УДК 004.42 Вестник УрФО № 3(57) / 2025, с. 24–29

Неклюдов Д. Н., Лебедь А. С., Кузьмина У. В. DOI: 10.14529/secur250303

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС МОНИТОРИНГА WI-FI СЕТЕЙ ДЛЯ ОБНАРУЖЕНИЯ И ПРОТИВОДЕЙСТВИЯ БПЛА

В данной статье рассматривается разработка программно-аппаратного комплекса для мониторинга Wi-Fi сетей с целью обнаружения и противодействия беспилотным летательным аппаратам (БПЛА). Предложен вероятностный подход к идентификации сетей БПЛА на основе анализа ключевых параметров беспроводного трафика. Описаны методы обработки зашумленных данных. Представлены способы определения местоположения БПЛА и оператора. В качестве меры активного противодействия рассмотрена атака деаутентификации, обеспечивающая разрыв связи между БПЛА и пультом управления.

Ключевые слова: *информационная безопасность, беспилотные летательные аппараты, мониторинг, обнаружение дронов, анализ трафика, трилатерация, атака деаутентификации.*

Neklyudov D. N., Lebed A. S., Kuzmina U. V.

SOFTWARE-HARDWARE SYSTEM FOR WI-FI NETWORK MONITORING TO DETECT AND COUNTERACT UAVS

This paper presents the development of a software-hardware system for Wi-Fi network monitoring designed to detect and counteract unmanned aerial vehicles (UAVs). We propose a probabilistic method for identifying UAV networks through analysis of key wireless traffic parameters. The study describes effective techniques for processing noise-contaminated signal data and demonstrates reliable methods for locating both UAVs and their operators. As an active countermeasure, we examine the implementation of deauthentication attacks to sever communication between UAVs and their control devices.

Keywords: *information security, unmanned aerial vehicles, network monitor-ing, drone detection, traffic analysis, signal trilateration, deauthentication attack.*

Современные беспилотные летательные аппараты находят широкое применение в различных сферах, включая доставку грузов, мониторинг террито-рий, видеосъемку и даже в военных и разведывательных операциях. Однако их активное использование создает серьезные угрозы безопасности, такие как несанкционированное наблюдение, вмешательство в работу критической инфраструктуры и потенциальные кибератаки. В связи с этим, компании и организации вынуждены внедрять меры противодействия, включая глушение радиоканалов, перехват управления и обнаружение дронов с помощью радиолокационных систем.

Множество существующих традиционных методов подавления БПЛА, такие как радиоэлектронное подавление каналов связи и радионавигации, обладают существенным недостатком: они могут нарушать работу собственных беспроводных сетей организации, включая сети Wi-Fi, Bluetooth, GSM и другие протоколы связи [1]. Это происходит из-за того, что подобные системы работают неизбирательно, создавая мощные помехи во всем рабочем диапазоне частот и подавляя не только сигналы БПЛА, но и легитимные устройства. Такие методы особенно критичны для предприятий, где стабильная работа сетевой инфраструктуры является одним из условий функционирования бизнес-процессов.

В связи с этим актуальной задачей становится разработка специализиро-ванных систем мониторинга, способных обнаруживать и идентифицировать БПЛА по их взаимодействию с Wi-Fi сетями без негативного влияния на существующую инфраструктуру связи. Подобные решения должны точно детектировать подозрительные сети и интегрироваться в комплексные системы защиты.

В качестве одного из способов идентификации подобных Wi-Fi сетей возможно применить анализ обмена кадров при общении БПЛА с пультом управления. Поскольку точное определение принадлежности Wi-Fi сети к БПЛА не всегда возможно, предлагается использовать вероятностный подход, основанный на анализе совокупности параметров беспроводного трафика [2].

К основным параметрам для оценки, перехваченных с помощью сниффера пакетам относятся:

- Анализ OUI (Organizationally Unique Identifier) MAC-адреса
- Количество устройств в сети
- SSID (имя сети)
- Анализ силы сигнала (RSSI) и динамики его изменения
- История и время жизни сети

В качестве базовой вычислительной платформы системы мониторинга была выбрана одноплатная микрокомпьютерная система Raspberry Pi 4 Model B с установленной операционной системой Raspberry Pi OS (ранее известной как Raspbian). Данный выбор обусловлен сочетанием вычислительной мощности, энергоэффективности, необходимых при анализе большого количества пакетов из множества сетей, а также компактных размеров устройства [3].

