НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
сентябрь–октябрь 2018 Том 18 № 5 ISSN 2226-1494 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
September–October 2018 Vol. 18 No 5 ISSN 2226-1494 http://ntv.ifmo.ru/en

УДК 004.75

АНАЛИЗ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ ГРУППЫ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

Е.Д. Мариненков[a], И.И. Викснин[a], Ю.А. Жукова[a], М.А. Усова[a]

[a] Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация
Адрес для переписки: mandarin-98@mail.ru

Информация о статье
Поступила в редакцию 30.05.18, принята к печати 25.06.18
doi: 10.17586/2226-1494-2018-18-5-817-825
Язык статьи – русский

Ссылка для цитирования: Мариненков Е.Д., Викснин И.И., Жукова Ю.А., Усова М.А. Анализ защищенности информационного взаимодействия группы беспилотных летательных аппаратов // Научно-технический вестник информационных технологий, механики и оптики. 2018. Т. 18. № 5. С. 817–825. doi: 10.17586/2226-1494-2018-18-5-817-825

Аннотация

Предмет исследования. Проанализировано информационное взаимодействие элементов группы беспилотных летательных аппаратов и их уязвимости к деструктивному информационному воздействию. В настоящий момент данная проблема актуальна для аппаратов, применимых в гражданских сферах. Кроме того, задача выявления скрытого деструктивного информационного воздействия является нерешенной в контексте группы беспилотных летательных аппаратов. **Метод.** Разрабатывается теоретико-множественная модель информационного взаимодействия группы беспилотных летательных аппаратов, на основе результатов сравнительной оценки стратегий группового управления. Проводится анализ разработанной модели, который позволяет выявить и оценить уязвимые элементы, осуществляющие информационное взаимодействие и подверженные деструктивному информационному воздействию. Проводятся эксперименты, в которых в процесс информационного взаимодействия (как внутреннего, так и внешнего) вводится деструктивная информация, приводящая к нарушению функционирования агента или группы в целом. **Основные результаты.** Информационное взаимодействие группы беспилотных летательных аппаратов нуждается в повышении фактора защищенности как от деструктивного информационного воздействия, так и от скрытого деструктивного информационного воздействия. Скрытое деструктивное информационное воздействие невозможно выявить классическими подходами обеспечения информационной безопасности, следовательно, необходимо разработать новые методы, позволяющие увеличить защищенность информационного взаимодействия от подобных атак. **Практическая значимость.** Результаты анализа теоретико-множественной модели информационного взаимодействия группы беспилотных летательных аппаратов позволят разработать новые методы обеспечения информационной безопасности для ликвидации специфических уязвимостей, связанных не только с классическими, но и с «мягкими» методами воздействия, которые будут востребованы для применения в автономных робототехнических системах.

Ключевые слова
информационная безопасность, информационное взаимодействие, деструктивное информационное воздействие, беспилотный летательный аппарат, самоорганизующаяся система

ANALYSIS OF INFORMATION INTERACTION SECURITY WITHIN GROUP OF UNMANNED AERIAL VEHICLES

E.D. Marinenkov[a], I.I. Viksnin[a], Iu.A. Zhukova[a], M.A. Usova[a]

[a] ITMO University, Saint Petersburg, 197101, Russian Federation
Corresponding author: mandarin-98@mail.ru

Article info
Received 30.05.18, accepted 25.06.18
doi: 10.17586/2226-1494-2018-18-5-817-825
Article in Russian
For citation: Marinenkov E.D., Viksnin I.I., Zhukova Iu.A., Usova M.A. Analysis of information interaction security within group of unmanned aerial vehicles. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2018, vol. 18, no. 5, pp. 817–825 (in Russian). doi: 10.17586/2226-1494-2018-18-5-817-825

Abstract

Subject of Research. The paper presents analysis of information interaction of the elements within the group of unmanned aerial vehicles and their vulnerability to destructive information impact. At the moment, this problem is relevant for devices used in civil areas. In addition, the task of identifying hidden destructive information impact is an unsolved problem within

the group of unmanned aerial vehicles. **Method.** A set-theoretical model of information interaction within the group of unmanned aerial vehicles is developed based on comparative evaluation results of the group control strategies. The developed model is analyzed, that gives the possibility to identify and evaluate the vulnerable elements, which carry out information interaction and are subjected to destructive information impact. Experiments are carried out, where destructive information is introduced into the process of information interaction (both internal and external), leading to disruption of the agent or group as a whole. **Main Results.** The information interaction of unmanned aerial vehicles group requires security factor increasing for contraction of the destructive information impact and a hidden destructive information impact. Hidden destructive information impact cannot be detected by classical approaches to information security, therefore, it is necessary to develop new methods to increase the information interaction security from such attacks. **Practical Relevance.** The results of the set-theoretical model analysis of information interaction within unmanned aerial vehicles group will enable the development of new information security methods to eliminate specific vulnerabilities associated not only with the classical, but also with the "soft" impact methods. They will be in demand for the use in autonomous robotic systems.

