УДК 004.896

Метод выявления вредоносных роботов на основе данных процесса коллективного принятия решений в роевых робототехнических системах

Рябцев С. С.

Постановка задачи: *Критическая значимость механизмов коллективного поведения для функционирования роевых робототехнических систем актуализирует вопросы выявления роботов с неисправным или вредоносным поведением, заключающимся в навязывании нецелесообразных альтернатив во время достижения консенсуса при коллективном принятии решений. Известные подходы обеспечения информационной безопасности зачастую не учитывают специфические особенности реализации роевых систем, таких, как коллективное принятие решений и используют физические параметры в качестве критериев выявления вредоносных роботов. Кроме того, большинство исследований рассматривает наличие вредоносных роботов только со стратегией поведения, заключающейся в голосовании против большинства при достижении консенсуса.* ***Целью работы:*** *является повышение уровня информационной безопасности роевых робототехнических систем в процессе коллективного принятия решения в условиях наличия роботов с неисправным или вредоносным поведением за счет их выявления на основе данных цепочки принятия решения. Повышение уровня информационной безопасности осуществляется на основе увеличения вероятности достижения консенсуса роевой робототехнической системой относительно наилучшей альтернативы. Предлагается использовать подход, основанный на применении распределенного реестра и анализа отклонений в цепочке процесса коллективного принятия решения. Использование данного подхода позволит выявлять вредоносное воздействие со стороны роботов с неисправным или вредоносным поведением вне зависимости от условий функционирования и аппаратной реализации роевой робототехнической системы.* ***Используемые методы****: решение задачи выявления вредоносных роботов в роевых робототехнических системах базируется на применении критерия степени уверенности робота в выборе альтернативы при достижении консенсуса в процессе коллективного принятия решений. Решение этой задачи основано на гипотезе о том, что распределение степени уверенности вредоносного робота в виду особенностей протекания процесса коллективного принятия решений при использовании вредоносной стратегии значительно отличается от аналогичного распределения в корректно функционирующих роботах.* ***Новизна:*** *к элементам новизны предлагаемого решения относятся: 1) использование критерия степени уверенности для обеспечения информационной безопасности коллективного принятия решения; 2) возможность учета различных стратегий поведения вредоносных роботов. Использование предлагаемого решения позволяет повысить эффективность процесса коллективного принятия решений в роевых робототехнических системах при наличии вредоносных роботов. Проведенное имитационное моделирование для роевых робототехнических систем, состоящих из 20 роботов, при наличии роботов с неисправным или вредоносным поведением в количестве, не превышающем 45% от общего числа роботов в системе, продемонстрировало прирост вероятности принятия наилучшего решения относительно метода-аналога в среднем на 20%. Предложенная модификация метода, не учитывающего проблемы информационной безопасности процесса коллективного принятия решений, позволила повысить вероятность принятия наилучшего решения при наличии вредоносных роботов с координированной стратегией поведения на 57%, с оппозиционной стратегией поведения на 12%, со случайной стратегией поведения на 19%.* ***Практическая значимость:*** *представленное решение можно реализовать в виде программного обеспечения*

Библиографическая ссылка на статью:
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

Reference for citation:
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, no. 3, pp. 105-137 (in Russian). DOI: 10.24412/2410-9916-2022-3-105-137

для роевых робототехнических систем, что позволит обеспечить увеличение вероятности достижения консенсуса относительно наилучшей альтернативы в процессе коллективного принятия решения в условиях наличия роботов с неисправным или вредоносным поведением.

Ключевые слова: *роевая робототехническая система, информационная безопасность, вредоносный робот, коллективное принятие решений, достижение консенсуса, технология распределенного реестра.*

Введение

Термин «рой» определен в контексте робототехники в исследовательской работе [1] как разновидность большой группы мобильных, однородных и относительно простых роботов, коллективно работающих над выполнением одной задачи. Таксономия роевых робототехнических систем (РРТС) предложена в работе [2], а вопросы терминологии и критически важные свойства коллективного поведения РРТС подробно рассмотрены в работе [3].

Современное состояние РРТС можно охарактеризовать как [4]:

- первые практические применения РРТС, способных автономно обучаться подходящему коллективному поведению роботов для решения определенного класса задач;
- гражданские применения РРТС для точечного земледелия, а также для проверки и обслуживания городской инфраструктуры;
- военные применения РРТС в основном сосредоточенные на использовании групп небоевых беспилотных летательных аппаратов для разведки и планирования совместных действий.

Преимущества использования РРТС заключаются в возможности выполнения задач, требующих большого покрытия и параллельного исполнения за счет легкой масштабируемости и высокой отказоустойчивости [5].

С другой стороны, применение РРТС как группы мобильных роботов согласно [6] характеризуется следующими условиями:

- непредсказуемой динамикой внешней среды вплоть до сознательного противодействия;
- неполнотой и противоречивостью знаний роботов (агентов) о состоянии внешней среды и других участников;
- разнообразием вариантов путей достижения цели, структур коллектива, распределения ролей;
- сложностью обеспечения надежной коммуникации, распределенностью группировки в пространстве и т.д.

В работе [6] подчеркивается, что перечисленные факторы можно расценивать как источники угроз, создающих опасность нарушения конфиденциальности и целостности информации, циркулирующей в робототехнической системе, а также угрозу доступности объектов соответствующей информационной сферы.

Данная работа фокусируется на проблеме выявления вредоносных роботов (ВР) при достижении консенсуса (ДК) в процессе коллективного принятия решения (КПР) для последующей защиты от информации, продуцируемой ВР. Под ВР используется понятие, изложенное в исследованиях [7, 8] – «Византий-

ский робот», как общий термин для описания роботов, которые демонстрируют непреднамеренное или непоследовательное поведение, независимо от основной причины. Данный термин берет начало из работ о проблеме «Византийских генералов» [9]. В данном исследовании термины «Византийский» и «вредоносный» являются синонимами.

Актуальность проблемы обеспечения ИБ процесса КПР в РРТС для защиты от информации, продуцируемой ВР, связана с ростом популярности распределенных систем в робототехнике и наличием уязвимостей с точки зрения ИБ.

Продуцируемая ВР информация может оказать влияние на работу РРТС путем проведения атак категории «изменение» по классификации Столингса [10] путем модификации данных процесса КПР необходимых РРТС для координации, кооперации и выполнения целевых функций. При этом ВР не только получает доступ к информации, обмениваемой роботами для ДК, но и фальсифицирует эту информацию. При этом типе атак ВР изменяет и модифицирует данные, необходимые для корректного ДК в ходе КПР, в результате чего нарушается целостность информации, необходимой для принятия верного решения. Таким образом, РРТС может принять неэффективное или противоречивое решение.

Сложность решения задачи выявления ВР в РРТС заключается в том, что существующая парадигма ИБ зачастую не подходит для использования в РРТС, поскольку, во-первых, РРТС имеет значительные ограничения в ресурсах, а во-вторых, обладает набором специфических признаков, не позволяющих применять классические методы анализа и обнаружения аномалий из-за децентрализованной структуры управления, локальных ограничений связи между роботами и эмерджентности РРТС.

В большинстве работ по РРТС, предлагаемые методы апробируются в лабораторных условиях и не учитывают наличие неблагоприятной внешней среды и угроз информационной безопасности (ИБ). При этом на практике упущение данных вопросов может привести к негативным последствиям и отказу РРТС. Наряду с традиционными угрозами ИБ РРТС подвержены угрозам реализации специфических атак за счет системных свойств РРТС. Одной из специфических атак на процесс КПР в РРТС является воздействие со стороны ВР на процесс КПР. Наличие одного или нескольких ВР может оказать существенное влияние на скорость работы РРТС. Кроме того, ВР, успешно выполнив навязывание нецелесообразных альтернатив во время ДК при КПР, может привести к принятию неэффективного или опасного решения (например, ведущего к физическому повреждению роботов или элементов среды, в которой функционирует РРТС). Таким образом, обеспечение ИБ в РРТС становится одним из барьеров для применения РРТС на практике.

Постановка, классификация и сравнение РРТС со схожими технологиями, такими, как мультиагентные системы, беспроводные сенсорные сети, беспроводные децентрализованные самоорганизующиеся сети MANET и мультироботизированные системы, приведены в работе [11]. Обзор возможных атак на РРТС рассматривается в статье [12]. В исследовании [13] представлены результаты анализа эффективности выполнения задач РРТС в условиях скрытого де-

структивного воздействия, приведена закономерность между эффективностью выполнения задачи группирования роботов и относительным числом ВР. В статье [14] предлагают к рассмотрению три возможных типа ВР: «The contrarians», «The wishy-washy», «The sect». В работе [15] рассматривается способ противодействия ВР со случайной стратегией поведения. Тем не менее, наиболее часто в качестве ВР в литературе рассматриваются роботы, голосующие против большинства в задачах с бинарным выбором. Вместе с тем, в реальной практике применения РРТС возможны разнообразные стратегий воздействий ВР на процесс КПР, а задачи, стоящие перед РРТС, часто связаны с выбором из большого числа доступных альтернатив. В связи с этим существенными отличиями настоящей работы являются, во-первых, исследование не только задач с бинарным выбором, но и задач с большим количеством альтернатив. Во-вторых, предлагается к рассмотрению три типа ВР: ВР со случайной стратегией поведения (голосование за случайную альтернативу), ВР с оппозиционной стратегией поведения (голосование против большинства) и ВР с координированной стратегией поведения (голосование за определённую альтернативу).

Анализ технологий обеспечения ИБ в РРТС позволил выделить основные направления современных исследований в области обеспечения ИБ в РРТС:

- методы, основанные на анализе трафика и поведения;
- методы, основанные на специальных моделях ИБ;
- методы, основанные на применении распределенного реестра.

Методы, основанные на анализе трафика и поведения, предполагают развитие и модификацию технологий, направленных на детектирование и отслеживание аномальных значений в компьютерных системах таких, как сигнатурные методы и методы на основе машинного обучения. Суть применения методов анализа поведения заключается в сравнении текущего поведения системы с поведенческим эталоном в РРТС [16]. Структура обеспечения ИБ в РРТС с помощью данного класса методов основана на поведенческих процессах [17] и позволяет обнаруживать такие атаки, как отклонение от штатного поведения. В работе [18] выполнен анализ трафика для обнаружения атак на сети мобильных роботов. В исследовании [19] представлена концепция системы обнаружения вторжений в РРТС и продемонстрировано, что обнаружение на основе сигнатур может использоваться для обеспечения ИБ в РРТС. Сложность практического применения данного направления заключается в том, что:

- отсутствует глобальный канал связи в РРТС, что ограничивает коммуникацию всей системы. Данная особенность, с одной стороны, является ключом к легкой масштабируемости и надежности РРТС, а с другой стороны, затрудняет применение методов анализа и детектирования вторжений;
- децентрализованный подход приводит к отсутствию центрального узла и как следствие сложности сбора информации для выявления аномалий.

Результат анализа трафика и поведения отдельных агентов роя в процессе информационного взаимодействия в современных исследованиях широко от-

ражается в подходах обеспечения ИБ в РРТС с помощью метрик доверия и репутации [20]. Сущность применения метрик доверия и репутации заключается в применении систем установления, доверенных отношений, на основе определения репутации отдельным агентам/узлам [21]. Под доверием понимается мера, характеризующая готовностью субъекта взаимодействовать в данной ситуации с объектом, а под репутацией понимается сформировавшееся во времени коллективное мнение о качествах того или иного агента-субъекта. Данный подход может позволить применять специальные протоколы для противодействия активным сетевым атакам в РРТС. В работе [22] рассмотрена группа мобильных роботов, а предлагаемое решение основано на использовании концепции доверия для нахождения достоверности узлов по нескольким критериям меры доверия. В статье [23] рассматривается модель безопасности РРТС в условиях проведения мягких атак, использующих перехват сообщений, формирование и передачу группе мобильных роботов дезинформации [24]. Представленная модель базируется на принципах модели Блэка-Шоулза, но отличающаяся введением показателя «уровень доверия» для каждого робота, что затрудняет эксплуатацию уязвимостей ИБ в РРТС. Сложность применения метрик доверия и репутации часто заключается в необходимости выполнять вычисления, связанные с физическими параметрами функционирования РРТС (например, скорость, позиционирование, показания сенсоров), что может затруднять применение в РРТС из-за аппаратных различий и ограничений разных платформ РРТС.

