



Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Московский государственный технический университет имени
Н.Э. Баумана
(национальный исследовательский университет)»
(МГТУ им. Н.Э. Баумана)

ФАКУЛЬТЕТ «Информатика и системы управления»

КАФЕДРА «Программное обеспечение ЭВМ и информационные технологии»

Научно-исследовательская работа

Тема Исследование методов генерации шумов и помех

Студент Котляров Н.А.

Группа ИУ7-51Б

Научный руководитель Тассов К.Л.

Москва — 2022 г.

Оглавление

Введение	3
1 Анализ предметной области	4
1.1 Классификация основных типов сигналов и модуляций . . .	4
1.1.1 Управляющий диапазон	4
1.1.2 Модуляции	4
1.2 Способы формирования помехи	5
1.2.1 Формирования помехи с помощью шума	5
1.2.2 Формирования помехи с помощью активного сигнала	7
1.3 Машинное обучение	8
1.3.1 Базовое понятие машинного обучения	9
1.3.2 Категории машинного обучения	10
Заключение	14
Литература	15

Введение

Беспилотные летательные аппараты (БПЛА) могут использоваться для различных видов незаконной деятельности (например, промышленный шпионаж, контрабанда, терроризм). Учитывая их растущую популярность и доступность, а также достижения в области коммуникационных технологий, необходимо искать способы вывести из строя эти транспортные средства. Для вывода из строя дронов используются различные способы формирования помехи, но более продвинутые методы, такие как обман и захват БПЛА, реализовать значительно сложнее, и в этой области существует большой пробел в исследованиях. В настоящее время популярны методы машинного и глубокого обучения, которые также используются в различных приложениях, связанных с дронами. Это обучение может помочь БПЛА переключаться на другую частоту при обнаружении факта формирования помехи. Однако если передаваемый на нужной частоте шум будет похож на осмысленный сигнал, будет возможность «обмануть» БПЛА и таким образом не дать аппарату переключиться на другую частоту.

Цель данной научно-исследовательской работы — провести обзор методов генерации с помощью нейронных сетей шумов и помех, напоминающих управляющие сигналы.

Для достижения поставленной цели необходимо решить следующие задачи:

- классифицировать основные типы сигналов и модуляций БПЛА;
- изучить основные методы формирования помехи;
- определить базовое описание и разделение машинного обучения и глубокого обучения;
- представить различные типы нейронных сетей;
- сравнить представленные нейронные сети в рамках генерации шума для формирования помехи.

1 Анализ предметной области

В данном разделе будут представлены классификация основных типов сигналов и изучены основные методов формирования помехи, описаны и разделены машинное обучение и глубокое обучение и представлены и сравнены нейронные сети, подходящие под поставленную цель.

1.1 Классификация основных типов сигналов и модуляций

1.1.1 Управляющий диапазон

Современные коммерческие дроны обычно работают в стандартном Wi-Fi диапазоне (2.4 ГГц и 5 ГГц) [1]. Даже базовые коммерческие дроны обычно имеют несколько запрограммированных автоматических функций, таких как отслеживание положения дрона или функция «возврат домой», срабатывающая в случае потери управляющего сигнала. Для этих функций используется «Глобальная Навигационная Система Позиционирования» (GNPS), однако уже началась интеграция 4G и 5G для управления дронами [2].

1.1.2 Модуляции

На данный момент для управления дронами используются сигналы с расширенным спектром [3]. Эти типы сигналов обладают хорошей устойчивостью к помехам, как естественным (шум) так и преднамеренным (глушение). Принцип расширения спектра заключается в модуляции [4] узкополосного сигнала, содержащего информацию, псевдослучайным широкополосным сигналом. При такой модуляции получается сигнал с расширенным спектром.

1.2 Способы формирования помехи

Постановка помех — это метод нейтрализации этих приемников сигнала. Самыми основными методами формирования помехи: с помощью шума и активного сигнала [5]. Важно отметить, что целью воздействия всегда является приемник, так как требуется меньшая мощность помех, чтобы обеспечить достаточное отношение помех к сигналу [6].

1.2.1 Формирования помехи с помощью шума

Принцип этого типа формирования помехи заключается в передаче шума требуемой формы, мощности и полосы пропускания, который используется для перекрытия изначального сигнала и предотвращая передачи между приемником и передатчиком. В результате уровень помех на стороне приемника увеличивается, что увеличивает отношение помех к сигналу [6]. Этот тип глушения широко используется против коммуникационных и не коммуникационных сигналов. Не коммуникационные сигналы обычно используются в области активной радиолокации, следовательно, рассматриваться не будут.

