Journal of Siberian Federal University. Engineering & Technologies, 2019, 12(5), 585-598
~ ~ ~

УДК 621.313.292

Hardware-Software Complex Protection of Telemetry and Telecontrol of Specialized Unmanned Aerial Vehicles

Vladimir V. Mitrashchuk* and Marina P. Baranova
Krasnoyarsk State Agrarian University
90 Mira, Krasnoyarsk, 660049, Russia

Received 09.04.2019, received in revised form 11.05.2019, accepted 01.06.2019

This article discusses the problem of creating a secure communication channel with specialized UAV. This problem is very relevant today, because an unprotected communication channel can destroy the UAV or distort data received from it. To solve this problem, an exchange protocol with the ability to protect transmitted information is required the core of this protocol is an encryption algorithm, based on which the algorithms for protecting the integrity, confidentiality and availability of the transmitted data for the UAV are implemented. The structure of the protocol for the secure exchange of information was developed. The selection of the hardware platform for the implementation of the software-hardware module of the protocol has been made. The results of cryptanalysis showed the feasibility of using an encryption algorithm in the protocol. The parameters of the protocol are determined, the protocol's configuration methodology is formulated depending on the possible data exchange channels in order to ensure the maximum permissible level of protection of the transmitted information, taking into account the characteristics of each channel. According to the results of this work, we can conclude that the proposed encryption algorithm is better resistant to cryptanalysis than other widely used algorithms.

Keywords: encryption algorithm, variable block fragmentation, UAV, secure information exchange protocol, hardware-software platform.

Citation: Mitrashchuk V.V., Baranova M.P. Hardware-software complex protection of telemetry and telecontrol of specialized unmanned aerial vehicles, J. Sib. Fed. Univ. Eng. technol., 2019, 12(5), 585-598. DOI: 10.17516/1999-494X-0158.

* Corresponding author E-mail address: rtimidalv@gmail.com

Программно-аппаратный комплекс защиты телеметрии и телеуправления специализированного беспилотного летательного аппарата

В.В. Митращук, М.П. Баранова
Красноярский государственный аграрный университет
Россия, 660049, Красноярск, пр. Мира, 90

В статье рассмотрена проблема создания защищенного канала связи со специализированным БПЛА. Эта проблема актуальна сегодня, потому что незащищенный канал связи может вывести БПЛА из строя или исказить данные, получаемые с него. Для ее решения необходим протокол обмена с возможностью защиты передаваемой информации. Ядро этого протокола – алгоритм шифрования, на основе которого реализуются алгоритмы защиты целостности, конфиденциальности и доступности передаваемых для БПЛА данных. В работе создана структура протокола защищенного обмена информацией, осуществлен выбор аппаратной платформы для программно-аппаратной реализации модуля протокола. Результаты криптоанализа показали целесообразность использования алгоритма шифрования в протоколе. Определены параметры протокола, сформулирована методика конфигурирования протокола в зависимости от возможных каналов обмена данными с целью обеспечения максимально допустимого уровня защиты передаваемой информации с учетом особенностей каждого канала. По результатам проведенной работы можно сделать вывод, что предложенный алгоритм шифрования более устойчив к криптоанализу по сравнению с другими широкораспространенными алгоритмами.

Ключевые слова: алгоритм шифрования, переменная фрагментация блоков, БПЛА, протокол защищенного обмена информацией, программно-аппаратная платформа.

Введение

Беспилотный летательный аппарат (БПЛА) требует повышенной защиты передаваемой информации, потому что возможность навязывания ложной или искаженной информации может повлечь за собой серьезные последствия: от недостоверности получаемых с БПЛА данных до утраты самого БПЛА.

Очень важным вопросом, требующим внимания и решения в процессе использования БПЛА в сельском хозяйстве и других областях, является вопрос защиты информационного канала связи с беспилотником, который обеспечит корректность и достоверность получаемой информации, повысит защиту беспилотника от выведения его из строя заведомо некорректными или поврежденными в процессе передачи данными, полученными по информационному каналу связи.

Схемы шифрования алгоритма «Шифратор 125» приведены в [1, 2]. Его программная реализация распространяется в рамках лицензии GPLv3 и имеет более 5000 строк (более 110 страниц формата А4) кроссплатформенного кода на языке Qt/C++. Исходный код программы доступен в [3], а также предоставляется по запросу на электронный адрес.

Цель работы – разработка протокола защищенного канала связи для повышения эффективности использования БПЛА в технологических процессах.

Для достижения цели были поставлены и решены следующие задачи:

– выбор аппаратной платформы для реализации протокола;
– проведение криптоанализа шифратора протокола;
– разработка структуры протокола на сеансовом уровне.

