УДК 004.056.53 DOI: 10.18698/2541-8009-2022-03-779

АНАЛИЗ ПРОБЛЕМ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ БЕСПРОВОДНЫХ САМООРГАНИЗУЮЩИХСЯ СЕТЕЙ НА ОСНОВЕ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

Г.И. Кулагин
gleb.kulagin@yandex.ru
SPIN-код: 9475-2356

МГТУ им. Н.Э. Баумана, Москва, Российская Федерация

Аннотация

Среди перспективных сетевых технологий в последнее время особую актуальность приобретают беспроводные самоорганизующиеся сети на основе беспилотных летательных аппаратов, характерные особенности которых предполагают наличие ряда проблем при их практическом применении. Одна из основных проблем — информационная безопасность, к решению которой на данный момент не существует общепризнанных и стандартизированных подходов. На основе результатов исследования особенностей беспроводных самоорганизующихся сетей на базе беспилотных летательных аппаратов проанализированы проблемы обеспечения их безопасности, в том числе с точки зрения защиты конфиденциальности, целостности и доступности циркулирующей в них информации.

Ключевые слова

Беспроводные самоорганизующиеся сети, беспилотные летательные аппараты, информационная безопасность, уязвимости безопасности, угрозы информационной безопасности, атака, защита информации, FANET

Поступила в редакцию 24.02.2022

Введение. Использование беспилотных летательных аппаратов (БЛА) в качестве основы для формирования сетевой инфраструктуры рассматривается как эффективный способ для повышения телекоммуникационных возможностей беспроводных самоорганизующихся сетей, главные преимущества которых состоят в универсальности, гибкости, сравнительно небольших расходах и исключении человеческого фактора при выполнении многочисленных задач в интересах различных отраслей экономики.

На сегодняшний день наибольший интерес представляют не только одиночные БЛА, но и целые их группы, применение которых повышает эффективность выполнения поставленных задач и сокращает время на их исполнение. Вместе с тем отличительные свойства беспроводных самоорганизующихся сетей на основе БЛА, такие как высокая мобильность и низкая плотность узлов, динамичные и частые изменения топологии сети, а также отсутствие централизованного управления осложняют реализацию требований по информационной безопасности при их практическом применении. Поэтому решение проблем обеспечения конфиденциальности, целостности и доступности информации, циркулирующей в беспроводных самоорганизующихся сетях на

основе БЛА, является одним из актуальных направлений исследований для развития сетей подобного типа.

Особенности беспроводных самоорганизующихся сетей на основе БЛА. Одно из перспективных направлений развития беспроводных самоорганизующихся сетей — сети, основу (узлы) которых составляют БЛА, известные в литературе как FANET (англ. *Flying Ad-Hoc Networks* — летающие специальные сети) [1].

Сети на основе беспилотных летательных аппаратов, образующих летающий сегмент сети, имеют распределенную структуру, обеспечивающую беспроводную связь между узлами (БЛА) без какой-либо дополнительной инфраструктуры с поддержкой самоорганизации, и могут быть применены при решении широкого спектра задач для гражданского сектора экономики, включая:

– мониторинг участков местности в процессе осуществления поисковых и иных видов аварийно-спасательных работ в режиме реального времени;

– сбор данных и контроль загрязнений окружающей среды, территорий возникновения чрезвычайных ситуаций природного и техногенного характера, состояния трасс газо- и нефтепроводов, линий электропередач, загруженности автомобильных магистралей, лесных и сельскохозяйственных угодий;

– создание условий для организации временной связи в районах ликвидации последствий стихийных бедствий;

