УДК 004.056.53 Вестник УрФО № 2(60) / 2026, с. 88–97

Ощепков Н.В.

DOI: 10.14529/secur260209

ОЦЕНКА ВЛИЯНИЯ МЕТОДОВ ВЕРИФИКАЦИИ ОТПРАВИТЕЛЯ НА БЫСТРОДЕЙСТВИЕ СИСТЕМЫ УПРАВЛЕНИЯ РЕЛЕЙНО-ПУСКОВЫМ БЛОКОМ ШТАНГОВОГО ГЛУБИННОГО НАСОСА ПРИ РАЗЛИЧНЫХ ТАКТОВЫХ ЧАСТОТАХ МИКРОКОНТРОЛЛЕРА

В статье выполнена оценка влияния методов верификации отправителя команд на быстродействие системы управления релейно-пусковым блоком штангового глубинного насоса, функционирующей на основе протокола Modbus RTU. Исследование проводилось непосредственно на объекте внедрения – скважине №309 куста №4 Чернушинского месторождения – при пяти тактовых частотах микроконтроллера ESP32, используемого в составе ведомого устройства: 20, 40, 80, 160 и 240 МГц, и трёх значениях битрейта: 9600, 19200 и 115200 бит/с, при длине линии RS-485 50 м. Показано, что увеличение битрейта и тактовой частоты микроконтроллера сужает разброс задержек доставки кадра, что позволяет обоснованно уменьшить длительность временного окна верификации и тем самым снизить вероятность успешной реализации атаки подмены мастера. Быстродействие системы в рабочем режиме определяется канальной задержкой RS-485, что обосновывает применимость разработанных методов на микроконтроллерных платформах с различными тактовыми характеристиками без ущерба для быстродействия системы управления.

Ключевые слова: *Modbus RTU, RS-485, верификация отправителя, XOR-аутентификация, HMAC-SHA1.*

EVALUATION OF THE IMPACT OF SENDER VERIFICATION METHODS ON THE PERFORMANCE OF THE CONTROL SYSTEM FOR A PUMP RELAY-START UNIT AT VARIOUS MICROCONTROLLER CLOCK FREQUENCIES

This article evaluates the impact of command-sender verification methods on the response speed of a control system for a pump relay-start unit operating via the Modbus RTU protocol. The study was conducted at the actual deployment site-Well No. 309, Cluster No. 4 of the Chernushinskoye oil field-using an ESP32 microcontroller as the slave device. Testing involved five clock frequencies (20, 40, 80, 160, and 240 MHz) and three bitrates (9,600, 19,200, and 115,200 bps) over a 50-meter RS-485 line. The results demonstrate that increasing the bitrate and microcontroller clock frequency reduces the variance in frame delivery latency; this allows for a justified reduction in the verification time window, thereby lowering the probability of a successful master-spoofing attack. Under normal operating conditions, system speed is determined by RS-485 channel latency, confirming the suitability of the developed methods for microcontroller platforms with varying clock speeds without compromising control system performance.

Keywords: *Modbus RTU, RS-485, sender verification, XOR authentication, HMAC-SHA1.*

Введение

Протокол Modbus RTU, разработанный компанией Modicon в 1979 году, по сей день остаётся одним из наиболее распространённых транспортных протоколов в промышленных системах управления – АСУ ТП, SCADA и «интернет вещей» (IoT) [1]. В нефтяной промышленности он традиционно используется для дистанционного управления приводным оборудованием скважин, в том числе релейно-пусковыми блоками штанговых глубинных насосов (ШГН). Вместе с тем протокол проектировался без учёта требований информационной безопасности: он не предусматривает ни механизмов аутентификации участников обмена, ни шифрования передаваемых данных.

Отсутствие аутентификации и шифрования в протоколе Modbus/TCP позволяет злоумышленнику реализовать атаку типа «человек посередине» (MITM), перехватывая и модифицируя трафик между SCADA-системой и программируемым логическим контроллером (ПЛК), а также внедряя ложные команды от имени легитимного мастера [2]. Практическая опасность таких уязвимостей подтверждается реальными инцидентами: в январе 2024 года вредоносная программа FrostyGoop, эксплуатирующая незащищённый протокол Modbus, была применена в кибератаке на предприятие теплоснабжения – более 600 жилых домов остались без отопления на двое суток при отрицательных температурах [3].

Katulić и соавторы предложили использо-

вание кодов аутентификации сообщений (MAC) для Modbus/TCP и экспериментально подтвердили их практическую применимость в промышленных сетях [4]. Для ресурсоограниченных устройств класса IIoT предложены лёгкие протоколы аутентификации на основе операций XOR и хэш-функций, обеспечивающие небольшое время выполнения при формально подтверждённой защищённости [5].

Калинкин Я.В. и Тутов И.А. разработали программно-аппаратный модуль фильтрации кадров Modbus RTU по белым спискам допустимых значений полей, однако данный подход не предусматривает верификации источника команды и не защищает от атаки подмены мастера [6].

