Методы и системы обработки информации

DOI 10.24412/2221-2574-2023-2-56-72 УДК 004.75

ПРОТОКОЛ АУТЕНТИФИКАЦИИ РАСПРЕДЕЛЁННОЙ СИСТЕМЫ СБОРА ДАННЫХ ПО ТЕХНОЛОГИИ БЛОКЧЕЙН ДЛЯ УМЕНЬШЕНИЯ ЭНЕРГОПОТРЕБЛЕНИЯ

Лукьянчиков Андрей Владимирович
кандидат технических наук, доцент кафедры «Инновационные телекоммуникационные технологии» Института радиоэлектроники и интеллектуальных технических систем ФГАОУ ВО «Севастопольский государственный университет».
E-mail: brain75@mail.ru

Адрес: 602264, Российская Федерация, г. Севастополь, ул. Университетская, д. 33.

Аннотация: Предложен способ уменьшения энергопотребления терминальных устройств в системе городского информационного портала, агрегирующего данные мониторинга окружающей среды и результатов аналитики. Способ заключается в модификации известного протокола «Wialon IPS» с целью уменьшения времени передачи модема и как следствие, уменьшения расхода энергии. Уменьшить время передачи удалось за счёт отказа от постоянной, начальной процедуры аутентификации. Предлагается не проводить аутентификацию при каждом сеансе связи, а только первый раз и затем поддерживать её с использованием технологии блокчейн. Для первоначальной аутентификации решена задача безопасной передачи путем модификации пакета логина. В решении предлагается убрать из открытого вида передачу логина и пароля.

Ключевые слова: распределённая система сбора данных, блокчейн, технологический суверенитет, терминальное устройство, Wialon IPS.

Введение

Тенденции развития современного общества направлены на осуществление «цифрового перехода» и, благодаря этому, улучшению качества жизни каждого человека. «Цифровой переход» (*Digital Transition*), или «цифровая трансформация» (*Digital Transformation*) — глубокие и всесторонние изменения в производственных и социальных процессах, связанные с тотальной заменой аналоговых технических систем цифровыми и широкомасштабным применением цифровых технологий. Цифровая трансформация охватывает не только саму производственную деятельность, но и изменение организационных структур компаний и бизнес-моделей. Одним из компонентов «цифрового перехода» являются распределённые системы сбора данных, которые позволяют осуществлять мониторинг окружающей среды и результатов аналитики. В таких системах присутствует большое количество терминальных устройств (например, метеостанции) оснащенных набором датчиков. Эти терминальные устройства стараются сделать максимально энергоэффективными, чтобы минимизировать затраты на их обслуживание, в связи с тем, что питание этих устройств автономное, их большое количество и они распределены на большой территории. Анализ показывает, что потребление энергии возрастает во время передачи информации на сервер в связи с тем, что начинает работать модем мобильного оператора.

Целью этой работы является сокращение промежутка времени передачи данных на сервер и разработка упрощённого алгоритма аутентификации, который с одной стороны обеспечит надёжность аутентификации, а с другой стороны позволит не повторять этот процесс несколько раз. Это позволит уменьшить расход элемента питания, а также увеличит период технического обслуживания тер-

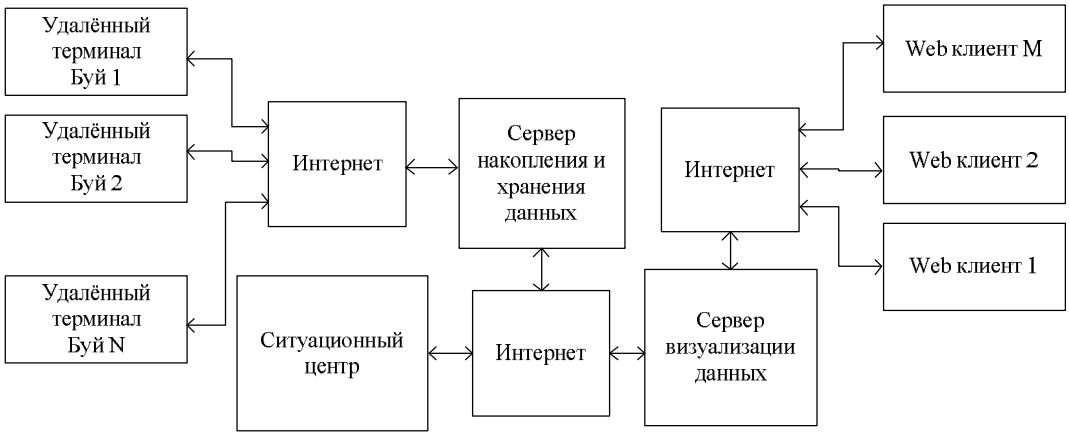

Рис 1. Структурная схема интеллектуальной системы мониторинга акватории Черного моря

минальных устройств распределённой системы сбора данных и как следствие снизит себестоимость её эксплуатации.

Анализ методов построения распределённых систем сбора данных

Для обоснованного выбора процедуры аутентификации удалённых терминалов можно рассмотреть системы мониторинга окружающей среды и, в частности, акватории Черного моря описанную в [1, 2, 3]. На рис. 1 изображена структурная схема распределённой системы сбора данных. Система состоит из N удалённых терминалов (буев), которые размещены в прибрежной акватории Черного моря. Каждый терминал имеет выход в интернет за счёт используемого GSM-модема.

Также в систему входит сервер сбора и накопления данных, к которому периодически подключаются терминалы с целью сохранения информации полученной от произвольного набора датчиков каждого терминального устройства.

Полученная информация должна храниться на сервере в привязке к удалённому терминалу. Клиенты (в общем случае их может быть M), заинтересованные в данных, предоставляемых интеллектуальной системой мониторинга, подключаются через интернет к серверу визуализации данных, используя обычный веб-браузер. Сервер визуализации представляет данные в графическом (графики, инфографика) или текстовом виде в зависимости от настроек клиента. С другой стороны сервер визуализации получает актуальные и/или обработанные данные от сервера накопления и хранения данных с использованием aRest API сообщений в JSON формате.

«Узким» местом такой системы является участок от терминального устройства до сервера накопления и обработки данных. Хотя есть большое количество готовых терминальных устройств, например [4], достаточно часто возникает необходимость самостоятельной разработки терминальных устройств как описано в [2]. В этом случае возникает задача выбора и обоснования протокола прикладного уровня. Здесь возникает вопрос, как хранить полезные данные и как их передавать на сервер. В [5] предлагается данные внутри программного обеспечения терминального устройства хранить не в виде бинарных структур, а передавать в текстовом формате. Последнее заключение выглядит спорным и конфликтует, на первый взгляд, с названием этой работы, поскольку передача текстовых сообщений требует больше байт по сравнению с бинарными сообщениями, следовательно, это увеличивает время работы устройства на передачу и приводит к большей трате энергии источника питания. Однако нашей задачей является уменьшение энергопотребления. Сравне-

