www.volsu.ru

DOI: https://doi.org/10.15688/NBIT.jvolsu.2018.1.8

УДК 621.39
ББК 32.884

ПРОТИВОДЕЙСТВИЕ НЕСАНКЦИОНИРОВАННЫМ ПОЛЕТАМ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

Борис Анатольевич Швырев

Доцент кафедры компьютерных технологий и информационной безопасности,
Кубанский государственный технологический университет
Bor2275@yandex.ru
ул. Московская, 2, 350072 г. Краснодар, Российская Федерация

Даниил Вячеславович Погорелов

Студент,
Кубанский государственный технологический университет
hartgun@yandex.ru
ул. Московская, 2, 350072 г. Краснодар, Российская Федерация

Мария Викторовна Бердник

Доцент кафедры компьютерных технологий и информационной безопасности,
Кубанский государственный технологический университет
marviktr@mail.ru
ул. Московская, 2, 350072 г. Краснодар, Российская Федерация

Аннотация. Разрешенные радиочастотные диапазоны используются для организации канала утечки информации и управления беспилотными летательными аппаратами, нарушающими права граждан. Приводится сравнительный анализ беспроводных технологий на частоте 2.4 ГГц. Предложены программные меры противодействия неконтролируемым полетам беспилотных летательных аппаратов.

Ключевые слова: беспроводные технологии, Bluetooth, Wifi, LoRa WAN, SDR-приемник, широкополосный сигнал, беспилотный летательный аппарат.

Развитие беспроводных технологий сформировало значительный кластер устройств как повышающих качество жизни, так и приносящие разнообразные трудности, связанные с контролем этих устройств неизвестными лицами или организациями с целью получения какой-либо своей или сторонней выгоды. К таким негативным воплощениям беспроводных технологий можно отнести беспроводные средства негласного съема аудио-, видеоинформации, набирающие впечатляющие обороты беспроводные летательные аппараты – коптеры, планеры и т. д. Летательные аппараты представляют собой объекты как участвующие в негласном съеме информации, так и могущие использоваться злоумышленниками для доставки определенных грузов, веществ, незаконный оборот которых преследуется законодательством России. Помимо бытовых трудностей, вызванных приме-

нением беспилотных летательных аппаратов (БЛА), из средств массовой информации известны случаи использование их террористами в Сирии против гражданского населения, а также против правительственных сил (БЛА, начиненные взрыво- и огнеопасными веществами).

Противодействие новым современным угрозам информационной безопасности является важной и актуальной задачей.

Из литературы известен основной способ противодействия беспроводным несанкционированным каналам – постановка помехи в диапазоне частот, где сосредоточена передача информации.

Однако постановка энергетической помехи приводит к блокированию и соседних каналов передачи данных, такая зависимость актуальна и для прицельных и для заградительных помех. При подавлении одного канала из 14 (как, например, в WIFI) передача данных по легитимным соседним каналам становится затруднительной.

Увеличение мощности шумы (или помехи) имеет значительный эффект обычно для случая узкополосных каналов передачи, обработки данных и информации.

Сигнал называется узкополосным, если ширина его спектра значительно меньше средней частоты $\Delta f << f_{ср}$, где $f_{ср}$ – средняя частота полосы сигнала.

Стремление повысить скорость передачи информации при высокой помехоустойчивость связи с многолучевым распространением радиоволн путем разделения лучей и работой многих абонентов в общей полосе частот, а также создание систем связи с повышенной скрытностью.

Реализация заявленных целевых показателей средств связи возможна при использовании широкополосными сигналов (ШПС) – сигналов у которых произведения активной ширины спектра F на длительность T много больше единицы. Это произведение называется базой сигнала B. Применительно к ШПС выполняется следующее соотношение $B = FT >> 1$.