Безукладников И.И. и Кон Е.Л. предложили универсальный подход к организации скрытых каналов в распределённых АСУ, проанализировали шлюз LonWorks–Internet и разработали способ организации скрытого канала в системе управления интеллектуальным зданием [7]. Капгер И.В., Сизов В.П. и Южаков А.А. разработали алгоритм потокового шифрования для промышленных сетей LON на основе функции косинуса с 48-битным ключом аутентификации и динамической сменой сессионных ключей каждые 256 циклов [8]. Капгер И.В. в диссертационном исследовании рассматривал проблему повышения уровня конфиденциальности в промышленных сетях систем автоматизации испытаний, разработав методы и средства криптографической защиты передаваемых данных применительно к ресурсоограниченным узлам промышленных сетей [9].

В работе Попова П.А., Розенберга Е.Н., Сабанова А.Г. и Шубинского И.Б. сформулированы концепции безопасности верхнего уровня управления АСУ ТП ЖТ как объектов критической информационной инфраструктуры (КИИ), включая концепции защищённой среды, взаимозависимости функциональной и информационной безопасности и единой модели угроз [10]. Dontha J.D. исследовала применение граничных вычислений в ICS, предложив многоуровневую архитектуру, объединяющую машинное обучение, блокчейн и шифрование для снижения задержек и повышения устойчивости к кибератакам [11].

Ádámkó É., Jakabóczki G. и Szemes P.T. предложили протокол защиты Modbus RTU на основе схемы разделения секрета Шамира с взаимной аутентификацией и AES-шифрованием без изменения структуры стандартного кадра, подтверждённый апробацией на реальном устройстве сбора данных [12]. Грешонков А.М. и Моисеев В.С. обосновали применение машинного обучения для выявления аномалий в IIoT-системах и предложили многоуровневую архитектуру системы безопасности с поддержкой протоколов Modbus, MQTT и OPC-UA [13].

Шигапов И.И., Ильмушкина А.А. и Юсупова А.С. разработали концептуальную архитектуру самоорганизующихся IIoT-сетей на базе IEEE 802.15.4/802.15.5, интегрирующую эллиптическую криптографию, пороговые схемы Шамира и модель управления доверием на основе риск-скора [14]. Patel H.S., Gautam C.S. и Waoo A.A. экспериментально показали на выборке из 120 устройств, что blockchain-механизмы и машинное обучение обеспечивают наивысшую эффективность обнаружения атак – 96% и 94% соответственно [15]. Santhiya R. и Barakath Begam A. установили, что интеграция SDN и провайдеров управления безопасностью существенно повышает защищённость IoT-устройств «умного дома», тогда как протоколы MQTT и CoAP требуют обязательного дополнения уровнем TLS/DTLS [16]. Таржанов Т.В. и Новиков С.Н. выполнили имитационное моделирование DoS-атаки на виртуальную IoT-сеть и подтвердили эффективность защиты посредством межсетевого экранирования средствами POX-контроллера [17].

Таким образом, анализ литературы показывает, что тематика защиты промышленных коммуникационных протоколов – в первую очередь Modbus RTU – в контексте АСУ ТП, IoT и IIoT вызывает устойчивый исследовательский интерес: работы охватывают широкий спектр подходов от лёгких криптографических протоколов и схем разделения секрета до методов машинного обучения и архитектур граничных вычислений, однако специфика последовательной шины RS-485 с жёсткими ресурсными ограничениями ведомых устройств и проблема верификации отправителя команд остаются недостаточно изученными областями.

Ранее автором был разработан и внедрён механизм верификации отправителя команд для системы управления релейно-пусковым блоком ШГН на скважине №309 куста №4 Чернушинского месторождения предприятия ООО «РОССМА» [18]. Механизм включает три компонента: метод XOR-аутентификации с 16-битным ключом [19], метод верификации на основе периодически открываемых вре-

менных окон с криптографическим согласованием параметров на базе HMAC-SHA1 [20], а также их комбинацию. По результатам натурных испытаний вероятность успешной реализации атаки подмены мастера при комбинированном методе составила $P \approx 3{,}27 \cdot 10^{-6}$.

В ходе эксплуатации системы был поставлен практический вопрос: как ведут себя разработанные методы верификации при изменении тактовой частоты микроконтроллера ведомого устройства? ESP32, применяемый в составе релейно-пускового блока, допускает программное переключение тактовой частоты ядра между штатными значениями 80, 160 и 240 МГц, а также может эксплуатироваться на пониженных частотах (20 и 40 МГц) с целью снижения энергопотребления или тепловыделения. Расширение парка устройств на аналогичных объектах предполагает использование платформ с различными тактовыми характеристиками, что ставит задачу обоснования переносимости разработанных методов без перенастройки параметров верификации.

Представленные результаты настоящего исследования состоят в следующем:

1. Выполнена количественная оценка влияния тактовой частоты микроконтроллера ESP32 (20 – 240 МГц) и битрейта RS-485 (9600 – 115 200 бит/с) на джиттер задержки доставки кадра Modbus RTU в условиях реальной промышленной эксплуатации.

2. Обоснована возможность динамического сужения параметра D (длительности временного окна верификации) на основе измеренного диапазона джиттера канала без потери надёжности приёма легитимных кадров.

