АЛГОРИТМЫ ОБРАБОТКИ ИНФОРМАЦИИ ДЛЯ АВТОНОМНЫХ ГРУПП БПЛА

Хмаро И.С., студент гр. 241301

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Лапцевич А.А. – канд. техн. наук, доцент

Аннотация. В работе рассматриваются вопросы построения архитектур управления группами автономных беспилотных летательных аппаратов (БПЛА). Проведен анализ основных векторов атак на каналы связи и предложены методы защиты данных в условиях ограниченных аппаратных ресурсов. Рассмотрены стандарты взаимодействия и протоколы маршрутизации, обеспечивающие устойчивость роя к внешним воздействиям.

Ключевые слова. БПЛА, автономные группы, роевой интеллект, информационная безопасность, криптография, *STANAG* 4586, децентрализованное управление.

Фундаментальной проблемой при создании автономных групп является обоснованный выбор базовой архитектуры управления и связи, которая должна соответствовать специфике выполняемых задач. Согласно глубокому анализу современных технических отчетов, исследователи выделяют три основных типа архитектур, каждая из которых имеет свои пределы применимости [1, 2]. Централизованная архитектура предполагает, что все высокоуровневые вычисления, обработка сенсорной информации и генерация управляющих команд осуществляются через единую мощную наземную станцию управления или через специально выделенный тяжелый ведущий аппарат. Главным и зачастую фатальным недостатком такого подхода является наличие «единой точки отказа», при физическом уничтожении или радиоэлектронном подавлении которой вся группа мгновенно теряет координацию и становится неуправляемой. Децентрализованная, или полностью распределенная, архитектура основана на фундаментальном принципе равноправия всех вычислительных узлов. В такой парадигме каждый отдельный аппарат принимает навигационные и тактические решения исключительно на основе собственных локальных сенсорных данных и непрерывного обмена телеметрической информацией с ближайшими соседями. Иерархическая структура представляет собой эффективный компромиссный вариант, при котором обширная группа БПЛА адаптивно делится на локальные кластеры, внутри которых путем автоматического голосования назначаются временные локальные лидеры, коммуницирующие как со своими подчиненными узлами, так и с лидерами соседних кластеров [2].

Для обеспечения бесперебойной высокоскоростной связи в полностью децентрализованных и иерархических группах в настоящее время повсеместно применяется концепция летающих самоорганизующихся ячеистых сетей (*Flying Ad-Hoc Networks*, *FANET*). В отличие от классических наземных мобильных сетей или автомобильных сетей, инфраструктура *FANET* должна учитывать экстремально высокую трехмерную мобильность узлов, частые и непредсказуемые разрывы радиосоединений из-за резкого изменения дистанции, а также сильное влияние эффекта Доплера при передаче радиосигналов на высоких встречных скоростях [1]. Помимо проблем маршрутизации, сети *FANET* сталкиваются с серьезными вызовами на канальном уровне (*MAC*-уровне). Традиционные механизмы множественного доступа, такие как *CSMA*/*CA*, используемые в обычных сетях *Wi-Fi*, оказываются крайне неэффективными в трехмерном пространстве роя из-за усугубленной проблемы «скрытого узла» и «экспонированного узла». Когда аппараты перемещаются в трехмерном пространстве с высокой скоростью, направленность антенн и зоны радиовидимости постоянно меняются, что приводит к массированным коллизиям пакетов в радиоэфире. Для решения этой проблемы в передовых роевых архитектурах внедряются гибридные протоколы канального уровня, сочетающие адаптивное временное разделение каналов (*TDMA*) с механизмами случайного доступа, что позволяет гарантировать выделенные таймслоты для передачи критически важной телеметрии без задержек.

Кроме того, моделирование движения в сетях *FANET* кардинально отличается от наземных систем. Использование классических моделей случайного блуждания не отражает реальной физики полета беспилотника. Поэтому для корректной настройки сетевых алгоритмов применяются специализированные полумарковские трехмерные модели мобильности, учитывающие аэродинамические ограничения аппарата, радиус разворота, максимальные углы тангажа и крена. Интеграция таких физически достоверных моделей мобильности в алгоритмы маршрутизации позволяет предсказывать моменты разрыва связи между конкретными узлами за несколько секунд до того, как они произойдут физически, что дает сети время на превентивную перестройку маршрутов [2].