В методах, основанных на специальных моделях управления ИБ, учитываются особенности РРТС. В работах [25, 26] представлен метод формирования самоорганизующейся системы управления ИБ в РРТС, реализующих модель полицейских участков. Сущность данной модели состоит в том, что вся зона работы роботов разбивается на отдельные участки, в каждом из которых находится управляющий узел, отвечающий за безопасность области. Сложность применения специальных моделей управления ИБ в РРТС заключается в том, что:

- практическая реализация специальных узлов может потребовать использование дополнительных систем контроля их работоспособности, иначе возможно наличие единой точки отказа;
- требуется разделение программной и аппаратной части роботов в РРТС, что затрудняет применение контролируемой зоны.

Методы на основе применения технологий распределенного реестра (ТРР) приведены в работах [7, 8]. Сущность применения алгоритмов ДК в блокчейн схожи с целями КПР в РРТС. Во-первых, блокчейн является распределенной системой КПР, предназначенной для работы в условиях недостатка доверия между сторонами, что соответствует условиям функционирования РРТС в агрессивной среде. Во-вторых, блокчейн-системы имеют встроенные механизмы поддержания актуальности информации, и, таким образом, РТСС, построенные с применением таких методов, не нуждаются в дополнительных механизмах для подтверждения записей. В-третьих, потеря отдельного узла децентрализованной блокчейн-системы не должна представлять угрозы как для процесса ДК, как и в РРТС.

Применение ТРР в задачах обеспечения ИБ процесса КПР для РРТС заключается в том, что противоречивое решение в РРТС может быть достигнуто полностью децентрализованным путем без априорного знания относительно того, какие роботы являются ВР. ТРР могут обеспечить необходимые возможности для того, чтобы сделать РРТС более безопасными, автономными и гибкими. Практические сложности применения ТРР при КПР в РРТС рассмотрены в статьях [27, 28]. Как правило, сложности состоят в существенной трудоемкости алгоритмов ДК и высоких аппаратных затратах, что приводит к существенному снижению скорости ДК [5]. Кроме того, стоит отметить ограничения вычислительных мощностей РРТС и отдельно взятых роботов [29, 30]. В связи с этим алгоритмы ДК в РРТС, несмотря на схожий подход, требуют своей модификации для применения в РРТС.

Перспективным является использование гибридных подходов, основанных на комплексном применении нескольких направлений обеспечения ИБ в РРТС для устранения их практических сложностей.

Целью работы является повышение уровня ИБ в РРТС на основе увеличения вероятности ДК в РРТС относительно наилучшей альтернативы в процессе КПР при наличии роботов с неисправным или вредоносным поведением. Под уровнем ИБ, понимается состояние защищенности процесса КПР, при котором обеспечивается выполнение РРТС, предписанных функций без нарушений целостности и модификации информации необходимой для принятия решения. Повышение уровня ИБ в РРТС предполагается за счет выявления и последующей блокировки роботов с неисправным или вредоносным поведением на основе данных цепочки принятия решения без использования дополнительных признаков, зависящих от условий функционирования.

Общая модель процесса КПР

Для формальной постановки и решения задачи в работе введены обозначения, представленные в таблице 1.

Таблица 1 – Обозначения

Обозначение	Физический смысл обозначения
A_i	– i-я альтернатива
A_{i*}	– альтернатива с наивысшим качеством P_i
R_i	– i-й робот РРТС
P_i	– качество альтернативы P_i, метрика характеризующая процентное соотношение i-й альтернативы в среде
G_i	– множество роботов РРТС, которые имеют локальную связь с R_i
S_j	– возможные начальные состояния среды
N_{ij}	– мера полезности, определяющая матрицу полезности N
N_{ij}^{BP}	– мера полезности, определяющая матрицу полезности N_{BP}
N_{i*j}	– наилучшее возможное состояние при выборе A_{i*}
N_{scene}	– площадь исследуемой среды
R_m	– множество роботов R_i РРТС
d	– расстояние, определяющее возможности связи между R_i
RT	– множество классов роботов

Обозначение	Физический смысл обозначения
RT_0	– корректно функционирующий, обычный робот (ОР)
RT_1	– ВР с случайной стратегией поведения (ССП)
RT_2	– ВР с оппозиционной стратегией поведения (ОСП)
RT_3	– ВР с координированной стратегией поведения (КСП)
Y_{abn}	– аномальное значение степени уверенности
$Y_{R_{cp}T_0}$	– средняя степень уверенность роботов R_m функционирующих нормально
$Y_{R_iT_k}$	– степень уверенность робота R_i функционирующего с отклонениями
τ_i	– время, в течение которого наблюдалась альтернатива A_i
T	– время выполнения процедуры исследования
Y_{R_i}	– уверенность робота R_i
$P_i^{\max}$	– качество наиболее распространённой альтернативы A_{i*} в среде
$T_N^{correct}$	– время, которое требуется РРТС для ДК относительно A_{i*}
E_N	– вероятность принятия наилучшего решения A_{i*}

На абстрактном уровне процесс КПР в РРТС предназначен для выбора наилучшего решения, в дальнейшем альтернативы (A_{i*}), из множества доступных альтернатив (A_m) некоторым набором роботов. Каждая альтернатива $A \in \{A_1,...,A_m\}$ характеризуется качеством $P_i \in (0,1]$ [31]. Роботы воспринимают качество альтернатив и всегда отдают предпочтение определенной альтернативе при ДК в процессе КПР.

Задача КПР считается успешно решенной, если выполняются 2 условия:

- РРТС достигает консенсуса относительно определенной альтернативы A_i в процессе КПР;
- альтернатива, относительно которой достигнут консенсус, связана с альтернативой A_{i*}, характеризующейся наивысшем качеством P_i.

Процесс КПР в самом общем виде представлен на рис. 1 и включает в себя три этапа последовательных итераций:

- исследование, этап на котором робот R_i исследует область и собирает информацию о качестве P_i альтернативы A_i;
- распространение, этап на котором робот R_i сообщает о своем выборе альтернативы A_i всем роботам G_i, имеющим с ним локальную связь, путем явного обмена сообщениями (например, по радио или инфракрасной связи), либо путем подачи сигналов (например, освещения светодиода RGB);
- смена мнения, этап на котором роботы РРТС следуют правилу КПР, например, модели избирателей или правилу большинства, для изменения или сохранения выбора альтернативы A_{i*}.

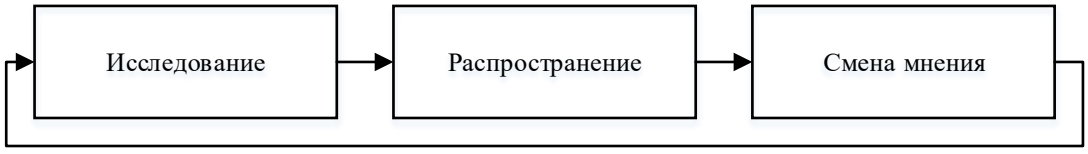

Рис. 1. Этапы процесса КПР в РРТС

Следует отметить, что отдельно взятым роботам РРТС не обязательно синхронно следовать этим этапам, за исключением тех моделей КПР в которых продолжительность фазы распространения коррелирует с качеством P_i. Каждый робот R_i РРТС имеет m доступных для выбора альтернатив $\{A_1, \ldots, A_m\}$ и n возможных начальных состояний $\{S_1, \ldots, S_n\}$.

В случае полной определенности относительно текущего состояния, робот R_i полностью уверен в текущем состоянии окружающей среды. При этом каждому роботу РРТС из поставленной задачи роботу R_i априорно известно качество P_i всех альтернатив и мера полезности N_{ij} для каждого A_i и S_j, что определяет матрицу полезности N:

$$N = (N_{ij})_{1 \le i \le m, 1 \le j \le n}. \quad (1)$$

При этом процесс принятия решения заключается в выборе альтернативы с наилучшей пользой A_{i*}, то есть такой:

$$A_{i*}, i* \in \{1, \ldots, m\} \mid N_{i*j} = \max_i N_{ij}. \quad (2)$$

В условиях неопределенности робот R_i не уверен в текущем состоянии окружающей среды, но предполагает вероятности нахождения в определенном состоянии. В этом случае робот R_i будет выбирать лучшее состояние, основываясь на текущих данных в процессе исследования внешней среды. На протяжении всей фазы исследования робот считывает и накапливает знания об альтернативах, из которых он может получить вероятность P_i преобладания альтернативы A_i. Поэтому роботы могут предпринимать действия, основываясь на трех обобщённых стратегиях [5]: осторожной (роботы не принимают решение только когда полностью не исследуют среду), рискованной (роботы принимают решение при ДК, даже если не исследовали всю среду) и комбинированной (роботы принимают решение только тогда, когда исследован заданный заранее процент от площади среды). В качестве стратегии КПР в данном исследовании использовалась рискованная стратегия, при которой, робот выбирает:

$$A_{i*}, i* \in \{1, \ldots, m\} \mid N_{i*j} = \max_i \max_j N_{ij}. \quad (3)$$

Согласно рискованной стратегии предполагаемое наилучшее возможное состояние j с максимальным качеством P_i максимизируется по всем возможным альтернативам i.

В качестве правила принятия решений в статье рассматривается модель большинства. Подробно модель большинства описана в статьях [32-34]. Робот R_i проверяет свою группу окрестностей G_i и подсчитывает P_i для каждой A_i. Затем робот переключает свое мнение на наиболее частый вариант:

$$A_{i*}, i* = \arg\max P_i. \quad (4)$$

Таким образом, робот R_i меняет выбранную им альтернативу A_{i*} на альтернативу, выбранную большинством роботов в группе G_i, которые имеют локальную связь с R_i.

Модель вредоносных роботов

Отталкиваясь от общей модели КПР, согласно работам [5, 14] можно выделить 3 типа стратегий ВР:

– ВР с случайной стратегией поведения (ССП);
– ВР с оппозиционной стратегией поведения (ОСП);
– ВР с координированной стратегией поведения (КСП).

Предлагаемая общая классификация рассматриваемых в данной работе возможных стратегий воздействия ВР на процесс КПР представлена на рис. 2.

Рис. 2. Классификация типов ВР по стратегии воздействия на процесс КПР в РРТС

Необходимость рассматривать различные стратегии ВР при их выявлении заключается в значительном отличии влияния ВР разных типов на процесс КПР. Использование классификации, а не простого порога отклонения при выявлении ВР позволит более эффективно учитывать специфику конкретного ВР при дальнейших разработках методов противодействия. Стоит отметить, что вредоносное поведение робота может быть не преднамеренным и являться следствием поломки или ошибок в системе управления. Таким образом, классификация позволит упростить процедуру реагирования на подобные инциденты в реальных приложениях РРТС.

Стратегия ВР с ССП может быть формализована как:

$$N_{i^*j} = \text{rand}\, N_{ij}, \tag{5}$$

где N_{ij} – полезность каждой альтернативы A_i и состояния S_j, а функция *rand* генерирует случайное целое число i в диапазоне от 1 до m и случайное целое j в диапазоне от 1 до n, таким образом с равной вероятностью для голосования выбирается случайное значение из матрицы полезности N_{ij}. Полезность N_{ij} определяется качеством P_i, рассчитанным на основе исследования среды. Данная стратегия поведения ВР характеризуется тем, что ВР выбирает на каждом ходу процесса КПР в качестве A_{i*} случайно выбранную альтернативу A_i. Такое поведение часто может быть следствием поломки или загрязнением сенсоров РРТС.

ВР с ОСП можно формализовано описать как:

$$N_{i^*j} = \min_i \max_j N_{ij}, \tag{6}$$

характеризующуюся тем, что ВР выбирают минимально возможное качество P_i (т.е. предполагаемое наихудшее возможное состояние j) из всех возможных альтернатив A_i. Данная стратегия поведения ВР характеризуется тем, что ВР поддерживают альтернативу, которая имеет наименьшую полезность в данный

момент времени, т.е. предполагаемое наихудшее возможное состояние S_j максимизируют по всем возможным альтернативам A_i.

ВР с КСП можно формализовать следующим образом:

$$N_{i^*j} = \max_i \max_j N_{ij}^{BP}. \quad (7)$$

где N_{ij}^{BP} – матрица полезности ВР с КСП. Данная стратегия поведения ВР характеризуется тем, что ВР выбирают альтернативу A_{i*} согласно своей вредоносной матрицы полезности N_{ij}^{BP}. Главное отличие КСП от предыдущих случаев заключается в том, что ВР с КСП имеют глобальную предустановку в виде своей матрицы полезности N_{ij}^{BP}. В КСП в отличие от ОСП решение не обязательно должно быть с минимальной полезностью, а выбор происходит в пользу A_{i*} всеми ВР с КСП. Таким образом, наихудшая полезность относительно G_i при $A_i>2$ и наличии ВР с ОСП может отличаться от другой локальной группы G_i, в то время как ВР с КСП имеет глобальную предустановку в выборе определенной A_{i*} всегда и при любых условиях.

