

ВЕРИФИКАЦИЯ УЗЛОВ СЕТИ ПРОМЫШЛЕННОГО ПРОТОКОЛА MODBUS

В данной работе анализируются особенности протокола Modbus, с акцентом на его уязвимости в контексте безопасности и защиты передаваемой информации. Рассмотрены основные риски, связанные с использованием Modbus в системах автоматизации и управления технологическими процессами (АСУ ТП), включая отсутствие механизмов шифрования и аутентификации, что делает его уязвимым к различным видам атак, таким как перехват данных или несанкционированный доступ, а также варианты решения проблемы верификации узлов.

Ключевые слова: информационная безопасность, АСУ ТП, промышленный протокол, Modbus

Yuzhakov A. A., Krotova E. L., Oshchepkov N. V.

VERIFICATION OF MODBUS INDUSTRIAL PROTOCOL NETWORK NODES

In this article, we analyzed the features of the Modbus protocol, with an emphasis on its vulnerabilities in the context of security and protection of transmitted information. The main risks associated with the use of Modbus in automation and process control systems (APCS) are considered, including the lack of encryption and authentication mechanisms, which makes it vulnerable to various types of attacks, such as data interception or unauthorized access. Options for solving the problem of node verification are considered.

Keywords: information security, APCS, industrial protocol, Modbus

Введение

В настоящее время большое внимание уделяется организации безопасной работы в системах АСУ ТП, работающих на базе промышленных сетевых протоколов (fieldbus). В перечень таких протоколов входят Profibus, DeviceNet, Modbus, CAN [1].

Modbus — это протокол коммуникации, имеющий клиент-серверную архитектуру, созданный в 1979 году компанией Modicon

для использования в промышленных системах автоматизации [2]. Modbus является стандартом передачи данных между контроллерами (PLC), сенсорами, исполнительными механизмами и прочим промышленным оборудованием. Протокол широко используется в различных сферах, включая:

- системы управления зданиями и домами
- промышленные и технологические системы

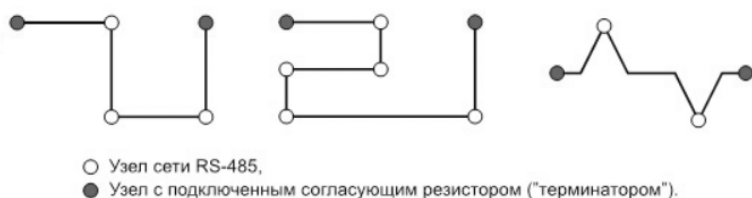


Рис. 1. Примеры топологий сетей RS-485

- электроэнергетика
- системы мониторинга и контроля различных технологических процессов.

Именно поэтому, в качестве исследуемого протокола использован широко применяемый в настоящее время протокол Modbus. Это обусловлено несколькими причинами [3]:

- существенно возросло количество новых разработок и объем организационной поддержки этого протокола
- отсутствует необходимость в специальных интерфейсных контроллерах
- простота программной реализации

Несмотря на всю простоту, широкое применение и удобство протокола, он не лишен недостатков, связанных с обеспечением безопасности и конфиденциальности передачи данных.

1. Описание протокола

Одним из ключевых преимуществ Modbus является устойчивость к искажениям данных, достигаемая благодаря строгой системы проверки ошибок [4]. Архитектура протокола предусматривает два формата передачи: компактный двоичный Modbus RTU (Remote Terminal Unit), оптимизированный для последовательных соединений, и текстовый Modbus ASCII, применяемый в специализированных задачах [3]. Режим RTU является обя-

зательным в спецификации Modbus, тогда как ASCII реализуется по необходимости. При конфигурации системы необходимо учитывать, что смешение режимов внутри одной сети недопустимо — все устройства должны функционировать в едином формате. На физическом уровне поддерживаются интерфейсы RS-232 и RS-485, однако в промышленных приложениях доминирует RS-485 [5].

