УДК 004.056.53 **DOI** 10.15622/ia.20.6.7

Е.С. Басан, Е.С. Абрамов, А.Г. Басюк, Н.А. Сушкин

МЕТОД ОБНАРУЖЕНИЯ АТАК НА СИСТЕМУ НАВИГАЦИИ БПЛА

Басан Е.С., Абрамов Е.С., Басюк А.Г., Сушкин Н.А. **Метод обнаружения атак на систему навигации БПЛА.**

Аннотация. В данной работе рассмотрены вопросы реализации методов защиты беспилотных летательных аппаратов (БПЛА) от атак спуфинга глобальной системы позиционирования (GPS), для обеспечения безопасной навигации. Глобальная навигационная спутниковая система (GNSS) широко используется для определения местоположения БПЛА и на сегодняшний день является самым популярным навигационным решением. Это связано с простотой и относительно невысокой стоимостью данной технологии, а также точностью передаваемых координат. Тем не менее, существует множество угроз безопасности GPS-навигации. Это в первую очередь связано с природой сигнала GPS, т.к. сигнал передается в открытом виде, поэтому злоумышленник может заблокировать или подделать его. В данном исследовании проведен анализ существующих методов защиты GPS. В рамках исследования был разработан экспериментальный стенд и сценарии атак на систему GPS БПЛА. Далее были собраны данные из журнала полетов БПЛА и проведен анализ кибер-физических параметров, чтобы увидеть влияние атаки на показания бортовых датчиков. Исходя из этого, был предложен новый метод обнаружения аномалий БПЛА, основанный на анализе изменений внутренних параметров БПЛА. Этот метод самодиагностики позволяет БПЛА самостоятельно оценивать наличие изменений в его подсистемах, и выявлять признаки кибератаки. Для выявления атаки БПЛА собирает данные об изменении кибер-физических параметров на протяжении определенного периода времени, затем обновляет эти данные. В результате БПЛА необходимо определить степень различий между двумя временными рядами собранных данных. Чем больше будет степень различий между обновленными данными и предыдущими, тем больше вероятность того, что на БПЛА проводится атака.

Ключевые слова: безопасность, атака, навигационная система, беспилотный летательный аппарат, вероятность, технология защиты, угроза, глобальная навигационная спутниковая система.

1. Введение. Основная проблема, на решение которой направлено данное исследование, предусматривает необходимость разработки метода детектирования, а в последствии и защиты от атак, направленных на подмену сигнала GPS, с целью повышения защищенности БПЛА. Глобальная навигационная спутниковая система (GNSS) широко используется для определения местоположения во многих гражданских и военных приложениях. Такие приемники GNSS, как GPS, GLONASS, Galileo и Beidou, принимают радиосигналы, передаваемые со спутников. Принятые спутниковые сигналы обрабатываются приемником и получают информацию о местоположении, скорости и времени приемника. Злоумышленник

пытается спроецировать ложное положение или ложную траекторию на целевой GPS-приемник.

Необходимость разработки новых методов и средств обнаружения аномалий, связанных с неисправностями, воздействием со стороны злоумышленника или со стороны окружающей среды на автономный БПЛА в режиме реального времени обусловлена тем, что большинство методов обнаружения аномалий для БПЛА основываются на использовании нейронных сетей или методов, где необходимо сравнивать нормальное поведение с аномальным. При этом создание шаблонов поведения БПЛА само по себе является сложной задачей, кроме того существуют ситуации, которые могут быть ложно приняты за аномальные или нормальные. Например, в случае сильного ветра БПЛА усиливает вращение двигателей, что приводит к ускоренному исчерпанию заряда аккумулятора, такое поведение может быть принято за атаку, направленную на исчерпание ресурсов.

Каждая модель БПЛА имеет собственные шаблоны поведения и диапазоны нормальных значений кибер-физических параметров. Метод детектирования аномалий для БПЛА должен быть универсальным и легко масштабируемым, но из-за большого разнообразия моделей БПЛА и отсутствия стандарта их производства, разработка масштабируемого и легко адаптируемого решения становится сложной.

Актуальность научной проблемы обусловлена тем, что большинство существующих подходов к обнаружению аномалий или атак сложно реализуются и требуют большого количества времени для разработки системы обнаружения. Рассмотрим основные принципы создания системы обнаружения вторжений для БПЛА (СОВ-БПЛА). Система обнаружения вторжений для беспилотных летательных аппаратов (СОВ-БПЛА) разрабатывается с целью обнаружения аномального поведения или непредвиденных действий в сети путем автоматического анализа поведения или анализа на основе заданной гипотезы и/или политик, которые регулируются правилами безопасности данной сети [1]. СОВ-БПЛА отслеживает конфигурацию системы, файлы данных и/или передачу данных по сети, чтобы проверить, присутствует ли атака. Кроме того, СОВ-БПЛА направлена на обнаружение неправомерного использования БПЛА. Неправильное использование может быть определено, как любое нежелательное действие, которое может вызвать какой-либо вред с точки зрения производительности или безопасности всей группы БПЛА. В БПЛА встроена кибер-физическая система, состоящая из датчиков и/или

исполнительных механизмов. Датчики предоставляют данные (или информацию) исполнительному механизму, который может управлять БПЛА. Собранные данные используются для анализа и принятия важных решений, связанных с полетной миссией. Ключевые механизмы СОВ можно классифицировать следующим образом. Это механизмы на основе:

– спецификации [2]: СОВ включает в себя набор соответствующих правил, определенных на основе ожидаемого поведения БПЛА. Эти указанные правила применяются для отслеживания успешных запусков системы БПЛА;

– сигнатур [3]: этот метод направлен на обнаружение известных атак на основе заранее определенных известных сигнатур. При обнаружении аномальных действий запускается операция обнаружения для определения совпадающей сигнатуры, чтобы гарантировать обнаружение вторжения;

– аномалий [3]: аномальное поведение обнаруживается на основе сбоя или нежелательной активности, наблюдаемой в системе. С целью обнаружения известных и/или неизвестных атак этот метод использует механизм обучения или фильтрации, который может значительно улучшить обнаружение неизвестных атак при отсутствии заранее определенных сигнатур неизвестных атак;

– гибридного подхода [4], объединяющего два или более методов обнаружения, таких как спецификация плюс аномалия, чтобы обеспечить строгую политику обнаружения, которая может обнаружить известные и/или неизвестные атаки.

Таким образом, для каждого из существующих методов должны быть заранее собраны и сформированы наборы данных для обучения, либо для построения шаблонов поведения или правил. Такие подходы требуют большого количества времени для сбора данных о БПЛА, а также их реализация может требовать дополнительных вычислительных ресурсов для БПЛА. В случае использования методов, которые основаны на использовании нейронных сетей, для реализации эффективного обнаружения аномалий требуется создание обучающей выборки, которая включает в себя, как правило, большое количество тестовых данных.

На основании вышесказанного научная значимость решения проблемы состоит в необходимости разработки нового подхода, основанного на других математических методах обнаружения аномалий БПЛА без необходимости предварительного сбора большого объёма данных и описания нормальных шаблонов поведения. Новый подход может упростить процесс создания системы обнаружения

аномалий, что в дальнейшем будет способствовать более простому внедрению СОВ в БПЛА.

Целью данного исследования является разработка метода детектирования атак в виде подмены сигналов GPS, поступающих на БПЛА, на основании параметров сенсорной системы беспилотного аппарата. Метод должен позволять БПЛА обнаруживать атаку без необходимости предварительных знаний об эталонном изменении сигналов с сенсорных датчиков, в режиме реального времени, автономно.

