2. Ковалева Т. Ю., Ермаков А. В., Иванов А. В., Ковалева А. Г., Старобинец И. М. Результаты разработки селективных защитных материалов для подвижных объектов военной техники // Актуальные проблемы защиты и безопасности: материалы всерос. научн.-практ. конф. Т. 3. Санкт-Петербург, 5–7 апреля 2014 г. М. : ИД ФГБУ РАРАН, 2014. С. 379–385.

3. Ковалева Т. Ю. Звукорадиопоглощающее покрытие. Пат. 132923 Российская Федерация; заявитель и патентообладатель Федеральное государственное образовательное бюджетное учреждение высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича». – 2013107890/08; заявл. 21.02.2013; опубл. 27.09.2013.

МЕТОД ОБНАРУЖЕНИЯ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ НА БАЗЕ АНАЛИЗА ТРАФИКА

Р.В. Киричек, А.А. Кулешов, А.Е. Кучерявый

С увеличением популярности беспилотных летающих аппаратов (БПЛА) и их доступности в 2014–2015 гг. значительно возросло число аварий и столкновений с препятствиями. В связи с этим, в 2015 г. в Российской Федерации, а также ряде других стран были приняты законы, регулирующие правила пилотирования и полетов БПЛА. Одним из основных положений данных законов явилась обязательная регистрация всех БПЛА тяжелее 250 граммов. В связи с появлением нормативно-правовой базы относительно БПЛА остро встает вопрос о незаконной эксплуатации незарегистрированных БПЛА лицами, не имеющих разрешения на выполнение полетов. Решением сложившейся ситуации является разработка аппаратуру, которая позволит зафиксировать факт запуска БПЛА, его координаты и координаты оператора, а также экстренно совершить посадку такого БПЛА. В статье предложен метод и алгоритм по обнаружению БПЛА и сопутствующих параметров полета на основе анализа сетевого трафика, перехваченного в радиоэфире.

Ключевые слова: беспилотный летательный аппарат, обнаружение, трафик, кадр, анализ, перехват

METHODS FOR DETECTION OF UNMANNED AERIAL VEHICLES BASED ON THE ANALYSIS OF NETWORK TRAFFIC

Kirichek R., Kuleshov A., Koucheryavy A.

With the increasing popularity of unmanned aerial vehicles (UAVs), and their availability in 2014-2015 significantly increased the number of accidents and collisions with obstacles. In this regard, in 2015 in the Russian Federation, as well as other countries the laws governing piloting rules and UAV flights were adopted. One of the main provisions of these laws was the mandatory registration of all UAV 250 grams heavier. In connection with the advent of the regulatory framework regarding the UAV sharply raises the question of the illegal exploitation of undocumented UAV persons who do not have permission to perform the flight. Decision of the situation is to develop equipment that will allow to fix the fact launch the UAV, its coordinates and the coordinates of the operator, as well as an emergency landing of the UAV. This paper proposes a method and an algorithm for the detection of UAVs and associated flight parameters based on the analysis of network traffic, intercepted the radio.

Key words: Unmanned aerial vehicle, detection, traffic, frame analysis, interception.

Обзор метода обнаружения БПЛА на основе анализа данных протокола MAVLink

Данный метод предоставляет возможность обнаружения БПЛА, а также оператора, управляющего им. Использование данного подхода целесообразно в случаях, когда управление осуществляется в реальном времени с помощью пульта дистанционного управления. Описанный метод подходит для большинства БПЛА общего пользования, реализованных на базе полетных контроллеров популярных торговых марок таких, как DJI Innovations, 3D Robotics, Blade, Parrot и др., а также большинства самодельных летательных аппаратов.

Исследования по тестированию метода обнаружения БПЛА на базе анализа сетевого трафика проводились в лаборатории Интернета Вещей СПбГУТ [1]. Один из сегментов модельной сети представлен в виде летающей сенсорной сети на базе квадрокоптеров IRIS+ от компании 3D Robotics [2, 3, 4]. На базе данного сегмента отрабатываются задачи по исследованию полного жизненного цикла размещения и обслуживания сети датчиков в отдаленных районах [5, 6], расчет оптимальных траекторий по облету сенсорных узлов [7], обнаружению преднамеренных электромагнитных воздействий на узлы сети и каналы связи [8], а также возможные методы деинсталляции сенсорной сети на завершающей стадии.

Рассмотрим упрощенную схему управление БПЛА на примере типового квадрокоптера с полетным контроллером Pixhawk от компании 3D Robotics (рис. 1).

