УДК 004.896 ISSN 1995-5499
DOI: https://doi.org/
Поступила в редакцию 30.11.2021
Подписана в печать 22.04.2022

МЕТОД ОБНАРУЖЕНИЯ НАРУШЕНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОЕВЫХ РОБОТОТЕХНИЧЕСКИХ СИСТЕМАХ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИЙ МАШИННОГО ОБУЧЕНИЯ

© 2022 В. И. Петренко, Ф. Б. Тебуева, С. С. Рябцев✉, А. С. Павлов, М. М. Гурчинский

Северо-Кавказский федеральный университет
ул. Пушкина, 1, 355017 Ставрополь, Российская Федерация

Аннотация. Интенсивное развитие роевой робототехники актуализирует вопросы обеспечения ее информационной безопасности. Известные подходы к обнаружению угроз информационной безопасности процесса коллективного принятия решений в роевых робототехнических системах используют физические параметры, которые сильно зависят от среды функционирования и аппаратной реализации системы. Поэтому трудно определить универсальные признаки аномального поведения робота, обеспечивающие точный порог отклонения и низкий процент ложных срабатываний. Целью работы является повышение эффективности достижения консенсуса в роевых робототехнических системах в условиях наличия неисправных или вредоносных роботов. Решение задачи обнаружения вредоносных роботов базируется на применении методов машинного обучения. В качестве классификатора вредоносных роботов использована искусственная нейронная сеть, обученная на наборе данных, сгенерированных с помощью разработанного ранее аналитического метода. Новизна представленного решения заключается в выборе параметров с варьируемыми значениями для проведения симуляций с целью формирования набора данных для обучения классификатора вредоносных роботов. Предложенный подход обеспечивает универсальность выявления вредоносных роботов независимо от их численности или стратегии поведения. Проведено имитационное моделирование роевой робототехнической системы, состоящей из 100 роботов. При наличии 20 % роботов с некорректным поведением, количество ложных срабатываний снижено на 41,07 % относительно метода-прототипа. Представленный метод реализован в виде программного обеспечения на языке программирования C++, которое может быть использовано при моделировании систем управления роевыми робототехническими системами.

Ключевые слова: роевые робототехнические системы, информационная безопасность, вредоносный робот, коллективное принятие решений, достижение консенсуса, машинное обучение.

ВВЕДЕНИЕ

Роевая робототехника активно внедряется в повседневную жизнь и находит свое применение во многих практических задачах: аварийно-спасательных операциях, космических полётах, военных действиях, точечном земледелии.

Одним из барьеров к широкому использованию роевых робототехнических систем (РРТС) является наличие уязвимостей с точки зрения информационной безопасности (ИБ). Постановка и классификация вопросов ИБ в РРТС, а также сравнение со схожими технологиями приведена в работе [1]. Обзор

✉ Рябцев Сергей Сергеевич
e-mail: nalfartorn@yandex.ru

возможных атак на РРТС выполнен в статье [2]. В статье [3] анализ алгоритмов функционирования роевых робототехнических систем дополняется их проверкой на устойчивость с точки зрения ИБ. В ряде работ подробно рассматриваются модели нарушителей и угроз ИБ РРТС [10, 11]. В работе [4] приведен анализ и исследование основных угроз актуальных для различных принципов, методов и особенностей группового управления РРТС. К основным механизмам атак на РРТС, формирующим угрозы, принято относить [6]:

– атаки на каналы связи;

– затруднение идентификации и аутентификации агентов в системе;

– физическое внедрение «инородных» роботов.

Однако, несмотря на наличие указанных исследований о необходимости обеспечения ИБ РРТС на практике, большинство исследований игнорируют проблемы ИБ и не учитывают вероятность того, что часть роботов может оказаться вредоносными (ВР) вследствие поломок или кибератак.

Термин ВР или «Византийский робот» используется в работах [7, 8] и применяется для общего описания роботов с непреднамеренным или непоследовательным поведением независимо от основной причины. Термин ВР берет начало из работ о проблеме «Византийских генералов» [9,10]. В практических приложениях одного или нескольких ВР может быть достаточно для нарушения работы всей РРТС.

В современных исследованиях наиболее часто в качестве ВР рассматриваются роботы, голосующие против большинства. При этом возможны разнообразные стратегии воздействия ВР на коллективное принятие решений (КПР). В данной работе на основе исследований [11, 12] рассматривается 3 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).

Угрозы для РРТС в целом не отличаются от угроз для традиционных социотехнических систем, однако существуют различия в типах атак и векторах атак. Это связано, прежде всего, со способностью манипулировать возникающим коллективным поведением РРТС путем воздействия на достижение консенсуса (ДК) в процессе КПР. Данный факт актуализирует необходимость совершенствования методов обнаружения ВР в РРТС.