3. Показана применимость разработанных методов верификации на микроконтроллерных платформах с различными тактовыми характеристиками без ущерба для быстродействия системы управления.

Объектом исследования является система дистанционного управления приводным комплексом (СДУПК) ШГН на скважине №309 куста №4 Чернушинского месторождения, подробно описанная в [18]. Система построена по топологии шины с протоколом «ведущий-ведомый». Ведущим устройством является АРМ оператора на базе ПК с адаптером USB-RS-485 [21]. Ведомыми устройствами выступают датчики и управляющее устройство релейно-пускового блока на базе микроконтроллера ESP32 под управлением MicroPython. Управление состоянием привода насоса осуществляется командой записи дискретного выхода с адресом 0x0000 посредством функционального кода FC05. Физическая среда передачи – двухпроводная линия RS-485, длина шины 50 м. Структурная схема СДУПК приведена на рис. 1. Система включает в себя ведущее устройство (мастер) и 6 ведомых устройств: датчик подсчёта количества наклонов, релейно-пусковой блок, динамограф, датчик давления, датчик температуры двигателя и датчик угла наклона.

Материалы и методы

Механизм верификации отправителя реализован в прошивке ESP32 ведомого устройства релейно-пускового блока и включает два метода, применяемых совместно.

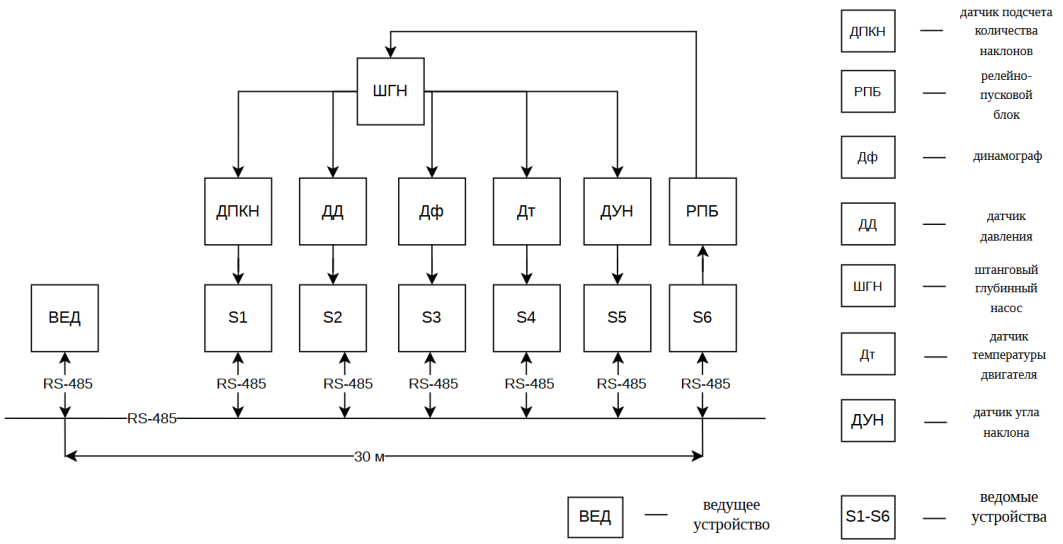

Рис. 1. Структурная схема системы дистанционного управления ШГН скважины

Метод XOR-аутентификации, при котором поле данных каждого исходящего кадра FC05 гаммируется мастером с использованием 16-битного разделяемого ключа K посредством операции побитового исключающего ИЛИ. Ведомое устройство при приёме выполняет обратную операцию и проверяет корректность результата. Вероятность того, что случайный кадр злоумышленника пройдёт XOR-проверку, равна $3{,}05 \cdot 10^{-5}$ (при заданном ключе равном 16 бит).

Метод временных окон. Ведомое устройство принимает кадры только в течение периодически открываемых временных окон. Параметры окон передаются мастером в кадре контракта с использованием функциональных кодов из пользовательского диапазона спецификации Modbus (65 – 72) с криптографическим согласованием на базе HMAC-SHA1 [20]. Параметр D задаёт длину временного окна: легитимный кадр считается действительным, если он поступил в интервале [0; D] от момента открытия окна. Параметр T задаёт длительность закрытого интервала между окнами. Полный период составляет D + T. Вероятность того, что произвольный кадр злоумышленника попадёт в открытое окно:

$$P_W = \frac{D}{T+D}. \quad (1)$$

Комбинированный метод является сочетанием обоих методов. События «кадр попал в окно» и «кадр прошёл XOR-проверку» независимы, поэтому вероятность успешной атаки подмены мастера:

$$P_{W\_XOR} = \frac{D}{2^{15} \cdot (T+D)}. \quad (2)$$

При подстановке исходных параметров объекта внедрения [18] D = 30 мс, T = 250 мс в формулу (2) вероятность реализации атаки подмены и отправки кадра на ведомое устройство составляет $3{,}27 \cdot 10^{-6}$.