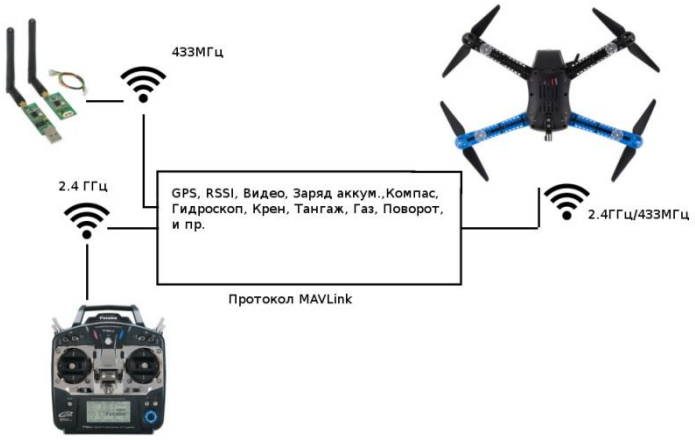

Рис. 1. Схема управления БПЛА типового квадрокоптера с полетным контроллером Pixhawk

Как видно из рисунка 1 управление осуществляется с помощью приемопередатчика 3DR radio v2 по частоте 433 МГц и пульта дистанционного управления на частоте 2,4 ГГц. Информационный обмен осуществляется в пакетном режиме с использованием протокола MAVLink. Данный протокол не использу-

ет шифрование и применяется в большинстве БПЛА общего пользования самолетного и вертолетного типа.

Структура кадра в протоколе MAVLink была описаны в 2009 г. Лоренц Майером и находятся в открытом доступе (LGPL лицензия) [9].

На рисунке 2 представлена структура кадра в протоколе MAVLink. Длина кадра составляет от 8 до 263 байт. Кадр имеет типовые поля, характерные для кадров Ethernet: поле данных, служебные поля, контрольная сумма и др.

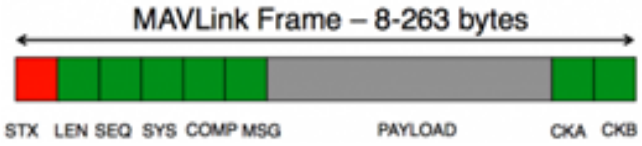

Рис. 2. Структура кадра в протоколе MAVLink

В таблице представлено описание различных типов кадров в протоколе MAVLink, допустимых значений и их особенностей.

ТАБЛИЦА. Описание различных типов кадров в протоколе MAVLink

	Знач. байта	Содержание	Значения	Особенности
STX	0	Packet start sign	v1.0: 0xFE (v0.9: 0x55)	Указывает на начало нового пакета
LEN	1	Payload length	0 - 255	Указывает длину следующего полезной нагрузки.
SEQ	2	Packet sequence	0 - 255	Каждый компонент подсчитывает его последовательность отправки. Позволяет обнаруживать потерю пакетов
SYS	3	System ID	1 - 255	Идентификатор передающей системе. Позволяет дифференцировать различные MAVS в той же сети.
COMP	4	Component ID	0 - 255	ID представляемого компонента. Позволяет дифференцировать различные компоненты системы, таким же, например, IMU и автопилот.
MSG	5	Message ID	0 - 255	Идентификатор сообщения - ID определяет, что полезной нагрузки "означает" и как она должна быть правильно декодировать.
PAYLOAD	6 to (n+6)	Data	(0 - 255) bytes	Данные сообщения, зависит от идентификатора сообщения.
CKA CKB	(n+7) to (n+8)	Checksum (low byte, high byte)	ITU X.25 / SAE AS-4 хэш, за исключением стартового пакета знака, так байта 1 .. (n + 6). Примечание: сумма также включает в себя MAVLINK_CRC_EXTRA (Количество вычисляется из полей сообщения защищает пакет от декодирования другую версию тот же самый пакет, но с различными переменными).	

Ниже представлен пример структуры перехваченного кадра MAVLink и его расшифровка, согласно таблице.

Пакет: 000001 01:41:58.680 FE 19 D3 01 01 16 00 00 00 00 10 01 B6
00 43 4F 4D 50 41 53 53 5F 4C 45 41 52 4E 00 00 00 02
000002 01:41:58.682 43 12

0) FE начало пакета.

2) d3 позволяет обнаруживать потерю кадров. 211(dec).

3) 01 позволяет идентифицировать аппарат.

4) 01 позволяет идентифицировать датчики в аппарате.

5) 16 позволяет определить, тип сообщения и метод его декодирования.

6) 00 00 00 00 10 01 B6 00 43 4F 4D 50 41 53 53 5F 4C 45 41 52 4E 00 00 00 02 полезное сообщение.

7–8) 43 12 контрольная сумма для проверки целостности кадра.