Выбор аппаратной платформы для реализации протокола

Одним из главных критериев выбора платформы является скорость ее работы, она должна быть сопоставима скорости работы UART интерфейса. При этом платформа должна быть мобильной, обеспечивать возможность программирования пинов, ШИМ-сигнала и поддерживать аппаратные протоколы передачи данных, таких как: I2C, UART, SPI и т.п. Ранее установлено [1], что скорость алгоритма «Шифратор 125» на ноутбуке составляет 120 килобайт/с. Но ноутбук– неподходящее устройство для встраивания его в электрические БПЛА, он недостаточно мобилен для этого и обладает избыточными техническими характеристиками. Для возможности встраивания алгоритма шифрования и «Протокола 125» [2] в технические устройства определена другая мобильная аппаратная платформа на базе процессора с архитектурой ARMhf – BeagleBone Black (BeaglePocket).

Результат расчета скорости на BeagleBone Black (BeaglePocket) с 1GHz 512 MB составляет свыше 5 килобайт/с (свыше 43 килобит/с). Случайная генерация ключа в среднем выдает скорость 12 килобайт/с (около 97 килобит/с – это стандартная скорость для большинства оборудования с поддержкой UART, попадающая в диапазон от 9.6 до 115.2 килобит/с). Увеличить скорость еще больше можно при помощи использования неприводимых многочленов меньшей степени, но это может повлиять на безопасность шифртекста. На рис. 1 показана скорость «Шифратора 125» в сравнении для процессоров разной мощности (на ноутбуке, рис. 1*a*, и на микрокомпьютере, рис. 1*b*). Данные рис. 1 показывают, что скорости работы алгоритма шифрования на микрокомпьютере достаточно для передачи данных телеметрии и команд управления БПЛА по протоколу UART.

В ходе исследования установлена зависимость скорости шифрования от конфигурационного ключа (КК). Использование КК с 1 раундом шифрования и неприводимым многочленом из 240 бит дадут на ноутбуке скорость шифрования 120 килобайт/с, а на BeagleBoneBlack (PocketBeagle) 5 килобайт/с, тогда как средняя скорость при случайно сгенерированном КК будет примерно в два раза больше. Злоумышленник может определить факт использо-

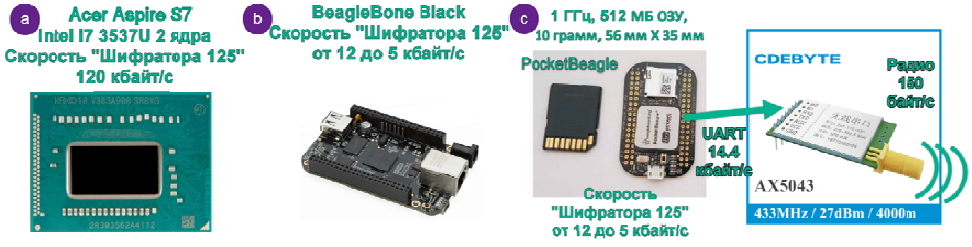


Рис. 1. Скорость шифрования на ноутбуке (a); скорость шифрования на BeagleBone Black (BeaglePocket) (b); вариант аппаратного модуля передачи данных БПЛА (c)

Fig. 1. Encryption speed on a laptop (a); Encryption speed on BeagleBone Black (BeaglePocket) (b); a variant of the UAV hardware data transfer module (c)

вания подблоков небольшого размера при скорости шифрования, большей 120 килобайт/с или 5 килобайт/с для ноутбука и платы соответственно. Для того чтобы не допустить таких случаев, рекомендуется создать дополнительный раунд, чтобы скорость шифрования не превышала значительно приведенные выше показатели. Целевая скорость подбирается при помощи фрагментации блоков от небольших к большим. На рис. 1*c* показан возможный вариант реализации аппаратного модуля телеметрии и телеуправления на данном шифре для малого сельскохозяйственного электрического беспилотного летательного аппарата (мБЭПЛА). В беспилотнике для решения задачи агрегирования информации с различных блоков устройств, находящихся в одном корпусе, можно использовать схему, где на вход PocketBeagle поступает информация для шифрования. Затем идет BeagleBoneBlack Industrial. Он собирает информацию с нескольких устройств PocketBeagle, выполняет окончательное агрегирование информации и передачу данных по Сети на большие расстояния (при использовании переходника информацию можно передавать по оптоволокну или в радиоэфире). Для проверки работоспособности шифратора проведено нагрузочное тестирование, осуществлен расчет энергопотребления в процессе шифрования. Учитывая, что мБЭПЛА в большинстве случаев работают непрерывно не более 2 ч, для проверки беспрерывного шифрования был выбран срок в 3 дня.