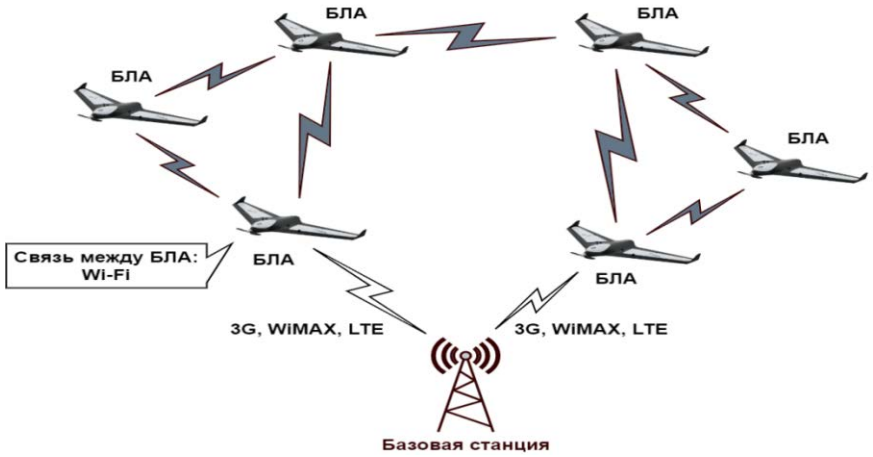
– обеспечение и сопровождение работ при проведении экологического контроля территорий и акваторий, зондирования и аэрофотосъемки земной поверхности.

Анализ практического применения БЛА показывает необходимость одновременного участия при решении большинства таких задач не одного, а целой группы взаимодействующих малоразмерных БЛА, благодаря чему обеспечиваются высокая отказоустойчивость, надежность, масштабируемость, увеличение времени действия, сокращение сроков и снижение стоимости выполнения конкретных заданий [2, 3].

При проектировании сетей с несколькими БЛА необходимо учитывать, что из-за динамических изменений окружающей среды, топологии сети и движения узлов, подобного типа сети не всегда поддерживают свои соединения. Альтернативное коммуникационное решение для систем с несколькими БЛА — организация сетей типа FANET.

В типичной структуре FANET в то время, когда одни БЛА связываются с базовой станцией, другие могут получать данные непосредственно через каналы связи с соседними БЛА, минуя базовую станцию. Пример архитектуры сети FANET представлен на рисунке [4].

Показанная на рисунке архитектура сети FANET представляет собой топологию ячеистой сети, узлы которой связываются друг с другом в воздушном пространстве посредством стандартных беспроводных технологий передачи данных (например, Wi-Fi). При взаимодействии узлов сети с базовой станцией используются мобильные сети сотовой связи (3G, WiMAX, LTE).



Пример архитектуры сети FANET

Беспроводные самоорганизующиеся сети на основе БЛА характеризуются:

– крайне высокой степенью мобильности узлов. Узлы сети (БЛА) перемещаются с большими скоростями, что приводит к динамичным изменениям топологии сети и ее разделению на отдельные части (разрывам каналов связи между отдельными узлами);

– разнообразными моделями мобильности узлов. Движение узлов в сети задается посредством некоторого алгоритма, которое в реальной среде может быть изменено из-за влияния внешних факторов (погодные условия, характер выполняемых задач и т. п.). В соответствии с этим существует несколько моделей мобильности узлов, образующих сети типа FANET [5]:

1) модели случайной мобильности — простейшие и самые часто применяемые модели движения, используемые при исследовании сетей;

2) модели мобильности, зависящие от пространственно-временных характеристик, — модели, основанные на устранении резких изменений скорости и траектории движения узлов;

3) модели мобильности с заранее определенной траекторией — модели, устанавливающие для узлов сети траекторию определенной формы;

4) модели групповой мобильности — модели, которые накладывают определенные пространственные ограничения на все узлы сети;

5) модели мобильности, основанные на контроле топологии сети, используемые в случаях, когда необходимо отслеживать топологию сети в режиме реального времени. Пример — модель, применяемая в сетях, предназначенных для обследования местности или поисковых операций, где каждый БЛА отмечает на карте сканируемые области и транслирует эти данные в сеть;

– достаточно низкой плотностью узлов. Узлы сети распределены в пространстве, а расстояние между БЛА может составлять несколько километров;

– более динамичными и частыми изменениями топологии сети. Высокая мобильность узлов, отказы в их работе, добавления к сети новых узлов и перебои в работе каналов связи приводят к быстрым и частым изменениям топологии;

– оптимизацией времени действия сети. У малоразмерных БЛА запаса мощности для осуществления полета и организации связи может быть недостаточно, что приводит к сокращению времени действия сети;

– адаптивностью к быстро меняющимся текущим наборам параметров сети. Многие параметры сети на основе БЛА изменяются во время выполнения задач. Сеть должна адаптироваться в соответствии с плотностью узлов, расстоянием между узлами и изменениями условий окружающей среды;

