Научная статья
УДК 004.056
https://doi.org/10.31854/1813-324X-2024-10-3-75-86

Алгоритм защиты роевых робототехнических систем от атак вредоносных роботов с координированной стратегией поведения

Игорь Алексеевич Зикратов[1], zikratov.ia@sut.ru
Татьяна Викторовна Зикратова[2], ztv64@mail.ru
Егор Анатольевич Новиков[1] ✉, novikov.ea@sut.ru

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, Санкт-Петербург, 193232, Российская Федерация
[2]Военно-морской политехнический институт ВУНЦ ВМФ «Военно-морская академия имени Адмирала Флота Советского Союза Н.Г. Кузнецова»
Санкт-Петербург, г. Пушкин, 196602, Российская Федерация

Аннотация

Актуальность: *Атаки вредоносных роботов относятся к так называемым «мягким» атакам, использующим перехват сообщений, формирование и передачу членам роя дезинформации, а также осуществляющих иные действия, которые не имеют идентифицируемых признаков вторжения роботов-диверсантов, и приводят к принятию ошибочного, или не являющегося оптимальным консолидированного решения группой роботов. Известные методы выявления и противодействия скоординированным деструктивным информационным воздействиям в роях роботов показывают свою эффективность при концентрации вредоносных элементов в рое не более 45 %. Данная статья посвящена описанию алгоритма, который позволит расширить возможности роя противодействовать «мягким» атакам.*
Постановка задачи: *построение механизмов защиты мобильных мультиагентных робототехнических систем от атак со стороны вредоносных роботов с координированной стратегией поведения.* ***Цель работы:*** *повышение вероятности противодействия атакам вредоносных роботов с координированной стратегией поведения на самоорганизующиеся мультиагентные робототехнические системы.* ***Используемые методы:*** *предлагаемый алгоритм является развитием механизма самоорганизации роя роботов на основе метрик доверия и репутации для решения задачи выявления и устранения влияния вредоносных роботов. Корректность предлагаемых решений подтверждалась имитационным моделированием типовой задачи коллективного восприятия заданного полигона.* ***Новизна****: алгоритм основан на квантификации процесса достижения консенсуса членами гомогенной группы (роя) на последовательные такты (периоды), с последующей внутри- и межпериодной обработкой информации, продуцируемой роботами роя и вредоносными роботами в процессе информационного взаимодействия.* ***Результат:*** *эксперимент показал способность самоорганизующегося роя противодействовать координированной атаке вредоносных роботов при превышении их концентрации 51 % с вероятностью, близкой к 1.* ***Практическая значимость:*** *разработанный алгоритм может быть использован при построении систем защиты мультиагентных робототехнических систем от атак вредоносных роботов, осуществляемых в процессе информационного взаимодействия при решении роем поставленной задачи. Алгоритм позволяет успешно отражать скоординированные атаки типа атака «51 процент».*

Ключевые слова: *групповая робототехника, коллектив роботов, роевый интеллект, мультиагентные робототехнические системы, атака «51 процент»*

Ссылка для цитирования: Зикратов И.А., Зикратова Т.В., Новиков Е.А. Алгоритм защиты роевых робототехнических систем от атак вредоносных роботов с координированной стратегией поведения // Труды учебных заведений связи. 2024. Т. 10. № 3. С. 75–86. DOI:10.31854/1813-324X-2024-10-3-75-86. EDN:XUDVOR

Original research
https://doi.org/10.31854/1813-324X-2024-10-3-75-86

Swarm Robotics System Algorithm for Defense Against Coordinated Behavior Strategy Attacks

Igor A. Zikratov[1], zikratov.ia@sut.ru
Tatyana V. Zikratova[2], ztv64@mail.ru
Egor A. Novikov[1] ✉, novikov.ea@sut.ru

[1]The Bonch-Bruevich Saint Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation
[2]Naval polytechnic institute of Navy Development of the Military Research and Educational Center of the Navy
"Naval Academy named after Admiral of the Fleet of the Soviet Union N.G. Kuznetsov"
St. Petersburg, Pushkin, 196602, Russian Federation

Annotation

Problem statement: *designing the defense mechanism against coordinated behavior strategy attacks for mobile multiagent robotic systems. Possible attacks of that kind may be carried out by use message interception, creating and transmitting disinformation, and other actions, that does not have identifiable characteristics of saboteur intrusion, and lead to making incorrect or non-optimal decision by group of robots.* ***The purpose of the work:*** *the increase of probability of detection coordinated behavior strategy attacks on mobile multiagent robotic systems.* ***Methods used:*** *proposed algorithm is further development of self organization mechanism, using trust and reputation metrics for detection and counteraction against malicious robots. Accuracy of proposed method is confirmed using imitation model of collective exploration task.* ***The novelty:*** *algorithm is based on quantification of consensus achievement process into consecutive time periods, which is followed by inter- and intraperiod processing of information, produces by robots of the swarm and by malicious robots during communication.* ***The result:*** *experiment shows that the swarm is capable to counteract against coordinated attack of malicious robots, when concentration of malicious units is more than 51 %. The probability of such counteraction is close to 1. Known detection and counteraction methods for destructive informational influence in homogeneous swarms of robots prove to be effective in cases, when concentration of malicious units is less than 45 %.* ***Practical significance:*** *developed algorithm may be used for multiagent robotic systems security system design to protect against attack, executed during interactions between agents of the swarm. Algorithm allows to successfully counteract coordinated attacks similar to «51 percent attack».*

Keywords: *group robotics, robot collective, swarm intelligence, multiagent robotics system, 51 percent attack*

For citation: Zikratov I.A., Zikratova T.V., Novikov E.A. Swarm Robotics System Algorithm for Defense Against Coordinated Behavior Strategy Attacks. *Proceedings of Telecommunication Universities.* 2024;10(3):75–86. (in Russ.) DOI:10.31854/1813-324X-2024-10-3-75-86. EDN:XUDVOR

Введение

Стремительное развитие групповой робототехники, которое находит отражение в совершенствование теории и практики построения интеллектуальных систем управления роботами, обусловлено очевидными преимуществами таких систем. Групповая робототехника реализует парадигму «умной пыли» (*от англ.* Smartdust) [1], когда группы или рои роботов (*от англ.* Swarm Robotics) состоят из самоорганизующихся агентов, обменивающихся сигналами по беспроводным локальным каналам связи, и работают как единая система. Применение самоорганизующихся групп (или роев – *далее эти понятия используются контекстно как синонимы*) относительно простых и дешевых роботов в ряде ситуаций приводит к уменьшению размерности решаемых вычислительных задач, увеличению радиуса действия за счет рассредоточения отдельных роботов (агентов) по всей рабочей зоне, более высокой вероятности выполнения задания, обусловленной возможностью перераспределения целей (задач) между роботами группы в случае выхода из строя части из них.

Вместе с тем применение самоорганизующихся групп мобильных роботов сопровождается воздействием следующих факторов:

– фрагментарность, а порой и противоречивость знаний агентов о состоянии внешней среды и других участников;

– стохастическая природа параметров внешней среды;

– разнообразие вариантов распределения ролей агентов в коллективе и способов достижения цели, стоящей перед роем;

– отсутствие или неустойчивость единого канала связи между центром управления и роем;

– сложность обеспечения устойчивой коммуникации между агентами роя ввиду распределенной группировки в пространстве и во времени.

Очевидно, что перечисленные факторы можно расценивать как системные уязвимости, позволяющие третьим лицам осуществлять сознательное противодействие рою в процессе выполнения ими задачи путем физического внедрения в рой вредоносных роботов (ВР) [2]. Это обстоятельство приводит к необходимости совершенствования механизмов обеспечения информационной безопасности самоорганизующихся мультиагентных робототехнических систем.