Keywords
information security, information interaction, destructive information impact, unmanned aerial vehicle, self-organizing system

Введение

В настоящее время в различных сферах деятельности ставятся задачи, которые могут быть решены с помощью беспилотных летательных аппаратов (БПЛА), организованных в «рой». Под роем БПЛА понимается самоорганизующаяся система, элементы которой общаются между собой и на основе этого могут искать коллективно-выработанные решения [1–4]. В контексте данной работы авторам интересны решения об исключении агентов, несущих угрозу для функционирования роя, из информационного взаимодействия (ИВ) при отсутствии человеческого фактора, т.е. на основе информации, передаваемой между агентами. Нарушения в области обеспечения информационной безопасности (ИБ) роя БПЛА могут привести к потерям работоспособности группы. Таким образом, авторы рассматривают вопрос анализа информационного взаимодействия, особенностей имеющихся уязвимостей и существующих угроз в качестве одного из основных вопросов с точки зрения достижения целей, поставленных перед роем.

В связи с популяризацией БПЛА в различных гражданских областях [5] повышается вероятность возникновения ситуаций нарушения работоспособности БПЛА из-за различных угроз [6]. Как правило, на всех этапах разработки робототехнической системы (РТС) фактору защищенности системы уделяется недостаточное внимание, в связи с чем такая система во время функционирования подвержена различным информационным угрозам [7]. В связи с этим одной из важнейших задач данного исследования является обеспечение защищенного группового функционирования БПЛА.

В контексте работы авторы рассматривают не только деструктивное информационное воздействие (ДИВ), но и скрытое деструктивное информационное воздействие (СДИВ). Под СДИВ понимается такое информационное воздействие, которое не может быть обнаружено при помощи классических методов обнаружения нарушений ИБ [7–9]. В рамках существующих научных концепций СДИВ относится к методам «мягкого» воздействия [10, 11].

Авторы нацелены реализовать ДИВ и СДИВ на элементы коллаборации БПЛА, что позволит выявить уязвимости ИВ и в последующем их ликвидировать. По мнению авторов, противодействие ДИВ позволит разработать обобщенную модель защищенного ИВ, применимую к объектам данного исследования.

В работах [12–15] рассматриваются компактные БПЛА, доступные в настоящее время на рынке для гражданского населения. В [12, 13] авторы анализируют канал связи с управляющим устройством на наличие уязвимостей, после чего приходят к выводу, что данные каналы связи необходимо защищать, используя криптографические методы с целью шифрования данных, передаваемых по каналу связи. В работе [14] анализируется канал связи, организованный по Wi-Fi. Исследование выявило необходимость в защите канала от Spoofing (фальсификации данных) и DDoS (отказа в обслуживании) атак. В статье [15] выявлено, что по стандартному каналу связи между БПЛА и управляющим устройством посторонние лица могут получить доступ к системе БПЛА и организовать в ней возможность удаленного подключения. Данные работы рассматривают уязвимости в каналах связи системы частного БПЛА, поэтому авторы считают, что результаты данных исследований неприменимы для групп БПЛА.

Авторы выделяют работу [16], в которой решается проблема обеспечения ИБ в группе БПЛА. Объектом исследования является беспилотный авиационный комплекс разведки, который функционирует совместно с наземным управляющим комплексом. Исследование показало уязвимость канала связи, а также вычислительного центра БПЛА для актуальных киберфизических угроз. Методы, используемые в работе, рассчитаны на централизованные стратегии группового управления, следовательно, они не подходят для анализа децентрализованно-организованных систем.

Авторы работы [17] рассматривают рой БПЛА, предполагающий самоорганизующуюся группу, основанную на мультиагентном подходе. Данное исследование нацелено на теоретическое обоснование необходимости организации защиты групп БПЛА от актуальных атак. Авторы обеспокоены наличием нестандартных уязвимостей в связи с особенностями децентрализованно-организованных групп. В дан-

ной работе не рассматривается ИВ элементов группы, что дает научный задел для разработки модели ИВ и ее анализа.

В работах [18, 19] рассматриваются группы БПЛА, использующие децентрализованные стратегии при взаимодействии БПЛА к БПЛА, но имеющие наземные центры управления, что означает внедрение смешанной стратегии группового управления. Анализ данных групп показал необходимость внедрения методов защиты ИВ. Несмотря на успешные исследования в области обеспечения ИБ ИВ, использование человеческого фактора, а также центров управления повышает риск нарушения функционирования группы.

Стоит отметить диссертационную работу [20], в которой автор проводит анализ сети, состоящей из БПЛА, на наличие уязвимостей и подверженность различным актуальным атакам, в число которых входят DDoS, Jamming (заполнение «эфира» нелегализованным трафиком), Spoofing. В работе рассматриваются централизованные и децентрализованные методы организации сети БПЛА как гражданского, так и военного назначения. В своих исследованиях автор рассматривает БПЛА как летательный объект (ЛА) самолетного типа, что дает научный задел для разработки системы коллективного группового управления БПЛА на основе мультироторных ЛА, включающих в себя трикоптеры, квадрокоптеры, гексокоптеры и октокоптеры [21].

Поскольку децентрализованные методы коллективного управления базируются на мультиагентном подходе, возможна адаптация и применение их в контексте групп БПЛА. Таким образом, еще одной задачей исследования является анализ данных методов по фактору защищенности передаваемой информации.