В процессе практической эксплуатации автономных групп, особенно в условиях целенаправленного радиоэлектронного противодействия, возникают специфические и весьма опасные угрозы информационной безопасности. Основными векторами атак на беспроводные радиоканалы

связи БПЛА на физическом уровне являются пассивный перехват данных и атаки типа отказ в обслуживании, реализуемые через подавление полезного радиосигнала направленным широкополосным или узкополосным белым шумом [4]. На сетевом уровне крайне опасны активная подмена данных, известная как спуфинг навигационных полей, и перехват управления путем инъекции вредоносных команд. Особую угрозу для децентрализованных алгоритмов маршрутизации представляют атаки типа «черная дыра», при которых скомпрометированный злоумышленником узел роя ложно объявляет себя оптимальным и кратчайшим маршрутом до цели, после чего начинает уничтожать все проходящие через него пакеты данных. Не менее разрушительны атаки «кротовины», когда два вредоносных узла создают выделенный высокоскоростной скрытый туннель связи для перехвата трафика и фатального искажения топологии всей сети, а также атаки Сивиллы, в ходе которых один нарушитель генерирует в радиоэфире множество фиктивных виртуальных узлов для фальсификации результатов алгоритмов кластерного голосования [4].

Для противодействия этим угрозам недостаточно применять только криптографию; требуется внедрение распределенных систем обнаружения вторжений (*IDS*), адаптированных специально для роевой архитектуры. В отличие от стационарных серверов, БПЛА не могут хранить огромные базы сигнатур вирусов и атак. Поэтому роевые *IDS* строятся на основе поведенческого анализа и концепции доверительной маршрутизации. Каждый узел в рое постоянно вычисляет индекс доверия для своих соседей на основе успешности доставки пакетов, интенсивности передачи и соответствия заявленных координат физическим законам движения. Если какой-либо аппарат начинает отбрасывать пакеты или его передаваемые координаты противоречат данным бортовых радаров других узлов, его индекс доверия стремительно падает, и сеть автоматически исключает этот скомпрометированный аппарат из таблиц маршрутизации, изолируя угрозу [4].

Учитывая предельно жесткие аппаратные ограничения подавляющего большинства БПЛА малого и микро-класса, выраженные в сильно ограниченной вычислительной мощности бортовых микроконтроллеров и строгом лимите энергопотребления из-за малой емкости аккумуляторов, использование классических тяжеловесных криптографических стандартов критически затруднено. В связи с этим безальтернативно рекомендуется применение новейших концепций облегченной криптографии. К таким передовым решениям относятся алгоритмы асимметричного шифрования на основе эллиптических кривых, которые при меньшей длине ключа обеспечивают высочайшую стойкость. Также активно внедряются современные высокоскоростные потоковые шифры вроде *ChaCha20* в связке с аутентификаторами *Poly1305* и стандарты криптографического хеширования нового поколения из семейства *ASCON*. Данные алгоритмы обеспечивают математическую криптостойкость, полностью сопоставимую с традиционными банковскими методами защиты, но при этом требуют на порядки меньших процессорных тактов [4]. Дополнительным перспективным направлением является безопасность на физическом уровне (*Physical Layer Security*), которая использует естественные характеристики радиоканала, такие как замирания и многолучевое распространение, для генерации симметричных криптографических ключей непосредственно между легитимными приемником и передатчиком без необходимости их предварительного распределения.

Для организации эффективного, безопасного и предсказуемого взаимодействия различных типов и классов БПЛА в рамках одной сложной гетерогенной группы необходимо строгое и неукоснительное соблюдение унифицированных международных стандартов обмена цифровыми данными. Одним из наиболее глубоко проработанных нормативных документов в этой области является стандарт *STANAG* 4586 [3]. Данный документ комплексно описывает сетевую архитектуру и программные интерфейсы базовой системы управления беспилотными аппаратами. Ключевой технологической особенностью этого стандарта является введение понятия аппаратно-зависимого модуля (*VSM*). Этот модуль выступает в роли интеллектуального программного транслятора между универсальными стандартизированными командами наземной станции и проприетарными протоколами конкретного производителя дрона [3].

