

Сравнительный анализ протоколов маршрутизации в рое БпЛА

В.В. Миронов, С.П. Селезнёв, И.Я. Круковская, Я.В. Круковский

Аннотация — В данной работе проведён аналитический обзор ключевых классов протоколов и методов маршрутизации, применяемых в динамических беспилотных сетях (FANet) высокой плотности. Рассмотрены три доминирующие концепции: табличные подходы (проактивные и реактивные), эпидемические (лавиновые) методы распространения данных и методы контентно-зависимой дедупликации в контексте реализации современных концепций маршрутизации. Проведён сравнительный анализ их вычислительной сложности по времени и памяти, величине служебных расходов трафика и устойчивости к внешним средствам деструктивного воздействия.

Ключевые слова: беспроводная сеть, рой, CB-BSD, маршрутизация, CB-RDE, шторм пакетов, лавинные методы, эпидемические протоколы, дедупликация, вычислительная сложность, БпЛА

I. ВВЕДЕНИЕ

Специфика роевых FANet (Flying Ad-Hoc Network) сетей для беспилотных летательных аппаратов (БпЛА) обусловлена рядом факторов, существенно отличающих их от традиционных MANet (Mobile Ad hoc Network) и стационарных сетей [1; 4; 56]. В роевых FANet классические протоколы маршрутизации сталкиваются с базовыми ограничениями [23; 24; 57]: скорость изменения топологии сети превышает темп сходимости таблиц маршрутизации, состав и плотность роя подвержены непрерывным флуктуациям. Кроме того, характеристики радиоканала ухудшаются из-за многолучёвости, поляризационных потерь, манёвров БпЛА, воздействию факторов деструктивного фона (ВДФ) [5]. При этом уязвимости канального уровня порождают угрозы ИБ [9; 61] и способны нарушить целостность маршрутной информации и корректность процедур маршрутизации.

Само общее определение сущности роя FANet задаёт особые требования при решении задачи маршрутизации в рамках масштабируемой самоорганизующейся сети с высокой динамикой

топологии, ролевой неоднородностью узлов сети (БпЛА) со своими приоритетами, "весами" в группе (рое), нацеленных на выполнение совместного полётного задания в сложных условиях и при жёстких ограничениях по массогабаритным и энергопотребительским характеристикам SWaP (Size, Weight, and Power). В MANet/FANet актуально состояние высокой плотности сети роя (от единиц до 100+ узлов сети), при котором в пределах зоны радиовидимости $R_{пр} \approx k_{сз} \cdot (\sqrt{h_a} + \sqrt{h_c})^1$ одновременно находится значительное число узлов. При этом интенсивность обмена служебными и полезными данными в период выполнения полётного задания приводит к существенному росту вероятности коллизий и межузловой интерференции, что проявляется в снижении доли успешно доставленных пакетов, росте задержек и падении эффективной пропускной способности на узел. В классических работах Н. Бусленко [3] был предложен математический аппарат, где каналы сопряжения между, в нашем случае – узлами сети роя, могут динамически меняться в процессе функционирования под воздействием случайных факторов. Для роя БпЛА это означает, что локальные правила взаимодействия отдельных узлов формируют эмерджентное (коллективное) поведение всей группы, способной решать общие глобальные задачи: от совместного сканирования местности до преодоления интенсивных помеховых воздействий со стороны внешних источников.

Устойчивость сети в этих условиях достигается за счёт одновременно системного подхода и дифференцированного выбора алгоритмов маршрутизации, обеспечивающих кросс-уровневую адаптацию в режиме полета роя и жизненном цикле сети. Особое значение в архитектуре роя имеет задача предотвращения столкновений и обеспечения безопасного пространственного разделения БпЛА в условиях

¹ обобщённо, где $k_{сз}$ — коэффициент (3,57 для дм/см-диапазона, 4,12 — для метрового, с учётом рефракции), h_a и h_c — высоты узлов сети над поверхностью; непосредственно

в рое эта формула даёт $R_{max} = 2 \cdot k_{сз} \cdot \sqrt{h_{узел}}$ зоны взаимной видимости узлов сети при одинаковой высоте полёта БпЛА.

отсутствия спутниковой или *бесплатформенной инерциальной навигационной системы* (БИНС). Эта задача выходит за рамки чисто навигационных функций и становится сетевой: своевременная доставка сообщений (*intent messages*) о намерениях, текущих траекториях и маневрах является необходимым условием для единого ситуационного управления.

Несмотря на различие частных целевых задач отдельного БпЛА, все узлы формируют единую *самоорганизующуюся сеть* (СС) и участвуют в общем сетевом стеке, обеспечивая сквозную связность, ситуационную осведомлённость и роевую слаженность. При этом требования к задержкам, надёжности и объёму трафика для каждого участника существенно различаются: для команд уклонения и предотвращения столкновений критичны минимальные задержки и гарантированная доставка, тогда как для передачи измерительных (разведывательных) данных допустимы более гибкие параметры. Обеспечение автономной работы сети, даже если часть узлов выйдет из строя, способность в режиме реального времени адаптировать свою конфигурацию под условия связности являются ключевыми требованиями для реализации живучести сети, в том числе при *внешнем воздействии ВДФ*, см. подробнее в [5; 23; 25; 26]. Подход к решению подобных задач на сетевом уровне апробирован в [29].

Важным аспектом является *динамическое масштабирование, изменение состава роя и изменение роли отдельных узлов при сохранении общей задачи* в ходе выполнения полётного задания: часть узлов может завершать локальные задачи и покидать рой (*зону покрытия / связности* сети роя), другие – присоединяться к рою, формируя подгруппы или кластеры. Такая динамика требует от сетевого стека не только способности к быстрой адаптации без централизованного управления и без потери связности, но и обеспечения гарантированного обмена сообщениями с детерминированными задержками, достаточными для расчёта безопасных траекторий и избегания коллизий с целью введения в определённое время акторов цели.

Таким образом, ключевая специфика радиосетей в концепции роевой FANet состоит в том, что такая сеть должна быть одновременно:

- *самоорганизующейся*, то есть без внешней инфраструктуры и внешнего управления;

- *адаптивной*, подстраивающейся под изменения топологии и условий канала, включая состояние плотности роя;

- *живучей*, способной сохранять связность и приемлемое время реакции при потере значительной доли узлов, воздействии ВДФ и снижении энергоресурса;

- *скрытной*, т.е. способной минимизировать предсказуемость поведения сети;

- *мультисервисной*, когда ролевой узел (БпЛА) имеет набор сервисов обеспечивающих как управляемый, так и автономный режимы выполнения полётного задания.

Базовые протоколы маршрутизации MANet, такие как AODV и DSR, в данных условиях демонстрируют недостаточную адаптивность и неприемлемо высокие задержки при перестройке маршрутов, а также избыточный служебный трафик (*Routing Overhead, ROH*). Широкие полосы и высокопроизводительные стеки (Wi-Fi и LTE-подобные реализации) оказываются избыточными по пропускной способности, но при этом более уязвимыми к прицельному подавлению и менее скрытными. То есть, первые характеризуются высокой временной инерционностью алгоритмов для динамично меняющейся топологии, вторые – слишком "заметны", имеют дополнительно повышенные требования к *синхронизации, наличию базового узла* ("одна точка отказа").

Несмотря на различные схемы организации FANet, использующие узкополосные и широкополосные радиоканалы, в любом случае система с узкополосными низкоскоростными каналами (например, целевая полезная скорость $\approx 9,6$ кбит/с), должна обеспечивать не только минимальные задержки в передаче команд, но *сбор и обработку видеоданных* в интересах ситуационной осведомлённости роя. Это достигается за счёт приоритизации трафика, сжатия на источнике, передачи ключевых кадров и метаданных, а также использования механизмов селективной ретрансляции. Тогда, даже при ограниченной пропускной способности канал остаётся полезным для тактического управления при любых полётных заданиях.

Наконец, в архитектуре управления роем всё большее значение приобретает **компонент автоматической адаптации в концепции искусственного интеллекта** (ИИ), решающего

параллельные задачи, в автономном режиме – задачи распределения ролей, планирования манёвров, адаптации сетевых параметров, прогнозирования и предотвращения деградации каналов. Компонент ИИ работает не изолированно, а как часть системной задачи: использует данные телеметрии, оценку качества и ресурсов каналов, динамические прогнозы для оптимизации параметров маршрутизации и, в том числе, задач инженерного зрения.

Таким образом, для роевых FANet требуется специализированная архитектура сетевого стека, обеспечивающая баланс между адаптивностью, живучестью, скрытностью и SWaP в целом. Для системного обоснования выбора способа и схем маршрутизации необходим анализ архитектуры сетевого стека для формализации основных классов угроз и соответствующих сценариев деградации сетей [5], характерных для роевых FANet. Угрозы целесообразно классифицировать по уровням воздействия: среда распространения, сеть, узел, прикладные задачи и комбинированные воздействия.

II. АНАЛИЗ УГРОЗ И КЛАССИФИКАЦИЯ СЦЕНАРИЕВ ДЕГРАДАЦИИ

2.1. Угрозы на уровне среды

На физическом уровне основными факторами, снижающими качество канала, являются:

- **Замирания сигнала**, обусловленные многолучевым распространением и быстрыми изменениями расстояния между узлами. Для описания замираний в условиях полёта БПЛА применимы модели Райса и Накагами [2; 48], учитывающие наличие прямого луча и рассеянных компонент.

- **Поляризационные потери**, возникающие при произвольной ориентации БПЛА относительно наземных или воздушных узлов. Несогласованность поляризации антенн может приводить к потерям до 10–15 дБ.

- **Воздействие ВДФ**, включая целенаправленное подавление отдельных частот, широкополосные помехи и имитацию легитимного трафика. Эти угрозы приводят к снижению отношения *сигнал/шум* (SNR), росту вероятности битовой ошибки (BER) и, как следствие, к увеличению числа повторных

передач и снижению полезной пропускной способности.

2.2. Угрозы на уровне сети

На сетевом и канальном уровнях основными угрозами являются:

- **Шторм пакетов (Flooding Storm, FS)**, возникающий при одновременной рассылке большого числа пакетов и отсутствии механизмов контроля дубликтов. В условиях высокой плотности (30 ... 100+ узлов) базовая лавинная маршрутизации (Pure Flooding) приводит к экспоненциальному росту числа копий пакетов и "захлёбыванию" канала.

- **Коллизии (Collisions) и перегрузки (Overload) MAC-уровня**, обусловленные одновременным доступом множества узлов к среде. Например, без адаптации в узкополосной реализации доступа CSMA/CA вероятность коллизий возрастает при росте плотности узлов и длительности передачи пакетов. Высокая плотность одновременно взаимодействующих узлов роя БПЛА, является один из факторов формирования *коллизийного домена* (КД)².

- **Лавинная маршрутизация без контроля**, когда узлы ретранслируют пакеты без учёта локальной плотности и состояния сети, что усиливает шторм (FS).

- **Асимметрия каналов**, приводящая к ошибкам в оценке связности и формированию "односторонних" маршрутов.

Ключевым показателем, характеризующим угрозу возникновения *широковещательного шторма* (Broadcast Storm, BS) [24] в радиосети, является доля (вероятность) дубликтов P_{dup} , которая в отсутствие адаптивных механизмов может достигать 40–60% и выше.

2.3. Угрозы на уровне узла

На уровне отдельного узла основными факторами деградации являются:

- **деградация энергоресурса**, приводящая к снижению мощности передачи, отключению второстепенных сервисов и, в крайних случаях, к потере узла из сети.

- **отказ узла** вследствие технических неисправностей, потери управления или преднамеренного воздействия.

² КД – зона радиовидимости с высокой вероятностью взаимных коллизий (коллапса сети связи роя).

- **ограничения** вычислительной мощности и объёма оперативной памяти (RAM), определяющие сложность реализуемых протоколов и объём буферизации пакетов.

В учёте состояния узла реализуется *политика управления энергоресурсом* (далее по тексту – SOC-политика) на основе метрики SOC (*State of Charge*) узла, предусматривающая поэтапное и адаптивное отключение ресурсоёмких сервисов при снижении уровня заряда батареи ниже установленных пороговых значений.

2.4. Угрозы на прикладном уровне и в задачах ситуационного управления

Этот уровень критически важен с учётом разнородности ролей и требований к безопасности полётов:

- **Потеря или задержка критических сообщений о намерениях и траекториях**, что напрямую угрожает предотвращению столкновений. Даже при сохранении общей связности сети, потеря этих сообщений может привести к недопустимым сближениям БпЛА.

- **Несбалансированное распределение ролей и задач** при динамическом масштабировании состава роя. Если компонент управления (в том числе, реализованный на основе встроенных технологий ИИ) не успевает адаптировать роли и приоритеты, сеть может оказаться перегружена служебным трафиком или потерять ключевых ретрансляторов и исполнителей.

- **Неэффективная передача видеоданных** на низкоскоростном канале: без приоритизации и сжатия канал может быть "занят" из-за второстепенных данных, что снижает ситуационную осведомлённость.

Таким образом, прикладной уровень становится не "надстройкой", а активным участником кросс-уровневого управления: приоритеты трафика, выбор формата данных и планирование манёвров напрямую влияют на нагрузку сети и требования к задержкам.

2.5. Комбинированные сценарии деградации

Наиболее реалистичными и критичными для оценки живучести радиосети роя являются комбинированные сценарии, имитирующие одновременное воздействие нескольких классов угроз. В данном случае рассматриваются следующие типовые сценарии:

- **искусственный шторм**: одновременная рассылка ≈ 100 пакетов с разных узлов при

плотности до 100 единиц. *Цель* – оценить эффективность механизмов контроля дубликатов и устойчивость канала к перегрузке трафика. *Ключевыми метриками* могут быть: % отфильтрованных дубликатов, вероятность доставки критических сообщений и деградация полезной пропускной способности.

- **деградация узлов сети (в рое)**: отключение $\approx 30\%$ узлов при сопутствующем снижении заряда батарей (SOC) у оставшейся части узлов до критических значений. *Цель* – оценить живучесть сети, время сходимости маршрутизации и сохранение критических функций при частичной потере узлов и ограничении их ресурсов. *Ключевые метрики*: время перестройки маршрутов, доля связанных пар узлов, доля доставленных приоритетных сообщений.

- **дестабилизирующее воздействие**: целенаправленное подавление в выделенной полосе радиочастот, например. *Цель* – оценить устойчивость сети к целенаправленному воздействию и эффективность механизмов адаптации при наличии в стеке алгоритма *псевдослучайной перестройки рабочих частот* (ППРЧ). *Ключевые метрики*: доля успешных переключений на свободные каналы, время восстановления связности, доля потерянных пакетов в период подавления.

- **комбинированный стресс**: реализуется одновременное воздействие всех перечисленных факторов: *шторм + ВДФ + потеря узлов + низкий SOC + интенсивный обмен данными* и др. *Цель* – оценка интегральной живучести системы и соответствие архитектуры целевым метрикам.

Таким образом, предложенная классификация угроз и сценариев деградации радиосети роя позволяет системно обосновать на каждом уровне стека выбор группы алгоритмов и в итоге сформулировать установленном порядке [60; 61] требования к сетевой архитектуре БпЛА-узла и референсной модели сети роя в целом [62].

III. СРАВНИТЕЛЬНЫЙ АНАЛИЗ ДОМИНИРУЮЩИХ КОНЦЕПЦИЙ МАРШРУТИЗАЦИИ

В системах автономных роевых роботизированных платформ (в частности, групп БпЛА) сетевая связность, достигаемая благодаря протоколам маршрутизации перестаёт быть "фоном" и становится тактическим ресурсом: её наличие, предсказуемость, адаптивность и живучесть напрямую обеспечивают выполнение целевой задачи. В условиях высокой динамики топологии, переменной плотности узлов, ВДФ, а

также ограничений по SWaP, требования к маршрутизации существенно отличаются от классических сетевых сценариев. Общие сведения о существующих типовых решениях и протоколах приведены в работе [23].