После анализа имеющихся работ по обеспечению ИБ РТС [12–20] авторы считают, что именно выявление уязвимостей в ИВ является одной из важнейших задач комплексного обеспечения ИБ групп БПЛА. Таким образом, формулируется цель исследования – анализ уязвимостей, возникающих в процессе ИВ между элементами самоорганизующейся группы БПЛА. Для достижения поставленной цели были сформулированы следующие задачи:

- анализ существующих подходов к организации коллективного управления группой БПЛА с точки зрения ИБ;
- разработка обобщенной модели функционирования группы БПЛА с учетом результатов анализа существующих подходов;
- выявление специфических уязвимостей в информационном взаимодействии агентов группы БПЛА, связанных не только с классическими, но и с «мягкими» методами воздействия;
- определение последствий от реализации частных угроз информационной безопасности, эксплуатирующих существующие уязвимости;
- организация экспериментальной проверки сформулированных выводов.

Для решения данных задач необходимо использование новых подходов к системному анализу разработанной теоретико-множественной модели ИВ группы БПЛА, поскольку концепция группы, предлагаемая авторами, отличается от базовых понятий киберфизических систем, mesh-сетей и тому подобных за счет отсутствия на данном этапе инструкций для исключения недостоверных агентов из ИВ. Анализ позволит авторам определить необходимые меры противодействия выявленным угрозам, внедрение которых позволит установить правила безопасности в группе, а также говорить о группе БПЛА как о рое.

Стратегии группового управления

Основываясь на работе [22], стратегии группового управления можно разделить на централизованные и децентрализованные.

Главным отличием централизованных стратегий является наличие центрального управляющего устройства (ЦУУ). Это устройство осуществляет тотальный контроль над всеми остальными агентами и является главным элементом системы. Преимуществом данного подхода является простота интеграции с алгоритмической стороны. Среди недостатков можно выделить загруженность ЦУУ, которая будет значительно увеличиваться при относительно малом приросте количества агентов в группе, а также низкую жизнеспособность.

В свою очередь, децентрализованные стратегии имеют большую жизнеспособность за счет отсутствия ЦУУ. Их подразделяют на коллективную стратегию, в которой агенты обмениваются информацией для достижения групповой цели, и стайную стратегию, агенты которой функционируют независимо друг от друга.

Преимуществом коллективного подхода является высокая жизнеспособность системы и ее быстродействие. Недостатками являются сложность алгоритмизации, а также наличие канала обмена информацией, которое может привести к нарушению функционирования системы при вмешательстве деструктивного характера.

В свою очередь, система, основанная на стайной стратегии, за счет отсутствия канала обмена информацией имеет наивысшую жизнеспособность среди остальных стратегий. Также среди преимуществ

стоит отметить минимальную загруженность агентов, не зависящую от их количества, и простоту алгоритмизации. Однако стайная стратегия не может быть применена к рою БПЛА для достижения общей цели, так как не позволяет сложным элементам (БПЛА) осуществлять коммуникацию, что может привести к нарушениям в функционировании системы. Следовательно, использование коллективной стратегии управления позволяет не только удалить из системы ЦУУ, но и обеспечить оптимальное выполнение сложных составных задач группой БПЛА [3, 4].

При этом информационное взаимодействие элементов роя БПЛА имеет значительные уязвимости. Для анализа этих уязвимостей и возможных путей их эксплуатации, а также последствий от их реализации, требуется представить обобщенную модель информационного взаимодействия группы БПЛА, управление которой основано на коллективной стратегии.

Обобщенная модель информационного взаимодействия. Для достижения цели исследования авторы разделяют ИВ на внутреннее и внешнее.

Во внутреннем ИВ участвуют следующие элементы: сенсоры и датчики, собирающие информацию о положении в пространстве и препятствиях в окружающей среде; процессорное устройство (ПУ), отвечающее за обработку информации и формулировании команд; моторы и иные устройства, необходимые для выполнения целей агента. Таким образом, в процессе внутреннего ИВ передается информация о координатах, положении в пространстве (углы тангажа, крена, рыскания), препятствиях, техническом состоянии агента, команды для регулировки положения в пространстве и для выполнения иных задач.

Во внешнем ИВ авторы рассматривают БПЛА как неделимый объект. Информация, получаемая агентами в процессе обмена информацией друг с другом, подразделяется на информацию о местоположениях других БПЛА группы, местоположениях препятствий в среде, техническом состоянии агентов. На основе вышеописанной информации коллаборация имеет возможность коллективно распределять задачи между агентами.

Данное исследование предполагает, что коллаборация БПЛА является сетью, устойчивой к разрывам, следовательно, все информационные сообщения доходят до адресата [23].

Рис. 1. Последовательность передачи информационных сообщений в модели внутреннего информационного взаимодействия элементов в группе беспилотных летательных аппаратов

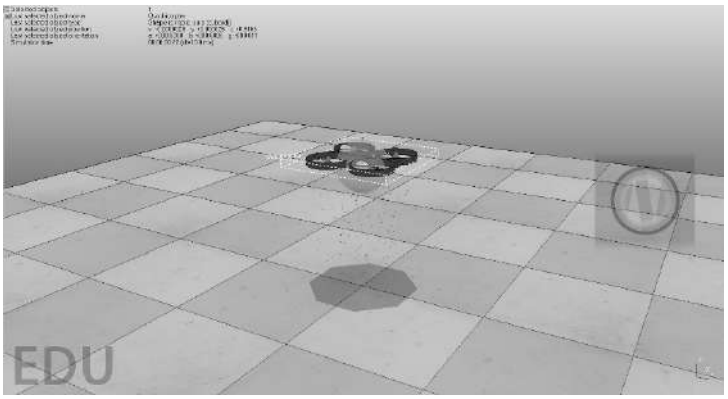
Рис. 2. Уязвимые информационные сообщения в модели внутреннего информационного взаимодействия элементов в группе беспилотных летательных аппаратов

