ЗАДАЧИ ВНЕДРЕНИЯ А-СЕТИ в управлении воздушным движением

С.Шаврин, д.т.н., профессор МТУСИ /sss@mtuci.ru,
Н.Лихачев, к.т.н., доцент МТУСИ / n.likhachev@inbox.ru,
М.Воронкова, зам. декана МТУСИ,
М.Лихачев, студент МТУСИ

УДК. 621.391, DOI: 10.22184/2070-8963.2022.106.6.70.74

Рассмотрены вопросы обеспечения ситуационной осведомленности пилотов воздушных судов средствами самоорганизующихся сетевых технологий (А–сети) автоматического зависимого наблюдения вещательного типа. Отмечается необходимость и рассматриваются средства обеспечения информационной безопасности передаваемых сообщений в плане поддержки как их конфиденциальности, так и аутентификации, целостности и защиты от повторов ранее переданных.

Обеспечение участников и органов управления воздушным движением ситуационной осведомленностью и фиксация фактов аварийных ситуаций и координат воздушных судов (ВС) для ускорения спасения и других действий, направленных на снижение последствий аварий – основное назначение систем наблюдения за воздушными судами [1, 2]. Сетевые технологии, не требующие привязки к инфраструктуре, существенно расширяют зону наблюдения, однако при низкой плотности воздушных судов в расчете на единицу земной поверхности, например, в океанических зонах и зоне вечной мерзлоты, объекты могут оказываться за пределами наблюдения.

Радикальным решением проблемы ограниченности зоны радиообзора может явиться включение в контур автоматического зависимого наблюдения вещательного типа (АЗН-В) низколетящих космических аппаратов (КА). Некоторые системы спутниковой связи, базирующиеся на низких круговых околоземных орбитах, хорошо соответствуют протоколам сетевых систем АЗН-В, обеспечивая возможность глобальной поддержки наблюдения в приемлемых стоимостных рамках [1].

Качественно новые возможности наблюдения объектов, передвигающихся в воздушном пространстве, открыла эпоха создания глобальных навигационных спутниковых систем (GPS, ГЛОНАСС и т.п.). Для передачи информации с этих систем пилотам других судов и наземным службам для радикального решения проблемы ситуационной осведомленности и регистрации аварийных ситуаций Международная организация гражданской авиации (ИКАО) разработала концепцию АЗН-В [1].

К сожалению, угрозы сегодня очень существенно возросли: квалифицированный терроризм в авиации и противостояние России со странами блока НАТО. Вследствие этого появляются возможности следующих видов атак на сигналы АЗН-В:

- радиоперехват с целью определения реальных координат конкретного ВС;
- организация целенаправленных квалифицированных помех, подобных реальным сигналам АЗН-В, – фантомов;

- завал спамом экрана диспетчера или ВС;
- атака на сигналы ГНСС ("грубое" подавление спутниковых сигналов наведенной помехой, генерация в эфир сигналов "ложных" спутников).

Радикальным решением проблемы наблюдения за ВС, обеспечивающим достаточную ситуационную осведомленность пилотов с охватом потенциально опасных объектов, является система АЗН-В на основе самоорганизующихся сетевых технологий – А-сеть [3]. Функциональное назначение А-сети заключается в обеспечении возможности конфиденциального аутентифицированного обмена информацией между объектами, находящимися в зоне взаимного радиодоступа (каждый объект имеет радиодоступ хотя бы к одному смежному объекту А-сети). При отсутствии прямого радиодоступа между двумя объектами передача информации между ними осуществляется через другие, смежные объекты.

А-сеть строится по самоорганизующимся принципам [4], карта сети содержит:

- текущую архитектуру сети в форме географических координат доступных для связи объектов и взаимных связей между ними;
- таблицу расстояний между объектами, вычисленных по их географическим координатам;
- таблицу расстояний между объектами, вычисленную по измеренному значению времени распространения сигналов между объектами;
- таблицу пропускной способности каналов между объектами;
- рельеф местности для прогнозирования пределов зоны прямого радиодоступа.

Механизмом организации сетей, аутентификации и обеспечения конфиденциальности служит комбинация принципов симметричной и двухключевой криптографии, причем двухключевые алгоритмы используются для аутентифицированного конфиденциального обмена сеансовым ключом, а симметричные – для поддержки вещательного, в пределах сети, режима защищенного обмена сообщениями.

На одной несущей частоте может быть обеспечена организация нескольких независимых сетей по общему принципу "каждому должно быть доступно только то, на что у него есть права". Возможна также организация каналов защищенного обмена между сетями. Таким образом, А-сеть обеспечивает решение задач наблюдения и ситуационной осведомленности в защищенном от перехвата, повторов, фантомов и других деструктивных воздействий режиме.