3.1. От требований к архитектуре: эшелонованная защита.

3.1.1. Архитектурные особенности реализации сетевой парадигмы

В роевой сети нельзя полагаться на единственный механизм обеспечения связности, угрозы действуют одновременно и на разных уровнях. Поэтому архитектура сетевого стека строится *по принципу эшелонованной защиты кросс-уровневого стека*, где каждый уровень отвечает за свой класс угроз:

- **Физический уровень (PHY):** выбор диапазона частот, способ доступа, устойчивость к замираниям и прицельному подавлению – например, поляризационно-разнесенного приёма сигналов, ППРЧ и др.

- **Канальный уровень (MAC):** управление доступом к среде и контроль коллизий. Например, в сочетании множественного доступа с контролем несущей и предотвращением коллизий (CSMA/CA) и адаптивным CCA (оценка занятости канала или анализ свободной частоты).

- **Сетевой уровень** (маршрутизация / фильтрация): контроль размножения пакетов, защита от факторов шторма, быстрая адаптация к плотности, сетевой близости.

- **Кросс-уровневые политики:** согласование приоритетов трафика, включая доступ к радиоканалу, уровень приложений с учётом ролевых позиций БПЛА-узла, энергопотребления и накладных расходов (SOC-политика, дифференцированное шифрование).

Таким образом, подобный подход позволяет обеспечить баланс между оперативностью доставки критических сообщений, энергоэффективностью, скрытностью и устойчивостью сети в условиях динамической топологии, ограниченной полосы частот и SWaP. Это позволяет сохранить детерминированность ключевых метрик (время реакции, доля подтверждённых пакетов) даже в условиях

комбинированных стрессов: шторм пакетов, потеря узлов, низкий заряд и др.

Вместе с тем, ключевым противоречием является *одновременное* требование высокой адаптивности к изменениям плотности и/или воздействию ВДФ и жёстких ограничений на время реакции, а также требование к автономности роя, необходимость обеспечения скрытности передачи и устойчивости к прицельному подавлению. Одновременно необходимо учитывать ограничения SWaP, касающиеся бортового оборудования.

Концепция А. Табличные протоколы (классические MANet/FANet протоколы). Этот класс разделяется на проактивные (OLSR, DSDV) [6; 21] и реактивные (AODV, DSR) [47] протоколы. Все они объединены общим признаком: узел обязан хранить, обрабатывать и непрерывно обновлять в оперативной памяти *структурированную таблицу маршрутов или топологическую карту сети (сетевой среды)*.

Под "табличным" обычно понимают подход, при котором решение принимается прямым поиском по заранее заданной таблице (*Lookup Table, LUT*) без ресурсоёмких вычислений в режиме реального времени – например, таблице маршрутизации, где по адресу узла назначения определяется следующий транзитный узел и выполняется соответствующий "хоп" (*Hop*)³. В FANet зависимость между общим числом узлов (N), топологической глубиной (диаметром сети – D), числом хопов (*HopCount*) и временем жизни пакета (*Time to Live, TTL*) и/или интервалом (*validity interval*) актуальности информации в пакете (на уровне приложения или метаданных полезной нагрузки) носит ограничительно-гарантирующий характер: $TTL \geq D$, чтобы пакеты могли дойти до максимально удалённых узлов. Безусловно, временной ограничитель TTL и пространственная метрика $HopCount$ должны быть разграничены в рамках рассматриваемой архитектуры. Метрика $HopCount$ фиксирует число физических ретрансляций пакета (хопов) в трёхмерном пространстве с учётом реальной геометрии расположения узлов сети (в рое) и условий радиосвязи. В свою очередь, параметр TTL в детерминированных бортовых системах *жёсткого реального времени (Hard Real-Time, HRT)* [27; 34], определяет абсолютное время

³ – шаг ретрансляции или транзитный переход [47; 51] от одного узла к другому, при котором TTL уменьшается на 1.

актуальности пакета, квантованное по тактам бортового таймера (Δt — шаг квантования), по истечении которого пакет принудительно уничтожается во избежание переполнения буферной памяти и деградации временных характеристик подсистем коммутации [18] *бортового вычислителя* (БВ) БПЛА.

Для обеспечения связности роя вводится граничное условие: временной ресурс должен гарантированно превышать максимальное время сквозной задержки транзита на всём топологическом диаметре сети (D). Время доставки по маршруту с h хопами: $T_{path} \approx h \cdot \tau_{hop}$, а условие доставки до самого дальнего узла (диаметр D): $TTL \geq D \cdot \tau_{hop}$. Избыточный TTL при этом резко увеличивает мультипликативный оверхед (*Overhead*) [43] и риски лавинной рассылки (см. далее "Концепция Б"), так как пакет необоснованно долго циркулирует в радиоэфире, генерируя паразитные дубликаты и смещая систему в точку бифуркации уравнения Ферхюльста [1; 30; 37]. Для аппроксимированной оценки сети роя можно использовать следующие эмпирические правила:

- если плотность узлов высокая и радиус радиовидимости (R) покрывает большую часть роя, то D составляет $\approx 3-4$ хопа;

- если рой пространственно "вытянут" в сублинейную структуру⁴, диаметр оценивается как $D \approx \frac{L}{R}$, где L — геометрическая длина роя, а TTL задаётся как $[D] + 1$ или $[D] + 2$. В этом случае, физическое ограничение связности для минимизации временных задержек принимает вид: $\forall_{i,j}: HopCount(i,j) \leq TTL / \Delta t$, что при крайних значениях приводит к структурному требованию $\lceil TTL / \Delta t \rceil \geq \max_{i,j} HopCount(i,j) = D$. Интеграция параметров D и N в единый контур управления осуществляется через стохастические модели пространственной связности роя.

Важно отметить, что для роя произвольной и переменной формации с переменным числом узлов топология сети является нестационарной, что обусловлено мобильностью узлов сети, вариативностью их количества $N(t)$ и внешними ограничениями среды. При этом параметры $N = N(t)$ и $D = D(t)$ зависят от времени, поэтому любые оценки, включая TTL, должны носить адаптивный характер. В такой конфигурации топологический диаметр сети $D(t)$ является нестационарной величиной, зависящей от мгновенной пространственной конфигурации и

радиуса радиовидимости $R(t)$. Соответственно, любые статические оценки (включая расчёт TTL) носят ограниченный характер и требуют периодической (t) актуализации на основе локальных метрик связности. Соответственно, для "компактных" *мгновенных конфигураций* сети роя справедлива аппроксимация $D(t) \approx 2-3$ хопа, для "вытянутых" (в том числе, сублинейных, см. выше): $D(t) \approx \frac{L(t)}{R(t)}$, где $L(t)$ — протяжённость роя в момент времени (t). Значение TTL при этом целесообразно поддерживать адаптивным: $TTL(t) = [D(t)] + \delta$, где $\delta \in \{1,2\}$ — запас на флуктуации топологии.

Примечание: Алгоритмические ограничения табличных подходов при масштабировании сети.

Вычислительная сложность процедур поиска, обновления и верификации записей в распределённых таблицах маршрутизации в условиях высокой плотности узлов составляет в лучшем случае $O(\log N)$, а при возникновении коллизий хэширования — $O(N)$ или $O(N^2)$. Вследствие экстремальной пространственной динамики роя БПЛА при выполнении полётного задания, изменения состава группировки, воздействия ВДФ и помеховой обстановки в целом, графы и таблицы топологии роя, сформированные в момент $(t-1)$ *перманентно утрачивают актуальность* [5; 9]. CPU БВ переходит в непрерывный ресурсоёмкий цикл пересчёта маршрутов, что вызывает вычислительную деградацию и исчерпание ресурса узла. При этом объём паразитного служебного трафика, расходуемого на синхронизацию топологических данных (пакеты маршрутизации (Hello, RREQ, RREP), передаваемые в кадрах канального уровня), возрастает экспоненциально. Это порождает вторичный широкоэвентуальный шторм (BS) [24] на сетевом уровне, приводя к лавинообразному падению полезной пропускной способности и нарушению временного детерминизма (HRT, см. в [27; 34]). Особенностью кадров, как единиц канального уровня (L2), в MANet (см. [14; 38]) является *MultiHop* доставка: кадр не обязательно идёт напрямую к конечному получателю: каждый промежуточный узел принимает кадр на L2, проверяет CRC, извлекает полезную нагрузку и (если узел не конечный получатель) заново формирует L2-

кадр для следующего хопа, часто с новым MAC-адресом получателя (MAC следующего хопа) —

⁴ — имеется ввиду пространственное распределение, при котором БПЛА выстраиваются вдоль доминирующей оси,

образуя, как правило, структуру типа "разомкнутой цепочки" или "эшелонированной линии".

из-за мобильности узлов сети роя и быстрой смены топологии. В MANet канальный уровень отвечает не только за кадрирование, но и за управление доступом к радиоканалу (например, CSMA/CA), используя кадры с флагами *спящего режима* или с временными параметрами *пробуждения*. Это позволяет снизить энергопотребление БЛА (узлов сети), но усложняет структуру кадра и логику обработки.

В роевых сетях кадры дополнительно могут нести поля для синхронизации времени, пространственных координат, идентификаторов роя и/или параметров ретрансляции (например, коэффициент $\beta(t)$ в (3) для адаптивной лавинной маршрутизации, см. раздел 3.3.2). Это помогает реализовать детерминированные схемы доставки и предотвращать штормы трафика.

Концепция Б. Динамика нестабильного распределения трафика в стохастических и детерминированных средах (лавинные и эпидемические подходы).

Данные подходы представляют собой два различающихся класса нестабильных протоколов распределения информационных потоков, обладающих специфическими принципами функционирования, граничными условиями применимости и особенностями аппаратно-программной реализации (средствами ПЛИС):

1. Лавинная маршрутизация (Flooding Routing и Avalanche-like dissemination).

Физический принцип. Базируется на детерминированном механизме широковещания, при котором каждый транзитный узел сети принудительно ретранслирует полученный пакет всем доступным в пределах радиуса радиовидимости (R) соседним узлам, за исключением узла-отправителя.

Функциональные особенности. Полностью исключает необходимость предварительного построения и хранения таблиц маршрутизации в памяти БВ. В условиях высокочлотных роев данный подход порождает экспоненциальный мультипликативный оверхед вследствие неконтролируемого дублирования пакетов в общем радиоэфире.

Область применения. В сетях класса FANet лавинный метод используется для трансляции широковещательных запросов, экстренного оповещения и координационной телеметрии

БИНС в режиме HRT [27; 34]. Кроме того, благодаря задействованию всех физически доступных траекторий в трёхмерном пространстве (воздушном рабочем объёме при выполнении полётных заданий роя), лавинная маршрутизация используется при верификации и сравнительном тестировании различных сетевых протоколов.

Преимущества: Вычислительная простота реализации алгоритма на аппаратном уровне (порядок сложности $O(1)$) и высокая живучесть (надёжность доставки), сохраняющаяся при масштабной деструкции и выходе из строя значительной части узлов группировки.

2. Эпидемическая маршрутизация (Epidemic Routing).

Физический принцип. Данная концепция как стохастическое обобщение лавинной доставки данных (flooding) ориентирована на *частично связанные беспроводные среды* – Delay-Tolerant Networks (DTN), см. в [25; 29]. Само понятие Epidemic Routing (ER) было введено в работах А. Вахдата и Д. Беккера [55], которые одними из первых описали распространение данных в нестабильных сетях с помощью аппарата математической эпидемиологии в виде модели **SI / SIR (Susceptible – Infected – Recovered)** [2; 29; 55]. Данный подход получил развитие у З. Хааса и Т. Смолл, применивших SIR-модели к анализу DTN-сетей, расширив базовую модель до *Shared Wireless Infestation Model (SWIM)* [31; 52]. Причём, если в своём (базовом) подходе А. Вахдат и Д. Беккер опираются на стохастические модели попарных контактов, то дальнейшее развитие ER-концепции объединило SIR-модели с аппаратом стохастической геометрии – точечными процессами, случайными геометрическими графами и теорией перколяции [10; 26].

Используем адаптацию модели SIR для описания динамики нагрузки в беспроводной сети роя: состояния S , I , R интерпретируются применительно к пакетам, что позволяет формализовать переход узлов между режимами низкой, повышенной и пиковой нагрузки в зависимости от доли пакетов в состоянии активной обработки. Обозначим подмножества узлов, соответственно:

- *Susceptible* (S), готовые к приёму и ретрансляции транзитного пакета. Такие узлы находятся в состоянии S , если уникальная хэш-сигнатура данного пакета не зарегистрирована в локальной структуре кэша истории;

- *Infected (I)*, осуществляющие физическую передачу (излучение) пакета в общий радиоэфир в текущий дискретный момент времени;
- *Recovered (R)*, успешно завершившие обработку пакетов и принудительно заблокировавшие их повторную ретрансляцию (по системному таймеру или по достижении граничного лимита счётчика).

В этой модели узел осуществляет трансляцию пакета не всем, а лишь случайно выбранному подмножеству встреченных соседних узлов с регулируемой вероятностью (β), зависящей от текущей нагрузки, коэффициента ретрансляции $\beta(t)$ и порога лавинной рассылки. Динамика переходов и их физический смысл может быть описана как: *поступление* пакета в активную обработку ($S \rightarrow I$), *завершение* обработки пакета ($I \rightarrow R$) и *обратный переход* – повторная постановка в очередь (*retransmission*), которую можно трактовать как возврат в S или "повторное заражение" (в модификации *SIRS*).

Функциональные особенности. В отличие от детерминированного широковещания (D-Broadcast), ER вводит вероятностное ограничение, которое трансформирует лавинный рост дубликатов (шторм) в контролируемый диффузионный процесс. Приращение избыточного трафика в канале описывается нелинейным дифференциальным уравнением логистического роста Ферхюльста [28; 30; 31; 37], где скорость генерации дубликатов тормозится по мере естественного насыщения среды.

Область применения. Перспективные децентрализованные системы управления роением, функционирующие в условиях интенсивного маневрирования, геометрического затенения антенн, внешнего электромагнитного и радио-электронного воздействия. Модификация эпидемического подхода путём внедрения аппаратного ПИД-регулятора (на ПЛИС, см. [12; 39]) позволяет динамически изменять параметр (β) в реальном времени, обеспечивая баланс между связностью сети и сохранением энергетического ресурса бортовых батарей БПЛА [9; 44].

В нетабличных стохастических протоколах маршрутизации (классов *Epidemic/Gossip* [31]) параметр TTL выступает ключевым регулятором времени жизни пакетов в сети, ограничивая их избыточное распространение и время хранения в буферах узлов. Ранее выведенное структурное требование $[TTL/\Delta t] \geq D$ гарантирует доставку сообщения на максимальное удаление (в хопах).

Однако, появление избыточного временного зазора: $\Delta\tau_{excess} = [TTL / \Delta t] - D > 0$ порождает физический феномен бесконтрольной генерации паразитного оверхеда (см. в [43]).

Примечание: существующие подходы по реализации основных нетабличных методов, опирающихся на хэш-функции имеют ряд особенностей и приведены в Таблице 1:

- маршрутизация на основе вероятностных хэш-структур (*Bloom Filters*) [18; 49];
- географическая хэш-маршрутизация без таблиц (*Geo-Hash Routing*);
- хэширование источника / маршрутизация от источника (*Source Routing* с хэш-метками);
- метод направленной рассылки с хэш-кэшированием (*Epidemic / Implicit Routing*) часто применяется в служебных радиосетях и сетях с большими задержками (DTN) с нестабильной топологией и частыми разрывами соединений.