Хотя плата Raspberry Pi 4 оснащена встроенным беспроводным сетевым адаптером Broadcom BCM4345 с поддержкой стандартов IEEE 802.11 b/g/n/ac (2,4/5 ГГц), способным работать в режиме мониторинга (monitor mode), для задач данного исследования его возможностей оказалось недостаточно. Для преодоления ограничений, таких как, недостаточная мощность и ограниченная чувствительность передатчика, был дополнительно подключен внешний беспроводной адаптер ALFA AWUS036ACM с чипсетом MediaTek MT7612U, а также резервные адаптеры [4].

Для захвата и анализа беспроводных пакетов в разработанной системе используется библиотека Scapy для языка Python, которая предоставляет воз-можности для низкоуровневой работы с сетевыми пакетами [5]. С помощью данного инструментария осуществляется перехват радиокадров, из которых извлекаются ключевые параметры для последующего анализа. Особое значение имеет получение показателя мощности принимаемого сигнала (RSSI), которое реализуется через обращение к полю dBm_AntSignal в RadioTap-заголовке пакета (*pkt[RadioTap].dBm_AntSignal*) [6].

При практическом применении системы в условиях плотной городской застройки или на промышленных объектах возникает существенная проблема, связанная с одновременным присутствием большого количества беспроводных сетей и подключенных к ним устройств. Массовый параллельный анализ всех обнаруженных сетей приводит к значительной нагрузке на вычислительные ресурсы системы и снижению оперативности обработки.

Для оптимизации работы системы был разработан многоуровневый подход к анализу сетей, основанный на принципе приоритезации. Новые, только что обнаруженные сети подвергаются наиболее тщательному и детальному анализу по всем доступным параметрам. По мере накопления статистики о сети и подтверждения ее стабильности и легитимности, интенсивность проверок постепенно снижается. Сети, длительное время присутствующие в зоне мониторинга и демонстрирующие предсказуемое поведение, переходят в категорию "известных" и проверяются по упрощенной схеме. Приоритезация позволяет снизить вычислительную нагрузку на систему, сохраняя при этом эффективность обнаружения подозрительной активности.

В условиях работы с сильно зашумленными беспроводными сигналами возникает необходимость в специальных алгоритмах обработки данных, позволяющих одновременно решать две задачи: снижение влияния случайных помех и сохранение актуальной информации о динамике изменения сигнала. Для этих целей в разработанной системе применяется метод взвешенного скользящего среднего (Weighted Moving Average, WMA).

$$WMA_i = \frac{\sum_{i=0}^{k-1} \omega_i \cdot x_{t-i}}{\sum_{i=0}^{k-1} \omega_i},$$

где: x_t – последовательность измеренных значений RSSI

ω_i – весовые коэффициенты

k – размер окна усреднения

Практические испытания показали, что применение WMA для обработки RSSI-сигналов в условиях городской застройки снижает среднеквадратичную ошибку позиционирования на 60–70% в сильнозашумленных сетях и на 13–20% в стабильных условиях по сравнению с использованием необработанных данных. На рисунке 1 визуализирована работа фильтра взвешенного, скользящего, среднего, примененного к искусственно зашумленному сигналу имитирующему динамику приближающегося и удаляющегося источника беспроводного сигнала.

Исходные данные содержат значительный уровень случайных помех, характерный для реальных условий работы в городской среде. Фильтр сглаживает высокочастотных шумовых составляющих, при этом сохраняя тенденции изменения уровня сигнала.

В дополнение к описанным ранее методам идентификации беспилотных летательных аппаратов по характеристикам Wi-Fi сетей, в разработанной сис-теме реализован альтернативный подход, основанный на перехвате и анализе кадров протокола MAVLink [7]. Данный протокол используется в большинстве коммерческих и любительских БПЛА.