ние энергетического выигрыша версии бинарного протокола относительно текстового приведено в конце работы, и забегая вперед, он оказался не критическим. С другой стороны такой подход позволяет делать систему масштабируемой. В частности, если используется бинарный протокол, в котором вместо имени поля используется смещение относительно начала пакета, то очень сложно обеспечить «обратную» совместимость при развитии ПО терминальных устройств, в связи с появлением в системе двух версий протокола, где используется разные карты бинарного поля, из-за отсутствия в бинарном протоколе метаданных описывающих эту структуру. От этого недостатка свободен текстовый протокол с разделителями DSV (Delimiter-Separated Values) [5]. Он включает в себя метаданные, позволяющие описать каждое поле и его тип (например: t:2:22.5 — поле t, тип float, значение 22,5). Таким образом, если сервер встречает поле, которое ещё не известно в базе данных, то он может его проигнорировать. Если отсутствует некоторое поле, допустим по причине отсутствия измерительной информации, сервер просто не включит это поле в запрос. Также в текстовом протоколе можно организовать обратный канал управления терминальными устройствами как описано в [6]. Поэтому, хотя есть много различных бинарных протоколов [7, 8], использование текстового протокола позволит создать распределённую систему сбора данных, где могут функционировать разные терминальные устройства и сервер сможет с ними взаимодействовать. Таким текстовым протоколом может быть протокол «Wailon IPS» [9], который уже используют отечественные производители терминальных устройств [4]. Этот протокол разработан компанией Gurtam для использования в персональных и автомобильных GPS- и ГЛОНАСС-трекерах, передающих данные на сервер системы спутникового мониторинга по протоколу TCP или UDP. Данный протокол является открытым и используется компанией для подключения к своим серверам, в настоящий момент по этому протоколу работает 53 тысячи устройств. Поиск показывает, что программного обеспечения серверной части этого протокола в открытом доступе нет, однако имеются сведения, что для своих устройств разработчик [4] предлагает свое облако, которое работает по этому протоколу. Надо отметить, что эта реализация протокола содержит некоторые отклонения от спецификации [10] (в частности передача даты и времени, перепутаны местами широта и долгота). Благодаря прозрачности и простоте протокола «Wialon IPS» его серверную часть достаточно просто реализовать на языке Python, используя библиотеку TCP сокетов и интерфейс подключения к СУБД mySQL, что и было сделано. Наличие в серверном ПО поддержки базы данных позволяет обеспечить его быстрое развертывание и модификацию. Всё это позволило создать доверенную информационную систему сбора и накопления данных, что является важным для обеспечения Россией технологического суверенитета. При этом использование текстового протокола обеспечивает обратную совместимость с терминальными устройствами. Структурно посылка протокола «Wailon IPS» состоит из двух частей: постоянной части (данные времени, GPS) и переменной (информация от датчиков). Такая архитектура позволяет объединять в одной базе данных информацию от разных категорий терминальных устройств (метеостанций, буев и т.д.). Поэтому в качестве базы данных выбрана реляционная структура хранения данных (mySQL), а не временных рядов (InfluxDB).

Анализируя структурную схему на рис. 1 можно заметить, что структура аппаратно-программного обеспечения системы мониторинга является распределённой. Разделение логики предметной области и презентационной логики позволяет сделать систему более масштабируемой [11]. С другой стороны это позволяет защитить данные от попыток взлома и искажения со стороны клиентов т.к. клиент взаимодействует только сервером отображения

данных и не имеет доступа к серверу накопления и хранения данных [12]. Другая угроза безопасности — это воздействие на сервер хранения данных со стороны удалённых терминалов. Чтобы снизить эту угрозу необходимо применить процедуру аутентификации. Бывает несколько методов аутентификации:

— парольные системы (самый простой и распространённый способ);

— системы PKI (криптографические сертификаты);

— системы одноразовых паролей;

— биометрические системы.

Простые парольные системы не являются надёжными, поскольку пароль передаётся через интернет и может быть перехвачен или подобран в результате сниффинга или брутфорса. Система криптографических сертификатов не подходит в силу своей вычислительной сложности и объёма. Система одноразовых паролей не подходит, поскольку данные надо сохранять периодично, а процедура получения одноразового пароля также упирается в то, что необходимо аутентифицировать того, кому выдаётся этот пароль. Биометрические системы не подходят в силу рассмотренной структуры системы. Таким образом, выбор системы аутентификации является затруднительным, т.к. не подходит ни одна система аутентификации. Однако если использовать совместно две системы, то это может решить поставленную задачу. Например, если терминалу и серверу хранения данных известен пароль, то нет необходимости передавать его в открытом виде через интернет, можно просто передавать его хеш-сумму (например, по алгоритму SHA256). Это может частично защитить от сниффинга, но по существу хеш-сумма является в данном случае тем же паролем, который передаётся через интернет. Поэтому этот пароль нужно сделать одноразовым, чтобы он менялся каждый сеанс связи. При этом с другой стороны необходимо, чтобы этот пароль был постоянным, чтобы терминал мог войти на сервер. Для решения этой задачи с исключающими друг друга условиями может быть полезно разделить пароль на две части — постоянная (которую знает и сервер и клиент) и переменная часть, которая вычисляется по определённой (известной на клиенте и сервере) функции, например от текущего времени [13]. В этом случае хэш сумма от такого пароля будет практически случайна и это кране затруднит как сниффинг так и брутфорс, таким образом, существенно повышая безопасность системы в целом.

Таким образом, в результате анализа установлено, что для обеспечения возможности масштабирования системы нужно использовать текстовый протокол обмена данными. В частности можно использовать простой, широко используемый отечественными производителями оборудования протокол «Wialon IPS». Разработав серверное программное обеспечение для этого протокола, можно создать доверенную информационную систему сбора и накопления данных от распределённых терминалов, тем самым внеся лепту в обеспечение технологического суверенитета России в условиях санкций.

Разработка процедуры начальной аутентификации с использованием технологии «Proof-of-work»

В распределённой системе сбора данных (см. рис. 1) каждый терминал, перед отправкой информации на сервер, создает новое TCP-подключение к серверу. Далее, согласно спецификации протокола, «Wailon IPS» [10] отправляет на него пакет аутентификации, в случае, если данные корректны, сервер отправляет подтверждение об успешной авторизации устройства, после которой устройство готово к обмену полезной информацией. Структурная схема пакета аутентификации и структурная схема расчёта CRC16 представлена на рис. 2, *а*) и рис. 2, *б*) соответственно.

Контрольная сумма нужна для передачи через сетевой транспорт без обязательного контроля целостности пакета (UDP, RAW

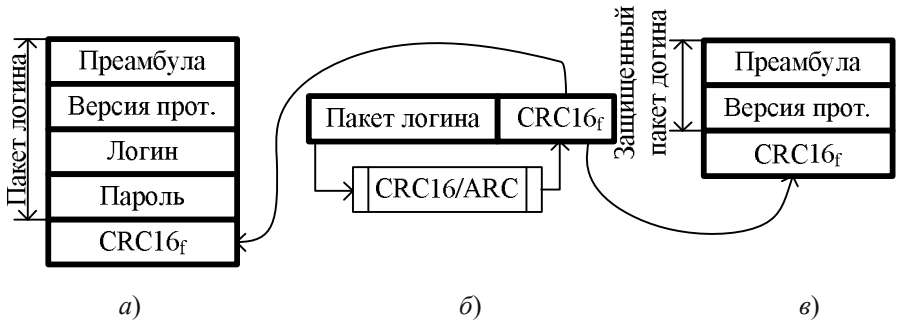

Рис. 2. Структурные схемы: *а*) — полного пакета аутентификации; *б*) — расчёта контрольной суммы полного пакета; *в*) — возможного варианта короткого пакета аутентификации без открытой передачи логина и пароля

Ethernet). При передаче через TCP транспорт, поле контрольной суммы в пакете можно не использовать. Из структуры пакета видно, что терминал передаёт на сервер запрос, хранящий в себе логин и пароль в открытом виде, что является небезопасным. Чтобы не передавать логин и пароль в открытом виде, можно данные для аутентификации передавать в контрольной сумме [14]. А именно, терминальное устройство рассчитывает контрольную сумму от полного пакета и передает её в коротком пакете. Короткий пакет состоит из преамбулы, версии протокола и контрольной суммы, как изображено на рис. 2 *в*). Данный алгоритм хоть и избавляет от возможности достать пароль из перехваченного запроса, но роль логина и пароля здесь выполняет контрольная сумма, которая также может быть перехвачена, поскольку она является постоянной. Чтобы защититься от брутфорса и перехвата контрольной суммы надо её сделать псевдослучайной, в частности вычислять при помощи дополнительного алгоритма, который исходя из текущего времени (с определённой точностью), «магического числа» (как в протоколе SIP [15], только генерируется оно на стороне клиента) и полного пакета аутентификации вычисляет контрольную сумму. Наличие временной метки в аргументах расчёта контрольной суммы даёт всегда разную контрольную сумму от одного и того же логина и пароля. Единственное требование — синхронизация с определённой точностью часов на клиенте и сервере. Вопросы временной синхронизации терминальных устройств рассматривались в работе [16]. Точность синхронизации может быть выбрана с учётом времени генерирования и доставки пакета аутентификации и задержки обработки на сервере. Была выбрана точность, равная 128 секундам, это удовлетворяет, как будет показано ниже, перечисленным выше условием и упрощает расчёт временной метки для аргумента контрольной суммы. Временная метка рассчитывается путём вычисления текущего времени в формате Unix Timestamp и обнуления младших 7 бит, которые являются незначащими.