Таблица 1 – Примеры нетабличных методов

Метод Routing	Замена классической таблицы	Роль хэш-таблицы / хэша
Bloom Filter	Битовые векторы (маски) на портах.	Хэширует адрес для проверки битов "да/нет", позволяет радикально сократить объём памяти.
Geographic Hash	Координаты пространства / Сетка.	Хэширует ID узла в точку на карте.
Source	Заголовок самого пакета.	Хэш-метка в пакете указывает физический порт.
Epidemic/Implicit	Кэш уникальных сигнатур (идентификаторов) пакетов.	Хэш пакета защищает радиоэфир от заикливания.

Концепция В. Контентно-ориентированные методы дедупликации и их модификации.

Для преодоления ограничений базовых схем дедупликации в части их применимости в динамических роевых сетях, нами рассматривается авторская концепция гибридного расширения контентно-ориентированных методов (*Content-Based Methods, CBM*) – схем и механизмов маршрутизации, где решения (об обработке пакетов) принимаются на основе анализа содержимого (криптографического хэша полезной нагрузки, либо иных семантических признаков и метрик), а не только заголовков или топологии, что должно повысить устойчивость сети. Примерами используемых нами контентно-зависимых подходов являются: фильтрация по семантике контента, адаптивная ретрансляция по значимости, семантическое объединение отчётов, контентно-зависимое разбиение потока, приоритезация на основе типа контента.

Для определения нашего подхода введём терминологическое обозначение – *Content-Based Remote Duplicate Elimination* (CB-RDE). В рамках подхода механизм Remote ориентирован на устранение дубликатов между удалёнными узлами, не только на уровне отдельного узла сети, а целевая функция Duplicate Elimination заключается в исключении избыточных копий данных с целью снижения нагрузки на радио-канал и экономии энергетических ресурсов сети.

1. *Функциональные аналоги нетабличных, контентно-ориентированных подходов.* Анализ выбранных нами подходов данного класса актуализируется в [58], в которой авторами подчеркивается, что связь в сети (рое БпЛА) сопряжена с высокой задержкой, энергопотреблением, ограничениями ресурсов и сбоями каналов связи. Там же указывается, что управление контентом становится серьёзной проблемой, но при этом обнаружение и распространение контента на основе ICN (*Information-Centric Networking*, ICN) [58] не получило широкого распространения в сетях с БпЛА. Поэтому, в работе обосновывается вариант решения проблемы оптимизации трафика как совместной задачи переадресации и планирования потоков с использованием модели распределения очередей *M* и предлагается эвристическое решение для распределения трафика между узлами, а эффективность решения по оптимизации оцениваются аналитически.

Вместе с тем, следует отметить, что именно контентно-ориентированный подход является актуальным для *гетерогенного* роя, в котором, несмотря на физическое "сетевое равенство" одноранговых узлов "плоской сети", существуют как ролевые, так и иные контентные приоритеты (метрики), необходимые для прямого выполнения полетного задания. Таким образом, в сетевой архитектуре роя нами в совокупности учитывается, что для малых и средних БпЛА (SWAP) в условиях интенсивного воздействия ВДФ важны решения, обеспечивающие:

- окно дедупликации (по времени/ количеству пакетов), чтобы хэш-таблица (*Hash Table*) не росла условно "бесконечно";

- ограничение длины сигнатур (короткие хэши экономят полосу, но увеличивают риск коллизий);

- кросс-уровневая интеграция: сигнатуры и политики могут формироваться на прикладном уровне, а применяться на канальном/сетевом.

Поэтому в нашей работе подходы, ориентированные на условия применения БпЛА в рое, сгруппированы и обозначены как *контентная дедупликация* – как методы удалённого устранения избыточности на основе анализа контента: RDE / CB-RDE и контентно-зависимого устранения избыточности и дедупликации – *Content-Based Redundancy Elimination and Deduplication* (CB-RED), см. в [14; 33; 42]. В RDE / CB-RDE узел вычисляет сигнатуру (хэш) полезной нагрузки: если такая сигнатура уже встречалась в окне дедупликации, то повторная передача подавляется. Это критично в роях БпЛА при лавинной/эпидемической рассылке.

В рамках метода *Counter-Based Broadcast with Self-Determination* (CB-BSDB) выполняется не только "удаление дублей", но и осуществляется разделение потоков по признакам контента (типу данных: телеметрия, команды, видео) и одновременно устраняется избыточность. Это эффективно в гетерогенных FANet сетях, где разные типы трафика требуют разной политики ретрансляции. Соответственно, чтобы не отправлять запросы flood-методом в радиосреду, реализуемая здесь логика *распределённых* хэш-таблиц – DHT (*Distributed Hash Table*, DHT) объединяется с физической маршрутизацией.

В рамках данного подхода ключевым идентификатором служит уникальная хэш-сигнатура (свёртка) самого содержимого блока данных, инвариантная к его имени или положению. Логика функционирования основана на сравнении контента через пороговые правила:

- а) вычисляется уникальный хэш от содержимого транзитного пакета;

- б) осуществляется ассоциативный поиск хэша в локальной таблице истории транзита;

- в) при обнаружении совпадения пакет классифицируется как избыточный дубликат и принудительно сбрасывается.

Хэш-таблица (*Hash Table*) [22; 57] здесь выполняет роль динамического индекса и хранилища состояния, а не классической таблицы решений. Однако программная реализация концепции CB-RDE может быть иметь серьёзный недостаток: при масштабировании роя БпЛА и интенсивном трафике объёмы таблиц истории сигнатур разрастаются экспоненциально, требуя значительных ресурсов оперативной памяти и непроизводительных циклов процессора БВ

(CPU) для очистки устаревших записей по алгоритмам вытеснения данных из кэша.

2. *Схемы широковещения на основе счётчиков (Counter-Based Broadcast Scheme)*. Исторически, концепция применения пороговых значений (*Thresholds*) – C_{th} для купирования BS и предотвращения эффекта лавины возникла применительно к беспроводным сенсорным сетям (*Wireless Sensor Networks, WSN*) [15; 33; 35; 53; 60]. Данный подход позволяет смежным (достижимым за 1 хоп) сетевым узлам первыми ретранслировать пакет и искусственно повысить значение его локального счётчика дубликатов, в результате чего энергодефицитный БпЛА легитимно уничтожает пакет в буфере и экономит заряд батареи на излучение радиосигнала. При этом можем отметить, что:

а) *Статические пороги (мягкие и жёсткие)* были впервые системно внедрены в специализированных иерархических протоколах TEEN (*Threshold sensitive Energy Efficient sensor Network protocol*) и APTEEN [14; 44]. Бортовые узлы блокировали отправку избыточных данных на верхний уровень, если текущее значение измеряемого физического параметра не превышало заданный предел [36; 45].

б) *Адаптивные / динамические пороги (Adaptive / Dynamic Thresholds)*. В контексте лавинного распространения данных (на базе протоколов типа *Directed Diffusion*) концепция⁵ динамического изменения порога [9] в зависимости от загрузки сети и уровня коллизий начала активно разрабатываться в 2010–2015 гг.

Например, в работах [42] предложена динамическая версия DCB (*Dynamic Counter Based, DCB*) – пороговое значение счётчика адаптируется под локальную плотность и мобильность узлов. В отличие от статических схем, такой подход позволяет находить баланс между подавлением шторма и сохранением связности в условиях быстро меняющейся топологии FANet, что согласуется в нашей концепции с коэффициентом ретрансляции $\beta(t)$, см. далее в разделе 3. Соответственно, схема на основе адаптивного счетчика [14; 42] может сократить количество повторных рассылок и, следовательно, снизить вероятность конфликтов и столкновений между соседними узлами.

Предложенный механизм селективной ретрансляции в рамках схемы CB-BSD реализует

принцип адаптивного подавления избыточных передач, аналогичный DCB подходам, но на детерминированной основе: решение о ретрансляции принимается по жёстким *пороговым правилам*, вычисляемым на основе локальных метрик (счётчик дубликатов, плотность соседей, включая радиоблизость [7; 8], интенсивность трафика и др.). Аппаратная поддержка обеспечивает детерминированные задержки и предсказуемое время обработки, что критично для систем жёсткого реального времени (HRT).

Хотя по своей физической сути классические реализации методов удалённого устранения избыточности (DCB) основаны на нетабличном принципе фильтрации контента, для практической верификации дубликатов транзитный узел должен использовать программную хэш-таблицу. В данном контексте Hash Table выступает исключительно в качестве динамического индекса для ускорения ассоциативного поиска, а не структуры, жёстко детерминирующей правила маршрутизации [22; 32; 57].

Однако при масштабировании беспроводной сети в диапазоне высокой плотности и интенсивном межэлементном трафике объёмы хэш-таблиц истории транзита разрастаются экспоненциально. Это генерирует критическую паразитную нагрузку на оперативную память БВ и непроизводительно расходует тактовые циклы CPU на выполнение процедур поиска и очистки устаревших записей по алгоритмам кэш-вытеснения, нарушая SWaP-ограничения роя.

Примечание: алгоритмы, использующие C_{th} изначально реализовывались программным способом на уровне операционной системы и оперировали табличными структурами хэшей. Однако в условиях переменного состава и масштаба роя БпЛА, интенсивного ВДФ [5; 9] или при дефиците бортовой вычислительной мощности узлов классические программные хэш-таблицы с динамическим распределением памяти порождают недетерминированную системную задержку (*Phase Lag*, см. Таблицу 2). Данный сбой детерминизма обусловлен необходимостью программного разрешения коллизий хэш-функций и ресурсоемким управлением памятью при вытеснении данных из кэша.

⁵ – см. исследования систем динамического load-balancing в беспроводных сетях: Lai W., Lin Y.C. и др. [36; 41; 53].

Таблица 2 – Математическая оценка системных параметров алгоритмов маршрутизации

Концепция/ Метрика	Слож- ность по памяти	Временная сложность обработки	ROH канала связи	Зависи- мость задержки от ВДФ
Табличная (OLSR/ AODV)	$O(N)$ — линейный рост от масштаба сети (числа узлов).	$O(\log N)$ в штатном режиме. Деградация до $O(N)$ при динамическом пересчёте графа топологии.	$O(N^2)$ — квадратич- ный рост трафика синхрониза- ции сигналь- ных пакетов (HELLO/ RREQ).	Экспоненци- альный рост задержки (из-за мас- совой поте- ри пакетов и лавинного пересчёта маршрутов).
Лавинная (Flooding)	$O(1)$ — таблицы сетевой топологии отсутствую- т.	$O(1)$ — принятие решения о ретрансляции без анализа маршрутных таблиц.	$O(\lambda \cdot N)$ — линейный рост загрузки канала копиями пакетов.	Коллапс сетевой среды (структур- ное насы- щение кана- ла связи за счёт коллизий L2-уровня).
Контентно- ориентиро- ванная	$O(M \cdot N)$ — требование к емкости кэш-памяти для хранения истории пакетов.	$O(1)$ — в штатном режиме. $O(\log M)$ — деградация до $O(M)$ при массовых коллизиях хэширования.	$O(1)$ — ROH мини- мизирован (отсутствует обмен топо- логиями).	Рост Phase Lag и джиттера из-за пере- полнения очереди и загрузки CPU.

Следует подчеркнуть, что классические подходы DCB (включая CB-BSR и RDE) не исчерпывают спектр нетабличных решений: в теоретических работах [31; 55], заложивших базис лавинного и стохастического широкополосного, рассматриваются различные модификации нетабличных протоколов, адаптируемые в настоящее время под специфику сетей роя.

3.2. Сравнительный анализ метрик
(математический и логический базис)
классического и перспективных методов

Реализация системных требований к сетям FANet переменной формации учитывает динамику топологии, при которой классические реактивные протоколы (AODV и аналоги) [47; 51] демонстрируют неудовлетворительное время сходимости. Интервал децентрализованной перестройки сквозных маршрутов при интенсивных пространственных маневрах БПЛА может составлять десятки секунд, что критично для выполнения высокоприоритетных тактических задач реального времени. В свою

очередь, проактивные протоколы (OLSR) [6; 21] в аналогичных условиях генерируют избыточный паразитный служебный трафик (ROH), приводящий к преждевременному насыщению канального ресурса.

Этот принцип предполагает сопряжение быстродействия нетабличных лавинных алгоритмов для обеспечения максимальной пространственной достижимости пакетов и адаптивных ограничителей, предотвращающих развитие BS и минимизирующих мультипликативный оверхед.

В контексте верификации параметров сетевых протоколов и систем удаленного устранения избыточности (CB-RDE), временная сложность процедур ассоциативного поиска дубликатов в классических хэш-таблицах истории транзита составляет в лучшем случае $O(\log N)$, а при возникновении коллизий хэширования деградирует до линейной $O(N)$ [18; 43].

3.2.1. Временная и пространственная
сложность сетевого стека

Пусть N – число узлов в рое, λ – интенсивность генерации пакетов одним узлом, а M – средний размер истории пакетов для контроля контентной избыточности. Параметры временной и пространственной сложности сетевого стека являются индикаторами непрерывности и эффективности сетевого обмена (таймингов).

В зависимости от выбранной архитектуры организации кэш-памяти БВ, показатели временной сложности процедур поиска и верификации дубликатов распределяются следующим образом:

- временная сложность $O(\log M)$ возникает, когда система последовательно упорядочивает идентификаторы (хэши) ранее полученных пакетов в виде графа, где переменная M определяет текущее количество записей в динамическом буфере устаревания пакетов;

- временная сложность $O(M)$ соответствует режиму катастрофической вычислительной деградации алгоритма при возникновении коллизий хэширования, что соответствует классическим хэш-таблицам (Hash Table со связными списками), которые изначально проектировались под константную скорость $O(1)$. Однако в условиях высокой плотности трафика и наложения хэш-функций они неизбежно деградируют до линейного уровня сложности от размера истории M [18; 22; 49].

Примечание:

1. Вычислительная деградация контентно-ориентированных алгоритмов происходит в условиях надкритической интенсивности трафика группировки и/или при деструктивном воздействии ВДФ [5; 9; 44], что приводит к ускоренному переполнению памяти, насыщению индексных структур и лавинообразному росту числа коллизий хэш-функций.

2. Механизм деградации временной сложности от уровня $O(1)$ до $O(M)$ активизируется, когда хэш-функция генерирует идентичные индексы для различных уникальных сигнатур пакетов. Вычислитель вынужден [27; 34] осуществлять последовательный перебор всех m элементов коллизийной цепочки хэш-таблицы $m \leq M$ для верификации уникальности поступающего пакета, что разрушает временной детерминизм функционирования системы реального времени.

3. В протоколах маршрутизации (OLSR/AODV) [21; 57] деградация при поиске пути возникает при одновременном выполнении двух условий: задержка обработки пакетов в узле достигает $O(N)$, и CPU не успевает обслуживать служебные запросы (управляющие сообщения Hello, RREQ, RREP).

Превышение тайм-аута приводит к маркировке узла как потерявшего связность и запускает лавинообразный пересчёт маршрутов, провоцируя коллизийный коллапс среды доступа. В алгоритмах концептуального типа (CB-RDE) для освобождения скользящего окна истории применяют алгоритмы FIFO или LRU (*Least Recently Used*, LRU). Однако, в FANet они неэффективны, FIFO преждевременно вытесняет хэш-сигнатуры пакетов, участвующих в скрытых петлях [57], что порождает повторную обработку дубликатов, а LRU при высокой плотности нагрузки вызывает деградацию CPU БВ в результате ресурсоёмкой перестройки индексов.

4) В сетях FANet дубликатом считается копия информационного пакета, идентификация которой БВ осуществляется на основе полного совпадения уникальной хэш-сигнатуры контента либо данных полезной нагрузки прикладного уровня. Качество обслуживания (QoS/QoE) в сетевом стеке роя БпЛА оценивают по кросс-уровневой матрице весов (модель OSI):

- *прикладной уровень* (L7) – степень деградации, актуальности или точности транслируемых целевых данных (телеметрии, видео-поток).

