УДК *004.031.4* ***DOI:*** *10.26731/1813-9108.2019.2(62).186–195*

И. А. Сорокин [1]***, А. Д. Обухов*** [2]***, П. Н. Романов*** [1]***, М. Ю. Шибаева*** [1]

[1] *Нижегородский государственный инженерно-экономический университет, г. Княгинино, Российская Федерация*
[2] *Петербургский государственный университет путей сообщения Императора Александра I, г. Санкт-Петербург, Российская Федерация*
Дата поступления: *15 марта 2019 г.*

ПРИМЕНЕНИЕ МЕТОДА ПЕРЕСТАНОВОЧНОГО ДЕКОДИРОВАНИЯ В СИСТЕМЕ УПРАВЛЕНИЯ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ МАЛОГО КЛАССА (ДРОНЫ, МУЛЬТИКОПТЕРЫ)

Аннотация. *В данной работе проведен анализ теории управления беспилотными летательными аппаратами. Обнаружено, что средства перестановочного декодирования позволяют на коротком отрезке времени выполнять маскировку реальной структуры сигнала. Незаконное использование и перехват являются обычной практикой, и это может непосредственно повлиять на безопасность сложных машин. Незаконный перехват, сетевое проникновение, атаки вредоносных программ для хищения данных по специальным проектам, а также технологии дронов относятся к наиболее желанным целям. В данной статье исследована способность атакующего, передающего фальсифицированные сигналы GPS, которые влияют на поведение автономного беспилотного летательного аппарата. Требования к открытому и скрытому захвату навигационной системы таких аппаратов были представлены вместе с результатами живых испытаний поддельных атак против нескольких коммерческих GPS-приемников. При анализе связанной динамики беспилотных летательных аппаратов и спуфинга было показано, что атака спуфинга GPS может заставить летательный аппарат неосознанно следовать траектории, наложенной спусковым механизмом. Верхний предел величины траектории опорного ускорения БЛА приводит к конструкции аппарата «Spoofer». Испытания скрытности на основе инноваций testing. Finally, полевые испытания показали, что разрушительное GPS-спуфинг нападение на винтокрылой БЛА является как технически и оперативно осуществимым.*

Ключевые слова: *безопасность, беспилотные летательные аппараты, канал связи, метод маскировки, недвоичные коды, перестановочное декодирование, спуфинг, GPS.*

I. A. Sorokin [1]***, A. D. Obukhov*** [2]***, P. N. Romanov*** [1]***, M. Yu. Shibaeva*** [1]

[1] *Nizhny Novgorod State University of Engineering and Economics, Knyaginino, Russian Federation*
[2] *St. Petersburg State University of Transport of Emperor Alexander I, St. Petersburg, Russian Federation*
Received: *March 15, 2019*

APPLICATION OF A PERMUTATION DECODING METHOD IN A SMALL-CLASS UNMANNED AERIAL VEHICLE CONTROL SYSTEM (DRONES, MULTICOPTERS)

Abstract. *This paper analyzes the theory of control of unmanned aerial vehicles. Permutation decoding tools have been found to allow masking of the actual signal structure for a short period of time. Cyber espionage and data leakage are common practices, and this can immediately influence the security of these complex machines. Cyber-attacks, network vulnerability, malware attacks to steal data from special projects, as well as unmanned aircraft technology are among the most desirable targets. This article will examine the ability of an attacker transmitting falsified GPS signals that affect the behavior of an autonomous UAV. The requirements for an open and hidden capture of the UAV navigation system were presented along with the results of live tests of fake attacks against several commercial GPS receivers. When analyzing the related dynamics of the UAV and spoofing, it was shown that the GPS spoofing attack can force the UAV to unconsciously follow the trajectory imposed by the trigger mechanism. The strict upper limit of the UAV reference acceleration trajectory was shown to lead to the construction of the Spoofer example of stealth testing based on innovation. Finally, field testing showed that a destructive GPS spoofing attack on a rotary-wing UAV is both technically and efficiently feasible. The demonstration is a proof of the concept of a simple special case in a wide class of GPS spoofing attacks on mobile targets.*

Keywords: *security, unmanned aerial vehicles, communication channel, masking method, system, non-binary codes, commutation decoding, spoofing, GPS.*

Введение

Беспилотный летательный аппарат (БПЛА) – это воздушное оборудование без экипажа на борту, действенное и безопасное оружие. Они могут закрадываться на границу врагов, оставаясь необнаруженными, для проведения шпионской миссии по сбору информации. Дроны также применяют для проверки неисследуемой местности, как следствие, их можно применять для атак в качестве навигационных устройств высокой точности, за счет использования квадракоптеров высокой точности наведения, что приводит к минимальным ненужным дополнительным разрушениям.

Такие летательные аппараты считаются новейшими разработками в области безопасности. На квадрокоптерах применяются самые прогрессивные технологии, которые постоянно совершенствуются для получения высокой результативности, автоматизации, хорошей универсальности, что приводит их к лучшему варианту для большинства областей использования. Они являются сложным оборудованием и теоретически могут быть перехвачены злоумышленниками, вследствие чего могут послужить оружием [1].

В настоящее время в различных прикладных областях находит широкое применение использования беспилотных летательных аппаратов. Использование подобных средств экономически оправдано при мониторинге различных объектов (сельхозугодий, лесных массивов, в системе силовых структур и т. п.). В «РЖД» планируют оснастить ремонтно-восстановительные поезда авиационными беспилотниками. Основные требования железнодорожников к беспилотникам: разведка местности и передача визуальной информации в условиях экстремальных температур, высокой скорости ветра, ограниченности связи, удаленности от населенных пунктов. В любом случае, такие аппараты управляются с некоторого удаленного пульта управления – это дает возможность перехватить управление, которое осуществляется по радиоканалу и вынудить беспилотный летательный аппарат выполнять искаженную задачу или даже овладеть нелегитивно. Главной проблемой в использовании квадрокоптеров служит защита данных от перехвата [1]. Возникает задача противостояния подобным действиям.