«Магическое» число генерируется с использованием технологии «proof-of-work» [17]. Условием быстрой проверки на сервере достоверности пакета является наличие n первых нулей при вычислении контрольной суммы от контрольной суммы пакета и «магического» числа. Другими словами, клиент перед передачей пакета должен найти такое «магическое» число, которое при вычислении контрольной суммы от него и контрольной суммы пакета даст n первых нулей в результате. Этот подход похож на «майнинг» криптовалюты и не позволяет сделать перебор пароля принципиально нерентабельным, поскольку устройство достаточно маломощное. Однако позволяет сделать «магическое» число случайным, чтобы оно не бросалось в глаза при перехвате пакета. Структурно в пакете «магическое» число и кон-

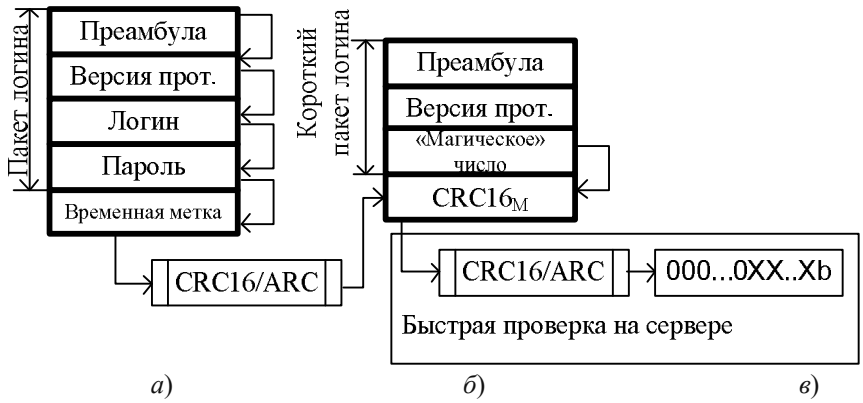

Рис. 3. Структурные схемы: *а*) — вычисления контрольной суммы пакета с учётом временной метки; *б*) — пакета, передаваемого на сервер; *в*) — варианта быстрой проверки «свой/чужой» на сервере

трольная сумма видны как непрерывный набор цифр и в реальной системе будет сложно отличить где «магическое число», а где контрольная сумма, особенно если использовать перемежение тетрад. Длина «магического» числа может быть достаточно большой, чтобы затруднить перебор. Структурная схема формирования пакета изображена на рис. 3.

Алгоритм генерации «магического» числа приведён на рис. 4, *б*). Пакет после прохождения быстрой проверки на предмет «свой/чужой», далее для аутентификации необходимо проверить в цикле для всех существующих в базе данных пользователей. Другими словами, надо к пришедшему короткому пакету добавить логин и пароль из базы данных, текущую временную метку (полученную на сервере по алгоритму, описанному выше) и создать из этого длинного пакета контрольную сумму, которую можно будет проверить с пришедшей в коротком пакете. Блок схема алгоритма аутентификации на стороне сервера

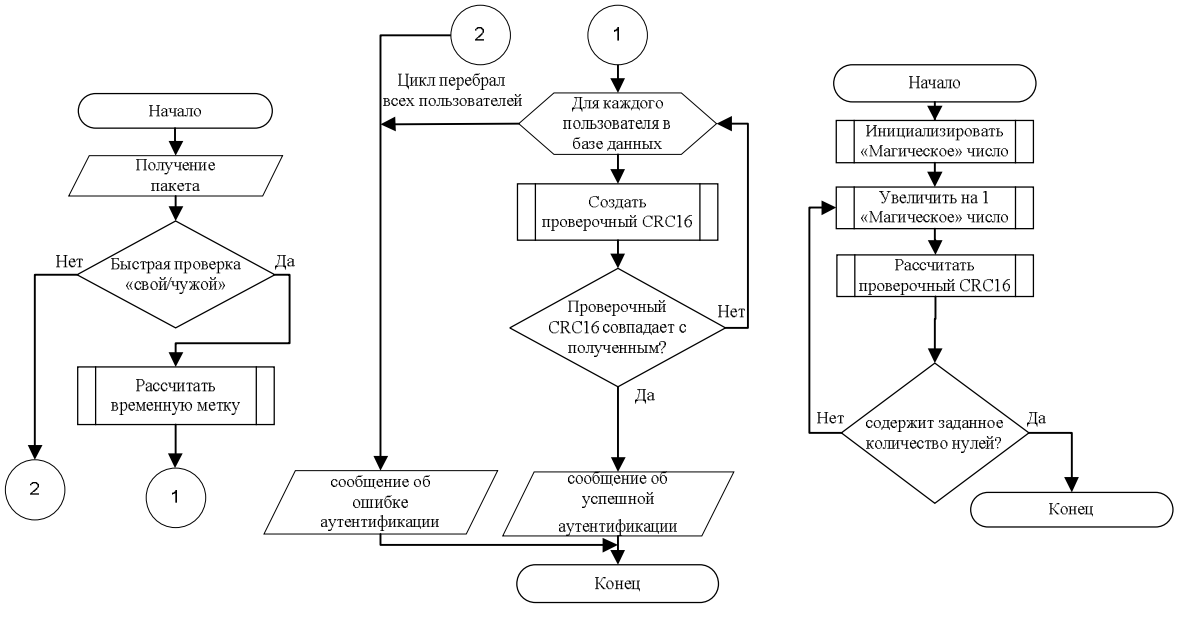

Рис. 4. Блок схемы: *а*) — алгоритма аутентификации устройства на сервере; *б*) — алгоритма генерации «магического» числа методом «proof-of-work» на терминальном устройстве

Таблица 1. Результаты расчёта контрольной суммы методом «proof-of-work» на терминальном устройстве

Кол-во бит	Максимальное количество итераций до консенсуса	Время нахождения консенсуса (мс)	«Магическое число»
1	5	0,8694	0x88be
2	18	2,7689	0x1261
3	35	5,3728	0xb44d
4	89	13,2469	0x870d
5	116	17,0591	0xa2ac
6	310	45,7643	0xe41d
7	514	75,7042	0x5e1b
8	1432	211,296	0x6c8d
9	3150	463,959	0x2aa1
10	3773	556,078	0xb322
11	10961	1624,49	0x7b7e
12	18674	2766,94	0xf51f
13	51945	7766,69	0xc362
14	88644	13210,4	0xbbb6

представлена на рис. 4, *а*). Теперь для доступа к серверу злоумышленнику придется подбирать длинную цифровую посылку («магическое» число плюс контрольная сумма с перемежением). На третьей неудачной попытке злоумышленник будет заблокирован на час, а в течение двух минут изменится «правильная» числовая последовательность.

Достоинством предложенного решения является отсутствие передачи логина и пароля по открытому каналу. Предложенный алгоритм расчёта контрольной суммы был реализован методом «proof-of-work» на микроконтроллере ESP8266 на языке uPython. Результаты работы сведены в таблицу 1. В таблице представлена зависимость максимального количества итераций «майнинга» и времени нахождения «консенсуса» от требуемого количества бит равного нулю в результате. Чтобы проанализировать результаты представим их в виде графика в логарифмическом масштабе (рис. 5).

По вертикали отложено количество милисекунд для нахождения «консенсуса», а по горизонтали требуемое количество бит, которое должно быть равно нулю при расчёте контрольной суммы от контрольной суммы полного пакета и «магического» числа. На графике точками обозначены табличные дан-