- *сетевой уровень* (L3) – фактическое число пройденных пакетом транзитных участков (*HopCount*), остаточный временной ресурс (*TTL*), а также общую топологическую стабильность сквозного маршрута;

- *канальный и физический уровни* (L1–L2) – отражает остаточный заряд батареи (SOC) как транзитного узла, так и инициировавшего ретрансляцию дубликата [9; 15, 44].

Таким образом, деградация вычислительной сложности до $O(M)$ или $O(N)$ служит критическим критерием эффективности радиосети роя БпЛА и отражает верхний предел её устойчивости. Второй ключевой уязвимостью радиосети роя БпЛА является пространственная сложность сетевого стека, которая прямо детерминируется объёмом памяти, требуемым для хранения топологических карт и таблиц истории сигнатур.

3.2.2. Пространственная сложность $O(N)$ – ресурсный риск кэширования

Вычислительная уязвимость алгоритмов LRU (процессорная деградация). Уязвимость алгоритма LRU обусловлена процессорной деградацией: при каждом приёме пакета CPU вынужден динамически перестраивать указатели, индексы или списки таблицы истории. При надкритической интенсивности трафика и воздействии ВДФ накладные расходы на поддержание упорядоченности структуры LRU приводят к критическому истощению ресурса CPU, что нарушает работу ключевых бортовых сервисов роя.

Линейный рост пространственной сложности $O(M)$ выступает дополнительным ограничением систем дедупликации класса RDE [18]: объём требуемой памяти линейно зависит от *глубины окна истории* M . Эта зависимость $O(M)$ формирует системное ограничение. В условиях жёстких ограничений по массе, габаритам и энергопотреблению (SWaP) у БпЛА лёгкого и среднего классов хранение растущих массивов хэш-сигнатур ведёт к исчерпанию дефицитных ресурсов памяти. В этом направлении, нами предложено аппаратно-архитектурное решение [12], снижающее кросс-уровневую сложность и преодолевающее программные ограничения. Оно предполагает перенос логики сигнатурного анализа в аппаратный конвейер ПЛИС с использованием энергоэффективной памяти (BRAM / URAM) в связке с параллельными

фильтрами Блума, что гарантирует достижение константной сложности вычислений $O(1)$ [18; 49]. Такой подход обеспечивает повышенные требования к информационной безопасности [61], аппаратному детерминизму таймингов (HRT) и гибкости БВ, что актуально для защищённых радиосетей FANet.

3.3. Оценка эффективности протоколов маршрутизации на основе математического описания RОН и эпидемического шторма

3.3.1. Интенсивность служебного трафика при проактивной маршрутизации

Для сравнительного анализа эффективности нетабличных, лавинных и топологических алгоритмов маршрутизации необходимо формализовать аналитическую величину оверхеда [43] – нагрузки, которую протоколы создают в физическом канале передачи данных. Пусть N — число активных узлов, λ — средняя интенсивность генерации уникальных пакетов прикладного уровня каждым узлом (пакетов/с). Тогда интегральная интенсивность полезной нагрузки в сети $\Lambda_0 = N \cdot \lambda$.

1) В табличных проактивных протоколах (типа OLSR) служебный трафик определяется периодической генерацией и рассылкой пакетов актуализации топологической карты (сообщений типа *Hello* локального зондирования смежности и ТС-сообщений (*Topology Control*) глобального распределения векторов путей). В худшем случае (соответствующем топологии полно-связного или высокоплотного КД), суммарный битрейт служебной нагрузки (бит/с) аппроксимируется зависимостью от пространственного масштаба сети:

$$\Lambda_{overhead}^{OLSR} = N \cdot (F_{Hello} \cdot L_{Hello} + F_{TC} \cdot K_{MPR} \cdot (N - 1) \cdot L_{TC}) , \quad (1.1)$$

где F_{Hello} и F_{TC} — фиксированные частоты генерации служебных пакетов Hello и ТС; K_{MPR} — коэффициент, отражающий долю узлов, назначенных в качестве MPR-ретрансляторов; L_{Hello} и L_{TC} — средняя длина пакетов Hello и ТС; N — число узлов. При больших значениях N доминирующей становится квадратичная составляющая, обусловленная трафиком ТС-сообщений. В этом случае интегральный оверхед проактивного сетевого стека допустимо аппроксимировать квадратичной функцией:

$$\Lambda_{overhead}^{OLSR} = \omega \cdot N^2 , \quad (1.2)$$

где ω — интегральный коэффициент (бит/с), агрегирующий параметры протокола (F , L , K) и

определяемый аппаратными параметрами радиотракта, профилем настроек таймеров и топологическими характеристиками сети [2; 32].

2) В лавинных (Flooding) и эпидемических Epidemic) протоколах маршрутизации RОН выражается не в процедурах циклического обмена таблицами топологии, а в неконтролируемом размножении копий одного и того же пакета в общем радиоэфире. В лавинном протоколе интенсивность дублирования определяется локальной степенью узла, то есть количеством его ортогональных соседей (d). В работах [45; 55] по ER лавинообразное размножение копий пакетов описывается стохастическими или дифференциальными уравнениями типа SI/SIR.

Для аналитической оценки эффективности существующих и перспективных нетабличных протоколов в условиях высокоплотных децентрализованных сетей FANet разработано обобщенное математическое описание RОН канала связи. В условиях динамического изменения топологических связей, отсутствие механизмов контроля контентной избыточности переводит сеть состояние BS.

Для математического описания первопричин КВИТ в сети роя нами использован аппарат теории *ветвящихся процессов* (ВП) — модель Гальтона–Ватсона [20], где в качестве детерминированной аппроксимации среднего поведения ВП. Суммарный поток пакетов в КД при условно неограниченном росте числа узлов сети (N_{max}) выражается как:

$$\Lambda_{overhead}^{Epidemic} = \Lambda_0 \cdot \prod_{j=1}^M d_j , \quad (2.1)$$

где Λ_0 — исходная интенсивность уникального трафика прикладного уровня, генерируемого узлом-источником (пакетов/с); d_j — локальный коэффициент мультипликации дубликатов (математическое ожидание коэффициента ветвления на j -м шаге ретрансляции, функционально зависящий от плотности); M — максимальная топологическая глубина ветвления (число хопов). В более общем виде:

$$\Lambda_{overhead}^{Epidemic} = \Lambda_0 \cdot \mu^M \cdot L_{pac} , \quad (2.2)$$

где μ — средний коэф. ветвления, зависящий от локальной плотности ($N_{neighbor}$), стратегии ретрансляции и временного зазора $\Delta\tau_{excess}$; $M = \min(D, \lceil TTL / \Delta t \rceil)$ — предельная (верхняя граница) глубина ветвления, ограниченная диаметром сети D и временем жизни пакета; L_{pac} — средняя длина пакета (бит). При $\mu > 1$

наблюдается экспоненциальный рост RON , что соответствует режиму коллизионного насыщения среды BS.

Примечание: С ростом масштаба сети диаметр графа роя демонстрирует сублинейный рост и асимптотически стремится к верхней границе, определяемой как $O(\log N)$. При увеличении числа узлов N в растущем рое диаметр графа перестает быть абстрактной величиной и жёстко ограничивается физическими параметрами: значением TTL и максимальной пропускной способностью канала I_{max} . При однородной плотности сети произведение $\prod_{j=1}^M d_j$ можно аппроксимировать как $\bar{d}^M$. Условие $\bar{d} > 1$ соответствует режиму КВИТ, поэтому для устойчивой работы сети необходимо поддерживать $\bar{d} < 1$.

Выводы по модели. Модель ВП показывает, что структурно-топологические свойства FANet являются первопричиной лавинного роста нагрузки на канальном уровне (L2) при отсутствии механизмов контроля избыточности. Оба протокола при масштабировании роя БпЛА приводят к коллизионному коллапсу общего радиоэфира, при котором полезная пропускная способность $I_{success}$ (интенсивность успешно доставленных уникальных пакетов) снижается до ничтожно малых значений.

Таким образом, выражение (2.2) можно представить как математическую модель КВИТ, которая описывает критический режим функционирования транспортной среды (сети) роя БпЛА при неконтролируемом эпидемическом распространении пакетов. Возникающий при этом эффект комбинаторного взрыва в децентрализованной высокоплотной сети роя БпЛА – это эмерджентный надкритический режим функционирования системы, при котором мультипликативное размножение дублирующих и устаревших пакетов в разделяемой среде передачи данных порождает сочетанную избыточность сетевого трафика (RON) и вычислительных процессов транзитных узлов. Механизм данного состояния обусловлен лавинообразным ростом числа альтернативных маршрутов ретрансляции в динамическом графе сети роя, что приводит к экспоненциальному насыщению радиоканала и переполнению приёмных буферов MAC-уровня.

На вычислительном уровне комбинаторный взрыв выражается в виде паразитного шторма прерываний, при котором процессор БпЛА вынужден непроизводительно расходовать

критический вычислительный ресурс на парсинг заголовков, десериализацию, верификацию контрольных сумм, а также фильтрацию идентичных или устаревших копий пакетов. Это приводит к блокированию приоритетных потоков бортовой операционной системы реального времени и влечёт за собой системный отказ контура управления полетом (Таблица 1).

На базе модели КВИТ обосновывается необходимость кросс-уровневых механизмов адаптивного ограничения ретрансляций.

Ключевая цель таких механизмов – обеспечить условие $\bar{d}^M \leq 1$ при заданной плотности роя и топологической глубине M , тем самым подавляя избыточные ретрансляции без потери связности сети. В частности, пороговые правила схем селективной ретрансляции (CB-RDE, CB-BSD) должны выбираться так, чтобы $\bar{d}$ оставался ниже критического ($\bar{d} < 1$). Это переводит неконтролируемый ветвящийся процесс в устойчивый режим и предотвращает коллизионный коллапс канала.

Реализация адаптивного управления может опираться на локальные метрики и включать контуры обратной связи – так например, применение ПИД-регулятора может быть одним из возможных способов динамической подстройки порогов (C_{th}) в реальном времени.

3.3.2. Модель комбинаторного взрыва избыточного трафика

Проблема возникновения BS в беспроводных ad-hoc средах была системно проанализирована в фундаментальной работе Ни С.-И. и др. [45], где были выделены три основные составляющие понятия "шторм" [24]: избыточные приёмы (*redundant receptions*), массовые коллизии (*collisions*) и конкуренция узлов за разделяемую среду (*contention*).

Для описания критических режимов жизни сети роя нами разработана модель КВИТ, которая базируется на модификации операторов стохастической эпидемиологии SIR (см. раздел 3.3.1.) и математическом аппарате нелинейной динамики канального уровня (L2). Необходимо разграничивать физическую сущность процессов: лавинное затопление представляет собой реальный физический процесс распределения потоков в радиоэфире, в то время как эпидемическая SIR-модель выступает математическим базисом его аппроксимации. Классические SIR-модели в сетях связи традиционно использовались для абстрактного описания диффузии информации в "чистой

среде" без учёта ёмкостных ограничений буфера. Как следствие, они не учитывают физику пакетных коллизий, динамические барьеры порогов, деструктивный помеховый фон, и не связывают эпидемический взрыв трафика с аппаратными ограничениями БВ.

Представим топологическую структуру сети связи децентрализованной группы БПЛА как динамический неориентированный граф связи $G = (V, E)$, где $G(t)$ — текущая интенсивность трафика определяющая нагрузку на канал в момент t ; V — множество узлов численностью $N = |V|$, а E — стохастических радиоканалов, определяемых мгновенной зоной радиопокрытия и условиями распространения сигнала в трёхмерном пространстве. Средняя степень связанности графа (математическое ожидание числа соседей в зоне радиопокрытия узла) определяется величиной k , которая для роя БПЛА является пространственно-динамической функцией и зависит от плотности группировки, высоты полёта, рельефа местности и геометрии диаграмм направленности бортовых антенн.

1. Уравнение лавинного затопления в условиях ёмкостных ограничений среды. Инициирование передачи уникального пакета хотя бы одним узлом децентрализованной сети порождает диффузионный процесс распространения данных, в котором суммарная интенсивность трафика (пакетов/с) для i -го узла, описывается как: $\sum(I_{\text{gen},i} + I_{\text{retx},i})$ — это прямая нагрузка на радиоканал. Для оценки динамики лавинно-образного роста трафика нами применяется математическая модель [1], аналогичная логистической модели Ферхюльста [37]. В этом процессе лавинообразный рост трафика происходит не за счёт генерации узлами новых (уникальных) пакетов, а за счёт повторной ретрансляции (ReTx) одного и того же пакета соседним узлам. Соответственно в контексте негативных эффектов, влияющих на состояние сети, доминирующим является I_{ReTx} . Представим интенсивность ретрансляции пакетов в сети в единицу времени $I_{\text{ReTx}}(t)$ в виде нелинейного дифференциального уравнения логистического типа:

$$\frac{dI_{\text{ReTx}}(t)}{dt} = \beta \cdot k \cdot I_{\text{ReTx}}(t) \cdot \left(1 - \frac{I_{\text{ReTx}}(t)}{I_{\text{max}}}\right), \quad (3)$$

где β — коэф. стохастической ретрансляции пакета каналным уровнем вычислителя; k — средняя степень связанности графа (среднее число соседей); t — локальное время узла (в среднем по рою); I_{max} — предельно допустимая

интенсивность потока пакетов в разделяемой среде (пакетов/с), определяемая ёмкостью КД.

В условиях высокоплотной сети роя с числом узлов N и пропускной способностью канала C (бит/с), данный предел аппроксимируется как: $I_{\text{max}} = \frac{C}{L_{\text{pac}} \cdot N}$, где L_{pac} — средняя длина пакета (бит). Таким образом, I_{max} учитывает как физические ограничения радиоканала, так и масштабируемость сети роя БПЛА (N).

Уравнение (3) предопределяет логистическую динамику лавинного процесса (2): на начальном этапе возникновения BS при выполнении условия загрузки канала $I_{\text{ReTx}}(t) \ll I_{\text{max}}$ нормирующий множитель $\frac{1 - I_{\text{ReTx}}(t)}{I_{\text{max}}} \rightarrow 1$. В этом режиме система переходит в состояние, математически описываемое экспоненциальным характером роста:

$$I_{\text{ReTx}}(t) = I_0 \cdot e^{\beta \cdot k \cdot t}, \quad (4.1)$$

где I_0 — начальная интенсивность инъекции ретрансляционного трафика; β — коэффициент стохастической ретрансляции; k — параметр, характеризующий локальную плотность узлов в КД; t — время циркуляции пакета в радиосети.

Из выражения (4.1) следует, что на ранней стадии рост интенсивности носит экспоненциальный характер и зависит от локальной плотности (k) и времени циркуляции пакетов. Предельное выражение (4.2), доказывает принципиальную неустойчивость чистых лавинных протоколов в высокоплотных роях БПЛА и служит обоснованием необходимости введения адаптивных кросс-уровневых механизмов ограничения ретрансляций:

$$\lim_{k \rightarrow (N-1), t \rightarrow TTL} (I_0 \exp[\beta_0 \cdot k \cdot t]) =$$

$$I_0 \exp[\beta_0 \cdot (N-1) \cdot TTL]. \quad (4.2)$$

Выражение (4.2) доказывает принципиальную неустойчивость чистых лавинных протоколов в высокоплотных роях БПЛА и служит обоснованием введения адаптивных кросс-уровневых механизмов ограничения ретрансляций (в аппроксимированной модели без учёта ограничений канального уровня).