Метод выявления аномалий поведения БПЛА, возникающих, как в результате проведения атак, так и в результате негативного воздействия со стороны окружающей среды, должен обнаруживать аномалии в режиме реального времени без предварительных затрат на обучение, с низкими требованиями к потреблению ресурсов БПЛА. Данный метод был ранее реализован авторами для анализа аномалий в беспроводной mesh-сети, имитирующей передачу данных в группе БПЛА, а также передачу видеопотока. Метод основан на вычислении значения энтропии, то есть разницы между вероятностными распределениями кибер-физических параметров. Метод показал свою эффективность и способность обнаруживать не только атаки, но и смену шаблонов поведения, а также режимов получения/отправки данных. При этом были получены наборы параметров, которые изменяются как под воздействием различных атак, так и в результате смены режима поведения. Данные наборы параметров оказались различными, степень различий между изменениями также отличалась (то есть можно анализировать интенсивность изменений), что в дальнейшем позволит различать типы атак и типы нормального поведения. Особенностью метода является отсутствие необходимости предварительного составления шаблонов поведения и базы данных для обучения. Данные об изменении параметров нужны только для тестирования и проверки эффективности метода, а также для отладки и установления переменных, с учетом которых метод будет работать лучше. Примером такой переменной может служить время обновления информации о параметрах и длинна временного ряда за прошедший и новый период времени, для сравнения друг с другом. Метод также был протестирован на данных, собранных по результатам летных испытаний БПЛА, полученных от полетного контроллера. При этом метод также показал эффективность при выявлении атаки GPS-спуфинг. Таким образом, можно утверждать, что метод может быть масштабирован и применен для различных наборов кибер-физических параметров и типов атак.

2. Анализ релевантных работ. Проблема обнаружения атак на БПЛА, является актуальной, так как в первую очередь выполнение функций БПЛА может быть связано с жизненно важными для человека областями. Авторы статьи [1] говорят о том, что подавление сигнала и спуфинг глобальной навигационной спутниковой системы (ГНСС) считаются основными угрозами для БПЛА. Это может привести к крушению и потере управления над БПЛА, которые используются в критически важных операциях. Зачастую БПЛА используют навигационные сигналы открытых служб без защиты. Несмотря на то, что для реализации защиты был предложен ряд методов на основе пре- и пост корреляции сигнала, в настоящее время актуальной становится разработка алгоритмов машинного обучения для обнаружения атак подавления и спуфинга. Один из популярных алгоритмов машинного обучения - машинная классификация на основе опорных векторов (C-SVM) используется для детектирования атак на систему навигации БПЛА. В статье [1] авторы предлагают использовать метод C-SVM на этапе приема сигнала в связи с тем, что на этом этапе обработки существует ряд изменений сигнала, которые можно проанализировать. Можно установить соотношение между нормальными измерениями и наблюдаемыми, и детектировать аномалии с помощью классификации C-SVM. Добавление реальных наборов данных спуфинга и подавления к лабораторным наборам данных на этапе обучения C-SVM, позволяет повысить точность исследования. Сравнительный анализ всех четырех экспериментов, представленных в этой статье, показывает, что авторам удалось достичь хороших результатов благодаря следующим аспектам: 1) дополненный обучающий набор данных является актуальным для обнаружения попыток манипулирования сигналами ГНСС; 2) метод C-SVM является эффективным для обнаружения попыток манипуляции сигналами ГНСС.

В статье [2] предлагается метод обнаружения спуфинга GPS, на основе использования системы ориентации и определения курса (AHRS), а также акселерометра для сравнения разницы значений ускорения, полученных от GPS-приемника, и от инерциальной системы навигации, что обеспечивает обнаружение ошибки значения ускорения. Ускорение, полученное от приемника GPS, оценивается с помощью фильтра Калмана. Разница, выявленная между значениями ускорения от GPS-приемника и акселерометра используется для обнаружения спуфинга. Величина ошибки ускорения может использоваться, как переменная решения. Кроме того, предлагается использовать величину северной (или восточной) составляющей ошибки ускорения в качестве другой переменной решения.

Эффективность использования двух переменных решения доказывается путем вычисления вероятности обнаружения спуфинга с учетом заранее определенной вероятности ложной тревоги и обнаружения. Если обе переменные решения используются вместе, удается получить наилучшую вероятность обнаружения спуфинга.

Если отсутствует возможность использования GPS, беспилотные летательные аппараты (БПЛА) для координации полета могут использовать инерциальные датчики. При этом, как правило, возникают погрешности в определении местоположения с помощью инерциальных датчиков, что может привести к аварийной ситуации. Чтобы избежать возникновения недопустимой погрешности датчиков в случае атак с подменой GPS, авторы статьи [3] предлагают методику управления с ограничениями безопасности. Данная методика позволяет адаптировать полет БПЛА путем перепланирования полётного задания для повышения устойчивости к атакам с подменой GPS. Детектор атак используется для обнаружения атак с подменой GPS и обеспечивает переключение между режимами надежного и аварийного управления. Система отслеживания местоположения злоумышленника (ALT) разработана для оценки выходной мощности устройства спуфинга с помощью фильтра Калмана (UKF). Используя оценки от ALT, авторы проектируют контроллер эвакуации (ESC) на основе модели прогнозирующего контроллера (MPC), чтобы БПЛА дислоцировался из зоны действия устройства злоумышленника в течение допустимого времени.

Другие методы предотвращения спуфинга GPS, такие как мониторинг исправности приемника в автономном режиме, измерение отношения сигнал/шум и обнаружение доплеровского сдвига, обсуждаются в [4]. В работе [5] был предложен метод, позволяющий БПЛА обнаруживать источник спуфинга GPS с помощью независимой наземной инфраструктуры, которая непрерывно анализирует содержание и время поступления информации о предполагаемом местоположении БПЛА. Было показано, что предложенный метод эффективен при обнаружении атак спуфинга менее чем за 2 с и позволяет определять местоположение источника поддельного сигнала с точностью до 150 м. В статье [6] для обнаружения и оповещении о потенциальных атаках используется анализ автоматической регулировки усиления сигнала GPS в приемнике GPS.

В работах [7-9] рассматривается возможность использования нескольких приемников для обнаружения атак с подменой GPS. В работе [8] использовалось несколько независимых GPS-приемников для обнаружения атак с подменой GPS. Предлагаемый метод

анализирует расстояние между приемниками и последующим измерением расстояния между указанными местоположениями приемников. При одинаковых сигналах GPS измеренные расстояния будут аналогичны ранее зафиксированным расстояниям. Однако при атаке с подменой GPS результаты измерения расстояния будут очень близки к нулю, поскольку все приемники передают информацию, где указано одно и то же местоположение, то есть разницы между приёмниками наблюдаться не будет. Автор работы [7] продемонстрировал возможность использования приемника с двумя антеннами для обнаружения атак с подменой GPS. Предлагаемый метод основан на анализе разницы фаз сигналов, полученных антеннами. Авторы работы [9] предлагают использовать несколько приемников для подтверждения подлинности сигналов GPS на основе сопоставления с сигналом GPS от военных спутников без необходимости его расшифровки. Предложенная методика показала свою эффективность даже тогда, когда приемники перекрестной проверки подделываются.

В статье [10] представлен подход к обнаружению атаки спуфинга GPS на беспилотный летательный аппарат на основе анализа оценки состояния с использованием машины опорных векторов (SVM). SVM используется в качестве инструмента для обнаружения аномалий. В этой работе были разработаны решения для обнаружения и среда моделирования атак с подделкой GPS для оценки функциональности и производительности метода. Подход не требует дополнительного оборудования, поэтому его можно использовать для небольшого БПЛА. С другой стороны, было показано, что, если нарушитель имеет абсолютное знание о позиционировании и траектории БПЛА, он сможет остаться незамеченным системой, вызывая при этом частые ложные срабатывания. В связи с тем что, как правило, нарушитель не знает фактическую траекторию БПЛА, было доказано: риск ложных срабатываний мал. Это означает, что система может обнаружить любую атаку спуфинга. Характеристики метода могут быть улучшены, если БПЛА будет оснащен другими датчиками (например, магнитометром).

