

Система обнаружения и подавления БПЛА, использующих инфраструктуру сотовых операторов для связи и управления

И. М. Кудрин, бакалавр; i.kudrin@ntc-rassvet.ru

И. Г. Афонин, ООО «НТЦ РАССВЕТ», технический директор; afonin_ig@ntc-rassvet.ru

УДК 621.396.969.34

DOI: 10.34832/ELSV.2024.59.10.006

Аннотация. Предлагается система обнаружения и подавления беспилотных летательных аппаратов (БПЛА), которая основана на использовании инфраструктуры сотовой связи 4G LTE. Управляемые через сети операторов БПЛА функционируют как стандартные абонентские устройства с SIM-картами, и их сигналы могут быть обнаружены через анализ управляющих каналов LTE (PBCH, PDCCH, PUSCH). Это позволяет выявлять несанкционированные БПЛА, анализируя их взаимодействие с базовыми станциями (БС) сотовой сети. Для локализации БПЛА предлагается использовать методы триангуляции (MLAT) и цифрового формирования луча (digital beamforming). Кроме того, система может подавлять сигнал БПЛА, нарушая обмен данными между БПЛА и БС посредством генерации помех на основе легитимных сигналов.

Ключевые слова: обнаружение БПЛА, подавление БПЛА, инфраструктура LTE, радиочастотные сигналы, цифровое формирование луча, multilateration (MLAT), генерация помех.

ВВЕДЕНИЕ

В последние несколько лет наблюдается активное развитие и распространение беспилотных летательных аппаратов. БПЛА широко используются, например, для наблюдения и мониторинга окружающей среды, разведывательных миссий, распыления удобрений в сельском хозяйстве, доставки грузов, в различных военных операциях. Кроме того, их планируется использовать для увеличения покрытия сетей 5G и сетей следующих поколений. БПЛА можно управлять дистанционно, они могут следовать по заранее обозначенному маршруту или осуществлять адаптивную навигацию.

Однако с увеличением доступности технологий БПЛА возрастает и угроза их использования в незаконных или угрожающих целях. Беспилотные летательные аппараты могут проникать в воздушное пространство, в котором установлен бесполетный режим, приближаться к важным объектам инфраструктуры и препятствовать их безопасной работе. Кроме того, они могут быть использованы в шпионаже, контрабанде и в террористических атаках.

Резкий рост объемов производства и продаж БПЛА в комбинации с их стремительным технологическим развитием представляет большую угрозу безопасности.

Актуальной является и проблема обнаружения беспилотных летательных аппаратов, которая стимулирует спрос на разработку новых технологий и методов обнаружения несанкционированных БПЛА.

СУЩЕСТВУЮЩИЕ РЕШЕНИЯ

Задача обнаружения БПЛА в настоящее время обычно решается с использованием датчиков обнаружения.

По принципу функционирования средства обнаружения БПЛА делятся на:

- акустические системы, анализирующие звук, издаваемый двигателями БПЛА, что позволяет обнаруживать их на расстоянии;
- оптические и инфракрасные системы, камеры которых могут визуально обнаруживать БПЛА;
- лидары, позволяющие обнаруживать БПЛА путем лазерного сканирования;
- радиолокационные системы, фиксирующие радиоволны, отраженные от БПЛА;
- радиочастотные системы, позволяющие детектировать сигналы, передаваемые между оператором и БПЛА, а также определять местоположение БПЛА с помощью анализа этих сигналов;
- комбинированные системы, основанные на использовании двух и более из вышеперечисленных методов для улучшения обнаружения.

Каждая из вышеупомянутых систем обладает как достоинствами, так и недостатками. Это относится как к самому средству и датчику, так и к предлагаемому комплексному решению на их базе. Сравнение применяемых в этих системах принципов приведено в таблице.