Сценарий КПР и условия среды моделирования

Исследование процесса КПР рассматривалось на примере сценария коллективного восприятия, постановка которого описана в работе [33].

Цель РРТС состоит в том, чтобы принять коллективное решение и выбрать на основе данных о внешней среде одну из нескольких альтернатив A_i (голосование за то, что определенный цвет преобладает на сцене) при наличии некоторого количества ВР такую, что выполняется условие (3). Альтернативами A_i в данном случае служат цвета на некоторой сцене, раскрашенной плитками. Альтернативы представлены клеточками для удобства расчета сложности экспериментов, считывание альтернатив отдельно взятым роботом происходит непрерывно при движении из расчета того, что в течение всего времени выполнения процедуры исследования робот подсчитывает время, в течение которого наблюдалась альтернатива, оценивая таким образом насколько часто она встречается на сцене. В текущем исследовании рассматриваются случаи с количеством цветов от двух до пяти (белый, черный, красный, синий, зеленый).

Мерой измерения сложности выполнения задачи РРТС взято соотношение между наиболее распространённым цветом (во всех проводимых экспериментах в рамках данной статьи – белый цвет) и прочими плитками на сцене. Сложность задачи можно варьировать, изменяя соотношение между процентами белых плиток и других цветов. В простой задаче разница между процентом белых и других плиток должна быть велика. Если один из признаков среды явно преобладает, например: P_1=0,72*;* P_2=P_3=P_4=P_5=0,07, сложность составит примерно 0,1. В сложной задаче, напротив, разница невелика. Например, в самой сложной задаче, при равновероятном распределении всех признаков среды P_1=P_2=P_3=P_4=P_5=0,2, сложность составит 1. Если сложность задана таким образом, что ее невозможно отобразить целыми клеточками, то остаток клеточек не учитывается и для удобства окрашивается в другой цвет, который не распозна-

ется алгоритмами работы РРТС в данном сценарии (в данном исследовании малиновый цвет).

Сцена проведения эксперимента (среда) представляет собой комнату, ограниченную 4 стенками и размером S_{scene}=4 м^2, в текущих экспериментах среда квадратная с длинной каждой стенки 2 м. Группа РРТС состоит из 20 роботов e-puck [35], перемещающихся по поверхности, размеченной цветными клетками, и способных воспринимать цвет поверхности под ними через градиент серого цвета. Роботы имеют диаметр 7 см, колесную платформу с максимальной скоростью движения 13 см/с, RGB светодиодную подсветку, 8 датчиков приближения, датчик определения цвета поверхности, а также модуль для локального обмена информацией. Роботы могут общаться друг с другом только в том случае, если расстояние между роботами для имитации физических ограничений связи в РРТС меньше, чем d=22 см.

В начале эксперимента генерируется сцена заданной сложности со случайным расположением цветов, и роботы случайным образом размещаются внутри арены. Пример начальных конфигураций эксперимента с высокой сложностью для S_{scene}=4 м^2, 20 роботами и 5 цветами приведен на рис. 3.

Траектория движения каждого робота представляется ломаной линией – робот чередует движение по прямой и вращение на месте. Направление вращения и движение также выбирается случайным образом. Кроме того, каждый робот оснащён дальномером, позволяющим определять расстояние до других роботов и препятствий. При появлении препятствия в поле зрения робот разворачивается и продолжает движение в противоположную сторону от препятствия.

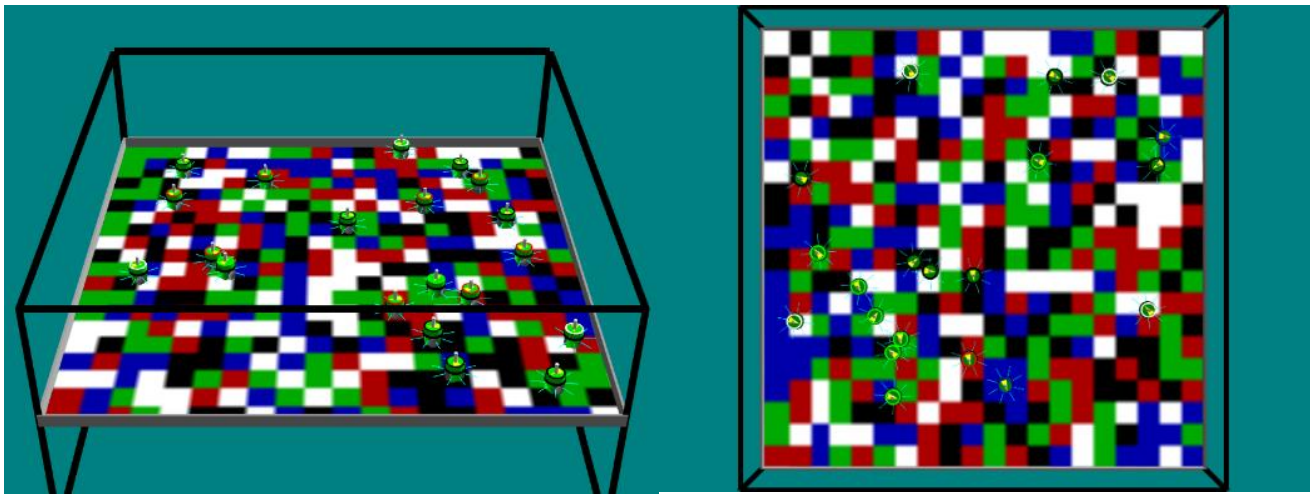

Рис. 3. Пример экспериментальной сцены с 5 альтернативами

В конце экспериментального запуска РРТС сформирует решение о том, какой цвет преобладает на сцене. Переход от данных, получаемых всеми обычными роботами (ОР) о цвете отдельных плиток ко всей экспериментальной сцене происходит с помощью процесса КПР по модели большинства (4) с рискованной стратегией (3). При этом в настоящей работе обеспечение «одинаковости» результатов съема информации об одном и том же участке полигона не учитывается, так как в рассматриваемом сценарии в классической постановке

[33] при рискованной стратегии принятия решения [5] точное позиционирования и управление строем не используются.

Постановка задачи

В данной работе рассматриваются вопросы ИБ в РРТС со следующими ограничениями:

1. РРТС является полностью гомогенной, возможность подключения робота со значительно большими вычислительными ресурсами не рассматривается. Эта проблема при применении предлагаемого подхода может быть решена дополнительным сравнением косвенных признаков в доверительном интервале [17].
2. В РРТС должна быть возможность масштабирования в процессе работы, т.е. роботы могут подключаться и отключаться в течение работы, при этом вновь прибывшие роботы сразу записываются в очередное обновление локальной копии реестра.
3. Вопросы ИБ ограничены процессом КПР и относятся к стадии исследования, т.е. ограничены рассмотрением «Византийской отказоустойчивостью». Т.е., при решении задачи не указываются причины возникновения вредоносного поведения. Вредоносное поведение может быть, как целенаправленной атакой, так и ошибкой, вызванной выходом из строя сенсоров робота РРТС. Исследование не затрагивает стадии распространения мнений и стадию смены мнений, проблемы на этих стадиях при применении предлагаемого подхода выявления ВР. К примеру, генерация пустых сущностей и подделка данных в реестре могут быть решены двумя путями: применением репутационных моделей [36] и методов, основанных на применении технологии блокчейн [7, 8]. Модификация метода-прототипа решений данной работы [37] с применением технологии блокчейн представлена в статье [38].
4. В работе изучается вопрос выявления ВР, противодействие выявленному воздействию ВР требует дополнительных исследований. В данной работе противодействие ВР ограничивается простой блокировкой данных выявленных ВР.
5. Для выявления ВР могут быть использованы только параметры, характеризующие процесс КПР. Это ограничение необходимо для исключения воздействий среды и влияния различий аппаратных платформ.
6. Приемлемый уровень ИБ ДК в процессе КПР согласно базовой постановки задачи о «Византийской отказоустойчивости» [9], должен обеспечиваться до тех пор, пока минимум 1/3 ОР РРТС не является ВР.

Гипотеза исследования состоит в том, что ВР, имея отличную от ОР стратегию поведения, не учитывает в полной мере признаки внешней среды и информацию от других роботов, а значит, подобный робот R_i будет исследовать среду и выбирать A_{i*} с характерными особенностями для каждого типа ВР. При этом его степень уверенности Y_{R_i} в выборе альтернативы A_{i*} окажется отличной

от ОР, работающего корректно при ДК в РРТС относительно наилучшей альтернативы.

Пусть дана РРТС, функционирующая в некоторой среде, состоящая из m роботов $R_i \in \{R_1, R_2, \ldots, R_m\}$, где каждый робот R_i представлен в виде набора параметров, хранящихся в его локальной копии распределённого реестра и представляющих собой набор данных, участвующий в процессе КПР. Каждого робота R_i РРТС можно отнести к одному из классов

$$RT \in \{RT_0, RT_1, \ldots, RT_k\}, \quad (8)$$

где RT_0– ОР, RT_1– ВР с ССП, RT_2 – ВР с КСП, RT_3 – ВР с ОСП.

Для выявления ВР необходимо каждому R_i поставить в соответствие некоторое значение критерия степень уверенности Y_{R_i} и определить Y_{abn}, (abnormal) – критерий аномальности фазы исследования и выбора лучшей альтернативы A_{i*} роботом R_i при ДК в процессе КПР в РРТС. Y_{abn} демонстрирует насколько нормально протекает процесс КПР в РРТС. Параметр Y_{abn} предназначен для соотнесения робота R_i к одному из одному из вредоносных типов $RT_{1\text{-}3}$, на основе отличия показателей предполагаемого ВР от среднего значения показателя $Y_{R_{cp}} T_0$ – роботов функционирующих нормально, т.е. класса RT_0.

Таким образом, задачу выявления ВР в РРТС на основе данных процесса КПР можно сформулировать следующим образом. Необходимо определить для робота R_i параметр степень уверенности и сравнить его с аналогичным параметром множества роботов G_i, которые имеют локальную связь с R_i. На основе показателя аномальной степени уверенности Y_{abn}, рассчитываемого как:

$$Y_{abn} = Y_{R_{cp}} T_0 - Y_{R_i}, \quad (9)$$

следует соотнести R_i к одному из классов $RT_k \mid \forall R_i \exists! k, R_i \in RT_k$ с учетом ограничений 1)-6) при выполнении РРТС целевой функции (3) выбора альтернативы A_{i*} с наивысшей пользой N_{i*j}.

Предлагаемый метод

Предлагаемый метод выявления ВР на основе данных процесса КПР в РРТС (РРСУ – распределенный реестр со степенью уверенности) основан на комплексном применении нескольких методах обеспечения ИБ в РРТС:

- методов, основанных на применении распределенного реестра;
- методов, основанных на анализе трафика и поведения.

Суть метода-аналога относительно группы ТРР [7] заключается в применении технологии блокчейн для обеспечения ИБ в РРТС. Выявление ВР осуществляется через смарт-контракт с помощью проверки соответствия голоса за цвет и сохраненному мнению в цепочке блоков. Схожими признаками с аналогом являются применение технологий распределенного реестра для ДК в процессе КПР, а также механизм игнорирования выявленных ВР. Выявление ВР происходит за счет использования смарт-контракта, который обнаруживает несоответствие, когда робот голосует за цвет, отличный от того, который был согласован в процессе консенсуса. При обнаружении ВР его открытый ключ добавляется в черный список в цепочке блоков и в дальнейшем КПР голоса

этого робота игнорируются до конца проведения эксперимента. Однако, при этом не учитываются возможность различных стратегий поведения ВР и рассматриваются ВР, которые всегда голосует за альтернативу с меньшим качеством. Вместе с тем возможна такая ситуация, когда сенсоры робота вышли из строя и робот выполняет подсчет голосов неверно, например, сенсоры загрязнились и воспринимают белый цвет как черный. В этом случае выбор A_i при ДК может оказаться ошибочным, однако несоответствие выбранной альтернативы сохраненному мнению в цепочке транзакций блокчейна выявлено не будет. Отличием предлагаемого метода РРСУ, позволяющего избежать указанную проблему, является применение в РРСУ степени уверенности робота в выборе альтернативы. Использование критерия степени уверенности позволит учесть вредоносное поведение, вызванное поломкой, поскольку данная метрика характеризует насколько робот часто изменял свое мнение в процессе КПР.