Методика измерений

Для оценки влияния тактовой частоты микроконтроллера и битрейта на джиттер доставки кадра измерения проводились непосредственно на объекте внедрения при трёх значениях битрейта (9600, 19200 и 115200 бит/с) и пяти тактовых частотах ESP32 (20, 40, 80, 160 и 240 МГц). Переключение тактовой частоты осуществлялось программно средствами MicroPython (machine.freq()). Для каждой из 15 комбинаций параметров формировалась выборка объёмом n = 1000 измерений задержки доставки кадра в установившемся режиме работы системы.

По каждой выборке фиксировался наблюдаемый диапазон задержек [D_{min}, D_{max}]. Фиксация значения момента времени попадания кадра мастера на ведомое устройство в рамках временного интервала приема сообщения производилась ведомым устройством благодаря встроенной в MicroPython функции time.ticks_us в момент получения первого байта кадра. На основе этого диапазона вычислялось скорректированное минимально допустимое значение параметра $D_{корр}$. Скорректированное значение $D_{корр}$ вычислялось как разность между исходным параметром окна D = 30 мс и наблюдаемым минимумом задержки D_{min} с добавлением страхового запаса в 2 – 3 мс для исключения ложных отказов при приёме легитимных кадров.

Результаты

Анализ данных, представленных в табл.1 и на рис. 2 – 4, позволяет выявить ряд закономерностей. Наиболее существенное влияние на величину джиттера оказывает увеличение битрейта: с ростом скорости передачи диапазон его значений уменьшается. Это связано с тем, что при более высоком битрейте время передачи каждого байта сокращается, вследствие чего уменьшается общая длительность передачи кадра и снижается временной разброс его доставки. Так, при скорости передачи 19200 бит/с становится возможным уменьшение длительности окна D с 30 до 12 мс. В результате при значении T = 250 мс вероятность успешной реализации атаки подмены кадра, рассчитанная по формуле (2), снижается до $1{,}40 \cdot 10^{-6}$.

Во-вторых, влияние тактовой частоты микроконтроллера на диапазон джиттера проявляется по-разному в зависимости от битрейта. При 19200 бит/с – рабочей скорости объекта внедрения – диапазон [D_{min}, D_{max}] практически не изменяется при смене частоты от 20 до 240 МГц, а значение $D_{корр}$ = 12 мс одинаково для всех пяти частот. При 9600 бит/с повышение частоты с 20 до 240 МГц позволяет сократить $D_{корр}$ с 25 до 22 мс. Наиболее выраженный эффект наблюдается при 115200 бит/с: повышение частоты с 20 до 240 МГц сокращает $D_{корр}$ с 7 до 4 мс – сужение почти вдвое.

Обсуждение

Наблюдаемые закономерности объясняются соотношением двух составляющих суммарной задержки доставки кадра: канальной задержки, определяемой временем побитовой передачи по линии RS-485, и программ-

Таблица 1

Диапазон задержек доставки кадра и скорректированное значение Dкорр при различных битрейтах и тактовых частотах ESP32

Битрейт, бит/с	Частота, МГц	D_{min} – D_{max}, мс	$D_{корр}$, мс
9600	20	6 – 20	25
	40	7 – 19	24
	80	8 – 18	23
	160	9 – 17	22
	240	9 – 16	22
19 200	20	18 – 25	12
	40	19 – 25	12
	80	19 – 25	12
	160	19 – 25	12
	240	20 – 25	12
115 200	20	25 – 29	7
	40	26 – 29	6
	80	27 – 29	5
	160	28 – 29	5
	240	28 – 29	4