На сегодняшний день на рынках не рассматриваются уникальные навигационные системы для БПЛА, удовлетворяющим всем запросам безопасности передвижения в воздушном пространстве. Варианты снижения стоимости, размерных параметров и энергетических качеств БПЛА приводят к минимизации помехозащищенности каналов связи.

Защищенность каналов связи является основной проблемой на сегодняшний момент. Мы все больше получаем из средств массовой информации новости о кибер-атаках – если это не преступники, совершающие противоправные действия с пользовательскими персональными данными, то это неизвестные хакеры, вскрывающие серверы «Uber». В средствах массовой информации часто всплывают статьи о кибер-войнах. В ближайшее время с переходом на автономные системы обстановка может резко измениться. Дроны будут являться одним из основных видов оружия в руках преступников.

Данная технология, использованная в боевых действиях, дают возможность создания сверхдержав. Основным показателем является «киберспособность» и «кибер-защищенность». Сверхдержавы с лучшими специалистами в области программирования получат больше возможности кибернетического производства.

Нехорошо исполненные автономные системы играют важную роль угрозы безопасности каждой страны. В отличие от управляемых БПЛА в цикле нет ведомого и ведущего, так есть возможность перехвата и перепрофилирования данных систем для выполнения задач вслепую, таких как слежение или активные действия, целенаправленная атака. Например, если преступникам потребовалось похитить проект военного самолета и собрать его, им бы понадобилось выкрасть много бумажных чертежей, затратить определенное количество времени на перепрофилирование заводских систем и годы на создание своих аналоговых устройств. Испытание заняли бы очень много времени. Автономные устройства самолетов содержатся как чертежи CAD, которые можно использовать при производстве. Сейчас существует возможность вскрыть чертежи CAD и похитить алгоритм полета, затратив на все про все вместо нескольких лет несколько недель.

Кибер-шпионаж и потеря данных представляют собой обычную практику, и это может повлиять на информационную безопасность этих сложных машин. Кибер-войны, сетевая уязвимость, штурм вредоносных программ для осуществления перехвата данных по специализированным проектам, а также технологии дрона являются к наиболее важным целям.

С точки зрения GPS-спуфинг является отправкой на систему контроля БПЛА фальшивых географических координат, это позволяет обойти бортовую систему и заменить изначальные команды устройства для дальнейшего отклонения от курса.

Похожая атака возможна за счет утечки употребления зашифрованного сигнала GPS, что приводит к перехвату на гражданской авиации.

Коптер направлен в определенное через его GPS, а спуфер имеет возможность принудить БПЛА «думать», что он располагается в другом месте и направить его на столкновение с какой-либо конкретной целью.

Система глобального позиционирования «Спуферы» представляют собой механизмы, которые образовывают неверные сигналы GPS, обходя тем самым приемники, вынуждая их «думать», что они находятся в другой местности или в другое

время. Такая картина атаки может употребляться в массе подобных случаев.

В случае налета жертва употребляет систему глобального позиционирования на основе локализации и синхронизируется со спутниками. Преступник приступает отправлять свои подражающие и глушащие сигналы, принуждающие жертву синхронизироваться с новейшими, ошибочными сигналами. Правонарушитель может задержать сигналы, а также отправить их раньше времени [1], вследствие отсутствия устройств аутентификации он может поменять содержание получаемых сигналов GPS или в любом порядке генерировать подражающие сигналы с применением параметров публичных GPS.

Преступнику нельзя генерировать функционирующие сигналы GPS, однако он может получить их и отдавать существующие сигналы.

Автономные БПЛА особенно уязвимы. Беспилотники применяют каналы передачи данных для работы и их наземные станции управления часто напрямую подсоединены к интернету. Большое количество коммерческих дронов будут функционировать с системой «UTM», представляя еще один вектор атаки для автономной войны.

Помимо этого, в случае применения дрона в качестве роботизированного средства, в центре внимания остается допустимое отсутствие проверки со стороны человека над немаловажными функциями, что разрешит автономным системам принимать решения без участия человека.

На сегодняшний момент в связи с обеспечением безопасности каналов связи используются недостаточные усилия.

Острая проблема обеспечения защищенности каналов связи от препятствий может быть разрешена путем создания алгоритмов комплексной обработки информации, что разрешает оценить погрешности каждой из подсистем и алгоритмы выявления и исключения отказов различного вида [1].

Устройства спуфинга и антиспуфинга подвергаются рассмотрению в современных приложениях GPS как самые важные аспекты.

Критерии предохранения, установленные в программном обеспечении (ПО) на GPS приемниках, могут быть систематизированы по следующим категориям:

– амплитудное несоответствие;

– несоответствие времени прихода сигнала.

Самые современные методы:

– перекрестная проверка содержания инерциального измерительного устройства (IMU);

– поляризационная проверка;

– проверка угла прихода сигнала;

– криптографическая аутентификация.

Рассмотренные возможные виды захватов и энергичная деятельность иностранных государств и кибер-террористов должны поднять направленность поставщиков БПЛА на то, чтобы обезопасить пользователей беспилотников. В недалекие годы число БПЛА будет до такой степени высоким, что безопасность должна быть главным требованием, нужен ввод многоуровневой защиты для предотвращения инцидентов, вызванных различными кибер-атаками [1].

Материалы и методы

Летательные аппараты классифицируют на военные и гражданские. Так как наиболее известным является деление, в которые дроны подразделяются по сферам их применения, а конкретнее, для исследовательских и прикладных целей делится, а также для гражданского и военного применения (рис. 1).

В сфере научной деятельности беспилотные летательные средства применяются для получения принципиально новых знаний, при этом, неважно, в какой области эти знания будут использованы. Это возможно исследование современной техники или для изучения природных явлений [2].