На рисунке 1 показана структура сети, использующей интерфейс RS-485 совместно с протоколом Modbus. Такая конфигурация предполагает последовательное подключение устройств — как передающих, так и принимающих — посредством витой пары [6].

Архитектура протокола Modbus соответствует трём уровням эталонной модели OSI [7] (рис. 2): физическому, каналному и прикладному. Особенностью протокола является отсутствие реализации сетевого, транспортного и сеансового уровней (3-6) — их функции делегированы прикладному уровню, который обеспечивает коммуникацию между устройствами [8].

1.1 Физический уровень

Передача данных осуществляется с использованием интерфейса, который может быть двухпроводным (полудуплексным) или

Модель OSI для Modbus

НОМЕР УРОВНЯ	НАЗВАНИЕ УРОВНЯ	РЕАЛИЗАЦИЯ
7	Прикладной	Modbus application protocol
6	Уровень представления	Нет
5	Сеансовый	Нет
4	Транспортный	Нет
3	Сетевой	Нет
2	Канальный (передачи данных)	Протокол «ведущий–ведомый». Режимы RTU и ASCII
1	Физический	RS-485 или RS-232

Рис. 2. Модель OSI для Modbus

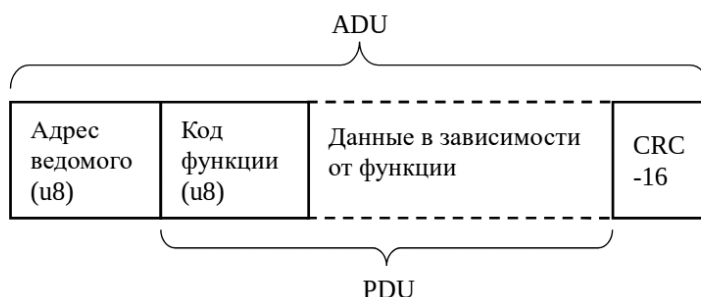


Рис. 3. Структура кадра MODBUS RTU

четырёхпроводным (дуплексным), соответствующим стандартам TIA/EIA-485 либо TIA/EIA-422 [9].

1.2 Канальный уровень

Протокол Modbus реализует классическую архитектуру по принципу "ведущий-ведомые", где ведущее устройство выступает в роли единственного управляющего устройства, подчиненные устройства являются исполнителями команд, принимаемых от ведущего устройства. Число подчинённых модулей в одной сети может достигать 247. Такая модель взаимодействия особенно важна в промышленных системах реального времени, где требуется строгий контроль за процессом [3].

1.3 Прикладной уровень

Прикладной уровень Modbus RTU обеспечивает связь между устройствами в режиме «ведущий-ведомый». Он функционирует независимо от нижележащих уровней — физического и канального — что обеспечивает совместимость с различными типами передачи данных, включая Ethernet TCP/IP (Modbus TCP/IP). Коммуникация на этом уровне осуществляется с помощью запросов, содержащих коды функций, которые определяют, какое действие должно быть выполнено ведомым устройством [3].

1.4 Формат пакета

Полный пакет (рис. 3), передаваемый по физическому каналу, включающий адрес ведомого и CRC, называют ADU – Application Data Unit. ADU инкапсулирует PDU – Protocol Data Unit – данные MODBUS, не зависящие от

среды передачи. Формат и размер PDU в свою очередь определяются кодом функции и числом регистров, которые должны быть записаны или прочитаны [11]. Минимальный размер фрейма в режиме RTU может достигать 5 байт.

Адрес устройства — адрес получателя, то есть slave-устройства, которому посылается управляющая команда.

Код функции — номер команды в виде 8 битного числа.

Данные — полезная нагрузка, посылаемая на ведомое устройство в зависимости от функции. Например, если выполняется функция чтения из регистров хранения, то внутри сегмента фрейма, отвечающего за данные, необходимо указать также адрес начального регистра и количество регистров.