Как видно из таблицы, существующие решения для обнаружения БПЛА имеют недостатки,

Характеристики датчиков обнаружения

Принцип работы датчиков обнаружения	Предельная дальность для эффективной площади рассеяния объекта 0,01 м ² , м	Факторы, влияющие на качество работы	Особенности функционирования
Акустический	200–300	шум внешней среды	возможность работы при радиомолчании БПЛА
Оптический	500–600	условия освещённости, погодные условия (туман, осадки)	требуется наличие прямой видимости, возможность работы при радиомолчании БПЛА
Лидар	1000	погодные условия (туман, осадки)	требуется наличие прямой видимости, возможность работы при радиомолчании БПЛА
Радиолокационный	2000	размер БПЛА (эффективная площадь рассеяния), фоновое электромагнитное излучение	требуется наличие прямой видимости, возможность работы при радиомолчании БПЛА
Радиочастотный	2000	мощность излучения передатчика на БПЛА, фоновое электромагнитное излучение	работа по БПЛА, управляемым дистанционно, возможность обнаружить оператора до взлёта дрона
Инфракрасный	500–600	погодные условия (туман, осадки)	требуется наличие прямой видимости, возможность работы при радиомолчании БПЛА
Анализ сигналов телеметрии сотовой связи	7000	нет влияния	наличие обмена информацией между БПЛА и БС

которые ведут к ухудшению функционирования систем обнаружения из-за различных окружающих факторов, например погодных условий, акустического шума, высокого уровня фонового электромагнитного излучения в мегаполисах. Также для применения этих методов необходимо развертывание сложных, дорогостоящих и визуально обнаруживаемых систем, что не всегда является возможным.

Основной научно-технической задачей проекта является разработка решения по обнаружению несанкционированных БПЛА, которое обладает устойчивостью к негативному влиянию погодных условий, не является чувствительным к размеру обнаруживаемых БПЛА, а также обладает минимальной стоимостью в сравнении с существующими решениями. В дополнении к функции обнаружения система должна обладать функцией точечного подавления БПЛА в случае необходимости без нарушения работоспособности других систем связи.

ПРЕДЛАГАЕМЫЙ ПОДХОД

В настоящий момент активно развивается технология обеспечения связи и управления БПЛА с использованием имеющейся инфраструктуры сотовых сетей связи стандарта 4G LTE (Long-Term Evolution) в силу их распространенности, широкого покрытия территории и легкого подключения к сети. Подобный способ управления БПЛА уже был протестирован многими зарубежными операторами, например AT&T, Telefonica, Vodafone и т.д. В этом случае каждый несанкционированный БПЛА, который передает любые данные в процессе полета, определяется как абонентский терминал, использующий идентичные обычному абонентскому устройству (сотовому телефону) принципы работы, т.е. обладает SIM-картой или eSIM и работает в соответствии со стандартами LTE, определенными организацией 3GPP (3rd Generation Partnership Project).

В связи с этим для обнаружения несанкционированных БПЛА, которые во время полета передают данные по беспроводному каналу связи, как это делает стандартный терминал LTE (например, мобильный телефон), предлагается метод обнаружения на базе управляющих сигналов LTE, излучаемых самим БПЛА в процессе полета. Для этого необходимо разработать оборудование приема и анализа сигналов взаимодействия между БС и абонентом сетей 4G LTE.

Во время работы каждый БПЛА, который использует инфраструктуру LTE, обменивается данными с оператором путем подключения и обмена сообщениями с БС LTE. Сигнал от БС в свою очередь имеет OFDM (Orthogonal frequency-division multiplexing) структуру и содержит ряд каналов, по которым передаются данные.

Предлагаемый подход предполагает обнаружение БПЛА на основе нисходящих сигналов в фи-

зических каналах PBCH (Physical Broadcast Channel) и PDCCH (Physical Downlink Control Channel) [1], а также информации из восходящего канала PUSCH (Physical Uplink Shared Channel) [2].

При этом, поскольку БПЛА в данном случае идентичен другим абонентским устройствам, например смартфонам, обязательно выполняется ряд процедур:

1) при появлении БПЛА в зоне покрытия БС, первой выполняется процедура установления соединения по радиоканалу случайного доступа RACH (Random Access Channel), во время которой абонент (БПЛА) устанавливает первоначальную связь с БС следующим образом:

а) БПЛА в заранее определенном спецификой работы устройств в сети случайном временном слоте генерирует специальный сигнал первичного доступа PRACH (Physical Random Access Channel) и отправляет его на БС;

б) БС принимает сигнал PRACH и в ответ отправляет сообщение RAR (Random Access Response), которое содержит информацию о выделенных ресурсах для следующего этапа связи;