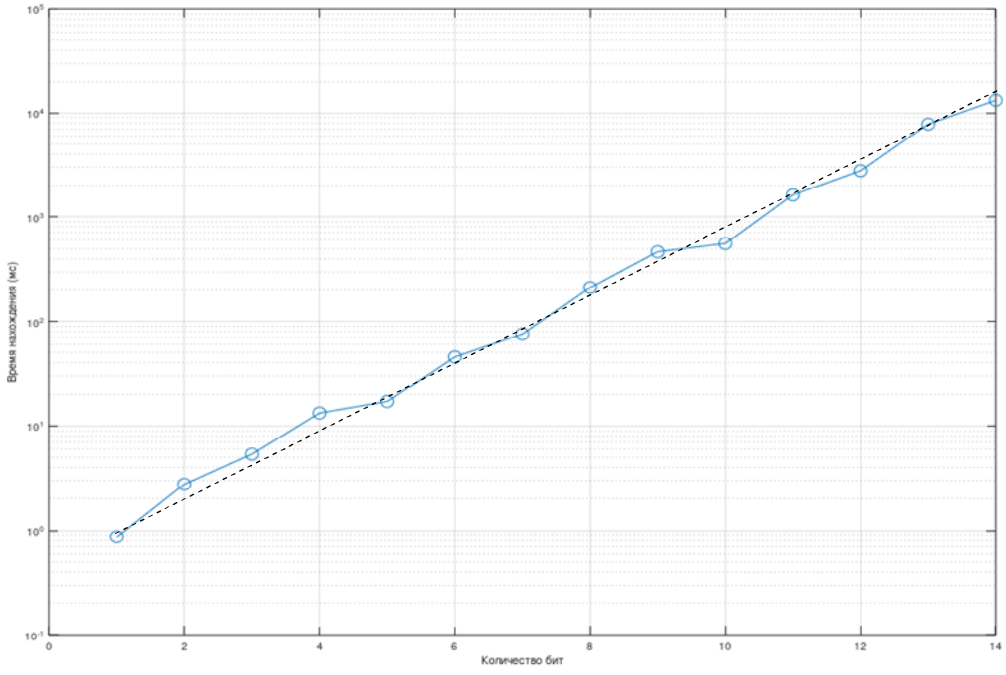

Рис. 5. Зависимость времени расчёта контрольной суммы методом «proof-of-work» от количества бит на терминальном устройстве

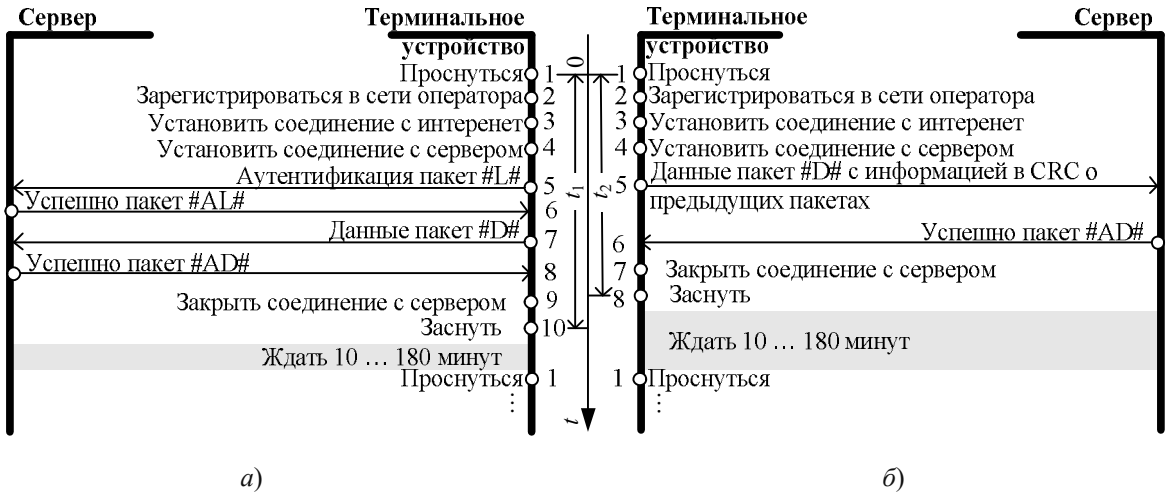

Рис. 6. Временная диаграмма последовательности обмена терминального устройства с сервером: *а*) — по оригинальному протоколу «Wialon IPS; *б*) по модифицированному протоколу «Wialon IPS

ные, а пунктирной прямой — усреднение результатов. Анализ графика показывает, что время нахождения «консенсуса» увеличивается в 100 раз на каждые требуемые шесть бит.

Таким образом, если нам требуется достаточно часто проходить процедуру аутентификации (например, при каждом выходе на связь) то следует выбирать количество бит, которые должны быть равны нулю порядка 10, это позволит найти «магическое число» за 500…700 мс. При этом стойкость алгоритма будет хуже. Если проводить процедуру аутентификации редко (например, раз в день), то можно выбрать количество бит, которые должны быть равны нулю, порядка 14. Это позволит получить «магическое» число за 13,2 сек, но при этом стойкость алгоритма существенно увеличится. Выбирать количество бит больше 14 не рекомендуется, так как нахождение «консенсуса» будет занимать десятки и сотни секунд.

Предположительно более надёжным является второй вариант для 14 бит, поэтому в следующем разделе рассматривается вопрос трансформации протокола «Wialon IPS», чтобы была возможность аутентификации один раз в день.

Уменьшение энергопотребления терминальных устройств за счёт использования технологии блокчейн

При наблюдении за экологическими параметрами, терминалы отправляют отчёты по состоянию своих датчиков один раз в достаточно продолжительный промежуток времени (от 10 минут до трёх часов). Делается это для обеспечения бюджета аккумулятора. На рис. 6, *а*) изображена последовательность обмена терминального устройства с сервером по протоколу «Wialon IPS». Последовательность обмена состоит из инициализации терминального устройства (поскольку интервал обмена большой и устройство находится в режиме глубокого сна для экономии энергии), установления соединения с сетью интернет, установления соединения с сервером. Далее происходит взаимодействие с серверной частью по протоколу «Wialon IPS», которое заключается в передаче пакета логина и пакета данных. Поскольку между сеансами связи терминала с сервером происходит разрыв соединения терминала с сервером, пакет логина надо посылать каждый раз при передаче данных, что влечёт дополнительный расход энергии.

Предлагается не передавать пакет логина

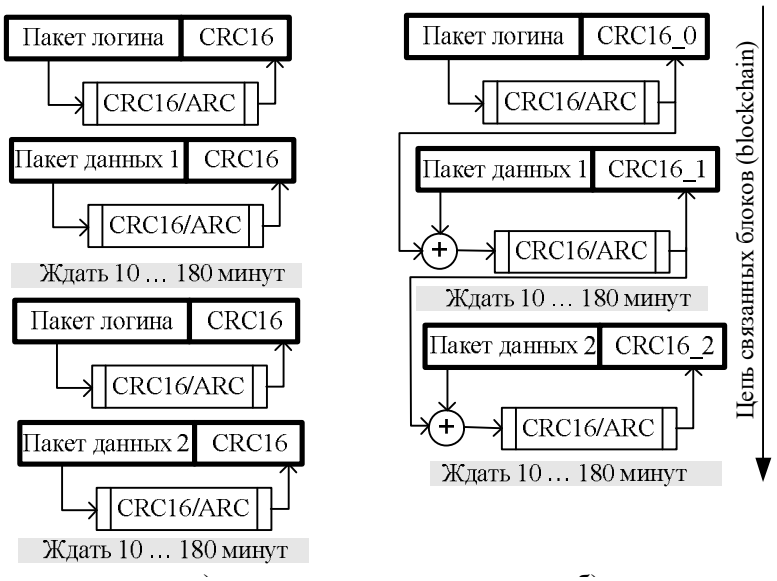

Рис. 7. Структурная схема формирования пакетов:
а) по оригинальному протоколу «Wialon IPS»;
б) по модифицированному протоколу «Wialon IPS»

при сеансе связи, а использовать ряд мероприятий по контекстной аутентификации терминального устройства внутри пакета данных, как изображено на рис. 6, *б*). В этом случае объём данных и время обмена в предложенном протоколе меньше, чем в оригинальном протоколе [18]. Более подробно протокольная часть обмена терминала с сервером изображена на рис. 7. Целостность каждого пакета контролируется с помощью процедуры циклической контрольной суммы CRC16/ARC, как изображено на рис. 7, *а*).

В отличие от оригинального варианта протокола, предлагаемый протокол, изображённый на рис. 7, *б*), требует передать пакет авторизации один раз в начале цепи пакетов данных, а затем учитывать этот пакет и все последующие пакеты до текущего пакета при расчёте его контрольной суммы. Это позволит, не меняя длину пакета данных, использовать его контрольную сумму для аутентификации с одной стороны, а с другой затруднит подделку пакетов данных злоумышленнику, поскольку надо знать всю последовательность, начиная с первого пакета аутентификации, и появляется возможность контролировать целостность всей цепочки пакетов данных. Эта является упрощенной технологией блокчейн. При попытке подбора злоумышленником поля контрольной суммы, сервер запросит повторный пакет аутентификации, если вместо этого придёт пакет данных с перебором или не валидный пакет аутентификации, то устройство может быть заблокировано на час с помощью правила IPTables. Если будет организована атака DDoS, то сервер постепенно заблокирует все устройства злоумышленника. При этом в это время также не смогут получить доступ к серверу и терминальные устройства системы, однако на борту каждого терминального устройства есть буфер для хранения пятидесяти посылок данных и устройство может позже подключиться к серверу, когда работоспособность восстановится.