Анализ модели внутреннего информационного взаимодействия. Анализируя внутреннее ИВ, можно говорить об уязвимости всех элементов, представленных в модели. Такой вывод можно сделать, заметив, что устройства сканирования окружающей среды и определения положения в пространстве получают информацию от окружающей среды, что подразумевает возможность ее искажения в процессе считывания, следовательно, эти устройства уязвимы для ДИВ. После сбора необходимых данных устройства сканирования окружающей среды и определения положения в пространстве обрабатывают и передают эти данные ПУ, следовательно, оно уязвимо к ДИВ со стороны данных устройств. По аналогии с ПУ, устройства регулирования положения в пространстве и дополнительные устройства, используемые для решения задач, уязвимы к ДИВ со стороны ПУ.

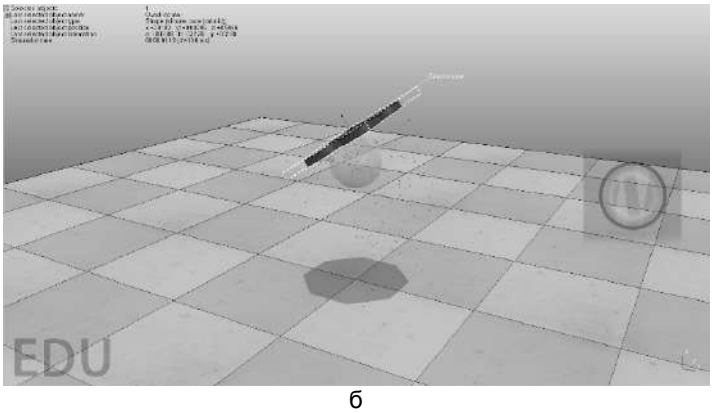
Если рассматривать обобщенную модель внутреннего ИВ в группе БПЛА как информационную цепочку (рис. 1), то можно говорить о том, что наиболее уязвимыми к ДИВ являются устройства регулирования положения в пространстве и дополнительные устройства, поскольку они являются последними элементами цепи, следовательно, в случае ДИВ на предыдущие элементы и нарушения их функционирования последние элементы получают наиболее искаженную информацию.

На рис. 2 представлена модель внутреннего ИВ с выделенной информацией, уязвимой к ДИВ.

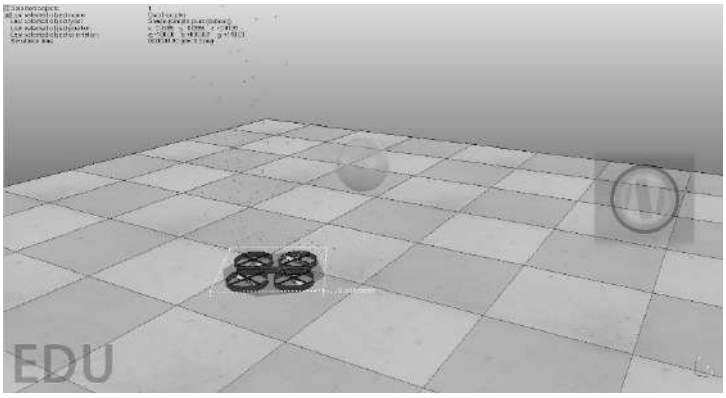
Нарушение функционирования системы частного БПЛА



а



б



в

Рис. 3. Нарушение функционирования беспилотного летательного аппарата: начало функционирования (а); отклонение от параллели (б); падение (в)

С целью визуализации частного случая ДИВ на систему БПЛА проводится эксперимент в симуляторе V-REP [24], где задачей агента является строгое перемещение по вертикали. Для выполнения задачи на каждый мотор БПЛА подается мощность, требуемая для взлета БПЛА (рис. 3, а). В данном случае СДИВ является внедрение негативной информации о требуемой мощности мотора в ИВ элементов системы частного БПЛА. Авторы вводят негативную информацию после 1 секунды функционирования агента, после чего наблюдается отклонение от положения корпуса параллельного плоскости *XY* (рис. 3, б). В конечном итоге БПЛА начинает перемещаться в сторону плоскости *XY* и падает на нее (рис. 3, в).

Таким образом, был рассмотрен пример, в ходе которого явно нарушается поведение элемента, если анализировать его поведение с точки зрения роя. При этом нарушения в рамках внутреннего ИВ могут быть оценены как СДИВ, так как ни один из внутренних элементов БПЛА не имеет возможности идентифицировать поведение других элементов, которые нарушают семантическую целостность информации, как деструктивное.

Анализ модели внутреннего информационного взаимодействия

Выявим уязвимости в обобщенной модели внешнего ИВ. Группа БПЛА состоит из *n* агентов, которые обмениваются некоторой информацией, на основе которой принимают дальнейшие решения (рис. 4). Авторы вводят допущение, что *i*-й БПЛА функционирует без сбоев и не может быть источником негативной информации.