Рис. 1. Область применения дронов

Прикладная сфера использования беспилотников делится на два направления – военное и гражданское.

Военные беспилотники классифицируются по функциональном признакам:

– наблюдательные (могут использоваться, в частности, для корректировки огня на поле боя);

– разведывательные;

– ударные (для ударов по наземным целям посредством ракетного вооружения);

– разведывательно-ударные;

– бомбардировочные;

– истребительные (для уничтожения воздушных целей);

– радиотрансляционные;

– БПЛА РЭБ (для целей радиоэлектронной борьбы);

– транспортные;

– БПЛА-мишени;

– БПЛА-имитаторы цели;
– многоцелевые БПЛА.

В гражданской сфере область использования беспилотников очень велика. Направления и разновидности услуг при помощи беспилотников разнообразна. Например, сельское хозяйство, строительство, сектор безопасности, а также область научно-исследовательских организаций и многое другое.

Для того чтобы обезопасить полеты БСС от несанкционированного перехвата за счет открытого канала связи беспилотника с пульта управления нами будет рассматриваться применение метода перестановочного декодирования в канале связи [2, 3].

Заявленное устройство расширяет арсенал мягкого декодирования двоичных избыточных блоковых кодов за счет исправления доли стираний, кратность которых выходит за пределы минимального кодового расстояния. Для этого используются известные свойства эквивалентных кодов. Для двоичных кодов реализация подобных свойств может иметь как положительный, так и отрицательный исход, который зависит от конфигурации конкретных перестановок принятых символов. Положительный результат формируется в том случае, когда выполненная по результатам оценки мягких решений перестановка символов принятой кодовой комбинации не приводит к линейной зависимости столбцов, адекватно переставленной порождающий матрицы. В противном случае формирование эквивалентного кода положительного результата не дает. Количество положительных решений из общего множества возможных решений составляет большую часть.

С технической точки зрения к данному оборудованию возможно применить способ мягкого декодирования систематических блоковых кодов [4], в основе которого лежит процедура ранжирования мягких решений символов (МРС) принятой кодовой комбинации, выделения из них наиболее надежных символов по показателям МРС, переход к эквивалентному коду с последующим вычислением вектора ошибок, действовавшего на принятый кодовый вектор в процессе передачи его по каналу связи. Достоинством способа является возможность исправления стираний не только кратности $(d-1)$, но и большей доли стираний кратности $(n-k)$, где d – метрика Хемминга, n – число символов в кодовом векторе, k – число информационных разрядов в нем.

Недостатком указанного способа является необходимость вычисления для каждой принятой кодовой комбинации определителя переставленной порождающей матрицы кода в соответствии с показателями МРС для ее первых k столбцов. При невырожденности указанной матрицы для нее выполняется поиск обратной матрицы, и расчет порождающей матрицы эквивалентного кода ведется в систематической форме.

Наиболее популярен способ мягкого декодирования систематических кодов, для кототого основная цель – это уменьшение вычислительных затрат в алгоритме поиска обратной матрицы, расчет массивов матрицы эквивалентного кода приведет к ее систематическому [5] виду, используют прием кластеризации множества разрешенных кодовых векторов, что позволяет обрабатывать определители матриц размерности не $(k\times k)$, а размерности $(k-f)\times(k-f)$, где f – число бит, отводимых на нумерацию (в двоичной системе) формируемых в коде кластеров. Указанная процедура обеспечивает снижение вычислительных затрат поскольку в значительной степени зависит от выбранного параметра f, где $1\le f<k$ [6].

Все указанные способы обладают одним общим недостатком, который заключается в том, что ряд кодовых комбинаций в процессе обработки данных могут повторяться и не только в текущем сеансе, но и по итогам предыдущих сеансов связи. Однако не один из указанных способов не учитывает этот факт и не хранит в своей памяти образец матрицы эквивалентного кода комбинации, когда-либо переданной в системе обмена данными.

Более того, всевозможные образцы переставленных порождающих матриц с положительным и отрицательным исходом могут быть вычислены с помощью внешних устройств и заранее внесены в память декодера. Сравнивая текущие перестановки символов кодовых векторов с имеющимися образцами, возможно заявить будет ли исход текущих преобразований кодового вектора положительным или отрицательным без производства сложных матричных вычислений.

Известно устройство – декодер с упорядоченной статистикой символов, в котором частично решается задача запоминания комбинаций номеров переставленных столбцов порождающей матрицы основного кода, определитель которых указывает на вырожденность переставленных матриц и невозможность реализовать декодирование с использованием эквивалентного кода. Следовательно, для невырожденных матриц процедура поиска переставленных порождающих матриц и приведение их к систематической форме для получения эквивалентного кода выполняется в деко-

дере даже в том случае, если образец переставленного вектора уже обрабатывался декодером.

Известно также устройство – декодер с повышенной корректирующей способностью, которое практически реализует способ, описанный в работе Р. Морелос-Сарагосы с незначительным уточнением процедуры получения МРС. В таком декодере, по сути, сохраняются все недостатки.

Близким по технической сущности к заявленному декодеру является устройство, в котором в блоке приема, первый выход которого через последовательно включенные блок мягких решений символов, накопитель оценок и блок упорядочения оценок присоединен к первому входу блока эквивалентного кода, второй выход которого скоммутирован с другим входом блока сравнения и обратных перестановок, выход которого соединен со вторым входом блока исправления стирания, при этом второй выход блока приема соединен с первым входом блока исправления стирания [7].

Достоинством прототипа является возможность мягкого декодирования комбинаций двоичного кода за пределами метрики Хемминга. Недостатком прототипа является выполнение повторных действий по вычислению порождающей матрицы эквивалентного кода для комбинаций переставленных столбцов порождающей матрицы основного кода, даже если какая-либо комбинация подобных перестановок уже обрабатывалась декодером ранее. Кроме того, прототип не способен реализовать процедуру предварительного вычисления переставленных матриц, что является по сути процедурой обучения и подготовки базы данных для фиксации перестановок с положительным или отрицательным исходами в системе поиска невырожденной матрицы эквивалентного кода.