Рассмотрим влияние потери пакетов в системе связи на потерю данных в распределённой системе сбора данных. Первый сценарий, когда теряется пакет данных на сервер, в этом случае сервер не отвечает на посылку терминального устройства, и терминальное устройство повторяет посылку пакета позже. В этом случае не требуется повторной аутентификации. Если сервером принята хотя бы часть пакета данных, то автоматически за счёт протокола более низкого уровня (TCP) произойдет запрос повреждённой части пакета. Таким образом, при потере пакета данных от терминального устройства к серверу не происходит серьезных нарушений во взаимодействии, это же справедливо, если сервер находится под DDoS атакой. Если теряется пакет, подтвер-

ждающий получение пакета данных, то терминал воспринимает передачу как неудачную и пробует отправить пакет данных на сервер повторно с прежней контрольной суммой. В этом случае цепочка блокчейн прервётся, и сервер вернет сообщение о необходимости отправки пакета аутентификации. Таким образом, в худшем случае потеря пакета данных в любом направлении приведёт к необходимости повторной отправки пакета логина, как и в оригинальной версии протокола. При использовании модемов операторов мобильной связи, наиболее вероятна потеря в канале «uplink» — от терминального устройства к серверу, что не приводит к необходимости повторной аутентификации.

Количественная оценка уменьшения энергопотребления терминальных устройств проводилась в два этапа. На первом этапе проведено несколько измерений расхода энергии аккумулятора терминального устройства. На втором этапе с учётом полученных данных рассчитан выигрыш в продолжительности работы от аккумулятора терминального устройства в различных режимах работы.

На первом этапе измерялся расход энергии терминального устройства для метеостанций. Основные элементы терминального устройства, потребляющие энергию аккумулятора это:

— микроконтроллер STM32F103RBT6;

— GPRS модем SIM800L

Считывание датчиков метеостанции осуществляется по интерфейсу RS485. Все элементы потребляющие энергию (делители, преобразователь интерфейса RS485, вспомогательные DC-DC преобразователи, модем) отключаются на время сна с помощью ключей на полевых транзисторах.

Для количественной оценки выигрыша в энергопотреблении необходимо знать какое количество энергии аккумулятора тратится на:

— один опрос датчиков метеостанции ($kW_{дат}$);

— один сеанс связи с сервером по протоколу Wailon IPS без модификации, т.е. с пакетом логина ($kW_{сл}$);

— один сеанс связи с сервером с использованием упрощённой технологии блокчейн т.е. без пакета логина при каждом сеансе ($kW_{сбл}$);

— режим сна терминального устройства, пересчитанный в мгновенное потребление раз в минуту ($kW_{сон}$).

Опрос датчиков и связь с сервером имеет импульсное потребление тока. Например модем при напряжении питания 3,6 В, может потреблять в импульсе до 2 А. Поэтому следует измерять расход энергии за промежуток времени, например за 1 час. Для упрощения дальнейших расчётов определим, что внутри измерительного интервала опрос датчиков или связь с сервером осуществляется с периодичностью в одну минуту. Другими словами, за измерительный интервал будет осуществлено 60 сеансов связи или опросов датчиков. Далее, проведя нормировку, можно определить, сколько энергии расходуется только на один сеанс связи или опрос датчиков. Измерения проводились интегрирующим USB тестером нагрузки Ruideng UM34C, к которому был подключен DC-DC преобразователь с выходным напряжением 3,6 В. Преобразователь питает тестируемое терминальное устройство. Также модифицировано программного обеспечения терминального устройства, которое позволяет выбирать различные режимы работы; сон; связь с сервером с/без пакета логина; опрос датчиков и т.д. Режим работы терминального устройства в процессе измерения потребления энергии при опросе датчиков и связи с сервером описывается следующей последовательностью: опрос датчиков, связь с сервером, затем режим сна до начала следующей минуты, потом повторить сначала и так в течение часа. При измерении потребления только опроса датчиков из последовательности исключается связь с сервером. Произведённые измерения включают в себя потребление терминального устройства в выбранном режиме,

Таблица 2. Потребление энергии терминального устройства в различных режимах

Измеряемый режим	Расход энергии, мВт·ч
Опрос датчиков $W_{\text{Гдат}}$	310
Связь с сервером с пакетом логина и опрос датчиков $W_{\text{Гсл\_дат}}$	470
Связь с сервером без пакета логина и опрос датчиков $W_{\text{Гсбл\_дат}}$	447
Режим сна $W_{\text{Гсон}}$	288

собственное потребление DC-DC преобразователя и платы отладчика. Чтобы учесть это, также проводилось измерение потребления энергии терминального устройства в режиме сна с помощью интегрирующего USB тестера нагрузки при питании через DC-DC преобразователь. Результаты измерений сведены в таблицу 2.

На основе измеренных данных рассчитаем потребление энергии за один опрос датчиков/сеанс связи:

$$kW_{\text{дат}} \approx \left(W_{\text{Гдат}} - W_{\text{Гсон}}\right)\Big/60 = 0{,}37\,\text{мВт}\cdot\text{ч};$$

$$\text{k}W_{\text{сл}} \approx \left(W_{\text{Гсл\_дат}} - W_{\text{Гдат}}\right)\Big/60 = 2{,}67\,\text{мВт}\cdot\text{ч};$$

$$kW_{\text{сбл}} \approx \left(W_{\text{Гсбл\_дат}} - W_{\text{Гдат}}\right)\Big/60 = 2{,}28\,\text{мВт}\cdot\text{ч}. \quad (1)$$

Потребление энергии терминального устройства только в режиме непрерывного сна осуществлялось измерением потребляемого тока устройства, запитанного от аккумулятора (амперметр включался в цепь питания аккумулятора) и затем пересчёта его в мВт·ч. Величина тока в этом режиме составила 2,1 мА, из них микроконтроллер в режиме STOP потребляет 540 мкА. Для единства рассуждения приведём непрерывное потребление энергии только в режиме сна к импульсному потреблению раз в минуту в течение часа, получим:

$$kW_{\text{сон}} \approx \frac{I_{\text{сон}}\cdot U_{\text{акк}}\cdot t}{10^{-3}\cdot 3600\cdot 60} = \frac{0.0021\cdot 3{,}6\cdot 3600}{3{,}6\cdot 60} = 0{,}126\,\text{мВт}\cdot\text{ч}. \quad (2)$$

Выражения (1) и (2) позволяют получить математическую модель для временной зависимости расхода ёмкости аккумулятора для разных задач, выполняемых терминальным устройством. Учитывая, что ёмкость аккумулятора измеряется в мА·ч и обозначается буквой C, а задачи опроса датчиков и связи с сервером могут проводиться с разными интервалами времени, получим:

$$C_{\text{дат}}\left(t, N_{\text{дат}}\right) = \frac{kW_{\text{дат}}\cdot t}{U_{\text{акк}}\cdot N_{\text{дат}}};\ C_{\text{сл}}\left(t, N_{\text{св}}\right) = \frac{kW_{\text{сл}}\cdot t}{U_{\text{акк}}\cdot N_{\text{св}}};$$

$$C_{\text{сбл}}\left(t, N_{\text{св}}\right) = \frac{kW_{\text{сбл}}\cdot t}{U_{\text{акк}}\cdot N_{\text{св}}};\ C_{\text{сл}}\left(t, N_{\text{св}}\right) = \frac{kW_{\text{сл}}\cdot t}{U_{\text{акк}}\cdot N_{\text{св}}};$$

$$C_{\text{сон}}\left(t\right) = \frac{kW_{\text{сон}}\cdot t}{U_{\text{акк}}}, \quad (3)$$

где t — время в минутах; $U_{\text{акк}}$ — напряжение аккумулятора принимается постоянным и равным 3,6 В, т.е. в этой модели не учитывается падение напряжение при разряде аккумулятора; $N_{\text{св}}$ — количество минут между ближайшими сеансами связи; $N_{\text{дат}}$ — количество минут между ближайшими опросами датчиков; $C_{\text{дат}}$ — временная зависимость расхода ёмкости аккумулятора, обусловленная только опросом датчиков; $C_{\text{сл}}$ — временная зависимость расхода емкости аккумулятора, обусловленная только связью с сервером по не модифицированному протоколу (т.е. с передачей пакета логина при каждом сеансе связи); $C_{\text{сбл}}$ — временная зависимость расхода ёмкости аккумулятора, обусловленная только связью с сервером по модифицированному протоколу (т.е. без передачи пакета логина); $C_{\text{сон}}$ — временная зависимость расхода ёмкости аккумулятора, обусловленная только режимом сна терминального устройства.