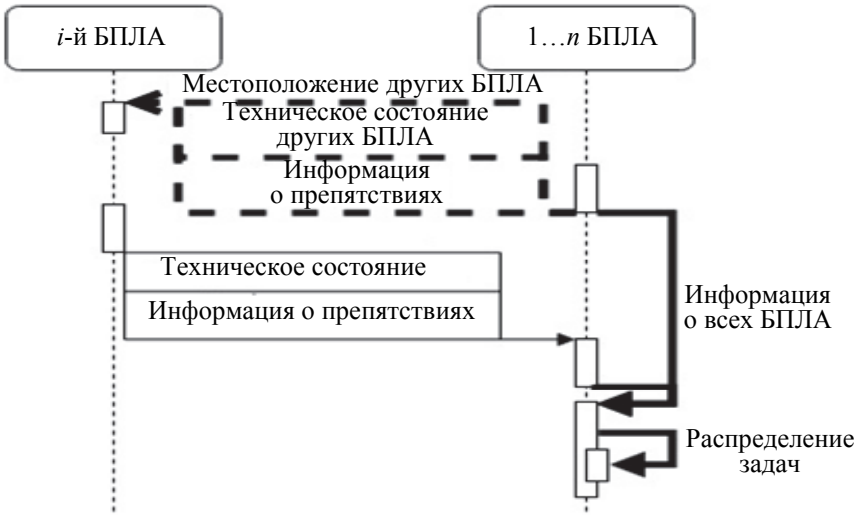


Рис. 4. Уязвимые информационные сообщения и процессы в модели внешнего информационного взаимодействия элементов в группе беспилотных летательных аппаратов

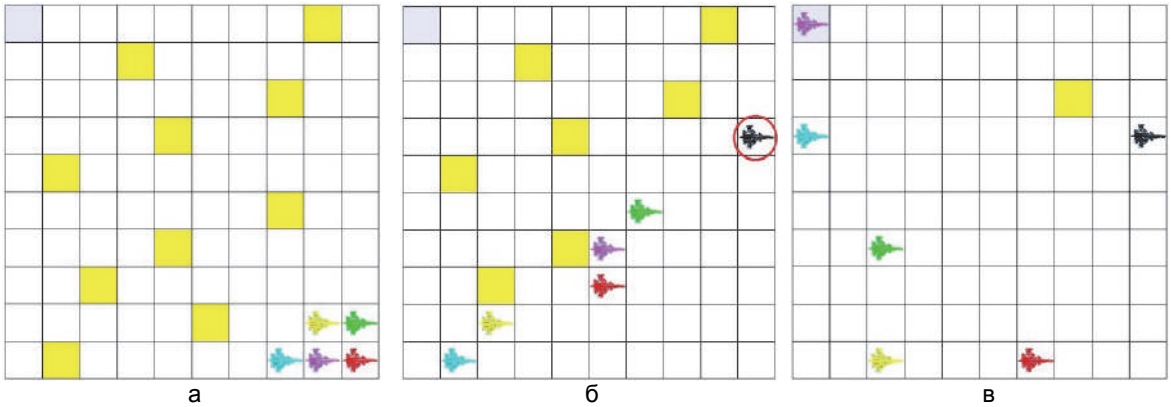
Информация, получаемая *i*-м БПЛА от других агентов, а также информация, передаваемая между этими агентами, уязвима для ДИВ. В данном случае первая информация передается напрямую от агентов, в то время как вторая передается и обрабатывается всеми агентами группы, после чего результат передается всем агентам группы.

Нарушение функционирования группы БПЛА

Смоделируем частную ситуацию функционирования группы в симуляторе Anylogic [25]. Группа функционирует внутри квадрата 10×10 клеток и состоит из 5 агентов, каждый из которых имеет собственную клетку для начала функционирования и собственный идентификационный номер id (от 1 до 5). Целью группы является выполнение 10 задач, в виде перемещения «флагов» в зону сдачи задания, обозначенную серым цветом (рис. 5, а). Для выполнения групповой цели агенты коллективно распределяют задачи. Агенту достается задача, если расстояние до нее от агента – наименьшее среди всех агентов, а агент свободен (не выполняет другую задачу). Задачи имеют свои порядковые номера от 1 до 10 и могут иметь статус «невыполненная», если ни один из агентов не взял ее для выполнения; «выполняется», если агент взял ее для выполнения, но еще не выполнил; «выполнена», если агент выполнил данную задачу. Условиями выполнения задачи являются достижение агентом квадрата, где лежит «флаг», и перенос данного флага в зону сдачи задания, после этого статус задачи меняется на «выполнена», а статус агента – на «свободен». Группа достигает цели только при условии, что все задачи имеют статус «выполнена». Для исключения спорных ситуаций вводятся следующие условия: при равных минимальных расстояниях выбирается агент с большим id; при нескольких задачах для одного агента выбирается задача с наименьшим порядковым номером.

Для экспериментального доказательства уязвимости внешнего ИВ к ДИВ внедрим ложного агента на 30-ой секунде функционирования группы (рис. 5, б). Цель данного агента – нарушить функционирование группы, взяв задачу, но не выполнив ее, тем самым группа БПЛА не сможет достичь цели, что является нарушением функционирования группы.