В табл. 1 представлены результаты тестирования энергопотребления и трехдневный тест непрерывного шифрования. Конфигурация алгоритма шифрования: три раунда, один раунд с заменой по неприводимому многочлену 240 бит, остальные – случайно сгенерированы. Размер файла шифрования 13,6 гигабайт. Аккумулятор A-Data 20000 mAh, Li-ion. Во время шифрования процессор был загружен вычислениями на 100 %. Температура окружающей среды 25 °C. Корректность шифрования проверялась по объему зашифрованных данных и по количеству прошедшего времени с учетом известной скорости шифрования алгоритма, и только в случае совпадения результатов проверка непрерывного шифрования признавалась успешной.

Таблица 1. Тестирование работы алгоритма шифрования на аппаратной платформе

Table 1. Testing the operation of the encryption algorithm on the hardware platform

Вид теста	Время	Результаты
Разряд аккумулятора и непрерывное шифрование	19.05.2018 [16:29]	Успешный запуск устройства и шифратора
Разряд аккумулятора и непрерывное шифрование	19.05.2018 [20:17]	Проверка. Непрерывное шифрование 4 ч. Потребление 2000 mAh (500 mAh/ч)
Разряд аккумулятора и непрерывное шифрование	20.05.2018 [12:07]	Проверка. Непрерывное шифрование 20 ч. Потребление 11660 mAh (728 mAh/ч)
Непрерывное шифрование	20.05.2018 [22:00]	Проверка. Непрерывное шифрование 1 день 6 ч
Непрерывное шифрование	21.05.2018 [20:23]	Проверка. Непрерывное шифрование 2 дня 2 ч
Непрерывное шифрование	22.05.2018 [02:00]	Проверка. Непрерывное шифрование 2 дня 8 ч
Непрерывное шифрование	22.05.2018 [16:30]	Проверка. Непрерывное шифрование 3 дня

Компьютерная плата, на которой проводился непрерывный тест шифрования эксплуатируется без сбоев более трех лет. Один год из трех лет плата работала практически в круглосуточном режиме, осуществляя периодические операции чтения/записи без серьезных проблем. Также ранее проведен месячный тест непрерывной работы платы с шифрованием файлов небольшой длины два раза в день в случайное время.

Все тесты «Шифратора 125» проведены на оборудовании BeagleBoneBlack (есть его компактный аналог BeaglePocket) с 1GHz-процессором и 512MB ОЗУ.

Криптоанализ шифратора протокола

В литературе рассмотрен статистический криптоанализ и описание двух критерий проверки (К1 и К2) [1]. Для оценки возможности проведения линейного криптоанализа был рассчитан строгий лавинный критерий (СЛК) [4] для «Шифратора 125», так как он является показателем хорошей конфузии и диффузии [5]. Исходное сообщение одинаково для всех ключей («Текст для тестирования СЛК шт» в таблице UNICODE). Проводили 240 замеров для каждого ключа. В каждом замере изменяли один бит блока, а полученный шифртекст сравнивали с обычным шифртекстом сообщения. Для исследования использовали второй блок с данными, первый нормировочный блок не задействовали. Получены результаты, которые показывают, что «Шифратор 125» успешно выполнил СЛК для диффузии и конфузии (табл. 2), потому что эти значения практически полностью совпадают с поведением

Таблица 2. Результаты криптоанализа диффузии и конфузии шифра

Table 2. The results of cryptanalysis of diffusion and confusion of the cipher

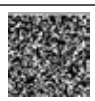
	Максимальное отклонение от ½ среди всех битов блока	Кол-во бит, выполняющих строгий лавинный критерий с точностью 0.1	Кол-во бит, выполняющих строгий лавинный критерий с точностью 0.01	Лавинный эффект	Частотный анализ
Эталон, для расчета использованы ПСП	0.10	239	53	0.50	-
Диффузия, 1 раунд, небольшие блоки	0.50	0	0	0.02	 К1:- К2: 26 %
Диффузия, 1 раунд, большой блок	0.09	240	33	0.50	 К1:+ К2: 63 %
Диффузия, 3 раунда	0.09	240	51	0.50	 К1:+ К2: 64 %
Конфузия, 1 раунд	0.50	0	0	0.49	-
Конфузия, 2 раунда	0.09	240	44	0.50	-

Таблица 3. Сравнительная таблица характеристик различных алгоритмов шифрования

Table 3. Comparative table of the characteristics of various encryption algorithms

Шифр	Блок, бит	Ключ, бит	Возможность изменения таблиц замен	Количество раундов	Переменная фрагментация блоков замен и сложения с ключом
IDEA	64	128	нет	8.5	нет
SEED	128	128	нет	16	нет
DES, 3DES, DESX	64	64, 112, 168, 184	нет	16, 48	нет
Camellia	128	128, 192, 256	нет	18, 24	нет
ГОСТ Р 34.12-2015	128	256	нет	10	нет
Twofish	128	128, 192, 256	нет	16	нет
AES	128	128, 192, 256	нет	10, 12, 14	нет
RC2, 4 (arcfour), 5, 6	32, 64, 128	0-2040	нет	1-255	нет
ГОСТ 28147-89	64	256	да, 4 бит	16, 32	нет
Blowfish	64	32-448	да, 8 бит	16	нет
CAST5, 6	128	128, 160, 192, 224	да, 8 бит	48	нет
Шифратор 125	240	0-5040<	да, 0-240 бит	0-21<	да