На рис. 8 приведена временная зависимость расхода аккумулятора на различные задачи терминального устройства.

Из графика видно, что при ежеминутном сеансе связи с сервером и опросе датчиков основная часть энергии потребляется при связи с сервером. Также можно заметить, что связь с сервером без пакета логина потребляет меньше

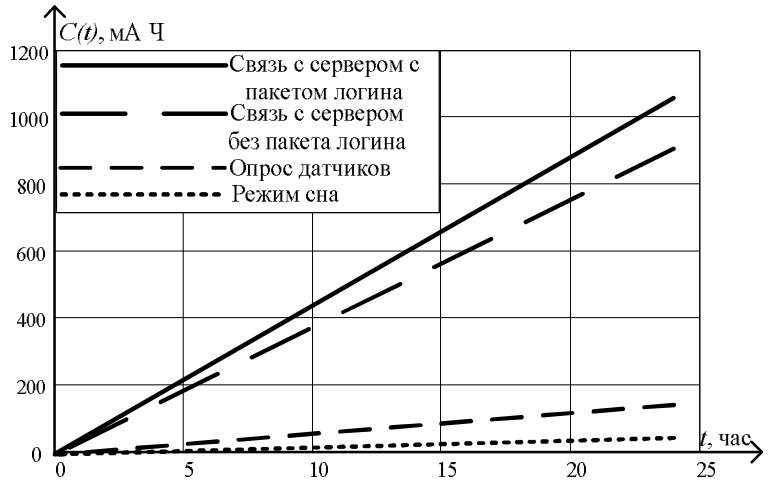

Рис. 8. Временная зависимость расхода аккумуляторной батареи терминального устройства на различные задачи в течение суток с интервалом опроса датчиков и связью с сервером 1 минута

энергии, чем при использовании для связи немодифицированного протокола с пакетом логина при каждом сеансе.

Введём количественную оценку выигрыша длительности работы от аккумулятора при использовании технологии блокчейн. Для этого надо определить временную зависимость полного потребления терминального устройства. Полное потребление энергии терминальным устройством для не модифицированного протокола определяется выражением:

$$C_{\text{л}}\left(t,N_{\text{св}},N_{\text{дат}}\right)=C_{\text{сл}}\left(t,N_{\text{св}}\right)+ \\ +C_{\text{дат}}\left(t,N_{\text{дат}}\right)+C_{\text{сон}}\left(t\right). \qquad (4)$$

Полное потребление энергии терминальным устройством для протокола с применением технологии блокчейн определяется выражением:

$$C_{\text{бл}}\left(t,N_{\text{св}},N_{\text{дат}}\right)=C_{\text{сбл}}\left(t,N_{\text{св}}\right)+ \\ +C_{\text{дат}}\left(t,N_{\text{дат}}\right)+C_{\text{сон}}\left(t\right). \qquad (5)$$

Из выражений (4) и (5) выразим время работы от батареи емкостью $C_{\text{бат}}$, для этого положим в выражениях (4) и (5), что $C_{\text{л}}(t,\ N_{\text{св}},\ N_{\text{дат}}) = C_{\text{бат}}$ и $C_{\text{бл}}(t,\ N_{\text{св}},\ N_{\text{дат}}) = C_{\text{бат}}$ и выразим t, получим:

$$T_{\text{л}}\left(C_{\text{бат}},N_{\text{св}},N_{\text{дат}}\right)=\frac{C_{\text{бат}}\cdot U_{\text{акк}}}{\dfrac{kW_{\text{сл}}}{N_{\text{св}}}+\dfrac{kW_{\text{дат}}}{N_{\text{дат}}}+kW_{\text{сон}}}, \qquad (6)$$

$$T_{\text{бл}}\left(C_{\text{бат}},N_{\text{св}},N_{\text{дат}}\right)=\frac{C_{\text{бат}}\cdot U_{\text{акк}}}{\dfrac{kW_{\text{сбл}}}{N_{\text{св}}}+\dfrac{kW_{\text{дат}}}{N_{\text{дат}}}+kW_{\text{сон}}}. \qquad (7)$$

Используя выражения (6) и (7) определим относительное время увеличения длительности работы терминального устройства или выигрыш от использования протокола с технологией блокчейн в процентах:

$$\eta\left(N_{\text{св}},N_{\text{дат}}\right)=\left(T_{\text{бл}}\left(C_{\text{бат}},N_{\text{св}},N_{\text{дат}}\right)-T_{\text{л}}\left(C_{\text{бат}},N_{\text{св}},N_{\text{дат}}\right)\right)\times \\ \times\frac{1}{T_{\text{л}}\left(C_{\text{бат}},N_{\text{св}},N_{\text{дат}}\right)}\cdot 100\%\,. \qquad (8)$$

Как видно из выражения (8), выигрыш зависит от интервала связи с сервером и интервала опроса датчиков. На рис. 9 изображен график зависимости выигрыша времени работы от аккумулятора при использовании протокола с технологией блокчейн от интервала связи с сервером при условии $N_{\text{св}} = N_{\text{дат}}$, т.е. на каждый опрос датчика приходится один сеанс связи с сервером.

Как можно заметить из графика, с ростом интервала связи с сервером эффективность падает с 14% при интервале в одну минуту до 2% при интервале 3 часа, так как в этом случае существенную роль играет потребление в режиме сна терминального устройства.

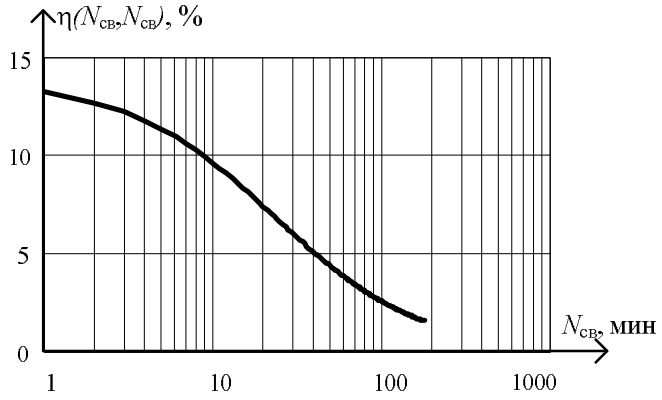

Рис. 9. Зависимость выигрыша времени работы от аккумулятора терминального устройства при использовании протокола с технологией blockchain от интервала связи с сервером при условии $N_{св} = N_{дат}$

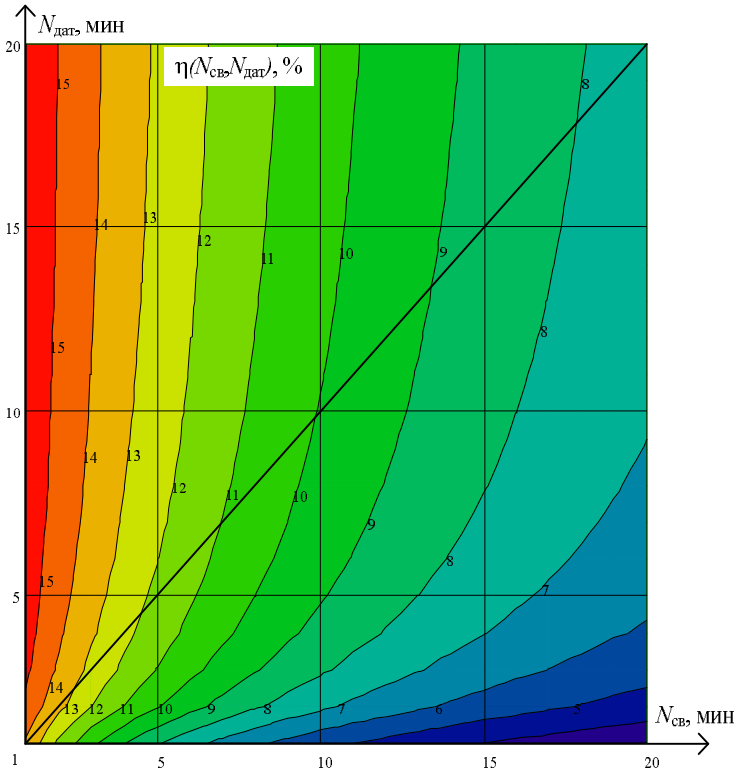

Рис. 10. Зависимость выигрыша времени работы от аккумулятора терминального устройства при использовании протокола с технологией blockchain от интервала связи с сервером $N_{св}$ и интервала опроса датчиков $N_{дат}$