В конце эксперимента остается лишь одна задача, которую агенты группы не могут выполнить (рис. 5, в), следовательно, внедренный агент нарушил функционирование группы с помощью ДИВ. При этом можно также утверждать, что агент, не прошедший процедуру аутентификации, оказывает не только ДИВ, но и СДИВ, так как БПЛА-нарушитель предоставляет ложную информацию о своей способности/готовности выполнить поставленную перед ним задачу или в общем случае действовать в интересах всей группы БПЛА.



а б в

Рис. 5. Нарушение функционирования группы беспилотных летательных аппаратов: группа в начале функционирования (а); внедрение ложного агента в функционирующую группу (б); нарушение функционирования группы (в)

Заключение

Данное исследование было нацелено на определение уязвимостей в информационном взаимодействии элементов группы беспилотных летательных аппаратов. В результате была выбрана децентрализованная коллективная стратегия, исходя из возможности выработки коллективных решений агентами, а также из высокой жизнеспособности такой системы, в контексте обеспечения информационной безопасности. Несмотря на это, информационное взаимодействие роя имеет уязвимые элементы. Для выявления уязвимостей были описаны внешнее и внутреннее информационные взаимодействия, а именно все элементы и информация, участвующие в данном взаимодействии. Описание данных взаимодействий позволяет говорить о разработанной теоретико-множественной модели информационного взаимодействия элементов группы беспилотных летательных аппаратов с учетом результатов проведенного анализа существующих подходов к организации группового функционирования. Разработанная модель была проанализирована на наличие уязвимостей для возникновения деструктивного информационного воздействия и скрытого деструктивного информационного воздействия. Было выявлено, что во внутреннем информационном взаимодействии все элементы и вся информация могут быть подвержены деструктивному информационному воздействию, а также скрытому деструктивному информационному воздействию, поскольку элементы не имеют возможности выявить аномалии в поведении других элементов. Был проведен эксперимент по внедрению в информационное взаимодействие деструктивной информации, что привело к нарушению функционирования агента. Во внешнем информационном взаимодействии вся информация, передаваемая частному доверенному агенту, может быть подвержена деструктивному информационному воздействию и скрытому деструктивному информационному воздействию. Был проведен эксперимент, в котором внедренный агент передавал деструктивную информацию, вследствие чего было нарушено функционирование всей группы беспилотных летательных аппаратов. Анализ информационного взаимодействия группы беспилотных летательных аппаратов и выявление уязвимостей позволяют говорить о достижении авторами цели исследования. В результате проведенного исследования авторы работы делают вывод о возможности защиты от деструктивного информационного воздействия путем использования классических методов обеспечения информационной безопасности (методы аутентификации, мобильной криптографии и т.д.), однако для защиты от скрытого деструктивного информационного воздействия требуется разработать новые методы, позволяющие обнаруживать и противодействовать «мягкому» воздействию.

Дальнейшие перспективы исследования направлены на разработку модели защищенного информационного взаимодействия, моделирование различных сценариев атак на рой беспилотных летательных аппаратов, оценку и повышение надежности и устойчивости системы к потенциальной реализации угроз информационной безопасности. Выполнение данных задач позволит разработать группу беспилотных

летательных аппаратов, устойчивую к возникновению различных нарушений в области информационного обмена, что позволит применять данную систему в условиях агрессивной окружающей среды.

Литература

1. Chung T.H., Jones K.D., Day M.A., Jones M., Clement M. 50 vs. 50 by 2015: Swarm vs. Swarm UAV live-fly competition at the naval postgraduate school // AUVSI. 2013. P. 1792–1811.
2. Yakimenko O.A., Chung T.H. Extending autonomy capabilities for unmanned systems with CRUSER // Proc. 28th Congress of the International Council of the Aeronautical Sciences (ICAS 2012). 2012. P. 47–49.
3. Yang J.H., Kapolka M., Chung T.H. Autonomy balancing in a manned-unmanned teaming (MUT) swarm attack / In: Robot Intelligence Technology and Applications. 2012. P. 561–569. doi: 10.1007/978-3-642-37374-9_54
4. Chung T.H., Burdick J.W., Murray R.M. A decentralized motion coordination strategy for dynamic target tracking // Proc. IEEE Int. Conf. on Robotics and Automation. 2006. P. 2416–2422. doi: 10.1109/ROBOT.2006.1642064
5. Трубников Г.В. Применение беспилотных летательных аппаратов в гражданских целях [Электронный ресурс]. 2017. Режим доступа: http://www.uav.ru/articles/civil_uav_th.pdf, своб. Яз. рус. (дата обращения: 12.03.2018).
6. Коваль Е.Н., Лебедев И.С. Общая модель безопасности робототехнических систем // Научно-технический вестник информационных технологий, механики и оптики. 2013. № 4(86). С. 153–154.
7. Зикратов И.А., Козлова Е.В., Зикратова Т.В. Анализ уязвимостей робототехнических комплексов с роевым интеллектом // Научно-технический вестник информационных технологий, механики и оптики. 2013. № 5(87). С. 149–154.
8. Викснин И.И. Модель обеспечения информационной безопасности киберфизических систем // Наука и бизнес: пути развития. 2018. № 2(80). С. 15–20.
9. Комаров И.И., Юрьева Р.А., Дранник А.Л., Масленников О.С., Коваленко М.Е., Егоров Д.А. Исследование деструктивного воздействия роботов-злоумышленников на эффективность работы мультиагентной системы // Процессы управления и устойчивость. 2014. Т. 1. № 1. С. 336–340.
10. Зикратов И.А., Зикратова Т.В., Лебедев И.С., Гуртов А.В. Построение модели доверия и репутации к объектам мультиагентных робототехнических систем с децентрализованным управлением // Научно-технический вестник информационных технологий, механики и оптики. 2014. № 3(91). С. 30–38.
11. Юрьева Р.А., Комаров И.И., Дородников Н.А. Построение модели нарушителя информационной безопасности для мультиагентной робототехнической системы с децентрализованным управлением // Программные системы и вычислительные методы. 2016. № 1. С. 42–48. doi: 10.7256/2305-6061.2016.1.17946
12. Kirichenko V.V. Information security of communication channel with UAV // Electronics and Control Systems. 2015. N 3. P. 23–27. doi: 10.18372/1990-5548.45.9892
13. Rivera E., Baykov R., Gu G. A Study on Unmanned Vehicles and Cyber Security. Texas, USA, 2014.
14. Hooper M., Tian Y., Zhou R. et al. Securing commercial WiFi-based UAVs from common security attacks // Proc. IEEE Military Communications Conference. 2016. P. 1213–1218. doi: 10.1109/MILCOM.2016.7795496
15. Watkins L., Li C., Ramos J. et al. Exploiting multi-vendor vulnerabilities as back-doors to counter the threat of rogue small unmanned aerial systems // Proc. ACM MobiHoc Workshop on Mobile IoT Sensing, Security, and Privacy. Los Angeles, 2018. doi: 10.1145/3215466.3215467
16. Тутубалин П.И., Кирпичников А.П. Обеспечение информационной безопасности функционирования комплексов беспилотной разведки // Вестник Казанского технологического университета. 2017. Т. 20. № 21. С. 86–92.
17. Higgins F., Tomlinson A., Martin K.M. Threats to the swarm: security considerations for swarm robotics // International