Суть метода-аналога [17] относительно группы методов поведенческого анализа состоит в обнаружении несоответствия между текущим режимом работы РРТС и штатной моделью поведения данного алгоритма, «портрета». Метод выявления деструктивного воздействия на РРТС на основе косвенных характеристик предполагает изменение некоторых косвенных параметров группы (например, скорость снижения уровня заряда батареи, скорость достижения РРТС поставленной задачи), которое можно оценить до начала выполнения алгоритма. Однако на практике такие показатели могут иметь недостаток, заключающийся в различиях аппаратной реализации или погрешности из-за нахождения части роботов РРТС G_i в других условия окружающей среды. Например, часть роботов может оказаться на сцене покрытой отличной поверхностью, что может привести к отличию в скорости и расходуемого заряда батареи и будет расценено как отклонение от «портрета».

Отличием предлагаемого метода РРСУ, позволяющим избежать указанную проблему, является использование не косвенных признаков, а признаков, характеризующих протекание ДК в процессе КПР, который не имеет зависимостей от физической реализации и воздействий внешней среды.

Предлагаемый в статье метод РРСУ является модификацией метода-прототипа DL [37]. Он вносит изменение в реализацию процесса КПР путем добавления в распределенной базы данных (БД) метрики критерия степени уверенности, которая рассчитывается на основе данных ДК при КПР и используется для выявления ВР.

Блок-схема предлагаемого метода представлена на рис. 4. Входными данными метода являются измерения сенсоров РРТС, выходными данными является выбор альтернативы РРТС. Предлагаемый метод РРСУ вносит изменения в этапы процесса КПР и добавляет процедуру расчета степени уверенности (блок «расчет уверенности» на рис. 4), позволяет выявить аномалии (блок «сравнение уверенности» и блок «обнаружение ВР» на рис. 4) и исключить выявленные ВР (блок «блокировка ВР» на рис. 4).

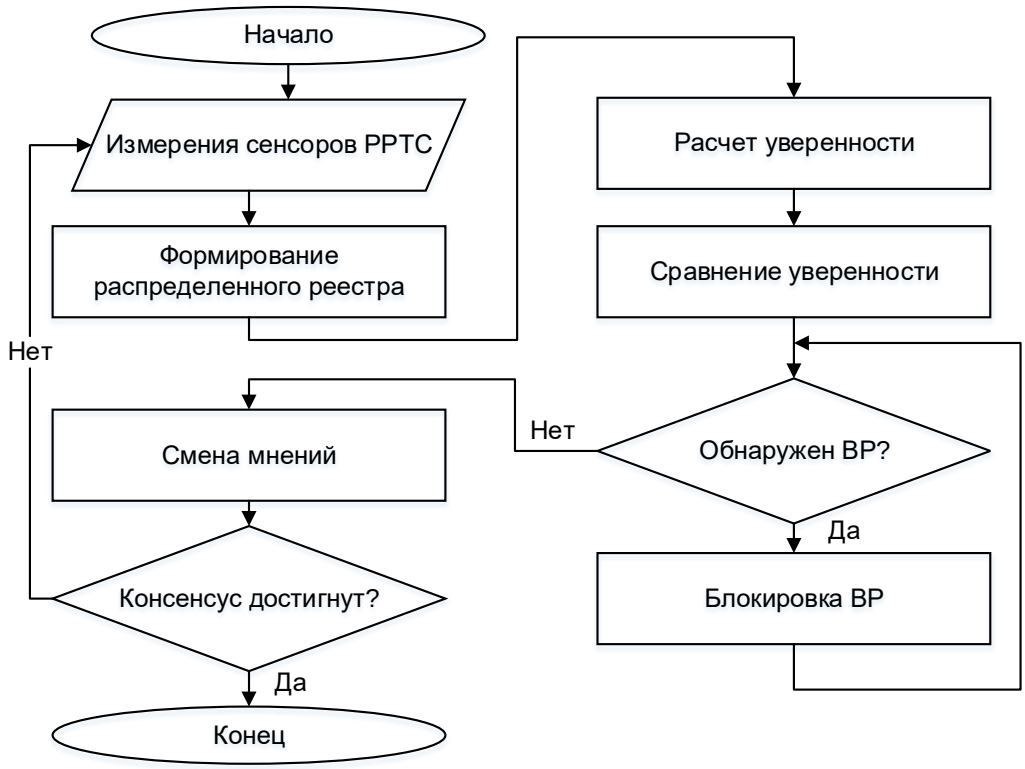

Рис. 4. Блок-схема метода РРСУ выявления ВР
на основе данных процесса КПР в РРТС

Блок «измерения сенсоров РРТС». Каждый робот R_i выполняет исследование среды и ведет подсчёт признаков альтернатив A_i и записывает их качество P_i в свою локальную БД, структура локальной БД робота приведена на рис. 5.

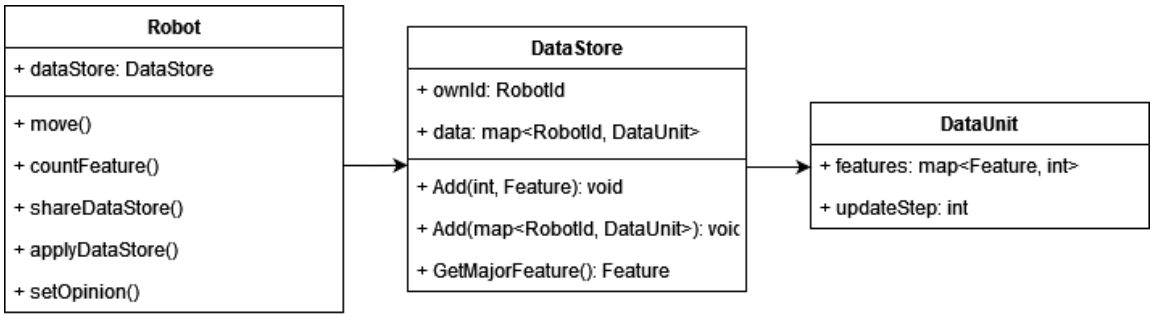

Рис. 5. Структура локальной БД робота

В состоянии исследования робот R_i анализирует среду путем выполнения процедур случайного движения и, при необходимости, обхода препятствия. В то же время робот выполняет процедуру оценки альтернативы A_i. В процессе выполнения процедуры оценки альтернативы A_i робот использует сенсор поверхности для сбора информации о качестве P_i представленных альтернатив. В течение всего времени T выполнения процедуры исследования робот подсчитывает время τ_i, в течение которого наблюдалась альтернатива A_i.

По итогу выполнения процедуры оценки вычисляется качество P_i альтернативы A_i:

$$P_i = \frac{\tau_i}{T}. \quad (10)$$

По итогу выполнения процедуры оценки отдельный робот принимает решение о том, какая альтернатива преобладает в среде.

Блок «формирование распределенного реестра». Робот R_i при встрече с другим роботом из множества роботов G_i, которые имеют с ним локальную связь и на протяжении времени сохранения локальной связи, выполняет процедуру распространения накопленной БД (DataStore). Распространение происходит путем деления БД на блоки данных, соответствующих каждому отдельному роботу R_i (DataUnit) и отправки этих блоков другим роботам. Приняв DataUnit, робот R_i должен обновить соответствующий блок у себя в БД (DataStore) только в том случае, если метка времени принятого блока (updateStep) актуальнее уже имеющихся блоков в БД, а также в случае, если соответствующий локальный блок не найден. Таким образом, через некоторое время с начала работы у большинства роботов в группе накапливается и обновляется распределенная БД измерений других роботов.

Блок «расчет уверенности». Уверенность Y_{R_i} робота R_i в выборе A_{i*} рассчитывается по формуле:

$$Y_{R_i} = \frac{1 - P_i^{\max}}{(m-1)(P_i^{\max})}, \quad (11)$$

где i – порядковый номер альтернативы, P_i – процентное соотношение i-й альтернативы в среде, $P_i^{\max}$ – процентное соотношение наиболее распространённой альтернативы A_{i*} в среде, т.е. имеющей наибольшее качество. В случае равного распределения нескольких альтернатив A_i в качестве $P_i^{\max}$ можно выбрать любую из них.

Степень уверенности робота $Y_{R_i} \in [0, 1]$, где 0 означает полную уверенность R_i в выборе A_{i*}, а 1 полную неуверенность (случайный выбор). Уверенность показывает, какое соотношение в качестве альтернатив получилось для текущего шага процесса КПР, т.е. только по уже исследованным РРТС областям и то насколько часто работ меняет свое мнение при голосовании.

Блок «сравнение уверенности». Аномалия определяется как отклонение степени уверенности Y_{R_i} предполагаемого ВР от средней уверенности нормально функционирующих роботов $Y_{R_{cp}T_0}$ по формуле (9). На основании значения Y_{abn} полученного по формуле (9) принимается решение об отнесении робота к одному из классов: $R_i \in RT_k$ и его дальнейшей блокировке, согласно выражению:

$$\begin{cases} \left(Y_{\text{abn}} \to 0\right) \leftrightarrow \left(k = 0\right), \\ \left(Y_{\text{abn}} < 0\right) \leftrightarrow \left(k = 1\right), \\ \left(Y_{\text{abn}} = Y_{R_{\text{cp}}T_0}\right) \leftrightarrow \left(k = 2\right), \\ \textit{otherwise} \ \ \left(k = 3\right). \end{cases} \quad (12)$$

Оператор *otherwise* выполняет функцию иного выбора – в случае если робот не принадлежит к классам $RT_{0\text{-}2}$, то он считается классом RT_3.

Блок «обнаружен ВР?». В случае если $k = 0$, выполняется блок «смены мнений» на рис. 4, в ином случае – блок «блокировки ВР» на рис. 4.

Блок «блокировки ВР». В случае обнаружения ВР выполняется его блокировка и все данные, накопленные ВР, исключатся из общей матрицы полезности N и не принимают участие при реализации блока «смены мнений».

Блок «смены мнений». Робот проверяет свою версию БД и подсчитывает вхождение P_i для каждой A_i. Затем робот переключает свое мнение на наиболее частую альтернативу по правилу (4), т.е. на A_{i*} большинства своих соседей G_i согласно данным распределенной БД. В случае равенства разных A_i выбирается случайное из них.

Блок «консенсус достигнут?». После смены мнения робот R_i сигнализирует о своем мнении (о наиболее распространенной альтернативе A_{i*}) и подсчитывает голоса и при наличии 100% сигнализирующих ОР за альтернативу A_{i*} процесс КПР завершается, иначе РРТС возвращается к исследованию среды (блок «измерения сенсоров РРТС», на рис. 4).

Экспериментальные исследования степени уверенности роботов

Для апробации предложенного метода была выполнена его программная реализация на языке программирования C++. Эксперименты проводились с использованием имитационной среды ARGoS [39] и метода ДК, описанного в [37]. Для моделирования и выполнения широкого набора экспериментальных исследований разработан модуль для среды ARGoS, который доступен по ссылке [40]. При проведении симуляции был использован компьютер с характеристиками: процессор Intel Core i7-8550U 1.8GHz, 8Gb RAM. Использованы параметры моделирования, указанные в таблице 2.

Таблица 2 – Параметры моделирования

Наименование параметра	Значение
Количество роботов в РРТС	20
Максимальная скорость движения	10 см/с
Количество альтернатив доступных для выбора	2; 5
Площадь среды S_{scene}	4 м^2
Количество ВР с ОСП	0-9
Количество ВР с ССП	0-9
Количество ВР с КСП	0-9
Альтернатива для подсчета	белый
Количество роботов необходимое для ДК (кворум)	100% ОР

№3. 2022
ISSN 2410-9916

Для доказательства возможности применения степени уверенности для выявления ВР были проведены экспериментальные исследования в задачах с бинарным выбором и доступными для выбора пятью A_i.

Цель первого эксперимента состоит в оценке степени уверенности при минимальных условиях задачи КПР: бинарном выборе, т.е. выборе одного из двух доступных альтернатив $A_i \in \{A_1, A_2\}$.

Проведены 2 серии экспериментов: с высокой сложностью 1 (50:50) и низкой сложность 0,33 (75:25). Каждая серия представляет собой по 100 экспериментов при двух альтернативах для 17 ОР, и по одному ВР на каждый рассматриваемый тип ВР. Усредненные показатели исследования по 100 экспериментам приведены на рис. 6 и 7. Графики на рис. 6 и 7, демонстрирует среднее значение уверенности Y отдельных роботов РРТС, взятое по 100 экспериментальным прогонам в зависимости от времени (шага) процесса КПР.