В данной работе рассмотрены механизмы защиты роев от так называемых «мягких» атак ВР. Суть этих атак заключается в предоставлении по штатным каналам связи и протоколам, внедренными в рой ВР, недостоверной информации о своем состоянии и состоянии окружающей среды. На основе этой недостоверной информации роем может быть принято ошибочное решение, которое часто связано с выбором из некоторого числа N доступных альтернатив A_i, ($i = 1, 2, \dots, N$), или приведет к выбору способа достижения цели, отличного от оптимального. Опасность «мягких» атак на рой состоит в том, что факт проведения атаки в процессе выполнения задачи выявить затруднительно, так как роботы, их системы и каналы связи функционируют в штатном режиме, однако вероятность выбора консенсусом роботов искомой альтернативы A_{opt} снижается до неприемлемого уровня.

Угрозы безопасности гомогенных телекоммуникационных сетей и групп роботов с децентрализованным управлением от воздействия ВР обсуждались в работах [3–6]. Предлагались методы защиты, основанные на введении метрик доверия и репутации агентов [7–11] на основе технологий распределенного реестра [12, 13] путем вычисления степени уверенности [14], и другие подходы [15, 16].

При этом в литературе выделяют три типа стратегий ВР при осуществлении «мягких» атак:

1) случайная стратегия поведения (ССП);

2) оппозиционная стратегия поведения (ОСП);

3) координированная стратегия поведения (КСП).

Формальное описание этих стратегий подробно приведено в работе [14]. Суть ССП состоит в том, что каждый ВР на каждой итерации процедуры достижения консенсуса предлагает альтернативу A_i из множества доступных, выбранную случайным образом. ВР с ОСП предлагает любую A_i, но которая никогда не совпадает с A_{opt}. Главное отличие КСП от других стратегий ВР заключается в том, что все ВР с КСП изначально имеют глобальную предустановку, и выбор на каждой итерации процесса достижения консенсуса происходит в пользу некой альтернативы A^* всеми ВР с КСП [14]. Здесь:

$$A^* \in \{A_1, A_2, \dots, A_L\}, \ A_{opt} \in \{A_1, A_2, \dots, A_L\}, \ A^* \neq A_{opt}.$$

Указанные выше методы защиты децентрализованных самоорганизующихся групп обеспечивают эффективную защиту от ВР с ССП и ОСП. Однако эффективность защиты резко снижается в случае использования ВР с КСП при концентрации диверсантов в рое более 50 %. Это обусловлено тем, что гомогенные рои с децентрализованным управлением принимают решение о выборе альтернативы A_i путем достижения консенсуса независимых агентов, поэтому для принятия деструктивного решения, основанного на выборе альтернативы A^*, лоббируемой группой ВР, достаточно обеспечить 51 % голосов участников голосования. Подобные атаки в среде распределенных реестров, осуществляемые хакерскими группировками для захвата контроля над криптовалютами, получили название атаки «51 процент».

Целью настоящей работы является повышение степени защищенности самоорганизующихся групп роботов от атак ВР с КСП.

Проблемный сценарий коллективного принятия решения

Для того, чтобы быть эффективными, стратегии коллективного принятия решений должны быть не только быстрыми и точными, но и достаточно общими, чтобы их можно было адаптировать и повторно использовать в различных проблемных областях. В работе [17] предложен новый проблемный сценарий – коллективное восприятие, суть которого состоит в том, что роботы должны исследовать окружающую среду, оценить частоту определенных функций и коллективно определить, какая функция встречается чаще всего.

В работе [14] реализован такой сценарий коллективного восприятия в роевой робототехнической системе и проведены эксперименты с ВР со всеми рассмотренными стратегиями. В качестве

полигона использована модель внешней среды в виде сцены, раскрашенной плитками пяти цветов. На сцене инициируются роботы со случайными начальными координатами и случайными маршрутами движения. Передвигаясь по сцене, роботы выбирают для каждой клетки одну из пяти альтернатив – цвет, в который окрашена текущая клетка. Цель роя – на основе консенсуса определить, клетки какого именно цвета преобладают на сцене. Очевидно, что сложность задачи можно варьировать, изменяя соотношение между процентами плиток преобладающего цвета и других цветов. Используемая в данной статье модель сценария коллективного восприятия альтернативы также содержит сцену из клеток разных цветов (рисунок 1).

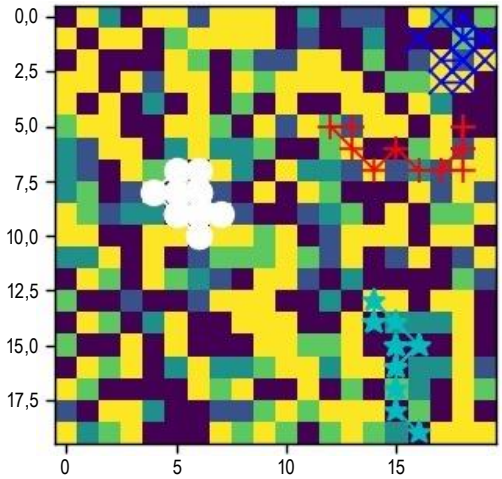

Рис. 1. Пример сцены, состоящей из 400 клеток с пятью альтернативами и маршрутами 4 роботов; 40 % клеток окрашены в желтый цвет

Fig. 1. Example of a Scene, Which Consists of 400 Cells, Each with 5 Alternative and Routes of 4 Robots; 40% of Cells are Colored Yellow

Считывание альтернатив каждым отдельно взятым роботом происходит при последовательном перемещении из расчета того, что в течение всего процесса достижения консенсуса робот подсчитывает частоту всех альтернатив на сцене (рисунок 2, блоки синим цветом). После запуска итерационного цикла j-й робот последовательно обходит клетки сцены: $r_j \in R$, где R – множество роботов группы. При достижении количества итераций j-го робота $k_{r_j}^{\text{ит}}$ заданного числа Kr_j вырабатывает решение в отношении альтернативы A_{ij}. Вероятность события $P(A_{ij} = A_{opt})$ зависит от количества клеток разного цвета, встретившихся роботу на пути.

Коллективное решение задачи предполагает обмен альтернативами в процессе обследования сцены [18]. В этом случае алгоритм действий робота будет иметь вид, также представленный на рисунке 2 (блоки синим + красным цветом. На каждой итерации j-й робот получает статус активного агента, перемещается на k-ю соседнюю свободную клетку, оценивает ее свойства (цвет) посредством своих сенсоров, и выбирает для текущей клетки соответствующую альтернативу A_{ij}^k. О принятом решении он сообщает по сети связи членам коллектива, находящимся в пассивной фазе итерационного цикла: $r \in R$. В зависимости от расстояния до активного агента и внешних условий члены коллектива могут либо принять информацию от j-го робота, либо не «услышать» ее в случае неустойчивой радиосвязи. Т. е. роботы, которые приняли информацию, записывают альтернативу A_{ij}^k в соответствующую хэш-таблицу. Для каждого члена коллектива каждый агент имеет отдельную хэш-таблицу. Статус активного агента поочередно получают все роботы группы.