– особыми моделями распространения радиоволн. Рабочая среда сети обладает рядом проблем, оказывающих влияние на характеристики распространения радиоволн, а именно: большие различия расстояний между узлами; типы антенн (всенаправленного или узконаправленного действия); природно-климатические условия и т. п.;

– ограничениями платформы БЛА. Применение малоразмерных БЛА накладывает ограничения на размеры и вес полезной нагрузки для размещения на борту необходимого вычислительного и коммуникационного оборудования;

– устойчивостью полета БЛА. Малоразмерные БЛА сильно подвержены неустойчивым потокам естественной турбулентности атмосферы;

– необходимостью точного определения местоположения узлов сети. Из-за высокой скорости и различных моделей мобильности систем с БЛА требуются более точные данные о местоположении узлов, что достигается путем применения системы глобального позиционирования GPS с инерциальным измерительным блоком.

Характерные особенности беспроводных самоорганизующихся сетей на основе БЛА осложняют реализацию функций безопасности при их практическом применении и создают необходимость детального и точного анализа проблем обеспечения конфиденциальности, целостности и доступности циркулирующей в них информации.

Причины и источники уязвимостей безопасности беспроводных самоорганизующихся сетей на основе БЛА. Обеспечение безопасности беспроводных самоорганизующихся сетей является определяющим фактором и вместе с тем сложной задачей при их создании и эксплуатации [6]. Главным образом реализация функций безопасности осложняется для беспроводных самоорганизующихся сетей на основе БЛА, характерные особенности функционирования которых постоянно формируют новые условия для возникновения уязвимостей, что делает возможным реализацию угроз их безопасности. Наиболее частыми причинами и источниками возникновения уязвимостей безопасности в сетях типа FANET являются [7]:

– общая доступность среды передачи данных. Предоставляет возможность осуществления несанкционированного доступа к каналам управления и связи злоумышленникам с целью прослушивания, перехвата и анализа циркулирующей в сети информации, а также подмены циркулирующих в сети сообщений;

– низкая живучесть и защищенность узлов сети. Приводит к возможности целенаправленных воздействий любого рода на узлы сети со стороны злоумыш-

ленников вплоть до их физического уничтожения, компрометации, устранения из сети или использования в собственных целях;

– отсутствие стандартизации, централизованного управления и системы доверенной верификации узлов сети. Допускает размещение в сети как изначально вредоносных узлов, так и легитимных узлов с уязвимым управляющим программным обеспечением;

– отсутствие инфраструктуры, фиксированной топологии и центральных узлов. Делает невозможными реализацию единой политики безопасности, а также применение классических схем безопасности, таких как центры сертификации и центральные серверы;

– более динамичный и частый характер изменения топологии сети. Требует использования специализированных протоколов маршрутизации, учитывающих вероятность появления некорректной информации от скомпрометированных узлов в результате изменения топологии сети.

Уязвимости безопасности дают возможность реализации угроз безопасности информации, циркулирующей в сетях типа FANET, за счет несанкционированного доступа и (или) воздействия на сетевые элементы.

Особенности угроз информационной безопасности беспроводных самоорганизующихся сетей на основе БЛА. Целью определения угроз информационной безопасности является установление того, существует ли возможность нарушения конфиденциальности, целостности и доступности информации, циркулирующей в беспроводных самоорганизующихся сетях на основе БЛА, а также приведет ли изменение хотя бы одного из указанных свойств к серьезным негативным последствиям (неприемлемому ущербу) для защищенности информационной среды сетей подобного типа [8].

Необходимо отметить, что беспроводные самоорганизующиеся сети на основе БЛА уязвимы как к классическим типам атак, которым подвержены все беспроводные сети, так и к атакам специфическим, особенным. Ввиду того, что сети подобного типа не имеют фиксированной топологии, центральных узлов, стабильных источников питания, постоянной связи между узлами задача злоумышленника по реализации успешной атаки становится легче выполнимой.