References

1. Chung T.H., Jones K.D., Day M.A., Jones M., Clement M. 50 vs. 50 by 2015: Swarm vs. Swarm UAV live-fly competition at the naval postgraduate school. *AUVSI*, 2013, pp. 1792–1811.
2. Yakimenko O.A., Chung T.H. Extending autonomy capabilities for unmanned systems with CRUSER. *Proc. 28th Congress of the International Council of the Aeronautical Sciences, ICAS 2012*, 2012, pp. 47–49.
3. Yang J.H., Kapolka M., Chung T.H. Autonomy balancing in a manned-unmanned teaming (MUT) swarm attack. In *Robot Intelligence Technology and Applications*, 2012, pp. 561–569. doi: 10.1007/978-3-642-37374-9_54
4. Chung T.H., Burdick J.W., Murray R.M. A decentralized motion coordination strategy for dynamic target tracking. *Proc. IEEE Int. Conf. on Robotics and Automation*, 2006, pp. 2416–2422. doi: 10.1109/ROBOT.2006.1642064
5. Trubnikov G.V. *The use of unmanned aerial vehicles for civilian purposes*, 2017. Available at: http://www.uav.ru/articles/civil_uav_th.pdf (accessed 12.03.2018).
6. Koval E.N., Lebedev I.N. General model of robotic systems information security. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2013, no. 4, pp. 153–154. (in Russian)
7. Zikratov I.A., Kozlova E.V., Zikratova T.V. Vulnerability analysis of robotic systems with swarm intelligence. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2013, no. 5, pp. 149–154. (in Russian)
8. Viksnin I.I. A model of information security for cyberphysical systems. *Science and Business: Ways of Development*, 2018, no. 2, pp. 15–20. (in Russian)
9. Komarov I.I., Yur'eva R.A., Drannik A.L., Maslennikov O.S., Kovalenko M.E., Egorov D.A. Research on destructive impact of robots-sabouters" influence on multi-agent system"s productivity. *Control Processes and Stability*, 2014, vol. 1, no. 1, pp. 336–340. (in Russian)
10. Zikratov I.A., Zikratova T.V., Lebedev I.S., Gurtov A.V. Trust and reputation model design for objects of multi-agent robotics systems with decentralized control. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2014, no. 3, pp. 30–38. (in Russian)
11. Yur'eva R.A., Komarov I.I., Dorodnikov N.A. Designing the information interloper model for the multi-agent decentralized control robotic system. *Software Systems and Computational Methods*, 2016, no. 1, pp. 42–48. doi: 10.7256/2305-6061.2016.1.17946 (in Russian)
12. Kirichenko V.V. Information security of communication channel with UAV. *Electronics and Control Systems*, 2015, no. 3, pp. 23–27. doi: 10.18372/1990-5548.45.9892
13. Rivera E., Baykov R., Gu G. *A Study on Unmanned Vehicles and Cyber Security*. Texas, USA, 2014.
14. Hooper M., Tian Y., Zhou R. et al. Securing commercial WiFi-based UAVs from common security attacks. *Proc. IEEE Military Communications Conference*, 2016, pp. 1213–1218. doi: 10.1109/MILCOM.2016.7795496
15. Watkins L., Li C., Ramos J. et al. Exploiting multi-vendor vulnerabilities as back-doors to counter the threat of rogue small unmanned aerial systems. *Proc. ACM MobiHoc Workshop on Mobile IoT Sensing, Security, and Privacy*. Los Angeles, 2018. doi: 10.1145/3215466.3215467
16. Tutubalin P.I., Kirpichnikov A.P. Ensuring information security of functioning of unmanned reconnaissance complexes. *Vestnik KSTU*, 2017, vol. 20, no. 21, pp. 86–92. (in Russian)
17. Higgins F., Tomlinson A., Martin K.M. Threats to the swarm: Security considerations for swarm robotics. *International Journal on Advances in Security*, 2009, vol. 2, no. 2&3, pp. 288–297.
18. Sedjelmaci H., Senouci S.M. Cyber security methods for aerial vehicle networks: taxonomy, challenges and solution.

