УДК 004.056

ОБЗОР УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И НАРУШЕНИЯ ФУНКЦИОНИРОВАНИЯ АГЕНТОВ АВТОНОМНЫХ ВОЗДУШНЫХ РОЕВЫХ СИСТЕМ

Домницкий Е.А. (ИТМО)
Научный руководитель – кандидат технических наук, Попов И.Ю.
(ИТМО)

Введение. Обеспечение безопасности информации и бесперебойного функционирования агентов робототехнических систем бессмысленно рассматривать в отрыве от реальных систем и контекста их использования. Абстрактные модели угроз без привязки к конкретной архитектуре не позволяют выявить критические уязвимости. Сценарий применения роя (мониторинг, поиск, логистика) определяет исходные данные для типов и свойств взаимодействия агентов, а также выдвигает требования к техническому облику системы (инфраструктуре и оснащению).

Технический облик (каналы связи, сенсоры) и программная оснастка (бортовой автомат, протоколы) в совокупности определяют возможные точки отказа и поверхности для атаки. В данной работе рассматриваются сценарии группового мониторинга, поиска и логистики. Цель работы — принципиальное разделение уровней потенциальных воздействий на систему для последующего детального моделирования угроз.

Основная часть. В качестве прототипа системы для рассмотрения принимается гетерогенная группа, состоящая из агентов мультироторного и самолетного типа. Агенты-мультироторы оснащены модулями ближней связи (Wi-Fi Mesh, OSPF/OLSR) и дальней связи (LoRaWAN). Для навигации: ГНСС, опционально СШП дальномеры для валидации и взаимного позиционирования. Сенсоры: камера (1080p, 70–80°), лазерный высотомер. ПО: детерминированный автомат, выполняющий миссию по гео-точкам. Коллаборация между агентами происходит через обмен высокоуровневыми сообщениями и распределенный консенсус для распределения задач. Агенты-самолеты выполняют роль ретрансляторов дальней связи и опорных точек для пеленгации. Вызываются коптерами при нахождении цели для обеспечения дополнительного контроля и в качестве ретранслятора. Наземная станция состоит из приемников дальней связи и АРМ оператора, подключенной по IP к серверной контейнерной архитектуре (включающей базу данных телеметрии, миссий, событий, ресурсов и бэкэнд приложения для обработки ввода оператора и поступающей информации).

Анализ угроз начинается с аппаратного уровня, где физическая реализация системы создаёт фундаментальные риски. Наиболее критичной является возможность спуфинга или глушения сигналов ГНСС, что приводит к потере навигации и отводу агентов с маршрута; современные исследования показывают, что даже одна скомпрометированная единица в рое может дестабилизировать всю группу, если не реализованы механизмы кросс-валидации [3]. Вторым ключевым вектором выступает подавление каналов Wi-Fi Mesh, что разрывает связи между агентами и фрагментирует рой, лишая его возможности коллективного принятия решений. Третьей существенной угрозой остаётся физический захват аппарата, позволяющий злоумышленнику извлечь криптографические ключи и проанализировать прошивку, что компрометирует безопасность всей сети в долгосрочной перспективе [1].

Переходя к уровню бортового программного обеспечения, следует отметить уязвимости логики автономного функционирования. Критическим риском является нарушение алгоритмов распределённого консенсуса, когда внедрение ложных данных о состоянии агентов приводит к хаотичному распределению задач и истощению ресурсов группы; защита от таких атак требует внедрения механизмов византийской отказоустойчивости, что существенно усложняет архитектуру ПО [5]. Не менее опасна манипуляция состоянием детерминированного автомата, например, принудительный перевод в режим ожидания через эксплуатацию уязвимостей логики переходов состояний, что особенно актуально для систем

с ограниченными вычислительными ресурсами [2]. Также высока вероятность подмены сообщений целеуказания, что при отсутствии должной аутентификации позволяет перенаправить группу на ложные координаты.

Инфраструктурный уровень объединяет каналы связи и наземный сегмент, создавая поверхность атаки на управление роем. Здесь наибольшую опасность представляет отравление таблиц маршрутизации протоколов OLSR/OSPF, что создаёт петли или разрывы в сети передачи данных внутри роя; специализированные атаки на изоляцию узлов в OLSR-сетях демонстрируют высокую эффективность даже при ограниченных возможностях злоумышленника [4]. В каналах дальней связи LoRaWAN возможны replay-атаки, позволяющие повторить ранее перехваченные команды управления, если не используются уникальные nonce-значения. Кроме того, компрометация наземной станции через уязвимости серверной архитектуры даёт злоумышленнику полный контроль над планированием миссий, однако требует преодоления нескольких уровней защиты периметра [1].

На системном уровне угрозы проявляются как комплексные сценарии, влияющие на функционирование роя как единого организма. Наиболее разрушительным сценарием является фрагментация роя, достигаемая комбинацией радиоэлектронного подавления и подмены координат, что делает невозможным выполнение групповых задач мониторинга или логистики. Вторым критическим сценарием выступает хайджек миссии, когда через компрометацию лидера или наземного узла противник получает возможность использовать рой в своих интересах. Наконец, специфической уязвимостью данной архитектуры является блокировка вызова самолётов-ретрансляторов, что изолирует удалённые группы коптеров от наземной станции и приводит к потере управления на больших дистанциях.

Выводы. Дальнейшая работа необходима в направлении уточнения технического облика для проработки сценариев реализации наиболее актуальных угроз. В частности, требуется детализация криптографических примитивов для защиты каналов Wi-Fi/LoRa, разработка механизмов валидации данных ГНСС (с использованием СШП) и аудит безопасности контейнерной архитектуры наземного сервера. Без внедрения контрмер на уровне архитектуры (Security by Design) обеспечение безопасности на уровне ПО будет неэффективным.

Список использованных источников:

1. Wang X. et al. A survey on security of UAV swarm networks: Attacks and countermeasures // ACM Computing Surveys. – 2024. – Т. 57. – №. 3. – С. 1-37.
2. Agarwal Y., Raghunathan V. SecuPilot: A Security Coprocessor-Integrated Platform for Autonomous UAV Security //ACM Transactions on Embedded Computing Systems. – 2025. – Т. 24. – №. 5s. – С. 1-25.
3. Gu Z. et al. A Defense Strategy for UAV Swarm Against GNSS Spoofing Attacks Based on Game Model //International Conference on Intelligent Computing. – Singapore : Springer Nature Singapore, 2024. – С. 383-395.
4. Schweitzer N. et al. Persuasive: A node isolation attack variant for olsr-based manets and its mitigation //Ad Hoc Networks. – 2023. – Т. 148. – С. 103192.
5. Strobel V., Pacheco A., Dorigo M. Robot swarms neutralize harmful Byzantine robots using a blockchain-based token economy. Sci. Robot. 8 (79), eabm4636 (2023) [Электронный ресурс].