С точки зрения анализа информационной системы беспроводные самоорганизующиеся сети на основе БЛА представляют собой интегрированный комплекс таких функций, как сбор, передача и обработка данных, а также контроль, что делает их уязвимыми для многих атак различного типа [9, 10]. Угрозу информационной безопасности в сетях типа FANET представляют самые разные категории нарушителей, которых в большинстве случаев можно распределить на внешних и внутренних.

Внешний нарушитель не является участником FANET, не имеет каких-либо ключей, аутентификационных и любых других данных, повышающих его статус в сети. Внешний нарушитель может пытаться попасть в сеть, манипулировать трафиком и передаваемыми данными, влиять на работоспособность сети и на внешние источники данных, которые используют узлы сети (БЛА). Внутренний

нарушитель является активным или пассивным участником сети и обладает криптографическими данными, необходимыми для прохождения аутентификации. Внутренний нарушитель пытается снизить работоспособность сети или манипулировать трафиком и передаваемыми данными для того, чтобы добиться своих целей.

По свойствам информации (конфиденциальность, целостность, доступность) в рамках рассматриваемых беспроводных самоорганизующихся сетей на основе БЛА могут быть выделены следующие три класса угроз информационной безопасности.

Класс 1. Угрозы конфиденциальности (неправомерный доступ к информации). Является основным классом угроз для беспроводных сетей, поскольку этому способствует сама среда передачи данных. Нарушителю не нужен физический порт для подключения к сети, ему достаточно находится в относительной близости к беспроводной сети для того, чтобы ее атаковать.

Наиболее типичными атаками, которые могут быть направлены на сети типа FANET в контексте данного класса угроз, являются:

– атака типа «Человек посередине» (от англ. *Man In The Midle* — MITM). Тип атаки, подразумевающий, что нарушитель тайно ретранслирует и при необходимости изменяет сообщения между двумя участниками сети, которые считают, что они непосредственно общаются друг с другом. Это метод компрометации канала связи, при котором нарушитель, подключившись к каналу между двумя участниками сети, осуществляет вмешательство в протокол передачи, перехватывая, прослушивая, удаляя или изменяя сообщения;

– атака типа «Прослушивание среды передачи» (от англ. *Eavesdropping*), заключающаяся в том, что нарушитель использует поддельные узлы для прослушивания циркулирующей в сети информации;

– атаки, направленные на кражу идентификационных данных или попытку их подмены. Подразумевается попытка нарушителя выдать себя за участника сети после кражи криптографических ключей.

Класс 2. Угрозы целостности (неправомерное изменение данных). Такие угрозы связаны с вероятностью модификации циркулирующей в сети информации, что может быть вызвано различными факторами — от умышленных действий нарушителей до выхода из строя оборудования. Основными атаками угроз данного класса являются:

– атаки, направленные на подмену данных, получаемых участниками сети от внешних источников. Эти атаки нацелены на изменение или искажение данных, которые не являются частью сети, но все равно являются одним из источников данных для конкретного участника сети, например, это может быть GPS. Подменяя спутниковые данные GPS, нарушитель может обмануть участника сети и заставить его действовать так, как необходимо нарушителю;

– атаки, направленные на искажение сообщений. Нарушитель может намеренно пытаться исказить информацию, передаваемую в сообщении, для прерывания связи между узлами сети.

Класс 3. Угрозы доступности (осуществление действий, делающих невозможным или затрудняющих доступ к ресурсам сети). Любые беспроводные сети изначально уязвимы к данным угрозам, так как нарушитель может подавлять сигналы, используя для этого более мощные передатчики. К основным атакам этого класса угроз могут быть отнесены:

– атаки типа «Отказ в обслуживании» (от англ. *Denial of Service* — DoS) на сеть целиком. Атаки данного типа представляют собой попытки подавить радиосигнал на определенной частоте. Таким атакам способствует среда передачи данных, в которой распространяется радиосигнал, поскольку она никак не ограничена и доступна потенциальному нарушителю;

– атаки типа «Отказ в обслуживании» (DoS) на отдельные узлы сети или конкретного участника. Атаки такого типа являются аналогом атак типа «наводнение» (от англ. *Flood*) в TCP/IP-сетях. Цель таких атак — заставить узел сети обрабатывать большое количество сообщений, вследствие чего настоящие сообщения могут теряться и не обрабатываться этим узлом;

– атаки типа «Отказ в обслуживании» (DoS) на уровне приложений и протокола. Нарушителю необходимо обнаружить в протоколе или приложениях операции, требующие больших энергетических и вычислительных затрат. Затем нарушитель сможет воспользоваться этим, заставляя сетевое устройство выполнять подобные операции постоянно, из-за чего оно будет работать вплоть до израсходования энергетических ресурсов. Кроме того, устройство перестает быть доступным для выполнения других задач.