Перехваченные кадры MAVLink имеют четко определенную структуру, включающую несколько обязательных полей: начальный маркер пакета (STX), длина полезной нагрузки (LEN), последовательность пакетов (SEQ), идентификаторы системы (SYS) и компонента (COMP), тип сообщения (MSG), полезные данные (PAYLOAD), контрольная сумма (CKA, CKB) (рисунок 2).

Анализ перехваченных кадров MAVLink позволяет получить текущие координаты БПЛА. В полезной нагрузке кадров часто содержатся данные от бортового GPS-приемника, включающие точные координаты аппарата.

Для вычисления расстояния до беспроводного источника (в частности, БПЛА) в разработанной системе применяется метод трилатерации, основанный на анализе уровня принимаемого сигнала. Трилатерация позволяет оценить местоположение излучающего устройства без необходимости использования специализированного оборудования [8].

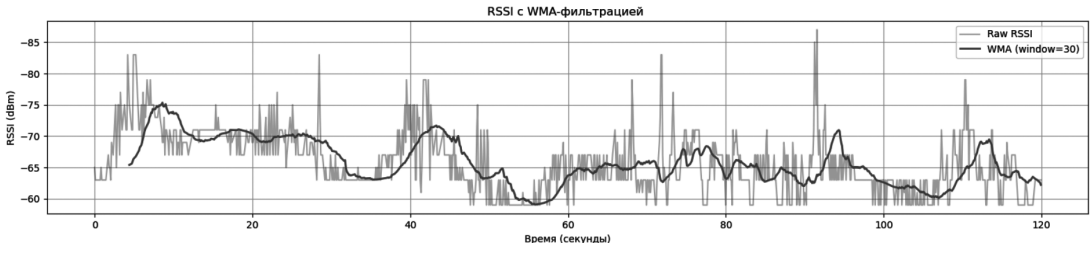

Рис. 1. Динамика RSSI-сигнала до и после применения WMA-фильтра

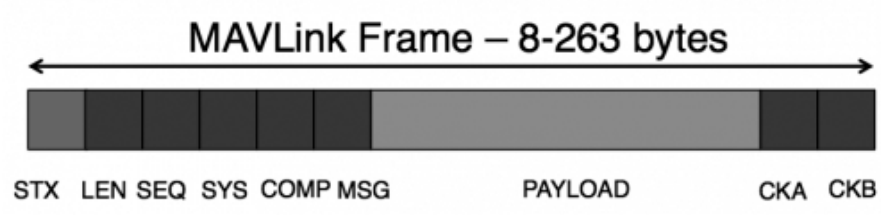

Рис. 2. Структура кадра протокола MAVLink

Метод базируется на известной модели затухания радиосигнала в свободном пространстве, которая математически выражается соотношением:

$$RSSI = P_{tx} - 10 \cdot n \cdot \lg(d) + X_{\sigma},$$

где: P_{tx} – мощность передатчика источника сигнала (дБм)

n – коэффициент затухания, зависящий от характеристик среды распро-странения (значения 2 - 4)

d – расстояние от приемника до источника (метры)

X_{σ} – случайная составляющая, учитывающая эффекты многолучевого распространения и шумы

Подход, несмотря на определенные ограничения по точности (погреш-ность в условиях городской застройки может составлять 5-15 метров), обеспе-чивает достаточную эффективность для задач обнаружения и примерного позиционирования БПЛА, особенно при использовании в сочетании с другими методами анализа.

Для определения местоположения оператора (пульта дистанционного управления) также используется метод трилатерации на основе показателей RSSI, полученных в трех различных точках пространства [9].

Математически задача решается с помощью системы уравнений:

$$\begin{cases} E0 = \sqrt{(x_o - x_e)^2 + (y_o - y_e)^2 + (z_o - z_e)^2}, \\ B0 = \sqrt{(x_o - x_b)^2 + (y_o - y_b)^2 + (z_o - z_b)^2}, \\ C0 = \sqrt{(x_o - x_c)^2 + (y_o - y_c)^2 + (z_o - z_c)^2}, \end{cases}$$

где: (x_o, y_o, z_o) – искомые координаты оператора,

$(x_e, y_e, z_e), (x_b, y_b, z_b), (x_c, y_c, z_c)$ – координаты БПЛА в разные моменты времени.

