УНИВЕРСИТЕТ ИТМО

НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
ноябрь–декабрь 2021 Том 21 № 6 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
November–December 2021 Vol. 21 No 6 http://ntv.ifmo.ru/en/
ISSN 2226-1494 (print) ISSN 2500-0373 (online)

НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК УНИВЕРСИТЕТ ИТМО
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

doi: 10.17586/2226-1494-2021-21-6-919-928
УДК 004.77

Модель маршрутизации каналов информационного взаимодействия в сети FANET с использованием аппарата нечеткой логики

Зуи Хань Чан[1], Игорь Иванович Комаров[2]✉, Лам Хань Ву[3], Ван Хиеу Лэ[4]

[1,2,3,4] Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация

[1] viewtheworld93@gmail.com, https://orcid.org/0000-0002-4891-8924
[2] iik_st@mail.ru✉, https://orcid.org/0000-0002-6542-4950
[3] vulamkhanh@gmail.com, https://orcid.org/0000-0003-3902-3413
[4] dragon220294@gmail.com, https://orcid.org/0000-0002-9413-5138

Аннотация

Концепция Flying Ad Hoc Network (FANET) используется подвижными воздушными объектами и обеспечивает формирование самоорганизующихся сетей, которые организуют каналы информационного взаимодействия между этими объектами. Специфическим свойством воздушных объектов – агентов FANET является высокая скорость перемещения и ограниченная дальность коммуникации, что приводит к постоянным преобразованиям топологии при изменении помеховой обстановки. Изменения приводят к нарушениям доступности данных и к невыполнению задачи группировкой объектов в целом. Один из путей повышения качества информационного взаимодействия агентов в сети FANET — оптимизация маршрутизации каналов в динамической топологии мобильных агентов. В работе предложена модель маршрутизации каналов информационного взаимодействия в сети FANET с использованием аппарата нечеткой логики для группировки беспилотных воздушных судов ограниченной производительности. Модель позволяет учитывать не только технические факторы, но и состояние информационной безопасности взаимодействующих объектов, что обеспечивает более высокую устойчивость системы коммуникации при наличии внутреннего нарушителя информационной безопасности в группировке беспилотных воздушных судов. Приведены данные сравнительного анализа разработанного протокола Fuzzy с известными протоколами AODV, OLSR.

Ключевые слова

канал информационного взаимодействия, динамическая маршрутизация, информационная безопасность, БВС, Fuzzy logic, FANET

Ссылка для цитирования: Чан З.Х., Комаров И.И., Ву Л.Х., Лэ В.Х. Модель маршрутизации каналов информационного взаимодействия в сети FANET с использованием аппарата нечеткой логики // Научно-технический вестник информационных технологий, механики и оптики. 2021. Т. 21, № 6. С. 919–928. doi: 10.17586/2226-1494-2021-21-6-919-928

Model of information interaction channel routing on the FANET network using fuzzy logic

Duy Khanh Tran[1], Igor I. Komarov[2]✉, Lam Khanh Vu[3], Van Hieu Le[4]

[1,2,3,4] ITMO University, Saint Petersburg, 197101, Russian Federation

[1] viewtheworld93@gmail.com, https://orcid.org/0000-0002-4891-8924
[2] iik_st@mail.ru✉, https://orcid.org/0000-0002-6542-4950
[3] vulamkhanh@gmail.com, https://orcid.org/0000-0003-3902-3413
[4] dragon220294@gmail.com, https://orcid.org/0000-0002-9413-5138

Abstract

The Flying Adhoc (FANET) network is focused on the use of mobile airborne objects and makes it possible to form self-organizing networks, which can provide channels of information interaction between these objects and not be limited.

A specific property of airborne objects (FANET agents) is a high speed of movement and a limited communication range, which leads to frequent topology changes in a changing noise environment. This entails a data availability violation and may lead to the impossibility of performing the task by the group. One of the ways to improve the quality of information interaction between agents in the FANET network is to optimize the routing of information interaction channels in the dynamic topology of mobile agents. The paper proposes a model for routing communication channels in the FANET network using a fuzzy logic approach for grouping unmanned aerial vehicles (UAVs) with limited performance. The proposed model provides higher stability of the communication system for mobile objects when there are potential threats to the UAV grouping. The productivity of the described solutions is confirmed by the study of the developed Fuzzy protocol implemented in the NS3 environment: an analysis of quality indices is carried out in comparison with the well-known routing protocols AODV, OLSR.

Keywords
information communication channel, dynamic routing, information security, UAV, Fuzzy logic, FANET

For citation: Tran D.K., Komarov I.I., Vu L.K., Le V.H. Model of information interaction channel routing on the FANET network using fuzzy logic. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2021, vol. 21, no. 6, pp. 919–928 (in Russian). doi: 10.17586/2226-1494-2021-21-6-919-928

Введение

Необходимое условие выполнения задачи для группировки беспилотных воздушных судов (БВС) — безопасное информационное взаимодействие. Ряд специфических характеристик БВС (подвижность, ограниченность вычислительных и энергетических ресурсов, ограниченность дальности взаимодействия, меняющаяся помеховая обстановка) делают малоэффективными традиционные способы организации их информационного взаимодействия. Концепция Flying Ad Hoc Network (FANET) [1] предлагает решение, связанное с созданием динамической самоорганизующейся сети, предусматривающее в общем случае участие каждого из агентов в формировании графа коммуникационной связности.

Известны [2] общетехнические ограничения, связанные как с конструктивными особенностями БВС, так и с технико-экономическими соображениями. На них накладываются дополнительные проблемы информационной безопасности [3, 4], связанные с динамичностью не только топологии сети, но и *состава элементов*, угроз внешних кибератак, преднамеренных и непреднамеренных внутренних нарушителей и воздействия окружающей среды.

К числу наиболее жестких ограничений в рассматриваемом классе микро- и мини-БВС ближнего радиуса действия (по классификации[1]) относится энерговооруженность, которая в свою очередь ограничивает вычислительную мощность, доступную для решения как функциональных, так и сервисных задач. Традиционно для оценки производительности вычислителей с плавающей точкой используется показатель MFLOPS [5]. По результатам экспериментальных исследований[2] определены следующие ограничения (рис. 1) общих вычислительных ресурсов, исходя из энерговооруженности БВС.

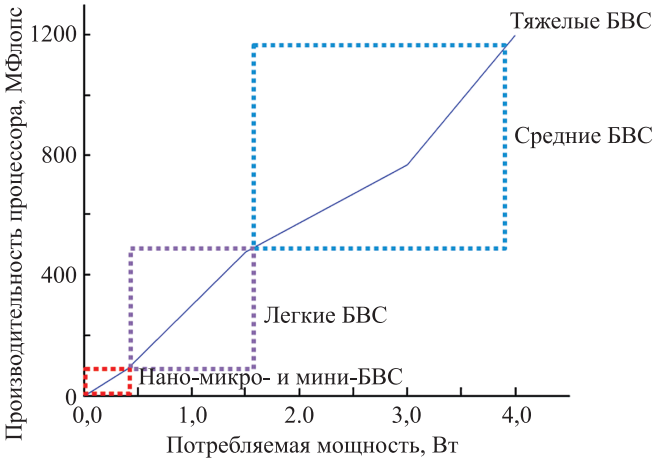

Рис. 1. Доступные вычислительное ресурсы и энерговооруженность бортовых вычислительных устройств беспилотных воздушных судов

Fig. 1. Available computing resources and the power-to-weight ratio of unmanned aerial vehicles onboard computing devices

В настоящее время комплексная задача обеспечения безопасного (обладающего свойствами конфиденциальности, целостности и доступности) информационного взаимодействия БВС с ограниченными ресурсами не имеет универсального решения. В связи с этим решение данной задачи имеет высокую актуальность и практическую значимость.