Также необходимо выделить актуальные для сетей типа FANET атаки, объединяющие в себе несколько классов угроз, среди которых следует отметить [11]:

– атаки, направленные на физическую компрометацию одного из узлов сети. Нарушитель может похитить аутентификационные данные участника сети, а также изменить программу самого устройства и его задачи так, чтобы атаковать сеть;

– атаки, основанные на повторном использовании аутентифицированных или корректных сообщений. Примером может служить атака типа «Переотправка сообщений» (от англ. *Replay* — повтор) (от англ. *Replay*), обусловленная возможностью внешнего нарушителя прослушивать беспроводную среду передачи данных и осуществлять перехват передаваемых сообщений с целью их дальнейшей ретрансляции. Реализуя данную атаку на физическом уровне, внешний нарушитель способен вызывать отказ в обслуживании сетевых сервисов, работающих на более высоких уровнях сетевой модели;

– атаки, направленные на сетевые протоколы. Например, атака типа «Подмена адреса» (от англ. *Address Spoofing*), по аналогии с известной атакой ARP-spoofing, применяемой в сетях с использованием протокола ARP (англ. *Address Resolution Protocol* — протокол разрешения адресов) и являющейся разновидностью сетевой атаки типа MITM;

– атаки, направленные на транспортные протоколы и протоколы маршрутизации. Для беспроводных самоорганизующихся сетей в целом характерны не-

сколько типов атак, направленных на маршрутизацию в сети, которые в итоге могут приводить к возможности реализации других атак. Например, атаки, связанные с объявлением себя маршрутизирующим устройством, могут привести к атакам типа MITM и DoS путем уничтожения всего сетевого трафика. К числу подобного рода атак относят следующие:

1) атака типа «Воронка» (от англ. *Sinkhole*), в ходе которой нарушитель компрометирует узел, расположенный ближе к узлу-получателю (узел «воронки») и делает его особенно привлекательным для соседних узлов сети относительно слабых протоколов маршрутизации, тем самым направляя через него почти весь трафик из определенной области сети. Последствия — изменение или утечка конфиденциальных и иных данных;

2) атака типа «Черная дыра» (от англ. *Black Hole*), заключающаяся в способности ее реализации внутренним нарушителем путем предотвращения дальнейшего распространения переданных ему пакетов данных. Данная атака актуальна для сетей, в которых используются протоколы маршрутизации. В сетях с широковещательным распространением сообщений нарушителю необходимо скомпрометировать все узлы, связанные с целевым узлом атаки, для ее успешной реализации;

3) атака типа «Выборочная пересылка» (от англ. *Grey Hole* — серая дыра) — заключается в том, что нарушитель влияет на протокол маршрутизации с целью построения маршрутов для соседних узлов сети, которые будут проходить через узел нарушителя (аналогично Black Hole). Далее нарушитель выборочно выполняет сброс пересылаемых через него пакетов данных, выбор которых осуществляется как случайным образом, так и по определенному алгоритму;

4) атака типа «Червоточина» (от англ. *Wormhol*), суть которой заключается в том, что внутренний нарушитель, осуществляющий контроль над более чем одним узлом сети, способен отслеживать путь передачи сообщений благодаря использованию более быстрого и менее загруженного выделенного канала связи между подконтрольными узлами с целью получения предпочтения при формировании пути в динамических протоколах маршрутизации либо связи в протоколах построения сети;

5) атака типа «Фальсификация параметров маршрутизации» (от англ. *Alteration* — изменение), заключающаяся в способности внутреннего нарушителя осуществлять передачу поддельной информации, используемой в качестве параметров выбора оптимального пути в протоколах маршрутизации. Реализуя данный тип атаки, нарушитель влияет на построение маршрута передачи сообщений в сети с целью их дальнейшего перехвата, изменения либо сброса;

6) атака типа «Переполнение таблиц маршрутизации» (от англ. *Routing Table Overflow*) для реализации которой нарушитель вмешивается в работу протоколов маршрутизации и создает множество маршрутов к несуществующим узлам сети. Цель — «переполнение» таблиц маршрутизации узлов сети, что делает невозможным добавление в них легитимных маршрутов.