2) после процедуры установления соединения по радиоканалу случайного доступа RACH БПЛА получает по каналу PDCCH сообщение DCI (downlink control indication), которое содержит информацию о выделенных ресурсах для передачи данных и передается без использования протоколов шифрования. Сообщение DCI в свою очередь содержит специальную команду для передачи сигналов SRS (sounding reference signals), которые используются для корректной оценки качества беспроводного канала связи планировщиком на БС;

3) после получения информации о предоставленных ресурсах БПЛА использует канал PUSCH в выделенные для него временные промежутки для передачи данных;

4) также базовая станция передает по каналу PBCH важную системную информацию, которая содержит параметры сети, необходимые абонентскому устройству или БПЛА.

Функционал подавления БПЛА основан на использовании генератора помех. Генератор помех включается на радиочастоте абонента во время обмена служебными сообщениями между БС и абонентом. Данный способ позволяет нарушать целостность служебной информации, что приведет к адресному подавлению стандартного механизма оценки состояния канала между БС и абонентом и, как следствие, прерыванию сеанса связи абонента без нарушения работы других абонентов в сети.

Предлагаемое решение с помощью специального приемника, устанавливаемого в зоне работы БС, декодирует и анализирует нисходящие сигналы от БС, тем самым определяя координаты и скорость БПЛА.

Декодирование нисходящих каналов БС возможно, поскольку сигналы в физических каналах PBCH и PDCCH не используют протоколы шифрования.

После обнаружения наличия БПЛА в сети для определения точного местоположения БПЛА в пространстве и прогнозирования его перемещения предлагается применить метод триангуляции, основанный на обработке сигналов на физическом уровне. Это позволит идентифицировать БПЛА вне зависимости от того, какой именно трафик они передают по каналу управления, какие для этого используются транспортные протоколы и т.д. Такой подход также позволит обнаруживать БПЛА без вмешательства в работу сети оператора.

Для непосредственного определения координат и скорости БПЛА на основе декодированных сигналов предлагаемая система использует технологии мультilaterации (multilateration, MLAT) [3] и цифрового формирования луча (digital beamforming):

1. MLAT представляет собой технологию определения местоположения воздушных объектов на основе измерения расстояний от него до точек, координаты которых известны. В системах управления воздушным движением измерение упомянутых расстояний осуществляется с помощью различного радиолокационного оборудования (передающая антенна на БПЛА, дополнительные приемники в зоне действия базовой станции), которое размещено в этих точках.

В случае применения этой технологии в предлагаемой системе не требуется размещения на приемниках сложного и дорогого радиоборудования, достаточным является установка одного трансивера и обычной штыревой антенны. Кроме того, в этой технологии применяется простой алгоритм цифровой обработки сигналов (ЦОС). При использовании такого подхода мы можем определить координаты несанкционированного БПЛА, который является излучателем сигнала, по относительному времени прихода сигналов. Скорость БПЛА определяется на основе доплеровского смещения частоты передаваемого сигнала.

Преимуществом использования данного метода в сравнении с аналогами является его простота и низкая стоимость оборудования.

Данный метод подходит для определения расстояния и высоты в случае необходимости временного запрета полетов БПЛА над определенной территорией за счет возможности размещения одного из приемников на «дружественном» БПЛА.

2. Цифровое формирование луча — это технология, используемая в системах радиолокации, беспроводной связи и других областях, которая позволяет управлять направлением и формой радиоволн, излучаемых антенными массивами. В отличие от аналогового формирования луча, где управление

осуществляется с помощью фазовых сдвигов и амплитудных регулировок на уровне аналоговых компонентов, цифровое формирование луча выполняется на уровне цифровых сигналов.

Данная технология определяет направление прихода сигнала с помощью вычисления разности фаз, что позволяет определить координаты БПЛА. Приемник с данной технологией может применяться для определения высоты полета при размещении на земле и как дополнительный источник данных для MLAT. Как и в случае с MLAT для определения скорости целевого БПЛА необходимо вычисление доплеровского сдвига.

