

УДК 004.72

Doi: 10.31772/2712-8970-2023-24-2-260-272

Для цитирования: Кустов Н. Д., Евдокимов К. С., Шахматов А. В. Интегрированная космическая сеть: обоснование архитектурных и технических решений космической миссии ReshUCube-2 // Сибирский аэрокосмический журнал. 2023. Т. 24, № 2. С. 260–272. Doi: 10.31772/2712-8970-2023-24-2-260-272.

For citation: Kustov N. D., Evdokimov K. S., Shahmatov A. V. [Space integrated network: architectural and technical solutions justification of the ReshUCube-2 space mission]. *Siberian Aerospace Journal*. 2023, Vol. 24, No. 2, P. 260–272. Doi: 10.31772/2712-8970-2023-24-2-260-272.

Интегрированная космическая сеть: обоснование архитектурных и технических решений космической миссии ReshUCube-2

Н. Д. Кустов^{*}, К. С. Евдокимов, А. В. Шахматов

Сибирский государственный университет науки и технологий имени академика М. Ф. Решетнева
Российская Федерация, 660037, г. Красноярск, просп. им. газ. «Красноярский Рабочий», 31

^{*}E-mail: kustovnd@sibsau.ru

Космические миссии с применением малых космических аппаратов типа CubeSat получили широкое распространение. В связи с этим перспективным направлением развития данной отрасли являются интегрированные космические сети. В данной работе предложена архитектура такой сети. Планируется, что первым узлом данной сети станет аппарат ReshUCube-2.

Были определены функциональные требования и технические ограничения описанной архитектуры. На основе требований проведен обзор и сравнительный анализ сетевых протоколов и технологий разных уровней. В результате предложен сетевой стек, который соответствует данным требованиям. Ключевыми протоколами в стеке были выбраны: LoRa, 802.15.4, IPv6, 6LoWPAN, RPL, TCP, UDP и CoAP. Предложены методы программной и аппаратной реализации узлов сети. Продемонстрирован тестовый стенд на основе специально разработанных унифицированных устройств, на котором предлагается отрабатывать функции сетевого взаимодействия. Также показана тестовая плата полезной нагрузки для малых космических аппаратов – узлов космического сегмента.

Полученные результаты будут использованы в процессе разработки будущих космических миссий СибГУ им. М. Ф. Решетнева. Кроме того, результаты могут быть полезны при проектировании сетей интернета вещей, интернета транспортных средств и подобных сетей. Результаты работы могут также послужить основой для будущих исследований в области сетевых технологий, цифровой обработки сигналов, межспутникового взаимодействия и космических информационных систем.

Ключевые слова: космическая интегрированная сеть, CubeSat, LoRa, IEEE 802.15.4, 6LoWPAN, IPv6, RPL.

Space integrated network: architectural and technical solutions justification of the ReshUCube-2 space mission

N. D. Kustov^{*}, K. S. Evdokimov, A. V. Shahmatov

Reshetnev Siberian State University of Science and Technology
31, Krasnoyarskii Rabochii prospekt, Krasnoyarsk, 660037, Russian Federation

^{*}E-mail: kustovnd@sibsau.ru

Space missions using small CubeSat-type spacecraft have become widespread. In this regard, integrated space networks are a promising direction for the development of this industry. In this paper, the architecture of such a network is proposed. It is planned that the first node of this network will be the ReshUCube-2 device.

Functional requirements and technical limitations of the described architecture were determined. Based on the requirements, a review and comparative analysis of network protocols and technologies of different levels: physical, channel, network, transport and application. As a result, a network stack is proposed that meets these requirements. The key protocols in the stack were chosen: LoRa, 802.15.4, IPv6, 6LoWPAN, RTL, TCP, UDP and CoAP. Methods of software and hardware implementation of network nodes are proposed. A test bench based on specially developed unified devices is demonstrated, on which it is proposed to work out the functions of network interaction. A test payload board for small spacecraft – nodes of the space segment is also shown.

The results obtained will be used in the development of future space missions of the Reshetnev Siberian State University. In addition, the results can be useful in the design of the Internet of Things, the Internet of vehicles and similar networks. The results of the work can also serve as a basis for future research in the field of network technologies, digital signal processing, inter-satellite interaction and space information systems.

Keywords: Space Integrated Network, CubeSat, LoRa, IEEE 802.15.4, 6LoWPAN, IPv6, RPL.

Введение

В настоящее время наблюдается активный период развития сферы малых космических аппаратов (МКА). На текущий момент, к примеру, в рамках проекта «Space-л» было запущено 29 МКА типа CubeSat. В том числе, аппарат ReshUCube-1 СибГУ им. М. Ф. Решетнева [1]. Все-го по проекту «Space-л» в течение нескольких лет планируется запустить, в общей сложности, 100 таких МКА. Таким образом, актуальным направлением развития этой отрасли представляется организация межспутникового взаимодействия и интеграция космического сегмента с наземными сетями [2]. В связи с этим, приоритетной задачей для грядущей космической миссии ReshUCube-2 является тестирование архитектуры интегрированной космической сети. Очевидно, что речь идет об относительно низкоскоростной передаче (порядка 2^{10} – 2^{18} бит/с) в связи с дальностью передачи.

Данная работа посвящена обоснованию принятых архитектурных решений и применяемых технологий, а также демонстрации промежуточных результатов при разработке описанной сети.

Предлагаемая сетевая архитектура

Сетевая архитектура подразумевает наличие как минимум наземного и космического сегмента. Узлы космического сегмента – МКА на низких околоземных орбитах. Наземный сегмент может быть представлен привычными сетями (Ethernet, Wi-Fi, WiMAX, Bluetooth и т. д.), сетями интернета вещей (Internet of Things, IoT) [3] или интернета транспортных средств, как это представлено в работе [4].