Помимо формальных стандартов высокого уровня, на практике архитектура взаимодействия в рое критически зависит от используемых микропротоколов и промежуточного программного обеспечения (*Middleware*). Индустриальным стандартом де-факто для обмена телеметрией на уровне микроконтроллеров стал протокол *MAVLink*. Это чрезвычайно легковесный протокол обмена сообщениями, специально разработанный для систем с ограниченной пропускной способностью. *MAVLink* упаковывает полетные данные, команды и координаты в компактные бинарные структуры, размер заголовка которых составляет всего несколько байт, что делает его идеальным для использования в зашумленном радиоэфире. Современные версии этого протокола (*MAVLink* 2.0) поддерживают встроенные механизмы цифровой подписи пакетов, что решает часть проблем подмены команд на базовом уровне [1, 3].

Для решения более сложных задач роевого взаимодействия, таких как распределенное компьютерное зрение, синхронное картографирование и комплексирование данных с множества датчиков, применяется концепция Робототехнической операционной системы (*ROS*). Переход современных групп БПЛА на архитектуру *ROS2* привел к внедрению стандарта обмена данными *DDS* (*Data Distribution Service*). *DDS* обеспечивает децентрализованную архитектуру обмена сообщениями

по принципу «издатель-подписчик» в режиме жесткого реального времени. В контексте роя это означает, что один аппарат может публиковать данные со своего оптического сенсора, а несколько других БПЛА могут одновременно подписываться на этот поток данных для совместного анализа, причем *DDS* берет на себя все низкоуровневые задачи по обеспечению качества обслуживания, надежности доставки и фильтрации сетевого трафика. Такая программная архитектура позволяет абстрагироваться от сложности радиоканалов и сосредоточиться на высокоуровневой логике поведения группы [1].

Для обеспечения по-настоящему высокого уровня автономности, адаптивности и пространственной самоорганизации группы в современной инженерии активно и успешно применяются сложные метаэвристические алгоритмы, математически вдохновленные биологическими макросистемами живой природы. Наиболее яркими и исследованными примерами являются метод оптимизации муравьиной колонии и метод оптимизации роя частиц. В специфичном контексте самоорганизующихся сетей алгоритм муравьиной колонии элегантно используется для динамической и отказоустойчивой маршрутизации пакетов данных в условиях постоянного разрыва связей. Бортовые вычислители периодически генерируют небольшие служебные пакеты, которые оставляют в таблицах маршрутизации транзитных аппаратов виртуальный числовой «феромонный след». Чем быстрее и безопаснее радиоканал связи, тем выше концентрация этого феромона, что заставляет узлы отдавать приоритет именно этому пути [2].

Математические модели оптимизации роя частиц применяются в основном для высокоточного удержания геометрического строя. В дополнение к биологическим алгоритмам, для локального предотвращения столкновений на сверхмалых дистанциях широко используется метод искусственных потенциальных полей (*APF*). Суть метода заключается в том, что цель миссии генерирует виртуальное поле притяжения, в то время как препятствия и соседние БПЛА генерируют поля отталкивания. Суперпозиция этих векторных полей в каждой точке пространства позволяет вычислителю дрона мгновенно определять оптимальный вектор безопасного движения без сложных кинематических расчетов. Однако классические потенциальные поля подвержены проблеме локальных минимумов, когда аппарат может застрять в равновесной точке [1].