Преимуществом данной технологии является большое количество получаемой информации, поскольку в дополнение к дальности и скорости, также можно определить и угловое отклонение, что позволит определить, откуда исходит сигнал, и устойчивость к многолучевому распространению. Также технология предоставляет возможность более точных измерений высоты полета БПЛА.

Недостатками технологии цифрового формирования луча являются необходимость развертывания нескольких приемников с хорошей синхронизацией и массивами антенн с жестко заданными фазовыми характеристиками, высокая сложность алгоритмов ЦОС и меньшая стабильность работы в условиях слабого сигнала в сравнении с MLAT.

В предлагаемом решении возможно использование MLAT и цифрового формирования луча как по отдельности, так и в комбинации, в зависимости от условий установки оборудования и требований к стоимости и сложности развертывания.

Использование вышеописанных подходов позволяет достичь высокой точности локализации несанкционированных БПЛА.

В большинстве сотовых систем отношение сигнал-шум (signal-to-noise ratio, SNR) составляет около 10 дБ, но оно может быть повышено за счет направленных антенн при размещении приемников на «дружественных» БПЛА. Ширина канала, выделяемого планировщиком базовой станции 4G LTE, составляет обычно порядка 10 МГц (но бывает и 5 МГц). В данном случае точность определения расстояния до БПЛА имеет порядок, определяемый соотношением, приведенном в формуле [4]:

$$\delta R \approx \frac{c_0}{2B\sqrt{2\text{SNR}}},$$

где R — погрешность измерения расстояния; c_0 — скорость света; B — ширина канала, выделенного БС БПЛА для передачи данных [Гц]; SNR — отношение сигнал/шум. Однако БПЛА передает сигналы с высокой частотой, например, в случае передачи сигналов DMRS (Demodulation Reference Signal) каждые 0,5 мс, и обрабатывая несколько сигналов подряд

можно последовательно увеличивать точность локализации. При равномерном движении по прямой итоговая точность локализации может составлять порядка 2–3 м.

При локализации объектов с использованием технологии цифрового формирования луча точность измерения угловых отклонений зависит от расстояния между антенными элементами и ширины спектра сигнала. Увеличение расстояния между антеннами приводит к увеличению разности времени прихода сигналов при одинаковом угловом отклонении. Это позволяет более точно определять направление, откуда поступает сигнал. Широкий спектр сигнала улучшает точность измерения разности времени прихода, что также способствует более точному определению угловых отклонений. Кроме того, как и в случае с определением дальности, можно усреднять результаты нескольких замеров для повышения общей точности. Это особенно важно при определении высоты объекта над землей, например, для различения низколетящего БПЛА от автомобиля.

В дополнение к обнаружению и определению координат несанкционированного БПЛА предлагаемый подход предоставляет возможность подавления обнаруженных беспилотников.

Передача данных по восходящему каналу от БПЛА по физическому каналу PUSCH имеет как минимум один DMRS сигнал, который представляет собой последовательность Задова-Чу (ZCS) [5]. Также в сигнале DCI, который передается по физическому каналу PDCCH от БС, может содержаться команда о передаче информации о состоянии канала связи SRC. Эта информация также содержит в себе последовательность ZCS.

Подавление несанкционированного БПЛА в предлагаемом решении происходит за счет целенаправленного создания помех вместо сигналов DMRS и SRS, которые должен отправлять абонент. Помехи создаются в виде легитимных ZCS для целевого абонента, передаваемых размещенными в зоне действия БС передатчиками с высокой мощностью в момент времени, когда БС их ожидает от абонента. Получая две копии ZCS, базовая станция в соответствии со стандартизированными протоколами 3GPP использует наиболее сильный сигнал для настройки мощности и эквалайзера. Поскольку более мощный сигнал передан с передатчика, а не с БПЛА, то БС не может корректно декодировать восходящий сигнал, так как неверно выделила ресурсы для передачи, что приводит к мгновенной потере сигнала оператором БПЛА. При этом, поскольку предлагаемая система «глушит» конкретный БПЛА, а не весь сигнал в соте, то остальные абоненты продолжают нормальную работу.