В работе рассмотрена группировка БВС, структура которой показана на рис. 2.

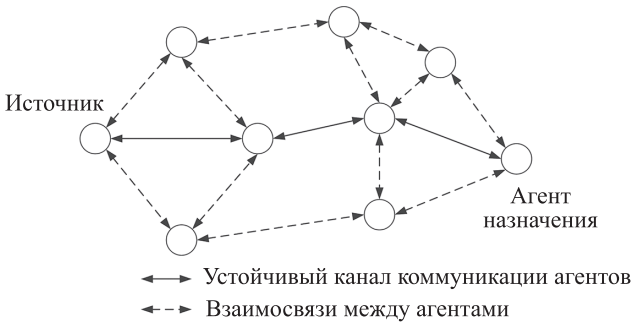

Рис. 2. Схема взаимодействия между агентами в группировке беспилотных воздушных судов

Fig. 2. Scheme of the interaction between agents in groups of unmanned aerial vehicles

[1] Современная классификация российских БЛА [Электронный ресурс]. URL: https://intuit.ru/studies/courses/622/478/lecture/21074?fbclid=IwAR0nhLAIGOIl2mTvKZHFGAgR6UR8OwM4mRHBE0eUZ3Re6KfZOt2jp1KA6eg, свободный (дата обращения: 03.11.2021).

[2] Сравнительные характеристики процессоров. НОУ «ИНТУИТ» [Электронный ресурс]. URL: https://intuit.ru/studies/courses/622/478/lecture/21074, свободный (дата обращения: 12.11.2021).

Современные модели и протоколы маршрутизации в самоорганизующихся сетях

В настоящие время протоколы маршрутизации в мобильных системах разрабатываются в условиях частных ограничений для адаптации к конкретным условиям. Концепция FANET является развитием сетей MANET (Mobile Ad hoc Network) и Vehicular Ad hoc Network (VANET). Известны исследования, применяющие протокол маршрутизации данных сетей в FANET. Реальные группировки БВС динамичны и работают в открытой среде под угрозой информационной безопасности, поэтому применимость известных протоколов ограничена.

Использование протокола OLRS (Optimized Link State Routing Protocol) [6] в FANET исследовано в работах [7, 8]. Протокол маршрутизации основан на диагностике состояния канала взаимодействия БВС с помощью периодического обмена пакетами приветствия. Промежуточные агенты пересылают сообщение от источника к месту назначения и всегда обновляют текущий статус доступа. Проблема этого протокола заключается в масштабируемости и нестабильности линии передачи, что приводит к снижению качества обслуживания.

Маршрутизация DSDV (Destination-Sequenced Distance Vector) [9] основана на алгоритме Беллмана–Форда с использованием двух индикаторов для предотвращения зацикливания и обновления локальной информации при изменении топологии, которая представляет собой порядковый номер и таблицу маршрутизации. Протокол используется в маршрутизации FANET [10, 11]. Таблицы маршрутизации периодически обновляются, а приоритет имеет путь с более высоким порядковым номером. Протокол не учитывает данные о контексте безопасности коммуницирующих агентов и, следовательно, об информационной безопасности канала взаимодействия.

AODV (Ad hoc On-demand Distance Vector) [12] реализует маршрутизацию шаг за шагом и полагается на свою таблицу маршрутизации на основе выполнения алгоритма вектора расстояния. Кратчайшие маршруты выбираются пакетами RREQ и RREP. Применение AODV для сетей FANET исследовано в [13, 14]. Недостаток этого протокола заключается в том, что процесс иерархического разбиения и наличие непрерывного служебного трафика снижает полезную пропускную способность сети.

В работе [15] предложен алгоритм нейронной сети для оптимизации маршрутизации FANET на основе Hopfield neural network (CHNN) и Discrete Hopfield neural network (DHNN). Алгоритм помог повысить стабильность канала и эффективность связи.

Важная часть маршрутизации — механизм управления соединениями, который устанавливает логические связи между агентами. Потенциально выгодная ситуация, когда каждый агент владеет топологией сети и таблицей маршрутизации. Ситуация становится неприменима при следующих условиях: ведение таблицы маршрутизации в проактивных протоколах (OLSR, DSDV и ряде других) несовместимо с динамичной сетью FANET, а в протоколах реактивной маршрутизации (AODV, DSR [16]) повторение таблицы маршрутизации для каждого запроса приводит к перегрузке.

Все вышеперечисленные протоколы имеют общий недостаток — отсутствие механизма учета состояния информационной безопасности агентов. Доказано [17], что они уязвимы для ряда атак, в том числе: черные и белые дыры, спуфинг, эгоистичность, червоточина.

Для обеспечения информационной безопасности в беспроводных сетях ряд протоколов маршрутизации основывается на криптографических преобразованиях [18, 19]. Тем не менее, ввиду вычислительной сложности и ограниченности ресурсов БВС, данные преобразования могут привести к неприемлемым накладным расходам и большой задержке трафика. А в условиях ограниченного времени взаимодействия агентов, связанных с их взаимным перемещением, становятся неприменимы для группировки БВС.

Алгоритмы AntHocNet и BeeAdHoc [20], специфичные для «роевой» модели взаимодействия агентов, были разработаны для решения проблемы маршрутизации в сети FANET. Алгоритмы основаны на аналогии поведения биологических объектов — пчел и муравьев. Результаты их работы демонстрируют бóльшую пропускную способность сети роя по сравнению с традиционными алгоритмами, но они подвержены угрозе потери доступности ввиду сложной процедуры многоэтапной проверки оптимальности маршрутов.

В работе [21] изучены протоколы маршрутизации на основе анализа запаса энергии в группировках БВС. Оптимальный путь основан на максимизации оставшейся энергии БВС на выбранном пути. Исследование показало уменьшение энергопотребления и повышение стабильности связи. Подобный подход — представитель класса *частных* решений и в данном случае направлен на поддержание максимальной работоспособности *группировки в целом* за счет противодействия неравномерному потреблению энергии БВС. Вместе с тем имеется вероятность возникновения угрозы информационной безопасности, относящейся к взаимодействию с *неаутентичным источником информации*, что может привести к «введению в заблуждение» одного или нескольких агентов и некорректному расчету запаса энергии.