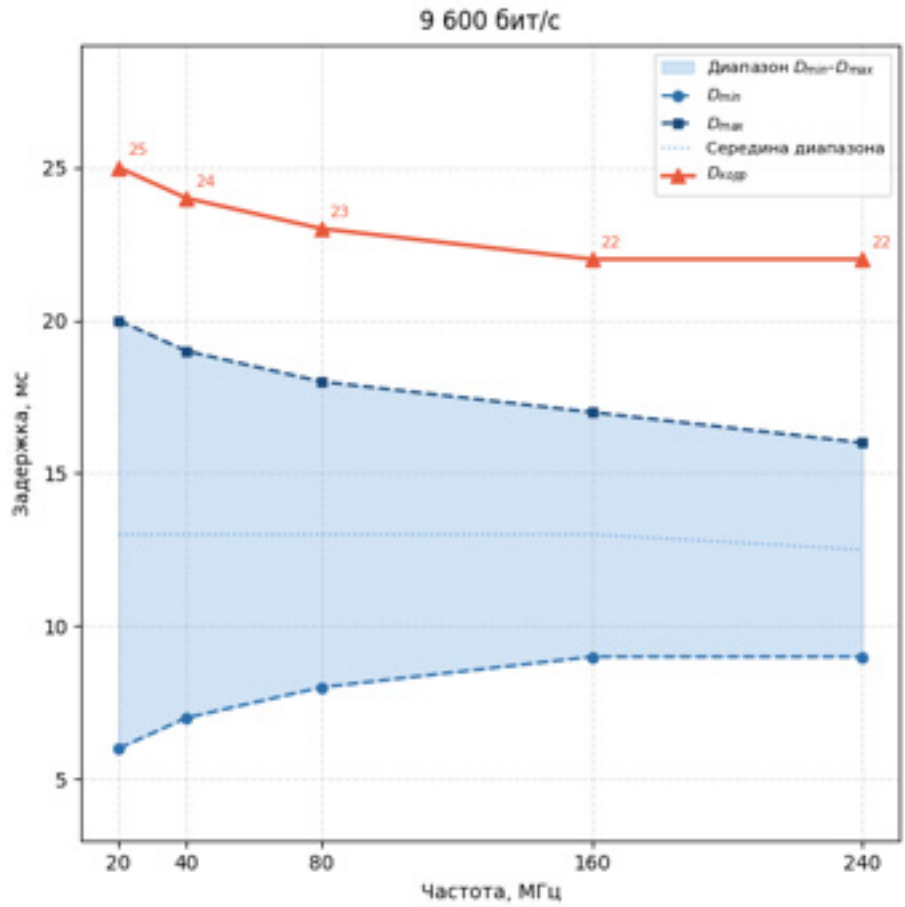

Рис. 2. Распределение задержек Modbus по битрейту при 9600 бит /с

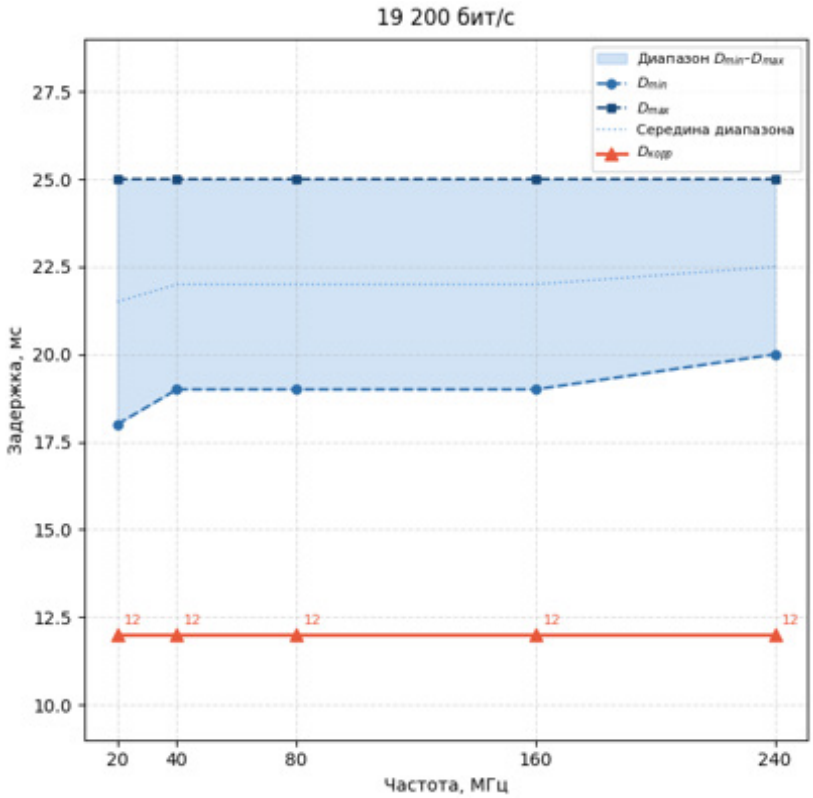

Рис. 3. Распределение задержек Modbus по битрейту при 19200 бит /с

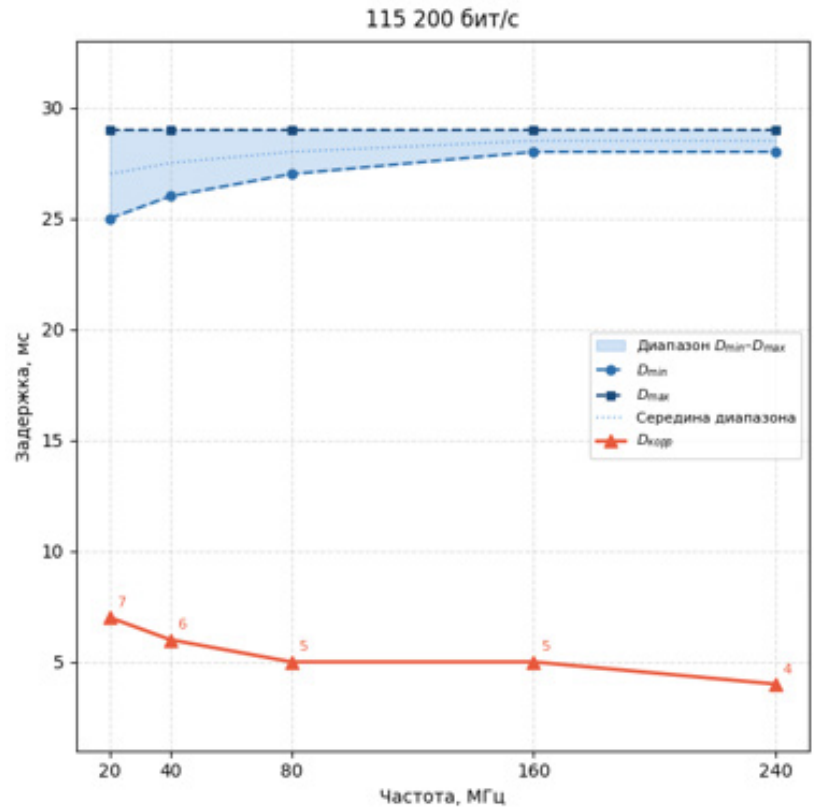

Рис. 4. Распределение задержек Modbus по битрейту при 115200 бит /с

ной задержки, обусловленной временем реакции стека MicroPython на прерывание UART.