Широкополосными сигналами часто называют сигналы сложные, значительно отличающиеся от простых гармонических сигналов. В отличие от гармонических сигналов, имея малую длительность, такие сигналы являются импульсными со спектром неограниченной протяженности. Измерение спектра является сложной задачей, требующей значительных усилий. Для сужения задачи рассмотрим существующие беспроводные радиотехнологии диапазона 2.4 ГГц. В таблице приводятся сравнительные характеристики беспроводных технологий 2.4 ГГц.

Беспроводные технологии

Наименование	Частота	Вид модуляции	Мощность выходного сигнала	Шифрование	Технология
Nrf52832	ISM*	(G)FSK	100 мВт	SAFER+	Bluetooth
SX1280	ISM*	Поддерживаемые виды модуляции: LoRa, FLRC, (G)FSK	100 мВт Высокий уровень чувствительности: -132 дБм	AES-128	LoRa и другие
SX1281	ISM*	Поддерживаемые виды модуляции: LoRa, FLRC, (G)FSK	100 мВт Высокий уровень чувствительности: -132 дБм	AES-128	LoRa и другие
nRF24L01+	2.4–2.525 ГГц	(G)FSK	100 мВт	-	
cc3200	ISM*	(G)FSK	100 мВт	SAFER+	Bluetooth
DMX512	ISM*	(G)FSK	20 dBm	-	
esp8266	ISM*	(G)FSK	100 мВт	WEP, TKIP, CKIP, WPA, WPA2, WPA23	Wifi
DECT	ISM*	GMSK	10 мВт	DECT Standard Cipher (DSC)	

Примечание. * – 2.4–2.483,5 ГГц – это ISM-диапазон.

Из таблицы видно, что доступные беспроводные технологии имеют фазовую манипуляцию с различными параметрами, при этом используются передатчики не более 100 мВт. Ограниченный набор методов шифрования, используемый для организации передачи данных, не обладает высокой стойкостью и может быть перехвачен и прочитан.

Рассмотрим способ противодействия несанкционированной передаче данных на открытом канале.

Одними из самых распространенных передатчиков для управления БЛА являются nRF24L01+ и их аналоги за счет низкой стоимости, простоты разработки и высокой помехоустойчивости передачи данных, реализуемой на них.

При использовании полудуплексного трансивера nRF24L01+, в отличие от esp8266, Nrf52832 и их аналогов, невозможно обнаружить факт передачи данных без применения комплекса радиомониторинга и анализа сигналов или анализаторов спектра радиочастотного диапазона. Данный факт позволяет реализовывать на nRF24L01+ скрытый канал передачи данных. Также из сравнительной таблицы видно, что nRF24L01+ может функционировать на каналах 84–125 вне частотного диапазона стандарта ISM.

Для обнаружения сигнала в заданном диапазоне с заранее известными/неизвестными характеристиками используется SDR-приемник, который в реальном времени сканирует эфир и детектирует передачу сигнала, выделяет несущую частоту и демодулирует сигнал, после чего передает его в программу, которая обрабатывает. Это программное обеспечение для обработки принятого демодулированного сигнала обнаруживает полезные данные по преамбуле, после чего выделяет пакет из общего потока данных.

Подавление несанкционированного канала осуществляется в зависимости от вида используемого сигнала. Таким образом, предлагаемое решение позволяет подавлять одно или несколько нелегитимных устройств или, напротив, подавлять все устройства, не подходящие по заданным параметрам, то есть подавлять все устройства, кроме легитимных, оставляя возможность функционирования для полезного оборудования.

СПИСОК ЛИТЕРАТУРЫ

1. Волков, Л. Н. Системы цифровой радиосвязи: базовые методы и характеристики : учеб. пособие / Л. Н. Волков, М. С. Немировский, Ю. С. Шинаков. – М. : Эко-Трендз, 2005. – 392 с.

2. Гоноровский, И. Радиотехнические цепи и сигналы / И. Гоноровский. – Изд. 3-е, перераб. и доп. – М. : Сов. радио, 2006. – 608 с.