Технический результат достигается тем, что блок приема, первый выход которого через последовательно включенные блок мягких решений символов, накопитель оценок и блок упорядочения оценок подключен к первому входу блока эквивалентного кода. Второй выход которого подключен к другому входу блока сравнения и обратных перестановок, выход которого подключен к второму входу блока исправления стирания, при этом второй выход блока приема подключен к первому входу блока исправления стирания [7], отличающийся тем, что дополнительно введены

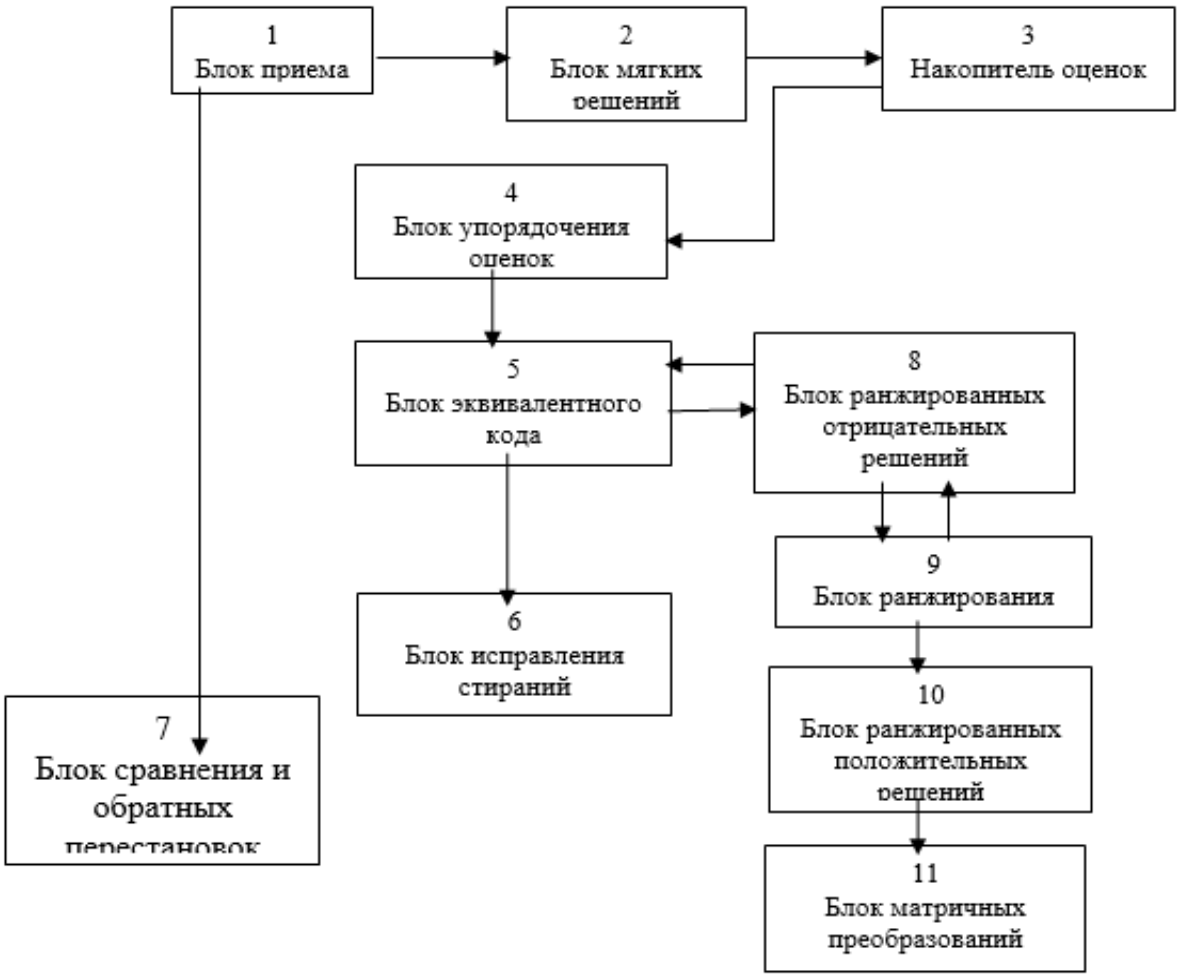

Рис. 2. Структурная схема декодера

блок ранжирования [8], блок ранжированных отрицательных решений, блок ранжированных положительных решений и блок матричных преобразований, выход которого подключен к одному входу блока сравнения и обратных перестановок [7]. При этом первый выход блока эквивалентного кода подключен к одному входу блока ранжирования, первый выход которого через блок ранжированных отрицательных решений подключен к другому входу блока ранжирования, тогда как второй выход этого блока подключен к второму входу блока эквивалентного кода. Третий выход блока ранжирования подключен к второму входу блока матричных преобразований и четвертый выход блока ранжирования через блок ранжирования положительных решений подключен к первому входу блока матричных преобразований, а его выход подключен к одному входу блока сравнения и обратных перестановок.

Структурная схема декодера (рис. 2) содержит блок приема 1, первый выход которого через последовательно включенные блока мягких решений символов 2, накопитель оценок 3 и блок упорядочения оценок 4 подключен к первому входу блока эквивалентного кода 5. Второй выход блока эквивалентного кода 5 подключен к другому входу блока сравнения и обратных перестановок 7, выход которого подключен к второму входу блока исправления стираний 6. Второй выход блока приема 1 подключен к первому входу блока исправления стираний 6. Первый выход блока эквивалентного кода 5 подключен к одному входу блока ранжирования 9, а первый выход этого блока через вход блока ранжированных отрицательных решений 8 и его выход подключен к другому входу блока ранжирования 9. Второй выход блока ранжирования 9 подключен к второму входу блока эквивалентного кода 5, а третий выход блока ранжирования 9 подключен к второму входу блока матричных преобразований 11 и выход этого блока подключен к одному входу блока сравнения и обратных перестановок 7. Четвертый выход блока ранжирования 9 через блок ранжированных положительных решений 10 подключен к первому входу блока матричных преобразований 11 [9].