Рассмотренные технологии были представлены и защищены российской делегацией на 38-й сессии Ассамблеи ИКАО и вошли в том 6 приложения 10 Конвенции по гражданской авиации.

Обмен информацией между объектами А-сети осуществляется в спектре 118–136,975 МГц, где для этой цели для международных полетов выделены две несущие частоты: 113,250 и 136,925 МГц – и необходимое количество может быть выделено для национальных требований.

В целях более рационального использования общего спектрального ресурса с учетом статистики трафика в разных регионах представляется целесообразным разделение национальных каналов АЗН-В на магистральные – общие для страны или больших территорий – и местные, назначаемые из числа наиболее свободных в данном регионе. Следует учитывать, что в будущем диапазон настройки для передатчика может также охватывать любой из каналов шириной 25 кГц в диапазоне от 112,0 до 117,975 МГц, а для приемника может использоваться любой из каналов шириной 25 кГц.

Каждый объект А-сети (ВС, наземное транспортное средство, а также наземная станция) должен быть оснащен системами для определения местоположения для синхронизации передачи и приема данных. В стандарте передачи данных время канала делится на слоты, имеющие во времени постоянную длину 13,33 мс. "Суперфрейм", который является важным термином, используемым в канальном управлении, состоит из группы слотов, которые охватывают период в 60 с. Он содержит 4 500 слотов (75 слотов в секунду).

Каждый временно́й слот доступен для приема или передачи информации от любого объекта А-сети, поддерживающего связь на одной несущей частоте. Одно сообщение минимальной длины, содержащее информацию только о местоположении объекта, занимает один временно́й слот. Другие, более длинные, сообщения могут занимать несколько слотов, вплоть до 75. Такое сообщение размером 2 400 байт будет передаваться в течение 1 с.

Гибкая структура сообщения позволяет станции передавать сообщение и одновременно

резервировать слоты для ответа или будущего использования.

Применяемый для построения А-сети протокол требует синхронизации времени для обеспечения бесконфликтного доступа к частотному ресурсу без взаимных помех (UTC – стандарт времени, который является универсальным скоординированным временем). Концепция синхронизации времени должна удовлетворять самым строгим требованиям к точности, непрерывности и целостности работы для авиации.

Синхронный характер сети обеспечивает возможность локализации источников злонамеренных воздействий, а также в целях навигации в отсутствие сигналов ГНСС.

Для работы системы установлены три категории точности синхронизации в зависимости от источника данных времени и степени надежности синхронизации источника:

- первичная синхронизация, обеспечивающая наивысшую точность привязки к UTC; основана на использовании внешних источников времени. Объект А-сети должен получать первичное время от приемника ГНСС, который всегда будет источником при наличии выбора, кроме случаев, когда он недоступен;
- при недоступности первичного времени применяется вторичная синхронизация, требования к точности которой ниже. Вторичное время можно получить от других объектов А-сети, включая наземные и бортовые транспондеры, которые имеют сертифицированное первичное время. Вторичное время может быть получено, например, на основании анализа временны́х границ слота во время передачи сообщений от ближайших объектов;
- при недоступности первичного и вторичного источников применяют третичные источники времени, для которых требования к точности еще ниже.

Режимы вторичного и третичного времени считаются режимами отказа и должны индицироваться в А-сети.

Интересы безопасности полетов диктуют необходимость разработки концепции и средств обеспечения информационной безопасности А-сети, гарантирующих защиту от:

- перехвата сообщений, содержащих одновременно идентификатор ВС и его координаты, несанкционированными органами или частными лицами;
- навязывание ложной информации со стороны террористов и легальных участников воздушного движения;
- возможности отрицания легальным участником воздушного движения фактов передачи в эфир сообщений АЗН-В;
- повторов ранее переданных сообщений, передаваемых "в записи" террористами или легальными участниками воздушного движения с целью формирования фантома;
- возможности навязывания террористами или легальными участниками воздушного движения сообщений "от чужого имени" – от лица других участников движения;
- подавление сигналов глобальных навигационных спутниковых систем.