При этом предусматривается три основных класса устройств такой сети:

- 1) конечный узел (Host) – узел (например, датчик, сенсор), передающий и принимающий сообщения, не имеющий функций маршрутизации;
- 2) маршрутизатор (Router) – узел, выполняющий, в том числе, функции конечного узла и обладающий функциями маршрутизации внутри сети;
- 3) граничный маршрутизатор (Border Router) – узел, выполняющий, в том числе, функции конечного узла и маршрутизатора, обладающий при этом функциями маршрутизации между сетями различных стандартов.

Общий вид предлагаемой сетевой архитектуры представлен на рис. 1.

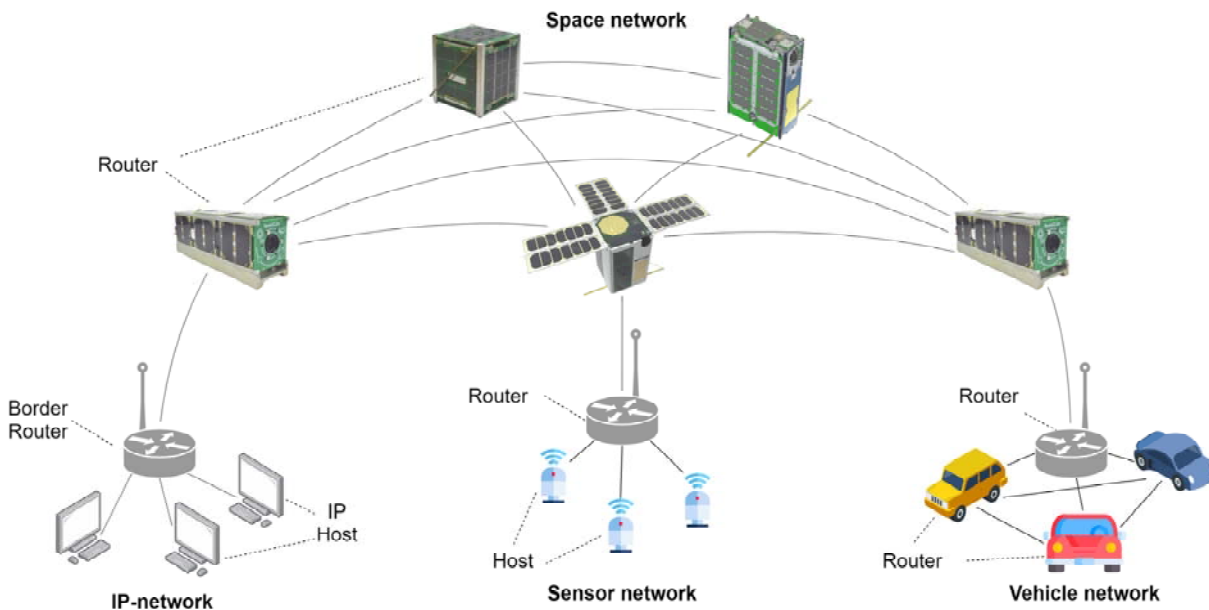


Рис. 1. Общий вид сетевой архитектуры интегрированной космической сети

Fig. 1. Network architecture general view of the space integrated network

Описание требований к архитектуре

В работе [5] представлены исходные требования, которые были определены при проектировании архитектуры интегрированной космической сети. Ниже предложен уточненный, на текущий момент, перечень этих требований:

- низкая стоимость электронной компонентной базы;
- возможность передачи на большое расстояние;
- помехоустойчивость и устойчивость к эффекту Доплера;
- высокая энергоэффективность;
- низкое потребление аппаратных ресурсов;
- обеспечение динамической маршрутизации и поддержка ячеистой топологии сети;
- поддержка стандартных протоколов верхних уровней стека TCP/IP (Transmission Control Protocol / Internet Protocol);
- минимальное, насколько возможно, преобразование на границе разных сегментов сети (наземного и космического);
- сжатие сетевых заголовков для увеличения соотношения полезной нагрузки к общему объему кадра;
- минимальное, насколько возможно, количество операций фрагментации и сборки пакетов;
- автоконфигурация сетевых адресов в отсутствии возможности централизованного управления адресами и поиск соседних узлов;
- возможность использования «облегченных» прикладных протоколов;
- поддержка функций безопасности.

Первые пять требований определяют состав аппаратных компонентов и применяемых технологий физического уровня передачи. В первую очередь, это состав полезной нагрузки МКА. Кроме того, состав устройств, принадлежащих наземному сегменту.

Остальные функции могут быть реализованы программно. Это, в свою очередь, подразумевает выбор соответствующих сетевых протоколов, общесистемного и прикладного программного обеспечения.

Предлагаемый стек сетевых технологий

Использовать стандартный стек TCP/IP в исходном виде не представляется возможным, в связи с чем предлагается использовать сочетание различных протоколов.

Большинство функциональных требований могут быть удовлетворены при использовании протоколов прикладного и сетевого уровня модели OSI (Open Systems Interconnection), разработанных для IoT. Это протоколы 6LoWPAN (IPv6 over Low power Wireless Personal Area Networks) [6], RPL (IPv6 Routing Protocol for Low-Power and Lossy Networks) [7], CoAP (Constrained Application Protocol) [8] и др. Однако данные протоколы были разработаны для группы стандартов персональных сетей IEEE (Institute of Electrical and Electronics Engineers) 802.15.4 [9]. Очевидно, что физические ограничения данного стандарта не удовлетворяют требованиям по дальности связи и помехоустойчивости. В связи с этим, предлагается использовать технологию физического уровня LoRa (Long Range) [10], отказавшись при этом от канального уровня, входящего в технологию LoRaWAN [11] (Long Range Wide-Area Networks). Для того чтобы обеспечить совместимость канального и физического уровней, необходимо ввести дополнительный подуровень, содержащий PHY-MAC драйвер.

Общий вид предлагаемого стека сетевых технологий приведен на рис. 2, а обоснование принятых решений представлено в следующем разделе.

