УДК: 004.056

В.В. Баранов[2], М.А. Гудков[1], А.М. Крибель[1], О.С. Лаута[1], А.П. Нечепуренко[1]

[1]Россия, г. Санкт-Петербург, Военная академия связи им. С.М. Буденного
[2]Россия, г. Новочеркасск, Южно-Российский государственный политехнический университет имени М.И. Платова

ЗАЩИТА КАНАЛА УПРАВЛЕНИЯ РОБОТИЗИРОВАННЫХ СИСТЕМ

В статье разработан робототехнический комплекс и система, позволяющая управлять этим комплексом по надежному криптографически стойкому соединению. Основным элементом данной системы является криптографический чип stm32f415. Он позволяет уменьшить нагрузку на центральный процессор для выполнения алгоритмов управления, освободив его от криптографических операций, тем самым, гарантируя выигрыш во времени.

Ключевые слова: канал управление, киберфизические системы, роботизированные системы, криптографические алгоритмы.

Автоматизированные и роботизированные системы обладают неразрывной связью между входящими в них вычислительными и физическими элементами. Сегодня представители таких систем могут быть найдены в самых разнообразных областях – космос, автомобильные, химическая технология, гражданская инфраструктура, энергетика, здравоохранение, производство, транспорт, и потребительские устройства. Такой класс систем часто рассматривается как киберфизические системы.

С целью проверки работы криптографического ускорителя была разработана роботизированная система (рисунок 1), состоящая из следующих частей:

– BeagleBone Black (главный процессор роботизированной системы);
– Mini Maestro 18-Channel USB Servo Controller (драйвер–двигатель);
– MG996R (сервоприводы);
– STM32F415 (криптографический чип);
– блок питания;
– Wifi адаптер.

Корпус представляет собой металлический скелет, который связывает и объединяет необходимую периферию в единое целое, при этом, обеспечивая защиту и целостность компонентов. Все детали, из которых он состоит, были

спроектированы в программе КОМПАС–3D V16 и вырезаны на фрезерном станке. Управление роботизированной системой осуществляется использованием wi-fi адаптера в качестве передатчика радиосигнала.

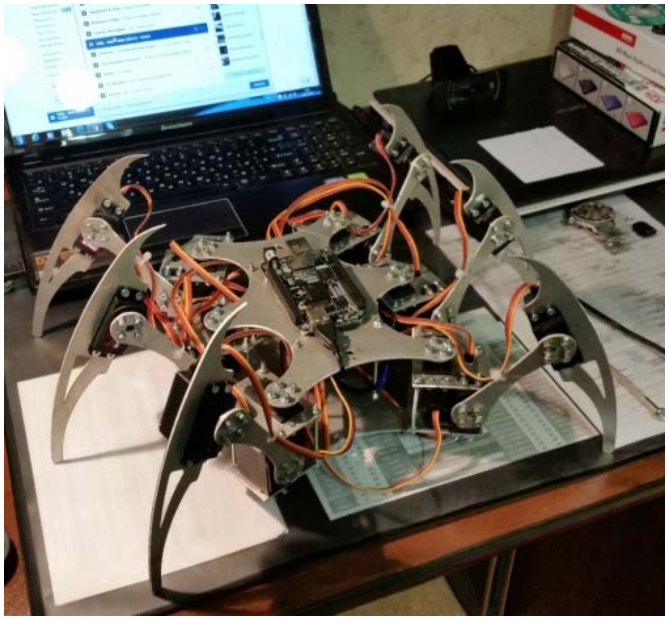

Рисунок 1 – Роботизированная система в сборке

Для обеспечения криптографически стойкого протокола управления в роботизированной системе используется микроконтроллер с 32-разрядным ядром ARM Cortex–M4F с криптографическим ускорителем stm32f415rgt производства компании «STMicroelectronics».

Используя техническую документацию, был проведен анализ выводов криптографического чипа с выводами микроконтроллера stmf0, после которого было принято решение внедрить чип в плату stm32f0discovery, заземлив несколько контактов (рисунок 2).