псевдослучайной последовательности (ПСП). ПСП использовали вместо текста. При каждом новом замере брали новую ПСП и вычитали из первой ПСП, затем все характеристики рассчитывали как и при расчете СЛК шифра. Конфузия может определяться только для ключа раунда. С учетом наличия конфигурационного ключа ключ раунда может использоваться как временный ключ [1] или для имитозащиты (в протоколе на временных ключах). Необходимо добавлять второй раунд, если требуются хорошие показатели конфузии ключа раунда, или сцепку блоков.

Проанализированы данные по возможности применения известных атак на шифраторы [6-8]. Определен перечень возможных атак на шифр с оценкой устойчивости алгоритма шифрования к ним, в частности атака полным перебором: наибольшее количество свободных входных параметров «Шифратора 125» среди других широкораспространенных решений (табл. 3) делает его защищенным от данной атаки лучше, чем другие решения; статистический криптоанализ: наличие режима сцепки блоков с вектором инициализации из ПСП, успешное выполнение статистических тестов (например, частотного анализа) [1]; атака на основе связанных ключей: ключи всегда являются случайными последовательностями (принимаются по результатам выполнения статистических тестов, например частотного анализа); дифференциальный и интегральный криптоанализ: не имеет смысла, потому что S-блоки переменной длины со случайно сгенерированными неприводимыми многочленами [9], они могут быть большими и равными размеру блока с исходным текстом. Шифр не в режиме простой замены (кодовой электронной книги), так как использована сцепка блоков. Все это сводит на нет возможность взлома шифра по каждому раунду в отдельности, зная структуру небольших блоков замен.

Структура протокола на сеансовом уровне

Основным требованием к разработке структуры протокола сельскохозяйственного БПЛА [10, 11] является наличие параметров конфигурации протокола в зависимости от типа передаваемых данных: передача команд изменения конфигурации, критичных обновлений; передача управляющих команд и телеметрии; передача большого потока данных в реальном времени, например видео и звука, обновлений системы.

Для определения структуры защищенного протокола передачи данных сформулированы ключевые параметры, повышающие безопасность передачи данных для «Протокола 125»: длина блока или ключа шифрования, количество раундов шифрования, количество временных ключей на количество переданных зашифрованных данных. Эти параметры необходимо задать таким образом, чтобы для передаваемых данных получались шифртексты с высокими показателями криптозащиты. Параметр длины блока – один из немногих фиксированных значений. Учитывая наличие режима сцепки шифра, посылку временных ключей на определенный объем информации, аутентификацию и взятие хэша, в том числе учитывая наличие конфигурационного ключа в протоколе, менять его нет необходимости. Блок из 240 бит для таблицы UNICODE позволяет зашифровать 15 символов, иначе говоря, он работает «на уровне» слов и небольших словосочетаний. Повторения в словах достаточно редки, тем более в словосочетаниях, учитывая непредсказуемость смещения их начала, в отличие от символов. А благодаря сцепке по предыдущему шифртексту проблему повторений можно исключить практически полностью. Сцепка обеспечивает защиту от повторений в рамках одного временного ключа, смена временного ключа меняет все последовательности сцепок на новые, аутентификация и хэш каждого сообщения не дают возможности использовать какие-то его части, конфигурационный ключ делает неизвестным все свободные параметры «Шифратора 125». На рис. 2-6 можно ознакомиться с созданной схемой инициализации сессии протокола.

Количество раундов шифрования может изменяться для обеспечения большего множества уникальных конфигураций ключа, выполнения тестов на больших объемах данных. Максимальная длина общего ключа определяется количеством раундов, а минимальная – дополненным до кратности 240 бит введенным общим ключом. Дополнение происходит копированием необходимого количества бит из начала общего ключа. Параметр объема данных в сообщении для одного временного общего ключа создает незначительную избыточность, но и повышает безопасность шифра и делает уникальным каждую пересылку данных в сообщении, даже если они повторяются. Следующие параметры определены непосредственно в протоколе (они не зависят от шифратора): задержка повторной посылки пакета, диапазон случайной добавки к задержке повторной посылки пакета, количество попыток до потери сессии, количество попыток до потери соединения, количество шагов таймера до повторной посылки параметров режима без уведомлений, режим передачи с уведомлением или без, количество попыток до признания ошибки аутентификации, количество попыток до повторного создания пакета из исходных данных. Количество раундов выбирается для повышения надежности в случае избыточной пропускной способности канала и отсутствия требований по энергоэффективности либо когда шифртекст не проходит результаты тестирования. В случае передачи команд изменения конфигурации необходимо одну команду слать в отдельном сообщении, так как для каждого сообщения есть новый временный ключ. Это обеспечивает наибольшую защиту целостности и