Узкополосный шум

Этот тип полосы пропускания определяется частотным спектром изначального сигнала, (см. рисунок 1.1). В связи с тем, что в настоящее время для целей связи широко используются сигналы с расширенным спектром, этот шум обычно непригоден для создания помех БПЛА.

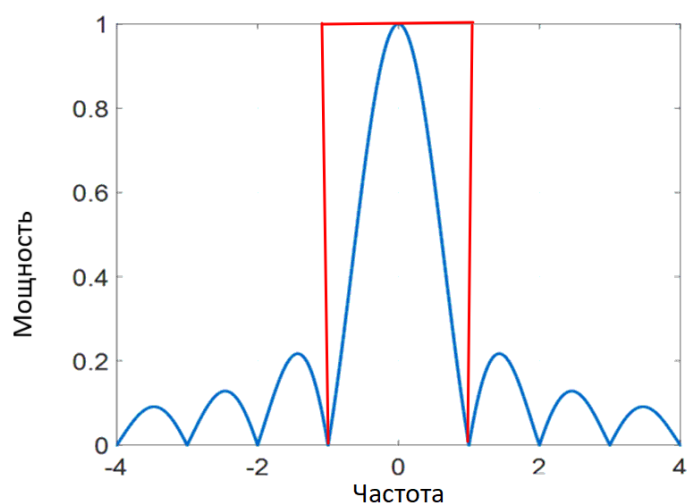


Рисунок 1.1 – Спектр узкополосных шумовых помех

Сверхширокополосный шум

Этот тип шумовых помех охватывает всю полосу пропускания сигнала связи, (см. рисунок 1.2). Его недостатком является необходимость высокого уровня мощности для обеспечения достаточного отношения шума к сигналу для эффективного формирования помехи. В результате сверхширокополосный шум снижает пропускную способность канала системы. Это приводит к уменьшению отношения сигнала к шуму на стороне приемника и увеличению количества ошибок передачи.

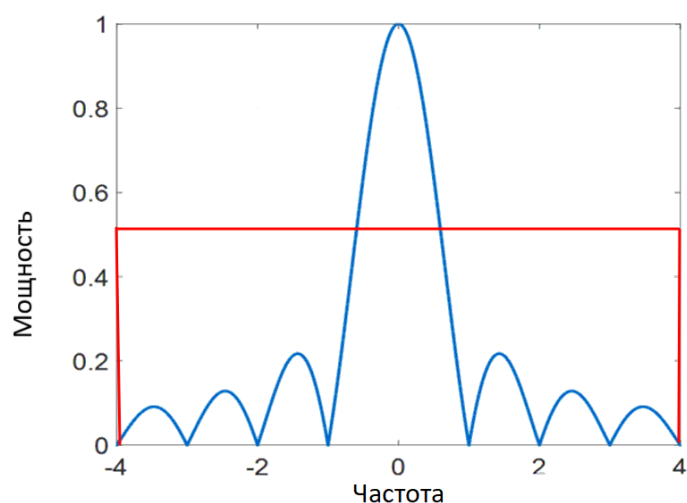


Рисунок 1.2 – Спектр сверх широких шумовых помех

Развертка шума

Принцип этого типа формирования помехи заключается в быстром перемещении относительно узкополосного сигнала по всему интересующему диапазону. Сигналом помехи может быть шум или импульсный сигнал. Забивается только одна частота. Хотя охватывается весь спектр скачкообразной перестройки частоты, скачки выполнять не обязательно. Из-за слабой мощности сигнала GPS также происходит экономия необходимой мощности помехового сигнала для достижения требуемого отношения помех к сигналу. Поскольку большинство БПЛА имеют некоторую функцию автопилота (например, упомянутую выше функцию «возврата домой»), глушение сигналов GPS является одним из способов нейтрализовать дроны, не уничтожая их.