Подход позиционной маршрутизации — мощное средство адаптации сети FANET. В [22] предложен протокол географической маршрутизации (GRAA), адаптирующийся к изменениям высоко динамичной топологии группировки БВС. Протокол основан на учете географического положения и мобильной информации агентов. Результаты исследования показали стабильность канала передачи, а также высокий коэффициент доставки пакетов из-за ограниченного отбрасывания пакетов. Теоретически задержка может увеличиться, так как один агент будет удерживать пакет и перемещаться, пока не встретит подходящего агента для дальнейшей пересылки данных. Уязвимости информационной безопасности этого протокола порождают проблемы доступности и целостности.

Выполненный обзор современных решений подтверждает тезис о разработке моделей и протоколов маршрутизации в системе частных ограничений, учиты-

вающих особенности реализации как самих мобильных агентов, так и моделей взаимодействия в группировке. Представленные решения не соответствуют требованиям к системам информационного взаимодействия группировки БВС *ограниченной производительности*, функционирующих в *роевой* модели в условиях существования внутренних (преднамеренных или непреднамеренных) *угроз информационной безопасности* в группе.

Модель маршрутизации каналов информационного взаимодействия в сети FANET с использованием аппарата нечеткой логики

Определим условия функционирования группировки БВС:

— БВС — элементарные агенты — считаются аутентифицированными для работы в составе исследуемой группировки в начальный момент времени;
— таблица маршрутизации нового агента не определена, заполняется по протоколу IPv4 по мере вхождения в зону информационного взаимодействия элементов группировки;
— для обмена информацией используется технологический стек интернет-протоколов.

Предложенная модель маршрутизации (рис. 3) использует метод нечеткой логики (блок «Расчет качества переходов») для *выбора доверенных агентов* с целью построения стабильного маршрута и минимизации вероятности передачи ошибок при обмене данными между агентом-источником и агентом-получателем.

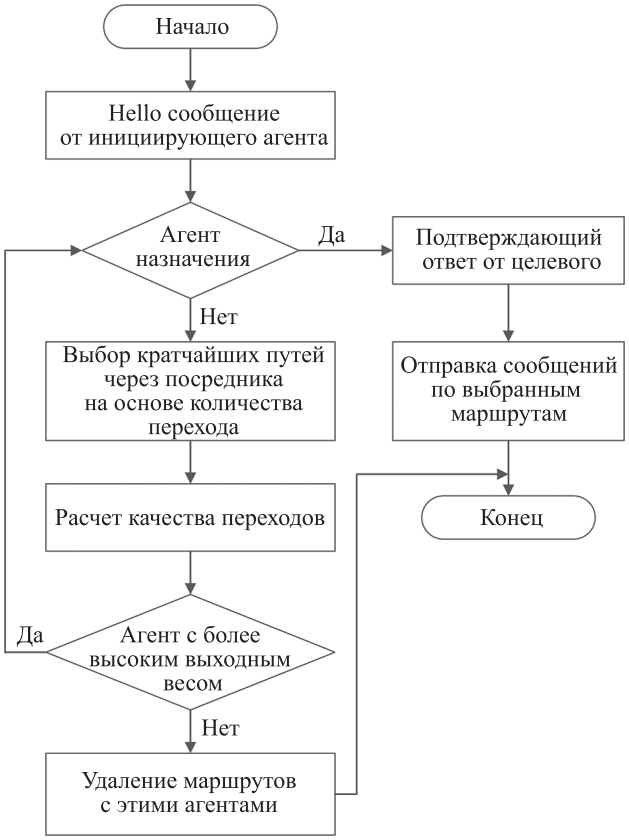

Рис. 3. Обобщенная схема маршрутизации с использованием аппарата нечеткой логики

Fig. 3. Generalized scheme routing based on fuzzy logic

Обобщенная схема (рис. 4) оценки качества канала информационного взаимодействия с использованием аппарата нечеткой логики направлена на применение концепции FANET в группировке БВС ограниченной производительности при функционировании в динамических средах. Отметим, что предлагаемый подход ориентирован не на оценку *канала передачи данных*, а на оценку *канала информационного взаимодействия*, так как учитывает и *безопасность агентов* — как промежуточных, так и конечных.

Предлагаемое решение по выбору маршрута информационного взаимодействия основано на анализе значений нескольких показателей агентов. К таким показателям относятся: скорость (Speed), уровень доверия (Trust) [23] и уровень мощности сигнала (RSSI). Степень принадлежности данных к оптимальному подмножеству задаются в интервале [0, 1].

RSSI — показатель, характеризующий состояние окружающей среды через мощность сигнала, измеренного при приеме пакета данных, полученного агентом. Значение RSSI рассчитывается с помощью регистра радио-приемопередатчика, входящего в подсистему связи агента. Чем выше значение RSSI, тем лучше качество связи. И наоборот, низкое значение данного показателя свидетельствует о значительном расстоянии между агентами или высокой помеховой обстановке. Значение RSSI агентов рассчитывается по формуле

$$RSSI_i = \frac{RSSI_{ij}}{n}, \quad (1)$$

где $RSSI_{ij}$ — мощность сигнала j-го агента, принимаемого i-м агентом, имеет вид

$$RSSI_{ij} = \mu - 10\zeta \log_{10} \sqrt{|x_a - x_b|^2 + |y_a - y_b|^2 + |z_a - z_b|^2}, \quad (2)$$

где ζ — показатель потери мощности сигнала на трассе (для воздуха $\zeta = 2$ и увеличивается при наличии препятствий); μ — уровень принимаемого сигнала на расстоянии 1 м; (x_a, y_a, z_a), (x_b, y_b, z_b) — координаты агентов; n — количество связей.

Значение скорости (Speed) определяется подсистемой навигации агента (инерционно, системой взаимного позиционирования, с помощью глобальной навигационной системы и др.). Вектор скорости существенно

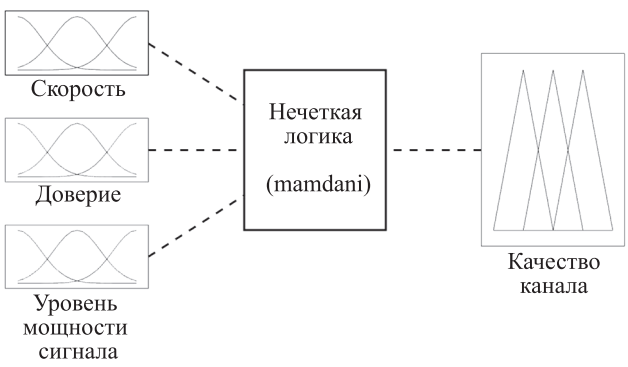

Рис. 4. Обобщенная схема оценки качества канала информационного взаимодействия мобильных агентов

Fig. 4. Generalized scheme for evaluating the quality of communication channel of mobile agents

Таблица 1. Диапазон значений показателей на входе системы маршрутизации
Table 1. Range of values of indicators at the input of the routing system

Показатель	Диапазон		
	Низкий	Средний	Высокий
Скорость, м/с	[0, 5]	[4, 14]	[> 13]
Доверие	[0, 0,4]	[0,35, 0,65]	[0,6, 1]
Уровень сигнала, дБ	[–125, –85]	[–90, –60]	[< –65]

влияет на топологию сети группировки, что отражается на качестве связи. Направление скорости в данной версии не учитывается, но можно предложить несколько способов, основанных как на знании взаимного расположения [22], так и на динамике RSSI. Модуль скорости имеет вид

$$v_i = \frac{\sqrt{|x_0 - x_1|^2 + |y_1 - y_0|^2 + |z_0 - z_1|^2}}{|t_1 - t_0|}, \quad (3)$$

где (x_0, y_0, z_0), (x_1, y_1, z_1) — координаты агентов; t_0, t_1— время нахождения агента в точках 0 и 1 соответственно.