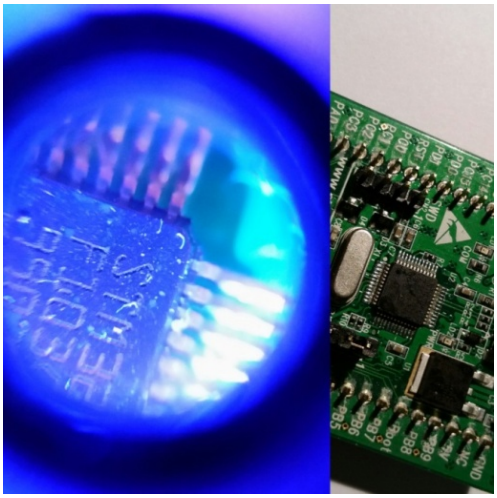

Рисунок 2 – Криптографический чип STM32F415

Для того, чтобы чип дешифровал принятые пакеты, в качестве алгоритма дешифрования использовался AES с длиной ключа 128 бит. Данный алгоритм был выбран за своё быстродействие и криптостойкость.

В качестве алгоритма распределения ключей был рассмотрен и реализован алгоритм Диффи–Хеллмана, который позволяет двум сторонам получить общий секретный ключ, используя незащищенный от прослушивания, но защищенный от подмены, канал связи.

Функциональная схема криптографически стойкого протокола управления роботизированной системой представлена на рисунке 3.

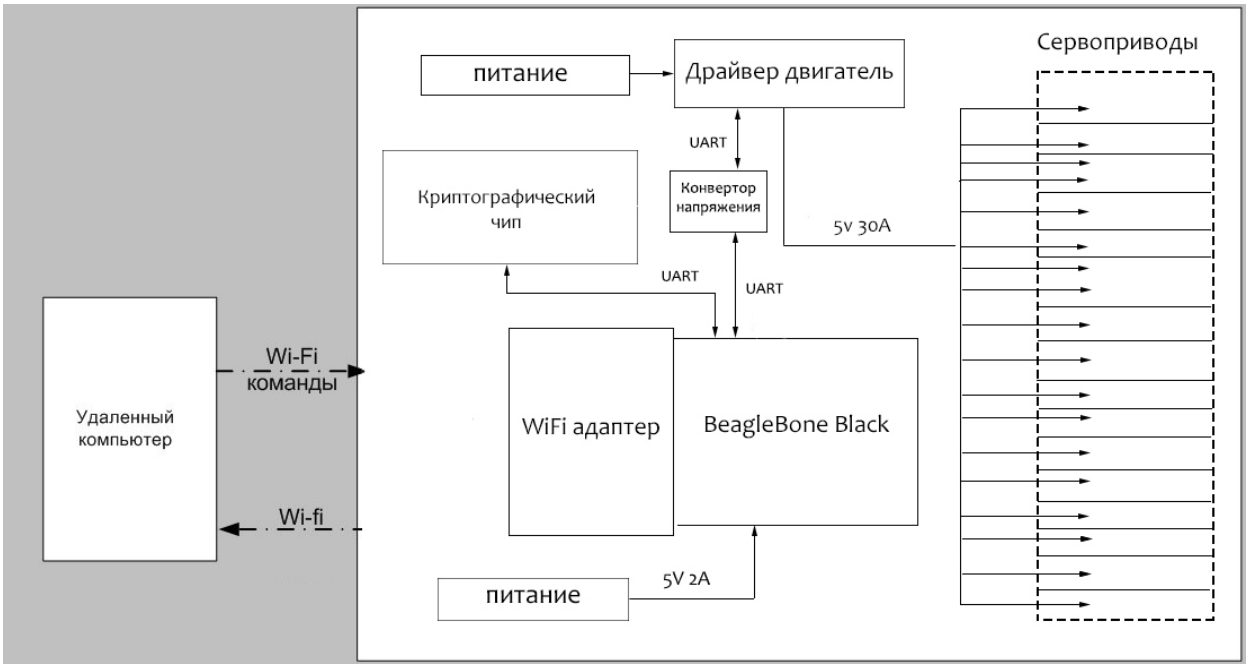

Рисунок 3 – Функциональная схема

В качестве центрального процессора и электронного мозга для робота был выбран одноплатный компьютер BeagleBone Black (BBB).

С целью подключения драйвера-двигатель (Mini Maestro 18–Channel USB Servo Controller) к главному процессору (BeagleBone Black) по UART–интерфейсу был взят конвертор AduM1201, который предназначен для преобразования электроэнергии одних параметров или показателей качества в электроэнергию с другими значениями параметров или показателей качества. На рисунке 4 изображена плата перед вытравкой, нарисованная в программе P–CAD 2006.

Для того чтобы провести исследования реализованной криптографической системы на предмет обнаружения проблем и ошибок, был осуществлен перехват и анализ передаваемых пакетов с помощью программы Wireshark.