Основным преимуществом метода является его эффективность при работе с большинством коммерческих БПЛА, использующих протокол MAVLink.

После успешного обнаружения БПЛА с использованием вероятностного подхода и подтверждения его принадлежности к потенциально опасным объектам, система инициирует механизм активного противодействия [10]. В качестве эффективного метода нейтрализации применяется атака деаутентификации, направленная на разрыв установленного соединения между БПЛА и пультом управления оператора. Данный подход основан на отправке специально сформированных управляющих кадров, которые принудительно завершают активную сессию связи. По результатам атаки оператор теряет возможность управления дроном и получать видеопоток с его бортовой камеры, что вынуждает аппарат либо автоматически возвращаться в точку взлета (при наличии соответствующей функции), либо совершать аварийную посадку.

В результате проведённого исследования был разработан программно-аппаратный комплекс мониторинга Wi-Fi сетей для противодействия БПЛА, сочетающий в себе несколько взаимодополняющих методов обнаружения и нейтрализации беспилотников. Комплекс реализует многоуровневый вероятностный подход к идентификации сетей БПЛА на основе анализа совокупности параметров беспроводного трафика. В качестве активного средства противодействия используется селективная атака деаутентификации, обеспечивающая разрыв соединения между БПЛА и пультом управления без нарушения работы легитимных беспроводных устройств.

Несмотря на достигнутые результаты, следует отметить некоторые огра-ничения системы. Точность определения местоположения в условиях плотной городской застройки требует дальнейшего совершенствования, а эффек-

тивность противодействия может снижаться при работе с новыми моделями БПЛА. Кроме того, система требует оптимизации вычислительных ресурсов для обработки трафика в режиме реального времени при большом количестве одновременно активных сетей и подключенных к ним устройств.

Применимые в исследовании методы в рамках разработки комплекса сохраняют практическую значимость, поскольку основаны на фундаментальных характеристиках беспроводной связи, не зависящих от конкретных моделей БПЛА или используют общепринятые протоколы взаимодействия. Эти способы в совокупности образуют сбалансированное решение, сочетающее достаточную эффективность с относительно низкими требованиями к вычислительным ресурсам, что делает комплекс практичным для широкого внедрения.

Литература

1. Способы подавления радиозакладных устройств / И. И. Баранкова, У. В. Кузьмина, А. Р. Федорова, Ю. А. Кульевич // Безопасность информационного пространства: Сборник трудов XXII Всероссийской научно-практической конференции студентов, аспирантов и молодых учёных, Челябинск, 30 ноября 2023 года. – Челябинск: Издательский центр ЮУрГУ, 2024. – С. 77-83. – EDN KVEVUI.

2. Неклюдов, Д. Н. Разработка алгоритма обнаружения Wi-Fi-сетей БПЛА / Д. Н. Неклюдов, А. С. Лебедь, У. В. Кузьмина // Актуальные проблемы современной науки, техники и образования. – 2024. – Т. 15, №1. – С. 29-30.

3. Баранова, Ж. М. Основные требования к функционалу сетевого анализатора трафика на основе Raspberry Pi / Ж. М. Баранова, Д. С. Большаков, Д. В. Ковтунович // Энергетика, информатика, инновации - 2022 (электроэнергетика, электротехника и теплоэнергетика, математическое моделирование и информационные технологии в производстве) : сборник трудов XII международной научно-технической конференции, Смоленск, 23 ноября 2022 года / филиал ФГБОУ ВО «НИУ «МЭИ» в г. Смоленске. Том 1. – Смоленск: Б. и., 2022. – С. 149-150. – EDN MFSEUM.

4. Фаткуллин, А. Р. современные средства радиоразведки / А. Р. Фаткуллин, У. В. Михайлова // Актуальные проблемы современной науки, техники и образования: Тезисы докладов 79-й международной научно-технической конференции, Магнитогорск, 19–23 апреля 2021 года. Том 1. – Магнитогорск: Магнитогорский государственный технический университет им. Г.И. Носова, 2021. – С. 402. – EDN NXUIZG.