Контрольная сумма — алгоритмы проверки целостности пакетов. Для хранения и передачи в Modbus RTU используются 2 последних байта фрейма, а в качестве алгоритма применяется CRC16 [12].

На рисунке (рис. 4) представлен режим передачи RTU, в котором данные передаются младшими разрядами вперед [3].

1.5 Вычисление контрольной суммы CRC16

Расчёт начинается с инициализации регистра значением 0xff. Для вычисления используется только содержимое байтов данных, без учёта стартовых, стоповых битов и бита чётности. Каждый байт последовательно обрабатывается с применением операций сдвига и побитового исключающего ИЛИ. Алгоритм повторяет цикл обработки для каждого байта, в результате чего формируется итоговая CRC16-сумма [10].

Стартовый бит	1 МЗР	2	3	4	5	6	7	8	Бит паритета	Стоп-бит
---------------	-------	---	---	---	---	---	---	---	--------------	----------

Рис. 4. Последовательность битов в режиме RTU

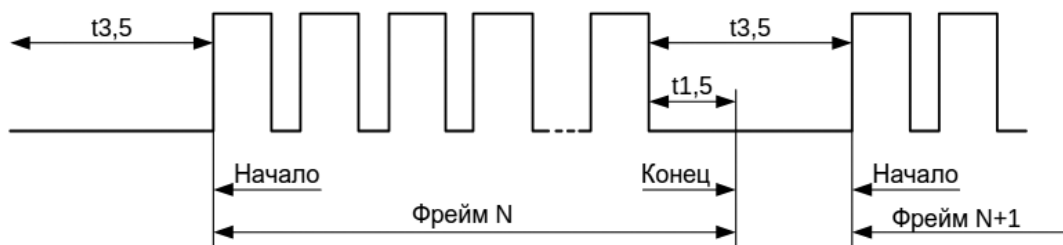


Рис. 5. Диаграмма передачи фреймов

1.6 Особенности протокола

Для разделения сообщений была внедрена система временных пауз, позволяющий идентифицировать, что фрейм пришел в полной мере [13]. На рисунке 5 представлен возможный формат общения ведущего и ведомого устройства [9].

Пауза между фреймами должна быть не короче времени передачи 3,5 символов при текущей скорости обмена. Формула для её вычисления представлена ниже (1) [13]:

$$t_{3.5}(\text{мс}) = \frac{3.5 \cdot 11}{\text{скорость} (\text{бит/с})} \cdot 1000 . \quad (1)$$

При скорости выше 19200 бит/с вместо формул используют фиксированные интервалы: 0,75 мс для t1.5 и 1,75 мс для t3.5, чтобы избежать чрезмерных срабатываний таймеров и сбоев в работе системы.

Существует три типа функций передачи [3]:

- Стандартные. Описание этих функций опубликовано и утверждено Modbus-IDA [14]. Эта категория включает в себя как опубликованные, так и свободные в настоящее время коды.
- Пользовательские. Два диапазона кодов (от 65 до 72 и от 100 до 110), для которых пользователь может создать произвольную функцию.
- Резервированные. В эту категорию входят коды функций, не являющиеся стандартными, но уже используемые в устрой-

ствах, производимых различными компаниями.

Типы данных протокола Modbus представлены на рисунке 6.

Проведя анализ, можно выделить следующие достоинства и недостатки протокола.