Преобразовав, данные полезного сообщения в кодировку win-1251 получим сообщение: COMPASS_LEARN и два числовых значения. Это значения с бортового компаса БПЛА [10].

Согласно предлагаемого метода, декодирование осуществляется на наземной станции или портативном приборе, обладающего соответствующей вычислительной мощность. Для контроля канала взаимодействия БПЛА и оператора в радиоэфире происходит постоянный обмен кадрами, содержащими параметр показателя уровня принимаемого сигнала RSSI (*Received Signal Strength Indicator*). Таким образом, осуществив перехват и последующий анализ данных кадров с параметрами RSSI возможно вычислить расстояние между источником сигнала (БПЛА) и приемником (пульт дистанционного управления). Кроме этого, получив значения RSSI в трех разных точках нахождения БПЛА, а также параметры с бортового GPS-приемника БПЛА можно составить уравнения [11]:

$$EO = \sqrt{(x_o - x_e)^2 + (y_o - y_e)^2 + (z_o - z_e)^2},$$

$$BO = \sqrt{(x_o - x_b)^2 + (y_o - y_b)^2 + (z_o - z_b)^2},$$

$$CO = \sqrt{(x_o - x_c)^2 + (y_o - y_c)^2 + (z_o - z_c)^2},$$

где координаты точки O – местоположение пульта дистанционного управления (ПДУ), а координаты точек E, B и C – местоположение БПЛА. Обнаружив местоположение ПДУ возможно задержать оператора БПЛА.

На рисунке 3 представлена схема определения координат ПДУ по расстоянию в разный момент времени полета БПЛА.

Альтернативный вариант обнаружения ПДУ возможен с помощью перехвата кадров, содержащих GPS координаты ПДУ. Как показал натурный эксперимент, данные кадры передаются в канале связи для использования вспомогательных функций БПЛА, например функция «следуй за мной», но стоит отметить, что такой тип кадров поддерживается не во всех типах БПЛА.

Основываясь на вышеизложенном, был разработан алгоритм нахождения ПДУ (рис. 4), который лег в основу разработки специализированного портативного программно-аппаратного комплекса по обнаружению и контролю незаконных запусков БПЛА общего пользования.

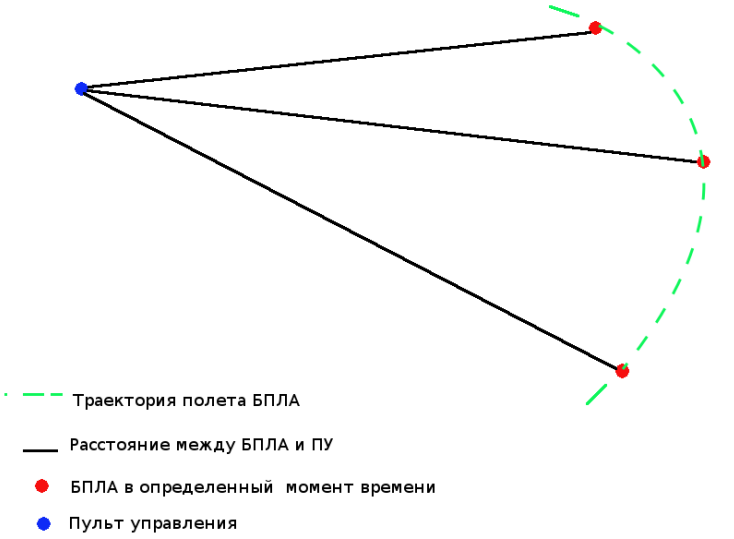

Рис. 3. Схема определения координат ПДУ по расстоянию
в разный момент времени полета БПЛА