При битрейте 19200 бит/с время передачи кадра по каналу является доминирующей составляющей задержки и полностью маскирует вариацию программной задержки обработки прерывания. Независимо от тактовой частоты ядра ESP32 суммарный джиттер определяется физическим каналом RS-485, что и объясняет постоянство $D_{корр}$ = 12 мс во всём диапазоне 20 – 240 МГц.

При битрейте 115200 бит/с время передачи кадра сокращается примерно в шесть раз по сравнению с 19200 бит/с, и программная составляющая задержки становится сопоставимой с канальной. В этом режиме тактовая частота микроконтроллера начинает существенно влиять на джиттер, что и даёт наблюдаемый эффект двукратного сужения $D_{корр}$ при увеличении частоты с 20 до 240 МГц.

Заключение

При рабочей скорости объекта внедрения 19200 бит/с значение $D_{корр}$ = 12 мс не зависит от тактовой частоты микроконтроллера в диапазоне 20 – 240 МГц. Это означает, что исходный параметр окна D = 30 мс, установленный при внедрении, может быть безопасно сокращён до 12 мс без риска ложных отказов при приёме легитимных кадров и без перенастройки при смене тактовой частоты. Сокращение окна с 30 до 12 мс уменьшает вероятность успешной атаки подмены мастера с $3{,}27 \cdot 10^{-6}$ до $1{,}40 \cdot 10^{-6}$, то есть более чем вдвое, при этом не требуя ни повторных натурных измерений, ни изменений в алгоритме верификации, ни модификации аппаратной конфигурации системы. Дополнительным следствием является возможность перевода микроконтроллера на пониженную тактовую частоту – например, с 240 МГц до 80 МГц или ниже – с целью снижения энергопотребления или тепловыделения в условиях промышленной эксплуатации, без какого-либо ущерба для корректности работы механизма верификации при данном битрейте. Следует отметить, что при битрейте 115 200 бит/с тактовая частота микроконтроллера уже оказывает заметное влияние на джиттер, и повышение частоты с 20 до 240 МГц позволяет сократить $D_{корр}$ почти вдвое – с 7 до 4 мс. Это свидетельствует о том, что при наличии возможности дальнейшего увеличения тактовой частоты микроконтроллера сверх 240 МГц джиттер мог бы сузиться ещё больше, что позволило бы дополнительно уменьшить параметр D и тем самым повысить защищённость системы от атаки подмены мастера без каких-либо изменений в алгоритме верификации.

Литература

1. Modbus Protocol Specification [Электронный ресурс]. – Режим доступа: https://www.modbus.org/file/secure/modbusprotocolspecification.pdf. – Дата обращения: 05.06.2026.

2. Parian C., Guldimann T., Bhatia S. Fooling the Master: Exploiting Weaknesses in the Modbus Protocol [Электронный ресурс] // Procedia Computer Science. – 2020. – Vol. 171. – P. 2453–2458. – DOI: 10.1016/j.procs.2020.04.265. – URL: https://www.sciencedirect.com/science/article/pii/S1877050920312576 (дата обращения: 10.06.2026).

3. Нефёдова М. Вредонос FrostyGoop нацелен на промышленные системы управления [Электронный ресурс] // Хакер. – 2024. – 24 июля. – URL: https://xakep.ru/2024/07/24/frostygoop/ (дата обращения: 10.06.2026).

4. Katulić F., Sumina D., Groš S., Erceg I. Protecting Modbus/TCP-Based Industrial Automation and Control Systems Using Message Authentication Codes // IEEE Access. – 2023. – Vol. 11. – P. 47007–47023. – DOI: 10.1109/ACCESS.2023.3274592. – URL: https://ieeexplore.ieee.org/document/10122945 (дата обращения: 10.06.2026).

5. Lara E., Aguilar L., Sanchez M.A., García J.A. Lightweight Authentication Protocol for M2M Communications of Resource-Constrained Devices [Электронный ресурс] // Sensors. – 2020. – Vol. 20, No. 2. – Art. no. 501. – DOI: 10.3390/s20020501. – URL: https://www.mdpi.com/1424-8220/20/2/501 (дата обращения: 10.06.2026).

6. Калинкин Я.В., Тутов И.А. Модуль информационной безопасности в сетях Modbus RTU // Электронные средства и системы управления: материалы XVIII Международной научно-практической конференции, 16–18 ноября 2022 г. – Томск, 2022. – С. 57–60.