	LoRaWAN netstack	6LoWPAN netstack		ReshUCube netstack	
Application layer	Application protocols	CoAP	Application protocols	CoAP	Application protocols
Transport layer	-	TCP	UDP	TCP	UDP
Network layer	-	IPv6		IPv6	RPL
		6LoWPAN		6LoWPAN	
Data link layer	LoRa MAC	802.15.4 MAC		802.15.4 MAC	
				PHY-MAC driver	
Physical layer	LoRa PHY	802.15.4 PHY		LoRa PHY	

Рис. 2. Общий вид предлагаемого стека сетевых технологий

Fig. 2. General view of the proposed network technology stack

Обоснование выбора сетевых технологий

Применяемые сетевые технологии должны, в первую очередь, удовлетворять предъявленным выше требованиям и, кроме того, не иметь критичных ограничений по совместимости с другими технологиями (нижележащие уровни должны предоставлять необходимые сервисы вышележащим). Далее приводится анализ функций различных протоколов и технологий в соответствии с уровнями модели OSI.

1. Физический уровень

На данном уровне необходимо провести сравнительный анализ основных функций и параметров технологий LoRa и IEEE 802.15.4.

Ключевыми являются следующие функции и параметры:

– обнаружение активного канала. Для 802.15.4 предусмотрена функция ED (Energy Detection), предназначенная для использования сетевым уровнем как часть алгоритма выбора канала. Это оценка мощности принятого сигнала в пределах полосы пропускания канала. Для LoRa подобной технологии не предусмотрено, однако приемник LoRa может переключиться на другой канал по запросу;

– определение качества приема. Для 802.15.4 предусмотрено измерение LQI – это характеристика силы и/или качества принятого кадра. Измерение может быть реализовано с использованием ED приемника, оценки отношения сигнал/шум или комбинации этих методов. Для LoRa нет механизма, объединяющего параметры качества, однако можно получить параметры RSSI (Received Signal Strength Indicator) и SNR (Signal-to-Noise Ratio) по отдельности;

– идентификация активности. 802.15.4 должен обеспечивать возможность выполнения CCA (Clear Channel Assessment) в соответствии, по крайней мере, с одним из следующих методов:

энергия выше порогового значения и/или обнаружение несущей, или CCA постоянно должен сообщать о том, что передатчик находится в состоянии ожидания. Обнаружение активности канала CAD (Channel Activity Detection) LoRa используется для обнаружения присутствия сигнала путем обнаружения преамбулы или символов данных;

– настройка параметров передачи. Для 802.15.4 параметры передачи зависят от используемого метода модуляции. Для LoRa: SF (Spreading Factor) – соотношение между номинальной скоростью передачи данных и скоростью модуляции, BW (Bandwidth) – ширина полосы пропускания (в кГц), CR (Coding Rate) – частота кодирования для защиты от ошибок;

– оптимизация низкой скорости передачи. Для низких скоростей передачи данных в LoRa и длительной передачи полезных нагрузок может быть включена оптимизация низкой скорости передачи данных – LDRO (Low Data Rate Optimization). Для 802.15.4 такой технологии не предусмотрено;

– скорость передачи. Для 802.15.4 может составлять до 250 кбит/с, для LoRa – от 300 бит/с до 27 кбит/с;

– максимальное расстояние передачи. Для 802.15.4 ограничено 100 м, для LoRa может достигать 500 км и более.

Сравнительная таблица физического уровня LoRa и 802.15.4 представлена ниже (табл. 1).

Таблица 1

Физический уровень: 802.15.4 и LoRa

Функция или параметр	802.15.4 PHY	LoRa PHY
Обнаружение активного канала	ED	–
Определение качества приема	LQI на основе ED и/или SNR	RSSI или SNR
Идентификация активности	CCA	CAD
Настройка параметров передачи	Зависит от модуляции	SF, BW, CR
Оптимизация низкой скорости передачи	–	LDRO
Скорость передачи	до 250 кбит/с	300 бит/с – 27 кбит/с
Максимальное расстояние передачи	до 100 м	свыше 500 км

Основные аппаратные функции, реализованные в стандарте 802.15.4, имеют аналогичные в стандарте LoRa, за исключением обнаружения активного канала. Однако, если канал один, это не представляется критичным. В противном случае, можно рассмотреть механизмы переключения канала на более высоком уровне.

Качество приема в LoRa определяется теми же параметрами, что и в 802.15.4, но они не объединены в общий механизм (как LQI в 802.15.4). Оценка качества хотя бы по одному из параметров (RSSI, что предпочтительнее, или SNR) является достаточной (описание LQI в стандарте 802.15.4 это допускает).

Идентификация активности в LoRa с помощью CAD также соответствует требованиям (в стандарте 802.15.4 один из вариантов работы механизма CCA аналогичен).

В результате замены стандарта физического уровня удовлетворяются необходимые требования в части дальности передачи и, помимо того, в части помехоустойчивости и устойчивости к эффекту Доплера за счет механизма LDRO.

2. Канальный уровень

Для данного уровня необходимо провести аналогичное сравнение (канальные функции LoRa определены в стандарте LoRaWAN) по следующим функциям и параметрам:

– механизм «суперкадра». В 802.15.4 суперкадр ограничен маяками, может иметь активную (период, в течение которого устройства могут случайным образом получать доступ к среде, и период гарантированного доступа) и неактивную (период, в который координатор может перейти в режим низкого энергопотребления) части. Такая структура используется опционально. Для LoRa такой механизм не предусмотрен;

- проверка целостности кадров. В 802.15.4 циклическая проверка избыточности (CRC) используется для обнаружения ошибок в каждом кадре, а также к каждому фрагменту прилагается последовательность проверки целостности фрагмента. Для LoRa такая функция может опционально использоваться как на канальном, так и на физическом уровне;
- подтверждение доставки кадров. Успешный прием и проверка кадра опционально сопровождается подтверждением. Это применимо к обеим технологиям;
- доступ к среде. Методы доступа, определенные в стандарте 802.15.4, следующие: Unslotted/Slotted CSMA-CA (Carrier Sense Multiple Access With Collision Avoidance), TSCH (Time Slotted Channel Hopping) CCA, TSCH CSMA-CA, CSMA-CA с PCA (Priority Channel Access), LECIM (Low-Energy Critical Infrastructure Monitoring) ALOHA с PCA. Методы доступа, определенные в стандарте LoRa: Pure/Slotted ALOHA;
- размер кадра. Для 802.15.4 – 127 байт, для LoRa 59-230 байт;
- поддерживаемые топологии. Для 802.15.4 – звездообразная или одноранговая, для LoRa – звездообразная или «звезда из звезд»;
- функции безопасности. В обоих стандартах приведен аналогичный алгоритм шифрования AES (Advanced Encryption Standard) на канальном уровне, который может использоваться опционально. Однако, в дополнение, для LoRa предусмотрен механизм от атак воспроизведения.