Авторы работы [11] предлагают защитный механизм, основанный на концепции совместной локализации [12], который представляет собой методологию, позволяющую БПЛА определять свое реальное местоположение в двухмерной системе координат, используя местоположение трех других БПЛА. Предполагается, что каждый БПЛА имеет средства измерения относительных расстояний до других, соседних БПЛА путем определения расстояния между

БПЛА. При совместной локализации БПЛА выбирает любые три соседние БПЛА для обновления своего местоположения, учитывая, что выбранные БПЛА не лежат на одной прямой. После этого БПЛА может точно определить свое местоположение в двухмерной системе координат. Механизм совместной локализации, описанный в [12], может помочь БПЛА определить свое местоположение. Однако он предложен для случая потери сигналов GPS и не может использоваться напрямую в атаке спуфинга GPS. При атаке спуфинг GPS БПЛА не может доверять своему местоположению по GPS или местоположению других БПЛА. Выбор соседнего БПЛА для механизма совместной локализации сопряжен с риском, поскольку он также может подвергнуться атаке. Для преодоления этого ограничения, авторы [11] предлагают механизм защиты, основанный на том, что злоумышленник, использующий спуфинг GPS, может атаковать только один БПЛА. В предлагаемом механизме для определения своего реального местоположения БПЛА учитывает местоположение четырех соседних аппаратов вместо трех. Путем идентификации БПЛА, находящийся под воздействием атаки, он исключается из расчетов. Предлагаемый механизм имеет те же требования кооперативной локализации, то есть неколлинеарные БПЛА. БПЛА может запрашивать местоположение других аппаратов через связь между БПЛА, и каждый БПЛА должен иметь возможность измерять свои относительные расстояния до соседних БПЛА. Таким образом, необходимо отметить, что данный метод накладывает большое количество ограничений на область его применения. В работе [13] представлен метод противодействия атакам на GPS, основанный на использовании системы технического зрения, которая позволяет дополнительно вычислять скорость БПЛА и некоторые другие показатели и коррелировать их с данными полученными от GPS.

В таблице 1 представлена сравнительная характеристика методов противодействия атакам на GPS.

Таблица 1. Сравнение существующих методов противодействия атакам на GPS

Тип реализации метода	Тим метода	Достоинства	Недостатки
Программный	Методы на основе сравнения с эталонными значениями	Быстродействие, обнаружение простых атак	Невозможность обнаруживать сложные атаки
	Методы на основе интеллектуального анализа	Повышение качества обнаружения атак, универсальность для разных конфигураций БПЛА	Сложность реализации, энергозатратность
Программно-аппаратный	Методы на основе использования нескольких GPS-приемников	Сложнее атаковать, более высокое качество обнаружения	Сложность реализации, могут поддерживаться не всеми БПЛА. Могут использовать дополнительные ресурсы. Требуется значительная проработка решений. Возможны сложности при реализации.
	Методы на основе использования других типов датчиков	Повышается уровень и скорость обнаружения атаки	Плохо масштабируются из-за того, что конфигурация каждого БПЛА индивидуальна

В результате анализа текущего состояния исследований можно сказать, что задача детектирования и предотвращения атак на систему навигации БПЛА достаточно актуальна [13].

3. Разработка и реализация сценария атаки на БПЛА. Открытый характер структуры сигнала GPS делает его уязвимым для спуфинг атак, которые могут выполняться как открыто, так и скрытно. В первом случае сигнал атакующего транслируется значительно мощнее, чем сигнал, приходящий от спутников. Такая атака выполняется проще, но использует более мощные сигналы и легче обнаруживается [14]. При реализации подхода, когда атака проводится скрытно, мощность сигнала постепенно увеличивается до тех пор, пока целевая система полностью не переключится на транслируемый атакуемым сигнал. Этот подход является более сложным и требует большего количества компонентов и более детальной подготовки, но потребляет меньше энергии и обеспечивает плавный переход целевой

системы на другой сигнал. Данные, полученные с помощью датчиков GPS, могут быть сфальсифицированы, что приводит к ложной оценке положения БПЛА бортовой навигационной системой. Если БПЛА полностью автоматизирован, то бортовая система наведения приведет БПЛА к ложному целевому местоположению или «домашней» наземной станции.

При проведении атаки, важно учитывать ряд факторов для снижения риска обнаружения атаки. В первую очередь нужно определить точную геопозицию и время начала атаки. Если место положения атакуемого БПЛА будет выбрано недостаточно точно, система безопасности БПЛА может обнаружить атаку, и тогда аппарат может перейти на ручное управление или изменить траекторию движения, согласно предустановленному сценарию поведения [15]. Неточность определения времени также может привести к обнаружению атаки или к сбою внутренней синхронизации системы. Все эти факторы необходимо учитывать на подготовительном этапе атаки [16].

Проведение атаки возможно только в том случае, если система управления БПЛА переведена в автоматический режим, и полностью полагается на систему навигации, использующую датчики GPS/ГЛОНАСС. Для БПЛА существует два сценария использования систем навигации в автоматическом режиме: сохранение позиции с фиксированными координатами и движение по заданному маршруту.

Для получения экспериментальных данных и моделирования поведения БПЛА во время атаки и в нормальных условиях был выбран способ натурного моделирования. Для реализации натурного моделирования разработан БПЛА, который включает в себя следующие компоненты:

– полетный контроллер: Pix Hawk 4 (PX4) (прошивка Stable 10.1);

– рама: S500;

– моторы: 2XD2212 920KV по часовой стрелке против часовой стрелки CW бесщеточный двигатель;

– регуляторы оборотов: XT-XINTE 30A;

– телеметрия: 3DR радиотелеметрия 915 МГц 100 мВт воздушно-наземный модуль передачи данных для Pixhawk 4;

– приемник: FS-I6B;

– аккумулятор: ZOP Power 3S 11.1V 4200mAh 40C Lipo Battery XT60 Plug;

– камера: мини-камера: 1200TVL;

– передатчик видео: Eachine TX805 5,8G;

– навигационный модуль: Модуль Ublox Neo-M8N.

Для управления полетом БПЛА использовался планировщик QGroundControl. QGroundControl обеспечивает полный контроль полета и планирование миссий для любого БПЛА с поддержкой протокола MAVLink.

По результатам выполнения миссии формировалось два типа журналов, которые в дальнейшем анализировались.

Типы журнала: Dataflash и Telemetry. Есть два способа записи полетных данных с БПЛА:

– журнал DataFlash можно использовать на плате самого полетного контроллера или PX4, которые можно загрузить после полета;

– журнал телеметрии записывается с помощью программного обеспечения (ПО) Mission Planner (или другой наземной станцией) путем передачи данных от БПЛА по беспроводному каналу на наземную станцию.

Для проведения атаки использовался специализированный радиочастотный модуль HackRF One.

Таким образом, проходила отработка нескольких сценариев нормального полета, а затем нескольких сценариев атаки. Всего было выполнено до 20 тестовых испытаний. В результате испытаний были собраны экспериментальные данные для анализа из журналов логирования. Сценарии атаки.

Один из сценариев заключается в том, что БПЛА, определив свое текущее местоположение, получает статические координаты цели. БПЛА коптерного типа перемещается в заданную точку и фиксирует свое положение в пространстве с сохранением высоты. При внешнем воздействии, например при влиянии природных факторов или другого объекта, система автопилота БПЛА увеличивает обороты двигателей и задает направление, противоположное направлению воздействия, для сохранения заданной позиции. При смещении БПЛА от заданной позиции, система сохранения позиции увеличивает мощность оборотов двигателей в зависимости от дистанции между заданной точкой и фактическим расположением БПЛА. При возвращении в заданную точку работа двигателей переходит в штатный режим поддержания высоты, как показано на рисунке 1.

