Способ обнаружения и подавления беспилотных летательных аппаратов

И.Г. АФОНИН, технический директор ООО “ЮБИТЕЛ”

В последние несколько лет наблюдается активное развитие и распространение беспилотных летательных аппаратов (БПЛА). Они широко используются, например, для наблюдения и мониторинга окружающей среды, разведывательных миссий, распыления удобрений в сельском хозяйстве, доставки грузов, в различных военных операциях.

Однако с увеличением доступности технологий БПЛА возрастает и угроза их использования в незаконных или угрожающих целях. Беспилотные летательные аппараты могут нарушать воздушное пространство и препятствовать безопасной работе аэропортов, приближаться и атаковать важные объекты инфраструктуры. Кроме того, они могут быть использованы в шпионаже, контрабанде и террористических атаках.

Рис. 1. Управляемый через SIM-карту БПЛА

В настоящий момент активно развивается технология обеспечения связи и управления БПЛА с использованием имеющейся инфраструктуры операторов сотовой связи стандарта 4G LTE из-за его распространенности, широкого покрытия территорий и легкого подключении к сети. При этом каждый несанкционированный БПЛА, который передает 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 (рис. 1).

Специалистами нашей компании были рассмотрены два метода обнаружения несанкционированного БПЛА: анализ трафика или сигналов взаимодействия между абонентом сети (БПЛА) и базовыми станциями.

Анализ трафика был признан менее перспективным, так как различные производители БПЛА могут использовать различные виды кодирования и шифрования информации. Кроме того, они могут меняться со временем. Сигналы взаимодействия стандартизованы 3GPPP, все базовые станции, работающие по стандарту LTE, используют обязательные алгоритмы и процедуры управления абонентами, поэтому все абоненты сети обязаны их выполнять или им не будет предоставлен канал связи.

Таким образом, 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 базовой станцией и абонентом сетей 4G LTE.

Предлагаемый подход предполагает обнаружение БПЛА на основе

Рис. 2. Снимок экрана программы управления комплексом

нисходящих сигналов в логических каналах к PBCH и PDCCH, а также информации из восходящего канала PUSCH.

Функционал подавления БПЛА основан на использовании генератора помех. Генератор помех включается на радиочастоте абонента в момент обмена между БС и абонентом служебными сообщениями. 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 (рис. 2).

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

1) абонент входит в зону действия базовой станции и инициирует процедуру RACH;

2) базовая станция в ответ на RACH передает DCI по физическому каналу PDCCH, содержащему управляющую информацию, в частности, выделенные ресурсы для передачи и запрос на информацию о канале связи от абонента SRS;

3) предлагаемое устройство декодирует сигналы RACH и DCI. Сигнал от абонента сотовой сети при нормальной работе принимает несколько базовых станций (обычно от 3 до 5). Так как БПЛА находится выше уровня человеческого роста и быстро перемещается, то его сигнал одновременно принимает значительно больший список БС, который постоянно меняется. Кроме этого, в сигнале присутствует допплеровское смещение. Анализируя эти данные, можно отличить БПЛА от всех других абонентов;

4) если целевой абонент является БПЛА, то происходит процедура подавления БПЛА за счет генерации легитимных более мощных сигналов контроля состояния радиоканала, которые должен отправлять БПЛА на базовую станцию по каналу PUSCH, и информации SRS;

5) базовая станция, получая два различных сигнала — от БПЛА и предлагаемого устройства, выбирает более мощный сигнал, т. е. сигнал помехи, и настраивает мощность передачи на его основе;

6) поскольку сигнал контроля состояния канала, сгенерированный предлагаемым устройством, не является истинным сигналом от БПЛА, базовая станция неправильно настраивает мощность передачи, что приводит к мгновенной потери связи между оператором и БПЛА.

Новизна предлагаемой системы заключается в использовании стандартизованной 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. Также инновационность метода заключается в высокой устойчивости к погодным условиям, шуму и отсутствию чувствительности к размеру несанкционированного БПЛА.

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: парков, концертов, стадионов и т. д.

Защита абонентов

Компании, которые звонят абонентам мобильных операторов, должны будут предоставлять ***информацию о цели звонков****. Это нужно, чтобы граждане видели, кто и зачем им звонит. В противном случае такой вызов будет блокироваться. На официальном сайте для размещения информации о подготовке нормативных правовых актов и результатах их обсуждения опубликован соответствующий проект федерального закона.*

Работать это будет следующим образом: компании, совершающие звонки абонентам мобильной сети, особенно массового характера, будут обязаны сообщать своему оператору, кто они и зачем звонят; полученные данные автоматически передаются от оператора к оператору, и на телефоне абонента определится источник звонка; при этом абонент будет вправе отказаться от массовых вызовов или выбрать только те компании, вызовы от которых он готов принимать.

Если компания не предоставит необходимую информацию, вызов будет блокироваться. Критерии массовых звонков и правила передачи сведений определит правительство.

Данные меры введены, потому что каждый месяц только крупнейшие мобильные операторы блокируют в среднем до 0,5 млрд нежелательных звонков. Такие вызовы часто применяют для навязывания сомнительных услуг или с мошенническими целями.

Стоит отметить, что у некоторых операторов уже есть сервисы, которые позволяют определить, кто совершает обзвон. Важно, чтобы эта функция была доступна для всех абонентов на постоянной основе. Такое информирование позволит абонентам отличать полезные звонки от нежелательных.

Некорректно работающие сервисы

В связи с появлением информации о доступности ресурсов со ссылкой на данные сервиса isitblockedinrussia.com специалисты ***Центра мониторинга и управления сетью связи общего пользования предупреждают****, что сервис не предоставляет достоверную информацию о доступности интернет-ресурсов. Работа сервиса основана на проверке данных только в Едином реестре запрещенной к распространению информации.*

Доступ к запрещенным интернет-сервисам также может ограничиваться в рамках оперативного централизованного реагирования на угрозы согласно Постановлению Правительства РФ от 12 февраля 2020 года № 127.