Сравнительная таблица канального уровня LoRa и 802.15.4 представлена в табл. 2.

Стандарт канального уровня LoRaWAN по большей части соответствует 802.15.4. По некоторым параметрам LoRa выигрывает (например, в части гибкости CRC, защите от атак воспроизведения). В части механизма управления доступом – проигрывает за счет отсутствия вариативности. Однако наибольшей проблемой является отсутствие поддержки у LoRaWAN одноранговой (ячейстой) топологии [12]. Кроме того, возникает вопрос адаптации вышележащих уровней.

Таким образом, наиболее правильным решением представляется использование 802.15.4 в качестве протокола канального уровня. Основной задачей, в этом случае, является адаптация функций канального уровня к сервисам, предоставляемым физическим уровнем (в данном случае – LoRa PHY). Функции драйвера, которые следует реализовать, приведены на рис. 3.

Таблица 2

Канальный уровень: 802.15.4 и LoRa

Функция или параметр	802.15.4 MAC	LoRa MAC
Механизм «суперкадра»	+	–
Проверка целостности кадров	На канальном уровне	На физическом и канальном уровнях
Подтверждение доставки кадров	+	+
Доступ к среде	Unslotted/Slotted CSMA-CA, TSCH CCA, TSCH CSMA-CA, CSMA-CA с PCA, LECIM ALOHA с PCA	Pure/Slotted ALOHA
Размер кадра	127 байт	59–230 байт
Поддерживаемые топологии	Звездообразная или одноранговая	Звездообразная или «звезда из звезд»
Функции безопасности	AES	AES, счетчик кадров

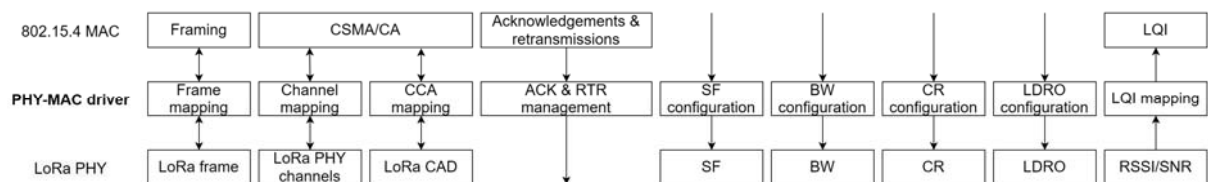


Рис. 3. Функции PHY-MAC драйвера

Fig. 3. Functions of the PHY-MAC driver

3. Сетевой уровень

Базовым сетевым протоколом в описываемом стеке для поддержки TCP/IP сетей предлагается применять протокол IPv6. Минимальная единица передачи для IPv6 составляет 1280 октетов, однако максимальный размер MAC-кадра, определенный IEEE 802.15.4, составляет 127 байт, где 25 байт зарезервированы для накладных расходов на кадр и оставлено только 102 байта для полезной нагрузки. Ситуация ухудшается, если канальный уровень накладывает дополнительные накладные расходы в целях безопасности, добавляя вспомогательный заголовок безопасности в MAC-кадр, который в максимальном случае оставляет только 81 байт для пакета IPv6. Таким образом, полный пакет IPv6 не помещается в кадр 802.15.4.

Кроме того, поскольку заголовок IPv6 в пакете IPv6 составляет 40 байт, для верхних уровней остается только 41 байт. Резервируя либо 8-байтовый заголовок протокола UDP (User Datagram Protocol), либо 20-байтовый заголовок протокола TCP, добавленный на транспортном уровне, пакет IPv6 непрактично оставляет только несколько байт пространства для прикладных данных.

Таким образом, предлагается применять в качестве уровня адаптации между канальным и сетевым уровнями протокол 6LoWPAN. Данный протокол включает в себя следующие функции:

- сжатие заголовка. В настоящее время IETF (Internet Engineering Task Force) в документе RFC6282 [13] рекомендует использовать IPHC для сжатия заголовка IPv6. IPHC обеспечивает эффективное сжатие IPv6-адресов – локальных, многоадресных и глобальных. В лучшем случае (при обмене между устройствами в одной сети) заголовок может быть сжат до 2 байт. В худшем случае (при глобальной маршрутизации) IPHC обеспечивает около 50 % сжатия;

- фрагментация и повторная сборка. Уровень адаптации должен фрагментировать пакеты IPv6 перед их отправкой и повторной сборкой при приеме. Каждому фрагменту предшествует 4- или 5-байтовый заголовок фрагментации;

- маршрутизация [14]. Маршрутизация – функция передачи пакета данных с одного устройства на другое, иногда с помощью ретрансляций через несколько промежуточных узлов. В зависимости от уровня, на котором расположен механизм маршрутизации, определены две ее категории: mesh-under или route-over.

В системе mesh-under маршрутизация данных происходит прозрачно, следовательно, mesh-under-сети можно считать одной IP-подсетью. В такой системе есть только один IP-маршрутизатор – граничный, установлен один широкоэвещательный домен, чтобы гарантировать совместимость с протокола IPv6 более высокого уровня, такого как обнаружение дублирования адреса.