Обзор особенностей угроз информационной безопасности беспроводных самоорганизующихся сетей на основе БЛА предоставляет возможность конкретизации требований к обеспечению защиты конфиденциальности, целостности и доступности циркулирующей в них информации.

Требования к информационной безопасности беспроводных самоорганизующихся сетей на основе БЛА. Главное требование к информационной безопасности любой вычислительной сети — сбалансированная защита конфиденциальности, целостности и доступности информации, циркулирующей в этой сети, с учетом целесообразности применения и без какого-либо ущерба ее производительности [10].

Данный подход, а также особенности угроз безопасности информации в сетях типа FANET позволяют определить следующие требования к их информационной безопасности:

– возможность защиты любых каналов связи сети от атак типа «Человек посередине» (MITM) и «Переотправка сообщений» (Replay), а также атак, направленных на искажение сообщений, и атак, направленных на подмену данных от внешних источников. Указанные атаки дают возможность злоумышленнику подорвать работоспособность сети и нарушить конфиденциальность циркулирующей в ней информации, поскольку без надлежащей защиты он может перехватывать и модифицировать пакеты данных таким образом, чтобы добиться своих целей, например, захватить управление сетью и использовать ее для собственной выгоды. Названные требования могут быть выполнены при применении криптографических протоколов аутентификации и групповой аутентификации, а также с использованием инфраструктуры открытых ключей (от англ. *Public Key Infrastructure* — PKI) и шифрования каналов связи;

– осуществимость проведения мероприятий, направленных на снижение риска и влияния на каналы связи сети и сеть в целом атак типа «Отказ в обслуживании» (DoS), поскольку гарантировать полную защиту от атак этого типа не представляется возможным из-за общей доступности самой среды передачи данных. Также необходимы меры по выявлению и реагированию на попытки реализации атак данного типа, например, определение местоположения устройств, используемых для подавления выявленных и передаваемых по каналам связи сигналов;

– возможность выявления скомпрометированных устройств и механизмов исключения участника из сети путем внедрения в сеть доверительных отношений между узлами (БЛА). Кроме того, необходимы аппаратно-программные средства, усложняющие компрометацию конкретного узла сети при физическом доступе к нему;

– допустимость использования сетевых протоколов и протоколов маршрутизации, которые исключают или снижают вероятность проведения атак на сетевой уровень, таких как атаки типа MITM или типа DoS. В данных протоколах также могут применяться механизмы доверительных отношений;

– масштабируемость всех мероприятий, направленных на обеспечение информационной безопасности сети. Вместе с тем на проведение этих мероприя-

тий не должны оказывать влияние такие характерные особенности сети, как высокая мобильность и низкая плотность узлов, а также динамичные и частые изменения топологии.

Анализ угроз безопасности информации, циркулирующей в беспроводных самоорганизующихся сетях на основе БЛА, и требований к защите ее конфиденциальности, доступности и целостности, показывает, что наиболее важными с точки зрения информационной безопасности являются сетевой и канальный уровни, мероприятия в отношении защищенности которых целесообразно осуществлять как за счет разработки методов построения устойчивой к угрозам архитектуры сети, так и за счет исследования различных подходов и механизмов обеспечения безопасности сетей подобного типа и их дальнейшей реализации.

Выводы. В статье на основе исследования отличительных свойств беспроводных самоорганизующихся сетей с беспилотными летательными аппаратами, проведен анализ проблем обеспечения их информационной безопасности, в том числе с точки зрения оценки причин и источников уязвимостей, особенностей угроз их информационной безопасности, а также требований к защите конфиденциальности, целостности и доступности информации. Отличительные свойства беспроводных самоорганизующихся сетей на основе БЛА формируют новые условия для возникновения уязвимостей, которые создают возможности для реализации различных угроз, направленных на нарушение конфиденциальности, целостности и доступности циркулирующей в сетях подобного типа информации, и осложняют выполнение функций безопасности в процессе их функционирования.