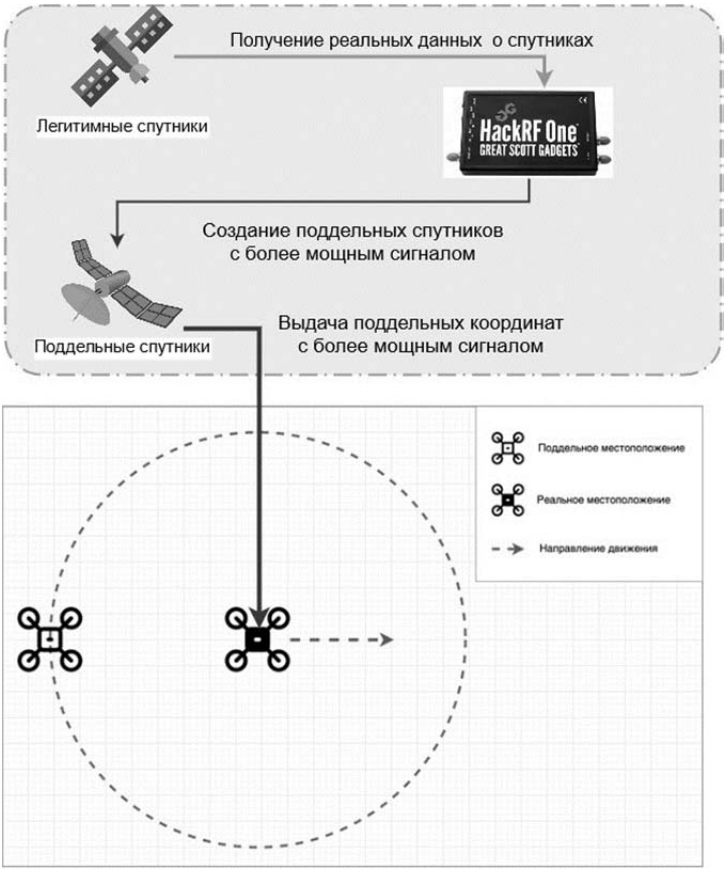


Рис. 1. Сценарий атаки на БПЛА, зависающий надо одной точкой

Из рисунка 1 видно, что когда на БПЛА проводится атака, то он начинает смещаться и изменять свое местоположение, которое было ему изначально задано. Злоумышленник с помощью специализированного оборудования, посылая сигнал большей мощности, передает БПЛА свою информацию от поддельных спутников GPS, тем самым заставляя БПЛА смещаться от заданной позиции. Данное смещение сопровождается также изменением высоты, мощности принимаемого сигнала и иногда сбоями и крушением БПЛА.

Вторым сценарием использования системы навигации в автоматическом режиме является движение по заданному маршруту. Квадрокоптер заранее получает полностью построенный маршрут, и при выполнении миссии движется согласно этой траектории. В случае отклонения от заданной траектории, как и при статической фиксации, БПЛА в автоматическом режиме предпринимает действия по возвращению на маршрут. Помимо применения этого сценария для выполнения заданной миссии или решения задач при движении по маршруту, он может использоваться для обнаружения атак на канал управления.

Транслируя поддельную геопозицию, можно задать вектор направления и скорость движения атакуемого устройства [17]. Изменяя расстояние от поддельной геопозиции до заданной, можно увеличивать или уменьшать скорость движения, для более точного направления и контроля атакуемого БПЛА, как показано на рисунке 2.

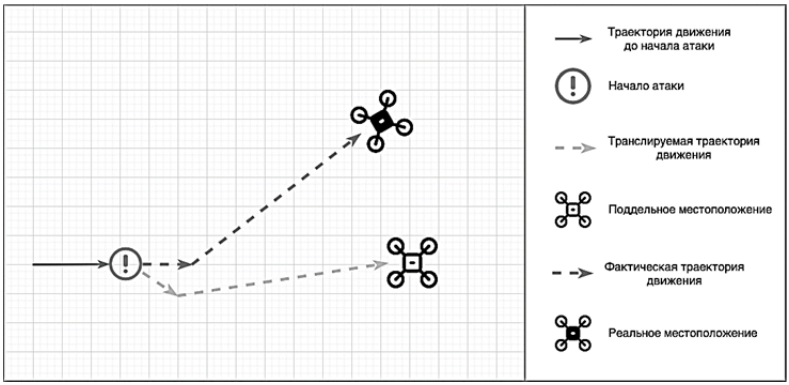


Рис. 2. Сценарий атаки на БПЛА, движущийся по заданной траектории

Рисунок 2 показывает желаемую траекторию движения БПЛА, которая отображена верхней, более темной линией, и ту траекторию, по которой будет двигаться БПЛА после проведения атаки злоумышленником (пунктирная нижняя линия). Восклицательным знаком обозначен момент начала атаки. В процессе проведения эксперимента БПЛА изменял свою траекторию движения и отклонился от той, что была задана его автопилоту.

В процессе испытаний при нормальных условиях полета оператором задавалось полетное задание для БПЛА и аппарат выполнял его на протяжении 10 минут.

В процессе испытаний атака на БПЛА осуществлялась после 3-5 минут полета и проводилась 10 минут. Во время атаки злоумышленник задавал поддельное местоположение БПЛА. В процессе экспериментов наблюдалось изменение высоты БПЛА, а также плавное смещение БПЛА в ложную точку. В ряде экспериментов, когда атака резко прерывалась, наблюдалось падение БПЛА.

4. Алгоритм обнаружения атаки на систему GPS БПЛА. Для обнаружения атаки предлагается учитывать следующие кибер-физические параметры:

– загруженность центрального процессорного устройства (ЦПУ),
– высота полета БПЛА (ha),
– состояние фиксации по спутникам (Gn),
– неопределенность GPS (Gu),
– шум GPS (Gnoi).

С учетом этих параметров алгоритм обнаружения аномалий предлагается представить в виде следующих шагов:

1. Фиксация «сырых» значений анализируемых кибер-физических параметров на протяжении определенного промежутка времени.

2. Построение подходящего типа распределения для собранных кибер-физических параметров (в данном случае распределение Пуассона).

3. С использованием скользящего окна осуществить выборку предыдущих значений и дополнить их собранными в новый момент времени, построить временной ряд значений.

4. Построение нового распределения для новых значений по тому же закону распределения.

5. Вычисление значения дивергенции Кульбака-Лейблера [18] для двух соседних функций распределения.

6. Чем выше полученное значение дивергенции Кульбака-Лейблера, тем больше вероятность, что на систему оказано влияние в виде атаки или внешнего деструктивного воздействия. Как правило такое значение должно превышать или быть равным 2 (было установлено авторами ранее экспериментальным путем) [19].

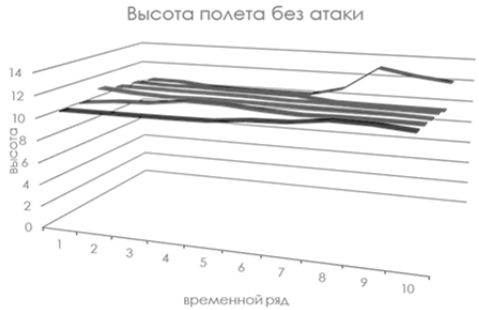
7. Повторить алгоритм для последующих новых значений кибер-физических параметров, начиная с пункта 3 (сдвиг окна).

Далее, были проведены вычисления энтропии для собранных значений кибер-физических параметров и оценка эффективности метода.

