Информационные угрозы в системе радиосвязи.

Пылаева Анастасия
МФТИ
Физтех-школа радиотехники и компьютерных технологий
Б01-906
Преподаватель:Семака Вадим Юрьевич

Долгопрудный 2022

Радиосвязь — способ передачи сообщений на расстояние посредством радиоволн, а также область науки и техники, связанная с изучением физических явлений, лежащих в основе этого способа, и с его использованием для связи, звукового вещания, передачи изображений, сигнализации, контроля и управления, обнаружения различных объектов и определения их местоположения и для других целей.

Проанализируем безопасность радиосвязи на примере польского проекта беспилотных летательных аппаратов "Самолет для мониторинга" SAMONIT.Рассмотрим угрозы безопасности для системы радиосвязи и возможные меры по обеспечению защищенности информации.

Беспилотные летательные аппараты (БПЛА) — аппараты, выполняющие полет без пилота и экипажа. Для управления БПЛА, телеметрии и передачи других данных используется канал радиосвязи. Он неизбежно столкнулся бы с угрозами: потерей радиосвязи, передаваемой информации, контроля или преднамеренного внешнего вмешательства. Чтобы избежать этих нежелательных последствий, необходимо принять меры информационной безопасности. Различают угрозы двух типов: те, которые не зависят от людей, и те, которые связаны с людьми. Угрозы, связанные с человеком, включают прослушивание канала связи, изменение или повреждение информации и блокирование канала.

Рассмотрим **меры информационной безопасности**.
Злоумышленник может попытаться манипулировать передаваемыми данными с намерением скрыть, изменить или задержать команды управления. Такие критические неисправности в БПЛА влияют на успех миссии или опасности полета. Манипуляция может быть осуществлена путем искажения, воспроизведения или блокирования данных во время их сбора или распространения. Однако во время работы БПЛА в режиме реального времени интегрированные устройства генерируют оповещения об атаках. Кроме того, злоумышленник может пассивно подслушивать критически важные данные, чтобы получить информацию, которая может быть использована для других атак. Хотя две вышеуказанные угрозы не представляют непосредственной опасности для полетов, они могут быть использованы для будущих атак.

Физическая защита и логические (программные) меры безопасности могут быть использованы для обеспечения информационной безопасности. Меры физической безопасности относятся к техническим гарантиям (физическая защита устройств хранения информации). Кодирование информации, сложные протоколы передачи данных и алгоритмы шифрования и т.д. Все меры информационной безопасности должны быть интегрированы в систему радиосвязи. Системы радиосвязи SAMONIT по умолчанию не включают в себя оборудование безопасности для защиты передачи информации.

Чтобы смягчить все вышеупомянутые угрозы, предлагают следующие рекомендации:

1)Надежность радиоканала: на качество радиосвязи на летательных аппаратах влияют различные факторы: используемая полоса частот, расстояние, погодные условия, интенсивность внешнего шума, положение самолета и т.д. Для обеспечения качества и надежности радиосвязи необходимо использовать дублирующие передатчики с перпендикулярными антеннами. При возникновении проблемы со связью с основным устройством, автоматически включает второй передатчик и продолжает поддерживать связь. Для системы связи SAMONIT используется несколько различных частот (35 МГц, 2,4 ГГц). При использовании передатчика очень высокой частоты (ГГц) поляризация сигнала имеет значение, и поэтому рекомендуется устанавливать дублирующие антенны передатчика в разных плоскостях, перпендикулярных друг другу, обеспечивая таким образом требуемую поляризацию.

2)Материал, из которого изготовлен корпус самолета. Для корпуса SAMONIT исполь-

зуются композитные материалы на основе углеродных волокон. Углерод является проводником и экранирует электрическое оборудование, которое находится внутри корпуса.

3) Антенны связи должны быть установлены на поверхности SAMONIT. Если невозможно установить антенны на поверхности, в корпус должны быть встроены “окна” из других материалов (например, стекловолокно).

4)Целостность: канал связи SAMONIT должен быть защищен от несанкционированного изменения данных злоумышленником, пытающимся скрыть, например, изменение команд управления или данных телеметрии. Следовательно, данные, полученные от БПЛА должны быть идентичными данным, отправленным исходным БПЛА.

5)Подлинность:беспилотный летательный аппарат также должен быть защищен от получения вводящих в заблуждение данных, отправляемых неавторизованными наземными станциями. Чтобы предотвратить внешние враждебные атаки, при получении данных беспилотный летательный аппарат должен иметь возможность проверять достоверность как источника, так и сообщения. Для защиты от взломанных наземных станций беспилотный летательный аппарат может использовать распределенные решения, такие как схема голосования большинством голосов, которая может совместно определять действительность.

6)Конфиденциальность: не вся информация, передаваемая в/из БПЛА, является общедоступной: команды управления, данные телеметрии и т.д.