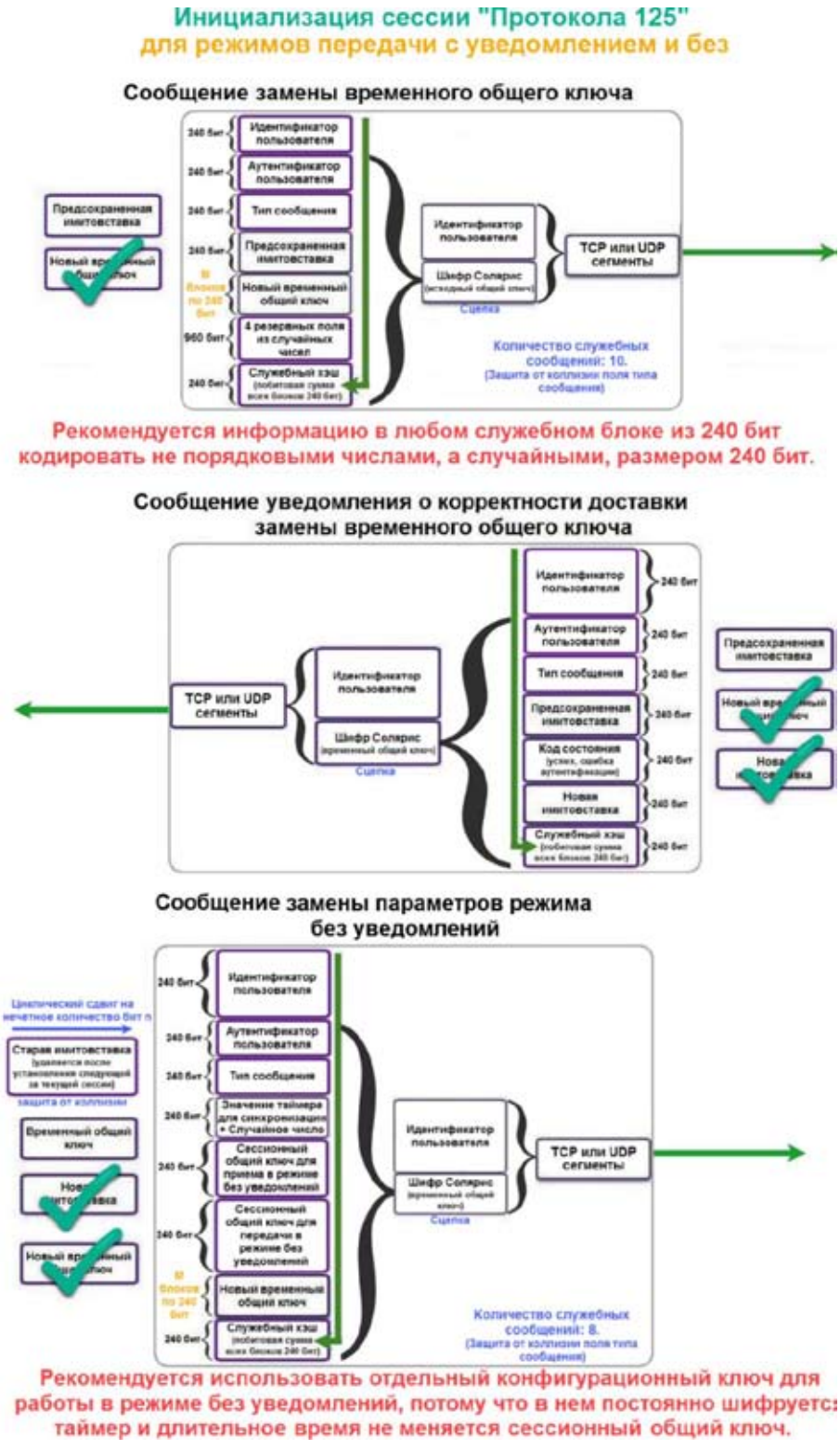


Рис. 2. Схема работы протокола (часть 1)

Fig. 2. Protocol operation diagram (part 1)

Рис. 3. Схема работы протокола (часть 2)

Fig. 3. Protocol operation diagram (part 2)