Работу предлагаемого устройства рассмотрим на примере кода Хэмминга (7, 4, 3) с истиной порождающей матрицей G вида:

$$G=\begin{pmatrix}1&0&0&0&1&0&1\\0&1&0&0&1&1&1\\0&0&1&0&1&1&0\\0&0&0&1&0&1&1\end{pmatrix}.$$

Столбцы истиной матрицы G нумеруются от 1 до 7 слева направо. Пусть передатчик передает информационный вектор $V_{инф}=1010$, тогда в канал связи будет отправлен вектор $V_{кан}=V_{инф}\times G=1010011$. Пусть вектор ошибок V_e имеет вид $V_e=1100100$. В ходе фиксации вектора приема $V_{пр.}$ в блоке приема 1 и выработки для каждого бита этого вектора мягких решений в блоке мягких решений символов 2 в накопителе оценок 3 фиксируется последовательность жестких решений символов и соответствующие им целочислительные МРС вида:

$$V_3=\begin{matrix}0&1&1&0&1&1&1\\3&4&5&6&4&7&7\end{matrix}.$$

Последовательность МРС в блоке 2 формируется по правилу $\lambda_i=\left\lfloor\frac{\lambda_{max}}{\rho\sqrt{E_в}}\cdot Z\right\rfloor$, где ρ – интервал стирания; $E_в$ – энергия сигнала, приходящаяся на один информационный бит; Z – уровень принятого модулируемого параметра (сигнала); λ_{max} – фиксированная оценка МРС с максимальным значением, как правило, определяемая конструктором декодера [10]. В примере $\lambda_{max}=7$. В блоке упорядочения оценок 4 вектор V_3 после перестановок жестких решений по убыванию и соответствующих им МРС принимает вид:

$$V_4=\begin{matrix}1&1&0&1&1&1&0\\7&7&6&5&4&4&3\end{matrix}.$$

При этом в ходе упорядочения оценок формируется перестановочная матрица P, которая в последующем через блок эквивалентного кода 5 поступает в блок сравнения и обратных перестановок для осуществления обратных перестановок с использованием транспонированной матрицы P^T.

$$P=\begin{pmatrix}0&0&0&0&0&0&1\\0&0&0&0&1&0&0\\0&0&0&1&0&0&0\\0&0&1&0&0&0&0\\0&0&0&0&0&1&0\\1&0&0&0&0&0&0\\0&1&0&0&0&0&0\end{pmatrix}.$$

Одновременно с этим блок 5 получает переставленную последовательность номеров столбцов истиной матрицы G в порядке убывания значений МРС в виде $V_5 \rightarrow 6743251$.

Для последующей обработки данных важны первые четыре номера этой последовательности (6, 7, 4, 3). Для быстрого поиска положительного или отрицательного решения по данной перестановке в блоке 9 указанная последовательность ранжируется к виду (3 4 6 7). Все упорядоченные последовательности отрицательных решений хранятся в блоке 8, а упорядоченные значения ранжированных положительных решений в блоке 10. Упорядоченные последовательности могут быть подсчитаны заранее и введены соответственно в блоки 8 и 10. Для используемого в примере кода представлены все сочетания номеров отрицательных и положительных решений (табл. 1, 2).

Таблица 1

Ранжированные сочетания номеров отрицательных решений

1235	1247	1256	1367	1456	2346	3457

Для любого ранжированного сочетания решений (см. табл. 1) справедливы будут всевозможные перестановки, общее число которых определяется как *k!*. Например, для первой позиции таблицы: 1253; 1325; 1352; …; 5123.

Общее число различных сочетаний номеров столбцов для блокового кода определяется выражением вида C_n^k. Тогда $C_7^4 = 35$. Следовательно, с учетом показателей (табл. 1) число положительных решений (табл. 2) должно быть равным 28.

Таблица 2

Ранжированные сочетания номеров положительных решений

1234	1236	1237	1245	1246	1256	1257
1267	1345	1346	1347	1356	1357	1457
1467	1567	2345	2347	2365	2357	2367
2456	2457	2467	3456	3467	3567	4567

Сравнивая значения номеров столбцов, поступивших из блока 5 устанавливает отсутствие такой комбинации виде (6 7 4 3), и приведенные в блоке 9 к виду (3 4 6 7) с указанными значениями (см. табл. 1) декодер в отрицательных решениях. Сравнивая это же значение (3 4 6 7) с ранжированными положительными решениями, декодер находит аналогичную комбинацию в памяти блока 10 и приступает к формированию порождающей матрицы эквивалентного кода. На оставшихся (n – k) позиция обрабатываемого вектора могут быть только номера символов не вошедшие в первые *k* номеров. Если их упорядочить по возрастанию, то получится эталонная переставленная матрица некоторого эквивалентного кода. Такими номерами в примере является последовательность (1 2 5). Образцы эталонных матриц в систематической форме для всех 28 элементов (см. табл. 2) хранятся в блоке матричных преобразований. Для приведенного примера эталонная матрица $G_{3467125}$ в систематическом виде имеет вид

$$G_{3467125} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

С учетом номеров строк и столбцов проверочной части матрицы

$G^{эталь}_{3467125} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$	3 4 6 7
1 2 5	