Наиболее адекватным средством решения задачи обеспечения информационной безопасности в сложившихся условиях представляется использование двухключевых (Public-Key) алгоритмов криптографической защиты информации. Необходимый уровень безопасности полета в текущих условиях можно обеспечить за счет внедрения системы информационной безопасности в соответствии со следующими требованиями:

- система должна быть снабжена автоматическими невыключаемыми/неостанавливаемыми средствами наблюдения, сигнал от которых, несущий идентификатор воздушного судна (должен быть открыт), временны́е и пространственные координаты, должен быть защищен криптографическими средствами от перехвата террористами и несанкционированными пользователями;
- система должна защищать процесс наблюдения от неверной информации, поступившей из несанкционированных источников; источники всех сообщений должны быть аутентифицированы и проверены на подлинность; прием информации из несанкционированных источников должен стать невозможным. Получатель сообщения должен иметь возможность убедиться, что принятое сообщение не было изменено при передаче; у нарушителя не должно быть возможности заменить подлинное сообщение на ложное. Получатель также должен иметь возможность убедиться в его происхождении; у нарушителя не должно быть возможности замаскироваться под кого-либо другого;

- система должна предоставить поддержку функции идентификации, обеспечивая возможность отличать фантомы от реальных ВС;
- система должна позволить определить местонахождение сигналов-призраков, чтобы надлежащим образом подавить их;
- система должна обеспечивать неотрекаемость: у отправителя не должно быть возможности ложно отрицать позднее, что он посылал сообщения. Отправитель не может отрицать, что он является автором сообщения и ссылаться на то, что он его не посылал; кроме того, получение каждого сообщения сопровождается подтверждением и пересылкой отправителю уведомления об этом, включая регистрацию у получателя;
- необходимо обеспечить в масштабе системы возможность управления и навигации воздушных судов на случай подавления сигналов ГНСС;
- в целях записи и последующей интерпретации событий, включая поисково-спасательные действия, сообщения АЗН-В следует соотнести со шкалой времени (метка времени); это позволит записать положение всех ВС в четырех измерениях;
- все действия по обеспечению безопасности должны строиться на основном принципе, когда применяемые меры безопасности должны быть соизмеримыми с угрозами. После оценки риска, проводимой соответствующими национальными полномочными органами, должна быть обеспечена разработка мер защиты критически важных систем информационных и связных технологий, используемых для целей гражданской авиации, вмешательство в которые может поставить под угрозу безопасность гражданской авиации. Политика риска должна быть прозрачной, предсказуемой и контролируемой, сосредоточенной на самом высоком риске, объективной;
- помимо защиты от несанкционированного доступа и использования, система безопасности должна обнаруживать кибератаки на систему, обеспечивая надлежащую защиту от вирусов и хакерских программ, выполняя записи, анализ и разработку соответствующего противодействия;
- криптографические алгоритмы, используемые в системе, должны иметь подтвержденный статус (Approved), а средства защиты – сертифицированы. Длина ключа должна обеспечивать требуемый уровень защиты. При использовании двухключевых алгоритмов криптозащиты система должна обеспечивать устойчивость к попыткам составления террористом "словаря" зашифрованных открытым ключом двухключевого алгоритма сообщений известного содержания, дающего возможность распознавания этих сообщений в составе потока сообщений.

Решение поставленных проблем может быть достигнуто использованием самоорганизующихся сетевых технологий – построением А-сети на основе специальных коммутирующих радиотранспондеров, функционирующих на базе протоколов сети. Системный подход к процессу наблюдения за воздушными судами в рамках А-сети снимет проблему наложения во времени сигналов разных воздушных судов, передаваемых на одной частоте, и обусловленные этим положением взаимные помехи.

Конфиденциальность передачи сообщений в А-сети обеспечивается:

- на этапе формирования общего сеансового ключа – шифрованием передаваемого сообщения открытым ключом двухключевой криптосистемы приемника сообщения;
- на этапе работы в сети – использованием сформированного сеансового ключа для шифрования сообщений.

Аутентификация источника сообщений в А-сети обеспечивается:

- на этапе формирования общего сеансового ключа – шифрованием передаваемого сообщения закрытым ключом двухключевой криптосистемы источника и (при наличии) промежуточного узла передачи сообщения;
- на этапе работы в сети – использованием сформированного сеансового ключа для шифрования сообщений.

Предлагаемая концепция обеспечивает следующие дополнительные функции зависимого наблюдения-вещания:

- масштабируемость. При необходимости пилот любого ВС может расширить зону наблюдения (в пределах зоны А-сети) в любую сторону на требуемую глубину;
- живучесть. Распад А-сети на несколько частей не приводит к потере наблюдения. Каждая часть сохраняет способность автономного функционирования;

- надежность и безопасность. Наличие обходных направлений А-сети обеспечивает сохранение информационного обмена при потере прямого радиодоступа, например, вызванного влиянием препятствий;
- защищенность от наведенных целенаправленных помех типа создания ложного объекта. Измерение реального расстояния до объекта или его реальных координат (за счет измерения значения времени распространения) дает основание игнорировать подобные объекты и исключать их из образа сети.