Таким образом, информационная безопасность остается одной из основных проблем при создании и использовании беспроводных самоорганизующихся сетей с БЛА. К решению этой проблемы на данный момент не существует общепризнанных и стандартизированных подходов. Тем не менее проведенные и планируемые дальнейшие исследования в этой области дают основания рассчитывать на появление уникальных механизмов и методов, нацеленных на обеспечение устойчивого состояния информационной безопасности беспроводных самоорганизующихся сетей на основе БЛА.

Литература

[1] Bekmezci I., Sahingoz O.K., Temel S. Flying ad-hoc networks (FANETs): a survey. *Ad Hoc Networks*, 2013, vol. 11, no. 3, pp. 1254–1270. DOI: http://dx.doi.org/10.1016/j.adhoc.2012.12.004

[2] Krichen L., Fourati M., Fourati L.C. Communication architecture for unmanned aerial vehicle system. *ADHOC-NOW*. Springer, 2018, pp. 213–225. DOI: https://doi.org/10.1007/978-3-030-00247-3_20

[3] Чертова О.Г., Чиров Д.С. Построение опорной сети связи на базе малоразмерных беспилотных летательных аппаратов с отсутствием наземной инфраструктуры. *Наукоемкие технологии в космических исследованиях Земли*, 2019, т. 11, № 3, с. 60–71.

[4] Hentati A.I., Fourati L.C. Comprehensive survey of UAVs communication networks. *Comput. Stand. Interfaces*, 2020, vol. 72, art. 103451. DOI: https://doi.org/10.1016/j.csi.2020.103451

[5] Bujari A., Palazzi C.E., Ronzani D. FANET application scenarios and mobility models. *DroNet '17*, 2017, pp. 43–46. DOI: https://doi.org/10.1145/3086439.3086440

[6] Бельфер Р.А. Угрозы информационной безопасности в беспроводных саморегулирующих сетях. *Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение*, 2011, № S1, с. 116–124.

[7] Демидов Р.А., Зегжда П.Д. Унифицированная модель многоуровневых угроз нарушения информационной безопасности в сетях с динамической топологией. *Интеллектуальные технологии на транспорте*, 2019, № 2, с. 10–14.

[8] Sampigethaya K., Poovendran R., Bushnell L. Security of future eEnabled aircraft ad hoc networks. *AIAA Meeting Paper*, 2008, no. 2008-8894. DOI: https://doi.org/ 10.2514/6.2008-8894

[9] Altawy R., Youssef A.M. Security, privacy and safety aspects of civilian drones: a survey. *ACM Trans. Cyber-Phys. Syst.*, 2016, vol. 1, no. 2, pp. 1–25. DOI: https://doi.org/10.1145/3001836

[10] Dahiya S., Garg M. Unmanned aerial vehicles: vulnerability to cyber attacks. *Proc. UASG 2019*. Springer, 2020, pp. 201–211. DOI: https://doi.org/10.1007/978-3-030-37393-1

[11] He C., Chan S., Guizani M. Drone-assisted public safety networks: the security aspect. *Commun. Mag.*, 2017, vol. 55, no. 8, pp. 218–223. DOI: https://doi.org/ 10.1109/MCOM.2017.1600799CM

Кулагин Глеб Игоревич — аспирант кафедры «Информационная безопасность», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Научный руководитель — Лебедев Анатолий Николаевич, кандидат физико-математических наук, доцент кафедры «Информационная безопасность», МГТУ им. Н.Э.Баумана, Москва, Российская Федерация.

Ссылку на эту статью просим оформлять следующим образом:
Кулагин Г.И. Анализ проблем обеспечения безопасности беспроводных самоорганизующихся сетей на основе беспилотных летательных аппаратов. *Политехнический молодежный журнал*, 2022, № 03(68). http://dx.doi.org/10.18698/2541-8009-2022-03-779

ANALYSIS OF SECURITY ISSUES OF WIRELESS SELF-ORGANIZING NETWORKS BASED ON UNMANNED AERIAL VEHICLES

G.I. Kulagin

gleb.kulagin@yandex.ru
SPIN-code: 9475-2356

Bauman Moscow State Technical University, Moscow, Russian Federation

Abstract

Among the promising network technologies, wireless self-organizing networks based on unmanned aerial vehicles have recently become particularly relevant, and their characteristics cause a number of issues in their practical application. One of the main problems is information security for which there are no generally accepted and standardized approaches at present. Based on the study results of the features of wireless self-organizing networks based on unmanned aerial vehicles the problems of ensuring their security, including the protection of confidentiality, integrity and accessibility of circulating information in them are analyzed.