В итоге, алгоритм обнаружения и подавления несанкционированного БПЛА имеет следующую последовательность действий:

1) абонент входит в зону действия БС и инициирует процедуру установления соединения по радиоканалу случайного доступа RACH;

2) БС в ответ на установку соединения передает сообщение DCI по физическому каналу PDCCH, которое содержит управляющую информацию, в частности, выделенные ресурсы для передачи и запрос на информацию о канале связи от абонента;

3) предлагаемое устройство декодирует сигналы RACH и DCI. Сигнал от абонента сотовой сети в нормальных условиях принимает несколько базовых станций, обычно от трех до пяти. Так как БПЛА находится выше уровня человеческого роста и быстро перемещается, то его сигнал одновременно принимает значительно больший список БС, который постоянно изменяется. Кроме этого, в его сигнале присутствует доплеровское смещение. Анализируя эти данные, можно отличить БПЛА от всех других абонентов;

4) если целевым абонентом является БПЛА, то происходит процедура подавления БПЛА за счет генерации легитимных более мощных ZCS вместо тех, которые должен отправлять БПЛА на БС;

5) БС, получая две ZCS (от БПЛА и предлагаемого устройства), выбирает более мощный сигнал, т.е. сигнал помехи, и настраивает мощность передачи на его основе;

6) поскольку ZCS, сгенерированная предлагаемым устройством, не является истинной ZCS от БПЛА, то БС неправильно настраивает мощность

передачи, что приводит к мгновенной потере связи между оператором и БПЛА.

Новизна предлагаемой системы заключается в использовании стандартизированной технологии беспроводной связи 4G LTE и методов цифровой обработки сигналов для обнаружения и подавления БПЛА, при реализации которой не нужны радиолокационные, оптические, акустические и другие системы, что существенно снижает стоимость развертывания, так как для реализуемой системы необходимы устройства с одной антенной и одним трансивером. Также инновационность метода заключается в высокой устойчивости к погодным условиям и шуму, а также в отсутствии чувствительности к размеру несанкционированного БПЛА.

В предлагаемом решении, помимо реализации систем обнаружения БПЛА, также применяется система подавления БПЛА за счет генерации ложной ZCS, которая приводит к мгновенному выходу из строя целевого БПЛА.

ЗАКЛЮЧЕНИЕ

Предлагаемый подход позволит обеспечить практическое решение задачи обнаружения и подавления (при необходимости) беспилотных летательных аппаратов, использующих инфраструктуру сотовых операторов для организации канала связи и управления, без нарушения работы сотовой сети. Данный метод подходит для организации защиты мест массового скопления людей: парки, концерты, стадионы и т.д.

СПИСОК ЛИТЕРАТУРЫ

1. 4G/LTE - Frame Structure/Downlink. – https://www.sharetechnote.com/html/FrameStructure_DL.html.

2. 4G/LTE - Frame Structure. – https://www.sharetechnote.com/html/FrameStructure_UL.html.

3. MLAT. – <https://ru.wikipedia.org/wiki/MLAT>.

4. Radars Accuracy. – <https://www.radartutorial.eu/01.basics/Radars%20Accuracy.en.html>.

5. Dahlman, E. 4G LTE/LTE-Advanced for Mobile Broadband / E. Dahlman, S. Parkvall, J. Sköld. – Oxford: Elsevier, 2011. – 431 с.

Получено 14.10.24

A system for detecting and suppressing UAVs using the infrastructure of cellular operators for communication and control

I.M. Kudrin, bachelor; i.kudrin@ntc-rassvet.ru

I.G. Afonin, NTC RASSVET LLC, technical director; afonin_ig@ntc-rassvet.ru

Abstract. A system for detecting and suppressing unmanned aerial vehicles (UAVs) is proposed, which is based on the use of 4G LTE cellular communications infrastructure. UAVs that are operated through network providers function like standard subscriber devices with SIM cards, and their signals can be detected through the analysis of LTE control channels (PBCH, PDCCH, PUSCH). This approach allows for the detection of unauthorized UAVs by analyzing their interaction with base stations. To localize UAVs, it is proposed to use multilateration (MLAT) and digital beamforming. In addition, the system can disrupt the UAV signal by interfering with the data exchange between the UAV and the base station through legitimate signal jamming.

Keywords: UAV detection, UAV suppression, LTE infrastructure, radio frequency signals, digital beamforming, multilateration (MLAT), interference generation.