Формальная криптографическая идентификация БПЛА на основе применения криптографических токенов аутентификации.

Филиппов Андрей Олегович

Аннотация—В статье рассмотрены проблемы сигнатурной и формальной идентификации БПЛА как с позиции внешнего наблюдателя, так и с позиции оператора наземной станции управления. Проведено сравнение криптографических и некриптографических методов идентификации и аутентификации в различных средах передачи данных и выработана экспериментальная концепция по организации циклической проверки подлинности дрона с помощью физического неклонируемого криптографического идентификатора. На основании сделанных выводов построена модель системы идентификации, позволяющей совершать циклический обмен файлами ЭЦП с целью доказательства подлинности дрона.

Index Terms—Дрон, идентификация, криптография, БПЛА, аутентификация, шифрование, протокол, модель

I. Введение

В настоящее время остро стоит вопрос регуляции применения гражданских и промышленных БПЛА с точки зрения их идентификации для защиты от противоправного и неконтролируемого применения. Существует несколько подходов к такой идентификации, часть из них предполагает наличие доступа к наземной станции управления и позволяет удостовериться в отсутствии подмены дрона или атак типа “человек посередине”. Другие подходы позволяют идентифицировать БПЛА без доступа к управлению им, то есть методами внешнего наблюдения. К таким методам можно отнести оптическое, акустическое и радиочастотное наблюдение. Технологии оптического распознавания позволяют определять наличие в воздухе дрона а также его марку и модель, но не предназначены для идентификации конкретного уникального экземпляра, поэтому здесь подробно рассмотрены не будут.

II. Методы

Теоретический анализ способов поиска уникальных идентификаторов в различных физических средах и способов организации формальной аутентификации конкретного экземпляра БПЛА в системе “базовая станция–дрон”, а также экспериментальная реализация внедрения неклонируемого физического идентификатора (криптографического токена) в цепочку передачи сигнала.

III. Модель угроз

В данной работе рассматривается защита от атак типа “человек посередине” или угроз внесения физических изменений в конфигурацию БПЛА со стороны злоумышленников, получающих физический доступ к дрону. К таким изменениям можно отнести разукомплектование дрона, навешивание опасной полезной нагрузки, установка внешних систем удаленного управления

IV. Обзор литературы

A. Акустическая идентификация

Акустические методы аутентификации рассмотрены в работе Soundarya Ramesh, Thomas Pathier, Jun Han Данный подход предполагает идентификацию на малых расстояниях с целью защиты от подмены дроновдоставщиков. Авторы исследуют шум винто-моторной группы, различающийся из-за дефектов при производстве бесколлекторных моторов и применяют алгоритмы машинного обучения для анализа акустического отпечатка. В рамках исследования тестовой выборки была получена точность 91.83

B. Радиочастотная идентификация

Методы сбора “отпечатков” на основе дефектов производства применимы и к радиочастотным методам идентификации. Такой подход продемонстрирован в работе Miers, Eric Jame

Авторы поставили задачи двоичной и множественной классификации устройств передачи радиотелеметрии как дополнительного фактора аутентификации пакетов. Для этого ими были с высокой частотой дискретизации записаны дампы сигналов, в этих дампах вырезаны участки, когда станция работает на передачу (так как имеет место быть временное мультиплексирование), эти участки разделены на малые образцы, а потом на их основе обучены различные типы нейронных сетей. Авторы сочли неудобным исследовать переходные процессы, ибо это не так легко воспроизводимая ситуация, они исследовали искажения в соотношении квадратурной и синфазной компонент сигнала в установившемся режиме. Для получения более реалистичных результатов в дампы сигнала программно добавлялся псевдослучайный шум разной амплитуды.