Keywords

Wireless self-organizing networks, unmanned aerial vehicles, information security, security vulnerabilities, information security threats, attack, information protection, FANET

Received 24.02.2022

References

[1] Bekmezci I., Sahingoz O.K., Temel S. Flying ad-hoc networks (FANETs): a survey. *Ad Hoc Networks*, 2013, vol. 11, no. 3, pp. 1254–1270. DOI: http://dx.doi.org/10.1016/j.adhoc.2012.12.004

[2] Krichen L., Fourati M., Fourati L.C. Communication architecture for unmanned aerial vehicle system. *ADHOC-NOW*. Springer, 2018, pp. 213–225. DOI: https://doi.org/10.1007/ 978-3-030-00247-3_20

[3] Chertova O.G., Chirov D.S. Building a core communication network which is based on small size unmanned aircraft vehicle without ground infrasrtucture. *Naukoemkie tekhnologii v kosmicheskikh issledovaniyakh Zemli* [High Technologies in Earth Space Research], 2019, vol. 11, no. 3, pp. 60–71 (In Russ.).

[4] Hentati A.I., Fourati L.C. Comprehensive survey of UAVs communication networks. *Comput. Stand. Interfaces*, 2020, vol. 72, art. 103451. DOI: https://doi.org/10.1016/j.csi.2020.103451

[5] Bujari A., Palazzi C.E., Ronzani D. FANET application scenarios and mobility models. *DroNet '17*, 2017, pp. 43–46. DOI: https://doi.org/10.1145/3086439.3086440

[6] Bel'fer R.A. Information security threat in wireless self-regulated networks. *Vestn. Mosk. Gos. Tekh. Univ. im. N.E. Baumana, Priborostr.* [Herald of the Bauman Moscow State Tech. Univ., Instrum. Eng.], 2011, no. S1, pp. 116–124 (In Russ.).

[7] Demidov R.A., Zegzhda P.D. Unified model of multilevel security threats in networks with dynamic topology. *Intellektual'nye tekhnologii na transporte* [Intellectual Technologies on Transport], 2019, no. 2, pp. 10–14 (In Russ.).

[8] Sampigethaya K., Poovendran R., Bushnell L. Security of future eEnabled aircraft ad hoc networks. *AIAA Meeting Paper*, 2008, no. 2008-8894. DOI: https://doi.org/ 10.2514/6.2008-8894

[9] Altawy R., Youssef A.M. Security, privacy and safety aspects of civilian drones: a survey. *ACM Trans. Cyber-Phys. Syst*., 2016, vol. 1, no. 2, pp. 1–25. DOI: https://doi.org/10.1145/3001836

[10] Dahiya S., Garg M. Unmanned aerial vehicles: vulnerability to cyber attacks. *Proc. UASG 2019*. Springer, 2020, pp. 201–211. DOI: https://doi.org/10.1007/978-3-030-37393-1

[11] He C., Chan S., Guizani M. Drone-assisted public safety networks: the security aspect. *Commun. Mag*., 2017, vol. 55, no. 8, pp. 218–223. DOI: https://doi.org/10.1109/MCOM.2017.1600799CM

Kulagin G.I. — Postgraduate Student, Department of Information Security, Bauman Moscow State Technical University, Moscow, Russian Federation.

Scientific advisor — Lebedev A.N., Cand. Sc. (Phys.-Math.), Assoc. Professor, Department of Information Security, Bauman Moscow State Technical University, Moscow, Russian Federation.

Please cite this article in English as:
Kulagin G.I. Analysis of security issues of wireless self-organizing networks based on unmanned aerial vehicles. *Politekhnicheskiy molodezhnyy zhurnal* [Politechnical student journal], 2022, no. 03(68). http://dx.doi.org/10.18698/ 2541-8009-2022-03-779.html (in Russ.).