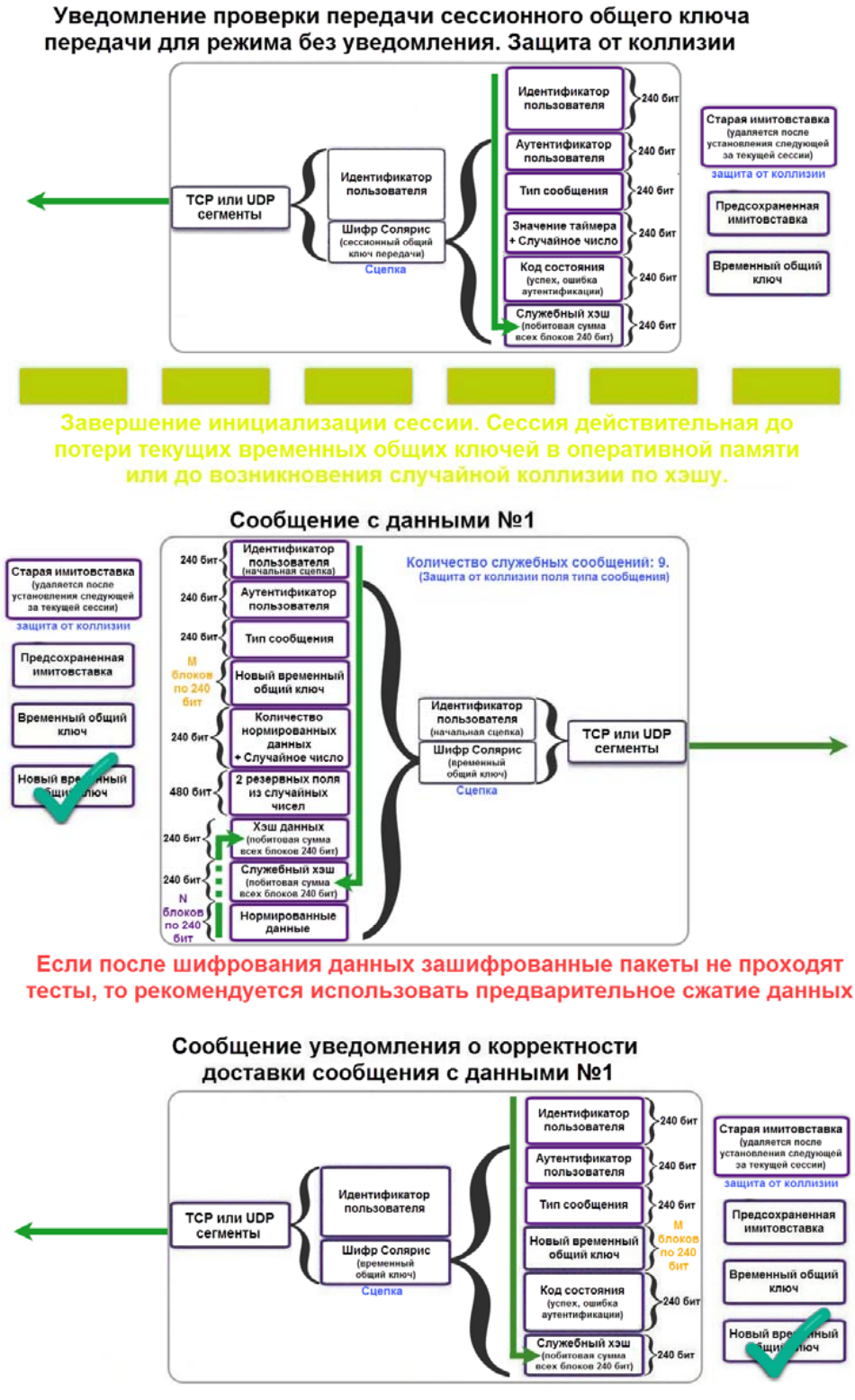


Рис. 4. Схема работы протокола (часть 3)

Fig. 4. Protocol operation diagram (part 3)

Рис. 5. Схема работы протокола (часть 4)

Fig. 5. Protocol operation diagram (part 4)