Уровень доверия (Trust) показывает *ретроспективную оценку* безопасности [23] каждого из агентов во время взаимосвязи, полученную по результатам взаимного оценивания агентов в группе. Это означает, что по результатам взаимной оценки можно с большей достоверностью предположить, что агент аутентичен, работает правильно, не имеет аппаратных или программных сбоев или последствий сетевых атак. Значение доверия для i-го агента ($Trust_i$) рассчитывается по формуле

$$Trust_i = \frac{\sum_{j=0}^{n} rep_j^+}{\sum_{j=0}^{n} rep_j^+ + \sum_{j=0}^{n} rep_j^-}, \quad (4)$$

где i — оцениваемый агент; j — оценивающий агент в группе; rep_j^+ и rep_j^- — положительный и отрицательный уровни *репутации* агентов оцениваются соседними агентами в зоне взаимодействия (соответствие индексов «+» или «–», если j-й агент положительно или отрицательно оценил действия i-ого агента), рассчитываются по соотношению количества положительных и отрицательных «голосов» (v^+, v^-):

$$rep_j = \frac{v^+}{v^+ + v^-}. \quad (5)$$

По результатам экспериментов ([24] и в разделе «Исследование предложенной модели») входные значения анализируемых показателя разделены на три диапазона (табл. 1).

В табл. 1 и рис. 5 показаны функции и значения степеней принадлежности анализируемых показателей, которые заданы, исходя из предположения о равной значимости факторов, влияющих на процесс аутентификации. В зависимости от прикладного назначения и условий функционирования группировки БВС они могут пересматриваться для варьирования значимостью факторов и наиболее правильной настройки процедуры аутентификации.

Например, при использовании воздушных судов с увеличенной дальностью связи, снижается критичность высокой скорости их расхождения ввиду сохранения большего времени информационного взаимодействия. Исходя из этого, значения (низкого, среднего и высокого) качества показателей скорости могут быть увеличены.

Множество правил нечеткой системы приведено в табл. 2, где обозначен результат оценивания соответствующего показателя и его принадлежность к диапазо-

Таблица 2. Правила оценки качества канала информационного взаимодействия
Table 2. Rules for evaluating the quality of the communication channel

Правила оценки			
Speed	Trust	RSSI	K
Низкий	Низкий	Низкий	Плохо
		Средний	Плохо
		Высокий	Плохо
	Средний	Низкий	Плохо
		Средний	Нормально
		Высокий	Отлично
	Высокий	Низкий	Плохо
		Средний	Отлично
		Высокий	Отлично
Средний	Низкий	Низкий	Плохо
		Средний	Плохо
		Высокий	Плохо
	Средний	Низкий	Плохо
		Средний	Нормально
		Высокий	Отлично
	Высокий	Низкий	Плохо
		Средний	Отлично
		Высокий	Отлично
Высокий	Низкий	Низкий	Плохо
		Средний	Плохо
		Высокий	Плохо
	Средний	Низкий	Плохо
		Средний	Нормально
		Высокий	Нормально
	Высокий	Низкий	Плохо
		Средний	Нормально
		Высокий	Нормально

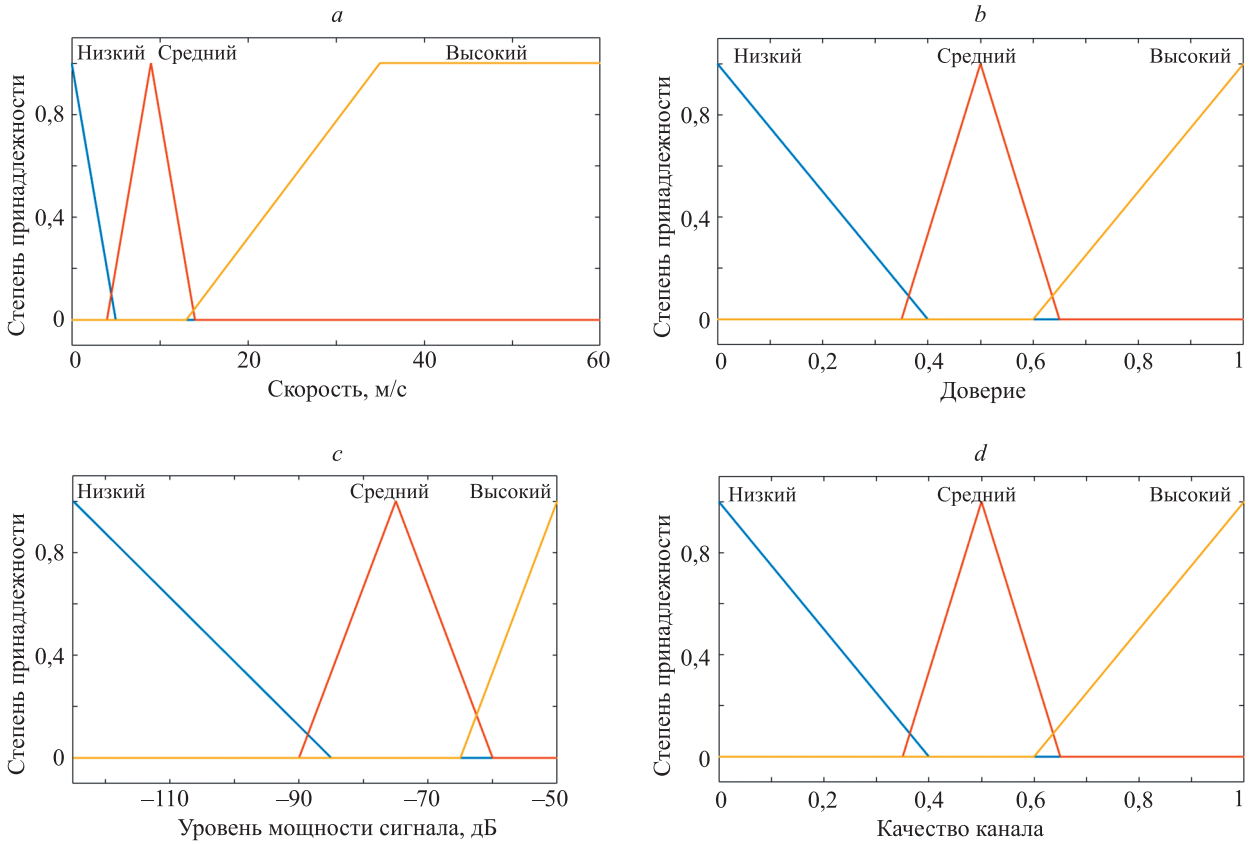

Рис. 5. Правила для оценивания: значений параметров скорости (*a*), доверия (*b*), уровня сигнала (*c*) и качества (К) канала информационного взаимодействия (*d*)

Fig. 5. The rules for evaluating the values: speed parameter (*a*), trust parameter (*b*), signal strength parameter (*c*), quality of the communication channel (*d*)

ну. Основываясь на правилах, можно получить оценку качества канала информационного взаимодействия (К) в сети FANET, наиболее подходящего для текущей конфигурации графа связности группировки, а также характеристик информационной безопасности агентов и помеховой обстановки.