В route-over-сетях маршрутизация имеет место на сетевом уровне. Наиболее широко используемым протоколом маршрутизации в route-over-сетях 6LoWPAN на сегодня является RPL, как определено IETF в RFC6550 [7]. RPL поддерживает два различных режима маршрутизации: режим с сохранением и режим без сохранения. В режиме с сохранением все устройства в 6LoWPAN-сети конфигурируются как маршрутизаторы, которые поддерживают таблицу маршрутизации и хранят таблицу соседних узлов. В режиме без сохранения есть единственное устройство с таблицей маршрутизации – граничный маршрутизатор. Следовательно, используется маршрутизация от источника.

При route-over пакет IPv6 восстанавливается на каждом промежуточном устройстве, чтобы принять решение о маршрутизации. И наоборот, в mesh-under решение о маршрутизации принимается на уровне 6LoWPAN и, следовательно, только с фрагментами пакета IPv6. В этом случае пакет IPv6 восстанавливается только на оборудовании назначения. Следовательно, mesh-under позволяет сократить задержку передачи, route-over более эффективна в ухудшенных условиях (потеря пакетов);

- автоконфигурация IP-адреса и обнаружение соседнего узла. Автономная генерация IPv6-адреса устройства. Для IPv6 он позволяет устройству автоматически генерировать свой IPv6-адрес без какого-либо взаимодействия с внешним сервером DHCP или аналогичным устройством. Чтобы получить адрес, хост может связываться через протокол NDP (Neighbor Discovery Protocol) [15]. Впрочем, многие из функций NDP также включены в RPL;

– функции безопасности [16]. Использование IPsec (IP Security) возможно, но шифрование потребляет много ресурсов и метод обмена ключами IKEv2 использовать нельзя. Необходимым условием является управление ключом шифрования с использованием минимальной полезной нагрузки, а также ограничение сообщений, которыми обмениваются узлы. Для сетей 6LoWPAN было реализовано расширение протокола SEND (SEcure Neighbor Discovery protocol), RFC3971 [17], для защиты механизма обнаружения соседей, которое называется LSEND (Lightweight Secure Neighbor Discovery Protocol).

При применении протокола 6LoWPAN достигается:

- поддержка стандартных протоколов стека TCP/IP;
- обеспечение динамической маршрутизации и поддержка ячеистой топологии. При этом представляется оптимальным использование дополнительного протокола RPL в режиме с сохранением, чтобы каждый промежуточный узел выполнял функции маршрутизатора и хранил собственную таблицу маршрутизации (так как это наиболее эффективное решение в условиях потери пакетов за счет того, что пакеты восстанавливаются на каждом промежуточном узле, и, кроме того, минимизируется количество избыточной служебной информации в пакете);
- минимальное преобразование на границе сегментов (за счет установки на границе специальных пограничных маршрутизаторов);
- сжатие сетевых заголовков (за счет механизмов IPHC и, опционально, NHC (Next Header Compression));
- минимальное количество операций фрагментации и сборки (за счет того же сжатия);
- автоконфигурация сетевых адресов и поиск соседних узлов (за счет механизма ND и протокола RPL).

4. Транспортный уровень

На транспортном уровне, как упоминалось ранее, предлагается использовать привычные протоколы TCP и UDP. Также, как было замечено, для UDP можно использовать механизм NHC для дополнительного сжатия UDP заголовка от 8 до 4 байт.

На транспортном уровне в 6LoWPAN-сетях, рекомендуется использовать механизм TLS (Transport Layer Security). TLS, как определено в RFC8446 [18], работает поверх TCP. В условиях ограниченных ресурсов, где UDP выбран в качестве протокола транспортного уровня, для обеспечения безопасности на транспортном уровне может использоваться DTLS (Datagram Transport Layer Security), RFC6347 [19]. Однако нужно отметить, что реализация TLS/DTLS требует, чтобы устройства имели необходимые ресурсы, такие как аппаратный механизм шифрования и другие.

5. Прикладной уровень

На прикладном уровне, теоретически, могут использоваться любые протоколы стека TCP/IP. Разумеется, предпочтительно использовать протоколы, обеспечивающие минимальный уровень загрузки сети.

Помимо этого, предлагается использовать специальные «облегченные» протоколы для IoT. К примеру, протокол CoAP. CoAP – это протокол со следующими основными характеристиками: клиент-серверная архитектура; REST-архитектура (Representational State Transfer); нижележащий протокол – UDP; асинхронная транзакционная модель; поддержка URI (Uniform Resource Identifier) и MIME (Multipurpose Internet Mail Extensions); простой и небольшой заголовок (менее 10 байт); настройка системы прокси и «кеширования»; для безопасности используется DTLS.

Практическая реализация

Аппаратные решения, на основе которых может функционировать данный стек, могут быть различными. В рамках космической миссии ReshUCube-2, в частности, было принято решение использовать микроконтроллер STM32WLE5CC [20], отвечающий требованиям производи-

тельности и энергоэффективности, а также оснащенный приемопередатчиком, поддерживающим модуляцию LoRa.

С точки зрения программной реализации также могут быть рассмотрены различные варианты. К примеру, операционные системы для IoT Contiki-NG и RIOT. В данном случае было отдано предпочтение последней в связи с высоким уровнем поддержки этой операционной системы. Так или иначе, обе системы поддерживают стек TCP/IP, 6LoWPAN и стандарт 802.15.4, однако их совместное использование с технологией LoRa требует дополнительных разработок в части драйвера адаптации, о котором упоминалось ранее.

На сегодняшний день был создан тестовый стенд, на основе которого планируется отладка сетевого взаимодействия между узлами. Для тестового стенда были разработаны 5 унифицированных плат на основе упомянутого микроконтроллера STM32WLE5CC. Данные платы оснащены LoRa-приемопередатчиками с мощностью 25 мВт, работающими на нелицензируемой частоте 868 МГц. Внешний вид развернутого тестового стенда и пример тестовой архитектуры приведен на рис. 4. Здесь три узла могут выполнять функции маршрутизатора или конечного узла: один узел – граничный маршрутизатор, один узел – сетевой сниффер, позволяющий перехватывать пакеты, передаваемые между платами. К граничному маршрутизатору подключен IPv6 узел. К этому же узлу подключен сниффер, чтобы обеспечить интерфейс.