5. Федорова, А. Р. Анализ защищенности скрытых беспроводных сетей / А. Р. Федорова, В. А. Шпак // Этнополитический и религиозный экстремизм в России: социально-культурные истоки, угрозы распространения в информационной среде, методы противодействия: Сборник материалов Всероссийской молодежной научной школы-конференции, Уфа, 04–05 декабря 2020 года. – Уфа: ООО "Издательство "Диалог", 2020. – С. 184-189. – EDN WJJJUC.

6. Пахомов С. Анатомия беспроводных сетей // КомпьютерПресс. 2018. №1. С. 155-158.

7. Киричек, Р. В. Метод обнаружения беспилотных летательных аппаратов на базе анализа трафика / Р. В. Киричек, А. А. Кулешов, А. Е. Кучерявый // Труды учебных заведений связи. – 2016. – Т. 2, № 1. – С. 77-82.

8. Мельничук, А. И. К проблеме синтеза многопозиционной радиолокационной станции обнаружения беспилотных летательных аппаратов / А. И. Мельничук, Н. В. Горячев, Н. К. Юрков // Надежность и качество сложных систем. – 2022. – № 3(39). – С. 33-41. – DOI 10.21685/2307-4205-2022-3-4.

9. Kosmanos D., Pappas A., Tzes A., Cantos-Romanos D. RSSI-Based Indoor Localization with the Internet of Things. J. of Sensor and Actuator Networks, 2018, vol. 7, no.4, available at: https://www.researchgate.net/publication/325561044_RSSI-Based_Indoor_Localization_with_the_Internet_of_Things (accessed [1.04.2025]).

10. Гриценко Н.С., Лукьянов Г.И., Михайлова У.В. Безопасность сетей беспроводной передачи данных / Безопасность информационного пространства. Сборник трудов XVII Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых: в 2 томах. 2018. С. 64-69.

References

1. Sposoby podavlenija radiozakladnyh ustrojstv / I. I. Barankova, U. V. Kuz'mina, A. R. Fedorova, Ju. A. Kul'evich // Bezopasnost' informacionnogo prostranstva : Sbornik trudov XXII Vserossijskoj nauchno-prakticheskoj konferencii studentov, aspirantov i molodyh uchjonyh, Cheljabinsk, 30 nojabrja 2023 goda. – Cheljabinsk: Izdatel'skij centr JuUrGU, 2024. – S. 77-83. – EDN KVEVUI.

2. Nekljudov, D. N. Razrabotka algoritma obnaruzhenija Wi-Fi-setej bpla / D. N. Nekljudov, A. S. Lebed', U. V. Kuz'mina // Aktual'nye problemy sovre-mennoj nauki, tehniki i obrazovanija. – 2024. – T. 15, №1. – S. 29-30.

3. Baranova, Zh. M. Osnovnye trebovanija k funkcionalu setevogo analizatora trafika na osnove Raspberry Pi / Zh. M. Baranova, D. S. Bol'shakov, D. V. Kovtunovich // Jenergetika, informatika, innovacii - 2022 (jelektrojenergetika, jelektrotehnika i teplojenergetika, matematicheskoe modelirovanie i informacionnye tehnologii v proizvodstve): sbornik trudov XII mezhdunarodnoj nauchno-tehnicheskoj konferencii, Smolensk, 23 nojabrja 2022 goda / filial FGBOU VO «NIU «MJel» v g. Smolenske. Tom 1. – Smolensk: B. i., 2022. – S. 149-150.

4. Fatkullin, A. R. sovremennye sredstva radiorazvedki / A. R. Fat-kullin, U. V. Mihajlova // Aktual'nye problemy sovremennoj nauki, tehniki i obrazovanija : Tezisy dokladov 79-j mezhdunarod-noj nauchno-tehnicheskoj konferencii, Magnitogorsk, 19–23 aprelja 2021 goda. Tom 1. – Magnitogorsk: Magnitogorskij gosudarstven-nyj tehnicheskij universitet im. G.I. Nosova, 2021. – S. 402.