В соответствии с результатами оценивания канала информационного взаимодействия будет выбрано наивысшее выходное значение из допустимых маршрутов, которые включены в таблицу маршрутизации агента.

На рис. 6 представлены трехмерные визуализации четырехмерного пространства примеров расчетов показателей качества потенциальных каналов информационного взаимодействия в зависимости от анализируемых параметров.

Поверхности цвета *1* ассоциированы с каналами, которые характеризуются агентами, имеющими «хорошие» параметры скорости, доверия и уровня мощности сигнала, что гарантирует поддержание стабильной коммуникации. По мере деградации одного или нескольких анализируемых параметров выделяются поверхности цветов *2*, *3* и *4*, характеризующие все меньшую вероятность успешной коммуникации. Поверхности цветов *5* и *6* характеризуют недопустимые направления информационного обмена, что определяется выходом за допустимые пределы одного или нескольких параметров.

Результаты моделирования (раздел «Исследование предложенной модели») позволяют сделать заключение, что в рамках приведенных алгоритмов расчетов (выражения (1)–(5) с *равновесными коэффициентами*) значение логического вывода выше или равное 0,5 характеризует устойчивую коммуникацию источника и получателя сообщения.

Результаты компьютерного эксперимента подтверждают интуитивное представление о том, что наилучшая коммуникация происходит в сценарии, когда взаимодействуют агенты с низкой относительной скоростью перемещения, высоким значением доверия и высокой мощностью сигнала.

При адаптации к конкретной аппаратной реализации, назначению и условиям функционирования группировки БВС могут быть изменены весовые коэффициенты значимости тех или иных параметров путем модификации табл. 1 и 2, а также вида функций принадлежности.

Исследование предложенной модели

Выполним компьютерное моделирование реализации протокола Fuzzy, базирующегося на рассматриваемой модели, для анализа продуктивности предложенных решений. В качестве инструментального средства использован симулятор с открытым исходным кодом

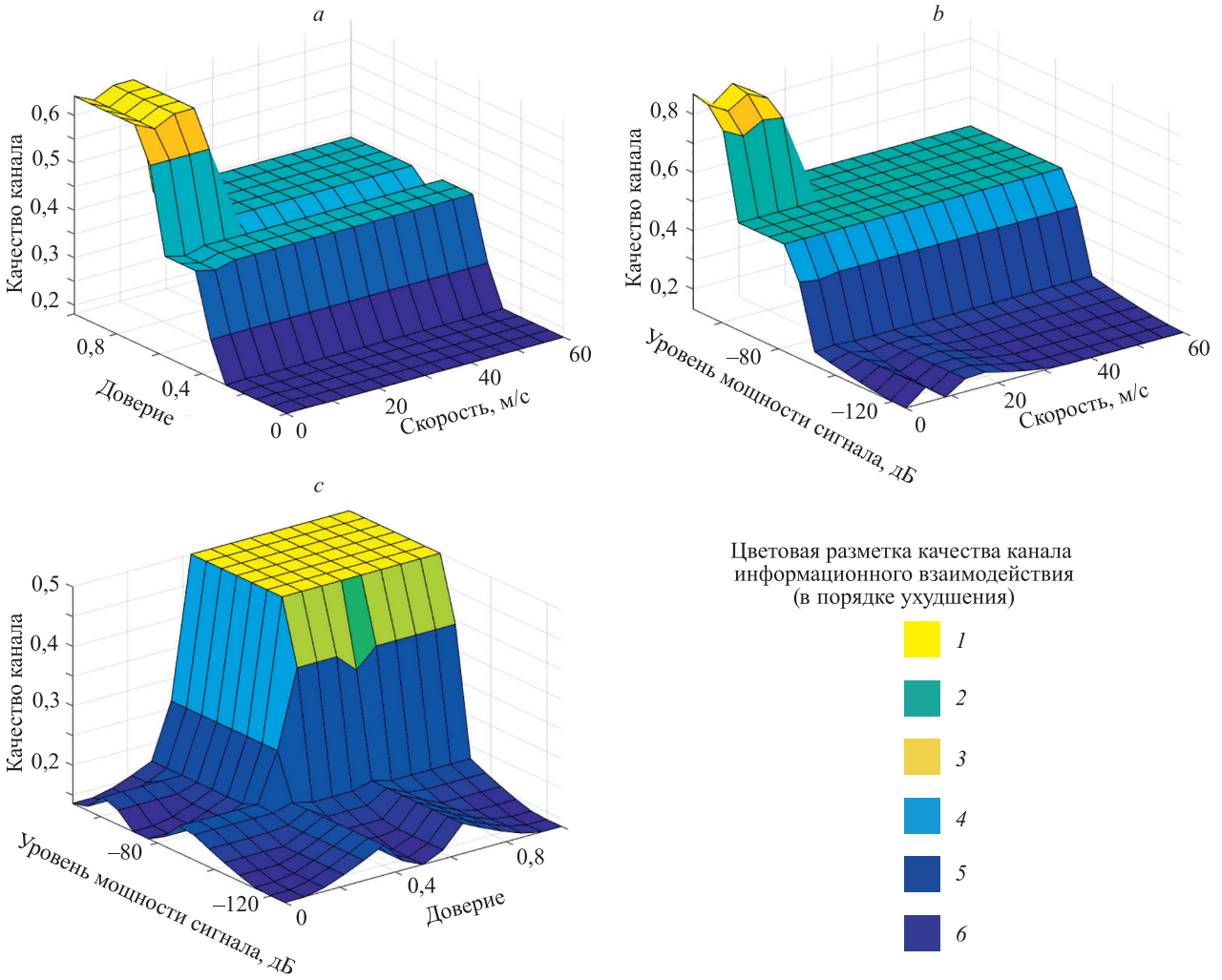

Рис. 6. Диаграммы альтернатив маршрутизации при изменении: доверия и скорости (*a*), скорости и уровня мощности сигнала (*b*); уровня мощности сигнала и доверия (*c*).
Цветовая разметка качества канала информационного взаимодействия

Fig. 6. Diagram of routing alternatives on change: Trust and Speed (*a*), Speed and RSSI (*b*), RSSI and Trust (*c*).
Channel quality color mark

NS3[1], направленный на моделирование дискретных событий, с объектно-ориентированной парадигмой и языком программирования C++. Параметры модели и инструментального стенда представлены в табл. 3.

Понятие комплексной эффективности протокола взаимодействия сложно, контекстно зависимо и в работе не затрагивается. По этой причине используем оценку качества протокола по трем параметрам: пропускная способность, коэффициент доставки пакетов (PDR) и средняя сквозная задержка.

Определение 1. Пропускная способность определяется как общее количество битов данных, переданных в канале связи за общее время моделирования.

Определение 2. Коэффициент доставки пакетов (PDR, Packet Delivery Ratio) определяется как отношение общего количества пакетов, полученных целевыми агентами, к общему количеству пакетов, переданных от исходных агентов.