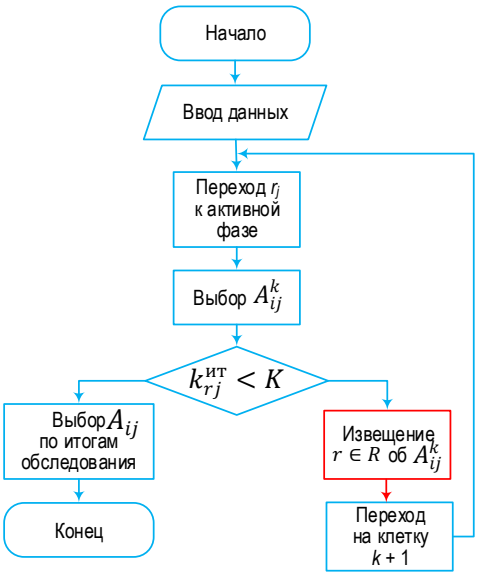

Рис. 2. Итерационный алгоритм обследования сцены одиночным роботом (блоки синим цветом) и в активной фазе итерационного цикла при коллективном принятии решения (блоки синим + красным цветом)

Fig. 2. Iterative Algorithm of Scene Exploration by Single Robot (Blue Blocks) and in Active Phase of Iterative Cycle in Case of Group Decision Making (Blue + Red Blocks)

После каждой итерации роботы на основе анализа всех хэш-таблиц оценивают частоту каждой альтернативы на исследуемой сцене и делают вывод об оптимальной альтернативе A_{opt}. Такой обмен информацией позволяет сформировать более полное представление каждого робота об окружающей среде, которое выходит за рамки исследованной области непосредственно самим роботом. Проиллюстрируем это на примере рисунка 1.

Пример 1. Анализ ситуации показывает, что робот белого цвета (далее – «белый» робот) обследовал 9 клеток, из которых 3 клетки оказались желтого цвета, 1 – зеленого, 4 – фиолетового, 1 – серого. Клетки голубого цвета роботу не встретились. Результаты сведены в таблицу 1; аналогично для «красного» и «синего» роботов.

Таким образом, первый робот выбирает альтернативу A_3 (преобладающий цвет сцены – фиолетовый). Второй робот – альтернативу A_1 или A_4, и только третий робот – альтернативу $A_1 = A_{opt}$ (преобладающий цвет сцены – желтый). Очевидно, что в такой ситуации для достижения консенсуса в рое потребуются дополнительные итерации. Если же эти три робота будут находиться в зоне радиосвязи, тогда в результате информационного обмена у каждого сформируется итоговая таблица (см. таблицу 1).

ТАБЛИЦА 1. Результаты оценки сцены роботами: «белым» / «красным» / «синим» / группой

TABLE 1. Results of Scene Assessing by Robots: by «white» One / by «Red» One / by «Blue» One / by Group

Цвет клетки	Альтернативы	Процент
Желтый	3 / 3 / 4 / 10	33,3 / **30,0** / **40,0** / **34,5**
Зеленый	1 / 1 / 1 / 3	11,1 / 10,1 / 10,0 / 10,3
Фиолетовый	4 / 2 / 3 / 9	**44,4** / 20,0 / 30,0 / 31,0
Серый	1 / 3 / 1 / 5	11,1 / **30,0** / 10,0 / 17,2
Голубой	0 / 1 / 1 / 2	0,0 / 10,0 / 10,0 / 6,9
Всего	9 / 10 / 10 / 29	

Очевидно, что наличие информационного обмена приводит к увеличению вероятности выбора альтернативы $A_1 = A_{opt}$ при тех же затратах вычислительных и временны́х ресурсов каждого робота. Синергетический эффект усиливается при увеличении количества роботов на сцене (рисунок 3).

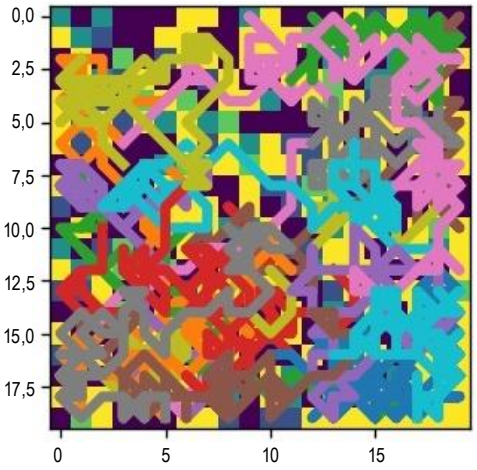

Рис. 3. Сцена, состоящая из 400 клеток с пятью альтернативами и маршруты 20 роботов после 60 итераций

Fig. 3. Scene, Which Consists of 400 Cells with 5 Alternatives and Routes for 20 Robots after 60 Iterations

Как видно на рисунке 4, при 20 роботах в рое, когда каждый отдельный робот исследовал не более 10 % сцены, за счет информационного взаимодействия в его итоговой хэш-таблице будет содержаться информация о более, чем 90 % клеток.

Ситуация меняется, если даже один из трех роботов, например «красный» (см. рисунок 1), окажется вредоносным. Если он будет руководствоваться случайной стратегией поведения, то выбор альтернативы на каждой итерации будет осуществляться не сенсорными устройствами робота, а датчиком случайных чисел. При этом не исключено совпадение на k-м шаге реального цвета клетки со сгенерированным датчиком случайных чисел ВР ($A^* = A_{opt}$). Пример реализации такой атаки представлен в таблице 2. Если ВР использует ОСП, то для каждой клетки будет выполняться условие $A^* \neq A_{opt}$. В случае использования КСП, ВР на каждой итерации выбирает одну и ту же стратегию $A^* = A_2$ – якобы все обследованные «красным» роботом клетки на сцене зеленого цвета.

ТАБЛИЦА 2. Результаты совместной оценки сцены тремя роботами при 1 ВР с ССП / ОСП / КСП

TABLE 2. Results of Cooperative Assessing of Scene by three Robots in Case of 1 Malicious Robot with Random Behavior Strategy / Opposing Behavior Strategy / Coordinated Behavior Strategy

Цвет клетки	Альтернативы	Процент
Желтый	8 /7 / 7	27,6 / 24,1 / 24,1
Зеленый	6 /6 / 12	20,7 / 20,7 / **41,4**
Фиолетовый	9 / 9 / 7	**31,0** / **31,0** / 24,1
Серый	2 / 3 / 3	6,9 / 10,3 / 10,3
Голубой	4 / 4 / 1	13,8 / 13,8 / 3,4
Всего	29 / 30 / 29	

Как видно из этих тривиальных примеров, все стратегии ВР приводят к снижению вероятности выбора искомой альтернативы $P(A_1 = A_{opt})$. Причем в наибольшей степени вероятность сделать ошибочный выбор возникает при использовании ВР стратегии КСП. Очевидно, что если количество таких ВР с КСП превысит 50 % от количества роботов в рое, то $P(A_1 = A_{opt}) = 0$.

Как показано в ряде приведенных выше работ, выявление ВР с ССП и ОСП успешно решается различными методами. Например, использование метрики доверия и/или репутации позволяет выявить случаи дезинформации, продуцируемой ВР, и роботы с метрикой меньшей некоего порога исключаются из дальнейшего информационного обмена [19]. В ряде сценариев метод, основанный на расчете доверия и репутации агентов друг к другу, позволяет успешно выполнить задачу и при атаке «51 процент». К такому сценарию относится задача целераспределения [18], когда роботы, имеющие высокий уровень доверия, способны достичь поставленной цели без достижения консенсуса с агентами всего роя.

Однако для рассматриваемого сценария коллективного принятия решения атака «51 процент» является фатальной даже при наличии механизма оценки доверия и репутации. Это обусловлено тем, что оценки доверия и репутации, выставляемые агентами роя друг другу в процессе обследования

сцены, являются взаимными. Иначе говоря, если «обычные» роботы на основе проверки информации, сообщаемой ВР, выставляют им низкие значения доверия и репутации, то ВР, используя тот же самый алгоритм определения метрик доверия и репутации, будут выставлять такие же низкие оценки всем другим роботам. Тогда, при наличии большинства ВР в рое (> 50 %), в результате консенсуса будет принята альтернатива, «лоббируемая» ВР.

Во избежание такого явления возможно проведение следующих мероприятий:

1) осуществлять непрерывный контроль за количеством роботов в группе; такой способ позволит избежать атаки «51 процент», но потребует дополнительных механизмов защиты от влияния ВР – независимых систем объективного контроля, не интегрированных в рой, резервных (защищенных) каналов связи с центром управления и наличие весомого запаса дронов;

2) обеспечить наличие в рое специальных роботов, выполняющих функции полицейских участков [20].