7. Безукладников И.И., Кон Е.Л. Скрытые каналы в распределенных автоматизированных системах // Вестник УГАТУ. – 2010. – Т. 14, № 2(37). – С. 245–250.

8. Капгер И.В., Сизов В.П., Южаков А.А. Криптографическое преобразование сообщений, передаваемых в промышленных сетях LON // Вопросы защиты информации. – 2010. – № 1(88). – С. 28–43.

9. Капгер И.В. Повышение уровня конфиденциальности в промышленных сетях систем автоматизации испытаний: дис. ... канд. техн. наук: 05.13.19. – Пермь, 2012. – 175 с.

10. Попов П.А., Розенберг Е.Н., Сабанов А.Г., Шубинский И.Б. Концепции обеспечения комплексной безопасности АСУ ТП верхнего уровня управления для объектов КИИ железнодорожного транспорта // Надёжность. – 2025. – Т. 25, № 3. – С. 42–49.

11. Dontha J.D. Edge Computing and Security in Industrial Control Systems // International Scientific Journal of Engineering and Management. – 2023. – Vol. 2, No. 9. – DOI: 10.55041/ISJEM01305.

12. Ádámkó É., Jakabóczki G., Szemes P.T. Proposal of a Secure Modbus RTU Communication with Adi Shamir›s Secret Sharing Method // International Journal of Electronics and Telecommunications. – 2018. – Vol. 64, No. 2. – P. 107–114. – DOI: 10.24425/119357.

13. Грешонков А.М., Моисеев В.С. Интеллектуальные системы обеспечения информационной безопасности в промышленном интернете вещей (IIoT) // Регион: системы, экономика, управление. – 2026. – № 4(71). – С. 210–211.

14. Шигапов И.И., Ильмушкина А.А., Юсупова А.С. Самоорганизующиеся беспроводные сети IIoT с учётом приоритетов безопасности // Экономика и управление: проблемы, решения. – 2025. – Т. 8, № 6(159). – С. 71–78.

15. Patel H.S., Gautam C.S., Waoo A.A. Advanced Security Vulnerabilities and Defense Mechanisms in IoT Networks // International Scientific Journal of Engineering and Management. – 2026. – Vol. 5, No. 6.

16. Santhiya R., Barakath Begam A. IoT Network Security in Smart Homes // International Scientific Journal of Engineering and Management. – 2026. – Vol. 5, No. 4.

17. Таржанов Т.В., Новиков С.Н. Исследование угроз информационной безопасности в приложениях IoT и методов защиты от этих угроз // Интерэкспо Гео-Сибирь. – 2021. – Т. 7, № 2. – С. 184–189.

18. Ощепков Н.В. механизм верификации отправителя команд в протоколе Modbus RTU: разработка и апробация на приводном оборудовании штангового глубинного насоса // Научно-технический вестник Поволжья. Научный журнал. №4, 2026. – С. 253-259.

19. Исключающее «или» // Википедия: [сайт]. – URL: https://ru.wikipedia.org/wiki/Исключающее_«или» (дата обращения: 09.06.2026).

20. RFC 4226: HOTP: An HMAC-Based One-Time Password Algorithm [Электронный ресурс]. – Режим доступа: https://www.rfc-editor.org/info/rfc4226. – Дата обращения: 05.06.2026.

21. RS-485 // Википедия: [сайт]. – URL: https://ru.wikipedia.org/wiki/RS-485 (дата обращения: 06.06.2026).

References

1. Modbus Protocol Specification [Electronic resource]. – Mode of access: https://www.modbus.org/file/secure/modbusprotocolspecification.pdf. – Date of access: 05.06.2026.

2. Parian C., Guldimann T., Bhatia S. Fooling the Master: Exploiting Weaknesses in the Modbus Protocol // Procedia Computer Science. – 2020. – Vol. 171. – P. 2453–2458. – DOI: 10.1016/j.procs.2020.04.265.

3. Nefyodova M. FrostyGoop malware targets industrial control systems [Vredonos FrostyGoop natseleen na promyshlennye sistemy upravleniya] // Haker [Hacker]. – 2024. – 24 July. – URL: https://xakep.ru/2024/07/24/frostygoop/ (date of access: 10.06.2026).

4. Katulić F., Sumina D., Groš S., Erceg I. Protecting Modbus/TCP-Based Industrial Automation and Control Systems Using Message Authentication Codes // IEEE Access. – 2023. – Vol. 11. – P. 47007–47023. – DOI: 10.1109/ACCESS.2023.3274592.

5. Lara E., Aguilar L., Sanchez M.A., García J.A. Lightweight Authentication Protocol for M2M Communications of Resource-Constrained Devices // Sensors. – 2020. – Vol. 20, No. 2. – Art. no. 501. – DOI: 10.3390/s20020501.

6. Kalinkin Ya.V., Tutov I.A. Information security module for Modbus RTU networks [Modul informatsionnoy bezopasnosti v setyakh Modbus RTU] // Elektronnye sredstva i sistemy upravleniya [Electronic Tools and Control Systems]: proceedings of the XVIII International Scientific and Practical Conference, 16–18 November 2022, Tomsk. – Tomsk, 2022. – P. 57–60.