Определение 3. Средняя сквозная задержка определяется как среднее время, необходимое для успешной доставки и передачи данных от исходного агента к месту назначения.

Эксперименты выполнены при нормальных условиях, когда в группировке отсутствует внутренний преднамеренный или случайный нарушитель, а также при наличии внутреннего нарушителя.

В результате эксперимента (рис. 7) видно, что протокол Fuzzy показывает стабильную пропускную способность в динамической среде, такой как группировка БВС, а у других протоколов маршрутизации пропускная способность значительно падает.

Протокол OLSR характеризуется низкой задержкой в динамических средах с различными размерами пакетов. Причем при наличии внутреннего нарушителя, коэффициент доставки пакетов для исследованных протоколов существенно снижается (на 25–35 %) из-за потери пакетов во время взаимосвязи с нарушителем.

[1] Network Simulator NS3 [Электронный ресурс]. URL: https://www.nsnam.org/, свободный (дата обращения: 24.09.2021).

Таблица 3. Параметры модели и инструментального стенда
Table 3. Parameters of the model and the tool stand

Группа параметров	Параметры	Значение
Инструментальное средство	Операционная система	Ubuntu v.14.4.
	Среда моделирования	NS3 (v.3.25)
Модель связи	Тип антенны	Omni
	Тип канала	Беспроводной
	Протокол уровня MAC	IEEE 802.11 b
	Тип трафика	CBR (трафик с постоянной битовой скоростью)
	Размер пакета, Б	512
Характеристики группировки	Количество агентов, шт.	30
	Внутренний нарушитель, шт.	1
	Скорость агентов, м/с	20
	Радиус взаимодействия, м	250
	Модель мобильности	Random Waypoint
Исследуемые протоколы	Протоколы	AODV, OLSR, Fuzzy

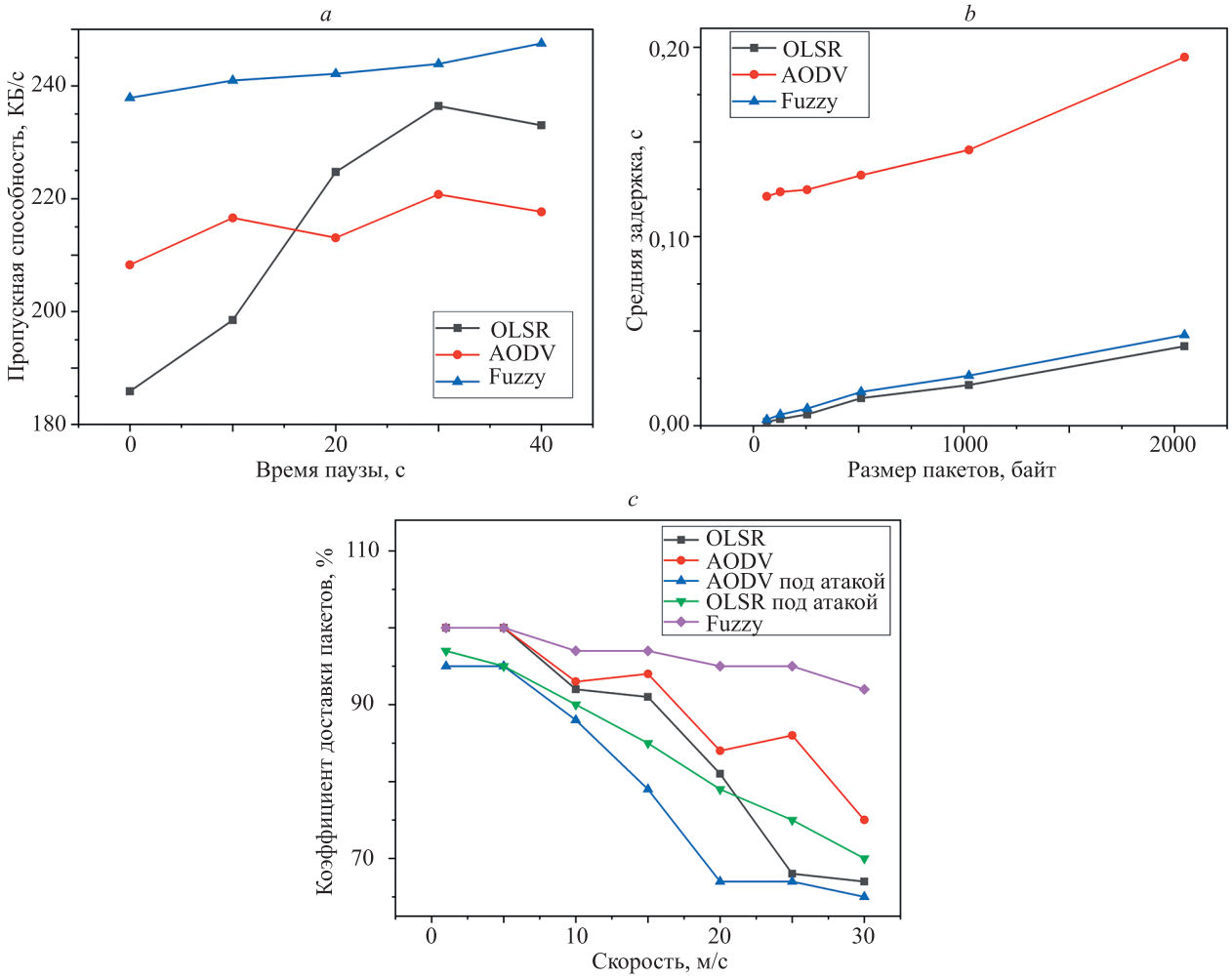

Рис. 7. Пропускная способность (*a*) и средняя задержка (*b*) в нормальных условиях; коэффициент доставки пакетов при наличии внутреннего нарушители (*c*)
Fig. 7. Throughput (*a*) and End-to-end delay (*b*) under normal conditions, Packet Delivery Ratio with insider attack (*c*)

В то время как коэффициент доставки пакетов протокола Fuzzy снижается не более, чем на 7 % из-за учета параметра $Trust_i$, рассчитываемого по формуле (4).

Отметим, что протокол Fuzzy имеет низкую ресурсоемкость, что обеспечивает его применимость в группировках БВС ограниченной производительности.

Заключение

В работе предложена модель маршрутизации каналов информационного взаимодействия в сети FANET с использованием аппарата нечеткой логики и учетом контекста информационной безопасности коммуницирующих агентов ограниченной производительности.

Приведены результаты компьютерного моделирования протокола Fuzzy, базирующегося на представленной модели, в сравнении с протоколами маршрутизации AODV и OLSR. Результаты компьютерного моделирования демонстрируют преимущество предлагаемого протокола по пропускной способности и коэффициенту доставки пакетов. Средняя сквозная задержка прокола Fuzzy превышает значения протокола OLSR на величину до 12 %, но она в 4–12 раз ниже, чем у протокола AODV.

Наибольшее преимущество протокол Fuzzy демонстрирует в условиях наличия в группировке внутреннего нарушителя (злоумышленника).