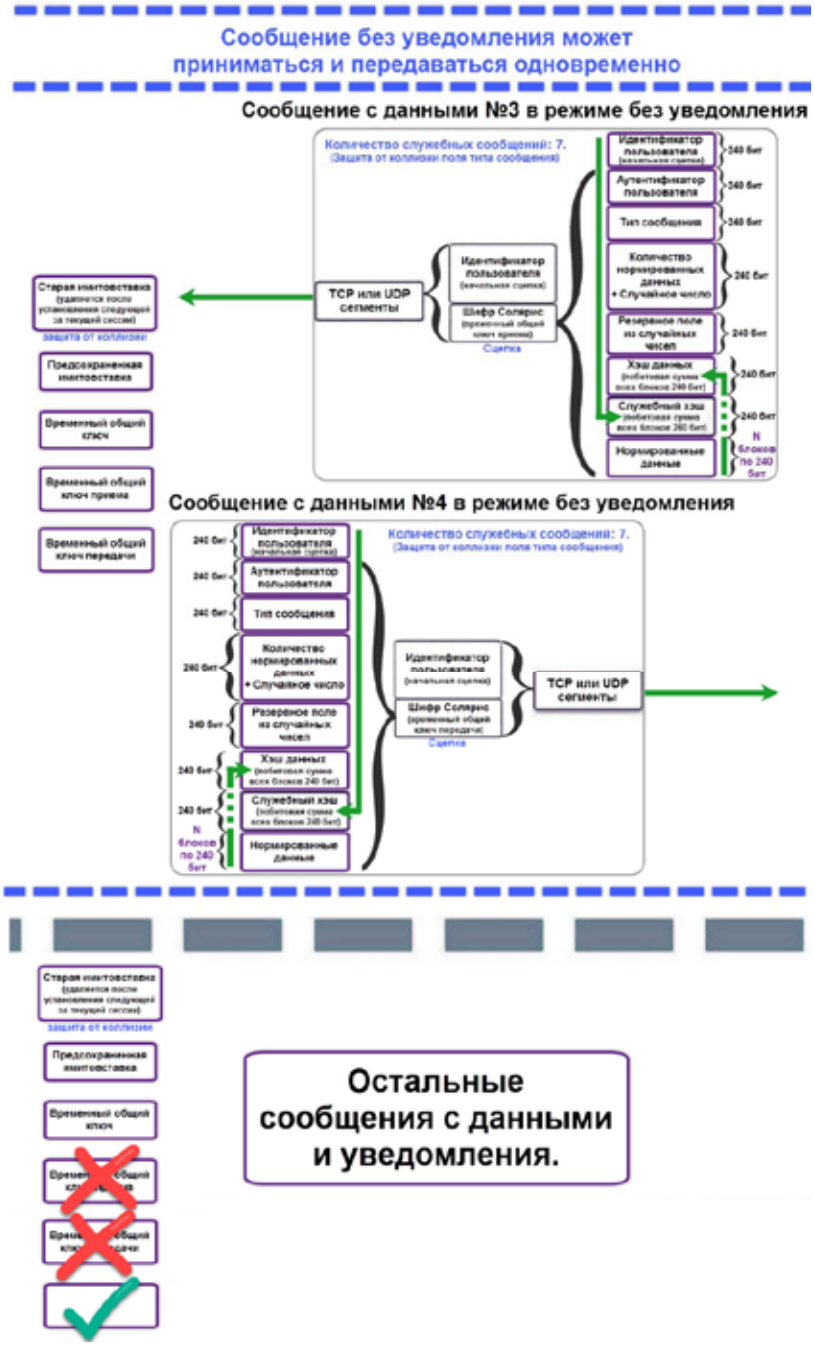


Рис. 6. Схема работы протокола (часть 5)

Fig. 6. Protocol operation diagram (part 5)

конфиденциальности. Для дополнительной защиты от коллизий необходимо слать минимум 3-5 сообщений с одинаковой командой подряд. Шифртекст конфигурируется с лучшими показателями криптозащиты. Раунды можно увеличивать, так как не требуется большая скорость обмена информацией. В случае передачи команд управления или данных телеметрии скорость

играет большую роль, но все равно можно при необходимости увеличить количество раундов. Так как данные команд управления не влияют на конфигурацию и постоянно обновляются, рекомендуется не защищать данные сообщения от возможности возникновения коллизий. Защита нужна, если параметр долго не обновляется и за это время оператор или программа может принять неправильное решение без возможности последующей корректировки. Тогда можно слать несколько сообщений, чтобы максимально снизить вероятность появления коллизий. Параметры телеметрии и управляющие команды можно отправлять в одном сообщении в соответствии с установленным параметром максимальной нагрузки данных на один временный ключ. В случае посылки потоковых данных большого объема, например видео или аудио, рекомендуется использовать только один раунд шифрования и режим без уведомлений.

Заключение

В результате проведенных исследований:

- произведен выбор программно-аппаратной платформы BeagleBone Black (BeaglePocket). Эта платформа позволяет внедрить разрабатываемый протокол в конструкцию БПЛА и использовать его для обеспечения защищенной передачи данных. Результаты тестирования непрерывности работы в процессе шифрования, энергопотребления платы подтвердили эффективность ее использования в БПЛА для обеспечения защищенного канала связи;
- результаты криптоанализа алгоритма шифрования протокола показали, что он лучше других широко распространенных алгоритмов устойчив к криптоатакам, так как имеет: наибольшее количество свободных входных параметров алгоритма; возможность изменения таблиц замен размером от 0 до размера блока шифра; переменную фрагментацию блоков на подблоки любого количества и любой длины;
- разработана структура протокола на сеансовом уровне. Наличие проверки хэша по шифру, а не по HMAC практически полностью исключит возможность навязывания подложной информации. Наличие хэша служебных полей и хэша данных обеспечит защиту корректности получаемой с беспилотника информации. Расшифровка и проверка хэша служебных полей до расшифровки данных повысит защищенность от вызова отказа в обслуживании беспилотника. Уникальное количество блоков служебных полей для каждого типа сообщения протокола обеспечит защиту от коллизии служебных полей. Все это практически полностью исключит возможность выведение беспилотника из строя через информационный канал связи.