5. Fedorova, A. R. Analiz zashhishhennosti skrytyh besprovodnyh setej / A. R. Fedorova, V. A. Shpak // Jetnopoliticheskij i religioznyj jekstremizm v Rossii: social'no-kul'turnye istoki, ugrozy raspro-stranenija v informacionnoj srede, metody protivodejstvija: Sbornik materialov Vserossijskoj molodezhnoj nauchnoj shkoly-konferencii, Ufa, 04–05 dekabrja 2020 goda. – Ufa: OOO "Izda-tel'stvo "Dialog", 2020. – S. 184-189. – EDN WJJJUC.

6. Pahomov S. Anatomija besprovodnyh setej // Komp'juterPress. 2018. №1. S. 155-158.

7. Kirichek, R. V. Metod obnaruzhenija bespilotnyh letatel'nyh appa-ratov na baze analiza trafika / R. V. Kirichek, A. A. Kuleshov, A. E. Kucherjavyj // Trudy uchebnyh zavedenij svjazi. – 2016. – T. 2, № 1. – S. 77-82. – EDN XCGQHF.

8. Mel'nichuk, A. I. K probleme sinteza mnogopozicionnoj radiolo-kacionnoj stancii obnaruzhenija bespilotnyh letatel'nyh appara-tov / A. I. Mel'nichuk, N. V. Gorjachev, N. K. Jurkov // Nadezhnost' i kachestvo slozhnyh sistem. – 2022. – № 3(39). – S. 33-41. – DOI 10.21685/2307-4205-2022-3-4. – EDN GPQOJN.

9. Kosmanos D., Pappas A., Tzes A., Cantos-Romanos D. RSSI-Based Indoor Localization with the Internet of Things. J. of Sensor and Actuator Networks, 2018, vol. 7, no.4, available at: https://www.researchgate.net/publication/325561044_RSSI-Based_Indoor_Localization_with_the_Internet_of_Things (accessed [1.04.2025]).

10. Gricenko N.S., Luk'janov G.I., Mihajlova U.V. Bezopasnost' setej besprovodnoj peredachi dannyh / Bezopasnost' informacionnogo prostran-stva. Sbornik trudov XVII Vserossijskoj nauchno-prakticheskoj konferencii studentov, aspirantov i molodyh uchenyh: v 2 tomah. 2018. S. 64-69.

НЕКЛЮДОВ Данил Николаевич, студент 5 курса по специальности «Информационная безопасность автоматизированных систем» кафедры информатики и информационной безопасности, ФГБОУ ВО «Магнитогорский государственный технический университет им Г.И. Носова». 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: dejeksdan@gmail.com

ЛЕБЕДЬ Александр Сергеевич, студент 5 курса по специальности «Информационная безопасность автоматизированных систем» кафедры информатики и информационной безопасности, ФГБОУ ВО «Магнитогорский государственный технический университет им Г.И. Носова». 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: mail23032019@mail.ru

КУЗЬМИНА Ульяна Владимировна, кандидат технических наук, до-цент кафедры информатики и информационной безопасности, ФГБОУ ВО «Магнитогорский государственный технический университет им Г.И. Носова». 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: Ylianapost@gmail.com

NEKLYUDOV Danil Nikolaevich, 5th year student majoring in "Information Security of Automated Systems" department of Computer Science and Information security, Nosov Magnitogorsk State Technical University, 455000, Magnitogorsk, Lenin Ave., 38. E-mail: dejeksdan@gmail.com

LEBED Alexander Sergeevich, 5th year student majoring in "Information Security of Automated Systems" department of Computer Science and Information security, Nosov Magnitogorsk State Technical University, 455000, Magnitogorsk, Lenin Ave., 38. E-mail: mail23032019@mail.ru

KUZMINA Ulyana Vladimirovna, candidate of Technical Sciences, asso-ciate professor of the department of Computer Science and Information security, Nosov Magnitogorsk State Technical University, 455000, Magnitogorsk, Lenin Ave., 38. E-mail: Ylianapost@gmail.com