Предложенные модель и протокол могут применяться как дополнительное средство при решении задач обеспечения информационной безопасности каналов информационного взаимодействия в группировках беспилотных воздушных судов ограниченной производительности.

Литература

1. Bujari A., Palazzi C.E., Ronzani D. FANET application scenarios and mobility models // Proc. of the 3rd Workshop on Micro Aerial Vehicle Networks, Systems, and Applications (DroNet 2017). 2017. P. 43–46. https://doi.org/10.1145/3086439.3086440
2. Леонов А.В., Чаплышкин В.А. Сети FANET // Омский научный вестник. 2015. № 3(143). С. 297–301.
3. Матвеев В.А., Бельфер Р.А., Глинская Е.В. Угрозы и методы защиты в сборных сенсорных узлах летающих сенсорных сетей // Вопросы кибербезопасности. 2015. № 5(13). С. 26–31.
4. Комаров И.И., Юрьева Р.А., Дранник А.Л., Масленников О.С. Постановка задачи обеспечения информационной безопасности роевых робототехнических систем // Наука и бизнес: пути развития. 2015. № 3. С. 66–72.
5. Илюхин С.Н., Клишин А.Н. Оценка производительности бортового вычислителя беспилотного летательного аппарата при реализации процесса наведения // Инженерный журнал: наука и инновации. 2018. № 7. С. 6. https://doi.org/10.18698/2308-6033-2018-7-1781
6. Clausen T., Jacquet P., Adjih C., Laouiti A., Minet P., Muhlethaler P., Qayyum A., Viennot L. Optimized Link State Routing Protocol (OLSR). 2003. ffinria-00471712f.
7. Singh K., Verma A.K. Applying OLSR routing in FANETs // Proc. of the 2014 IEEE International Conference on Advanced Communication, Control and Computing Technologies (ICACCCT). 2014. P. 1212–1215. https://doi.org/10.1109/ICACCCT.2014.7019290
8. Rosati S., Krużelecki K., Heitz G., Floreano D., Rimoldi B. Dynamic routing for flying ad hoc networks // IEEE Transactions on Vehicular Technology. 2016. V. 65. N 3. P. 1690–1700. https://doi.org/10.1109/TVT.2015.2414819
9. Perkins C.E., Bhagwat P. Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers // ACM SIGCOMM Computer Communication Review. 1994. V. 24. N 4. P. 234–244. https://doi.org/10.1145/190809.190336
10. Mariyappan K., Christo M.S., Khilar R. Implementation of FANET energy efficient AODV routing protocols for flying ad hoc networks [FEEAODV] // Materials Today: Proceedings. 2021. in press. https://doi.org/10.1016/j.matpr.2021.02.673
11. Anitha C., Asvini K.G. Performance of routing protocols and file transfer in fanet using shortes path algorithm // Science, Technology and Development. 2020. V. 9. N 2. P. 77–87.
12. Perkins C., Belding-Royer E., Das S. Ad Hoc On-Demand Distance Vector (AODV) Routing: document RFC 3561. 2003.
13. Leonov V., Litvinov G.A. Applying AODV and OLSR routing protocols to air-to-air scenario in flying ad hoc networks formed by mini-UAVs // 2018 Systems of Signals Generating and Processing in the Field of on Board Communications. 2018. P. 1–10. https://doi.org/10.1109/SOSG.2018.8350612
14. Garcia-Santiago A., Castaneda-Camacho J., Guerrero-Castellanos J.F., Mino-Aguilar G. Evaluation of AODV and DSDV routing protocols

References

1. Bujari A., Palazzi C.E., Ronzani D. FANET application scenarios and mobility models. *Proc. of the 3rd Workshop on Micro Aerial Vehicle Networks, Systems, and Applications (DroNet 2017)*, 2017, pp. 43–46. https://doi.org/10.1145/3086439.3086440
2. Leonov A.V., Chaplyshkin V.A. Flying Ad Hoc networks (FANETS). *Omsk Scietntific Bulletin*, 2015, no. 3(143), pp. 297–301. (in Russian)
3. Matveev V., Belfer R., Glinskaya E. Threats and protection methods in sink sensor nodes flying sensor networks. *Voprosy kiberbezopasnosti*, 2015, no. 5(13), pp. 26–31. (in Russian)
4. Komarov I.I., Yuryeva R.A., Drannik A.L., Maslennikov O.S. Statement of the problem of ensuring information security of swarm robotic systems. *Science and Business: Development Ways*, 2015, no. 3, pp. 66–72. (in Russian)
5. Ilukhin S.N., Klishin A.N. On-board computer efficiency evaluation of unmanned aerial vehicles (UAV) when implementing the targeting process. *Engineering Journal: Science and Innovation*, 2018, no. 7, pp. 6. (in Russian). https://doi.org/10.18698/2308-6033-2018-7-1781
6. Clausen T., Jacquet P., Adjih C., Laouiti A., Minet P., Muhlethaler P., Qayyum A., Viennot L. *Optimized Link State Routing Protocol (OLSR)*. 2003, ffinria-00471712f.
7. Singh K., Verma A.K. Applying OLSR routing in FANETs. *Proc. of the 2014 IEEE International Conference on Advanced Communication, Control and Computing Technologies (ICACCCT)*, 2014, pp. 1212–1215. https://doi.org/10.1109/ICACCCT.2014.7019290
8. Rosati S., Krużelecki K., Heitz G., Floreano D., Rimoldi B. Dynamic routing for flying ad hoc networks. *IEEE Transactions on Vehicular Technology*, 2016, vol. 65, no. 3, pp. 1690–1700. https://doi.org/10.1109/TVT.2015.2414819
9. Perkins C.E., Bhagwat P. Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. *ACM SIGCOMM Computer Communication Review*, 1994, vol. 24, no. 4, pp. 234–244. https://doi.org/10.1145/190809.190336
10. Mariyappan K., Christo M.S., Khilar R. Implementation of FANET energy efficient AODV routing protocols for flying ad hoc networks [FEEAODV]. *Materials Today: Proceedings*, 2021, in press. https://doi.org/10.1016/j.matpr.2021.02.673
11. Anitha C., Asvini K.G. Performance of routing protocols and file transfer in fanet using shortes path algorithm. *Science, Technology and Development*, 2020, vol. 9, no. 2, pp. 77–87.
12. Perkins C., Belding-Royer E., Das S. *Ad Hoc On-Demand Distance Vector (AODV) Routing*. Document RFC 3561. 2003.
13. Leonov V., Litvinov G.A. Applying AODV and OLSR routing protocols to air-to-air scenario in flying ad hoc networks formed by mini-UAVs. *2018 Systems of Signals Generating and Processing in the Field of on Board Communications*, 2018, pp. 1–10. https://doi.org/10.1109/SOSG.2018.8350612
14. Garcia-Santiago A., Castaneda-Camacho J., Guerrero-Castellanos J.F., Mino-Aguilar G. Evaluation of AODV and DSDV routing protocols