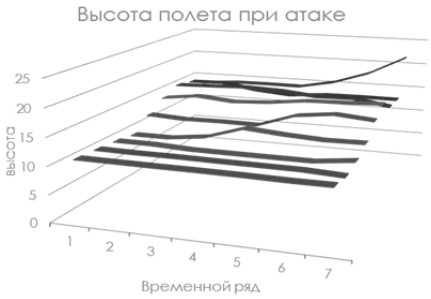
Установлено, что чем выше значение энтропии, тем больше вероятность, что изменение кибер-физического параметра говорит о наличии аномального поведения. Аномальное поведение может возникать не только из-за атаки, но также из-за воздействия со стороны окружающей среды

Так, например, скорость двигателей и высота полета могут быть не связаны с атакой, а могут изменяться из-за порывов ветра. Для однозначного определения атаки необходимо анализировать сразу несколько кибер-физических параметров и определять степень их отклонения [20].

5. Анализ результатов экспериментального исследования. Рассмотрим, как изменялась высота полета без атаки и во время атаки. На рисунке 3(а) показан результат представления сырых данных об изменении высоты полета без атаки и на рисунке 3(б) показан результат представления сырых данных об изменении высоты полета во время проведения атаки.



(а)



(б)

Рис. 3. Результат изменения высоты полета (а) без атаки (б) при атаке.

Из рисунка 3(а) видно, что несмотря на то, что атака не проводилось, небольшие изменения параметра всё же наблюдались. Такие изменения не фиксируются разработанным методом, как аномальные. Временные ряды позволяют сохранить информацию о возникшей аномалии и отражают ее на нескольких временных рядах, что возможно благодаря концепции скользящего окна. Из рисунка 3 (б) видно, что изменение вида временного ряда, наблюдаемое однажды, переносится на последующие временные ряды.

На рисунке 4 представлен результат вычисления дивергенции Кульбака-Лейблера для детектирования изменения высоты полета при атаке.

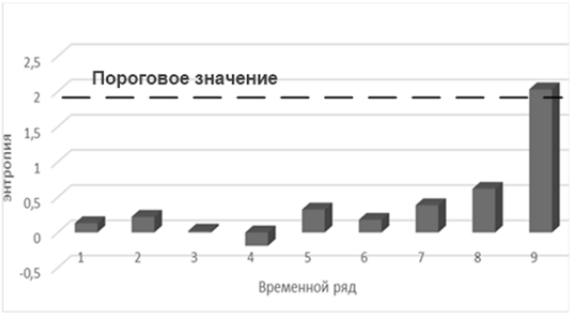
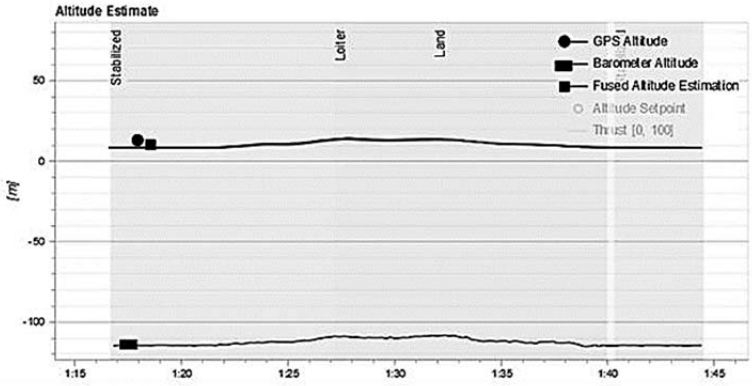


Рис. 4. Результат вычисления энтропии для высоты полета при атаке

Из рисунка 4 видим, что наблюдается превышение показателя дивергенции Кульбака-Лейблера в последнем временном ряду. Так как атака на БПЛА начиналась с задержкой, то первые несколько значений являются достаточно низкими, затем наблюдается скачок на последних трех значениях. Это связано в первую очередь с тем, что БПЛА в результате атаки могу потерпеть крушение. В результате атаки БПЛА начал резко снижаться, но благодаря вмешательству оператора крушение было предотвращено. Напомним, что снижение высоты полета лишь косвенно может подтвердить атаку.

Из графиков на рисунке 5 видно, что данные, полученные из лог-файлов результатов испытаний БПЛА во время нормального полета и атаки, показывают наличие аномалии. На рисунке 5(а) показания инерциальной системы и GPS для измерения высоты полета совпадают, отличаются только показания барометра (самая нижняя линия на графике). Показания барометра во всех экспериментах отличаются от показаний акселерометра и системы навигации GPS. Это связано с неполадкой оборудования, поэтому в данном исследовании они не рассматриваются. Существенные изменения

высоты полета наблюдались в конце реализации сценария, что видно из графика 5(б). При нормальном поведении также наблюдалось небольшое изменение высоты. Отличие составляет также то, что при нормальном полете высота по показаниям инерциальной системы навигации и системы GPS изменялась одинаково. При атаке результат вычисления высоты полета, полученный от инерциальной системы и системы GPS, отличается, как видно из рисунка 5(б). Верхняя линия обозначает значение высоты полета, полученное от системы GPS, средняя линия - от акселерометра, а нижняя линия - от барометра. Барометр дает погрешность и при нормальном полете, а GPS и акселерометр должны совпадать в своих показаниях, как на рисунке 5(а).



(а)

(б)

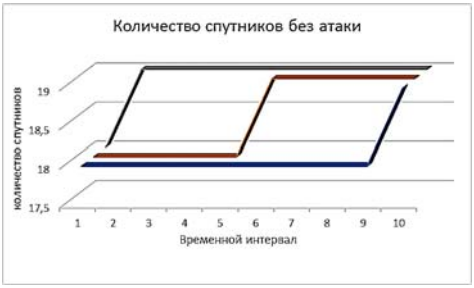
Рис.5. График высоты БПЛА (а) при нормальном полете (б) при атаке

Из рисунка 5 (б) видно, что изменение высоты полета наблюдалось дважды - ближе к началу (обозначено на рисунке, как обнаруженная аномалия) и в конце графика. В целом график выглядит менее гладким, чем рисунок 5 (а), где представлен график изменения высоты для нормального полета.

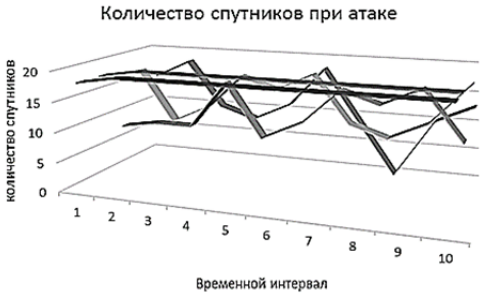
Проведённые эксперименты показывают, что аномалия, возникающая при атаке на подсистему GPS-навигации, успешно обнаруживается с помощью представленного метода.

Рассмотрим изменение другого кибер-физического параметра - количество спутников GPS. На рисунке 6(а) показан результат представления данных о количестве спутников без атаки и на рисунке 6(б) - при атаке.

Из рисунков видно, что изменения наблюдаются для обоих случаев, но для случая атаки колебания сильнее. Из рисунка 6(а) видно, как однажды возникшая аномалия переносится на все остальные временные ряды. Тем не менее, единичное повышение значения является случайным и незначительным, так как не влияет на процесс полета БПЛА. Как видно из рисунка 6(б), наблюдаются значительные изменения временных рядов.



(а)



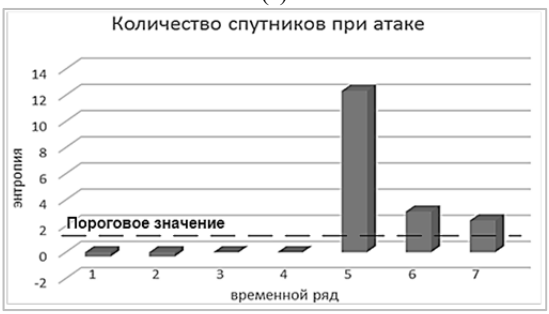
(б)

Рис. 6. Результат изменения количества спутников (а) без атаки, (б) при атаке

Теперь рассмотрим значение энтропии, которые получилось в результате вычисления дивергенции Кульбака-Лейблера для данного параметра.