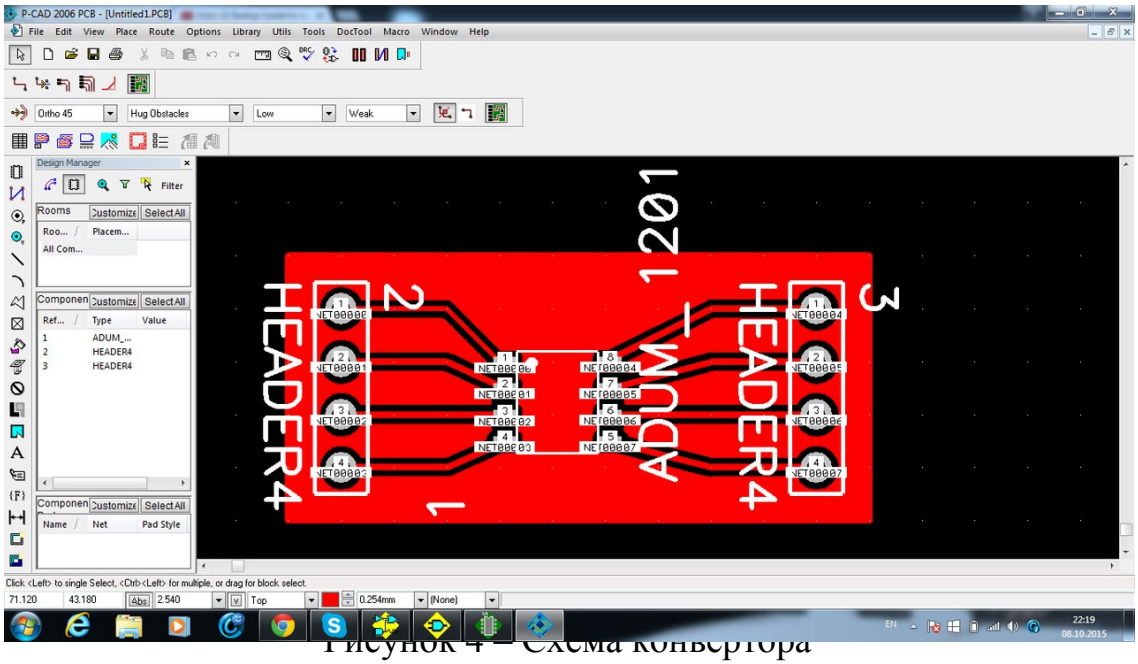

Рисунок 4 – Схема конвертора

На рисунке 5 можно увидеть, что с помощью Клиентской программы, передается сообщение «ololololo» роботу в открытом (незашифрованном) виде.