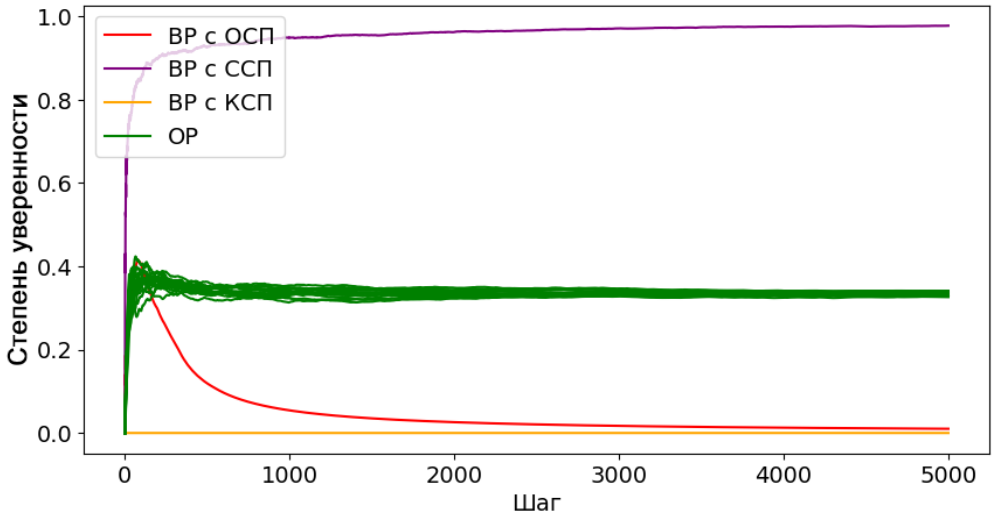

Рис. 6. Зависимость степени уверенности от шага процесса КПР при бинарном выборе, сложность 0,33 (75:25)

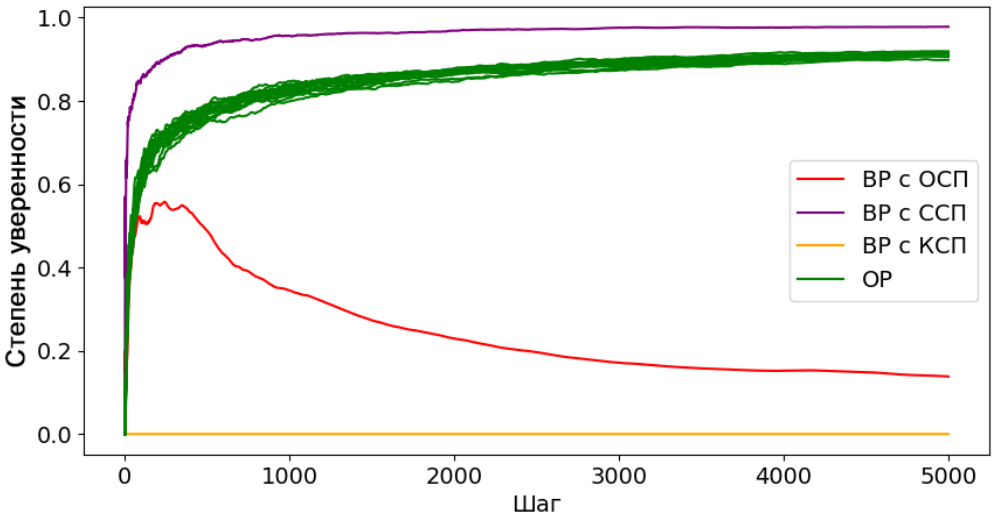

Рис. 7. Зависимость степени уверенности от шага процесса КПР при бинарном выборе, сложность 1 (50:50)

DOI: 10.24412/2410-9916-2022-3-105-137
URL: https://sccs.intelgr.com/archive/2022-03/06-Ryabtsev.pdf

Результаты оценивались как изменение степени уверенности *Y*: ВР с ОСП, ВР с ССП, ВР с КСП в процентном соотношении относительно значений, полученных для ОР в этом же эксперименте. Численные значения отличия степени уверенности ОР от ВР разных типов приведены в таблице 3.

Таблица 3 – Отличие степени уверенности ОР от ВР разных типов при бинарном выборе

Критерий сравнения	Шаг	Стратегия поведения вредоносного робота					
		оппозиционная		случайная		координированная	
		сложность		сложность		сложность	
		1	0,66	1	0,66	1	0,66
Отличие $Y_{R_{cp}T_0}$ от $Y_{R_mT_{1-3}}$ (%)	1000	-58,46	-83,89	15,24	181,60	-100,00	-100,00
	2000	-73,67	-92,24	11,32	187,69	-100,00	-100,00
	3000	-80,78	-94,92	9,63	189,15	-100,00	-100,00
	4000	-83,11	-96,20	8,45	191,47	-100,00	-100,00
	5000	-84,65	-96,98	8,68	191,93	-100,00	-100,00
	Среднее	-76,13	-92,85	10,66	188,37	-100,00	-100,00

Значения в таблице 3 со знаком минус демонстрируют значение степени уверенности меньшее, чем у ОР на указанную величину; значения без знака минус, напротив, демонстрируют большую степень уверенности. Значение изменения степени уверенности ВР с КСП обусловлено степенью уверенности, равной 0. При бинарном выборе ОСП с течением времени становится похожим на КСП. Это связано с тем, что с накоплением данных о качестве P_i альтернативы P_i роботы в РРТС все чаще будут голосовать за альтернативу с наибольшей полезностью N_{ij}, а, следовательно, ВР с ОСП будет всегда выбирать вторую альтернативу. Результаты проведенных экспериментов демонстрируют значительное отличие степени уверенности ВР от ОР.

Цель второго эксперимента состоит в оценке степени уверенности при увеличении количества признаков исследуемой среды: выборе одной из пяти доступных альтернатив: $A_i \in \{A_1, A_2, A_3, A_4, A_5\}$. Результаты исследования приведены на рис. 8 и 9.

Проведены 2 серии экспериментов: с высокой сложностью 1 (20:20:20:20:20) и низкой сложностью 0,66 (40:15:15:15:15). Каждая серия состоит из 100 запусков при 5 альтернативах для 17 ОР и по одному каждого типа ВР. Результаты оценивались как изменение $Y_{R_{cp}T_0}$ от $Y_{R_iT_{1-3}}$ в процентном соотношении относительно значений, полученных для ОР в этом же эксперименте.

Численные значения отличия степени уверенности ОР от ВР разных типов приведены в таблице 4.

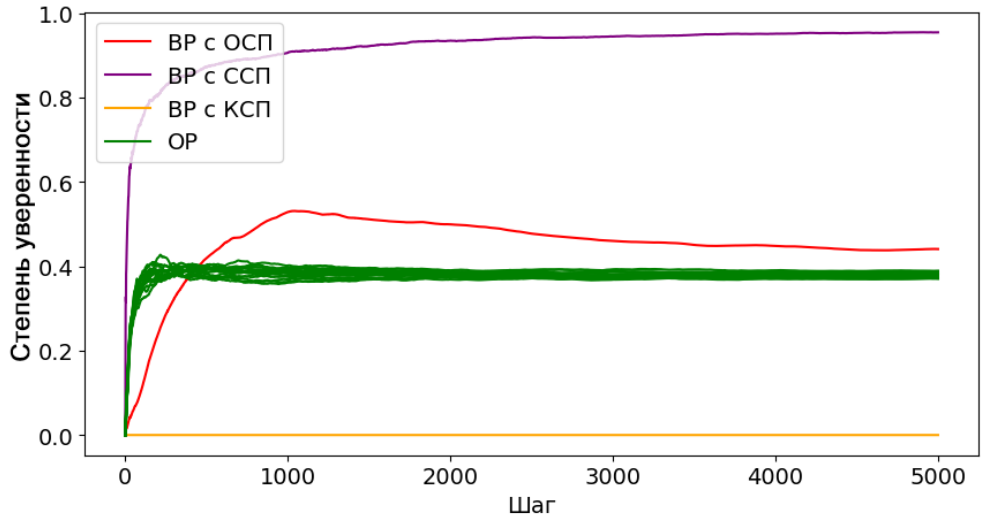

Рис. 8. Зависимость степени уверенности от шага процесса КПР при выборе из 5 альтернатив, сложность 0,66 (40:15:15:15:15)

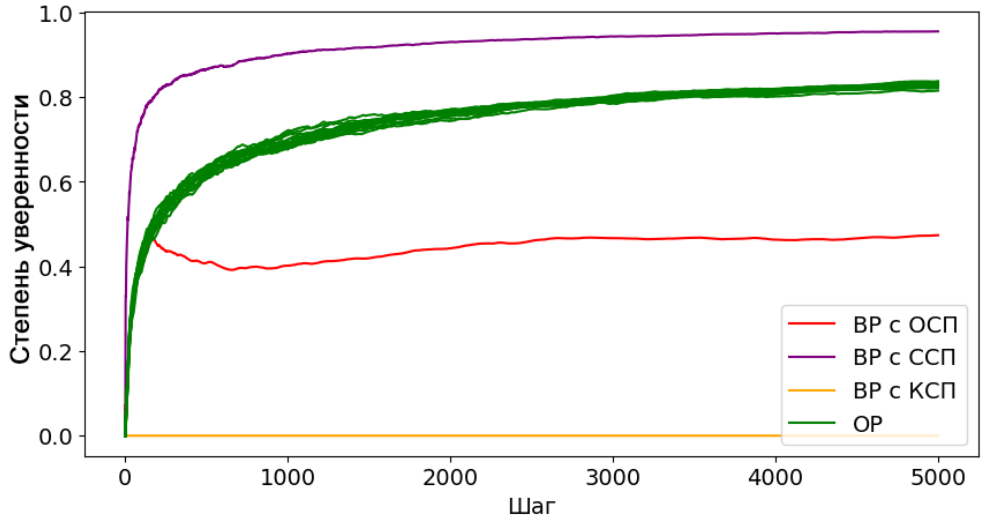

Рис. 9. Зависимость степени уверенности от шага процесса КПР при выборе из 5 альтернатив, сложность 1 (20:20:20:20:20)

Таблица 4 – Отличие степени уверенности ОР от ВР разных типов при выборе из 5 альтернатив

Критерий сравнения	Шаг	Стратегия поведения вредоносного робота					
		оппозиционная		случайная		координированная	
		сложность		сложность		сложность	
		1	0,66	1	0,66	1	0,66
Отличие $Y_{R_{cp}T_0}$ от $Y_{R_mT_{1-3}}$ (%)	1000	-41,78	37,81	30,80	136,31	-100,00	-100,00
	2000	-41,75	31,36	22,42	145,87	-100,00	-100,00
	3000	-41,59	21,53	17,95	149,64	-100,00	-100,00
	4000	-42,79	18,61	17,38	151,69	-100,00	-100,00
	5000	-42,93	16,84	15,12	152,98	-100,00	-100,00
	Среднее	-42,17	25,23	20,74	147,30	-100,00	-100,00

Согласно полученным результатам в ходе экспериментальных исследований степени уверенности *Y* можно сделать следующие выводы:

1. ВР с КСП имеет степень уверенности равную 0, это означает, что данный тип вредоносного поведения всегда голосует за выбранную заранее альтернативу и не учитывает информацию от других роботов и внешней среды.
2. ВР с ССП имеет высокий показатель степени уверенности, это демонстрирует, что данный тип вредоносного поведения голосует случайным образом постоянно меня альтернативу для выбора.
3. ВР с ОСП является наиболее трудным случаем для обнаружения, такая стратегия предполагает голосование против большинства и в отличии от КСП не голосует за определенную альтернативу, а выбирает наименее распространенную альтернативу. Учитывая локальные ограничения по связи в РРТС, ВР с ОСП будет голосовать против локального большинства в своей окрестности G_i, а не глобального. Этот факт затрудняет обнаружение такого типа ВР с помощью предлагаемого метода РРСУ на некоторых задачах, однако, учитывая полученные экспериментально показатели отклонения от отдельного взятого робота, предлагаемый критерий возможно применять для выявления ВР с ОСП.

Указанные факты и значительное отличие степени уверенности ОР от ВР по результатам проведенных экспериментальных исследований подтверждают выдвинутую гипотезу о том, что предлагаемый критерий степень уверенности робота в выборе альтернативы может служить значением аномальности протекания процесса КПР в РРТС. Таким образом, предлагаемый критерий выявления ВР – степень уверенности, может служить критерием аномального протекания процесса КПР в РРТС.

