – URL: https://soltau.ru/index.php/themes/dev/item/461-kak- (дата обращения: 07.03.2021).