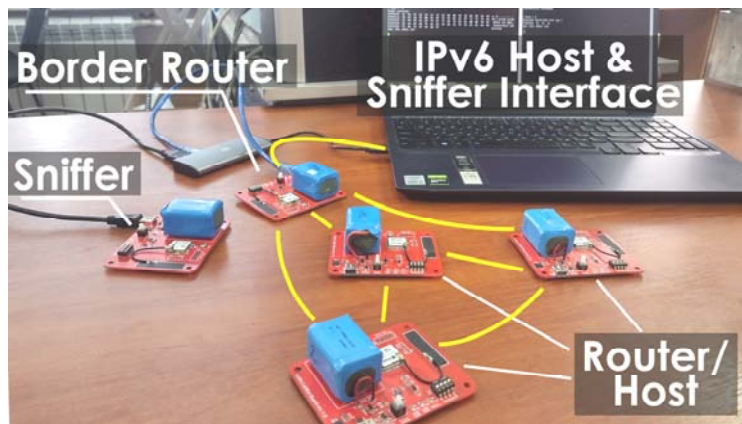


Рис. 4. Внешний вид тестового стенда

Fig. 4. Appearance of the test bench

На рис. 5 приведен пример инициализации устройств. Для каждого из четырех активных узлов выводится список соседних узлов (ND) и таблица маршрутизации (RPL). Граничный маршрутизатор (подключенный как /dev/ttyUSB0) выполняет функции корневого. Можно увидеть, что узлы, по-умолчанию, образуют топологию DODAG (Destination Oriented Directed Acyclic Graph). Дочерние узлы находятся в непосредственной близости к корневому маршрутизатору и, таким образом, автоматически относятся к первому уровню графа, что отмечено символом «X» в графе «parent table». Это говорит о том, что предложенное решение является вполне жизнеспособным: операционная система и, в том числе, сетевой стек функционируют в необходимом объеме.

Кроме того, был разработан прототип полезной нагрузки МКА ReshUCube-2. По аналогии, данная плата оснащена микроконтроллером STM32WLE5CC. Ключевым отличием является расчётная мощность – около 2 Вт и рабочая частота в лицензируемом частотном диапазоне – 435 МГц. Здесь проводится тестирование иных аспектов: аппаратных функций, работоспособности, надежности и т. д. Внешний вид платы прототипа полезной нагрузки приведен на рис. 6. На основе данного прототипа сейчас изготавливается радиомодуль, предназначенный непосредственно для установки на МКА.

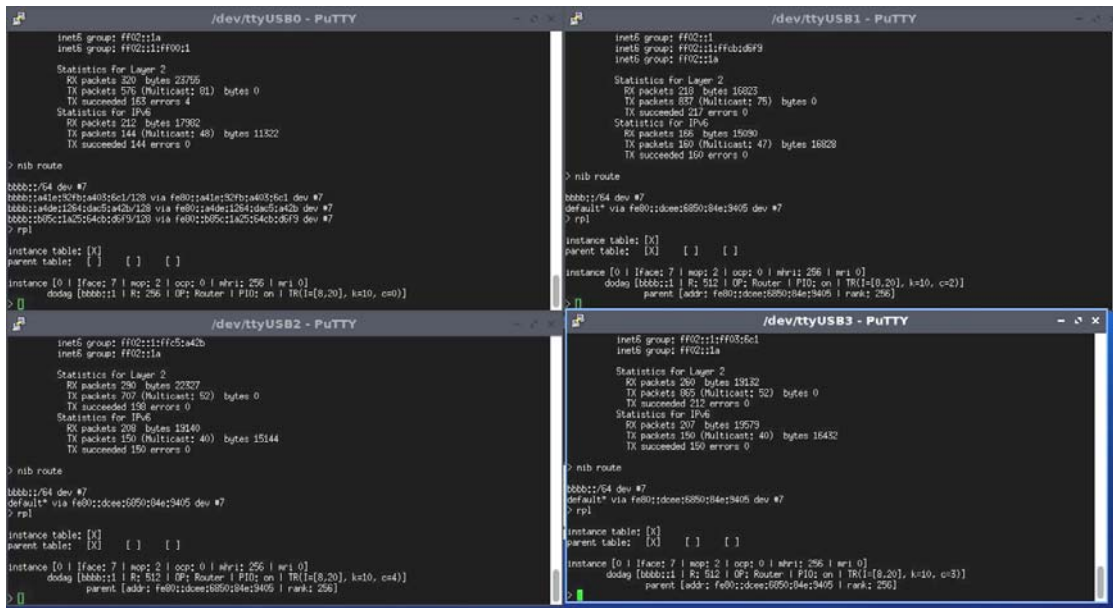


Рис. 5. Результат инициализации тестового стенда

Fig. 5. The result of initialization of the test bench



Рис. 6. Внешний вид тестовой платы полезной нагрузки

Fig. 6. Appearance of the payload test board

Заключение

В результате работы было приведено обоснование архитектурных и технических решений в соответствии с функциональными и техническими требованиями, выявленными в процессе проектирования МКА ReshUCube-2. Определен стек сетевых протоколов и технологий с учетом различных параметров настройки (режимов сжатия, маршрутизации и др.). Ключевые протоколы стека: LoRa, 802.15.4, IPv6, 6LoWPAN, RPL, TCP, UDP и CoAP. Создана аппаратная платформа, в основе которой микроконтроллер STM32WLE5CC. Выбрано и протестировано программное обеспечение: операционная система RIOT и PHY-MAC драйвер. Эти решения также могут быть полезны в перспективе развития проекта интегрированной космической сети и при разработке последующих космических миссий. Определенные в работе программные и аппаратные технологии могут быть использованы для воспроизведения полученных результатов. Кроме того, предложенный стек сетевых технологий может быть применен в иных отраслях (например, IoT, интернет транспортных средств и т. п.).

В будущем планируется провести исследование функций различных уровней предложенного сетевого стека, а также функций безопасности, как в рамках тестового стенда, так и в реальных условиях взаимодействия с МКА.