Интеллектуальный шум

При этом типе помех воздействуют только на необходимые сигналы в спектре, чтобы предотвратить связь между приемником и передатчиком. Однако требуется предварительное знание типа сигнала помехи. Для этого типа глушения необходим анализ протоколов, используемых различными производителями приемников. Из анализа протоколов и входящего сигнала можно определить критические точки, которые могут быть затронуты. Затем можно создать сигнал с аналогичными параметрами. Этот тип глушения является наиболее энергоэффективным и эффективным, но, по логике вещей, и наиболее технологически требовательным.

1.2.2 Формирования помехи с помощью активного сигнала

Этот способ также называется подделыванием. В отличие от шума, он не направлен на создание помех в определенной части спектра и, таким образом, на предотвращение передачи. Его цель — создать и отправить сигнал, аналогичный исходному сигналу. Такой сигнал с более высоким уровнем мощности, чем у законного передатчика, затем используется для обмана приемника. Это может иметь различные последствия, например,

сбить с толку GPS. Как следует из описанного принципа, конструкция такого глушителя более сложна по сравнению с шумовым глушителем. Для шумовых помех требуется использовать простой приемник, чтобы найти интересующий сигнал в спектре. В случае подделывания ответа необходимо принять исходный сигнал, изменить его и отправить новый ложный сигнал достаточной мощности, чтобы, приемник «поверил», что это настоящий контролирующий сигнал.

Декодирование исходного сигнала или его протокола является сложным и требует обратного проектирования, чтобы понять его структуру. Кроме того, требуется учитывать влияние окружающей среды, поскольку исходный сигнал может колебаться от различных воздействий колеблется (например, для GPS необходимо учитывать положение спутника и погоду). Некоторые неблагоприятные воздействия на передачу значительно устранены в приемниках цели: например, в GPS колебания амплитуды уменьшаются с помощью схем автоматической регулировки усиления [7]. Однако по принципу своей работы эта система делает устройство более склонным к глушению отклика — обман GPS может привести к путанице в данных навигации [8].

Еще одной проблемой, особенно с военной техникой, является шифрование, которое сильно усложняет получение изначального сигнала.

Хотя существуют различные способы перехвата и классификации сигналов [9], эти методы обычно требуют много времени. Таким образом возникает проблема реагирования в режиме реального времени.

1.3 Машинное обучение

Для того, чтобы не только перехватить и расшифровать, но и преобразовать сигнал, стоит использовать методы машинного и глубокого обучения. Данные методы помогают оптимизировать прием и расшифровку сигнала более эффективно, чем классические алгоритмы [10], следовательно стоит рассмотреть возможность использования машинного или глубокого обучения для преобразования сигнала.

1.3.1 Базовое понятие машинного обучения

Ассоциация машинного обучения основана на поиске связей между переменными в большой базе данных. Метод используется для установления сильных правил, обнаруженных в базе данных с помощью некоторых мер интересности [11]. Этот основанный на правилах подход генерирует также новые правила по мере анализа дополнительных данных. Конечной целью, исходя из достаточно большого набора данных, помочь машине имитировать выделение и создание возможности нахождения абстрактных ассоциаций из новых неклассифицированных данных.

Классификация машинного обучения — базовая проблема, которая часто решается при работе с большими объемами данных. Требуется классифицировать большой набор входных данных на несколько выходных классов. Простейшей классификацией является разделение на два класса (A и B). После обучения классификатора прошлыми данными правило классификации может выглядеть как *if/else*:

$$C = \begin{cases} A, \text{ если } condition_1 > \theta_1 \text{ и } condition_2 > \theta_2, \\ B, \text{ иначе.} \end{cases} \quad (1.1)$$

Многие приложения машинного обучения имеют разные типы классификаторов. Эти классификаторы часто используются для распознавания образов. Примером может служить преобразование рукописного текста в компьютерную запись. Здесь много переменных, так как у каждого человека разный почерк (наклон, размер шрифта, тип пера и т. д.). Проблема с разным почерком заключается в том, что у не существует стандартизированной системы того, как должны выглядеть отдельные буквы. Следовательно, уместно использовать классификатор на основе машинного обучения, который извлекает формулу из большой выборки обучающих данных, в которую, хотя и не все, удастся включить большинство шрифтов. Другим примером может быть распознавание дорожных знаков в автономных транспортных средствах. Здесь изображение с камеры представляет собой систему отдельных пикселей. Основываясь на контрасте, цветах и узорах, можно было идентифицировать соответствующий дорожный знак. Кроме

того, такие классификаторы могут быть использованы в медицине (для диагностики), распознавания речи или биометрии [11].