Более полную картину зависимости выигрыша дает трёхмерная зависимость, изображенная на рис. 10. По горизонтальной оси отложены значения интервала связи с сервером в минутах. По вертикальной оси отложены значения интервала опроса датчиков в минутах. Контурные линии определяют значения выигрыша (в процентах) времени работы от аккумулятора терминального устройства при использовании протокола с технологией блокчейн от интервала связи с сервером $N_{св}$ и интервала опроса датчиков $N_{дат}$. На графике также проведена диагональ из левого нижнего угла в правый верхний. Двумерный график на рис. 9 построен по этой диагонали. Используя эту диагональ, можно графически классифицировать распределенные системы сбора данных по интервалам опроса датчиков и интервалам связи с сервером на:

— распределённые системы сбора данных реального времени, включающие в себя устройства, режим работы которых расположен на диагонали (интервал опроса равен интервалу сохранения информации);

— распределённые системы сбора данных с задержкой обновления информации, включающие в себя терминальные устройства, режим работы которых расположен ниже диагонали (интервал связи с сервером больше чем интервал опроса датчиков);

— распределённые системы сбора данных реального времени с оперативной реакцией на команды сервера, включающие в себя устройства, режим работы которых расположен выше диагонали (интервал связи с сервером меньше чем интервал опроса датчиков).

```
120622;045710;0000.00000;N;00000.00000;E;0;0;0;0;NA;NA;NA;2917.13,33.50,948.50,550.50,1002.62,129.62,14.22,3,2;NA;ETY:1:1,TR:1:0,TP:1:2,dtu:1:14
TTTTCSLALALTLTSPCRALSHDCSIIIIOOOOA8F0000F0000F0000F0000F0000F0000F0000F0000CI00S0P4ETYI00TRI00TPI00dtuI0000
```

Рис. 11.

Таким образом, больший выигрыш будут иметь терминальные устройства распределённых систем сбора данных реального времени с оперативной реакцией на команды сервера, а наименьший выигрыш — терминальные устройства в распределённых системах с задержкой обновления информации.

Проведено сравнение текстовой [10] и бинарной версии протокола Wailon IPS [19] при передаче одного и того же набора данных в текстовом и бинарном виде. Две посылки приведены на рис. 11 друг под другом моноширным шрифтом, чтобы можно было сравнить их длину.

В бинарной строке реальные числовые данные заменены цифровыми символами, чтобы все символы были читаемыми и длину посылки можно было сравнить визуально. Количественное сравнение: длина текстовой посылки — 146 символов, длина бинарной посылки — 108 символов, разность — 26%. Терминальное устройство, передающее текстовую посылку в течение часа с интервалом одну минуту, израсходовало 442,24 мВт·ч энергии батареи. Терминальное устройство, передающее бинарную посылку в течение часа с интервалом одну минуту, израсходовало 441 мВт·ч энергии батареи. Экономия энергии есть, но не критическая. Малая разница в потреблении энергии может объясниться тем, что конкретно этот протокол занимает промежуточное место между бинарным и текстовым, поскольку позволяет передавать имена полей в текстовом виде, а данные в бинарном, являясь достаточно гибким, частично попадая под критерии, изложенные в [5], и может быть использован для распределённых систем сбора данных с разными типами терминальных устройств.

Заключение

В работе установлено, что для обеспечения возможности масштабирования системы, нужно использовать текстовый или бинарно-текстовый протокол обмена данными. Одним из возможных вариантов является открытый протокол «Wialon IPS». Для решения задачи создания доверенной информационной системы сбора и накопления данных от распределённых терминалов для обеспечения технологического суверенитета России в условиях санкций разработано серверное программное обеспечение для этого протокола.

Также предложено модифицировать протокол «Wialon IPS» в части процедуры аутентификации. Во-первых, в качестве пакета логина использовать короткий пакет без явной информации о логине и пароле как в оригинале. Вместо этого использовать цифровую посылку («магическое» число плюс контрольная сумма с перемежением), которая генерируется на основе постоянной и переменной части пароля.

Во-вторых, для аутентификации при каждом сеансе связи предложено использовать упрощенную технологию блокчейн. Это позволило с одной стороны увеличить срок работы терминального устройства от одного комплекта батарей примерно до 14% в пределе.

Предложена математическая модель (7) для быстрой оценки бюджета энергии аккумулятора терминального устройства при различных интервалах опроса датчиков и связи с сервером. Это позволит сократить время наладки распределённой системы сбора данных.

Литература

1. *Bezgin A. A., Lukyanchikov, A. V., Redkina, E. A.* Distributed system for measuring and collecting parameters of coastal water area and reservoir // Proceedings - 2020 7th All-Russian Microwave Con-

ference, RMC 2020. Pp. 320–323. DOI: 10.1109/RMC50626.2020.9312303

2. *Bezgin A.A. , Motyzhev S.V. , Lunev E.G., Redkina E.A. Lukyanchikov A.V.* Distributed intelligent measuring and information system for monitoring coastal environmental parameters // Journal of Physics: Conference Series. 2021. Vol. 2094(3). Pp. 032028. DOI: 10.1088/1742-6596/2094/3/032028

3. *Безгин А.А., Лунев Е.Г., Мотыжев С.В., Воликов М.С., Гимпилевич Ю.Б., Редькина Е.А., Лукьянчиков А.В.* Интеллектуальная система оперативного контроля пресноводных ресурсов и морских акваторий Севастополя // «Моря России: год науки и технологий в РФ – десятилетие наук об океане ООН». Тезисы докладов Всероссийской научной конференции, г. Севастополь, 20–24 сентября 2021 г. Севастополь: ФГБУН ФИЦ МГИ, 2021. С. 216-217.

4. Метеостанция Sokol-M1 [Электронный ресурс]: сайт фирмы «Sokol Meteo», 2023. URL: https://sokolmeteo.ru/p-sokolm/ (дата обращения 01.03.2023).

5. *Реймонд Э. С.* Искусство программирования для Unix.: Пер. с англ. М.: Издательский дом «Вильямс», 2005. 544 с.

6. *Гимпилевич Ю.Б., Лукьянчиков А.В., Редькина Е.А.* Особенности реализации управления терминалами в распределенной системе сбора данных // СВЧ-техника и телекоммуникационные технологии. Севастополь, 2021. С. 93–94.

7. *Abakumov Anton, Lukyanchikov Andrey* The WEB-applications development features for IOT using the MQTT protocol // Recent Achievements and Prospects of Innovations and Technologies. Керчь; ФГБОУ ВО «Керченский государственный морской технологический университет», 2019. С. 215–218.

8. *Saltzer J. H., Reed D. P., Clark D. D.* End-to-End Arguments in System Design. // Transactions on Computer Systems (Association for Computing Machinery). 1984. Pp. 277–288.

9. *Панкратьева А.* Wialon – передовые решения для спутникового мониторинга // Первая миля. 2013, Том. 37 № 4. С. 36–41.

10 Протокол Wialon IPS v.2.0. (RU) [Электронный ресурс]: сайт фирмы «Gurtam», © 2002-2023. URL: https://gurtam.com/hw/files/Wialon%20IPS%20%28RU%29%20%284%29.docx (дата обращения 01.03.2023).

11. *Гимпилевич Ю.Б., Лукьянчиков А.В., Редькина Е.А.* Алгоритм сохранения и отображения информации, поступающей от буйковых станций в интеллектуальной системе мониторинга параметров Севастопольской прибрежной акватории Черного моря // СВЧ-техника и телекоммуникационные технологии. Севастополь, 2020. С. 134–135.