Нейронные сети использовались 2 видов - с бинарным и множественным выходом. Множественный выход давал возможность определить к какому из известных образцов ближе исследуемый образец сигнала, а бинарный выход - только лишь узнать является ли радиопередатчик "знакомым"нейронной сети. При этом, разумеется, бинарные сети для получения сходной точности требовали меньшее число слоев и нейронов в них. По результатам исследования получены точности более 90

Также выяснено, что не наблюдается резкого снижения (или повышения) точности в зависимости от сложности примененной нейронной сети. Различия в точности при изменении числа слоев от 3 до 8 составляют единицы процентов.

Авторы приходят к выводу, что такой способ идентификации позволяет ввести дополнительный фактор аутентификации для пакетов, принимаемых дроном и защитить его от попыток подделки наземной станции, но при низких уровнях сигнала (10-2 децибел) такая аутентификация может давать false-negative реакции, нарушая стабильность приема пакетов (дрон начнет отбрасывать легитимные пакеты), поэтому алгоритм принятия решения должен ориентироваться на те нейронные сети, которые после обучения более склонны все-таки к "false-positive"прогнозам. Еще одним описанным вариантом применения является просто абстрактная возможность определять, что в канале есть злоумышленник, после чего принимать какие-то меры.

C. Формальная криптографическая идентификация

В исследовании Joseph A. Marty рассматриваются типы атак на протокол - MAVlink и способы им противодействия.

Авторы работы имитировали различные атаки на конфиденциальность, целостность и доступность информации передаваемой по протоколу, применяя для этого третий (помимо дрона и наземной станции) модуль телеметрии и инструмент MAVProxy в паре с wireshark. Это становится возможным благодаря тому, что сегмент с полезной нагрузкой протокола MAVlink по умолчанию не зашифрован, что с одной стороны создает крупную уязвимость к атакам, а с другой - дает возможность применить шифрование самостоятельно в зависимости от поставленных задач. Авторы рассматривают различные подходы к этому: применение "быстрых"потоковых алгоритмов шифрования (Rabbit, XXTEA) и более ресурсоемких блочных (AES-GCM, NaCl). С целью защиты от атак на целостность предлагается использовать схемы аутентифицированного шифрования. При передаче зашифрованной информации в качестве полезной нагрузки протокола MAVlink существует проблема ограничения ее размера в 255 байт, что создает трудности для добавления служебной информации при шифровании.

V. Выводы на основе изученной литературы

В результате анализа литературы принято решение о необходимости реализации собственного метода аутентификации БПЛА с помощью криптографических токенов. Причины такого решения:

- удобство масштабирования и унификация компонентов;
- отсутствие необходимости в точном и широкополосном радиочастотном оборудовании;
- возможность изменять правила идентификации и аутентификационные данные.

VI. Экспериментальная модель

A. Концепция модели

для получения криптографического идентификатора был применен криптографический токен Рутокен ЭЦП 3.0. Передача файлов подписи осуществляется по протоколу MAVFtp (рис. 1) с применением python-библиотеки Mavutil для работы с MAVLink-пакетами .

Для выполнения криптографического “рукопожатия” на наземной станции генерируется произвольная начальная последовательность байт, которая записывается в файл seed.txt. Этот файл по протоколу MAVFtp через радиоканал передается во внутреннюю память полетного контроллера, откуда скачивается одноплатным компьютером Orange Pi Zero, присоединенным непосредственно к полетному контроллеру через uart-порт телеметрии (рис. 2), где подписывается с помощью криптографического токена Рутокен ЭЦП 3.0 по алгоритму SHA-256, после чего файл отсоединенной электронной подписи тем же путем пересылается на наземную станцию, где с помощью открытого ключа подписи проверяется соответствие полученного файла подписи исходному файлу seed.txt.

B. Средства передачи файлов

Для управления пересылкой файлов, их подписыванием и проверкой подписи используются файлы python-кода handler.py и mavftp_lib.py, написанные для решения поставленной задачи. Файл mavftp_lib.py содержит класс FileTransfer, устанавливающий MAVLink-соединение с полетным контроллером и имеющий в своем составе методы self.init(self, connection_string, baud_rate), self.get(self, file_path), self.send(self, file_path) и self.close(), предназначенные соответственно для инициализации соединения, скачивания файла, отправки файла и закрытия соединения.