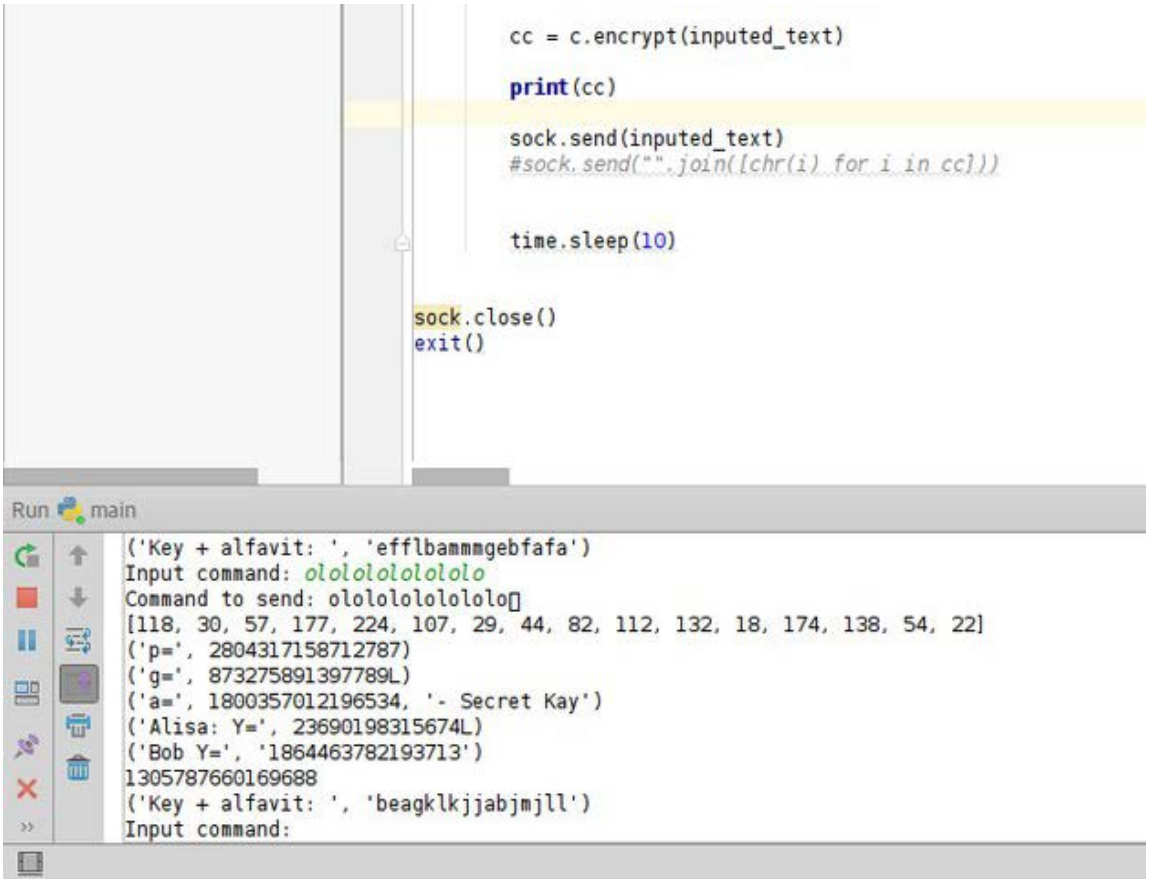

Рисунок 5 – Передача незашифрованного сообщения роботизированной системе

Предварительно авторизовавшись в wi-fi сети, нужно запустить Wireshark, с помощью которого будут перехвачены передаваемые пакеты. На рисунке 6 видно отправляемое слово.