Результаты исследования метода

Для оценки уровня ИБ в РРТС за счет выявления ВР на основе данных процесса КПР без использования дополнительных признаков было выполнено экспериментальное исследование, включающее в себя два этапа. На первом этапе выполнено сравнение метода-прототипа с распределенным реестром: «distributed ledger» (DL) [37], разработанного раннее и не учитывающего проблемы ИБ, с вновь предложенными решениями. На втором этапе выполнено сравнение с методом-аналогом, использующим в качестве правила принятия решений модель большинства с технологией блокчейн: «direct modulation of majority-based decisions with blockchain approach» (DMMD BA) [7].

Цель первого эксперимента состояла в оценке эффективности ДК в процессе КПР в РРТС при использовании предлагаемых решений – метода РРСУ. Результаты моделирования приведены на рис. 10.

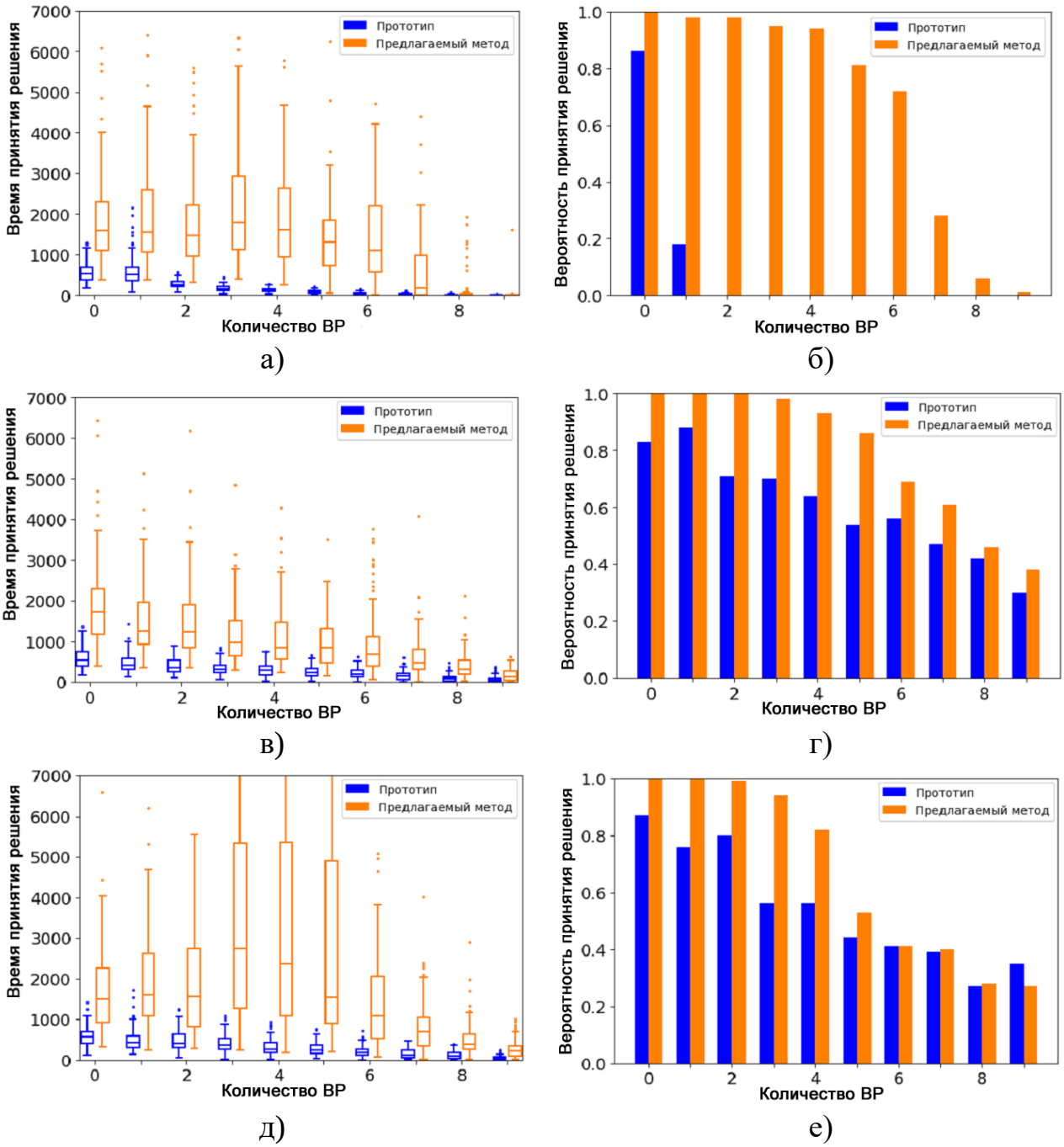

Рис. 10. Зависимость времени (а, в, д) и вероятности (б, г, е) принятия решения РРТС при использовании DL и РРСУ при наличии ВР с КСП (а, б), ВР с ССП (в, г) и ВР с ОСП (д, е)

Для оценки уровня ИБ на РРТС используется метрика изменения эффективности РРТС при выполнении задачи при наличии ВР по сравнению с выполнением такой же задачи без присутствия ВР. В качестве показателей эффективности КПР РРТС использованы следующие общепринятые показатели [7, 8]:

– вероятность E_N (%) принятия решения, характеризующаяся вероятностью ДК в РРТС относительно наилучшей альтернативы в процессе КПР;
– время $T_N^{correct}$ (шаг) принятия решения, характеризующееся количеством шагов процесса КПР, которое требуется РРТС, для ДК. Показа-

тель $T_N^{correct}$ рассчитывается по всем экспериментальным сериям, сходящимся к белому цвету. Цепочки КПР, сходящиеся к любой другой альтернативе, не учитываются.

Данный эксперимент проводился среде с 5 доступными для выбора альтернативами $A_i \in \{A_1, A_2, A_3, A_4, A_5\}$, при сложности 0,85 (23:19:19:19:19). Выполнена серия экспериментов по 100 экспериментальных прогонов для ВР в количестве от 0 до 9 (всего 900 экспериментов).

Результаты эксперимента демонстрируют значительный прирост E_N, однако снижают скорость принятия решения $T_N^{correct}$. Можно сделать вывод о том, что предлагаемый метод РРСУ увеличивает вероятность ДК в РРТС относительно наилучшей альтернативы в процессе КПР при наличии ВР. Полученные численные значения оценки приведены в таблице 5.

Оценка эффективности проводилась для РРТС, состоящей из 20 роботов, при наличии ВР, не превышающем 45% от общего числа роботов. Прирост значения E_N вероятности принятия наилучшего решения по сравнению с методом-прототипом демонстрирует повышение вероятности принятия наилучшего решения при наличии ВР разных типов: 57% при наличии ВР с КСП; 12% при наличии ВР с ОСП; 19% при наличии ВР с ССП.

Таблица 5 – Оценка эффективности РРТС при использовании РРСУ относительно DL

Кол-во вредоносных роботов	Стратегия поведения вредоносного робота					
	оппозиционная		оппозиционная		оппозиционная	
	сложность		сложность		сложность	
	время принятия (шаг)	вероятность принятия (%)	время принятия (шаг)	вероятность принятия (%)	время принятия (шаг)	вероятность принятия (%)
0	381,87	0,13	422,16	0,17	362,63	0,14
1	396,44	0,24	292,36	0,12	357,34	0,80
2	133,99	0,19	247,41	0,29	301,64	0,98
3	127,04	0,38	190,83	0,28	403,48	0,95
4	-33,91	0,26	65,65	0,29	446,53	0,94
5	9,19	0,09	32,52	0,32	147,59	0,81
6	3,97	0,00	3,75	0,13	-5,50	0,72
7	6,15	0,01	-3,70	0,14	-2,18	0,28
8	2,15	0,01	-0,70	0,04	-0,11	0,06
9	0,00	-0,08	0,02	0,08	-0,04	0,01

Цель второго эксперимента заключалась в оценке эффективности РРТС при использовании предлагаемого метода РРСУ относительно метода-аналога DMMD BA при полностью идентичных условиях.

В данном эксперименте были изменены некоторые параметры среды: d=22 см, $A_i \in \{A_1, A_2\}$. В качестве ВР рассматривается ВР с КСП. Изменения необходимы для соответствия параметрам моделирования в методе-аналоге [7]. Проведена серия экспериментов: со сложностью (0,52), представляющая из себя по 50 прогонов для ВР от 0 до 9 (всего 450 экспериментов). Сравнение про-

водилось только по метрике E_N, поскольку применение технологии блокчейн значительно увеличивает $T_N^{correct}$, но предоставляет дополнительный функционал, который не рассматривался в данной работе. Результаты исследований приведены на рис. 11.

Изменение вероятности ДК E_N отслеживалось относительно значений метода DMMD BA при идентичных условиях для количества ВР с КСП от 0 до 9. Численные значения изменения вероятности E_N ДК в РРТС относительно наилучшей альтернативы в процессе КПР приведены в таблице 6.

Результаты эксперимента позволяют утверждать о повышении вероятности E_N ДК в РРТС относительно наилучшей альтернативы в процессе КПР. Однако, имеется спад эффективности при наличии большого числа ВР – 9, тем не менее, условие наличия не более 1/3 ВР в РРТС соблюдается. Для РРТС, состоящей из 20 роботов, при наличии ВР не превышающем 45% от общего числа роботов, прирост значения вероятности принятия наилучшего решения E_N с применением метода выявления ВР на основе данных процесса КПР в РРТС, составил в среднем 20%.

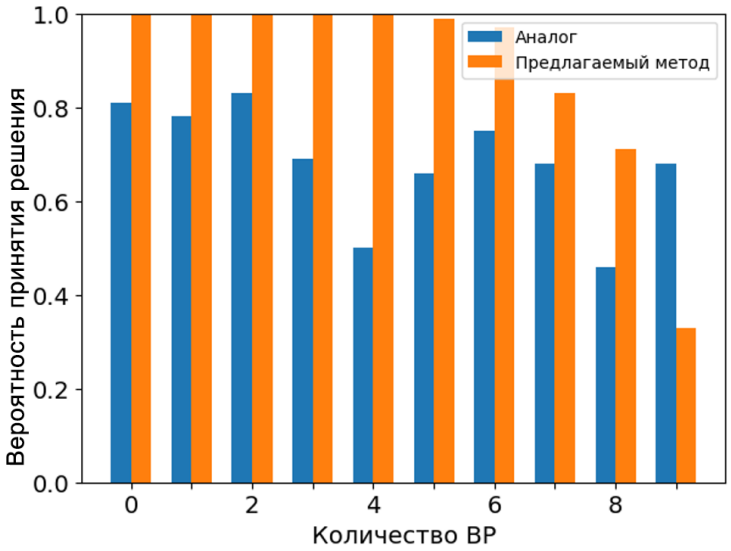

Рис. 11. Зависимость эффективности процесса КПР в РРТС от наличия ВР при использовании DMMD BA и РРСУ

Таблица 6 – Оценка эффективности РРТС при использовании РРСУ относительно DMMD BA

Кол-во вредоносных роботов	0	1	2	3	4	5	6	7	8	9
Изменение вероятности принятия наилучшего решения (%)	0,19	0,22	0,17	0,31	0,50	0,33	0,22	0,15	0,25	-0,35

Как следует из рис. 11 и таблицы 6 применение предлагаемого метода РРСУ обеспечивает более высокое значение вероятности принятия наилучшего решения E_N РРТС в процессе КПР при наличии ВР за счет выявления на основе применения степени уверенности.

Заключение

В данной работе рассматриваются задачи обнаружения воздействия со стороны ВР на ДК при КПР в РРТС. В работе представлен метод к выявлению ВР с разными стратегиями поведения, основанный на применении степени уверенности робота в выборе альтернативы при ДК в РРТС. Результаты проведенных экспериментальных исследований подтверждают выдвинутую гипотезу о том, что предлагаемый критерий степень уверенности робота в выборе альтернативы может служить значением аномальности процесса КПР в РРТС.

Проведенные экспериментальные исследования позволили выявить значительное отличия степеней уверенности ОР от ВР. Использование предлагаемого метода РРСУ выявления ВР на основе данных процесса КПР в РРТС – позволяет повысить вероятность принятия наилучшего решения по сравнению с методом-аналогом: для РРТС из 20 роботов при наличии ВР, не превышающем 45% от числа ОР в среднем на 20%. По сравнению с методом-прототипом и его модификации, представленной в данной статье, демонстрируется повышение вероятности принятия наилучшего решения при наличии ВР трех типов, не превышающем 45% от числа ОР, на: 57% при наличии ВР с КСП; 12% при наличии ВР с ОСП; 19% при наличии ВР с ССП.