7. Bezukladnikov I.I., Kon E.L. Covert channels in distributed automated systems [Skrytye kanaly v raspredelennykh avtomatizirovannykh sistemakh] // Vestnik Ufimskogo gosudarstvennogo aviatsionnogo tekhnicheskogo universiteta [Bulletin of Ufa State Aviation Technical University]. – 2010. – Vol. 14, No. 2(37). – P. 245–250.

8. Kapger I.V., Sizov V.P., Yuzhakov A.A. Cryptographic transformation of messages transmitted in LON industrial networks [Kriptograficheskoe preobrazovanie soobshcheniy, peredavaemykh v promyshlennykh setyakh LON] // Voprosy zashchity informatsii [Information Security Issues]. – 2010. – No. 1(88). – P. 28–43.

9. Kapger I.V. Improving the level of confidentiality in industrial networks of test automation systems: dissertation ... candidate of technical sciences: 05.13.19 [Povyshenie urovnya konfidentsialnosti v promyshlennykh setyakh sistem avtomatizatsii ispytaniy]. – Perm, 2012. – 175 p.

10. Popov P.A., Rozenberg E.N., Sabanov A.G., Shubinskiy I.B. Concepts of ensuring comprehensive security of upper-level control systems for critical information infrastructure objects of railway transport [Kontseptsii obespecheniya kompleksnoy bezopasnosti ASU TP verhnego urovnya upravleniya dlya obektov KII zheleznodorozhnogo transporta] // Nadyozhnost [Reliability]. – 2025. – Vol. 25, No. 3. – P. 42–49.

11. Dontha J.D. Edge Computing and Security in Industrial Control Systems // International Scientific Journal of Engineering and Management. – 2023. – Vol. 2, No. 9. – DOI: 10.55041/ISJEM01305.

12. Ádámkó É., Jakabóczki G., Szemes P.T. Proposal of a Secure Modbus RTU Communication with Adi Shamir›s Secret Sharing Method // International Journal of Electronics and Telecommunications. – 2018. – Vol. 64, No. 2. – P. 107–114. – DOI: 10.24425/119357.

13. Greshonkov A.M., Moiseev V.S. Intelligent systems for ensuring information security in the Industrial Internet of Things (IIoT) [Intellektualnye sistemy obespecheniya informatsionnoy bezopasnosti v promyshlennom interne veshchey (IIoT)] // Region: sistemy, ekonomika, upravlenie [Region: Systems, Economics, Management]. – 2026. – No. 4(71). – P. 210–211.

14. Shigapov I.I., Ilmushkina A.A., Yusupova A.S. Self-organizing wireless IIoT networks taking into account security priorities [Samorganizuyushchiesya besprovodnye seti IIoT s uchyotom prioritetov bezopasnosti] // Ekonomika i upravlenie: problemy, resheniya [Economics and Management: Problems, Solutions]. – 2025. – Vol. 8, No. 6(159). – P. 71–78.

15. Patel H.S., Gautam C.S., Waoo A.A. Advanced Security Vulnerabilities and Defense Mechanisms in IoT Networks // International Scientific Journal of Engineering and Management. – 2026. – Vol. 5, No. 6.

16. Santhiya R., Barakath Begam A. IoT Network Security in Smart Homes // International Scientific Journal of Engineering and Management. – 2026. – Vol. 5, No. 4.

17. Tarzhanov T.V., Novikov S.N. Study of information security threats in IoT applications and methods of protection against these threats [Issledovanie ugroz informatsionnoy bezopasnosti v prilozheniyakh IoT i metodov zashchity ot etikh ugroz] // InterEkspo Geo-Sibir. – 2021. – Vol. 7, No. 2. – P. 184–189.

18. Oshchepkov N.V. Sender verification mechanism for commands in the Modbus RTU protocol: development and testing on drive equipment of a sucker rod pump [Mekhanizm verifikatsii otpravitelya komand v protokole Modbus RTU: razrabotka i aprobatsiya na privodnom oborudovanii shtangovogo glubinnogo nasosa] // Nauchno-tekhnicheskiy vestnik Povolzhya [Scientific and Technical Bulletin of the Volga Region]. – 2026. – No. 4. – P. 253–259.

19. Exclusive or [Isklyuchayushcheye "ili"] // Wikipedia: the Free Encyclopedia [Vikipediya: Svobodnaya entsiklopediya]. – URL: https://ru.wikipedia.org/wiki/Исключающее_«или» (date of access: 09.06.2026).

20. RFC 4226: HOTP: An HMAC-Based One-Time Password Algorithm [Electronic resource]. – Mode of access: https://www.rfc-editor.org/info/rfc4226. – Date of access: 05.06.2026.

21. RS-485 // Wikipedia: the Free Encyclopedia [Vikipediya: Svobodnaya entsiklopediya]. – URL: https://ru.wikipedia.org/wiki/RS-485 (date of access: 06.06.2026).

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

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