Основной подход к операциям с протоколом MAVFtp выработан на основе официальной документации и исходного кода программы MAVProxy.

Для считывания и отправки файлов применяется операция BurstReadFile, размер полезной нагрузки в каждом пакете MAVLink используется равным 80 байтам (структура пакета изображена на рисунке 3).

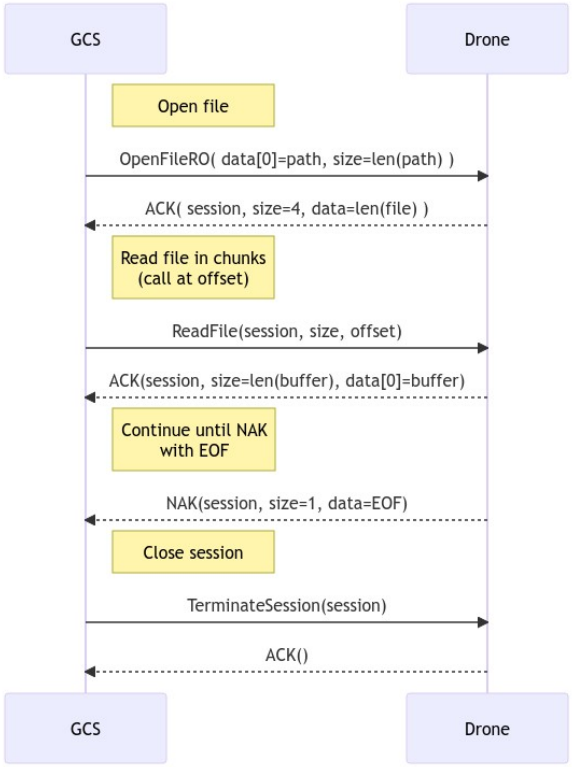

Рис. 1. Алгоритм передачи файлов по протоколу MAVFtp

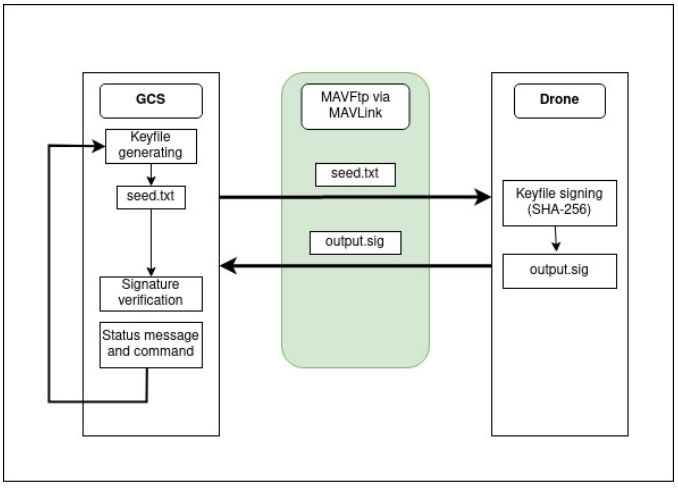

Рис. 2. Алгоритм совершения “рукопожатия”

C. Средства управления

Для подписи файлов на стороне полетного контроллера используется утилита pkcs11-tool, вызываемая в командной оболочке zsh с помощью python-модуля subprocess. Для работы с токеном ЭЦП применен программный пакет драйвера с сайта производителя, в т.ч. модуль librtpkcs11ecp.so для 32-битной ARM архитектуры процессора одноплатного компьютера.

VII. Результаты проведения моделирования

При моделировании процесса обмена криптографическими идентификаторами установлено, что использование вспомогательного одноплатного компьютера помогает избавиться от нагрузки на полетный контроллер дрона, что позволяет избежать негативного влияния на основные функции контроллера, такие как обработка сигналов с датчиков, команд управления и обработки навигационных данных. При это канал связи по протоколу MAVLink также не испытывает перегрузки из-за небольшого количества пакетов, передаваемых по протоколу MAVFtp на фоне общего количества MAVLink пакетов.