Новизной предлагаемого метода является использование выявления ВР не косвенных признаков, а признака, характеризующего протекание процесса КПР – степени уверенности робота в выборе альтернативы, которая не имеет зависимостей от физической реализации РРТС и воздействий внешней среды. Преимуществами метода являются учет большого числа альтернатив и возможных стратегий ВР. Предлагаемый метод может служить основой для разработки более сложных механизмов обеспечения ИБ в РРТС, однако имеет ряд вопросов, устранение которых определяет будущие направления работы в данной области:

1. В сложных задачах с особыми случаями среды, например, «шахматная доска» или «пешеходный переход» и равным соотношением признаков, близким равновероятному распределению, распределение ОР будет сильно схожим с распределением ВР. Этот факт может вызвать ложные срабатывания при выявлении ВР при длительной работе РРТС.
2. При быстро протекающем процессе КПР в РРТС (например, легких задачах, которые могут быстро завершаться) может сложиться ситуация с недостаточным количеством данных для принятия решения об блокировке ВР. Т.к. явные отличия ВР от ОР могут начать наблюдаться после выполнения некоторого количества шагов процесса КПР. Кроме того, существуют области, на которых степень уверенности ВР будет пересекаться со степенью уверенности ОР. Указанные факты затрудняют задачу своевременного выявления ВР.

Разработанный метод предполагает непрерывное выполнение на протяжении всего времени функционирования РРТС. Областью практического использования данного метода являются задачи, при которых необходимо обес-

печить приемлемый уровень ИБ КПР при наличии ВР, а также требующие продолжительного выполнения, например, мониторинг местности, поиск объектов, наблюдение и т.д.

К будущим направлениям работы следует отнести проведение экспериментальных исследований на физически воплощенных роботах и разработку более сложных механизмов блокировки и противодействия выявленным ВР, с учетом предложенной классификации ВР.

Исследование выполнено при финансовой поддержке Минобрнауки России (грант ИБ), проект № 10/2020.

Литература

1. Beni G., Wang J. Swarm Intelligence in Cellular Robotic Systems // Robots and Biological Systems: Towards a New Bionics. Berlin, Heidelberg: Springer. 1993. P. 703-712. doi: 10.1007/978-3-642-58069-7_38.

2. Dudek G., Jenkin M. R. M., Milios E., Wilkes D. A taxonomy for multi-agent robotics // Autonomous Robots. 1996. Vol. 3. № 4. P. 375-397.

3. Zakiev A., Tsoy T., Magid E. Swarm Robotics: Remarks on Terminology and Classification // Lecture notes in computer science. 2018. Vol. 11097. P. 291-300. doi: 10.1007/978-3-319-99582-3_30.

4. Dorigo M., Theraulaz G., Trianni V. Reflections on the future of swarm robotics Science Robotics // American Association for the Advancement of Science. 2020. Vol. 5. № 49. P. 1-3. doi: 10.1126/scirobotics.abe4385.

5. Hamann H. Swarm Robotics: A Formal Approach. – Springer International Publishing, New York City, 2018. – 210 p.

6. 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. Т. 5. № 87. С. 149-154.

7. Strobel V., Ferrer E. C., Dorigo M. Managing Byzantine Robots via Blockchain Technology in a Swarm Robotics Collective Decision Making Scenario: Robotics track // International Conference on Autonomous Agents and Multiagent Systems. 2018. Vol. 1. P. 541-549.

8. 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.

9. Lamport L., Shostak R., Pease M. The Byzantine Generals Problem // ACM Transactions on Programming Languages and Systems. 1982. Vol. 4. № 3. P. 382-401.

10. Stallings W. Network and Internetwork Security Principles and Practice. – Prentice Hall, Englewood Cliffs, NJ, 1995. – 462 p.

11. 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. № 2. P. 288-297.

12. Sargeant I., Tomlinson A. Review of Potential Attacks on Robotic Swarms // Proceedings of SAI Intelligent Systems Conference. 2018. P. 628-646. doi: 10.1007/978-3-319-56991-8_46.

13. 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.

14. Canciani F., Talamali M. S., Marshall J. A. R., Reina A. Keep calm and vote on: Swarm resiliency in collective decision making // International Conference on Robotics and Automation. 2019. – URL: https://www.cl.cam.ac.uk/~asp45/icra2019/papers/Canciani.pdf (дата обращения: 07.11.2021).

15. Tebueva F. B., Ryabtsev S. S., Struchkov I. V. A method of counteracting Byzantine robots with a random behavior strategy during collective design-making in swarm robotic systems // E3S Web of Conferences. 2021. Vol. 270. doi: 10.1051/e3sconf/202127001034.

16. Юрьева Р. А., Комаров И. И., Викснин И. И. Иммунологические принципы принятия решения в мультиагентных робототехнических системах // Глобальный научный потенциал. 2015. Т. 5. № 50. С. 87-91.

17. 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.

18. Basan E. S., Basan A. S., Makarevich O. B. Evaluating and Detecting Internal Attacks in a Mobile Robotic Network // International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery. IEEE. 2018. P. 516-518. doi: 10.1109/CyberC.2018.00102.

19. Sargeant I., Tomlinson A. Intrusion Detection in Robotic Swarms // Proceedings of SAI Intelligent Systems Conference. 2020. P. 968-980. doi: 10.1007/978-3-030-29513-4_71.

20. Басан Е. С. Разработка системы управления защитой беспроводной сенсорной сети на основе доверия. Дис. … канд. техн. наук. – Таганрог: ЮФУ, 2016. – 161 с.

21. Zikratov I. A., Lebedev I. S., Gurtov A. V. Trust and Reputation Mechanisms for Multi-agent Robotic Systems // International Conference on Next Generation Wired/Wireless Networking: Internet of Things, Smart Spaces, and Next Generation Networks and Systems. 2014. Vol. 8638. P. 106-120. doi: 10.1007/978-3-319-10353-2_10.

22. Basan A. S., Basan E. A., Makarevich O. B. Analysis of ways to secure group control for autonomous mobile robots // Proceedings of the 10th International Conference on Security of Information and Networks. 2017. P. 134-139. doi: 10.1145/3136825.3136879.

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. Т. 3. № 91. С. 30-38.

24. Зикратов И. А., Зикратова Т. В., Лебедев И. С. Доверительная модель информационной безопасности мультиагентных робототехнических систем с децентрализованным управлением // Научно-технический вестник информационных технологий, механики и оптики. 2014. Т. 2. № 90. С. 47-52.

25. Zikratov I. A. Lebedev I. S., Gurtov A. V. Kuzmich E. V. Securing swarm intellect robots with a police office model // International Conference on Application of Information and Communication Technologies. 2014. P. 1-5. doi: 10.1109/ICAICT.2014.7035906.

26. Зикратов И. А., Гуртов А. В., Зикратова Т. В., Козлова Е. В. Совершенствование police office model для обеспечения безопасности роевых робототехнических систем // Научно-технический вестник информационных технологий, механики и оптики. 2014. Т. 5. № 93. С. 99-109.

27. Beskopylny A., Lysenko A., Garanin E. Blockchain in Robotic Distributed Multi-Level Systems // Advances in Robotics & Mechanical Engineering. 2018. Vol. 1. № 4. P. 59-61. doi: 10.32474/ARME.2018.01.000116.

28. Nguyen T. T., Hatua A., Sung H. A. Blockchain Approach to Solve Collective Decision Making Problems for Swarm Robotics // International Congress on Blockchain and Applications. 2020. Vol. 1010. P. 118-125. doi: 10.1007/978-3-030-23813-1_1527.

29. Calderón-Arce C., Brenes-Torres J. C., Solis-Ortega R. Swarm Robotics: Simulators, Platforms and Applications Review // Computation. 2022. Vol. 6. № 10. P. 1-15. doi: 10.3390/computation10060080.

30. Navarro I., Matía F. An Introduction to Swarm Robotics // International Scholarly Research Notices Robotics. 2013. Vol. 1. P. 1-10. doi: 10.5402/2013/608164.

31. Valentini G. Self-Organized Collective Decision Making: The Weighted Voter Model // Proceedings of the 2014 international conference on Autonomous agents and multi-agent systems. 2014. P. 1703–1704.

32. Valentini G., Hamann H., Dorigo M. Efficient Decision-Making in a Self-Organizing Robot Swarm: On the Speed Versus Accuracy Trade-Off // Proceedings of the 14th International Conference on Autonomous Agents and Multiagent Systems. 2015. Vol. 2. P. 1305-1314.

33. Valentini G., Brambilla D., Hamann H., Dorigo M. Collective perception of environmental features in a robot swarm // International Conference on Swarm Intelligence 2016. Vol. 9882. P. 65-76. doi: 10.1007/978-3-319-44427-7_6.

34. Valentini G., Ferrante E., Hamann H., Dorigo M. Collective decision with 100 Kilobots: speed versus accuracy in binary discrimination problems // Autonomous Agents and Multi-Agent Systems. 2016. Vol. 30. P. 553-580. doi: 10.1007/s10458-015-9323-3.

35. Проект e-puck Сайт разработчиков робота e-puck [Электронный ресурс]. 28.10.2021. – URL: http://www.e-puck.org/ (дата обращения: 28.10.2021).

36. Басан Е. С., Басан А. С., Макаревич О. Б. Разработка и реализация метода обнаружения аномального поведения узлов в группе роботов // Безопасность информационных технологий. 2018. Т. 25. № 4. С. 75-85. doi: http://dx.doi.org/10.26583/bit.2018.4.07.

37. Petrenko V. I., Tebueva F. B., Ryabtsev S. S., Gurchinsky M. M., Struchkov I. V. Consensus achievement method for a robotic swarm about the most frequently feature of an environment // IOP Conference Series: Materials Science and Engineering. 2020. Vol. 919. № 4. P. 1-8. doi: 10.1088/1757-899x/919/4/042025

38. Petrenko V. I., Tebueva F. B., Ryabtsev S. S., Gurchinsky M. M., Struchkov I. V. Consensus achievement method for a robotic swarm about the most frequently feature of an environment based on blockchain technology // IOP Conference Series: Materials Science and Engineering. 2021. Vol. 1069. no. 1. P. 1-8. DOI: 10.1088/1757-899X/1069/1/012044.

39. Pinciroli C., Trianni V., O'Grady R., Pini G., Brutschy A., Brambilla M., Mathews N., Ferrante E., Caro G. D., Ducatelle F., Birattari M., Gambardella L., Dorigo M. ARGoS: A modular, parallel, multi-engine simulator for multi-robot systems // Swarm Intelligence. 2012. Vol. 6. № 4. P. 271-295. doi: 10.1007/s11721-012-0072-5.

40. Ncfu pmkb, swarm-robotics GitLab – веб-инструмент жизненного цикла DevOps [Электронный ресурс]. 05.11.2021. – URL: https://gitlab.com/pmkb/swarm-robotics (дата обращения: 05.11.2021).

References

1. Beni G., Wang J. Swarm Intelligence in Cellular Robotic Systems. *Robots and Biological Systems: Towards a New Bionics. Berlin, Heidelberg: Springer*, 1993, pp. 703-712. doi: 10.1007/978-3-642-58069-7_38.

2. Dudek G., Jenkin M. R. M., Milios E., Wilkes D. A taxonomy for multi-agent robotics. *Autonomous Robots*, 1996, vol. 3, no. 4, pp. 375-397.

3. Zakiev A., Tsoy T., Magid E. Swarm Robotics: Remarks on Terminology and Classification. *Lecture notes in computer science*, 2018, vol. 11097, pp. 291-300. doi: 10.1007/978-3-319-99582-3_30.

4. Dorigo M., Theraulaz G., Trianni V. Reflections on the future of swarm robotics Science Robotics. *American Association for the Advancement of Science*, 2020, vol. 5, no 49, pp. 1-3. doi: 10.1126/scirobotics.abe4385.

5. Hamann H. *Swarm Robotics: A Formal Approach.* Springer International Publishing, New York City, 2018. 210 p.

6. Zikratov I. A., Kozlova E. V., Zikratova T. V. Analiz uyazvimostej robototekhnicheskih kompleksov s roevym intellektom [Vulnerability analysis of robotic systems with swarm intelligence]. *Scientific and technical journal of information technologies, mechanics and optics*, 2013, vol. 5, no. 87, pp. 149-154 (In Russian).