Для преодоления ограничений эвристических подходов в современные системы управления роем все активнее внедряются методы глубокого машинного обучения и обучения с подкреплением (*Reinforcement Learning*). Агенты обучения с подкреплением, развернутые на борту каждого БПЛА, способны самостоятельно вырабатывать оптимальные стратегии уклонения и маршрутизации путем многократных симуляций методом проб и ошибок. Особенный интерес представляет парадигма федеративного обучения (*Federated Learning*). В условиях жестко ограниченной пропускной способности каналов связи аппараты не пересылают терабайты собранных изображений на наземную станцию для обучения нейросетей. Вместо этого они локально обучают распознающие модели на своих бортовых микрокомпьютерах, а в радиоэфир передают лишь обновленные весовые коэффициенты нейросети. Лидер кластера агрегирует эти коэффициенты и рассылает обновленную глобальную модель всему рою. Такой подход кардинально снижает нагрузку на канал связи и минимизирует риски компрометации исходных разведданных при перехвате [1, 2].

Абсолютно критичным и часто недооцениваемым аспектом функционирования автономных групп является проблема энергетической эффективности. В отличие от наземных сенсорных сетей, где датчики могут годами работать от одной батарейки, БПЛА тратят подавляющую часть энергии на работу винтомоторной группы и поддержание аппарата в воздухе. В связи с этим энергия, выделяемая на работу бортового компьютера и радиопередатчика, строго лимитирована. Классические протоколы маршрутизации, ориентированные только на поиск кратчайшего пути, часто приводят к тому, что узлы, находящиеся в центре построения роя, пропускают через себя весь транзитный трафик. Это вызывает их стремительный разряд, выход из строя и, как следствие, катастрофическое нарушение связности всей сети [2].

Для решения этой проблемы разрабатываются так называемые энерго-осведомленные (*Energy-Aware*) протоколы маршрутизации и управления топологией. В таких системах метрика стоимости радиомаршрута вычисляется не только исходя из расстояния или задержки, но и с обязательным учетом текущего остаточного заряда аккумуляторных батарей каждого транзитного узла. Если какой-либо БПЛА сигнализирует о критическом падении уровня заряда, сеть автоматически перестраивает маршруты таким образом, чтобы пустить цифровой трафик в обход истощенного аппарата, тем самым продлевая время его нахождения в воздухе. Более того, алгоритмы удержания строя могут адаптивно изменять дистанцию между аппаратами: при низком заряде дроны сближаются для снижения мощности радиопередатчиков, что экономит драгоценные миллиампер-часы [1].

Дальнейшим развитием концепции энергосбережения является применение технологий мобильных граничных вычислений (*Mobile Edge Computing*) внутри самого роя. Обработка алгоритмов компьютерного зрения высокого разрешения или криптографических хеш-функций требует значительных вычислительных затрат. Если отдельный малый дрон не располагает достаточной энергией или процессорной мощностью для обработки тяжелой задачи, он может динамически делегировать эту задачу более крупному аппарату в рое (узлу граничных вычислений), обладающему

емкими аккумуляторами и мощными тензорными сопроцессорами. Дрон пересылает сырые данные, а в ответ получает готовый результат вычислений. Интеллектуальное распределение вычислительной нагрузки между различными аппаратами внутри группы позволяет значительно увеличить общее время автономной работы роя и выполнять миссии, которые были бы технически невозможны для изолированных аппаратов [2, 4].

Список использованных источников:
1. UAV swarm communication and control architectures: a review - SciSpace, 2024. – 12 p.
2. Review of Unmanned Aerial Vehicle Swarm Communication Architectures and Routing Protocols - MDPI, 2020..
3. STANAG 4586 – Standard Interfaces of UCS for NATO UAV Interoperability, 2021.
4. Secure Communication in Drone Networks: A Comprehensive Survey – MDPI, 2023.

UDC

ALGORITHMS FOR CONTROL AND SECURITY OF COMMUNICATION CHANNELS IN AUTONOMOUS UAV GROUPS

Khmaro I.S.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Laptsevich A.A. – PhD, Associate Professor

Annotation. The paper discusses the issues of building architectures for managing groups of autonomous unmanned aerial vehicles (UAVs). It analyzes the main attack vectors on communication channels and proposes methods for protecting data in the context of limited hardware resources. The paper also examines communication standards and routing protocols that ensure the stability of the swarm against external influences.

Keywords. UAVs, autonomous groups, swarm intelligence, information security, cryptography, STANAG 4586, and decentralized management.