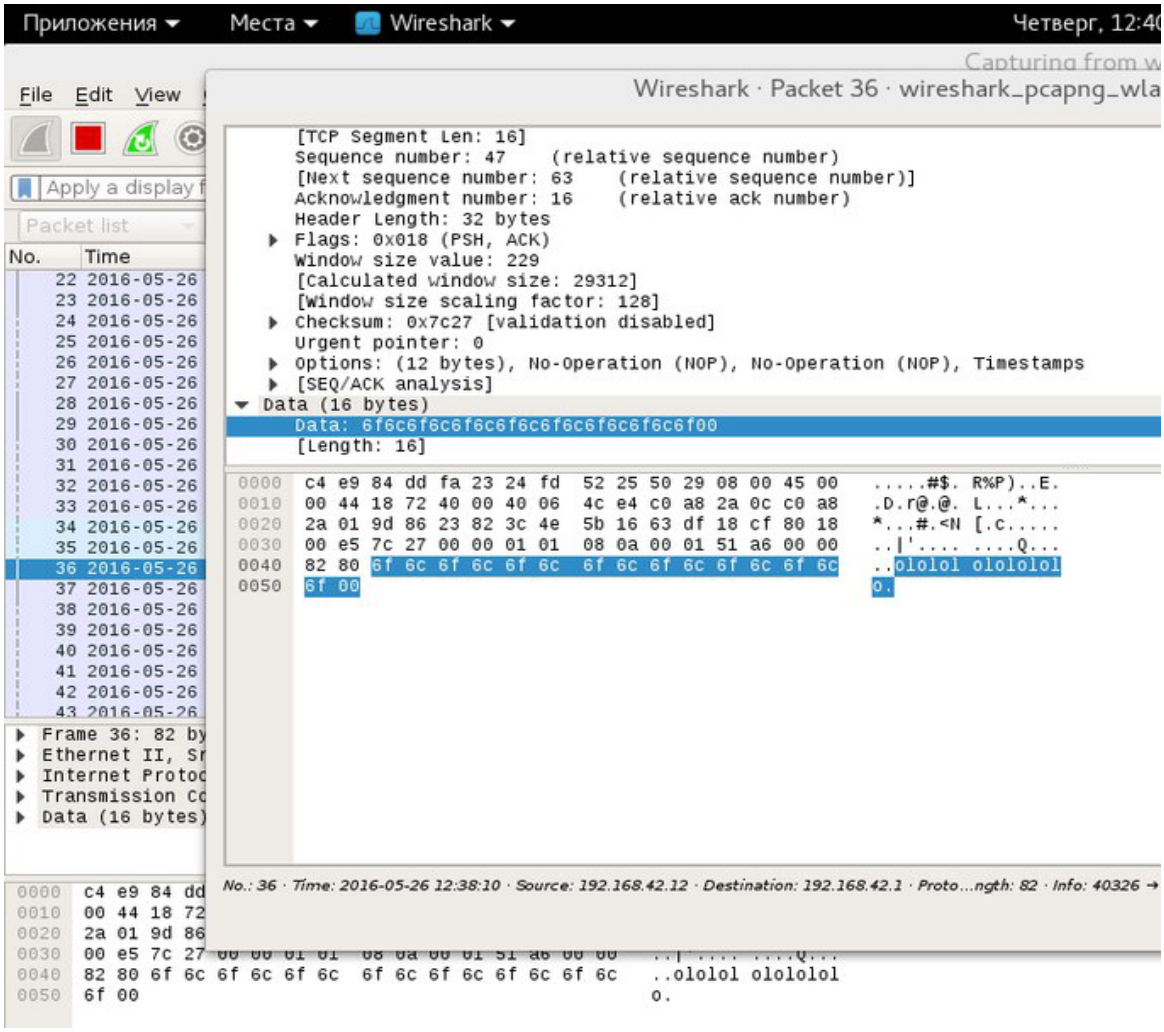

Рисунок 6 – Перехват незашифрованного сообщения с помощью программы Wireshark

Теперь передаем зашифрованное слово. Находим передаваемый пакет и видим шифротекст длиной в 16 байт (рисунок 7).

Анализ пакетов реализованной криптографической системы на предмет обнаружения проблем и ошибок с помощью программы Wireshark показал, что команда, передаваемая роботизированной системе, является зашифрованной а шифрование wi-fi сети (WPA2), в отличие от технологии Bluetooth, является дополнительным препятствием к расшифрованию секретной команды злоумышленником. Кроме этого, организована постоянная смена криптоключей, тем самым исключена возможность их подбора.

Таким образом, в настоящей статье представлен пример создания роботизированного комплекса, как элемента КБС, с защищенной системой управле-

ния им на основе алгоритма шифрования AES, являющимся на сегодняшний момент наиболее криптостойким.

Кром того, для защиты от атаки «грубого перебора» криптографического ключа в системе управления необходимо реализовывать алгоритм распределения ключей, позволяющий генерировать новый ключ, каждый раз перед выполнением команды.

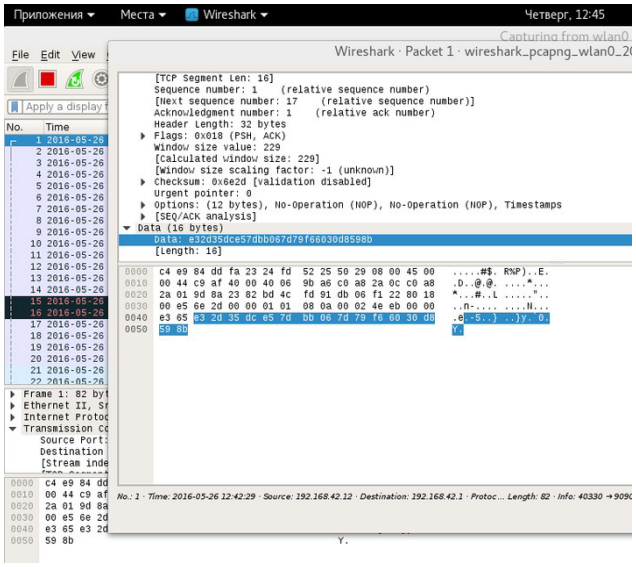

Рисунок 7 – Перехват зашифрованного сообщения с помощью программы Wireshark

Литература

1. Reference manual STM32F405/415, STM32F407/417, STM32F427/437 and STM32F429/439 advanced ARM®–based 32–bit MCUs [Электронный ресурс] // STMicroelectronics, 2016 — 1744 с.

2. Схема обмена ключами Диффи — Хеллмана [Электронный ресурс] // URL: http://kaf403.rloc.ru/POVS/Crypto/DiffieHellman.html

3. [BeagleBone Black] Enable All UART Ports at Boot [Электронный ресурс] // URL: https://billwaa.wordpress.com/2014/10/13/beaglebone–black–enable–all–uart–ports–at–boot.

4. Hexapod–робот под управлением ROS [Электронный ресурс] // URL: http://www.pvsm.ru/diy–ili–sdelaj–sam/62026.