В блок матричных преобразований 11, через третий выход блока ранжирования 9, поступают данные о текущей последовательности перестановок в виде (6 7 4 3 2 5 1). В блоке 11 по первым *k* элементам сортируются строки эталонной матрицы, по оставшимся (n – k) элементам сортируются столбцы проверочной части матрицы

$$G_{6743251} \Rightarrow \begin{matrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 2 & 5 \end{matrix} \Rightarrow \begin{matrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 2 & 5 & 1 \end{matrix} \Rightarrow$$

$$\Rightarrow G^{сис}_{6743251} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Умножая надежную часть вектора (1 1 0 1) из V_4 на $G^{сис}_{6743251}$ в блоке сравнения и обратных перестановок 7 получают вектор эквивалентного

кода вида $V_{экв}$ =110101. Складывая $V_4 \oplus V_{экв} = V_e^{пер}$ и умножая результат сравнения на P^T в блоке 7 получают истинный вектор ошибок, действовавший в канале связи в момент передачи вектора $V_{кан}$ или V_e = 1100100. Значение этого вектора позволяет исправить стирания в блоке исправления стираний 6.

Предложенное устройство в полной мере использует свойство линейных преобразований матриц и сокращает объем памяти для хранения эталонных матриц в $k! \times (n-k)!$ раз. При этом максимально используется введенная в код избыточность и исключаются такие матричные операции как вычисление определителей и последующий поиск порождающих матриц эквивалентных кодов и последующего приведения их к систематической форме.

Применение принципов эквивалентных кодов позволяет, создать в памяти декодера объективный образ реальных команд, содержание которых потребует дополнительных усилий от противника для вскрытия сути команды.

Результаты

Как результат работы получаем зашифрованный канал связи, который будет обеспечивать безопасную работу БПЛА от спуфинга. В определенный момент времени предоставления данных пользователя в беспроводные сенсорные сети при применении дронов в качестве средства доставки зависит от быстроты реагирования движения БПЛА, времени взаимодействия с узлом сети и наполнения узлов на исследуемой территории.

Работа беспилотников с узлами сенсорных сетей может быть представлена моделью системы массового обслуживания. Показатели данной системы зависят от расположения узлов на территории, а также времени обмена данными с узлами сети, радиусом действия и скорости передвижения беспилотника [11].

Представленная модель для создания роя БПЛА, отличающаяся от аналогичных систем тем, что создается на основе сети массового обслуживания, а главным показателем служит средняя длительность передача данных между элементами роя [12-18].

Обсуждение

Предыдущий анализ и демонстрация показывают, что открытые методы захвата и управления БПЛА практичны для реализации сегодня, а скрытые методы значительно сложнее для потенциального злоумышленника. Стоит отметить, что для подавляющего большинства доступных в настоящее время коммерческих GPS-приемников и навигационных систем БПЛА скрытый захват является синонимом открытого захвата.

Есть еще одна проблема тайного захвата, где предполагается, что спусковой механизм может управлять полученной имитируемой мощностью сигнала на целевом объекте, устанавливая собственную мощность передачи. На практике эффект затенения тела на мощность сигнала, получаемый антенной GPS, установленной на самолете, значителен для крупных самолетов. Для небольших самолетов и некоторых положений установки антенны затенение тела становится незначительным, но эффект усиления антенны остается значительным. Если спусковой механизм работает с низкого угла места, типичные GPS-антенны будут ослаблять симулированные сигналы. Низкоуровневый спусковой механизм может увеличить свою мощность передачи, чтобы компенсировать это ослабление, но без априорного знания схемы усиления антенны, которая характерна для модели антенны и местоположения установки, сабвуфер должен принимать большую неопределенность в низкой высоте затухание, и даже при таких знаниях затухание очень чувствительно к изменениям угла места, что приводит к значительной остаточной неопределенности. Эти эффекты гарантируют, что наземный спусковой механизм обнаружит, что он может точно определить энергетическое преимущество η полученных сигналов спуфинга. К знанию авторов все современные коммерческие гражданские GPS-приемники, даже те, которые обеспечивают измерения с высокой степенью целостности, уязвимых для гражданской подгонки GPS.

Итак, методы, представленные в статье, широко применимы к БПЛА, которые функционируют автономно или полуавтономно и зависят от гражданских сигналов GPS для навигации. Таким образом, датчики с низким, но отличным от нуля датчиком ослабляют возможности управления с помощью атаки спуфинга GPS, но не предотвращают такую атаку.

Заключение

Атакующий, который контролирует критические измерения сенсора, выполненные автономной системой, имеет большую власть над этой системой. В статье была исследована способность атакующего, передающего фальсифицированные сигналы GPS, влиять на поведение автономного БПЛА. Требования к открытому и скрытому захвату навигационной системы БПЛА были представлены вместе с результатами живых испытаний поддельных атак против