Указанные мероприятия потребуют дополнительных материальных затрат и усложнения организационной структуры роя, и по сути, лишают его преимуществ самоорганизующейся системы. Отсюда вытекает необходимость в разработке алгоритма, который в процессе информационного взаимодействия позволит однозначно идентифицировать ВР с КСП всеми участниками процедуры достижения консенсуса.

Алгоритм действия роботов группы, находящихся в пассивной фазе итерационного цикла

Предлагаемый в данной статье алгоритм противодействия атакам ВР с КСП основан на предположении о разности статистических характеристик сигналов, продуцируемых ВР и иными агентами роя, и на свойствах объектов сцены. Для этого каждому цвету сцены необходимо присвоить определенное числовое значение, в соответствии с некоторой таблицей кодировки (таблица 3).

ТАБЛИЦА 3. Таблица кодировки альтернатив

TABLE 3. Alternative Encodings

Цвет клетки	Желтый	Зеленый	Фиолет	Серый	Голубой
Номер и обозначение альтернативы	A_1 – ‘1’	A_2 – ‘2’	A_3 – ‘3’	A_4 – ‘4’	A_5 – ‘5’

Работу алгоритма удобно пояснить на простейшем примере.

Пример 2. Рассмотрим сцену размером 10 на 10, состоящую из клеток пяти цветов, которую исследуют два робота. Тогда при движении «белого» и «красного» робота по сцене (рисунок 4) их сообщения за пять итераций будут содержать, помимо сведений о текущем времени и номере посещаемой клетки, информацию о кодировке ее цвета в соответствии с таблицей 8:

$$C_{\text{белый}}^{\text{кортеж 1}} = \{4, 1, 5, 3, 2\},$$
$$C_{\text{красный}}^{\text{кортеж 1}} = \{1, 2, 2, 4, 1\}.$$

Средние значения $\mu(C)$ этих числовых рядов будут соответственно равны:

$$\mu\left(C_{\text{белый}}^{\text{кортеж 1}}\right) = 3 \text{ и } \mu\left(C_{\text{красный}}^{\text{кортеж 1}}\right) = 2.$$

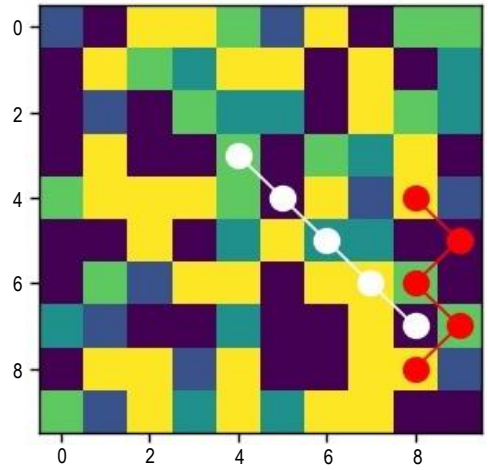

Рис. 4. Маршруты движения двух роботов по сцене 10×10 за 5 итерации

Fig. 4. Routes for 2 Robots in 5 Iterations in 10×10 Scene

Еще через пять итераций роботы проделают определенный путь (рисунок 5) и сформируют следующие кортежи:

$$C_{\text{белый}}^{\text{кортеж 2}} = \{3, 1, 3, 1, 1\}, \quad C_{\text{красный}}^{\text{кортеж 2}} = \{5, 2, 1, 3, 3\}.$$

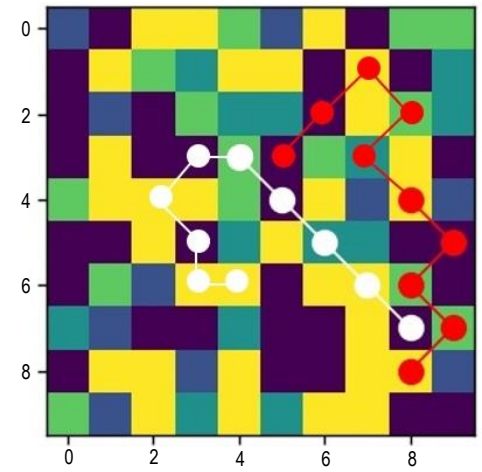

Рис. 5. Маршруты движения двух роботов по сцене 10×10 за 10 итерации

Fig. 5. Routes for Two Robots in 10 Iterations in 10×10 Scene

Средние значения $\mu(C)$ кортежей будут, соответственно, равны:

$$\mu\left(C_{\text{белый}}^{\text{кортеж 2}}\right) = 1{,}8 \text{ и } \mu\left(C_{\text{красный}}^{\text{кортеж 2}}\right) = 3.$$

Если предположить, что «красный» робот является ВР с КСП, который реализует предустановленную стратегию, например $A^* = '2'$, т. е. «лоббирует» преобладание клеток зеленого цвета на сцене, тогда:

$$C_{\text{красный}}^{\text{кортеж 1}} = \{2, 2, 2, 2, 2\},\ C_{\text{красный}}^{\text{кортеж 2}} = \{2, 2, 2, 2, 2\} \text{ и}$$

$$\mu\left(C_{\text{красный}}^{\text{кортеж 1}}\right) = \mu\left(C_{\text{красный}}^{\text{кортеж 2}}\right) = 2.$$

Таким образом, средние значения кортежей, продуцируемых роботами за первые пять итераций обследования сцены и последующие пять итераций для ВР, не изменяются, а для всех остальных роботов – изменяются. Это обстоятельство позволяет реализовать процедуру чересперiодного вычитания средних значений смежных кортежей, продуцируемых j-м роботом посредством реализации схемы, приведенной на рисунке 6.

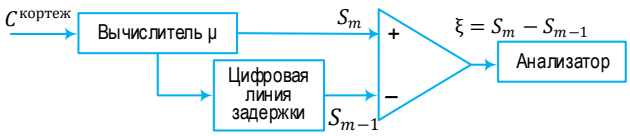

Рис. 6. Функциональная схема чересперiодного вычитания

Fig. 6. Functional Diagram of Through-Period Subtraction

Здесь $S_m = \mu(C^{\text{кортеж 2}})$, $S_{m-1} = \mu(C^{\text{кортеж 1}})$. Величина ξ вычисляется как разность:

$$\xi = S_m - S_{m-1}. \qquad (1)$$

Если «белый» и «красный» роботы продуцируют истинные значения кодов цветов, то, согласно приведенной схеме, для рассмотренного примера на выходе компаратора получим для «белого» робота:

$$\xi_{\text{белый}} = S_m - S_{m-1} = 3 - 1{,}8 = 1{,}2;$$

для «красного»:

$$\xi_{\text{красный}} = S_m - S_{m-1} = 2 - 3 = -1.$$

Если «красный» робот является вредоносным, то:

$$\xi_{\text{красный}} = S_m - S_{m-1} = 2 - 2 = 0.$$

Задача анализатора в этой схеме заключается в оценке полученных на выходе компаратора случайных величин ξ. В простейшем случае его роль может сводится к правилу:

$$r_i = \begin{cases} \text{ВР}, & \text{если } \xi = 0 \\ \text{ДР}, & \text{иначе} \end{cases}, \qquad (2)$$

где ДР – действующий робот группы.

Также можно использовать статистические критерии принятия решения [19].

Алгоритм, реализующий процедуру чересперiодного вычитания, показан на рисунке 7.