Для решения задачи стабилизации сетевой структуры нами применён замкнутый контур адаптивного управления, реализующий алгоритмический функционал ПИД-регулятора аппаратными средствами ПЛИС в логическом контуре БВ. При фиксации угрозы коллизионного коллапса (росте сигнала ошибки $e[k_{\text{pe}}]$) ПИД-

регулятор формирует управляющее воздействие $U_{PID}[k_{pez}]$, которое динамически снижает коэф. стохастической ретрансляции до минимально допустимого уровня ($\beta \rightarrow 0$). Это останавливает дифференциальный рост логистической функции ($\frac{dI_{ReTx}(t)}{dt} \rightarrow 0$). Дискретный шаг k_{pez} определяет момент времени опроса МАС-статистики, а текущий сетевой трафик $I_{ReTx}[k_{pez}]$ является результатом уравнения (3), где скорость роста лавинного процесса завязана на топологическую плотность сети (k). Текущий сигнал ошибки управления на k_{pez} -шаге определяется как $e[k_{pez}] = I_{target} - I_{ReTx}[k_{pez}]$.

В результате интенсивность трафика $I_{ReTx}(t)$ детерминировано стабилизируется на безопасном квазиконстантном уровне (I_{target}), не достигая критической точки насыщения канала I_{max} , что обеспечивает предотвращение развития BS и сохраняет связность роя БпЛА в условиях воздействия интенсивного ВДФ [5; 9; 44]. Предложенная стратегия управления позволяет удерживать сеть в докритической области, где $I_{ReTx}(t) < I_{max}$ и, тем самым, гарантировать выполнение целевых показателей QoS по задержке, доле успешно доставленных пакетов и устойчивости связности.

Этот подход согласуется с результатами работ [9; 44], где показано, что в высокоплотных MANet/FANet без механизмов селективной ретрансляции BS приводит к деградации полезной пропускной способности до пренебрежимо малых значений, а применение адаптивных политик позволяет удерживать сеть в докритическом режиме, что служит обоснованием необходимости введения механизмов ограничения ретрансляций.

2. Модель деградации МАС-уровня (учёт коллизий и внешнего зашумления радиосети).

Для комплексной оценки влияния коллизий в канале и внешнего зашумления на вероятность успешной доставки пакетов представлена эмпирическая модель, аппроксимирующая снижение пропускной способности передачи в условиях возрастающей паразитной загрузки канала. Экспоненциальное возрастание $I_{ReTx}(t)$ в реальных физических средах ограничено пропускной способностью радиоканала. Суммарная нагрузка канала определяется безразмерной величиной $G(t) = I_{ReTx} \cdot \tau$, где (τ) — длительность физической передачи одного пакета в радиоэфире: Физический смысл $G(t)$

заключается в оценке среднего числа попыток передачи, приходящихся на интервал τ , что соответствует классической трактовке предлагаемой нагрузки в теории телетрафика [4; 32]. Так, при использовании протоколов случайного множественного доступа (в качестве консервативной нижней оценки рассматривается модель типа ALOHA) реальная интенсивность успешно доставленных и обработанных бортовым CPU пакетов $I_{success}(t)$ снижается из-за возрастания коллизий и влияния помех.

Представим эту зависимость в виде эмпирической модели (5) деградации радиоканала, либо аппроксимацией вероятности успешной доставки:

$$I_{success}(t) = I_{ReTx}(t) \cdot e^{-2 \cdot G(t)} \cdot (1 - P_{PER}^{ВДФ}(t)), \quad (5)$$

где $I_{success}(t)$ — интенсивность успешно доставленных и верифицированных пакетов (пакетов/с); $P_{PER}^{ВДФ}(t)$ — интегральная оценка PER (Packet Error Rate) в условиях внешнего дестабилизирующего воздействия (ВДФ).

При $P_{PER}^{ВДФ}(t) \rightarrow 1$ мультипликативный множитель $(1 - P_{PER}^{ВДФ}(t)) \rightarrow 0$, что приводит к практически полному подавлению полезной пропускной способности.

Результаты [19] подтверждают, что в условиях высокой плотности и мобильности традиционные МАС-протоколы (включая CSMA/CA) демонстрируют резкое падение полезной пропускной способности из-за коллизий. Предложенная эмпирическая модель (5) отражает этот эффект и позволяет обосновать необходимость адаптивного контроля нагрузки с учётом следующих системных допущений:

а) зависимость $e^{-2 \cdot G}$ выбрана в качестве эмпирической аппроксимации снижения вероятности успешной передачи в условиях возрастающих коллизий, характерных для не-координированных сетей случайного доступа;

б) значение коэффициента, равное 2, подобрано для аппроксимации критических режимов функционирования механизмов CSMA/CA при околонушенных и надкритических нагрузках. Для повышения степени детерминизма модели и отражения динамики "окна конкуренции" (в CSMA/CA) базовое уравнение может быть расширено марковскими цепями класса Бьянчи [17]. Подставляя полученное ранее выражение

экспоненциального шторма (4.1) для $I_{ReTx}(t)$ в уравнение деградации MAC-уровня (5), получаем полную нестационарную математическую модель деградации транзитного узла роя БпЛА:

$$I_{success}(t) = (I_o \cdot e^{\beta \cdot k \cdot t}) \cdot \exp(-2 \cdot \tau \cdot I_o \cdot e^{\beta \cdot k \cdot t}) \cdot (1 - P_{PER}^{ВДФ}(t)) \quad (6)$$

Анализ критического предела полученной функции (6) в условиях развивающегося BS показывает системный отказ:

$$\lim_{G \rightarrow \infty} I_{success}(t) = \lim_{G \rightarrow \infty} \left[\frac{G}{\tau} \cdot \exp(-2 \cdot G) \right] \cdot (1 - P_{PER}^{ВДФ}(t)) = 0 \quad (7)$$

Анализ асимптотики показывает, что при $G \rightarrow \infty$ множитель $Ge^{-2G} \rightarrow 0$, следовательно, $I_{success} \rightarrow 0$. Это подтверждает, что без механизмов контроля ретрансляций сеть неизбежно переходит в режим коллапса, когда полезная пропускная способность стремится к нулю.

Представленные математические зависимости позволяют проиллюстрировать модель коллизионной деградации узлов сети роя БпЛА (Рисунок 1).

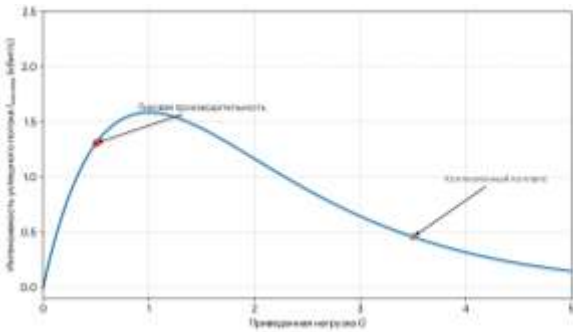


Рисунок 1 — Вид параметрического изменения системной производительности сети роя БпЛА

Полученный результат (7) находится в соответствии с положениями теории перколяции на случайных графах [10; 26]. Процесс децентрализованного лавинообразного распространения пакетов в ad-hoc буферах аналогичен связевой перколяции Бернулли с эффективной вероятностью заполнения ребер связного графа (T) [46]. Согласно данному изоморфизму, критический критерий эпидемиического порога ($k \cdot T \geq 1$) математически эквивалентен левой границе перколяционного ценза.

В условиях развивающегося коллизионного шторма ($G \rightarrow \infty$) деградация физической вероятности успешного приёма кадра ведёт к лавинообразному падению эффективной трансляционной способности связи ($T \rightarrow 0$). Это вызывает мгновенное нарушение неравенства: ($k \cdot T < 1$). В этот момент происходит фазовый переход второго рода – разрушение гигантской компоненты связности графа (*Greatest Connected Component*, GCC) [46]. Сеть распадается на изолированные кластеры, что делает общую перколяцию (установление сквозных маршрутов в FANet при превышении критической плотности узлов) пакетов – невозможной.

Таким образом, предел (7) содержательно описывает нижний РНУ/MAC-механизм верхнего топологического коллапса сети, доказывая, что топологический ценз перколяции [26] инвариантен к физической природе процессов распространения волн. Предельное выражение (7) подтверждает, что при достижении роём БпЛА критической плотности (при интенсивном забитии каналов источниками интенсивных помех [5]), неконтролируемый рост предлагаемой нагрузки $G(t)$ порождает лавинообразное увеличение числа коллизий на канальном уровне (L2) и кумулятивный рост пакетных ошибок на физическом уровне (L1).

В результате комплексного математического описания процессов в разрабатываемом стеке для алгоритма маршрутизации роя предложен трёхшаговый математический конвейер деградации сетевой структуры, описывающий механизм развития системной аварии при отсутствии адаптивных механизмов контроля:

Шаг 1. Топологический катализатор: Процесс мультипликативного ветвления в динамическом графе роя, описываемый разработанной МКВИТ через оператор произведения локальных степеней связанности $\prod d_j$, превращает единичный инжектированный пакет прикладного уровня A_o в лавину избыточных дубликатов в общем радиоэфире, стремящуюся к своему верхнему теоретическому пределу при $t \rightarrow TTL$.

Шаг 2. Динамика притока: логистическое дифференциальное уравнение Ферхюльста [1; 30; 37] принимает параметры топологического ветвления в качестве входного возмущения и определяет нестационарную скорость нарастания интегрального пакетного потока $\frac{dI_{gen}(t)}{dt}$ во времени (t) с учётом предельной физической ёмкости среды I_{max} .

Шаг 3. Коллизионный коллапс: эмпирическая деградация MAC-уровня принимает перегруженный поток $I_{ReTx}(t)$ и через коллизионную $\exp(-2 \cdot G(t))$ асимптотически устремляет полезную пропускную способность $I_{success}(t)$ до неприемлемо малых значений.

Эмпирическая модель деградации MAC-уровня принимает перегруженный поток предлагаемой нагрузки $I_{ReTx}(t)$ и через нелинейную коллизионную экспоненту $\exp(-2 \cdot G(t))$ асимптотически устремляет полезную пропускную способность $I_{success}(t)$ к нулю, что означает полную деструкцию информационного обмена в рое БПЛА под влиянием сочетанных факторов коллизий и ВДФ.

3. Границы применимости модели и кросс-уровневый ПИД-контур управления.

Представленная в работе математическая модель описывает нестационарное поведение беспроводной ad-hoc сети роя БПЛА в условиях фиксированной рабочей частоты. Подобное допущение позволяет изолированно выделить деструктивный эффект комбинаторного роста интенсивности ретрансляций без маскирующего влияния алгоритмов частотного разнесения. Полученные результаты служат нижней границей устойчивости сетевой среды и определяют граничные требования к бортовым механизмам защиты от перегрузки канала (I_{ReTx}):

- *Автономность роя:* Модель абстрагируется от наличия внешних опорных навигационных или управляющих сигналов и полностью полагается на локальные распределенные механизмы сетевого стека (аппаратные хэш-индексы, адаптивные пороговые барьеры и кольцевые счётчики класса DCB (см. в [14]).

- *Децентрализованные локальные счётчики и пороги:* Модуль ПЛИС осуществляет независимый высокоскоростной подсчёт локальных ретрансляций и применяет пороговые правила фильтрации автономно на каждом отдельном узле. Это позволяет снижать общую предлагаемую нагрузку (I_{ReTx}) в асинхронном распределенном режиме.

- *Локальная хэш-индексация контента:* Операция верификации уникальности хэш-сигнатуры транзитного пакета носит строго локальный характер. Смена макросостояний узла в рамках марковских переходов [41] (в частности, из состояния готовности к приёму (S) в состояние

блокировки дубликатов (R) модели КВИТ) осуществляется изолированно, превентивно предотвращая повторную ретрансляцию избыточного контента в общий радиоэфир.

В работах [40; 45; 50] исследованы базовые сетевые контрмеры борьбы с избыточностью (вероятностные, счётчиковые и дистанционные схемы), однако ни одна из них не обладает свойством универсальной адаптивности к динамике среды. Дальнейшие исследования, включая схемы класса *DNA-BSP (Dynamic Node-Density Based Adaptive Counter Scheme)* и их гибридные модификации развили данные концепции, однако остались в рамках эвристических подходов и эмпирического имитационного моделирования. В более поздних работах (например, в [29]) базовые подходы дополнили механизмами адаптивности – учётом ресурсов узла, что частично решает проблему статичности исходных схем.

Предлагаемая математическая модель развивает классические теоретические направления, заложенные в работах [45; 55], путём перехода от чистых эвристик к аналитической оценке критических порогов загрузки среды и аппаратной реализации детерминированных механизмов подавления широкоэмиттерного шторма. Сохраняя распределенную локальность как физический уровень исполнения алгоритмов, модель формирует правила управления, которые опираются на глобальную динамику, критические пороги и кросс-уровневое взаимодействие сетевых слоев. Разработанное аналитическое описание динамики лавинного распространения трафика (логистическое дифференциальное уравнение для $I_{ReTx}(t)$ и нелинейной деградации MAC-уровня (эмпирическая модель для $I_{success}(t)$) позволяет строго идентифицировать критический порог загрузки канала (G_{crit}). На основе данного порога формируются технические требования к бортовым механизмам адаптации на ПЛИС (БВ), задача которых заключается в удержании предлагаемой нагрузки ниже безопасного расчётного уровня: $G(t) < G_{safe}$, при котором интенсивность успешно доставленных пакетов $I_{success}(t)$ гарантированно удерживается выше минимально допустимого системного порога QoS. Аппаратная реализация алгоритмов на кристалле ПЛИС обеспечивает выполнение условия $G(t) < G_{safe}$ в режиме реального времени

(HRT, наносекундный диапазон), превентивно исключая переход сети в состояние BS.

Научная новизна предложенного конвергентного подхода заключается в замыкании бортового ПИД-контура управления платформы на внутренний параметр логистического уравнения Ферхюльста (3) — коэффициент стохастической ретрансляции $\beta(t)$.

Аппаратная модификация и подавление данного коэффициента в логических ячейках ПЛИС со стабильной константной сложностью $O(1)$ позволяют искусственно купировать дифференциальный рост генерируемого паразитного трафика: $\frac{dI_{ReTx}(t)}{dt} \rightarrow 0$ что полностью предотвращает переход эмпирической модели деградации канала в область коллизионного коллапса физической среды обмена данными.

3.3.3. Сравнительный анализ поведения алгоритмов маршрутизации (на примерах)

Сравнительный анализ устойчивости различных алгоритмических концепций к изменению масштаба сети представлен в Таблице 3. Каждый из рассмотренных базовых подходов обладает ограничениями:

- табличные протоколы (OLSR/AODV) уязвимы из-за квадратичного роста служебного трафика и длительных перерывов связи при изменении топологии;
- чистые лавинные схемы (Flooding) обеспечивают мгновенную адаптацию, но приводят к шторму (BS) и коллапсу пропускной способности при увеличении плотности и размера роя;
- механизмы DCB (см. в [14]) и контентно-ориентированных протоколов сохраняют преимущества лавинной схемы, обеспечивая адаптацию и отсутствие таблиц маршрутов. При этом классические решения (DCB) не лишены собственных ограничений: расширение окна истории может привести к дефициту RAM и росту латентности операций, что особенно критично для БпЛА.