Библиографические ссылки

1. Предварительные результаты космической миссии ReshUCube-1 / В. Х. Ханов, Д. М. Зуев, А. В. Шахматов [и др.] // Решетневские чтения : материалы XXVI Междунар. науч.-практич. конф., посвященной памяти генерального конструктора ракет.-космич. систем ак. М. Ф. Решетнева, Красноярск, 09–11 ноября 2022 г. Красноярск : СибГУ им. ак. М. Ф. Решетнева, 2022. С. 452–454.
2. Liu J., Shi Y., Fadlullah Z. M. Space-Air-Ground Integrated Network: A Survey // IEEE Communications Surveys & Tutorials. 2018. Vol. 20, No. 4. P. 2714-2741. DOI: 10.1109/COMST.2018.2841996.
3. Internet of Things for Smart Cities / A. Zanella, N. Bui, A. Castellani et al. // IEEE Internet of Things Journal. 2014. Vol. 1, No. 1, P. 22–32. DOI: 10.1109/IJOT.2014.2306328.
4. Кустов Н. Д. Применение концепций интегрированной космической сети и интернета транспортных средств // Инновации в информационных технологиях, машиностроении и автотранспорте : сб. материалов VI Междунар. науч.-практич. конф. 2022. С. 378–382.
5. Кустов Н. Д., Евдокимов К. С. Определение стека сетевых протоколов и технологий для космических интегрированных сетей // Решетневские чтения : материалы XXVI Междунар. науч.-практич. конф., посвященной памяти генерал. конструктора ракет.-космич. систем акад. М. Ф. Решетнева, Красноярск, 09–11 ноября 2022 г. Красноярск : СибГУ им. ак. М. Ф. Решетнева, 2022. С. 434–436.
6. Transmission of IPv6 Packets over IEEE 802.15.4 Networks, RFC 4944 / G. Montenegro, N. Kushalnagar, J. Hui, D. Culler. DOI: 10.17487/RFC4944, September 2007 [Электронный ресурс]. URL: <https://www.rfc-editor.org/info/rfc4944> (дата обращения 03.01.2023).
7. RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks, RFC 6550 / A. Brandt, J. Hui, R. Kelsey et al. DOI: 10.17487/RFC6550. March 2012 [Электронный ресурс]. URL: <https://www.rfc-editor.org/info/rfc6550> (дата обращения 03.01.2023).
8. Shelby Z., Hartke K., Bormann C. The Constrained Application Protocol (CoAP), RFC 7252, DOI: 10.17487/RFC7252. June 2014 [Электронный ресурс]. URL: <https://www.rfc-editor.org/info/rfc7252> (дата обращения 05.01.2023).
9. IEEE Standard for Low-Rate Wireless Networks in IEEE Std 802.15.4-2020 (Revision of IEEE Std 802.15.4-2015), 23 July 2020. DOI: 10.1109/IEEESTD.2020.9144691.
10. Semtech, AN1200.22 LoRa™ Modulation Basics, Application Note [Электронный ресурс]. URL: <http://www.semtech.com/images/datasheet/an1200.22.pdf> (дата обращения 05.01.2023).
11. LoRaWAN™ Regional Parameters, LoRa Alliance [Электронный ресурс]. URL: <https://www.loraalliance.org/> (дата обращения 08.01.2023).
12. Cotrim J. R., Kleinschmidt J. H. LoRaWAN Mesh Networks: A Review and Classification of Multihop Communication // Sensors (Basel). 2020. No. 20(15). P. 4273. DOI: 10.3390/s20154273.
13. Thubert P. Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks, RFC 6282, DOI: 10.17487/RFC6282. September 2011 [Электронный ресурс]. URL: <https://www.rfc-editor.org/info/rfc6282> (дата обращения 08.01.2023).
14. Yang Y., Kumar V. Routing in IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN): A Survey // Journal of Computer Networks and Communications. 2012. DOI: <https://doi.org/10.1155/2012/316839>.
15. Neighbor Discovery for IP version 6 (IPv6), RFC 4861 / T. Narten, E. Nordmark, W. Simpson, H. Soliman. DOI: 10.17487/RFC4861. September 2007 [Электронный ресурс]. URL: <https://www.rfc-editor.org/info/rfc4861> (дата обращения 08.01.2023).

16. Hennebert C., Dos Santos J. Security Protocols and Privacy Issues into 6LoWPAN Stack: A Synthesis // IEEE Internet of Things Journal. 2014. No. 1 (5). P. 384–398. DOI: 10.1109/JIOT.2014.2359538ff.
17. Kempf J., Zill B., Nikander P. SEcure Neighbor Discovery (SEND), RFC 3971. DOI: 10.17487/RFC3971. March 2005 [Электронный ресурс]. URL: <https://www.rfc-editor.org/info/rfc3971> (дата обращения 09.01.2023).
18. Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.3, RFC 8446. DOI: 10.17487/RFC8446. August 2018 [Электронный ресурс]. URL: <https://www.rfc-editor.org/info/rfc8446> (дата обращения 09.01.2023).
19. Rescorla, E. and N. Modadugu. Datagram Transport Layer Security Version 1.2, RFC 6347. DOI: 10.17487/RFC6347. January 2012 [Электронный ресурс]. URL: <https://www.rfc-editor.org/info/rfc6347> (дата обращения 09.01.2023).
20. STMicroelectronics. Datasheet – STM32WLE5xx STM32WLE4xx [Электронный ресурс]. URL: <https://www.st.com/resource/en/datasheet/stm32wle5cc.pdf> (дата обращения 11.01.2023).