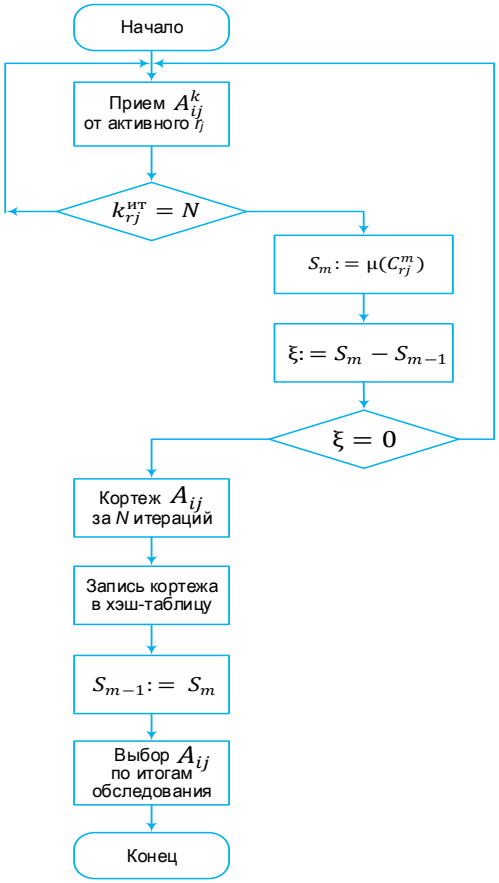

Рис. 7. Алгоритм действии робота в пассивной фазе итерационного цикла, реализующий схему чересперiодной компенсации

Fig. 7. Passive Phase of Iterative Cycle Behavior Algorithm, Which Implements Through-Period Subtraction

В пассивной фазе итерационного цикла коллективного принятия решения роботы роя, получая извещения о выбранной альтернативе A_{ij}^k от агента r_j, находящегося в активной фазе (см. рисунок 3), формируют m-й кортеж кодировок альтернатив $C_{r_j}^m$ из N элементов и вычисляют S_m. Далее по формуле (1) вычисляя разность ξ, и, используя правило (2), каждый робот принимает решение, является ли r_j ВР, или нет.

В зависимости от принятого решения, данные, полученные от активного агента r_j и записанные в хэш-таблицу, либо будут учитываться роботом при выборе альтернативы, либо не будут. Следует учесть, что из-за разных условий радиосвязи информация, получаемая роботами от активного агента, может отличаться. Вследствие этого решения, принимаемые роботами, как в отношении соседних роботов, так и выбираемой ими альтернативы также могут отличаться. Так как процедура чересперiодного вычитания является циклической, когда роботы постоянно проверяют корректность полученных сведений от соседей, выполняется операция запоминания на период текущего значения S_m.

Программная реализации модели роя с внедренными ВР с КСП

Для экспериментальной проверки работоспособности предложенного алгоритма разработана имитационная модель, представляющая собой программную реализацию рассмотренного проблемного сценария в среде Phyton с использованием объектно-ориентированного подхода. Цель эксперимента – оценить работоспособность алгоритма чересперiодного вычитания при обследовании сцены из 400 клеток пяти цветов двадцатью роботами (см. рисунок 4) при наличии в рое группы ВР с КСП.

Оцениваемой величиной (показателем степени защищенности роя от атаки «51 процент») являлась вероятность $P(A_{opt})$ того, что в результате консенсуса группой роботов будет выбрана альтернатива $A_1 = A_{opt}$ – «цвет сцены желтый». Консенсус достигался простым большинством голосов «не-ВР» роботов. Варьируемыми параметрами являлись: $N_{\text{ВР}}$ – концентрация ВР с КСП в рое; $D_{\text{СВ}}$ – дальность радиосвязи между роботами; L – длина кортежа; Sc – сложность сцены.

Под сложностью сцены понималось процентное соотношение превалирующего цвета по отношению к остальным. Рассматривались две ситуации: простая – сцена содержит 60 % клеток желтого цвета, остальные цвета распределены равномерно по оставшимся 40 % клеткам; сложная – сцена содержит 40 % клеток желтого цвета, 60 % клеток окрашены равномерно в 4 цвета.

В начале эксперимента генерировалась сцена заданной сложности со случайным расположением цветов, и роботы случайным образом размещались внутри арены. Номера ВР-роботов выбирались датчиком случайных чисел. Траектория движения каждого робота представляется ломаной линией – в своей активной фазе робот чередует движение в произвольно выбранном направлении либо вращение на месте, направление которых также выбирается случайным образом. Робот способен принимать извещения только от тех роботов, которые находятся на расстоянии, не превышающем заданную дальность радиосвязи.

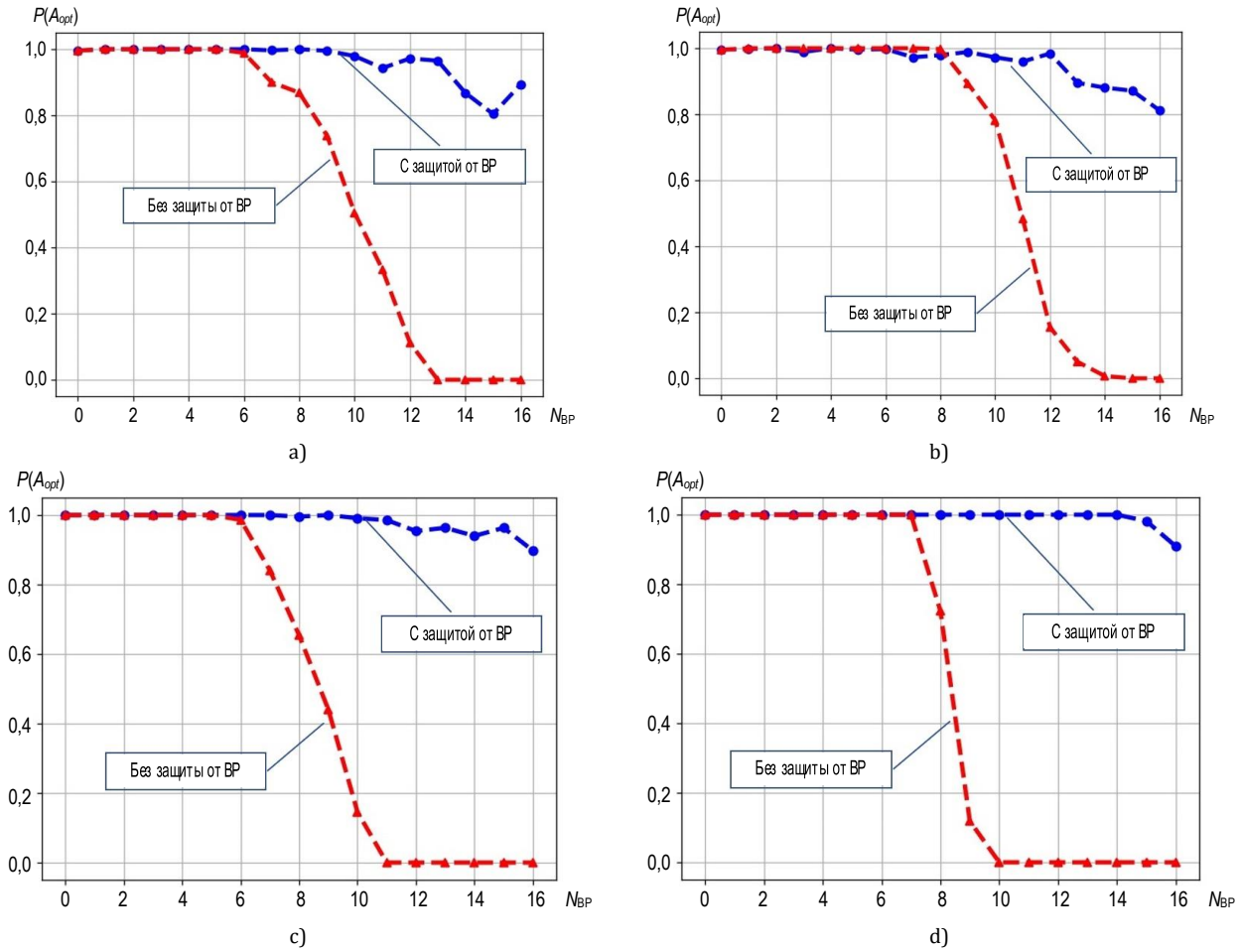

Рис. 8. Оценка алгоритма при изменении концентрации ВР в рое с использованием алгоритма чересперiодного вычитания и без него: a) $D_{\text{СВ}}$ = 6, L = 5, Sc = 40 %; b) $D_{\text{СВ}}$ = 6, L = 5, Sc = 60 %; c) $D_{\text{СВ}}$ = 6, L = 10, Sc = 40 %; d) $D_{\text{СВ}}$ = 11, L = 10, Sc = 60 %