Таблица 3 – Сравнительный анализ алгоритмов маршрутизации при флуктуациях размера роя

Алгоритмическая концепция	Поведение в малом рое (5–7 БпЛА)	Поведение в крупном рое (20...100+ БпЛА)	Влияние мгновенного выбывания до 50% узлов роя	Влияние лавинн. подключения новых узлов	Зависимость вычисл./латентности от размера сети
---------------------------	----------------------------------	--	--	---	---

Табличная (топологическая) (OLSR/AODV)	Высокая стабильность; переход минимален. Энергоэффективность CPU в норме.	Коллапс физической среды; лаг связи служебным трафиком обновлений/запросов (BS).	Длительный срыв связи (сек) из-за таймаутов разрывов рёбер графа и пересчёта таблиц путей.	Всплеск джиттера задержки; лавинообразный рост динамич. таблиц маршрутов в RAM.	Полиномиальная сложность $O(N)...O(N^2)$. Для OLSR (распылки топологии AODV – значител. рост числа запросов.
Чистая лавинная (Flooding/Gossip)	Устойчивая доставка, но локальная избыточность радио-эфира.	Мгновенное самоподавление сети встречными коллизиями пакетов-копий на L2.	Плавное снижение интеграл. Уровня коллиз. шума в канале. Тополог. адаптация за 0 такт.	Взрывной рост коллизий; полная блокировка пропуск. способности физич. канала.	Временная сложность константна и близка к $O(1)$, но общая ёмкость среды деградирует при росте масштаба N.
Нетабличная дедупликация. Контентно-зависимые протоколы	Стабильное функционирование локальные таблицы истории хэш-сигнатур не перегружены.	Деградация тактового ресурса CPU от устаревш. хэшей по алгоритмам кэш вытеснен.	Избыточность кэш-памяти; забивание RAM устаревшими хэш-сигнатурами уничтоженных узлов.	Риск аппаратного переполнения буферов памяти; рост латентности ассоциативного поиска дубликатов в кэше	Логарифмическая сложность $O(\log M)$, где ёмкость кэша M жёстко привязана к размеру роя как ёмкость окна истории.

3.4. Развитие классических способов и методов нетабличной маршрутизации в работах отечественных авторов.

3.4.1. Введение элементов адаптации

В развитие механизмов управления трафиком в децентрализованных системах рассмотрим решение, представленное в [13] – "Способ организации беспроводных одноранговых самоорганизующихся сетей" (далее, СО БОСС). В классе СС автором был предложен проприетарный способ, направленный на борьбу с дублированием пакетов. Его основные положения включают:

1. *Снижение сетевого трафика.* Алгоритм отслеживает дубликаты: когда узел получает пакет, он проверяет, не поступал ли уже пакет с такой же ключевой информацией. Если да – дубликат отбрасывается.
2. *Контроль распространения.* Если пакет прошёл проверку на дубликат, перед фактической передачей в эфир алгоритм сориентирован на 2 счётчика: сколько раз этот пакет уже был принят и сколько раз передан. Только если оба значения не превышают заданного порога, пакет отправляется дальше.
3. *Поддержка динамичности.* Учитывается природа СС, где топология меняется в реальном

времени: механизм со списками и счётчиками помогает такой сети оперативно адаптироваться к изменениям.

Однако в данном решении [13] сохранены особенности реализации, присущие ранним подходам. Так, хотя на оптимизацию алгоритмов и указывает определение "*начинать с последней добавленной записи*", физически это всё равно имеет место – "*линейный последовательный перебор элементов в памяти (массиве)*". Если окно истории N составляет значительное количество пакетов, а нужный дубликат пришёл с задержкой (например, из-за ретрансляции через дальний узел), системе придётся сделать множество операций сравнения. Время проверки пакета – нестабильно (высокий джиттер) и растёт линейно.

Как следует из [13], отдан приоритет *программной реализации*: описание структуры устройства данного способа прямо указывает на классическую архитектуру. Этот подход накладывает объективные ограничения на скорость обработки пакетов в высокоинтенсивных пакетных потоках.

Значения счётчиков сравниваются с "определённым заданным числом" (жёсткой константой, например – 3). Соответственно, в условиях интенсивных внешних помех, эта *жёсткая константа может* заблокировать передачу легитимных пакетов. Кроме того, реализация алгоритма на уровне CPU в условиях лавинного широковещательного шторма (BS) ведёт к исчерпанию вычислительных ресурсов борта.

Использование статически заданных пороговых констант для счётчиков повторов делает систему менее адаптивной. При возникновении внешних помеховых сигналов высокой интенсивности, когда поток транзитных дубликатов резко возрастает, расходы на выполнение этих (пусть и адаптивных) алгоритмов приводят к линейной вычислительной деградации задержек ($O(N)$) и дефициту энергетического ресурса (критерий SWaP). Математическим ограничением подхода является линейный рост пространственной сложности $O(N)$ и деградация временной сложности поиска в табличных хэш истории до уровней $O(\log N)$ и $O(N)$. Обобщающие показатели основных концепций маршрутизации, а также сравнение потенциала рассмотренных в нашей работе

способов в роевых сетях представлены в Таблицах 4 и 5.

Таблица 4 – Обобщающие показатели схем реализации и способа СО БОСС

Критерий сравнения	Методы контентной фильтрации и дедупликации	Сетевой стохастический метод	Структурно-алгоритмич. реализация (СО БОСС)
1	2	3	4
Базовый принцип функционирования)	Контентно-зависимые: выявление дубликатов на основе анализа уникальных хэш-сигнатур содержимого транзитных пакетов.	Стохастически: вероятностное адаптивное подавление избыточных широко-вещательных трансляций на канальном уровне.	Структурно-алгоритм: детерминир. динамическая организация внутренних связей и политик вытеснения.
Аппаратно-программный базис реализации	Программный стек CPU: динамич. хэш-таблицы истории в RAM; интенсивные операции поиска/вставки.	Программные средства канального уровня: мин. регистры и счётчики коллизий.	Бортовой микро-контроллер; фикс. окна истории и детерминир. политики вытеснения.
Временная сложность (наихудший случай)	Линейная деградация до $O(N)$ при массовых коллизиях хэшей или при поиске в больших скользящих окнах истории. Средняя сложность – $O(I)$.	Математически не определена (вероятн.расчёт интенсивности). Поведение определяют пороговые правила.	$O(\log N)$ — детерминир. гарантии верхней границы; риск взаимных блокировок минимизация аппаратной изоляции.
Пространственная сложность (объём оперативной памяти)	Линейная зависимость $O(N)$ от текущего размера скользящего окна истории (ёмкости хэш-кэша); масштабируется ростом числа отслеживаемых потоков.	Константная сложность $O(1)$ — при фиксированном размере локальных счётчиков и Bloom-фильтров; не зависит от числа узлов N .	$O(N)$ с верхн. границей; потребность в выделен. блоках RAM компенсирует фикс. размер окна истории M и отсутств. перестр. структур.
Устойчивость к ВДФ	Низкая: лавинно-образное переполнение буфер. хэш-памяти приводит к отказу в обслуживании, рост коллизий снижает эффективность фильтрации.	Средняя: при превышении порога шума переходит в режим подавления; возможна пауза нет гарантии сохранения связности.	Высокая: при аппаратной реализации: фикс. политики вытеснения и отсутствие ёмких операций перестройки структур.
Управление узловым энергопотреблением	Отсутствует: высокие энергозатраты CPU на непрерывную обработку полезной нагрузки, поиск в хэш-таблицах и очистку индексов.	Отсутствует: пассивная логика ожидания в режиме радиомодема; расход энергии на базовую обработку.	Отсутствует перенос крит. функций на ПЛИС, что снижает нагрузку CPU.
1	2	3	4

Влияние высокой плотности и масштаба сети	Резкое падение производительности из-за разрастания хэш-индексов и тактовых циклов очистки; задержки растут нелинейно.	Критический рост вероятности взаимного стохаст. подавления полезных сигналов; возможна потеря связности.	Высокий риск истощения ёмкости буферов при неоптимальн. М; РОН используем по политике вытеснения (фикс. пороги).	на канал (РОН)	масштабируемость резко падает с ростом N .	среды); избегает BS при β_{adan} в плотн. роях.
Устойчивость к ВДФ					Низкая: коллизии и ВДФ усугубляют BS, быстрое насыщение канала.	Высокая (динам. адаптация за счёт операт. изм. β_{adan}).
1	2	3				
Требования к вычисл. ресурсам (CPU)	Высокие: непрер. поиск и обновление хэш-истории, полная загрузка CPU при лавине дубликатов.	Умеренные при аппар. реализации счётчиков Bloom-фильтров.				
Зависимость задержек от плотности сети	Резкий рост задержек из-за коллизий и перегрузки буферов; асимптотически нестаб. при $N \gg 1$.	Контроль задержки за счёт β_{adan} ; возможна стабилизация в высокоплотных роях.				
Энергоэффективность (в рамках SWaP)	Низкая: постоянные передачи и обработка дубликатов ведут к перегреву и истощению аккумулятора.	Повышенная при адаптивном управлении: снижение числа избыт. передачи.				
Применимость в высокоплотных роях	Ограниченная: быстр. переход в режим BS и резкое падение полез. пропускной способности.	Перспективная при β_{adan} : позволяет $I_{ReTx} < I_{max}^{[min]}$ сохранять связность сети.				

Анализ научно-технической литературы и патентных источников в области управления трафиком децентрализованных сетей FANet показывает, что большинство известных решений – включая статистические методы класса DCB и подходы [5; 11] – ориентировано преимущественно на верхние уровни сетевой модели OSI. В таких системах фильтрация избыточных дубликатов осуществляется программно, только после полного физического приема и извлечения прикладных данных. Высокая вычислительная нагрузка, обусловленная именно таким способом реализации, выступает серьёзным сдерживающим фактором для прямой интеграции рассматриваемых концепций в БВ БпЛА лёгкого и среднего классов. Накладные расходы на непрерывную обработку индексов кэша вызывают предельную загрузку CPU. Дополнительным ограничением программно-ориентированных патентов является их энергетическая неэффективность в рамках критерия SWaP.

Таблица 5 – Сравнительная таблица среднего потенциала адаптации нетабличных способов маршрутизации в типовых решениях

Критерий сравнения	Лавинная концепция (Flooding)	Эпидемический стохастический протокол
1	2	3
Характер алгоритма	Строго детерминирован: (ретрансляция по факту новизны без учёта состояния сети.	Стохастический: решение о ретрансл. зависит от β и локальн. плотности узлов.
Решение о ретрансляции	Принимается всегда при подтвержд. новизны пакета (в локальн. истории уник.хэш-сигнатуры нет).	Функционально зависит от вероятности β_{adan} , локальн. плотн. и загрузки канала.
Нагрузка	Экспоненциальный рост служебного трафика;	Логистический рост (ограничен ёмкостью

Таким образом, эпидемический протокол имеет потенциал развития алгоритмов маршрутизации, способных сформировать адаптивную, автономную систему управления роём, которая устраняет избыточный трафик и переводит транзитные узлы в режим контролируемого снижения активности излучения (детерминированной паузы), сохраняя при этом полезную пропускную способность радиоканала и энергетический ресурс аккумуляторов БпЛА (SOC).

Данное решение базируется на идее гибридного подхода, сочетающего аппаратную специализации выделенных вычислительных блоков (типа ПЛИС, СнК [12]) с гибким программным управлением верхнего уровня, осуществляющим динамическую настройку бортовых ресурсов под текущую задачу роя [54]. Как было показано, (например, А. Вахдата и Д. Беккера [55] или З. Хааса [31]) классический эпидемический протокол маршрутизации использует статическую вероятность передачи данных β , единую для всей сети. В разработанном нами решении параметр β преобразуется в динамическую переменную, которая в реальном времени рассчитывается аппаратным ПИД-регулятором (например, на DSP-блоках ПЛИС) и позволяет трансформировать BS в адаптивно-управляемый процесс.

3.4.2. Теория сетевой близости и методы маршрутизации. Обзор смежных подходов.

Реализация контентно-ориентированных кросс-уровневых подходов концептуально связана с использованием сетевых метрик, обеспечивающих оптимальную связность и

целостность сети роя. Концепция технологий сетевой близости – NP (*Network Proximity*, NP), сформулированная в работах Д.Е. Намиота [7; 8], рассматривается нами в контексте совместных решений в перспективных сетевых платформах БпЛА-роя. Согласно данной концепции, в распределённых высоко-динамичных системах классические процедуры абсолютного геопозиционирования могут быть эффективно замещены и/или комплементарно дополнены моделями контекстной близости, оперирующими фактами взаимной радио-видимости узлов. Данная модель может получить профильное развитие, следующим образом:

1. Алгоритмы фиксации сетевой близости (NP) могут быть перенесены из программно-ориентированной среды верхних уровней непосредственно в аппаратный конвейер ПЛИС канального уровня со сложностью $O(1)$. Это позволит изолировать БВ от КВИТ, сохранив стабильность сервисов близости при жёстком ограничении по SWaP.

2. Представленные в [7; 8] подходы позволяют также рассмотреть решения по применению и развитию индикаторов и метрик маршрутизации. Так, например, *метрики сетевой близости* используются на базе счётчиков (совокупности Counter based-методов, см. в разделе 3.1.1.) с возможностью вместо измерения абсолютных координат, оперировать *следующими основными низкоуровневыми метриками*:

- *Индекс интенсивности близости* $I_{prox}[i]$ Определяется текущим (в момент (t)) дробным значением плавающего счётчика $H_i(t)$ для конкретной уникальной хэш-сигнатуры пакета. Высокое значение индекса I_{prox} свидетельствует о том, что источник данного информационного пакета локализован в зоне критически плотной сетевой близости относительно текущего транзитного узла. Данное состояние характеризуется минимальным количеством хопов, высоким энергетическим потенциалом радиоканала или избыточной ретрансляционной активностью локального окружения.

- *Градиент топологического дрейфа* (∇D_{prox}) отражает нестационарную скорость изменения состояния плавающего счётчика во времени ($\frac{dH[i]}{dt}$). Положительное значение градиента означает физическое сближение узлов сети или пространственное уплотнение тактической группы. Отрицательное значение градиента фиксирует пространственную диссипацию

элементов роя или же деградацию характеристик радиоканала под воздействием ВДФ, что в режиме реального времени регистрируется через экспоненциальное затухание коэффициента стохастической ретрансляции $\beta(t)$;

- *Коэффициент пространственно-сетевого резонанса* (K_{res}). Кросс-уровневая метрика, сопоставляющая I_{prox} с вектором относительного смещения БИНС. Если фиксируется маневр расхождения, а I_{prox} продолжает расти, система управления классифицирует это как аномалию – преднамеренное ВДФ методом "отравления кэша" или ретрансляции ложных дубликатов деструктивными средствами радиоэлектронного воздействия [5; 9; 44].

Можно полагать, что NP [7; 8] органично интегрируется в "модель агрегатов" Бусленко [3] в качестве заданных целевых метрик и критерия адаптации порогов, выступая сенсором для принятия решений в организации сети связи на основе эпидемической маршрутизации. Вместо абстрактной оценки плотности соседних узлов используется формализованная много-критериальная мера, рассчитываемая на основе индикатора уровня принимаемого сигнала (RSSI) [54], сетевой задержки, геометрической дистанции или топологической связности. Значение этой метрики напрямую определяет текущий порог ретрансляции пакетов $\beta(t)$.

Таким образом, применение сквозных механизмов адаптации на основе технологий сетевой близости (NP) позволит обеспечить радикальное повышение живучести, скрытности и автономности роевых структур FANet в условиях интенсивного воздействия ВДФ.

IV. ЗАКЛЮЧЕНИЕ

В нашей работе мы исследовали архитектурные и функциональные особенности реализации протоколов маршрутизации, а также граничные вычислительные возможности и системные недостатки традиционных табличных программно-ориентированных подходов к дедупликации трафика в условиях высоко-плотных беспроводных сетей с высокой динамикой топологии роя и интенсивным воздействием ВДФ.

Представлена авторская математическая модель комбинаторного взрыва интенсивности избыточного трафика в динамических FANet-сетях. Предложенная модель качественно отличается от рассмотренных аналогов

конвергентным сопряжением математического аппарата теории стохастических ВП Гальтона–Ватсона [20] и положений классической теории телетрафика [4]. Данная модель позволила доказать, что лавинообразная деградация полезной пропускной способности канала связи до нулевого значения ($\lim_{I_{gen} \rightarrow \infty} I_{success}(t) = 0$) обусловлена структурно-топологическими свойствами ad-hoc среды. Это обосновывает необходимость динамического децентрализованного управления хэш-индексами сигнатур на основе кросс-уровневых решений, учитывающих состояния радиосреды на основе сетевых и NP-алгоритмов.