На рисунке 7(а) представлен результат вычисления дивергенции без атаки, а на рисунке 7(б) - при атаке. Из рисунка 7 видно, что на пятом интервале обнаруживается резкое превышение исходного уровня. В общем случае это не означает, что число спутников увеличилось (оно могло и уменьшиться), главное, что вид распределения между 3 и 4 интервалами не совпадает, а значит произошли существенные изменения. В случае с количеством спутников, их число должно быть примерно одинаковым. Таким образом, становится важно фиксировать именно резкие изменения, а не пороговые значения, так как злоумышленник может действовать по-разному. Он может создавать больше логичных спутников, если располагает достаточными мощностями, а может, наоборот, делать меньшее количество этих спутников, чем первоначально зафиксировал БПЛА.

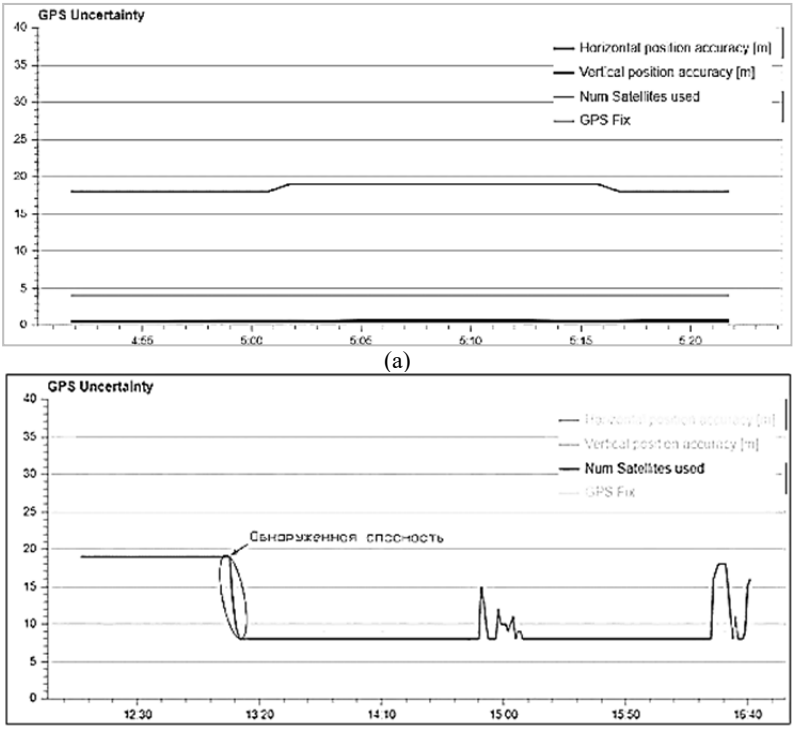
(а)



(б)

Рис. 7 – Результат вычисления энтропии для количества спутников (а) без атаки (б) при атаке

Для подтверждения эффективности методики рассмотрим результаты анализа лог-файлов, «сырых» данных, полученных в необработанном виде от БПЛА. Из рисунка 8(а) видно, что при нормальном полете число спутников менялось, но эти изменения были плавными и незначительными. При атаке изменение было резким, и при дальнейшем полете возникали колебания (рисунок 8(б)). Данные колебания могут быть связаны с отдалением или приближением БПЛА к устройству помех злоумышленника. Тем не менее, важно отметить, что метод позволяет зафиксировать аномалию. Эффективность работы метода основана на возможности оценки характера изменений кибер-физического параметра, при которой нет необходимости обладать информацией о нормальных значениях.

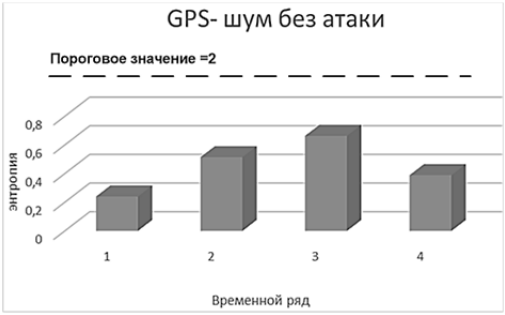


(а)

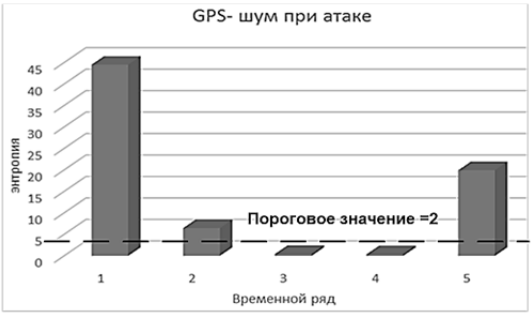
(б)

Рис.8. Количество используемых GPS спутников (а) при нормальном полете (б) при атаке на GPS систему БПЛА

Сравним результаты поиска аномалий при анализе уровня шума во время атаки и без нее, как показано на рисунке 9.



(а)



(б)

Рис. 9. Оценка энтропии кибер-физического параметра уровень шума GPS (а) в нормальных условиях (б) при атаке

Как видно из рисунка 9 (б), аномальное поведение обнаруживается с первого же значения рассчитанной дивергенции. Это связано с тем, что значение количества спутников изменилось достаточно резко и достаточно быстро, как видно на рисунке 8 (б). Таким образом обнаружение аномалии происходит после сравнения первых двух временных рядов. Ближе к концу опять наблюдаются скачки значений числа спутников и тем самым происходит повторное обнаружение аномалии во втором временном ряду и в пятом, что коррелирует с рисунком 8 (б).

6. Заключение. Несмотря на то, что опубликовано достаточно большое число работ с результатами исследований методов противодействия атакам спуфинга навигационной системы БПЛА, эта тема все еще актуальна [21-23]. На сегодняшний день

продемонстрирован ряд успешных атак на систему навигации БПЛА. Описанный в данной статье метод имеет ряд преимуществ по сравнению с известными подходами.

Метод может применяться для любых подсистем БПЛА, с которых можно снимать числовые показания. Главной задачей становится определение правильного типа распределения вероятностей для анализируемых параметров.

Метод вычислительно «легкий» и энергоэффективный. Программная реализация метода слабо влияет на загрузку процессора и энергопотребление БПЛА.

Поскольку метод позволяет анализировать любые параметры и может работать с любыми доступными данными, то не имеет значения, какими датчиками оснащен БПЛА.

С помощью разработанного метода можно не только обнаруживать аномалии, но и определять изменение закономерностей поведения БПЛА, изменение его состояний. Если значения определяемой энтропии не слишком высоки, и имеет место однократное увеличение, то это может указывать на изменение режима полета. Соотношение анализируемых параметров позволяет однозначно выявить атаку и определить ее тип. Каждая атака затрагивает определенный набор подсистем, поэтому тип атаки можно охарактеризовать по результирующим параметрам, на которые она влияет. Данные, собранные в виде временных рядов, могут быть использованы для обучения нейронных сетей принимать решения о проведении атаки. Метод может использоваться для анализа других наборов параметров и применяться не только к БПЛА, но и к любой киберфизической системе.

Дальнейшие исследования планируются в направлении разработки средств автоматизации и управления сценариями атак на БПЛА для упрощения и ускорения проведения экспериментов. Предусматривается продолжение работ по анализу влияния различных типов атак на киберфизические параметры БПЛА.

Литература

1. Semanjski S., Semanjski I., Wilde W.D., Gautama S. Use of supervised machine learning for GNSS signal spoofing detection with validation on real-world meaconing and spoofing data—Part II. Sensors. 2020. № 20(7):1806. pp. 1-15.
2. Kwon K.-C., Shim D.-S. Performance analysis of direct GPS spoofing detection method with HRS/Accelerometer. Sensors. 2020. № 20(4): 954.
3. Wan W., Kim H., Hovakimyan N., Sha L., Voulgaris P.G. A Safety Constrained Control Framework for UAVs in GPS Denied Environment. 59-th IEEE Conference on Decision and Control (CDC). Korea (South). 2020. pp. 214-219.