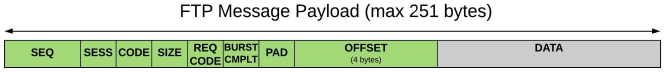

Рис. 3. Структура MAVLink-пакета

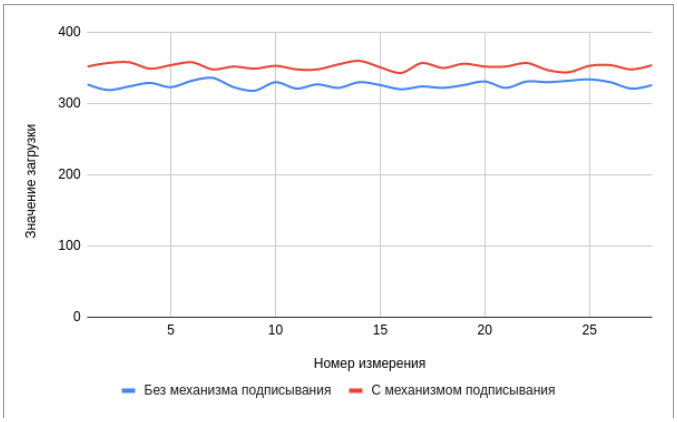

Рис. 4. График значений параметра нагрузки на полетный контроллер

Для анализа влияния работы механизма криптографической идентификации на загрузку процессора полетного контроллера было проведено исследование параметра значения загрузки, передаваемого в MAVLink-пакетах. Значения загрузки во время процесса обмена подписанными пакетами и без такового приведены на рисунке 4. Видно отсутствие существенных отличий в загрузке благодаря тому, что большая часть операций выполняется на наземной станции и одноплатном компьютере.

VIII. Сравнение с существующей технологией MAVLink2 Signing

В коде автопилота Ardupilot существует технология MAVLink2 Signing, используемая для защиты от подмены пакетов через несанкционированное подключение. Она позволяет полетному контроллеру проверять цифровую подпись переданных пакетов с командами управления с целью принятия решения об их исполнении, но она не предполагает идентификацию пакетов переданных от БПЛА на наземную станцию управления, что ограничивает функциональность ее применения. Технология же описанная в данной работе позволяет однозначно верифицировать полученные с дрона пакеты на наземной станции.

IX. Выводы в результате проведения исследования

В ходе исследования проанализированы различные технологии и подходы к идентификации БПЛА, изучены их достоинства и недостатки и выбран удобный способ построения системы идентификации БПЛА на основе криптографических токенов аутентификации. Для организации обмена криптографическими файлами использован одноплатный компьютер, размещаемый на дроне и аппаратный токен аутентификации, подключенный к нему. Такая схема обеспечивает защищенный от перехвата или подмены ключей шифрования процесс идентификации, так как секретный ключ ЭЦП записан в аппаратный токен и не может быть оттуда извлечен. Данная технология обеспечивает гибкий подход к применению различных алгоритмов шифрования, так как токен поддерживает множество из них, а также позволяет заменить токен на иное устройство генерации уникальных отпечатков, например устройство PUF (Физическая неклонируемая функция). Применение такого метода идентификации не требует дополнительных модификаций полетного контроллера дрона или дополнительных требований к качеству изготовления компонентов самого дрона. Также практически никак не требуется модификация наземной станции дрона, в том числе приемно-передающего радиооборудования на ней. Применение протокола MAVFtp не несет значительного увеличения нагрузки на канал передачи данных и никак не влияет на основную функциональность дрона.

Список литературы

[1] H. Kopka and P. W. Daly, A Guide to LaTeX, 3rd ed. Harlow, England: Addison-Wesley, 1999.