УДК 004.07

ПРОБЛЕМЫ БЕЗОПАСНОСТИ MESH-СЕТЕЙ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

Блинов А.В. (Университет ИТМО)
Научный руководитель – доцент, доктор технических наук, Беззатеев С.В.
(Университет ИТМО)

Введение. Точное определение местоположения объектов, картирование в реальном времени неизвестных или труднодоступных мест, а также сокращение времени выполнения задач по сравнению с одиночными устройствами делают рой БПЛА привлекательным для коммерческого и военного использования. Кроме того, рои БПЛА могут способствовать удовлетворению требований сетей будущего, обеспечивая высокую доступность, большую плотность соединений и низкую сквозную задержку.

Основная часть. Многие Mesh протоколы разработаны без обеспечения безопасности или предполагают, что вопросы безопасности решаются на более высоких уровнях.

Широковещательная природа беспроводного канала делает передачи на физическом уровне восприимчивыми к различным атакам и злонамеренным действиям. В целом, угрозы на физическом уровне могут быть классифицированы как пассивные или активные атаки.

Канальный уровень отвечает за мультиплексирование потоков данных, контроль ошибок и управление доступом к среде. Основная уязвимость на этом уровне заключается в подмене MAC-адреса, когда одна станция выдает себя за другого члена сети.

Сетевой уровень отвечает за инкапсуляцию IP-пакетов и маршрутизацию информации по сети. Атаки на этот уровень направлены на механизм маршрутизации механизм связи роя БПЛА и влияют на пересылку пакетов.

Транспортный уровень: уровень управляет потоком данных в коммуникационном стеке. Уязвимости этого уровня связаны с повреждением пакетов или использованием слабых мест в протоколах TCP/UDP/ICMP.

Операционная система робота (ROS) - это фреймворк, широко используемый для программного обеспечения роботов, как пример прикладного уровня в роях БПЛА. Отсутствие таких функций безопасности, как шифрование данных и аутентификация, делает ROS критической поверхностью для различных векторов атак в сетях БПЛА. ROS2 [1] построен на базе службы распределения данных (DDS) с архитектурой Real-Time Publish Subscribe (RTPS) [2] и был разработан для того, чтобы устранить уязвимости, обнаруженные в его предыдущей версии - добавление аутентификацию, шифрование и функции профиля процесса, которые полагаются на инфраструктуру открытых ключей.

Чтобы защитить сеть, ключевым инструментом является шифрование.

Одним из распространенных методов шифрования является AES [3], который использует ключи длиной 128, 192 или 256 бит, чтобы зашифровать и расшифровать данные.

AES используется для шифрования информации в Mesh-сети БПЛА таким образом:

1. Генерация ключа AES: перед началом шифрования ключ AES должен быть сгенерирован и доставлен на все аппараты, которые будут использовать эту сеть.
2. Шифрование данных: когда данные готовы к передаче по Mesh-сети, они шифруются с использованием ключа AES.
3. Передача данных: шифрованные данные передаются по Mesh-сети между аппаратами.
4. Дешифрование данных.

Другой распространенный метод шифрования – RSA [4]. В Mesh-сети БПЛА, RSA может использоваться для шифрования информации во время передачи данных между аппаратами в сети.

В этом случае, каждый БПЛА имеет уникальную пару ключей RSA, состоящую из открытого и закрытого ключа. Открытый ключ используется для шифрования данных,

которые передаются между аппаратами, а закрытый ключ используется для дешифрования полученных данных.

Защита закрытого ключа RSA на БПЛА может быть осуществлена с использованием различных методов, таких как хранение в зашифрованном виде, использование дополнительных протоколов аутентификации и авторизации, а также использование различных алгоритмов криптографической защиты.

Кроме того, для дополнительной защиты можно использовать мультиплексирование шифрования. Мультиплексирование шифрование – это технология, которая позволяет одновременно передавать несколько зашифрованных потоков данных по одной канальной линии. В контексте Mesh-сетей для БПЛА, это означает, что несколько БПЛА могут одновременно передавать зашифрованные данные друг другу через общую Mesh-сеть.

В случае если необходимо добавить новый БПЛА в Mesh-сеть, сначала происходит идентификация и аутентификация устройства.

Для идентификации новых БПЛА в Mesh-сети используется уникальный идентификатор, который может быть назначен администратором сети.

Процесс идентификации новых БПЛА в Mesh-сети включает в себя следующие этапы:

1. Обнаружение: каждый БПЛА в Mesh-сети постоянно пытается обнаружить другие БПЛА в окружении.

2. Обмен идентификационными данными: когда два БПЛА обнаружили друг друга, они начинают обмен идентификационными данными, которые могут включать в себя имя, тип БПЛА, версию ПО и т.д.

3. Валидация: когда БПЛА получили идентификационные данные друг друга, они проверяют, являются ли данные действительными и достоверными.

4. Утверждение: если данные другого БПЛА прошли валидацию, они подтверждают его идентификацию и добавляют его в свой список известных устройств.

После идентификации БПЛА производится аутентификация.

Аутентификация может происходить с использованием пары ключей, таких как RSA, или посредством проверки подлинности идентификаторов, таких как имена пользователей и пароли.

Выводы. Рои БПЛА используют беспроводную сеть Mesh для обеспечения инфраструктуры сетей Ad-hoc, как в простых приложениях, так и в сложных событиях. Однако недостатки, присущие протоколам и стандартам Mesh, привели к появлению новых поверхностей для атак и возникновению новых проблем безопасности. В этой статье мы выделили основные уязвимости во всем коммуникационном стеке сетки БПЛА - от физического до прикладного уровня. На основе этой информации мы предложили архитектуру безопасной Mesh-сети.

Список использованных источников:

1. URL: https://docs.ros.org/en/foxy/index.html.
2. Стандарт Real-Time Publish Subscribe // URL: https://www.omg.org/spec/DDSI-RTPS/2.3/PDF.
3. Стандарт AES // URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf.
4. Хеллман М., Диффи У. Новые направления в криптографии // URL: https://www-ee.stanford.edu/~hellman/publications/24.pdf.

Блинов А.В. (автор) _____
подпись

Беззатеев С.В. (научный руководитель) _____
подпись