12. *Кожемякин А.С., Лукьянчиков А.В.* Особенности организации связи в распределенной системе сбора данных // Современные проблемы радиоэлектроники и телекоммуникаций. 2020. №3 С. 95.

13. *Гимпилевич Ю.Б., Лукьянчиков А.В., Редькина Е.А., Мотыжев С.В.* Особенности процедуры аутентификации в системе мониторинга состояния Севастопольской прибрежной акватории // СВЧ-техника и телекоммуникационные технологии. Севастополь, 2020. С. 122–123.

14. *Лукьянчиков А.В., Безгин А.А., Нестеренко А.И.* Протокол распределенной системы сбора данных с использованием технологии майнинга // СВЧ-техника и телекоммуникационные технологии. Севастополь, 2022. С. 58–59.

15. SIP: Session Initiation Protocol [Электронный ресурс]: сайт RFC Series Working Group (RSWG). URL: https://www.rfc-editor.org/rfc/rfc3261.html (дата обращения 01.03.2023).

16. *Лукьянчиков А.В., Рязанова А.С., Рыжанков А.П., Шакиров И.Р.* Локальный сервер точного времени // Современные проблемы радиоэлектроники и телекоммуникаций. 2021. №4 С. 80.

17. *Dwork C, Naor M* Pricing via processing or combatting junk mail // Lecture Notes in Computer Science. 1993. Vol. 740. Pp. 139–147. DOI: 10.1007/3-540-48071-4_10

18. *Лукьянчиков А. В., Ильяш Д. И.* Уменьшение энергопотребления терминальных устройств за счет использования технологии блокчейн майнинга // СВЧ-техника и телекоммуникационные технологии. Севастополь, 2022. С. 60–61.

19 Протокол Wialon Combine [Электронный ресурс]: сайт фирмы «Gurtam», © 2002-2023. URL: https://gurtam.com/hw/files/Wialon%20Combine_v1.1.5%20%28RU%29.pdf (дата обращения 01.03.2023).

.

Поступила 4 марта 2023 г.

English

AUTHENTICATION PROTOCOL FOR A DISTRIBUTED DATA ACQUISITION SYSTEM AS PER BLOCKCHAIN TECHNOLOGY TO REDUCE POWER CONSUMPTION

Andrey Vladimirovich Lukyanchikov — PhD., Associate Professor of the Department of Innovative Telecommunication Technologies, Institute of Radio Electronics and Intellectual Technical Systems, Sevastopol State University.

E-mail: brain75@mail.ru

Address: 299053, Russian Federation, Sevastopol, Universiteskaya St., 33.

Abstract: The paper proposes a method to reduce power consumption of terminal devices of the city information portal system, which aggregates ambient monitoring data and analytics results. Parameter *t* is found that a text or binary-text data exchange protocol is to be used to ensure the possibility of scaling the system. One of the possible options is the open Wialon IPS protocol. Server-based software for this protocol was developed to solve the problem of creating a trusted information system for acquisition data from distributed terminals to ensure Russia's technological sovereignty under sanctions. Wialon IPS protocol was also proposed to modify in regards to the authentication procedure. First, a short packet is to be used as a login packet without explicit information about the login and password as it is in the original. Instead, a digital dispatch is used (magic number plus interleaved checksum) that is generated based on the constant and variable parts of the password. Second, a simplified blockchain technology is proposed to use for authentication during each communication session. This enabled, on the one hand, to increase the service life of the terminal device with one batteries' pack up to about 14% within the ambit. A mathematical model is proposed for a rapid assessment of the battery power budget of a terminal device at various intervals for sensors' scanning and communicating with the server. This will enable to reduce the setup time for a distributed data acquisition system.

Keywords: distributed data acquisition system, blockchain, technological sovereignty, terminal device, Wialon IPS.

References

1. *Bezgin A.A., Lukyanchikov, A.V., Redkina E.A.* Distributed system for measuring and collecting parameters of coastal water area and reservoir. Proceedings - 2020 7th All-Russian Microwave Conference, RMC. 2020, 9312303. Pp. 320–323. DOI: 10.1109/RMC50626.2020.9312303

2. *Bezgin, A.A. , Motyzhev, S.V. , Lunev, E.G., Redkina, E.A.* Lukyanchikov, A.V. Distributed intelligent measuring and information system for monitoring coastal environmental parameters. Journal of Physics: Conference Series. 2021. Vol. 2094(3). Pp. 032028. DOI: 10.1088/1742-6596/2094/3/032028

3. *Bezgin A.A., Lunev E.G., Motyzhev S.V., Volikov M.S., Gimpilevich Ju.B., Red'kina E.A., Lukyanchikov A.V.* The intellectual system of operational monitoring of freshwater resources and marine waterquakes of Sevastopol. Seas of Russia: the Year of Science and Technology in the Russian Federation - a decade of science of the UN ocean. Sevastopol': FGBUN FITs "Morskoj gidrofizicheskij institut RAN, 2021. Pp. 216–217.

4. The Sokol-M1 weather station [Electronic source]: website of Sokol Meteo, © 2023. URL: https://sokolmeteo.ru/p-sokolm/ (access date 01.03.2023).

5. *Raymond E.S.* The art of UNIX programming: Trans. from English. Moscow : Izdatel'skij dom "Vil'jams", 2005. 544 p.

6. *Gimpilevich Ju.B., Red'kina E.A., Lukyanchikov A.V.* Features of the implementation of terminals management in a distributed data collection system. SVCh-tekhnika i telekommunikacionnye tekhnologii. Sevastopol, 2021. Pp. 93–94.

7. *Abakumov A., Lukyanchikov A.* The WEB-applications development features for IOT using the MQTT protocol// Recent Achievements and Prospects of Innovations and Technologies. Kerch; FSBEI in Kerch State Marine Technological University, 2019. Pp. 215–218.

8. *Saltzer J.H., Reed D.P., Clark D.D.* End-to-End Arguments in System Design. Transactions on Computer Systems (Association for Computing Machinery). 1984. Pp. 277–288.

9. *Pankrat'eva A.* Wialon – advanced solutions for satellite monitoring. Pervaya milya. 2013.Vol. 37. No. 4. Pp. 36–41.

10 Protocol Wialon IPS v.2.0. (RU) [Electronic source]: The website of the company "Gurtam", © 2002-2023. URL: https://gurtam.com/hw/files/wialon%20ips%20%28ru%29%284%29.docx (access date 01.03.2023).

11. *Gimpilevich Ju.B., Red'kina E.A., Lukyanchikov A.V.* The algorithm for the conservation and display of information coming from the violet stations in the intellectual system for monitoring the parameters of the Sevastopol Coastal Walk of the Black Sea. Microwave technology and telecommunication technologies. Sevastopol, 2020. Pp. 134–135.

12. *Kozhemjakin A.S., Lukyanchikov A.V.* Features of the organization of communication in the distributed data collection system. Reasoning problems of radio electronics and telecommunications. 2020. No. 3 P. 95

13. *Gimpilevich Ju.B., Red'kina E.A., Lukyanchikov A.V., Motyzhev S.V.* Features of the authentication procedure in the monitoring system of the state of the Sevastopol coastal water area. SVCH-tekhnika i telekommunikacionnye tekhnologii. Sevastopol, 2020. Pp. 122–123.

14. *Lukyanchikov A.V., Bezgin A.A., Nesterenko A.I.* The protocol of the distributed data collection system using mining technology. SVCH-tekhnika i telekommunikacionnye tekhnologii. Sevastopol, 2022. Pp. 58–59.

15. SIP: Session Initiation Protocol [Electronic source]: The website of RFC Series Working Group (RSWG). URL: https://www.rfc-editor.org/rfc/rfc3261.html (access date 01.03.2023).

16. *Lukyanchikov A.V., Rjazanova A.S., Ryzhankov A.P., Shakirov I.R.* Local server of the precision time. The consistent problems of electronics and telecommunications. 2021. No. 4 P. 80.

17. *Dwork C., Naor M.* Pricing via processing or combatting junk mail // Lecture Notes in Computer Science. 1993. 740 LNCS 139-147. DOI: 10.1007/3-540-48071-4_10

18. *Lukyanchikov A.V., Il'jash D.I.* Reducing the energy consumption of terminal devices due to the use of blockchain mining blockchain. Microwave technology and telecommunication technologies. Sevastopol, 2022. Pp. 60–61.