Достоинства. На данный момент, протокол зарекомендовал себя как надежный, проверенный временем стандарт, который претерпел много изменений с момента создания. К его преимуществам можно отнести:

- простой и легко реализуемый протокол, что делает его популярным среди разработчиков и инженеров [15]
- используется двоичный формат передачи данных, что позволяет передавать большее количество информации за меньшее время [15]

Недостатки. В настоящее время не существует совершенных протоколов. О слабостях любого протокола стоит знать, чтобы иметь возможность оценить риски, которые возникают в процессе эксплуатации той или иной технологии. Ниже перечислены несколько существенных недостатков анализируемого протокола:

- Ключевым ограничением протокола Modbus является модель «ведущий-ведомый», при которой только мастер инициирует обмен, а ведомые устройства не могут передавать данные самостоятельно.
- В протоколе отсутствует механизм аутентификации ведущего и ведомых устройств, что создает риск внедрения злоумышленни-

Параметр	Тип данных	Тип доступа
Дискретные входы (Discrete Inputs)	один бит	только чтение
Регистры флагов (Coils)	один бит	чтение и запись
Регистры ввода (Input Registers)	16-битное слово	только чтение
Регистры хранения (Holding Registers)	16-битное слово	чтение и запись

Рис. 6. Типы данных протокола Modbus

ка, выдающего себя за ведущего и получающего полный контроль над сетью.

- Также протокол не предусматривает шифрование данных при передаче по открытым каналам, что создаёт риск несанкционированного доступа. Следовательно, необходимы доработки для внедрения надёжной и простой в реализации аутентификации.

Исходя из вышеизложенного, задачами исследования являются вопросы построения метода, модели и средств противодействия угрозам нарушения информационной безопасности в открытой промышленной сети, функционирующей в режиме RTU протокола Modbus.

Целью исследования является разработка метода верификации ведущего и ведомого устройства в процесс коммуникации протокола Modbus.

Задачи:

- Анализ существующих методов верификации, используемых в протоколах с ограничениями на длину полезной нагрузки
- Построение модели злоумышленника
- Внедрение предложенных методов
- Анализ влияния предложенных методов на доступность

Решения данной проблемы основаны на использовании 3 способов верификации:

1. Временного интервала между передачей фреймов как фактора верификации мастера и слейва. Если мастер и слейвы синхронизируются об «окнах»

передачи данных, то отправителя в каждом случае можно назвать валидным.

2. 16-битной вставки с помощью операции XOR, затрагивающий последний байт PDU и первый байт CRC16. При таком варианте внедряется легковесный алгоритм подписи сообщения, что позволит нам удостовериться, что сообщение происходит с легитимным устройством.
3. Одноразовый пароль (OTP) [16], который можно вычислить для мастера и слейва в любой момент времени в случае наличия между ними договорённости о ключе. В таком случае, можно установить ключ, на основании которого высчитывается пароль, без ограничений по длине, что усложнит возможность его подобрать за разумный промежуток времени.

Вывод

Исходя из вышеизложенного, можно сделать вывод, что протокол Modbus за более чем 40 лет существования не только не утратил свою популярность, но и существенно распространился и был внедрен во многие АСУ ТП. Протокол зарекомендовал себя как надёжное решение в качестве стандарта для промышленной сети. Повышение качества использования протокола Modbus основано на построении верификационных алгоритмов процесса коммуникации на основе предложенного в работе подхода.