Fig. 8. Algorithm Evaluation with Variable Concentration of Malicious Robots in Swarms, Which Uses and Does Not Use Through-Period Subtraction: a) D_CB = 6, L = 5, Sc = 40 %; b) D_CB = 6, L = 5, Sc = 60 %; c) D_CB = 6, L = 10, Sc = 40 %; d) D_CB = 11, L = 10, Sc = 60 %

Все роботы при обследовании сцены действовали по единым алгоритмам. Алгоритм, представленный на рисунке 3, использовался для роботов в активной фазе, на рисунке 7 – в пассивной. Отличие программного обеспечения ВР от «незараженных» роботов состояло в том, что все ВР в своей активной фазе выбирали единую альтернативу $A^* = A_2$ – «цвет зеленый». Для сравнения также осуществлялся расчет действий роя без использования алгоритма чересперiодного вычитания.

На рисунке 8 представлены результаты экспериментов, когда расчет вероятности P(A_opt) осуществлялся при увеличении количества ВР в рое; приведены значения, усредненные по 100 сериям экспериментов. Из рисунка видно, что если роботы используют алгоритмы, не имеющие механизмов защиты от атак ВР, то для сложной сцены (*Sc* = 40 %) ВР с КСП, количество которых превышает 30 % от числа роботов в группе, это приводит к резкому снижению вероятности $P(A_{opt})$ (см. рисунки 8a и 8c). Достижение концентрации ВР 50 % приводит к фатальным результатам – рой гарантированно не сможет определить преимущественный цвет сцены. Для простой сцены (*Sc* = = 60 %) ситуация незначительно лучше.

Таким образом, в соответствии с поставленной целью, можно утверждать, что защищенность роя роботов от атаки «51 процент» с использованием алгоритма чересперiодного вычитания возрастает до 80 %. Если роботы используют предложенный алгоритм чересперiодного вычитания, то даже при значительном преобладании ВР с КСП рой может выполнить поставленную задачу с вероятностью $P(A_i = A_{opt}) > 0{,}8$. Причем увеличение длины кортежа способствует большей стабильности результатов обследования сцены (см. рисунок 8d).

На рисунке 9 показана зависимость вероятности выбора верной альтернативы от дальности радиосвязи.

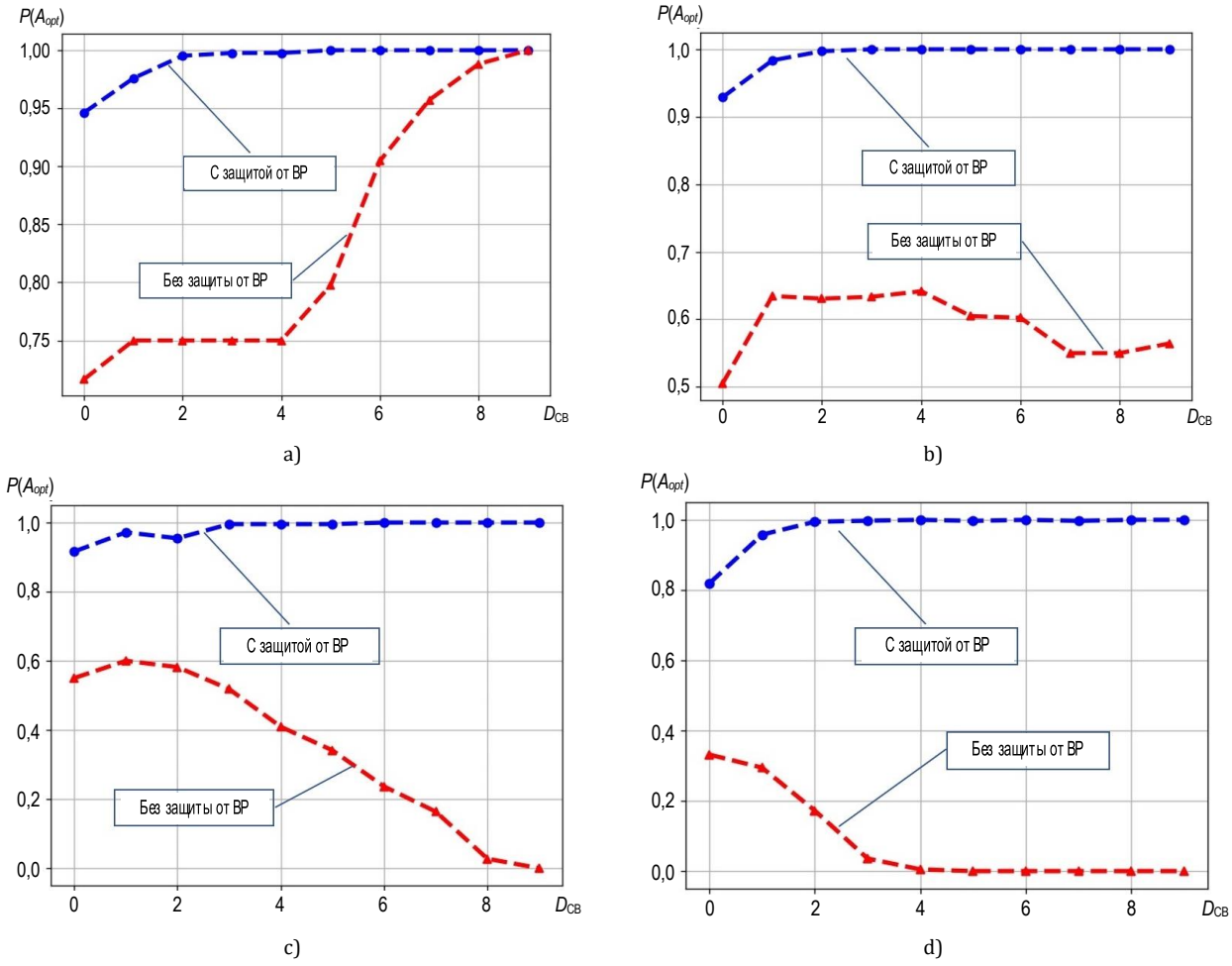

Рис. 9. Оценка алгоритма при изменении дальности радиосвязи между роботами в группе:
a) $N_{ВР}$ = 5, *L* = 10, *Sc* = 60 %; b) $N_{ВР}$ = 5, *L* = 10, *Sc* = 40 %; c) $N_{ВР}$ = 8, *L* = 10, *Sc* = 60 %; d) $N_{ВР}$ = 8, *L* = 10, *Sc* = 40 %

Fig. 9. Algorithm Evaluation with Variable Communication Range in Robot Group:
a) N_BP = 5, L = 10, Sc = 60 %; b) N_BP = 5, L = 10, Sc = 40 %; c) N_BP = 8, L = 10, Sc = 60 %; d) N_BP = 8, L = 10, Sc = 40 %

При небольшом количестве ВР и простой сцене увеличение дальности радиосвязи, а значит – и количества роботов, принимающих участие в достижении консенсуса, приводит к положительным результатам даже без принятия мер противодействия ВР (см. рисунок 9a). Однако при сложной сцене или при увеличении количества ВР эффективность такого алгоритма существенно снижается (см. рисунки 9b–9d).