7. Strobel V., Ferrer E. C., Dorigo M. Managing Byzantine Robots via Blockchain Technology in a Swarm Robotics Collective Decision Making Scenario: Robotics track. *International Conference on Autonomous Agents and Multiagent Systems*, 2018, vol. 1, pp. 541-549.

8. 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, pp. 54. Doi:10.3389/frobt.2020.00054.

9. Lamport L., Shostak R., Pease M. The Byzantine Generals Problem. *ACM Transactions on Programming Languages and Systems*, 1982, vol. 4, no. 3, pp. 382-401.

10. Stallings W. *Network and Internetwork Security Principles and Practice.* Prentice Hall, Englewood Cliffs, NJ, 1995. 462 p.

11. 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, pp. 288-297.

12. Sargeant I., Tomlinson A. Review of Potential Attacks on Robotic Swarms. *Proceedings of SAI Intelligent Systems Conference*, 2018, pp. 628-646. doi: 10.1007/978-3-319-56991-8_46.

13. Komarov I. I., Iureva R. A., Drannik A. L., Maslennikov O. S., Kovalenko M. E., Egorov D. A. Issledovanie destruktivnogo vozdejstviya robotov-zloumyshlennikov na effektivnost' raboty mul'tiagentnoj sistemy [Study of destructive impact of attackers robots on the efficiency of the multi-agent system]. *Control processes and stability*, 2014, vol. 1, no. 1, pp. 336-340 (In Russian).

14. Canciani F., Talamali M. S., Marshall J. A. R., Reina A. Keep calm and vote on: Swarm resiliency in collective decision making. *International Conference on Robotics and Automation*, 2019. Available at: https://www.cl.cam.ac.uk/~asp45/icra2019/papers/Canciani.pdf (дата обращения: 07.11.2021).

15. Tebueva F. B., Ryabtsev S. S., Struchkov I. V. A method of counteracting Byzantine robots with a random behavior strategy during collective design-making in swarm robotic systems. *E3S Web of Conferences*, 2021, vol. 270, doi: 10.1051/e3sconf/202127001034.

16. Iureva R. A., Komarov I. I., Viksnin I. I. Immunologicheskie principy prinyatiya resheniya v mul'tiagentnyh robototekhnicheskih sistemah [Immunological principles for making a decision in multi-agent robotic systems]. *Global scientific potential*, 2015, vol. 5, no. 50, pp. 87-91 (In Russian).

17. Iureva R. A., Komarov I. I., Maslennikov O. S. Razrabotka metoda obnaruzheniya i identifikacii skrytogo destruktivnogo vozdejstviya na mul'tiagentnye robototekhnicheskie sistemy [Development of a method for detecting and identifying a hidden destructive impact on multi-agent robotic systems]. *Software systems and computational methods*, 2016, no. 4, pp. 375-382, doi: 10.7256/2305-6061.2016.4.21128 (In Russian).

18. Basan E. S., Basan A. S., Makarevich O. B. Evaluating and Detecting Internal Attacks in a Mobile Robotic Network. *International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery. IEEE*, 2018, pp. 516-518. doi: 10.1109/CyberC.2018.00102.

19. Sargeant I., Tomlinson A. Intrusion Detection in Robotic Swarms. *Proceedings of SAI Intelligent Systems Conference*, 2020, pp. 968-980. doi: 10.1007/978-3-030-29513-4_71.

20. Basan E. S. *Razrabotka sistemy upravleniia zashchitoi besprovodnoi sensornoi seti na osnove doveriia*. Diss. kand. tehn. nauk [The Development of a Trust-Based Wireless Sensor Network Security Management System. Ph.D. Tesis]. Taganrog, South Federal University, 2016. 161 p. (In Russian).

21. Zikratov I. A., Lebedev I. S., Gurtov A. V. Trust and Reputation Mechanisms for Multi-agent Robotic Systems. *International Conference on Next Generation Wired/Wireless Networking: Internet of Things, Smart Spaces, and Next Generation Networks and Systems*, 2014, vol. 8638, pp. 106-120. doi: 10.1007/978-3-319-10353-2_10.

22. Basan A. S., Basan E. A., Makarevich O. B. Analysis of ways to secure group control for autonomous mobile robots. *Proceedings of the 10th International Conference on Security of Information and Networks*, 2017, pp. 134-139. doi: 10.1145/3136825.3136879.

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, vol. 3, no. 91, pp. 30-38 (In Russian).

24. Zikratov I. A., Zikratova T. V., Lebedev I. S. Trust model for information security of multi-agent robotic systems with a decentralized management. Scientific and *Technical Journal of Information Technologies, Mechanics and Optics*, 2014, vol. 2, no. 90, pp. 47-52 (In Russian).

25. Zikratov I. A. Lebedev I. S., Gurtov A. V., Kuzmich E. V. Securing swarm intellect robots with a police office model. *International Conference on Application of Information and Communication Technologies*, 2014, pp. 1-5. doi: 10.1109/ICAICT.2014.7035906.

26. Zikratov I. A., Gurtov A. V., Zikratova T. V., Kozlova E. V. Police office model improvement for security of swarm robotic systems. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2014, vol. 5, no. 93, pp. 99-109 (In Russian).

27. Beskopylny A., Lysenko A., Garanin E. Blockchain in Robotic Distributed Multi-Level Systems. *Advances in Robotics & Mechanical Engineering*, 2018, vol. 1, № 4, pp. 59-61. doi: 10.32474/ARME.2018.01.000116.

28. Nguyen T. T., Hatua A., Sung H. A. Blockchain Approach to Solve Collective Decision Making Problems for Swarm Robotics. *International Congress on Blockchain and Applications*, 2020, vol. 1010, pp. 118-125. doi: 10.1007/978-3-030-23813-1_1527.

29. Calderón-Arce C., Brenes-Torres J. C., Solis-Ortega R. Swarm Robotics: Simulators, Platforms and Applications Review. *Computation*, 2022, vol. 6, no. 10, pp. 1-15. doi: 10.3390/computation10060080.

30. Navarro I., Matía F. An Introduction to Swarm Robotics. *International Scholarly Research Notices Robotics*, 2013, vol. 1, pp. 1-10. doi: 10.5402/2013/608164.

31. Valentini G. Self-Organized Collective Decision Making: The Weighted Voter Model. *Proceedings of the 2014 international conference on Autonomous agents and multi-agent systems*, 2014, pp. 1703–1704.

32. Valentini G., Hamann H., Dorigo M. Efficient Decision-Making in a Self-Organizing Robot Swarm: On the Speed Versus Accuracy Trade-Off. *Proceedings of the 14th International Conference on Autonomous Agents and Multiagent Systems*, 2015, vol. 2, pp. 1305-1314.

33. Valentini G., Brambilla D., Hamann H., Dorigo M. Collective perception of environmental features in a robot swarm. *International Conference on Swarm Intelligence*, 2016, vol. 9882, pp. 65-76. doi: 10.1007/978-3-319-44427-7_6.

34. Valentini G., Ferrante E., Hamann H., Dorigo M. Collective decision with 100 Kilobots: speed versus accuracy in binary discrimination problems. *Autonomous Agents and Multi-Agent Systems*, 2016, vol. 30, pp. 553-580. doi: 10.1007/s10458-015-9323-3.

35. E-puck education robot. E-puck robot developers website, 28 October 2021. Available at: http://www.e-puck.org/ (accessed: 28 October 2021).

36. Basan E. S., Basan A. S., Makarevich O. B. Development and implementation of a method to detect an abnormal behavior of nodes in a group of robots. IT Security (Russia). 2018, vol. 25, no. 4, pp. 75-85, doi: http://dx.doi.org/10.26583/bit.2018.4.07 (In Russian).

37. Petrenko V. I., Tebueva F. B., Ryabtsev S. S., Gurchinsky M. M., Struchkov I. V. Consensus achievement method for a robotic swarm about the most frequently feature of an environment. *IOP Conference Series: Materials Science and Engineering*, 2020, vol. 919, no 4, pp. 1-8. doi: 10.1088/1757-899x/919/4/042025.

38. Petrenko V. I., Tebueva F. B., Ryabtsev S. S., Gurchinsky M. M., Struchkov I. V. Consensus achievement method for a robotic swarm about the most frequently feature of an environment based on blockchain technology. *IOP Conference Series: Materials Science and Engineering*, 2021, vol. 1069, no. 1, pp. 1-8. DOI: 10.1088/1757-899X/1069/1/012044.

39. Pinciroli C., Trianni V., O'Grady R., Pini G., Brutschy A., Brambilla M., Mathews N., Ferrante E., Caro G. D., Ducatelle F., Birattari M., Gambardella L., Dorigo M. ARGoS: A modular, parallel, multi-engine simulator for multi-robot systems. *Swarm Intelligence*, 2012, vol. 6, no 4, pp. 271-295. doi: 10.1007/s11721-012-0072-5.

40. Ncfu pmkb, swarm-robotics, GitLab is The DevOps Platform, 05 November 2021. Available at: https://gitlab.com/pmkb/swarm-robotics (accessed: 05 November 2021).

Статья поступила 18 ноября 2021 г.

Информация об авторе

Рябцев Сергей Сергеевич – соискатель ученой степени кандидата технических наук. Старший преподаватель кафедры компьютерной безопасности. Федеральное государственное автономное образовательное учреждение высшего образования «Северо-Кавказский федеральный университет». Область научных интересов: роевые робототехнические системы, информационная безопас-

ность, коллективное принятие решений, достижение консенсуса. E–mail: nalfartorn@yandex.ru

Адрес: 355017, Россия, Ставрополь, ул. Пушкина, д. 1

A method for detecting Byzantine robots based on data from the collective decision-making process in swarm robotic systems

S. S. Ryabtsev

Problem Statement: *The critical importance of collective behavior mechanisms for the functioning of swarm robotics systems updates the issues of identifying Byzantine robots with faulty or malicious behavior, which consists in imposing inappropriate alternatives during consensus-building in collective decision-making. Known information security approaches often leave out the particulars of the implementation of swarm systems, such as collective decision-making, and use physical parameters as criteria for detecting Byzantine robots. Moreover, most studies consider the presence of malicious robots only with a behavior strategy of voting against a majority after consensus was reached.* ***The purpose of the work*** *is to increase the level of information security of swarm robotics systems, which consists in increasing the probability of reaching consensus of swarm robotics systems about the best alternative in the process of collective decision-making in the presence of Byzantine robots by identifying them based on the data of the decision chain without using additional features that depend on the conditions of operation and hardware implementation. It is proposed to use an approach based on Distributed Ledger Technology and analysis of variances in the collective decision-making process chain. Using this approach will allow detecting malicious effects from Byzantine robots, regardless of the operating conditions and hardware implementation of the swarm robotic system.* ***Methods used:*** *solving the problem of detecting malicious robots in swarm robotics systems is based on the application of the robot confidence criteria in selecting an option when consensus is reached in the process of collective decision-making in swarm robotics systems. The solution is based on the hypothesis that the distribution of confidence of the Byzantine robot due to the peculiarities of the process of collective decision making when using a malicious strategy differs significantly from the same distribution in correctly functioning robots.* ***Novelty:*** *Elements of novelty of the presented decision include: 1) using the confidence criterion to ensure information security of collective decision-making; 2) possibility to take into account various strategies for the behavior of Byzantine robots. Using the presented solution allows you to increase the efficiency of achieving consensus with a swarm robotic system in the presence of Byzantine robots. The simulation conducted for a swarm robotic system consisting of 20 robots, in the presence of Byzantine robots in an amount not exceeding 45% of the total number of robots in the system, showed an increase in the probability of making the best decision regarding the analogue method by an average of 20%. Compared to the prototype method, the proposed modification made it possible to increase the probability of making the best decision in the presence of Byzantine robots with a coordinated behavior strategy by 57%, with an oppositional behavior strategy by 12%, with a random behavior strategy by 19%.* ***Practical significance:*** *the presented solution can be implemented in the software for swarm robotics systems, which will allow increasing the likelihood of reaching consensus with the swarm robotics system about the best alternative in the collective decision-making process in the presence of robots with faulty or malicious behavior.*

Key words: *swarm robotics; information security; Byzantine robot; collective decision-making; consensus achievement; distributed ledger technology.*

Information about Author

Sergey Sergeevich Ryabtsev – Senior Lecturer at the Department of Computer Security. Federal Autonomous Educational Institution of Higher Education North Caucasus Federal University. Fields of research: swarm robotics; consensus achievement; collective decision-making; information security. E–mail: nalfartorn@yandex.ru

Address: Russia, 355017, Stavropol, Pushkina str. 1.