Список литературы

[1] Митращук В.В. Разработка, тестирование и оценка шифратора с переменной фрагментацией блока для протокола безопасного обмена информацией. *Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки*. Москва: Научные технологии, 2018, 7, 118-125 [Mitrashchuk V.V. Development, testing and evaluation of a variable block fragmentation cipher for a secure communication protocol. *Modern science: current problems of theory and practice. Series: Natural and Technical Sciences*. Moscow: Scientific Technologies, 2018, 7, 118-125 (in Russian)]

[2] Митращук В.В. Протокол безопасного обмена данными на основе алгоритма шифрования с переменной фрагментацией блока. *Молодежь. Общество. Современная наука*, *техника и инновации*. Красноярск: Сиб. гос. аэрокосмич. ун-т., 2017, 299-301. [Mitrashchuk V.V. A secure data exchange protocol based on a variable block fragmentation encryption algorithm. *Youth. Society. Modern science, technology and innovation*. Krasnoyarsk: Siberian State Aerospace University, 2017, 299-301. (in Russian)]

[3] *Шифратор 125* [Электронный ресурс] – Режим доступа: https://github.com/malfis/Shifr] – Заглавие с экрана. [Shifrator 125 [Electronic resource] – Access: https://github.com/malfis/Shifr

[4] *Лавинный эффект* [Электронный ресурс] – Режим доступа: http://wp.wiki-wiki.ru/wp/index.php/Лавинный_эффект – Заглавие с экрана. [Avalanche effect [Electronic resource] – Access: http://wp.wiki-wiki.ru/wp/index.php/Лавинный_эффект]

[5] Shannon C.E. *Communication Theory of Secrecy Systems*. 1949, 28, 656-715.

[6] *Блочные шифры и их криптоанализ* [Электронный ресурс] – Режим доступа: http://cryptowiki.net/index.php?title=Блочные_шифры_и_их_криптоанализ/ – Заглавие с экрана. [Block ciphers and their cryptanalysis [Electronic resource] – Access: http://cryptowiki.net/index.php?title=Блочные_шифры_и_их_криптоанализ/]

[7] A Tutorial on Linear and Differential Cryptanalysis [Electronic resource] – Access: http://www.engr.mun.ca/~howard/PAPERS/ldc_tutorial.pdf

[8] Шнайер Б. *Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си*. Москва: Триумф, 2002. [Schneier B. *Applied cryptography. Protocols, algorithms*, *source texts in the C language*. Moscow: Triumph, 2002 (in Russian)]

[9] Митращук В.В. Устройство телеметрии и телеуправления с защитой передаваемой информации для сельскохозяйственного БПЛА. Сборник статей по материалам XIV международной научно-практической конференции «*Инновации в науке и практике*» (18 февраля 2019 г., г. Барнаул). В 2 ч. Уфа: Дендра, 2019, 152-161. [Mitrashchuk V.V. Telemetry and telecontrol device with the protection of transmitted information for agricultural UAV. Collection of articles based on the materials of the XIV International Scientific and Practical Conference "*Innovations in Science and Practice*" (February 18, 2019, Barnaul). In 2 parts, Ufa: Dendra, 2019, 152-161 (in Russian)]

[10] Митращук В.В., Баранова М.П. Применение беспилотного летательного аппарата в агропромышленном комплексе с целью автоматизации процессов на фермерских производствах. Материалы международной научной конференции "*ПРОБЛЕМЫ СОВРЕМЕННОЙ АГРАРНОЙ НАУКИ*". Красноярск: КГАУ, 2018, 107-110. [Mitrashchuk V.V., Baranova M.P. The application of an unmanned aerial vehicle in the agro-industrial complex with the aim of automating processes at farm production. Materials of the international scientific conference "*PROBLEMS OF MODERN AGRARIAN SCIENCE*". Krasnoyarsk, KGAU, 2018, 107-110 (in Russian)]

[11] Митращук В.В., Баранова М.П. Возможность использования малых электрических беспилотников в агропромышленном и лесном комплексе Сибири. Сборник III Всероссийской (национальной) научной конференции "*РОЛЬ АГРАРНОЙ НАУКИ В УСТОЙЧИВОМ РАЗВИТИИ СЕЛЬСКИХ ТЕРРИТОРИЙ*". Новосибирск: НГАУ, 2018, 625-628. [Mitrashchuk V.V., Baranova M.P. The possibility of using not big electric UAVs in the agro-industrial and forestry complex of Siberia. Collection of the III All-Russian (National) Scientific Conference *"ROLE OF AGRARIAN SCIENCE IN SUSTAINABLE DEVELOPMENT OF* RURAL *TERRITORIES"*, Novosibirsk, NGAU, 2018, 625-628 (in Russian)]