Сформулированные концептуальные требования к перспективным системам построения кросс-уровневого аппаратно-ориентированного сетевого стека в рамках единой платформы маршрутизации позволяют предотвращать вычислительную и коллизийную деградацию в рое БПЛА при критической плотности узлов и интенсивных внешних воздействиях.

Для снижения вычислительной сложности бортовых алгоритмов и исключения перегрузки центрального процессора в условиях коллизийного широкоэмитерного шторма представляется перспективным аппаратное разделение функций по иерархическим контурам с гибким программным управлением верхнего уровня.

БИБЛИОГРАФИЯ

- [1] Антонова В.М., Бужин И.Г., Гнездилов В.С., Кузнецов Н.А., Миронов Ю.Б. Математическое моделирование сетевых узлов и топологий современных сетей передачи данных // Информационные процессы. – 2024. – Т. 24, № 1. – С. 84–92.
- [2] Брычков Ю.А., Савищенко Н.В. Многомерные распределения Релея, Райса, Накагами и их применение в теории связи // Учёные записки Казан. ун-та. Серия: Физ.-матем. науки. – 2024. – Т. 166, кн. 2. – С. 127–146.
- [3] Бусленко Н.П. Моделирование сложных систем. – 2-е изд., перераб. – Москва: Наука, 1978. – 399 с.
- [4] Ливищ Б.С., Пишеничков А.П., Харкевич А.Д. Теория телетрафика. – Москва: Связь, 1979. – 224 с.
- [5] Макаренко С.И. Методики и методы повышения устойчивости системы связи в условиях деструктивного воздействия на протоколы сетевого и транспортного уровней // Системы управления, связи и безопасности. – 2017. – № 4. – С. 1–39.
- [6] Муратчаев С.С., Волков А.С., Маргарян Р.А., Бахтин А.А. Разработка адаптивной версии протокола маршрутизации OLSRV2 в сетях MANet // Труды МАИ. – 2022. – № 123.
- [7] Намиот Д.Е. Технологии сетевой близости: концепция, модели и алгоритмы, распределённые системы и сервисы : 05.13.11: диссертация ... доктора технических наук / Намиот Д.Е. Объединённый институт ядерных исследований. – Дубна, 2021. – 378 с.
- [8] Намиот, Д.Е., Покусев О.Н., Чекарев А.Е. Модели сетевой близости в информационных системах на транспорте // International Journal of Open Information Technologies. – 2020. – Т. 8, № 9. – С. 36–41.
- [9] Перегудов М.А. Вероятностная модель функционирования канального уровня сети цифровой радиосвязи в условиях деструктивных воздействий // Системы управления, связи и безопасности. – 2023. – № 1. – С. 64–89.
- [10] Тарасевич Ю.Ю. Перколяция: теория, приложения и алгоритмы. М.: Едиториал УРСС, – 2002. – 112 с.
- [11] Патент РФ № 2619471 С1. Крупномасштабная сеть ДКМВ радиосвязи со сплошной зоной радиодоступа / Зайцев В.В., Лихачёв А.М., Круковская И.Я., Круковский Я.В. и др. // Бюл. № 14. – опубл.: 16.05.2017.
- [12] Патент РФ № 2626550 С1. Программно-аппаратная платформа и способ её реализации для беспроводных средств связи / Архипкин В.Я., Завалин Ю.В., Лихачёв А.М., Круковская И.Я., Круковский Я.В., Присяжнюк С.П., Шпак В.В. и др. // Бюл. № 22. – опубл.: 28.07.2017.
- [13] Патент РФ № 2829497 С1. Способ организации беспроводных одноранговых самоорганизующихся сетей / Тютин А.П. // Бюл. № 31. – опубл.: 30.10.2024.
- [14] Al-Humoud, S.O., Mackenzie L.M., Vanderbauwhede W. Dynamic Counter-Based Broadcast in MANets // Proceedings of the 4th ACM Workshop on Performance Monitoring and Measurement of Heterogeneous Wireless and Wired Networks. – Glasgow: ACM, 2009. – P. 84–88.
- [15] Anastasi G. et al. Energy conservation in wireless sensor networks: A survey // Ad Hoc Networks. – 2009. – Vol. 7, No. 3. – P. 537–568.
- [16] Baccelli F., Blaszczyzyn B. Stochastic Geometry and Wireless Networks: Volume I Theory // Foundations and Trends in Networking. 2009. – Vol. 3, No. 3–4. – P. 249–449.
- [17] Bianchi G. Performance Analysis of the IEEE 802.11 Distributed Coordination Function // IEEE Journal on Selected Areas in Communication. – 2000. – Vol. 18, – No. 3. – P. 535–547.
- [18] Broder A., Mitzenmacher M. Network applications of Bloom filters: A survey // Internet Mathematics. – 2004. – Vol. 1, No. 4. – P. 485–509.
- [19] Bujari, A. et al. On the Performance of MAC Protocols for UAV-Based Networks // Ad Hoc Networks. – 2017. – Vol. 63. – P. 97–110.
- [20] Cloez B., Daufresne T., Keroui M., Fontez B. Galton–Watson process and Bayesian inference: A turnkey method for the viability study of small populations // arXiv.org. – 2019. – arXiv:1901.09562.
- [21] Clausen T., Jacquet P. Optimized Link State Routing Protocol (OLSR) // Internet Engineering Task Force, Info. Memo RFC 3626, – Oct. 2003. – 75 p.
- [22] Cormen T.H. et al. Introduction to Algorithms / 3rd ed. – MIT Press, 2009. – Ch. 11: Hash Tables. – P. 253–278.
- [23] Dong S., Tang Z., Ma H. A Review of Routing Protocols for FANet // IOSR Journal of Electronics and Communication Engineering. – 2024. – Vol. 19, iss. 6 (Sec. I). – P. 06–22.
- [24] De Melo Pire, R., Pinto A.S.R. Branco K.R.L.J.C. The Broadcast Storm Problem in FANets and the Dynamic Neighborhood-Based Algorithm as a Countermeasure // IEEE Access. – 2019. – Vol. 7. – P. 59737–59757.
- [25] Fall, K. A Delay-Tolerant Network Architecture for Challenged Internets // Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications (SIGCOMM '03). – New York : ACM, 2003. – P. 27–34.

- [26] Franceschetti M., Meester R. Random Networks for Communication: From Geometric Percolation to Information Theory / Cambridge: Cambridge University Press, – 2007. – 236 p.
- [27] Giorgio C.B. Hard Real-Time Computing Systems: Predictable Scheduling Algorithms and Applications. – Springer, 2011. – 522 p.
- [28] Godha P., Jadon S., Patle A. et al. Flooding and Forwarding Based on Efficient Routing Protocol // Advances in Intelligent Systems and Computing. – Springer, 2021. – Vol. 1161. – P. 215–223.
- [29] Garg P., Kumar H., Johari R. et al. Enhanced Epidemic Routing Protocol in Delay Tolerant Networks // 2018, 5th International Conference on Signal Processing and Integrated Networks (SPIN). – 2018. – P. 396–401.
- [30] Gross T.J., Abrão T., Jeszensky P.J.E. Distributed power control algorithm for multiple access systems based on Verhulst model // International Journal of Electronics and Communications. – 2011. – Vol. 65. – P. 361–372.
- [31] Haas Z.J., Halpern J.Y., Li L. Gossip-based ad hoc routing // IEEE/ACM Transactions on Networking. – 2006. – Vol. 14, No. 3. – P. 479–491.
- [32] Iversen V.B. Teletraffic Engineering / Study Group 2, Question 16/2. Handbook // ITU-D & ITC Revised ed. by Villy B. Iversen. – Geneva, January 2005. – 336 p.
- [33] Jung J.-Y., Seo D.-Y., Lee J.-R. Counter-Based Broadcast Scheme Considering Reachability, Network Density, and Energy Efficiency for Wireless Sensor Networks // Sensors. – 2018. – Vol. 18, No. 1. – Art. No. 120.
- [34] Kopetz H. Real-Time Systems: Design Principles for Distributed Embedded Applications. – Springer, 2011. – 376 p.
- [35] Krivtsova I., Lebedev I., Sukhoparov M., Bazhayev N., Zikratov I. et al. Implementing a Broadcast Storm Attack on a Mission-Critical Wireless Sensor Network. // 14th International Conference on Wired / Wireless Internet Communication (WWIC), Thessaloniki, Greece, May 2016. – Cham: Springer, – 2016. – P. 297–308.
- [36] Lai W., Lin Y.C. Load-Balance Directed Diffusion in Wireless Sensor Networks // IEEE Transactions on Wireless Communications. – 2005. – Vol. 4, No.3. – P. 1022–1029.
- [37] Leau, Y.-B., Manickam S. A Novel adaptive grey Verhulst model for network security situation prediction // International Journal of Advanced Computer Science and Applications. – 2016. – Vol. 7, No 1. – P. 90–95.
- [38] Liang M., Zhang Z., Liu C., Chen L. Multihop-Delivery-Quality-Based Routing in DTNs // IEEE Transactions on Vehicular Technology. – 2015. – Vol. 64, no. 3. – P. 1095–1104.
- [39] Lima J., Monotti R., Cardoso J.M.P. et al. A Methodology to design FPGA based PID controllers // IEEE International Conference on Systems, Man and Cybernetics. – Taipei: IEEE, 2006. – Vol. 3. – P. 2577–2583.
- [40] Lipman J., Hai Liu, Stojmenovic I. Broadcast in ad hoc networks. Guide to Wireless Ad Hoc Networks. – Springer London, 2009. – P. 121–150.
- [41] Liu, Z. et al. A Geographic Routing Protocol for Flying Ad-Hoc Network Based on Gauss-Markov Mobility Prediction // 2024 4th International Symposium on Computer Technology and Information Science (ISCTIS). – IEEE, 2024. – P. 115–122.
- [42] Mackenzie L., Mohammed A., Ould-Khaoua M. An Efficient Counter-Based Broadcast Scheme for Mobile Ad Hoc Networks // International Conference on Mobile Lightweight Wireless Systems. – 2007. – Vol.4712. – P.195–204.
- [43] Naserian M., Tepe K.E., Tarique M. Routing Overhead Analysis for Reactive Routing Protocols in Wireless Ad Hoc Networks // Proceedings of the IEEE International Conference on Wireless and Mobile Computing, Net-
- working and Communications, – Montreal, Canada, 2005. – IEEE, 2005. – Vol. 3. – P. 119–126.
- [44] Nguyen V.L., Lin P.C., Hwang R.H. Energy depletion attacks in low power wireless networks // IEEE Access. – 2019. – Vol. 7. – P. 51915–51932
- [45] Ni S.-Y., Tseng Y.-C., Chen Y.-S., Sheu J.-P. The broadcast storm problem in a mobile ad hoc network // Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom'99). – ACM, New York, 1999. – P. 151–162.
- [46] Penrose, J. Random Geometric Graphs / Oxford : Oxford University Press, 2003. – 320 p
- [47] Perkins C., Belding-Royer E., Das S. Ad hoc On-Demand Distance Vector (AODV) Routing // RFC 3561. – 2003. – 37 p.
- [48] Proakis J., Salehi. M. Digital Communications. – 5th ed. – New York: McGraw Hill, 2007. – 1150 p.
- [49] Putze F., Sanders P., Singler J. Cache-, hash-, and space-efficient Bloom filters // ACM Journal of Experimental Algorithmics. – 2009. – Vol. 14. – P.4:1–4:22.
- [50] Ramesh B., Manjula D. An Adaptive Congestion Control Mechanism for Streaming Multimedia in Mobile Ad-hoc Networks // IJCSNS International Journal of Computer Science and Network Security. – 2007. – Vol. 7, No. 6. – P. 290-295
- [51] Rosati S., Kruzelecki K. et al. Dynamic routing for flying ad hoc networks // IEEE Transactions on Vehicular Technology. – 2016. – Vol. 65, No. 3. – P. 1690–1700.
- [52] Small T., Haas Z.J. Resource and Performance Tradeoffs in Delay-Tolerant Wireless Networks // Proceedings of the 2005 ACM SIGCOMM Workshop on Delay-Tolerant Networking (WDTN-05). – New York : ACM Press, 2005. – P. 260–267.
- [53] Tan D., Kim D. Dynamic traffic-aware routing algorithm for multi-sink wireless sensor networks // Wireless Networks. – 2014. – Vol. 20. – P. 1239–1250.
- [54] Trinh M.L., Nguyen D.T., Dinh L.Q., Nguyen M.D., Setiadi D.R.I., Nguyen M.T. Unmanned Aerial Vehicles (UAV) Networking Algorithms: Communication, Control, and AI-Based Approaches // Algorithms. – 2025. – Vol. 18, No. 5. – Art. No. 244.
- [55] Vahdat A., Becker D. Epidemic routing for partially-connected ad hoc networks // Technical Report CS-2000-06, Duke University. – 2000. – Vol. 6. – 22 p.
- [56] Vera-Amaro R., Torres-Cruz N., Montiel-Cruz A.L., et al. Multi-Hop Heterogeneous UAV Swarm Networking for Post-Disaster Internet Access // 32nd International Conference on Telecommunications: proceedings, Thessaloniki, Greece, May 2026. – [S. l.] : IEEE, 2026. – P. 332–335.
- [57] Zhang, L. et al. Adaptive Cache Replacement Policies for Mobile and Delay-Tolerant Networks // Ad Hoc Networks. – 2021. – Vol. 115. – Art. 102432.
- [58] Zhu L., Karim M.M., Sharif K. et al. Traffic Flow Optimization for UAVs in Multi-Layer Information-Centric Software-Defined FANet // IEEE Transactions on Vehicular Technology. – 2023. – Vol. 72, No. 2. – P. 2453–2467.
- [59] ГОСТ 34.11-2018. Информационная технология (ИТ). Криптографическая защита информации. Функция хэширования (с попр. от 15.03.2021) / Официальное издание. – Москва: Стандартинформ, 2018 – 20 с.
- [60] ГОСТ Р ИСО/МЭК 29182-1-2018. Информационные технологии. Эталонная архитектура для сенсорных сетей (SNRA). Часть 1. Общий обзор и требования. / Официальное издание. – Москва: Стандартинформ, 2018 – 10 с.
- [61] ГОСТ Р 59162-2020. Национальный стандарт Российской Федерации. Информационные технологии. Методы и средства обеспечения безопасности.

Безопасность сетей. Часть 6. Обеспечение информационной безопасности при использовании беспроводных IP-сетей. / Официальное издание. – Москва: Стандартинформ, 2020 – 26 с.

[62] ГОСТ Р 59519-2021. Беспилотные авиационные системы. Компоненты беспилотных авиационных систем. Спецификация и общие технические требования. / Официальное издание. – Москва: Стандартинформ, 2021 – 6 с.

[63] Управление подвижными объектами. Библиографич. указатель. В 3 выпусках. Выпуск 2. Аэродинамические объекты / под ред. В.М. Глумова; Учреждение РАН Институт проблем управления им. В.А. Трапезникова РАН. – Москва: 2011. – 374 с.