4. Seo S.-H., Lee B.-H., Im S.-H., Jee G. Effect of spoofing on unmanned aerial vehicle using counterfeited GPS signal. Journal of Positioning Navigation and Timing. 2015. № 6. pp. 57-65.
5. Shepard D., Humphreys T., Fansler A. Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks. International Journal of Critical Infrastructure Protection. 2012. № 5(3-4). pp. 146-153.
6. Jansen K., Schäfer M., Moser D., Lenders V., Pöpper C., Schmitt J. Crowd-GPS-sec: Leveraging crowdsourcing to detect and localize GPS spoofing attacks. Proc. IEEE Symp. Security Privacy (SP). San Francisco. CA. USA: IEEE. 2018. pp. 1018-1031.
7. Montgomery P.Y., Humphreys T.E., Ledvina B.M. Receiver-autonomous spoofing detection: Experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer. Proceedings of the 2009 International Technical Meeting of The Institute of Navigation. Anaheim. CA. 2009. pp. 124-130.
8. Jansen K., Tippenhauer O., Pöpper C. Multi-receiver GPS spoofing detection: Error models and realization. Proceedings of the 32nd Annual Conference on Computer Security Application. New York, United States: Association for Computing Machinery. 2016. pp. 237-250.
9. Heng L., Work D.B., Gao G.X. GPS signal authentication from cooperative peers. IEEE Trans. Intell. Transp. Syst. 2015. vol. 16. № 4. pp. 1794-1805.
10. G. Panice et al. A SVM-based detection approach for GPS spoofing attacks to UAV. 23-rd International Conference on Automation and Computing (ICAC). Hudders-field. 2017. pp. 1-11.
11. Eldosouky A., Ferdowsi A., Saad W. Drones in Distress: A Game-Theoretic Countermeasure for Protecting UAVs Against GPS Spoofing. IEEE Internet of Things Journal. 2020. vol. 7. № 4. pp. 2840-2854.
12. Qiao Y., Zhang Y., Du X. A Vision-Based GPS-Spoofing Detection Method for Small UAVs. 13-th International Conference on Computational Intelligence and Security (CIS). Hong Kong. 2017. pp. 312-316.
13. Choudhary G., Sharma V., You I., Yim K., Chen I.-R., Cho J.-H. Intrusion Detection Systems for Networked Unmanned Aerial Vehicles: A Survey. 14-th IEEE International Wireless Communications & Mobile Computing Conference. Limassol. Cyprus. 2018. pp. 560-565.
14. Bekmezci I., Senturk E., Turker T. Security issues in Flying Adhoc Networks (FANETs). Journal of Aeronautics and Space Technologies. 2016. vol. 9. № 2. pp. 13-21.
15. Li C., Wang X. Jamming research of the UAV GPS/INS integrated navigation sys-tem based on trajectory cheating. 9-th International Congress on Image and Signal Processing, BioMedical Engineering, and Informatics (CISP-BMEI). 2016. Datong. pp. 1113-1117.
16. Schmidt D., Radke K., Camtepe S., Foo E., Ren M. A survey and analysis of the GNSS spoofing threat and countermeasures. ACM Comput. Surveys (CSUR). 2016. vol. 48. № 4. pp. 64-69.
17. Joshi D. Commercial Unmanned Aerial Vehicle (UAV) Market Analysis – Industry Trends Companies and What You Should Know. Business Insider. 2017.
18. Afgani M., Sinanovic S., Haas H. Anomaly detection using the Kullback-Leibler divergence metric. First International Symposium on Applied Sciences on Biomedical and Communication Technologies. 2008. Aalborg. pp. 1-5.
19. Basan, E., Basan, A., Nekrasov, A., .Gamec, J., Gamcová, M. A self-diagnosis method for detecting UAV cyber attacks based on analysis of parameter changes. Switzerland. 2021. № 21(2). pp. 1–17.
20. E. Basan, A. Basan, A. Nekrasov. Method for detecting abnormal activity in a group of mobile robots. Sensors. 2019. Vol. 19. № 18:4007. pp. 1-21.

21. В.Н. Максименко, Д.А. Ухин. [Анализ уязвимостей каналов связи спутниковых навигационных систем LBS-услуги]. Экономика и качество систем связи. 2019. №1. С. 18–22. http://nirit.org/wp-content/uploads/2019/06/18-22.pdf
22. L.A. Dobryakova, Ł.S. Lemieszewski., E.F. Ochin. [Атаки на глобальные навигационные спутниковые системы и обнаружение спуфинга беспилотных кораблей, базирующееся на облачных технологиях]. Ural radio engineering journal. 2018. Vol.2 № 2. DOI: https://doi.org/10.15826/urej.2018.2.2.003
23. Котенко И. В., Саенко И. Б. Архитектура системы интеллектуальных сервисов защиты информации в критически важных инфраструктурах // Труды СПИИРАН. 2013. № 1 (24). С. 21–40.

Басан Елена Сергеевна — канд. техн. наук, доцент, кафедра безопасности информационных технологий, Южный федеральный университет. Область научных интересов: разработка и исследование технологий обнаружения атак и вторжений, обнаружение аномального поведения, безопасность робототехнических систем, анализ угроз и уязвимостей. Число научных публикаций — 55. ebasan@sfedu.ru; Чехова, 2, 347922, Таганрог, Россия; р.т.: +7(951)520-54-88.

Абрамов Евгений Сергеевич — канд. техн. наук, доцент, заведующий кафедрой, кафедра безопасности информационных технологий, Южный федеральный университет. Область научных интересов: технологии обнаружения сетевых атак, модели атак, технологии threat intelligence, применение методов искусственного интеллекта в информационной безопасности. Число научных публикаций — 80. abramoves@sfedu.ru; Чехова, 2, 347922, Таганрог, Россия; р.т.: +7(863)37-19-05.

Басюк Анатолий Геннадьевич — аспирант, кафедра безопасности информационных технологий, Южный федеральный университет. Область научных интересов: анализ угроз и уязвимостей программного обеспечения, разработка кибербезопасности БПЛА. Число научных публикаций — 3. basyuk@sfedu.ru; Чехова, 2, 347922, Таганрог, Россия; р.т.: +7(863)37-19-05.

Сушкин Никита Андреевич — аспирант, кафедра безопасности информационных технологий, Южный федеральный университет. Область научных интересов: разработка и исследование сценариев атак на БПЛА, разработка систем кибербезопасности БПЛА. Число научных публикаций — 2. sushkin@sfedu.ru; Чехова, 2, 347922, Таганрог, Россия; р.т.: +7(863)37-19-05.

DOI 10.15622/ia.20.6.7

E. BASAN, E. ABRAMOV, A. BASYUK, N. SUSHKIN

SPOOFING ATTACK DETECTION METHOD FOR UAV NAVIGATION SYSTEM

Basan E., Abramov E., Basyuk A., Sushkin N. **Spoofing Attack Detection Method for UAV Navigation System.**

Abstract. An implementation of methods for protecting unmanned aerial vehicles (UAVs) from spoofing attacks of the global positioning system (GPS) to ensure safe navigation is discussed in this paper. The Global Navigation Satellite System (GNSS) is widely used to locate UAVs and is by far the most popular navigation solution. This is due to the simplicity and relatively low cost of this technology, as well as the accuracy of the transmitted coordinates. However, there are many security threats to GPS navigation. Primarily this is due to the nature of the GPS signal, the signal is transmitted in the clear, so an attacker can block or tamper with it. This study analyzes the existing GPS protection methods. As part of the study, an experimental stand and scenarios of attacks on the UAV GPS system were developed. Data from the UAV flight logbook was collected and an analysis of cyber-physical parameters was carried out to see an effect of the attack on the on-board sensors readings. Based on this, a new method for detecting UAV anomalies was proposed, based on an analysis of changes in UAV internal parameters. This self-diagnosis method allows the UAV to independently assess the presence of changes in its subsystems and identify signs of a cyberattack. To detect an attack, the UAV collects data on changes in cyber-physical parameters over a certain period of time, then updates this data. As a result it is necessary for the UAV to determine the degree of difference between the two time series of the collected data. The greater the degree of difference between the updated data and the previous ones, the more likely the UAV is under attack.