Литература

1. All About Fieldbus Protocols: сайт Inst Tools. [Электронный ресурс]. – Режим доступа: <https://instrumentationtools.com/fieldbus-protocols/> (дата обращения 10.03.2025).
2. Modbus. Сайт Modbus. [Электронный ресурс]. – Режим доступа: <https://www.modbus.org/specs.php> (дата обращения 05.03.2025)
3. Промышленные сети и интерфейсы. Сайт «RealLab!». [Электронный ресурс]. — Режим доступа : <https://www.reallab.ru/bookasutp/2-promishlennii-seti-i-interfeisi/2-8-modbus/> (дата обращения 05.03.2025).
4. Денисенко В. В. Протоколы и сети Modbus и Modbus TCP / Денисенко В. В. // Современные технологии автоматизации. – 2010. – № 4, с. 90 - 94.
5. RS-485: Википедия. Свободная энциклопедия. [Электронный ресурс]. – Режим доступа: <https://ru.wikipedia.org/wiki/RS-485> (дата обращения 05.03.2025)
6. Лемешко К.О. Диспетчеризация электроснабжения и система мониторинга на основе протокола modbus // Аллея науки. 2019. Т. 3. № 5 (32). С. 244-248.
7. OSI model: Википедия. Свободная энциклопедия. [Электронный ресурс]. – Режим доступа : https://en.wikipedia.org/wiki/OSI_model (дата обращения 07.03.2025)
8. Томас Д. Введение в протокол Modbus. Часть 2. Modbus Serial и Modbus TCP. Современные технологии автоматизации. – 2009. – № 3, с. 22 - 26.
9. Краткое описание протокола Modbus/RTU. Сайт «Интеллект модуль». [Электронный ресурс]. - Режим доступа: https://intellect-module.ru/downloads/manuals/inode_35D/ModBus_RTU.pdf (дата обращения 08.03.2025)
10. Введение в Modbus протокол. Сайт «Быстрые проекты». [Электронный ресурс]. - Режим доступа: https://fast-project.ru/upload/Description_Modbus_ru.pdf (дата обращения 07.03.2025)
11. Савинков А.Ю. Реализация протокола modbus rtu на микроконтроллерах семейства stm32 // Информатика: проблемы, методы, технологии. Материалы XXII Международной научно-практической конференции им. Э.К. Алгаинова. Под редакцией Д.Н. Борисова. Воронеж, 2022. С. 86-95.
12. Как общаются машины: протокол Modbus. Сайт «Хабр». [Электронный ресурс]. - Режим доступа: <https://habr.com/ru/companies/advantech/articles/450234/> (дата обращения 14.03.2025)
13. Заметки о Modbus. Сайт «ОВЕН». [Электронный ресурс]. - Режим доступа: https://ftp.owen.ru/CoDeSys3/98_Books/ModbusTips.pdf (дата обращения 12.03.2025)
14. MODBUS APPLICATION PROTOCOL SPECIFICATION V1.1b3. Сайт Modbus. [Электронный ресурс]. – Режим доступа: https://modbus.org/docs/Modbus_Application_Protocol_V1_1b3.pdf (дата обращения 14.03.2025)
15. Сальников М.С. Введение в протокол modbus rtu: основные принципы и преимущества / М.С. Сальников, А.А. Суханкин // Научное обозрение: актуальные вопросы теории и практики. Сборник статей VI Международной научно-практической конференции: в 2 ч. Том Часть 1. Пенза, 2023.
16. One-time password: Википедия. Свободная энциклопедия. [Электронный ресурс]. – Режим доступа: https://en.wikipedia.org/wiki/One-time_password (дата обращения 16.03.2025)

References

1. All About Fieldbus Protocols. Available at: <https://instrumentationtools.com/fieldbus-protocols/> (accessed 10.03.2025)
2. Modbus. Available at: <https://www.modbus.org/specs.php> (accessed 05.03.2025)
3. Promishlennii seti i interfeysi [Industrial networks and interfaces]. Available at: <https://www.reallab.ru/bookasutp/2-promishlennii-seti-i-interfeisi/2-8-modbus/> (accessed 05.03.2025)
4. Denisenko V.V. Protokoli i seti Modbus i Modbus TCP [Protocols and networks of Modbus and Modbus TCP]. Modern automation technologies, 2010, no. 4, p. 90-94. (in Russ.)
5. RS-485. Available at: <https://ru.wikipedia.org/wiki/RS-485> (accessed 05.03.2025)
6. Lemeshko K.O. Dispetcherizaciya elektrosnabzheniya i sistema monitoring na osnove protokola modbus [Power supply dispatching and monitoring system based on modbus protocol]. Alley of Science, 2019, vol. 3, no. 5 (32), p. 244-248. (in Russ.)
7. OSI model. Available at: https://en.wikipedia.org/wiki/OSI_model (accessed 07.03.2025)
8. Tomas D. Vvedenie v protokol Modbus. Chast 2. Modbus serial i Modbus TCP [Introduction to Modbus protocol. Part 2. Modbus serial and Modbus TCP]. Modern automation technologies, 2009, no. 3, p. 22-26. (in Russ.)