При использовании алгоритма чересперiодной компенсации увеличение дальности радиосвязи положительно сказывается на достижении консенсуса. Очевидно, это связано с тем, что увеличение дальности радиосвязи приводит к повышению осведомленности каждого отдельного робота об исследуемой сцене.

Заключение

Предложенный алгоритм выявления ВР с КСП показал высокие результаты при использовании в рассмотренном проблемном сценарии коллективного восприятия. Роботы смогли исследовать окружающую среду, оценить частоту определенных функций и коллективно определить, какая функция встречается чаще всего даже при высокой концентрации в рое ВР. В отличие от механизмов выявления ВР, основанных на моделях доверия и/или репутации, каждый робот в группе получает однозначно интерпретируемую оценку «полезности» своих соседей.

В отличие от известных алгоритмов, эта оценка, получаемая путем реализации эвристического алгоритма чересперiодного вычитания, не требует дополнительных организационных мер, внедрения дополнительных информационных объектов и вычислительных ресурсов для контроля за ситуацией, так как алгоритм реализуется бортовыми вычислительными устройствами каждого робота.

В качестве ограничения, принятого авторами статьи, можно указать следующее. В статье не рассматривалась ситуация, когда ВР использовали бы рефлексию второго порядка, что предполагает осознанное противодействие со стороны ВР алгоритмам противодействия этим ВР роботов группы [21]. Практическая реализация рефлексии второго порядка может заключаться в том, что вредоносные роботы будут прибегать к сочетанию КСП со стратегиями ССП или ОСП. Очевидно, что это усложнит работу анализатора (см. рисунок 7), и вынудит использовать более сложные теории и представления знаний о социумах роботов [22, 23]. Однако можно утверждать, что эффективность атаки ВР при отказе от КСП также будет снижена.

Задача информационного противоборства в социуме роботов представляет все более возрастающий интерес, и может быть рассмотрена в дальнейших исследованиях авторов.

Список источников

1. Sailor M.J., Link J.R. Smart dust: nanostructured devices in a grain of sand // Chemical Communications. 2005. Iss. 11. P. 1375.

2. 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. Iss. 2&3. PP. 288–297.

3. Page J., Zaslavsky A., Indrawan M. A Buddy model of security for mobile agent communities operating in pervasive scenarios // Proceeding of the Australasian Information Security Workshop (AISW 2004), the Australasian Workshop on Data Mining and Web Intelligence (DMWI 2004), the Australasian Workshop on Software Internationalisation (AWSI 2004), Dunedin, New Zealand, January 2004. Sydney: Australian Computer Society, 2004. Vol. 54. PP. 17–25.

4. Schillo M., Funk P., Rovatsos M. Using trust for detecting deceitful agents in artificial societies // Applied Artificial Intelligence. 2000. Vol. 14. Iss. 8. PP. 825–848. DOI:10.1080/08839510050127579

5. Golbeck J., Parsia B., Hendler J. Trust Networks on the Semantic Web // Proceeding of the 7th International Workshop on Cooperative Information Agents (CIA 2003, Helsinki, Finland, 27–29 August 2003). Lecture Notes in Computer Science. Berlin Heidelberg: Springer-Verlag, 2003. Vol. 2782. PP. 238–249.

6. Garcia-Morchon O., Kuptsov D., Gurtov A., Wehrle K. Cooperative security in distributed networks // Computer Communications. 2013. Vol. 36. Iss. 12. PP. 1284–1297. DOI:10.1016/j.comcom.2013.04.007

7. Strobel V., Castelló Ferrer E., Dorigo M. Blockchain Technology Secures Robot Swarms: A Comparison of Consensus Protocols and Their Resilience to Byzantine Robots // Frontiers in Robotics and AI. 2020. Vol. 7. P. 54. DOI:10.3389/frobt.2020.00054

8. Fagiolini A., Pellinacci M., Valenti G., Dini G., Bicchi A. Consensus-based Distributed Intrusion Detection for Multi-Robot Systems // Proceeding of the International Conference on Robotics and Automation (ICRA 2008, Pasadena, USA, 19–23 May 2008). IEEE, 2008. DOI:10.1109/ROBOT.2008.4543196

9. Бешта А.А., Кирпо М.А. Построение модели доверия к объектам автоматизированной информационной системы для предотвращения деструктивных воздействий на систему // Известия Томского политехнического университета. 2013. Т. 322. № 5. С. 104–108. EDN:QOXUKV

10. Зикратов И.А., Зикратова Т.В. Использование поведенческих моделей для исследования социумов роботов // Информация и космос. 2022. № 4. С. 170–174. EDN:DQASLC

11. Basan A., Basan E., Makarevich O. Analysis of ways to secure group control for autonomous mobile robots // Proceedings of the 10th International Conference on Security of Information and Networks (Jaipur, India, 13–15 October 2017). New York: Association for Computing Machinery, 2017. PP. 134–139. DOI:10.1145/3136825.3136879

12. Strobel V., Castelló Ferrer E., Dorigo M. Managing Byzantine Robots via Blockchain Technology in a Swarm Robotics Collective Decision Making Scenario: Robotics track // Proceedings of the International Conference on Autonomous Agents and Multiagent Systems (IntelliSys 2016). Lecture Notes in Networks and Systems. Vol. 16. Cham: Springer, 2018. PP. 541–549.

13. Sargeant I., Tomlinson A. Review of Potential Attacks on Robotic Swarms // Proceedings of the International Conference on Autonomous Agents and Multiagent Systems (IntelliSys 2016). Lecture Notes in Networks and Systems. Vol. 16. Cham: Springer, 2018. PP. 628–646. DOI:10.1007/978-3-319-56991-8_46

14. Рябцев С.С. Метод выявления вредоносных роботов на основе данных процесса коллективного принятия решений в роевых робототехнических системах // Системы управления, связи и безопасности. 2022. № 3. С. 105–137. DOI:10.24412/2410-9916-2022-3-105-137. EDN:SVSCHG

15. Юрьева Р.А., Комаров И.И., Викснин И.И. Иммунологические принципы принятия решения в мультиагентных робототехнических системах // Глобальный научный потенциал. 2015. № 5(50). С. 87–91. EDN:UKOVSB

16. Юрьева Р.А., Комаров И.И., Масленников О.С. Разработка метода обнаружения и идентификации скрытого деструктивного воздействия на мультиагентные робототехнические системы // Программные системы и вычислительные методы. 2016. № 4. С. 375–382. DOI:10.7256/2305-6061.2016.4.21128. EDN:XIAJDB

17. Valentini G., Brambilla D., Hamann H., Dorigo M. Collective Perception of Environmental Features in a Robot Swarm // Proceedings of the International Conference on Swarm Intelligence. Lecture Notes in Computer Science. Vol. 9882. Cham: Springer, 2016. PP. 65–76. DOI:10.1007/978-3-319-44427-7_6

18. Каляев И.А., Гайдук А.Р., Капустян С.Г. Модели и алгоритмы коллективного управления в группах роботов. М.: ФИЗМАТЛИТ, 2009. 280 с. EDN:MUWSIT

19. Зикратова Т.В. Метод группового управления в мультиагентных робототехнических системах в условиях воздействия дестабилизирующих факторов // Труды учебных заведений связи. 2021;7(3):92–100. DOI:10.31854/1813-324X-2021-7-3-92-100. EDN:JFMYBF

20. Zikratov I.A., Lebedev I.S., Gurtov A.V., Kuzmich E.V. Securing swarm intellect robots with a police office model // Proceedings of the 8th IEEE International Conference on Application of Information and Communication Technologies (AICT, Astana, Kazakhstan, 15–17 October 2014). IEEE, 2014. DOI:10.1109/ICAICT.2014.7035906

21. Лефевр В.А., Смолян Г.Л. Алгебра конфликта. М., 1968. 51 с.