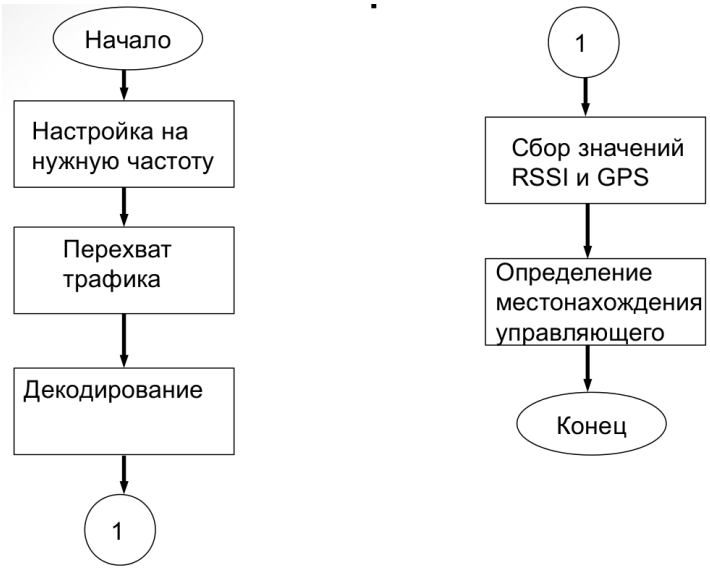

Рис. 4. Алгоритм нахождения ПДУ на базе анализа трафика

Заключение

Предложенный метод позволяет с помощью перехвата и расшифровки трафика между БПЛА и ПДУ зафиксировать факт запуска БПЛА, его координаты и координаты оператора, а также экстренно совершить посадку такого БПЛА. Одной из основных проблем на сегодняшний день является зашумленность каналов 433 МГц и 2,4 ГГц, что затрудняет процесс перехвата соответствующих данных из общего радиоэфира. Данный метод не потеряет свою актуальность в ближайшем будущем в связи с тем, что введен запрет на шифрование каналов связи БПЛА общего пользования. После проведения серии экспериментальных работ авторами будут представлены материалы, которые покажут особенности применения данного метода при различных уровнях зашумления канала.

Список используемых источников

1. Kirichek R., Koucheryavy A. Internet of Things Laboratory Test Bed // Lecture Notes in Electrical Engineering – Heidelberg: Springer, 2016. T. 348. PP. 485–494.
2. Кучерявый А. Е., Владыко А. Г., Киричек Р. В., Парамонов А. И., Прокопьев А. В., Богданов И. А., Дорт-Гольц А. А. Летающие сенсорные сети // Электросвязь. 2014. № 9. С. 2–5.
3. Киричек Р. В., Владыко А. Г., Захаров М. В., Кучерявый А. Е. Модельные сети для Интернета Вещей и программируемых сетей // Информационные технологии и телекоммуникации. 2015. № 3 (11). С. 17–26.
4. Kirichek R., Vladyko A., Zakharov M., Koucheryavy A. Model networks for Internet of Things and SDN // 18th international conference on advanced communication technology (ICACT). Phoenix Park, Korea : IEEE, 2016. PP. 76–79.
5. Koucheryavy A., Vladyko A., Kirichek R. State of the Art and Research Challenges for Public Flying Ubiquitous Sensor Networks // Internet of Things, Smart Spaces, and Next Generation Networks and Systems / Ed. by S. Balandin, S. Andreev, Y. Koucheryavy. Springer International PublishingSwitzerland. 2015, LNCS. Vol. 9247. PP. 299–308.
6. Кучерявый А. Е., Владыко А. Г., Киричек Р. В. Теоретические и практические направления исследований в области летающих сенсорных сетей // Электросвязь. 2015. № 7. С. 9–11.
7. Kirichek R., Paramonov A., Vareldzhyan K. Optimization of the UAV-P's motion trajectory in public flying ubiquitous sensor networks (FUSN-P) // Lecture Notes in Computer Science. 2015. PP. 352–366.
8. Hoang T., Kirichek R., Paramonov A., Koucheryavy A. Influence of intentional electromagnetic interference on the functioning of the terrestrial segment of flying ubiquitous sensor network // Lecture Notes in Electrical Engineering. 2016. T. 376. PP. 1249–1259.
9. MAVLink Micro Air Vehicle Communication Protocol [Электронный ресурс] // Message Specification. URL: http://qgroundcontrol.org/mavlink/start (дата обращения: 15.03.2016).
10. MAVLINK Common Message Set [Электронный ресурс] // MAVLink Protocol. URL: https://pixhawk.ethz.ch/mavlink/ (дата обращения: 18.03.2016).
11. Kirichek R., Grishin I., Okuneva D., Falin M. Development of a node-positioning algorithm for wireless sensor networks in 3D space // 18th International Conference on Advanced Communication Technology (ICACT). Phoenix Park, Korea : IEEE, 2016. PP. 279–282.

ШИРОКОПОЛОСНЫЕ СИГНАЛЫ ДАННЫХ С РАСШИРЕНИЕМ СПЕКТРА ПРЯМОЙ ПОСЛЕДОВАТЕЛЬНОСТЬЮ И ИХ ХАРАКТЕРИСТИКА

О.С. Когновицкий

Широкополосные сигналы позволяют обеспечить высокую помехоустойчивость передачи данных в канале при соотношении сигнал/шум по мощности близком к единице, а при определенных условиях и ниже единицы. Широкое применение сегодня они находят, прежде всего, в беспроводных системах передачи данных. Актуальной задачей является выбор широкополосных сигналов и их обработка. Рассматривается возможность повышения скорости передачи данных.

Ключевые слова: расширение спектра, шумоподобный сигнал, вероятность ошибки