Сведения об авторах:

Миронов В.В., генеральный директор ООО "Интеллектуальные системы поддержки", г. Воронеж, Россия (e-mail: miropov.vitalii@ya.ru)

Селезнёв С.П., к.т.н., научный редактор журнала г. Москва, Россия (e-mail: spseleznev@ya.ru)

Круковская И.Я., с.н.с., аналитик, г. Москва, Россия, (e-mail: tssnpk@ya.ru)

Круковский Я.В., к.э.н., доцент по кафедре ИТ, зам. директора по науке, г. Санкт-Петербург, Россия (e-mail: info@tssnpk.ru)

Comparative Analysis of Routing Protocols in a High-Density UAV Swarm

V.V. Mironov, S.P. Seleznev, I.Y. Krukovskaya, Y.V. Krukovsky

Abstract - This article provides an analytical review of key protocol classes and routing methods used in high-density dynamic unmanned networks (FANets) (from a few to 200+ nodes). Three dominant concepts are considered: classical table-based approaches (proactive and reactive), epidemic (avalanche) data dissemination methods, and emerging concepts of content-aware deduplication (CB-RDE), CB-BSD. A comparative analysis of their computational complexity in terms of time and memory, service overhead, and resistance to electronic countermeasures (EW) is provided.

Keywords — UAV swarm, FANet, routing, epidemic protocols, content deduplication, CB-RDE, CB-BSD, computational complexity, electronic warfare., broadcast storm problem, cross-layer optimization, hardware deduplication, computational complexity.

REFERENCE

- [1] Antonova V.M., Buzhin I.G., Gnezdilov V.S., Kuznecov N.A., Mironov Ju.B. Matematicheskoe modelirovanie setevykh uzlov i topologij sovremennykh setej peredachi dannykh // Informacionnye processy. – 2024. – T. 24, # 1. – S. 84–92.
- [2] Brychkov Ju.A., Savishhenko N.V. Mnogomernye raspredeleniya Releja, Rajsa, Nakagami i ih primenenie v teorii svyazi // Uchjonye zapiski Kazan. un-ta. Serija: Fiz.-matem. nauki. – 2024. – T. 166, kn. 2. – S. 127–146.
- [3] Buslenko N.P. Modelirovanie slozhnykh sistem. – 2-e izd., pererab. – Moskva: Nauka, 1978. – 399 s.
- [4] Livshic B.S., Pshenichkov A.P., Harkevich A.D. Teorija telegrafika. – Moskva: Svyaz', 1979. – 224 s.
- [5] Makarenko S.I. Metodiki i metody povysheniya ustojchivosti sistemy svyazi v usloviyakh destruktivnogo vozdejstviya na protokoly setevogo i transportnogo urovnej // Sistemy upravleniya, svyazi i bezopasnosti. – 2017. – # 4. – S.1–39.
- [6] Muratchaev S.S., Volkov A.S., Margarjan R.A., Bahtin A.A. Razrabotka adaptivnoj versii protokola raspredeleniya OLSRv2 v setjah MANet // Trudy MAI. – 2022. – # 123.
- [7] Namiot D.E. Tehnologii setevoy blizosti: koncepcija, modeli i algoritmy, raspredeljonnye sistemy i servisy : 05.13.11: dissertacija ... doktora tehnikeskikh nauk / Namiot D.E. Ob"edinjonnyj institut jademykh issledovanij. – Dubna, 2021. – 378 s.
- [8] Namiot, D.E., Pokusaev O.N., Chekmarev A.E. Modeli setevoy blizosti v informacionnykh sistemah na transporte // International Journal of Open Information Technologies. – 2020. – T.8, #9. – S. 36–41.
- [9] Peregudov M.A. Veroyatnostnaja model' funkcionirovaniya kanal'nogo urovnja seti cifrovoj radiosvyazi v usloviyakh destruktivnykh vozdejstvij // Sistemy upravleniya, svyazi i bezopasnosti. – 2023. – #1. – S. 64–89.
- [10] Tarasevich Ju.Ju. Perkoljacija: teorija, prilozheniya i algoritmy. M.: Editorial URSS, – 2002. – 112 s.
- [11] Patent RF # 2619471 S1. Krupnomasshtabnaja set' DKMV radiosvyazi so sploshnoj zonoj radiodostupa / Zajcev V.V., Lihachjov A.M., Krukovskaja I.Ja., Krukovskij Ja.V. i dr. // Bjul. # 14. – opubl.: 16.05.2017.
- [12] Patent RF # 2626550 C1. Programmno-apparatnaja platforma i sposob ejo realizacii dlja besprovodnykh sredstv svyazi / Arhipkin V.Ja., Zavalin Ju.V., Lihachjov A.M., Krukovskaja I.Ja., Krukovskij Ja.V., Prisjajzhnjuk S.P., Shpak V.V. i dr. // Bjul. # 22. – opubl.: 28.07.2017.
- [13] Patent RF # 2829497 C1. Sposob organizacii besprovodnykh odnorangovykh samoorganizujushchisja setej / Tjutin A.P. // Bjul. # 31. – opubl.: 30.10.2024.
- [14] Al-Humoud, S.O., Mackenzie L.M., Vanderbauwhede W. Dynamic Counter-Based Broadcast in MANets // Proceedings of the 4th ACM Workshop on Performance Monitoring and Measurement of Heterogeneous Wireless and Wired Networks. – Glasgow: ACM, 2009. – P. 84–88.
- [15] Anastasi G. et al. Energy conservation in wireless sensor networks: A survey // Ad Hoc Networks. – 2009. – Vol. 7, No. 3. – P. 537–568.
- [16] Baccelli F., Blaszczyzyn B. Stochastic Geometry and Wireless Networks: Volume I Theory // Foundations and Trends in Networking. 2009. – Vol.3, No.3-4. – P.249–449.
- [17] Bianchi G. Performance Analysis of the IEEE 802.11 Distributed Coordination Function // IEEE Journal on Selected Areas in Communication. – 2000. – Vol. 18, – No.3. – P. 535–547.
- [18] Broder A., Mitzenmacher M. Network applications of Bloom filters: A survey: A survey // Internet Mathematics. – 2004. – Vol. 1, No. 4. – P. 485–509.
- [19] Bujari, A. et al. On the Performance of MAC Protocols for UAV-Based Networks // Ad Hoc Networks. – 2017. – Vol. 63. – P. 97–110.
- [20] Cloez B., Daufresne T., Keroui M., Fontez B. Galton–Watson process and Bayesian inference: A turnkey method for the viability study of small populations // arXiv.org. – 2019. – arXiv:1901.09562.
- [21] Clausen T., Jacquet P. Optimized Link State Routing Protocol (OLSR) // Internet Engineering Task Force, Info. Memo RFC 3626, – Oct. 2003. – 75 p.
- [22] Cormen T.H. et al. Introduction to Algorithms / 3rd ed. – MIT Press, 2009. – Ch. 11: Hash Tables. – P. 253–278.
- [23] Dong S., Tang Z., Ma H. A Review of Routing Protocols for FANet // IOSR Journal of Electronics and Communication Engineering. – 2024. – Vol. 19, iss. 6 (Sec. I). – P. 06–22
- [24] De Melo Pire, R., Pinto A.S.R. Branco K.R.L.J.C. The Broadcast Storm Problem in FANets and the Dynamic Neighborhood-Based Algorithm as a Countermeasure // IEEE Access. – 2019. – Vol. 7. – P. 59737–59757.
- [25] Fall, K. A Delay-Tolerant Network Architecture for Challenged Internets // Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications (SIGCOMM '03). – New York : ACM, 2003. – P. 27–34.
- [26] Franceschetti M., Meester R. Random Networks for Communication: From Geometric Percolation to Information Theory / Cambridge: Cambridge University Press, – 2007. – 236 p.
- [27] Giorgio S.B. Hard Real-Time Computing Systems: Predictable Scheduling Algorithms and Applications. – Springer, 2011. – 522 p.
- [28] Godha P., Jadon S., Patle A. et al. Flooding and Forwarding Based on Efficient Routing Protocol // Advances in

- Intelligent Systems and Computing. – Springer, 2021. – Vol. 1161. – P. 215–223.
- [29] Garg P., Kumar H., Johari R. et al. Enhanced Epidemic Routing Protocol in Delay Tolerant Networks // 2018, 5th International Conference on Signal Processing and Integrated Networks (SPIN). – 2018. – P. 396–401.
- [30] Gross T.J., Abrão T., Jeszensky P.J.E. Distributed power control algorithm for multiple access systems based on Verhulst model // International Journal of Electronics and Communications. – 2011. – Vol. 65. – P. 361–372.
- [31] Haas Z.J., Halpern J.Y., Li L. Gossip-based ad hoc routing // IEEE/ACM Transactions on Networking. – 2006. – Vol. 14, No. 3. – P. 479–491.
- [32] Iversen V.B. Teletraffic Engineering / Study Group 2, Question 16/2. Handbook // ITU-D & ITC Revised ed. by Villy B. Iversen. – Geneva, January 2005. – 336 p.
- [33] Jung J.-Y., Seo D.-Y., Lee J.-R. Counter-Based Broadcast Scheme Considering Reachability, Network Density, and Energy Efficiency for Wireless Sensor Networks // Sensors. – 2018. – Vol. 18, No. 1. – Art. No. 120.
- [34] Kopetz H. Real-Time Systems: Design Principles for Distributed Embedded Applications. – Springer, 2011. – 376 p.
- [35] Krivtsova I., Lebedev I., Sukhoparov M., Bazhayev N., Zikratov I. et al. Implementing a Broadcast Storm Attack on a Mission-Critical Wireless Sensor Network. // 14th International Conference on Wired / Wireless Internet Communication (WWIC), Thessaloniki, Greece, May 2016. – Cham: Springer, – 2016. – P. 297–308.
- [36] Lai W., Lin Y.C. Load-Balance Directed Diffusion in Wireless Sensor Networks // IEEE Transactions on Wireless Communications. – 2005. – Vol. 4, No.3. – P. 1022–1029.
- [37] Leau, Y.-B., Manickam S. A Novel adaptive grey Verhulst model for network security situation prediction // International Journal of Advanced Computer Science and Applications. – 2016. – Vol. 7, No 1. – P. 90–95.
- [38] Liang M., Zhang Z., Liu C., Chen L. Multihop-Delivery-Quality-Based Routing in DTNs // IEEE Transactions on Vehicular Technology. – 2015. – Vol. 64, no. 3. – P. 1095–1104.
- [39] Lima J., Monotti R., Cardoso J.M.P. et al. A Methodology to design FPGA based PID controllers // IEEE International Conference on Systems, Man and Cybernetics. – Taipei: IEEE, 2006. – Vol. 3. – P. 2577–2583.
- [40] Lipman J., Hai Liu, Stojmenovic I. Broadcast in ad hoc networks. Guide to Wireless Ad Hoc Networks. – Springer London, 2009. – P. 121–150.
- [41] Liu, Z. et al. A Geographic Routing Protocol for Flying Ad-Hoc Network Based on Gauss-Markov Mobility Prediction // 2024 4th International Symposium on Computer Technology and Information Science (ISCTIS). – IEEE, 2024. – P. 115–122.
- [42] Mackenzie L., Mohammed A., Ould-Khaoua M. An Efficient Counter-Based Broadcast Scheme for Mobile Ad Hoc Networks // International Conference on Mobile Light-weight Wireless Systems. – 2007. – Vol.4712. – P.195–204.
- [43] Naserian M., Tepe K.E., Tarique M. Routing Overhead Analysis for Reactive Routing Protocols in Wireless Ad Hoc Networks // Proceedings of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications. – Montreal, Canada, 2005. – IEEE, 2005. – Vol. 3. – P. 119–126.
- [44] Nguyen V.L., Lin P.C., Hwang R.H. Energy depletion attacks in low power wireless networks // IEEE Access. – 2019. – Vol. 7. – P. 51915–51932
- [45] Ni S.-Y., Tseng Y.-C., Chen Y.-S., Sheu J.-P. The broadcast storm problem in a mobile ad hoc network // Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom'99). – ACM, New York, 1999. – P. 151–162.
- [46] Penrose, J. Random Geometric Graphs / Oxford : Oxford University Press, 2003. – 320 p
- [47] Perkins C., Belding-Royer E., Das S. Ad hoc On-Demand Distance Vector (AODV) Routing // RFC 3561. – 2003. – 37 p.
- [48] Proakis J., Salehi. M. Digital Communications. – 5th ed. – New York: McGraw Hill, 2007. – 1150 p.
- [49] Putze F., Sanders P., Singler J. Cache-, hash-, and space-efficient Bloom filters // ACM Journal of Experimental Algorithmics. – 2009. – Vol. 14. – P.4:1–4:22.
- [50] Ramesh B., Manjula D. An Adaptive Congestion Control Mechanism for Streaming Multimedia in Mobile Ad-hoc Networks // IJCSNS International Journal of Computer Science and Network Security. – 2007. – Vol. 7, No. 6. – P. 290-295
- [51] Rosati S., Kruzelecki K. et al. Dynamic routing for flying ad hoc networks // IEEE Transactions on Vehicular Technology. – 2016. – Vol. 65, No. 3. – P. 1690–1700.
- [52] Small T., Haas Z.J. Resource and Performance Tradeoffs in Delay-Tolerant Wireless Networks // Proceedings of the 2005 ACM SIGCOMM Workshop on Delay-Tolerant Networking (WDTN-05). – New York : ACM Press, 2005. – P. 260–267.
- [53] Tan D., Kim D. Dynamic traffic-aware routing algorithm for multi-sink wireless sensor networks // Wireless Networks. – 2014. – Vol. 20. – P. 1239–1250.
- [54] Trinh M.L., Nguyen D.T., Dinh L.Q., Nguyen M.D., Setiadi D.R.I., Nguyen M.T. Unmanned Aerial Vehicles (UAV) Networking Algorithms: Communication, Control, and AI-Based Approaches // Algorithms. – 2025. – Vol. 18, No. 5. – Art. No. 244.
- [55] Vahdat A., Becker D. Epidemic routing for partially-connected ad hoc networks // Technical Report CS-2000-06, Duke University. – 2000. – Vol. 6. – 22 p.
- [56] Vera-Amaro R., Torres-Cruz N., Montiel-Cruz A.L., et al. Multi-Hop Heterogeneous UAV Swarm Networking for Post-Disaster Internet Access // 32nd International Conference on Telecommunications: proceedings, Thessaloniki, Greece, May 2026. – [S. l.] : IEEE, 2026. – P. 332–335.
- [57] Zhang, L. et al. Adaptive Cache Replacement Policies for Mobile and Delay-Tolerant Networks // Ad Hoc Networks. – 2021. – Vol. 115. – Art. 102432.
- [58] Zhu L., Karim M.M., Sharif K. et al. Traffic Flow Optimization for UAVs in Multi-Layer Information-Centric Software-Defined FANet // IEEE Transactions on Vehicular Technology. – 2023. – Vol. 72, No. 2. – P. 2453–2467.
- [59] GOST 34.11-2018. Информационная технология (ИТ). Криптографическая зашита информации. Функция хеширования (s popr. ot 15.03.2021) / Oficial'noe izdanie. – Moskva: Standartinform, 2018 – 20 s.
- [60] GOST R ISO/MJEK 29182-1-2018. Информационные технологии. Структура архитектуры для сенсорных сетей (SNRA). Част' 1. Общий обзор и требования. / Oficial'noe izdanie. – Moskva: Standartinform, 2018 – 10 s.
- [61] GOST R 59162-2020. Национальный стандарт Российской Федерации. Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей. Част' 6. Обеспечение информационной безопасности при использовании беспроводных IP-сетей. / Oficial'noe izdanie. – Moskva: Standartinform, 2020 – 26 s.
- [62] GOST R 59519-2021. Беспилотные авиационные системы. Компоненты беспилотных авиационных систем. Спецификация и общие технические требования. / Oficial'noe izdanie. – Moskva: Standartinform, 2021 – 6 s.
- [63] Управление подвижными объектами. Библиографический указатель. V 3 выпуск. Выпуск 2. Аэродинамические объекты / под ред. В.М. Глумова; Учреждение РАН Институт проблем управления им. В.А. Трапезникова РАН. – Moskva: 2011. – 374s