References

1. Khanov V. Kh., Zuyev D. M., Shakhmatov A. V. [Predvaritel'nyye rezul'taty kosmicheskoy missii ReshUCube-1]. *Reshetnevskiy chteniya: materialy XXVI Mezhdunarodnoy nauchno-prakticheskoy konferentsii, posvyashchennoy pamyati general'nogo konstruktora raketno-kosmicheskikh sistem akademika M. F. Reshetneva*. Krasnoyarsk, 2022, P. 452–454 (In Russ.).
2. Liu J., Shi Y., Fadlullah Z. M. Space-Air-Ground Integrated Network: A Survey. *IEEE Communications Surveys & Tutorials*. 2018, Vol. 20, No. 4, P. 2714–2741. DOI: 10.1109/COMST.2018.2841996.
3. Zanella A., Bui N., Castellani A. et al. Internet of Things for Smart Cities. *IEEE Internet of Things Journal*. 2014, Vol. 1, No. 1, P. 22–32. DOI: 10.1109/JIOT.2014.2306328.
4. Kustov N. D. [Primeneniye kontseptsii integrirovannoy kosmicheskoy seti i interneta transportnykh sredstv]. *Innovatsii v informatsionnykh tekhnologiyakh, mashinostroyenii i avtotransporte: sbornik materialov VI Mezhdunarodnoy nauchno-prakticheskoy konferentsii*. Kemerovo, 2022, P. 378–382 (In Russ.).
5. Kustov N. D., Yevdokimov K. S. [Opredeleeniye steika setevykh protokolov i tekhnologiy dlya kosmicheskikh integrirovannykh setey]. *Reshetnevskiy chteniya : materialy XXVI Mezhdunarodnoy nauchno-prakticheskoy konferentsii, posvyashchennoy pamyati general'nogo konstruktora raketno-kosmicheskikh sistem akademika M. F. Reshetneva*. Krasnoyarsk, 2022, P. 434–436 (In Russ.).
6. Montenegro G., Kushalnagar N., Hui J., Culler D. Transmission of IPv6 Packets over IEEE 802.15.4 Networks, RFC 4944. DOI: 10.17487/RFC4944. September 2007. Available at: <https://www.rfc-editor.org/info/rfc4944>.
7. Brandt A., Hui J., Kelsey R. et al. RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks, RFC 6550. DOI: 10.17487/RFC6550. March 2012. Available at: <https://www.rfc-editor.org/info/rfc6550>.
8. Shelby Z., Hartke K., Bormann C. The Constrained Application Protocol (CoAP), RFC 7252. DOI: 10.17487/RFC7252. June 2014. Available at: <https://www.rfc-editor.org/info/rfc7252>.
9. IEEE Standard for Low-Rate Wireless Networks in IEEE Std 802.15.4-2020 (Revision of IEEE Std 802.15.4-2015), 23 July 2020. DOI: 10.1109/IEEESTD.2020.9144691.
10. Semtech, AN1200.22 LoRa™ Modulation Basics, Application Note. Available at: <http://www.semtech.com/images/datasheet/an1200.22.pdf>.
11. LoRaWAN™ Regional Parameters, LoRa Alliance. Available at: <https://www.loraalliance.org/>.
12. Cotrim J. R., Kleinschmidt J. H. LoRaWAN Mesh Networks: A Review and Classification of Multihop Communication. *Sensors (Basel)*. 2020, No. 20(15), P. 4273. DOI: 10.3390/s20154273.
13. Thubert P. Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks, RFC 6282. DOI: 10.17487/RFC6282. September 2011. Available at: <https://www.rfc-editor.org/info/rfc6282>.

14. Yang Y., Kumar V. Routing in IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN): A Survey. *Journal of Computer Networks and Communications*. 2012. DOI: <https://doi.org/10.1155/2012/316839>.
15. Narten T., Nordmark E., Simpson W., Soliman H. Neighbor Discovery for IP version 6 (IPv6), RFC 4861. DOI: 10.17487/RFC4861. September 2007. Available at: <https://www.rfc-editor.org/info/rfc4861>.
16. Hennebert C., Dos Santos J. Security Protocols and Privacy Issues into 6LoWPAN Stack: A Synthesis. *IEEE Internet of Things Journal*. 2014, No. 1 (5), P. 384–398. DOI: 10.1109/JIOT.2014.2359538ff.
17. Kempf J., Zill B., Nikander P. SEcure Neighbor Discovery (SEND), RFC 3971. DOI: 10.17487/RFC3971. March 2005. Available at: <https://www.rfc-editor.org/info/rfc3971>.
18. Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.3, RFC 8446. DOI: 10.17487/RFC8446. August 2018. Available at: <https://www.rfc-editor.org/info/rfc8446>.
19. Rescorla E., Modadugu N. Datagram Transport Layer Security Version 1.2, RFC 6347. DOI: 10.17487/RFC6347. January 2012. Available at: <https://www.rfc-editor.org/info/rfc6347>.
20. STMicroelectronics. Datasheet – STM32WLE5xx STM32WLE4xx. Available at: <https://www.st.com/resource/en/datasheet/stm32wle5cc.pdf>.

© Кустов Н. Д., Евдокимов К. С., Шахматов А. В., 2023

Кустов Никита Дмитриевич – ассистент; кафедра безопасности информационных технологий, Сибирский государственный университет науки и технологий имени академика М. Ф. Решетнева. E-mail: kustovnd@sibsau.ru.

Евдокимов Климент Сергеевич – инженер; научно-производственная лаборатория «Малые космические аппараты», Сибирский государственный университет науки и технологий имени академика М. Ф. Решетнева. E-mail: klimevdokimov@mail.ru.

Шахматов Александр Владимирович – инженер; кафедра безопасности информационных технологий, Сибирский государственный университет науки и технологий имени академика М. Ф. Решетнева. E-mail: sanecsan@mail.ru.

Kustov Nikita Dmitrievich – Assistant, Department of Information Technology Security; Reshetnev Siberian State University of Science and Technology. E-mail: kustovnd@sibsau.ru.

Evdokimov Klim Sergeevich – Engineer, Research and Production Laboratory «Small Spacecraft»; Reshetnev Siberian State University of Science and Technology. E-mail: klimevdokimov@mail.ru.

Shahmatov Alexandr Vladimirovich – Engineer, Department of Information Technology Security; Reshetnev Siberian State University of Science and Technology. E-mail: sanecsan@mail.ru.
