УДК 004.056

Построение модели нарушителя в децентрализованной группе беспилотных воздушных судов.

Шамрай П.Ю. (ИТМО)
Научный руководитель – кандидат физико-математических наук, доцент Бойко А.М. (ИТМО)

Введение.

Методы децентрализованного управления группой беспилотных воздушных судов (БВС) активно развиваются с появлением реально работающих систем [1]. Поэтому стоит уделять пристальное внимание вопросам безопасности, в том числе связанные с присутствием нарушителя в самой группе. С точки зрения информационной безопасности [2], такой нарушитель может совершать все те противоправные действия, которые он может совершать в сети: от атак типа отказ в обслуживании до прослушивания передаваемых данных. В данной работе рассматривается децентрализованная группа БВС, в которой принятие решений происходит на каждом агенте самостоятельно, основываясь на полученных от датчиков данных. В такой системе нет центрального лидера или связи с наземной станцией. Вследствие этого обмен данными между БВС может быть сведен к минимуму или вовсе отсутствовать. В последнем случае агентам доступна только навигационная информация о ближайших соседях [3]. Модель нарушителя, предложенная в данной работе, схожа с рассмотренной в работах по противодействию с помощью механизмов доверия и репутации [4], но с тем отличием, что отсутствует информационный обмен между агентами. Кроме того, несмотря на детектирование присутствия нарушителя, определение пространственного положения нарушителя в группе может быть сильно затруднено без постоянной коммуникации между агентами.

Основная часть.

Нарушитель в децентрализованной группе БВС обладает навигационной информацией, поступающей с его датчиков. Это могут быть измерения расстояния, углов направления, скоростей, уровня сигнала, а также данные от дополнительных нагрузок, например камеры. Этой информации может быть достаточно для определения взаимного положения и позиционирования в составе группы БВС. Нарушитель не обладает информацией о заранее определенных параметрах поведения агентов в группе. Такими параметрами могут быть целевое время между перестроениями или между целенаправленным обменом сообщениями, расстояние между БЛА. Агенты в группе не знают о присутствии нарушителя, так как он для них такой же объект взаимодействия.

Нарушитель может быть подразделен на внутреннего и внешнего. В первом случае доступ злоумышленника к БВС может быть осуществлен между полетами с внедрением вредоносного программного обеспечения. Во втором случае БВС обладает минимальным набором навигационного оборудования, позволяющим ему взаимодействовать с агентами в группе.

Среди действий, совершаемых нарушителем, можно выделить разведку, перехват информации, внесение возмущений в структуру группы БВС. Последнее может привести к повышенному расходу энергии и невыполнению миссии. Такое воздействие даже в отсутствие информационного обмена может быть осуществлено тремя способами. Первый, прямой способ — это умышленное изменение траектории. Второй, грубый – засветка датчиков, например камер, или зашумление радиоэфира. Третий, косвенный - искажение получаемой навигационной информации, или «мягкая» атака. Степень искажения зависит от использованного типа датчика для взаимного позиционирования. Так, для сверхширокополосных дальномеров это может быть подделка временных меток при обмене сообщениями в процессе измерения расстояния. В случае использования оптоэлектронной

системы взаимного позиционирования осуществляется одностороннее излучение модулированного сигнала. В этом случае нарушитель может излучать искаженную диаграмму направленности или менять частоты модуляции.

Одним из методов противодействия такому виду нарушителей может являться псевдослучайное перестроение, например, с уменьшением расстояния. После этого нарушитель с большой долей вероятности окажется на краю группы, что, по крайней мере, усложнит его воздействие на группу в целом. Для снижения энергозатрат такое перестроение нужно осуществлять только после децентрализованного детектирования аномального поведения. Такой подход позволяет противодействовать нарушителю без знания его точного местоположения.

Выводы.

В данной работе была описана модель нарушителя в группе БВС с децентрализованным управление, с возможным отсутствием информационного обмена. Были определены основные характеристики нарушителя и потенциальные атаки. Предложен метод противодействия нарушителю. Дальнейшая работа будет посвящена разработке методов детектирования и противодействия такому роду нарушителей.

Список использованных источников:

1. Zhu F. et al, «Swarm-LIO2: Decentralized, Efficient LiDAR-inertial Odometry for UAV Swarms», 26 сентябрь 2024 г., arXiv: arXiv:2409.17798. doi: 10.48550/arXiv.2409.17798.

2. Игоревич В. И. и Денисович М. Е., «Противодействие скрытому деструктивному воздействию в роях беспилотных летательных аппаратов», International Journal of Open Information Technologies, т. 6, вып. 12, Art. вып. 12, 2018.

3. Boyko A. и Girgidov R., «Maintaining the spatial stability of a swarm of autonomous unmanned aerial vehicles», Rob. and Tech. Cyb. J., т. 9, вып. 2, сс. 85–90, июн. 2021, doi: 10.31776/RTCJ.9201.

4. Зикратов И.А., Зикратова Т.В., Лебедев И.С., и Гуртов А.В., «Построение модели доверия и репутации к объектам мультиагентных робототехнических систем с децентрализованным управлением», Научно-технический вестник информационных технологий, механики и оптики, вып. 3 (91), Art. вып. 3 (91), 2014.