3. Тихвинский, В. О. Сети мобильной связи LTE: технологии и архитектура / В. О. Тихвинский, С. В. Терентьев, А. Б. Юрчук. – М., 2010.

4. Цифровая обработка сигналов в беспроводных широкополосных системах / Е. П. Ворошилин, Е. В. Рогожников, А. С. Вершинин, В. А. Чигринец, Д. А. Долгих . – Томск : В-Спектр, 2012. – 154 с.

5. Channel Estimation & Equalization for WiMAX. Application notes 434. ALTERA corporation, version 1.1. 2007.

6. LTE: the UMTS long term evolution. – New York : John Wiley & Sons, 2009.

REFERENCES

1. Volkov L.N., Nemirovskiy M.S., Shinakov Yu.S. *Sistemy tsifrovoy radiosvyazi: bazovye metody i kharakteristiki* [Digital Radio Communication Systems: Basic Methods and Characteristics]. Moscow, Eko-Trendz Publ., 2005. 392 p.

2. Gonorovskiy I. *Radiotekhnicheskie tsepi i signaly* [Radio Engineering Circuits and Signals]. Moscow, Sovetskoe radio Publ., 2006. 608 p.

3. Tikhvinskiy V.O., Terentyev S.V., Yurchuk A.B. *Seti mobilnoy svyazi LTE: tekhnologii i arkhitektura* [Mobile Networks LTE: Technologies and Architecture]. Moscow, 2010.

4. Voroshilin E.P., Rogozhnikov E.V., Vershinin A.S., Chigrinets V.A., Dolgikh D.A. *Tsifrovaya obrabotka signalov v besprovodnykh shirokopolosnykh sistemakh* [Digital Signal Processing in Wireless Broadband Systems]. Tomsk, V-Spektr Publ., 2012. 154 p.

5. *Channel Estimation & Equalization for WiMAX*. Application notes 434. ALTERA corporation, version 1.1. 2007.

6. *LTE: the UMTS long term evolution*. New York, John Wiley & Sons, 2009.

COUNTERACTION TO UNAUTHORIZED FLIGHTS OF UNMANNED AERIAL VEHICLES

Boris Anatolyevich Shvyrev

Associate Professor, Department of Computer Technologies and Information Security,
Kuban State Technological University
Bor2275@yandex.ru
Moskovskaya St., 2, 350072 Krasnodar, Russian Federation

Daniil Vyacheslavovich Pogorelov

Student, Department of Computer Technologies and Information Security,
Kuban State Technological University
hartgun@yandex.ru
Moskovskaya St., 2, 350072 Krasnodar, Russian Federation

Mariya Viktorovna Berdnik

Associate Professor, Department of Computer Technologies and Information Security,
Kuban State Technological University
marviktr@mail.ru
Moskovskaya St., 2, 350072 Krasnodar, Russian Federation

Abstract. The development of wireless technologies has formed a significant cluster of devices that both improve the quality of life and bring a variety of difficulties associated with the control of these devices by unknown persons or organizations in order to obtain any of their own or third-party benefits. Such negative embodiments of wireless technologies include wireless means of coverting audio and video capture, wireless aircraft-copters and gliders which can gain impressive speed, etc. Aircraft is an object involved in the covert removal of information, and can be used by criminals for the delivery of certain goods, substances illegal trafficking of which is punishable by Russian legislation.

Countering new modern threats to information security is an important and urgent task.

Permitted radio frequency ranges are used to detect a channel for information leakage and to control unmanned aerial vehicles that violate the rights of citizens. The article presents the comparative analysis of wireless technologies at a frequency of 2.4 GHz. The authors suggest program measures of counteraction to uncontrolled flights of unmanned aerial vehicles.

Key words: wireless technologies, Bluetooth, Wifi, LoRa WAN, SDR receiver, broadband signal, unmanned aerial vehicle.