Journal on Advances in Security. 2009. V. 2. N 2&3. P. 288–297.
18. Sedjelmaci H., Senouci S.M. Cyber security methods for aerial vehicle networks: taxonomy, challenges and solution // The Journal of Supercomputing. 2018. P. 1–17. doi: 10.1007/s11227-018-2287-8
19. Sidorov V., Ng W.K., Lam K.Y., Salle M.F.B.M. Cyber-threat analysis of a UAV traffic management system for urban airspace // Air Transport Research Society World Conference. 2017. 9 p.
20. Javaid A.Y. Cyber security threat analysis and attack simulation for unmanned aerial vehicle network. PhD Dissertation. University of Toledo, 2015.
21. Барбасов В.К., Гаврюшин Н.М., Дрыга Д.О., Батаев М.С., Алтынов А.Е. Многороторные беспилотные летательные аппараты и возможности их использования для дистанционного зондирования Земли // Инженерные изыскания. 2012. № 10. С. 38–42.
22. Каляев И.А., Гайдук А.Р., Капустян С.Г. Модели и алгоритмы коллективного управления в группах роботов. М.: Физматлит, 2009. 280 с.
23. Gao L., Yu S., Luan T.H., Zhou W. Delay Tolerant Networks. Springer, 2015. 85 p. doi: 10.1007/978-3-319-18108-0
24. Rohmer E., Singh S.P.N., Freese M. V-REP: a versatile and scalable robot simulation framework // Proc. 2013 IEEE/RSJ Int. Conf. on Intelligent Robots and Systems. 2013. P. 1321–1326. doi: 10.1109/iros.2013.6696520
25. Grigoryev I. AnyLogic 7 in Three Days: A Quick Course in Simulation Modeling. 2015. 256 p.

The Journal of Supercomputing, 2018, pp. 1–17. doi: 10.1007/s11227-018-2287-8
19. Sidorov V., Ng W.K., Lam K.Y., Salle M.F.B.M. Cyber-threat analysis of a UAV traffic management system for urban airspace. *Air Transport Research Society World Conference*, 2017, 9 p.
20. Javaid A.Y. *Cyber security threat analysis and attack simulation for unmanned aerial vehicle network*. PhD Dissertation. University of Toledo, 2015.
21. Barbasov V.K., Gavryushin N.M., Dryga D.O., Bataev M.S., Altynov A.E. Multimotor unmanned aerial vehicles and their capabilities for using in the field of Earth remote sensing. *Inzhenernye Izyskaniya*, 2012, no. 10, pp. 38–42. (in Russian)
22. Kalyaev I.A., Gaiduk A.R., Kapustyan S.G. *Models and Algorithms of the Collective Control of Robots Group*. Moscow, Fizmatlit Publ., 2009, 280 p. (in Russian)
23. Gao L., Yu S., Luan T.H., Zhou W. *Delay Tolerant Networks*. Springer, 2015, 85 p. doi: 10.1007/978-3-319-18108-0
24. Rohmer E., Singh S.P.N., Freese M. V-REP: a versatile and scalable robot simulation framework. *Proc. 2013 IEEE/RSJ Int. Conf. on Intelligent Robots and Systems*, 2013, pp. 1321–1326. doi: 10.1109/iros.2013.6696520
25. Grigoryev I. *AnyLogic 7 in Three Days: A Quick Course in Simulation Modeling*. 2015, 256 p.

Авторы

Мариненков Егор Денисович – лаборант, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, ORCID ID: 0000-0001-9895-239X, mandarin-98@mail.ru

Викснин Илья Игоревич – аспирант, научный сотрудник, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, Scopus ID: 57191359693, ORCID ID: 0000-0002-3071-6937, wixnin@mail.ru

Жукова Юлия Александровна – студент, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, ORCID ID: 0000-0002-7877-1660, zhukova1998@gmail.com

Усова Мария Андреевна – студент, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, ORCID ID: 0000-0001-6981-035X, gipurer@gmail.com

Authors

Egor D. Marinenkov – laboratory assistant, ITMO University, Saint Petersburg, 197101, Russian Federation, ORCID ID: 0000-0001-9895-239X, mandarin-98@mail.ru

Ilya I. Viksnin – postgraduate, Scientific researcher, ITMO University, Saint Petersburg, 197101, Russian Federation, Scopus ID: 57191359693, ORCID ID: 0000-0002-3071-6937, wixnin@mail.ru

Iuliia A. Zhukova – student, ITMO University, Saint Petersburg, 197101, Russian Federation, ORCID ID: 0000-0002-7877-1660, zhukova1998@gmail.com

Maria A. Usova – student, ITMO University, Saint Petersburg, 197101, Russian Federation, ORCID ID: 0000-0001-6981-035X, gipurer@gmail.com