Изучение правил или формул извлечения данных создает простую модель, описывающую эти данные. Это дает объяснение заданного набора данных, которое было бы невозможно получить при анализе этих данных человеком (такая обработка заняла бы нереальное количество времени). Еще одним преимуществом этого подхода является сжатие. Формула является гораздо более простым объяснением проблемы, чем сами данные. В результате это экономит память и вычислительные требования на компьютере. Другим выгодным применением может быть установка границ, когда классификатор выбирает входные данные, которые не попадают в выбранные классы. Эти входные данные могут потребовать особого внимания при обработке данных [11].

Регрессия машинного обучения — модель взаимосвязи между несколькими входными переменными и выходной зависимой переменной.

Регрессия делится на несколько видов:

- линейная — метод для моделирования отношений между одной независимой входной переменной (переменной функции) t и выходной зависимой переменной;
- множественная линейная — взаимосвязь создается между несколькими входными переменными и выходной зависимой переменной;
- полиномиальная — модель становится нелинейной комбинацией входных переменных, то есть среди них могут быть экспоненциальные переменные;
- логистическая — метод классификации данных по двум классам с помощью сигмоидальной функции. Этот тип регрессии обычно используется для распределения данных по классам вероятности.

1.3.2 Категории машинного обучения

Машинное обучение можно разделить на несколько категорий: контролируемое обучение, неконтролируемое, полууправляемое и обучение с под-

крепленим.

Контролируемое обучение

В эту категорию попадают как проблемы регрессии, так и проблемы классификации. Имеется набор входных данных X и требуемых выходов Y , задача состоит в том, чтобы найти функцию или формулу, описывающую связь между X и Y . Подход машинного обучения предполагает модель, определенную как:

$$Y = g(X|\theta), \quad (1.2)$$

где $g()$ — модель, θ — ее параметр. Y — номер регрессии и код класса для классификации. $g()$ — функция регрессии или дискриминаторная функция. Алгоритм машинного обучения затем оптимизирует θ так, чтобы ошибка аппроксимации была минимальной по отношению к обучающему набору данных. Входной набор данных X обычно делится на обучающие и тестовые данные. Данные обучения используются для создания модели зависимости между входными данными X и выходными данными Y и, таким образом, для нахождения $g()$. Тестовые данные используются для измерения точности модели, таким образом, описанная оптимизация θ . Поэтому для контролируемого обучения необходимо иметь достаточный набор обучающих данных X , для которых известны правильные выходные данные Y . Эти выходные данные предоставляются «учителем» (экспертом, создающим алгоритм). Поэтому эта категория называется обучением с учителем [12].

Неконтролируемое обучение

В неконтролируемом обучении нет «учителя», и нет доступных правильных результатов. Доступны только входные данные, и цель состоит в том, чтобы найти закономерность во входных данных. Во входном наборе одни паттерны появляются чаще других, и мы хотим знать, что вообще происходит, а что нет. В статистике эта задача называется функцией плотности вероятности [13]. Одним из методов определения функции плотности вероятности является так называемая кластеризация. Здесь мы пытаемся найти разные группы со схожими параметрами во входных данных. Приме-

ром кластеризации является сжатие изображений. В этом случае входными данными являются пиксели со значениями RGB. Алгоритм кластеризации объединяет пиксели с похожими цветами в одну группу. Созданные таким образом группы соответствуют цветам, часто встречающимся на изображении. Таким образом можно значительно уменьшить количество используемых цветов (или количество битов, присваиваемых одному цвету) и таким образом добиться требуемого сжатия [11].

Полууправляемое обучение

Полууправляемое обучение представляет собой комбинацию двух вышеупомянутых типов, где обучающие данные доступны с известными выходными данными и без них [13]. Имеется набор неразмеченных данных, а для части из них у есть дополнительная информация (небольшое количество размеченных данных). Полууправляемое обучение имеет большое практическое значение, так как во многих случаях маркируется только часть данных, а получение остальных меток может быть весьма затруднительным (например, необходимость в специальных устройствах или дорогостоящие и медленные эксперименты). Есть две задачи, которые решает полууправляемое обучение [14].

- 1) Индуктивное полууправляемое обучение — предсказание меток для данных тестирования.
- 2) Трансдуктивное полууправляемое обучение — маркировка неразмеченных данных в обучающем наборе.