нескольких коммерческие GPS-приемники. Помещая эти коммерческие приемники на повторные атаки спуфинга на различные коэффициенты плюсового влияния мощности паутины, было сделано заключение, что, если ошибки оценки спутника в позиции и скорости БПЛА ниже 50 м и 10 м/с соответственно, спусковая способность надежно и скрытый захват контуров отслеживания приемника-получателя. Исследование управления пост-захватом спутника над целевым БПЛА изучалось с использованием упрощенных моделей для оценки состояния, состояния и контроллера состояния БПЛА. При анализе связанной динамики БПЛА и спуфинга было показано, что атака спуфинга GPS может заставить БПЛА следовать траектории, наложенной спусковым механизмом. Полевые испытания показали, что разрушительное GPS-спуфинг нападение на винтокрылой БПЛА является как технически, так и оперативно осуществимым. Практическая демонстрация является доказательством концепции простого частного случая в широком классе атак спуфинга GPS на мобильные цели.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Кондрякова М.А. Уязвимость каналов связи БПЛА. Аллея науки. 2018. Т. 5. No. 4 (20). С. 860–863.
2. Пат. 2438252 Рос. Федерация Декодер с повышенной корректирующей способностью / Ю. П. Егоров и др. No. 2010118639/08 ; заявл. 07.05.2010 ; опубл 27.12.2011, Бюл. No. 36.
3. Гладких А.А. Основы теории мягкого декодирования избыточных кодов в стирающем канале связи. Ульяновск : Изд-во УлГТУ, 2010. 379 с.
4. Ганин Д.В., Наместников С.М., Чилихин Н.Ю. Модифицированные алгоритмы лексикографического декодирования полярных кодов в системе обработки изображений // Вестник НГИЭИ. 2017. No. 11 (78) С. 7–22.
5. Дружинин Е. А., Яшин С. А., Крицкий Д. Н. Анализ влияния функционального назначения и зон применения на структуру и характеристики безопасных к использованию в воздушном пространстве БАК // Открытые информационные и компьютерные интегрированные технологии. 2012. No. 54. С. 60–67.
6. Беспилотная авиация: терминология, классификация, современное состояние [Электронный ресурс]: URL: http://coollib.com/b/322192/read#3 (Дата обращения 17.04.2019).
7. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы. алгоритмы. применение. М. : Техносфера, 2005. С. 213–216. http://coollib.com/b/322192/read#3 (Дата обращения 17.04.2019).
8. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. М. : Мир, 1976. С. 76–78.
9. Ростопчин В. В. Современная классификация беспилотных авиационных систем военного назначения // Интернет-издание UAV.ru. URL: http://uav.ru/articles/bas.pdf (Дата обращения 12.04.2019).
10. Шамин А. А. Повышение энергетической эффективности элементов сенсорных сетей методом перестановочного декодирования // Вестник НГИЭИ. 2017. No. 10 (77). С 24–34.
11. Шахтанов С. В. Перестановочное декодирование недвоичных избыточных кодов // Вестник НГИЭИ. 2017. No. 8 (75) С. 7–14.
12. Пат.2672300 Рос. Федерация. Перестановочный декодер с памятью / А.А. Гладких и др. No. 2017114324 ; заявл. 24.04.2017 ; опубл. 13.11.2018. Бюл. No. 32
13. Методы снижения внутрисетевой нагрузки в распределенных системах хранения данных // Гладких А. А., Климов Р. В. Сорокин И. А. // Автоматизация процессов управления. 2015. No. 3 (41). С. 34–40.
14. Гладких А.А., Наместников С.М., Пчелин Н.А. Эффективное перестановочное декодирование двоичных блоковых избыточных кодов // Автоматизация процессов управления. 2017. No. 1 (47). С. 67–74.
15. Патент 2444127 Рос. Федерация. Способ мягкого декодирования систематических блоковых кодов / А.А. Гладких. No. 2010135507/08 ; заявл. 24.08.2010 ; опубл. 27.02.2012, Бюл. No. 6.
16. Unmanned Aircraft Capture and Control via GPS Spoofing / Andrew J. Kerns, Daniel P. Shepard et al. The University of Texas at Austin Austin, TX 78712. 29 с.
17. Moin Uddin Chowdhury, Eyuphan Bulut, Ismail Guvenc. Trajectory Optimization in UAV-Assisted Cellular Networks under Mission Duration Constraint. IEEE Radio Wireless Week 2019, Orlando, FL. 2019. 5 с.
18. Cell-free Massive MIMO for UAV Communications / Carmen D'Andrea, Adrian Garcia-Rodriguez, et al. University of Cassino and Southern Latium, Cassino, Italy. 2019. 6 с.

REFERENCES

1. Kondryakova M.A. Uyazvimost' kanalov svyazi BPLA [Vulnerability of UAV communication channels]. *Alleya nauki* [*Alley of science*], 2018. Vol. 5. No. 4 (20). Pp. 860–863.
2. Egorov Yu. P. et al. *Dekoder s povyshennoi korrektiruyushchei sposobnost'yu* [*A decoder with enhanced corrective ability*]. Pat. RF 2438252 No. 2010118639/08 ; appl. 07.05.2010 ; publ. 27.12.2011, Bull. No. 36.
3. Gladkikh A.A. Osnovy teorii myagkogo dekodirovaniya izbytochnykh kodov v stirayushchem kanale svyazi [Fundamentals of the theory of soft decoding of redundant codes in the erasing communication channel]. Ul'yanovsk : UlGTU Publ., 2010. 379 p.
4. Ganin D.V., Namestnikov S.M., Chilikhin N.Yu. Modifitsirovannye algoritmy leksikograficheskogo dekodirovaniya polyarnykh kodov v sisteme obrabotki izobrazhenii [Modified algorithms for the lexicographic decoding of polar codes in an image processing system]. *Vestnik NGIEI* [*Herald NGIEI*], 2017. No. 11 (78). Pp. 7–22.

5. Druzhinin E. A., Yashin C. A., Kritskii D. N. Analiz vliyaniya funktsional'nogo naznacheniya i zon primeneniya na strukturu i kharakteristiki bezopasnykh k ispol'zovaniyu v vozdushnom prostranstve BAK [Analysis of the influence of the functional purpose and application areas on the structure and characteristics of the UAV safe for use in the airspace]. *Otkrytye informatsionnye i komp'yuternye integrirovannye tekhnologii* [*Open information and computer integrated technologies*], 2012. No. 54. Pp. 60–67.

6. Bespilotnaya aviatsiya: terminologiya, klassifikatsiya, sovremennoe sostoyanie [Unmanned aircraft: terminology, classification, current state]: URL: http://coollib.com/b/322192/read#3 (Access date 17.04.2019).

7. Morelos-Saragosa R. Iskusstvo pomekhoustoichivogo kodirovaniya. Metody. algoritmy. Primenenie [The art of noise-tolerant coding. Methods, algorithms. Application]. Moscow: Tekhnosfera Publ., 2005. Pp. 213–216. http://coollib.com/b/322192/read#3 (Access date 17.04.2019).