6)Уменьшение помех в канале: злоумышленник может, например, использовать атаки с помехами, чтобы заблокировать или задержать распространение обнаружения критических неисправностей на наземную станцию. Следовательно, атаки с помехами каналу должны быть обнаружены как можно скорее и смягчены в беспилотном летательном аппарате.

7)Безопасная маршрутизация: беспилотный летательный аппарат и наземная станция должны передавать свои показания своевременно и надежно , даже когда они подвергаются атаке. Протокол маршрутизации беспилотных летательных аппаратов и наземных станций должен быть достаточно надежным, чтобы противостоять атакам помех, которые приводят к длинным и энергоэффективным маршрутам. Протокол маршрутизации также должен быть достаточно надежным, чтобы противостоять атакам, основанным на вводящих в заблуждение сообщениях маршрутизации. Например, если используется географическая маршрутизация, есть возможность изменять информацию о местоположении.

8)Раннее и правильное выявление манипуляций: любые манипуляции с передаваемой информацией должны быть обнаружены как можно скорее, при этом необходимо избегать ложных срабатываний. Для этой угрозы можно использовать систему обнаружения вторжений. Бортовой компьютер SAMONIT также должен иметь возможность создавать архив для всех событий.

Гарантия конфиденциальности.

Коммуникации в БПЛА, которые содержат служебные данные или конфиденциальные данные, способные помочь будущим атакам (например, уровень топлива в двигателе, собранные данные), должны быть защищены от пассивного прослушивания по беспроводным каналам. Самым простым решением является передача данных в формате открытого текста с использованием простого протокола передачи данных: start, data, checksum and stop bytes.

Этот способ передачи данных прост, но небезопасен. Кроме того, ни один из используемых радиомодемов не имеет интегрированных мер безопасности. Для обеспечения целостности, аутентичности и конфиденциальности связи с БПЛА может использоваться криптография. Все криптографическое оборудование может быть интегрировано в канал связи как аппаратное обеспечение, как встроенный инструмент, или могут использоваться

программные средства, интегрированные в главный компьютер SAMONIT. Существует простая интеграция аппаратного средства шифрования в канал связи, но это вызывает некоторые проблемы. Во-первых, это аппаратное обеспечение, и ему нужен источник питания, а это увеличивает вес. Во-вторых, мы теряем время на преобразование данных из разных протоколов. Программные средства не обладают слабостью, присущей аппаратным средствам, но время шифрования напрямую зависит от скорости основного процессора (8, 16, 32 или более бит), объема памяти и установленных программ. Поскольку БПЛА ограничены с точки зрения батареи (топлива) предпочтительна мощная симметричная криптография. Недостаток асимметричной криптографии заключается в том, что она относительно трудоемка в вычислениях и коммуникации.

В то же время, чтобы расширить функции БПЛА, решения на основе асимметричной криптографии, такие как цифровая подпись, могут использоваться для связи с другими подсистемами. Кроме того, решения, основанные на криптографии канального уровня, т.е. с использованием криптографического ключа, совместно используемого двумя соседями, являются более подходящими, чем решения, основанные на сквозной криптографии, т.е. с использованием ключа, который совместно используется каждым исходящим БПЛА и конечным пунктом назначения, который может быть агрегатором, беспилотным летательным аппаратом или базовой станцией. Для обеспечения конфиденциальности могут быть использованы стандартные средства шифрования, подобные тем, которые используются в беспроводных сетях.

Процесс шифрования требует гораздо больших возможностей для математических вычислений, и иногда этого трудно достичь в системе. Однако в настоящее время существуют решения, позволяющие интегрировать криптографические возможности в небольшие встроенные системы. Например, решения для шифрования могут быть получены на основе технологии смарт–карт. Большинство доступных систем радиосвязи имеют встроенные меры безопасности, которые настраиваются настройки по умолчанию. Для защиты передаваемой информации рекомендуется изучить все доступные комплексные меры безопасности.

Выводы

– Для безопасного использования БПЛА необходима безопасность передаваемой информации.

– Анализ системы радиосвязи в проекте SAMONIT показывает, что оборудования для обеспечения безопасности передаваемых данных недостаточно, и злоумышленник может осуществить внешнее вмешательство.

– Для безопасности передаваемой информации целесообразно использовать методы шифрования данных.

Список использованной литературы

Homziuk, A.; Hajduk, J. 2009. Opracowanie systemu akwizycji danych, telemetrii, autopilota I stacji bazowej BSP SAMONIT. In Projekt BSP SAMONIT. Warszawa.

Li, M.; Koutsopoulos, I.; Poovendran, R. 2007. Optimal jamming attacks and network defense policies in wireless sensor networks. In IEEE INFOCOM. 1307–1315.

Goraj, Z., 2007 UAV platforms designed in WUT for border surveillance. AIAA paper, 2965.