22. Городецкий В.И. Поведенческие модели кибер-физических систем и групповое управление: основные понятия // Известия ЮФУ. Технические науки. 2019. № 1(203). С. 144–162. DOI:10.23683/2311-3103-2019-1-144-162. EDN:LYUZBR

23. Карпов В.Э. Социальные сообщества роботов: от реактивных к когнитивным агентам // Мягкие измерения и вычисления. 2019. № 2(15). С. 61–78. EDN:SEFEFV

References

1. Sailor M.J., Link J.R. Smart dust: nanostructured devices in a grain of sand. *Chemical Communications*. 2005;11:1375.

2. Higgins F., Tomlinson A., Martin K.M. Threats to the Swarm: Security Considerations for Swarm Robotics. *International Journal on Advances in Security*. 2009;2(2&3):288–297.

3. Page J., Zaslavsky A., Indrawan M. A Buddy model of security for mobile agent communities operating in pervasive scenarios. *Proceeding of the Australasian Information Security Workshop (AISW 2004), the Australasian Workshop on Data Mining and Web Intelligence (DMWI 2004), the Australasian Workshop on Software Internationalisation (AWSI 2004), January 2004, Dunedin, New Zealand, vol.54*. Sydney: Australian Computer Society; 2004. p.17–25.

4. Schillo M., Funk P., Rovatsos M. Using trust for detecting deceitful agents in artificial societies. *Applied Artificial Intelligence*. 2000;14(8):825–848. DOI:10.1080/08839510050127579

5. Golbeck J., Parsia B., Hendler J. Trust Networks on the Semantic Web. *Proceeding of the 7th International Workshop on Cooperative Information Agents, CIA 2003, 27–29 August 2003, Helsinki, Finland. Lecture Notes in Computer Science, vol.2782*. Berlin Heidelberg: Springer-Verlag; 2003. p.238–249.

6. Garcia-Morchon O., Kuptsov D., Gurtov A., Wehrle K. Cooperative security in distributed networks. *Computer Communications*. 2013:36(12):1284–1297. DOI:10.1016/j.comcom.2013.04.007

7. Strobel V., Castelló Ferrer E., Dorigo M. Blockchain Technology Secures Robot Swarms: A Comparison of Consensus Protocols and Their Resilience to Byzantine Robots. *Frontiers in Robotics and AI*. 2020;7:54. DOI:10.3389/frobt.2020.00054

8. Fagiolini A., Pellinacci M., Valenti G., Dini G., Bicchi A. Consensus-based Distributed Intrusion Detection for Multi-Robot Systems. *Proceeding of the International Conference on Robotics and Automation, ICRA 2008, 19–23 May 2008, Pasadena, USA*. IEEE; 2008. DOI:10.1109/ROBOT.2008.4543196

9. Beshta A.A., Kirpo M.A. Automated Information System Objects Trust Model Design For Preventing Destructive Effects On The System. *Bulletin of the Tomsk Polytechnic University*. 2013;322(5):104–108. (in Russ.) EDN:QOXUKV

10. Zikratov I., Zikratova T. Using Behavioral Models To Study Robot Societies // Information and Space. 2022;4:170–174. (in Russ.) EDN:DQASLC

11. Basan A., Basan E., Makarevich O. Analysis of ways to secure group control for autonomous mobile robots. *Proceedings of the 10th International Conference on Security of Information and Networks, 13–15 October 2017, Jaipur, India*. New York: Association for Computing Machinery; 2017. p.134–139. DOI:10.1145/3136825.3136879

12. Strobel V., Castelló Ferrer E., Dorigo M. Managing Byzantine Robots via Blockchain Technology in a Swarm Robotics Collective Decision Making Scenario: Robotics track. *Proceedings of the International Conference on Autonomous Agents and Multiagent Systems (IntelliSys 2016). Lecture Notes in Networks and Systems, vol.16*. Cham: Springer; 2018. p.541–549.

13. Sargeant I., Tomlinson A. Review of Potential Attacks on Robotic Swarms. *Proceedings of the International Conference on Autonomous Agents and Multiagent Systems (IntelliSys 2016). Lecture Notes in Networks and Systems, vol.16*. Cham: Springer; 2018. p.628–646. DOI:10.1007/978-3-319-56991-8_46.
14. Ryabtsev S.S. A method for detecting Byzantine robots based on data from the collective decision-making process in swarm robotic systems. *Systems of Control, Communication and Security*. 2022;3:105–137. (in Russ.) DOI:10.24412/2410-9916-2022-3-105-137. EDN:SVSCHG
15. Yuryeva R.A., Komarov I.I., Viksnin I.I. Immunological Principles Of Decision-Making In Multiagent Robotic Systems. *Global Scientific Potential*. 2015;5(50):87–91. (in Russ.) EDN:UKOVSB
16. Yuryeva R.A., Komarov I.I., Maslennikov O.S. Development Of A Method For Detecting And Identifying Hidden Destructive Effects On Multi-Agent Robotic Systems. *Software Systems and Computational Methods*. 2016;4:375–382. (in Russ.) DOI:10.7256/2305-6061.2016.4.21128. EDN:XIAJDB
17. Valentini G., Brambilla D., Hamann H., Dorigo M. Collective Perception of Environmental Features in a Robot Swarm. *Proceedings of the International Conference on Swarm Intelligence. Lecture Notes in Computer Science, vol.9882*. Cham: Springer; 2016. p.65–76. DOI:10.1007/978-3-319-44427-7_6
18. Kalyaev I.A., Gaiduk A.R., Kapustyan S.G. *Models and algorithms of collective control in robot groups*. Moscow: FIZMATLIT Publ.; 2009. 280 p. (in Russ.) EDN:MUWSIT
19. Zikratova T. The Method of Group Control In Multi-Agent Robotic Systems Under The Influence Of Destabilizing Factors. *Proceedings of Telecommunication Universities.* 2021;7(3):92–100. (in Russ.) DOI:10.31854/1813-324X-2021-7-3-92-100. EDN:JFMYBF
20. Zikratov I.A., Lebedev I.S., Gurtov A.V., Kuzmich E.V. Securing swarm intellect robots with a police office model. *Proceedings of the 8th IEEE International Conference on Application of Information and Communication Technologies, AICT, 15–17 October 2014, Astana, Kazakhstan*. IEEE; 2014. DOI:10.1109/ICAICT.2014.7035906
21. Lefevr V.A., Smolyan G.L. *Algebra of Conflict*. Moscow, 1968. 51 p. (in Russ.)
22. Gorodetsky V.I. Behavioral Model For Cyber-Physical System And Group Control: The Basic Concepts. *Izvestiya SFedU. Engineering Sciences*. 2019;1(203):144–162. (in Russ.) DOI:10.23683/2311-3103-2019-1-144-162. EDN:LYUZBR
23. Karpov V.E. Social communities of robots: from reactive to cognitive agents. *Soft Measurements and Computing*. 2019;2(15):61–78. (in Russ.) EDN:SEFEFV

Статья поступила в редакцию 17.04.2024; одобрена после рецензирования 14.05.2024; принята к публикации 04.06.2024.
The article was submitted 17.04.2024; approved after reviewing 14.05.2024; accepted for publication 04.06.2024.

Информация об авторах:

ЗИКРАТОВ Игорь Алексеевич — доктор технических наук, профессор, профессор кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича
https://orcid.org/0000-0001-9054-800X

ЗИКРАТОВА Татьяна Викторовна — преподаватель кафедры информационных технологий Военно-морского политехнического института ВУНЦ ВМФ «Военно-морская академия имени Адмирала Флота Советского Союза Н.Г. Кузнецова»
https://orcid.org/0000-0001-8365-658X

НОВИКОВ Егор Анатольевич — аспирант кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича
https://orcid.org/0000-0003-3448-3015

Авторы сообщают об отсутствии конфликтов интересов.
The authors declare no conflicts of interests.