8. Piterson U., Ueldon E. Kody, ispravlyayushchie oshibki [Codes that correct errors]. Moscow: MIR Publ., 1976. Pp. 76–78.

9. Rostopchin V. V. Sovremennaya klassifikatsiya bespilotnykh aviatsionnykh sistem voennogo naznacheniya [Modern classification of unmanned aviation systems for military purposes]. Internet-izdanie UAV.ru. [Internet-edition UAV.ru]. URL: http://uav.ru/articles/bas.pdf (Access date 12.04.2019).

10. Shamin A. A. Povyshenie energeticheskoi effektivnosti elementov sensornykh setei metodom perestanovochnogo dekodirovaniya [Enhancing the energy efficiency of elements of sensor networks by the permutation decoding method]. *Vestnik NGIEI* [*Herald NGIEI*], 2017. No. 10 (77). Pp. 24–34.

11. Shakhtanov S. V. Perestanovochnoe dekodirovanie nedvoichnykh izbytochnykh kodov [Permutation decoding of nonbinary redundant codes]. *Vestnik NGIEI* [*Herald NGIEI*], 2017. No. 8 (75) Pp. 7–14.

12. Gladkikh A.A. et al. *Perestanovochnyi dekoder s pamyat'yu* [Permutation decoder with memory]. Pat. RF 2672300. No. 2017114324 ; applied 24.04.2017 ; publ. 13.11.2018. Bull. No. 32.

13. Gladkikh A. A., Klimov R. V. Sorokin I. A. Metody snizheniya vnutrisetevoi nagruzki v raspredelennykh sistemakh khraneniya dannykh [Methods to reduce internal network load in distributed data storage systems]. *Avtomatizatsiya protsessov upravleniya* [*Automation of management processes*], 2015. No. 3 (41). Pp. 34–40.

14. Gladkikh A.A., Namestnikov S.M., Pchelin N.A. Effektivnoe perestanovochnoe dekodirovanie dvoichnykh blokovykh izbytochnykh kodov [Effective commutation decoding of binary block redundant codes]. *Avtomatizatsiya protsessov upravleniya* [*Automation of management processes*], 2017. No. 1 (47). Pp. 67–74.

15. Gladkikh A.A. *Sposob myagkogo dekodirovaniya sistematicheskikh blokovykh kodov* [*Method for soft decoding of systematic block codes*]. No. 2010135507/08 ; Patent RF 2444127. applied 24.08.2010 ; publ. 27.02.2012, Bull. No. 6.

16. Kerns A. J., Shepard D. P. et al. Unmanned Aircraft Capture and Control via GPS Spoofing. The University of Texas at Austin Austin, TX 78712. 29 p.

17. Chowdhury M. U., Bulut E., Ismail Guvenc I. Trajectory Optimization in UAV-Assisted Cellular Networks under Mission Duration Constraint. IEEE Radio Wireless Week 2019, Orlando, FL. 2019. 5 p.

18. d'Andrea C., Garcia-Rodriguez A. et al. Cell-free Massive MIMO for UAV Communications. University of Cassino and Southern Latium, Cassino, Italy. 2019. 6 p.

Информация об авторах

Сорокин Иван Александрович – к. т. н., доцент кафедры инфокоммуникационных технологий и систем связи, Нижегородский государственный инженерно-экономический университет, г. Княгинин.

Обухов Андрей Дмитриевич – к. т. н., доцент кафедры управления эксплуатационной работой, Петербургский государственный университет путей сообщения им. Императора Александра I, г. Санкт-Петербург, e-mail: adobukhov@mail.ru

Романов Павел Николаевич – старший преподаватель кафедры инфокоммуникационных технологий и систем связи, Нижегородский государственный инженерно-экономический университет, г. Княгинино.

Шибаева Мария Юрьевна – преподаватель кафедры инфокоммуникационных технологий и систем связи, Нижегородский государственный инженерно-экономический университет, г. Княгинино.

Authors

Ivan Aleksandrovich Sorokin – Ph.D. in Engineering Science, Assoc. Prof. at the Subdepartment of Infocommunication Technologies and Communication Systems, Nizhny Novgorod State University of Engineering and Economics, Knyaginino

Andrei Dmitrievich Obukhov – Ph.D. in Engineering Science, Assoc. Prof. at the Subdepartment of Management of Operational Work, Emperor Alexander I St. Petersburg State Transport University, St. Petersburg

Pavel Nikolaevich Romanov – Senior Lecturer at the Subdepartment of «Infocommunication Technologies and Communication Systems» Nizhny Novgorod State University of Engineering and Economics, Knyaginino

Maria Yur'evna Shibaeva – Member of the Subdepartment of Infocommunication Technologies and Communication Systems, Nizhny Novgorod State University of Engineering and Economics, Knyaginino

Для цитирования

Сорокин И. А. Применение метода перестановочного декодирования в системе управления беспилотных летательных аппаратов малого класса (дроны, мультикоптеры) / И. А. Сорокин, А. Д. Обухов, П. Н. Романов, М. Ю. Шибаева // Современные технологии. Системный анализ. Моделирование. – 2019. – Т. 62, № 2. – С. 186–195. – DOI: 10.26731/1813-9108.2019.2(62).186–195

For citation

Sorokin I. A., Obukhov A. D., Romanov P. N., Shibaeva M. Yu. Primenenie metoda perestanovochnogo dekodirovaniya v sisteme upravleniya BPLA malogo klassa (drony, mul'tikoptery) [Application of a permutation decoding method in a small-class unmanned aerial vehicle control system (drones, multicopters)]. *Sovremennye tekhnologii. Sistemnyi analiz. Modelirovanie* [*Modern Technologies. System Analysis. Modeling*], 2019. Vol. 62, No. 2. Pp. 186–195. DOI: 10.26731/1813-9108.2019.2(62).186–195