Обучение с подкреплением

В обучении с подкреплением проблемы решаются с помощью последовательности действий, использующих правила проб и ошибок. Одно действие не важно — важно, чтобы вся последовательность приводила к правильному результату. В этом основное отличие от предыдущих категорий, которые основывались на использовании исторических данных, тогда как алгоритмы обучения с подкреплением обучаются на предыдущих попытках решить заданную сетевую задачу [13]. На рисунке 12 показаны пять основных элементов, необходимых для обучения с подкреплением [14]:



Рисунок 1.3 – Обучение с подкреплением

- агент: объект, который может выполнить действие A_t и получить вознаграждение R_t ;
- среда: представление реального мира, в котором действует агент;
- вознаграждение R_t : обратная связь агенту относительно выполненного действия A_t ;
- стратегия: обзор каждого состояния S_t по отношению к выполненному действию A_t ;
- значение функции: представляет, насколько хорошим является состояние S_t , но на самом деле это ожидаемое вознаграждение R_t в будущем по отношению к достигнутому состоянию S_t .

Таким образом, цель обучения с подкреплением состоит в том, чтобы выбрать стратегию (выполнение определенных действий A_t), которая максимизирует предопределенную функцию вознаграждения.

Заключение

Литература

- [1] UAV Communication Systems [Электронный ресурс]. Режим доступа: <https://www.extendingbroadband.com/aerial-tracking/drone-communication-systems/> (дата обращения: 23.11.2022).
- [2] Communications Standards for Unmanned Aircraft Systems: The 3GPP Perspective and Research Drivers [Электронный ресурс]. Режим доступа: <https://ieeexplore.ieee.org/document/9392776> (дата обращения: 23.11.2022).
- [3] SPREAD SPECTRUM SIGNALS IN MODERN COMMUNICATIONS [Электронный ресурс]. Режим доступа: https://www.researchgate.net/publication/228540839_SPREAD_SPECTRUM_SIGNALS_IN_MODERN_COMMUNICATIONS (дата обращения: 23.11.2022).
- [4] Модуляция сигнала [Электронный ресурс]. Режим доступа: <https://mobilradio.ru/information/vocabulary/modulation.htm> (дата обращения: 23.11.2022).
- [5] Радиоэлектронные помехи [Электронный ресурс]. Режим доступа: <http://zrv.ivo.unn.ru/pages/vtp/5/5-5-radioelektronnye-pomexi.htm> (дата обращения: 23.11.2022).
- [6] Отношение сигнал / помеха [Электронный ресурс]. Режим доступа: https://wiki5.ru/wiki/Signal-to-interference_ratio (дата обращения: 23.11.2022).
- [7] Автоматическая регулировка усиления [Электронный ресурс]. Режим доступа: https://en.wikipedia.org/wiki/Automatic_gain_control (дата обращения: 24.11.2022).
- [8] Development of a GPS spoofing apparatus to attack a DJI Matrice 100 Quadcopter [Электронный ресурс]. Режим доступа: <https://jgps.springeropen.com/articles/10.1186/s41445-018-0018-3> (дата обращения: 24.11.2022).

- [9] Analysis and decoding of radio signals for remote control of drones [Электронный ресурс]. Режим доступа: <https://ieeexplore.ieee.org/document/7747781> (дата обращения: 24.11.2022).
- [10] A Deep Learning-Based Intelligent Receiver for OFDM [Электронный ресурс]. Режим доступа: <https://ieeexplore.ieee.org/abstract/document/9637770> (дата обращения: 24.11.2022).
- [11] E. A. Introduction to Machine Learning. — MIT, 2020. Vol. 660. P. 33–34.
- [12] Artificial Intelligence for UAV-Enabled Wireless Networks: A Survey [Электронный ресурс]. Режим доступа: <https://ieeexplore.ieee.org/document/9411810> (дата обращения: 27.11.2022).
- [13] A Survey on Machine-Learning Techniques for UAV-Based Communications [Электронный ресурс]. Режим доступа: <https://www.mdpi.com/1424-8220/19/23/5170> (дата обращения: 27.11.2022).
- [14] Chapelle O., Scholkopf B., Zien Eds. A. Semi-Supervised Learning (Chapelle, O. et al., Eds.; 2006) [Book reviews] // IEEE Transactions on Neural Networks. 2009. T. 20, № 3. С. 542–542.