9. Kratkoe opisanie protokola Modbus/RTU [Brief description of the Modbus/RTU protocol]. Available at: https://intellect-module.ru/downloads/manuals/inode_35D/ModBus_RTU.pdf (accessed 08.03.2025)
 10. Vvedenie v Modbus protocol [Introduction to Modbus protocol]. Available at: https://fast-project.ru/upload/Description_Modbus_ru.pdf (accessed 07.03.2025)
 11. Savinkov A.U. [Implementation of the Modbus Rtu Protocol on Microcontrollers of the Stm32 Family]. Informatika: problemi, metodi, tehnologii [Computer Science: Problems, Methods, Technologies]. Voronezh, 2022, pp. 86-95. (in Russ.)
 12. Kak obsjyautsa mashini. Protokol Modbus [How Machines Communicate: The Modbus Protocol]. Available at: <https://habr.com/ru/companies/advantech/articles/450234/> (accessed 14.03.2025)
 13. Zametki o Modbus [Notes on Modbus]. Available at: https://ftp.owen.ru/CoDeSys3/98_Books/ModbusTips.pdf (accessed 12.03.2025)
 14. MODBUS APPLICATION PROTOCOL SPECIFICATION V1.1b3. Available at: https://modbus.org/docs/Modbus_Application_Protocol_V1_1b3.pdf (accessed 14.03.2025)
 15. Salnikov M.S. [Introduction to Modbus Rtu Protocol: Basic Principles and Advantages]. Nauchnoe obozrenie: aktualnie voprosi teorii i praktiki [Scientific Review: Current Issues of Theory and Practice]. Penza, vol. 1, 2023.
 16. One-time password. Available at: https://en.wikipedia.org/wiki/One-time_password (accessed 16.03.2025)
-

ЮЖАКОВ Александр Анатольевич, доктор технических наук, профессор, заведующий кафедрой Автоматики и телемеханики, Пермский национальный исследовательский политехнический университет (ПНИПУ). 614990, Пермский край, г. Пермь, Комсомольский проспект, д. 29. E-mail: uz@at.pstu.ru

КРОТОВА Елена Львовна, кандидат физико-математических наук, доцент кафедры Высшей математики, Пермский национальный исследовательский политехнический университет (ПНИПУ). 614990, Пермский край, г. Пермь, Комсомольский проспект, д. 29. E-mail: lenkakrotova@yandex.ru

ОЩЕПКОВ Никита Владимирович, аспирант кафедры Автоматики и телемеханики, Пермский национальный исследовательский политехнический университет (ПНИПУ). 614990, Пермский край, г. Пермь, Комсомольский проспект, д. 29. E-mail: maserati_2000@mail.ru

YUZHAKOV Alexander Anatolyevich, Doctor of Technical Sciences, Professor, Head of the Department of Automation and Telemechanics, Perm National Research Polytechnic University (PNIPU). 614990, Perm Region, Perm, Komsomolsky Prospekt, 29. E-mail: uz@at.pstu.ru

KROTOVA Elena Lvovna, Candidate of Physical and Mathematical Sciences, Associate Professor of the Department of Higher Mathematics, Perm National Research Polytechnic University (PNIPU). 614990, Perm Krai, Perm, Komsomolsky Prospekt, 29. E-mail: lenkakrotova@yandex.ru

OSHCHERPKOV Nikita Vladimirovich, postgraduate student of the Department of Automation and Telemechanics, Perm National Research Polytechnic University (PNIPU). 614990, Perm Region, Perm, Komsomolsky Prospekt, 29. E-mail: maserati_2000@mail.ru