Keywords: security, attack, navigation system, UAV, threat, probability, protection technology, global navigation satellite system.

Basan Elena — Ph.D., Associate Professor, Department of secure information technologies, Southern Federal University. Research interests: development and research of attack and intrusion detection technologies, detection of abnormal behavior, security of robotic systems, threat and vulnerability analysis. The number of publications — 55. ebasan@sfedu.ru; 2, Chekhova, 347922, Taganrog, Russia; office phone: +7(951)520-54-88.

Abramov Eugene — Ph.D., Associate Professor, Head of the department, Department of Secure Information Technologies, Southern Federal University. Research interests: technology for the detection of network attacks, attack models, threat intelligence technology, the use of artificial intelligence methods in information security. The number of publications — 80. abramoves@sfedu.ru; 2, Chekhova, 347922, Taganrog, Russia; office phone: +7(863)37-19-05.

Basyuk Anatoly — Postgraduate student, Department of Secure Information Technologies, Southern Federal University. Research interests: analysis of threats and vulnerabilities of software, development of UAV cybersecurity models. The number of publications — 3. basyuk@sfedu.ru; 2, Chekhova, 347922, Taganrog, Russia; office phone: +7(863)37-19-05.

Sushkin Nikita — Postgraduate student, Department of Secure Information Technologies, Southern Federal University. Research interests: development and research of UAV attack

scenarios, development of UAV cybersecurity systems. The number of publications — 2. sushkin@sfedu.ru; 2, Chekhova, 347922, Taganrog, Russia; office phone: +7(863)37-19-05.

References

1. Semanjski S., Semanjski I., Wilde W.D., Gautama S. Use of supervised machine learning for GNSS signal spoofing detection with validation on real-world meaconing and spoofing data—Part II. Sensors. 2020. № 20(7):1806. pp. 1-15.
2. Kwon K.-C., Shim D.-S. Performance analysis of direct GPS spoofing detection method with AHRS/Accelerometer. Sensors. 2020. № 20(4):954.
3. Wan W., Kim H., Hovakimyan N., Sha L., Voulgaris P.G. A Safety Constrained Control Framework for UAVs in GPS Denied Environment. 59-th IEEE Conference on Decision and Control (CDC). Korea (South). 2020. pp. 214-219.
4. Seo S.-H., Lee B.-H., Im S.-H., Jee G. Effect of spoofing on unmanned aerial vehicle using counterfeited GPS signal. Journal of Positioning Navigation and Timing. 2015. № 6. pp. 57-65.
5. Shepard D., Humphreys T., Fansler A. Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks. International Journal of Critical Infrastructure Protection. 2012. № 5(3-4). pp. 146-153
6. Jansen K., Schäfer M., Moser D., Lenders V., Pöpper C., Schmitt J. Crowd-GPS-sec: Leveraging crowdsourcing to detect and localize GPS spoofing attacks. Proc. IEEE Symp. Security Privacy (SP). San Francisco. CA. USA: IEEE. 2018. pp. 1018-1031.
7. Montgomery P.Y., Humphreys T.E., Ledvina B.M. Receiver-autonomous spoofing detection: Experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer. Proceedings of the 2009 International Technical Meeting of The Institute of Navigation. Anaheim. CA. 2009. pp. 124-130.
8. Jansen K., Tippenhauer O., Pöpper C. Multi-receiver GPS spoofing detection: Error models and realization. Proceedings of the 32nd Annual Conference on Computer Security Application. New York, United States: Association for Computing Machinery. 2016. pp. 237-250.
9. Heng L., Work D.B., Gao G.X. GPS signal authentication from cooperative peers. IEEE Trans. Intell. Transp. Syst. 2015. vol. 16. № 4. pp. 1794-1805.
10. G. Panice et al. A SVM-based detection approach for GPS spoofing attacks to UAV. 23-rd International Conference on Automation and Computing (ICAC). Hudders-field. 2017. pp. 1-11.
11. Eldosouky A., Ferdowsi A., Saad W. Drones in Distress: A Game-Theoretic Countermeasure for Protecting UAVs Against GPS Spoofing. IEEE Internet of Things Journal. 2020. vol. 7. № 4. pp. 2840-2854.
12. Qiao Y., Zhang Y., Du X. A Vision-Based GPS-Spoofing Detection Method for Small UAVs. 13-th International Conference on Computational Intelligence and Security (CIS). Hong Kong. 2017. pp. 312-316.
13. Choudhary G., Sharma V., You I., Yim K., Chen I.-R., Cho J.-H. Intrusion Detection Systems for Networked Unmanned Aerial Vehicles: A Survey. 14-th IEEE International Wireless Communications & Mobile Computing Conference. Limassol. Cyprus. 2018. pp. 560-565.
14. Bekmezci I., Senturk E., Turker T. Security issues in Flying Adhoc Networks (FANETs). Journal of Aeronautics and Space Technologies. 2016. vol. 9. № 2. pp. 13-21.
15. Li C., Wang X. Jamming research of the UAV GPS/INS integrated navigation sys-tem based on trajectory cheating. 9-th International Congress on Image and Signal Processing, BioMedical Engineering, and Informatics (CISP-BMEI). 2016. Datong. pp. 1113-1117.

16. Schmidt D., Radke K., Camtepe S., Foo E., Ren M. A survey and analysis of the GNSS spoofing threat and countermeasures. ACM Comput. Surveys (CSUR). 2016. vol. 48. № 4. pp. 64-69.
17. Joshi D. Commercial Unmanned Aerial Vehicle (UAV) Market Analysis – Industry Trends Companies and What You Should Know. Business Insider. 2017.
18. Afgani M., Sinanovic S., Haas H. Anomaly detection using the Kullback-Leibler divergence metric. First International Symposium on Applied Sciences on Biomedical and Communication Technologies. 2008. Aalborg. pp. 1-5.
19. Basan, E., Basan, A., Nekrasov, A., .Gamec, J., Gamcová, M. A self-diagnosis method for detecting UAV cyber attacks based on analysis of parameter changes. Switzerland. 2021. № 21(2). pp. 1–17.
20. E. Basan, A. Basan, A. Nekrasov. Method for detecting abnormal activity in a group of mobile robots. Sensors. 2019. Vol. 19. № 18:4007. pp. 1-21.
21. V.N. Maksimenko, D.A. Uhin. [Analiz uyazvimostej kanalov svyazi sputnikovyh navigacionnyh sistem LBS-uslugi]. Ekonomika i kachestvo sistem svyazi. 2019. №1. S. 18–22. http://nirit.org/wp-content/uploads/2019/06/18-22.pdf
22. L.A. Dobryakova, L.S. Lemieszewski., E.F. Ochin. [Ataki na global'nye navigacionnye sputnikovye sistemy i obnaruzhenie spufinga bespilotnyh korablej, baziruyushcheesya na oblachnyh tekhnologiyah]. Ural radio engineering journal. 2018. Vol.2 № 2. DOI: https://doi.org/10.15826/urej.2018.2.2.003
23. Kotenko I. V., Saenko I. B. Arhitektura sistemy intellektual'nyh servisov zashchity informacii v kriticheski vazhnyh infrastrukturah // Trudy SPIIRAN. 2013. № 1 (24). S. 21–40.