for a FANET: Further results towards robotic vehicle networks // Proc. of the 9th IEEE Latin American Symposium on Circuits & Systems (LASCAS). 2018. P. 1–4. https://doi.org/10.1109/LASCAS.2018.8399972
15. Yang H., Liu Z. An optimization routing protocol for FANETs // EURASIP Journal on Wireless Communications and Networking. 2019. N 1. P. 120. https://doi.org/10.1186/s13638-019-1442-0
16. Johnson D., Hu Y., Maltz D. The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4: document RFC 4728. February 2007. 107 p. https://doi.org/10.17487/RFC4728
17. Афанасьев А.Л., Гармонов А.В., Кащенко Г.А. Анализ угроз безопасности и протоколов безопасной маршрутизации в сетях MANET // Радиолокация, навигация и связь: XX Международная научно-техническая конференция, Воронеж, 15–17 апреля 2014 года. Воронеж: НПФ «САКВОЕЕ» ООО, 2014. С. 846–857.
18. Yi S., Naldurg P., Kravets R. A Security-aware routing protocol for wireless ad hoc networks // ACM Symp. on Mobile Ad Hoc Networking and Computing, 2001.
19. Maxa J.-A., Ben Mahmoud M.S., Larrieu N. Secure routing protocol design for UAV Ad hoc NETworks // Proc. of the 34th Digital Avionics Systems Conference (DASC). 2015. P. 4A5-1–4A5-15. https://doi.org/10.1109/DASC.2015.7311415
20. Leonov A.V. Modeling of bio-inspired algorithms AntHocNet and BeeAdHoc for Flying Ad Hoc Networks (FANETs) // Proc. of the 13th International Scientific-Technical Conference on Actual Problems of Electronic Instrument Engineering (APEIE). V. 2. 2016. P. 90–99. https://doi.org/10.1109/APEIE.2016.7806419
21. Mukherjee A., Misra S., Pradeep Chandra V.S., Raghuwanshi N.S. ECoR: energy-aware collaborative routing for task offload in sustainable UAV swarms // IEEE Transactions on Sustainable Computing. 2020. V. 5. N 4. P. 514–525. https://doi.org/10.1109/TSUSC.2020.2976453
22. Hyeon S.U., Kim K.-I., Yang S.W. A new geographic routing protocol for aircraft ad hoc networks // Proc. of the 29th Digital Avionics Systems Conference: Improving Our Environment through Green Avionics and ATM Solutions (DASC). 2010. P. 2.E.21–2.E.28. https://doi.org/10.1109/DASC.2010.5655476
23. 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.
24. Матвеева А.А., Ким Ю.В., Викснин И.И. Методы обеспечения информационной безопасности коммуникационных каналов в мультиагентных робототехнических системах // Научно-технический вестник информационных технологий, механики и оптики. 2019. Т. 19. № 1. С. 102–108. https://doi.org/10.17586/2226-1494-2019-19-1-102-108

for a FANET: Further results towards robotic vehicle networks. *Proc. of the 9th IEEE Latin American Symposium on Circuits and Systems (LASCAS)*, 2018, pp. 1–4. https://doi.org/10.1109/LASCAS.2018.8399972
15. Yang H., Liu Z. An optimization routing protocol for FANETs. *EURASIP Journal on Wireless Communications and Networking*, 2019, no. 1, pp. 120. https://doi.org/10.1186/s13638-019-1442-0
16. Johnson D., Hu Y., Maltz D. *The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4*. Document RFC 4728, February 2007, 107 p. https://doi.org/10.17487/RFC4728
17. Afanasiev A.L., Garmonov A.V., Kashchenko G.A. Security threat anatisis and securiry routing protocols of MANET. *Proc. of the XX International Scientific and Technical Conference «Radiolocation, Navigation, Communication» (RLNC 2014)*, Voronezh, 2014, pp. 846–857. (in Russian)
18. Yi S., Naldurg P., Kravets R. Security-aware ad hoc routing for wireless networks. *Proc. of the ACM Symposium on Mobile Ad Hoc Networking and Computing*, 2001.
19. Maxa J.-A., Ben Mahmoud M.S., Larrieu N. Secure routing protocol design for UAV Ad hoc NETworks. *Proc. of the 34th Digital Avionics Systems Conference (DASC)*, 2015, pp. 4A5-1–4A5-15. https://doi.org/10.1109/DASC.2015.7311415
20. Leonov A.V. Modeling of bio-inspired algorithms AntHocNet and BeeAdHoc for Flying Ad Hoc Networks (FANETs). *Proc. of the 13th International Scientific-Technical Conference on Actual Problems of Electronic Instrument Engineering (APEIE)*. V. 2. 2016, pp. 90–99. https://doi.org/10.1109/APEIE.2016.7806419
21. Mukherjee A., Misra S., Pradeep Chandra V.S., Raghuwanshi N.S. ECoR: energy-aware collaborative routing for task offload in sustainable UAV swarms. *IEEE Transactions on Sustainable Computing*, 2020, vol. 5, no. 4, pp. 514–525. https://doi.org/10.1109/TSUSC.2020.2976453
22. Hyeon S.U., Kim K.-I., Yang S.W. A new geographic routing protocol for aircraft ad hoc networks. *Proc. of the 29th Digital Avionics Systems Conference: Improving Our Environment through Green Avionics and ATM Solutions (DASC)*, 2010, pp. 2.E.21–2.E.28. https://doi.org/10.1109/DASC.2010.5655476
23. 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(91), pp. 30–38. (in Russian)
24. Matveeva A.A., Kim I.V., Viksnin I. Information security methods for communication channels in multiagent robotic systems. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2019, vol. 19, no. 1, pp. 102–108. (in Russian). https://doi.org/10.17586/2226-1494-2019-19-1-102-108

Авторы

Чан Хань Зуи — аспирант, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, SC 57221643170, https://orcid.org/0000-0002-4891-8924, viewtheworld93@gmail.com
Комаров Игорь Иванович — кандидат физико-математических наук, доцент, доцент, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, SC 57194932349, https://orcid.org/0000-0002-6542-4950, iik_st@mail.ru
Ву Хань Лам — аспирант, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, https://orcid.org/0000-0003-3902-3413, vulamkhanh@gmail.com
Лэ Хиеу Ван — аспирант, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, https://orcid.org/0000-0002-9413-5138, dragon220294@gmail.com

Authors

Duj Khanh Tran — Postgraduate, ITMO University, Saint Petersburg, 197101, Russian Federation, SC 57221643170, https://orcid.org/0000-0002-4891-8924, viewtheworld93@gmail.com
Igor I. Komarov — PhD, Associate Professor, Associate Professor, ITMO University, Saint Petersburg, 197101, Russian Federation, SC 57194932349, https://orcid.org/0000-0002-6542-4950, iik_st@mail.ru

Lam Khanh Vu — Postgraduate, ITMO University, Saint Petersburg, 197101, Russian Federation, https://orcid.org/0000-0003-3902-3413, vulamkhanh@gmail.com
Van Hieu Le — Postgraduate, ITMO University, Saint Petersburg, 197101, Russian Federation, https://orcid.org/0000-0002-9413-5138, dragon220294@gmail.com

Статья поступила в редакцию 08.07.2021
Одобрена после рецензирования 08.11.2021
Принята к печати 30.11.2021

Received 08.07.2021
Approved after reviewing 08.11.2021
Accepted 30.11.2021