Кроме того, обеспечиваются следующие дополнительные телекоммуникационные функции:

- поиск объекта в А-сети. При возникновении потребности передачи информации определенному объекту может быть использован принцип "штурма", заключающийся в рассылке запроса на соединение в широковещательном режиме (во всех направлениях) с защитой от повторной передачи по одному и тому же участку;
- приоритезация сообщений в соответствии со статусом содержания. Наличие образа А-сети на объекте дает возможность обеспечить "ручную" маршрутизацию сообщения или автоматическую в соответствии с его рангом;
- возможность организации речевого обмена для аварийных ситуаций, например, при отсутствии прямого радиодоступа или потере голосовой связи.

ЛИТЕРАТУРА

1. **Фальков Э., Шаврин С.** АЗН-В и информационная безопасность воздушного движения // ПЕРВАЯ МИЛЯ. 2020. № 5. С. 50–56.
2. **Фальков Э., Шаврин С., Алешин В.** СЕТЕВАЯ ТЕХНОЛОГИЯ АЗН-В-решение проблемы нахождения БПЛА в общем воздушном пространстве // ПЕРВАЯ МИЛЯ. 2022. № 4. С. 66–70.
3. **Григорьев И.Д., Орлов В.Г.** Анализ уязвимостей АЗН-В на базе 1090 // Материалы Международной научно-технической конференции "Фундаментальные проблемы радиоэлектронного приборостроения". INTERMATIC-2016. 2016. С. 171–174.
4. **Мирошниченко А., Татарчук И., Фальков Э., Шаврин С.** Сравнение пропускной способности систем автоматического зависимого наблюдения-вещания // ПЕРВАЯ МИЛЯ. 2020. № 3. С. 24–29.

Геннадий Иванович Мещанов

11 июня 1940 года – 12 сентября 2022 года

С глубоким прискорбием извещаем, что 12 сентября 2022 года ушел из жизни Геннадий Иванович Мещанов – яркий профессионал, посвятивший всю свою жизнь развитию российской кабельной промышленности.

Г.И.Мещанов родился в г. Егорьевск Московской области. Закончил Московский энергетический институт. В 1963 году по распределению пришел во ВНИИКП. Прошел путь от инженера до генерального директора (с 2003 года) Всероссийского научно-исследовательского института кабельной промышленности (ОАО "ВНИИКП"), который возглавлял до 2021 года. С 1998 года – вице-президент, а с 2011-го по 2021 год занимал пост президента международной Ассоциации "Электрокабель", объединяющей основных производителей кабельной продукции на постсоветском пространстве.

В последние годы Г.И.Мещанов возглавлял комплекс работ по созданию новых материалов, в том числе используемых в производстве кабелей и проводов оборонного значения. В числе важнейших из них – работы по организации первого в стране промышленного производства телекоммуникационного оптического волокна.

Г.И.Мещанов – доктор технических наук, заслуженный деятель науки Российской Федерации, лауреат премий Совета Министров СССР и Правительства России. Награжден четырьмя орденами и тремя медалями СССР и России. Его имя широко известно не только у нас в стране, но и признано в мире как выдающегося российского ученого и профессионала своего дела.

Редакционный совет и редакция журнала "ПЕРВАЯ МИЛЯ" выражают глубокое соболезнование родным и близким Геннадия Ивановича. Светлая память о нем навсегда останется в наших сердцах.

100% российское: "Ростелеком" обеспечил технологическую независимость цифровых услуг для населения

"Ростелеком" первым из федеральных операторов связи получил официальное подтверждение российского происхождения ключевых цифровых платформ для оказания услуг населению. Видеосервис Wink, цифровые платформы для управления многоквартирными домами "Ростелеком. Ключ" и квартирами "Умный дом" в 2022 году включены в реестр отечественного программного обеспечения, который ведет Минцифры России. Все три платформы с нуля созданы командами внутренних ИТ-разработчиков группы компаний "Ростелеком".

Независимая экспертиза, которая предшествует включению ПО в реестр, проверяет его соответствие системе критериев и подтверждает, что интеллектуальная собственность принадлежит российской компании. В текущих условиях это также говорит о том, что сервисы защищены от санкционных рисков. Созданное программное обеспечение, ЦОДы и другая цифровая инфраструктура для оказания услуг расположены в России, управляются только самой компанией и на их работу не могут повлиять зарубежные вендоры.

"Все наши цифровые сервисы для населения уверенно входят в число лидеров в своих сегментах российского рынка. Включение Wink, "Умного дома" и "Ключа" в реестр отечественного ПО свидетельствует о том, что ОТТ-платформы "Ростелекома" используют исключительно российские ИТ-разработки и могут управляться только нашей компанией. Это дает потребителям уверенность, что привычные сервисы будут работать вне зависимости от внешних факторов", – отметила вице-президент по цифровым продуктам массового сегмента "Ростелекома" Диана Самошкина.

По информации ПАО "Ростелеком"