Известные подходы выявления ВР в РРТС используют физические параметры, показатели которых связаны со средой функционирования РРТС и аппаратной реализацией [13, 14] (например, скорость снижения уровня заряда батареи, скорость достижения РРТС поставленной задачи). Вследствие чего трудно определить параметры аномальности с точным порогом отклонения и низким числом ложных срабатываний. Поэтому перспективным является использование методов на основе данных процесса КПР [8, 15, 16]. В работе [8] для выявления ВР используется технология блокчейн. Обнаружение ВР осуществляется через смарт-контракт с помощью процедуры проверки соответствия голоса за альтернативу и сохраненному мнению в цепочке транзакция блокчейн.

Настоящая статья является модификацией работы [15], в которой решение задачи выявления ВР в РРТС базируется на применении критерия степени уверенности робота в выборе альтернативы в процессе КПР. Процесс КПР реализован с помощью технологий распределенного реестра с моделью большинства при смене мнения роботов [17]. Данный критерий рассчитывается на основе данных КПР, обладает универсальностью и не зависит от аппаратной реализации РРТС. Однако, в предлагаемом решении используется аналитический подход к определению порога аномальности. Указанный подход имеет недостатки при динамических изменениях среды, которые связаны с необходимостью накопления некоторых сведений о процессе КПР для обнаружения ВР без ошибок.

Данные недостатки определяют возможность наличия ложных срабатываний при выявлении ВР и замедляют время принятия решений в РРТС. Настоящая работа фокусируется на совершенствовании процесса вы-

явления ВР на основе данных процесса КПР в РРТС с помощью использования технологий машинного обучения. В работе [18] приводится пример реализации и обоснование применения технологий машинного обучения в задачах обеспечения функциональной безопасности киберфизических систем, подвидом которых являются РРТС.

Целью работы является повышение эффективности процесса КПР в РРТС относительно наилучшей альтернативы в условиях наличия роботов с неисправным или вредоносным поведением за счет уменьшения количества ложных срабатываний при обнаружении ВР.

Гипотезой исследования является предположение о том, что применение методов машинного обучения позволит снизить число ложных срабатываний в процессе обнаружения ВР.

Практическая значимость представленные решений заключается в обеспечении устойчивости РРТС к воздействию на КПР со стороны роботов с неисправным или вредоносным поведением и, как следствие, повысит возможности применения РРТС в агрессивных средах.

1. ПОСТАНОВКА ЗАДАЧИ

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

1) РРТС является полностью гомогенной;

2) роботы могут подключаться и отключатся в течении работы;

3) вопросы ИБ ограничены процессом КПР и заключаются в рассмотрении «Византийской отказоустойчивости»;

4) противодействие ВР не является предметом данной работы и ограничивается простой блокировкой данных выявленных ВР.

Для оценки эффективности решений используется число ложных срабатываний F, обозначающее количества ошибочно обнаруженных ВР. Данная работа является модификацией метода выявления ВР на основе показателя уверенности робота в выборе альтернативы [15] с помощью методов машинного обучения.

В общем виде задача выявления ВР заключается в определении для робота R_i параметра степени уверенности Y_{R_i}, сравнения его с аналогичным параметром каждого робота в пределах локальной связи G_i, и расчете показателя аномальной уверенности Y_{abn}:

$$Y_{abn} = Y_{R_{cp}T_0} - Y_{R_i},$$

где $Y_{R_{cp}T_0}$ – средняя уверенность, корректно работающих роботов; Y_{R_i} – уверенность робота в пределах локальной связи.

На основании того критерия требуется соотнести R_i к одному из классов T так, что $\forall R_i \, \exists! k, \; R_i \in T_k$, где RT_0 – ОР; T_1 – ВР с ССП; T_2 – ВР с КСП, T_3 – ВР с ОСП.

Вербально постановка научной задачи может быть сформулирована следующим образом: необходимо обучить искусственную нейронную сеть (ИНС), используемую как модуль прошивки РРТС, для уменьшения числа ложных срабатываний при обнаружении ВР с сохранением или улучшением эффективности функционирования РРТС.

Формально постановка научной задачи имеет следующий вид. Необходимо получить такой метод:

$$Z : R, Y_{abn}, T, Q, F \to \Delta f_i \geq 0, \; f_i \in F,$$

где $R = \{R_1, R_2, \ldots, R_m\}$ – РРТС численностью m; Q – множество рассматриваемых критериев оценки функционирования РРТС; изменение числа ложных срабатываний $\Delta f_i = f_i^n - f_i^\partial$, где индекс «д» значит «до использования предложенных решений, индекс «п» – «после использования предложенных решений». При ограничениях 1–4 и сохранения условия ДК относительно наилучшей альтернативы.

2. МЕТОДЫ И МАТЕРИАЛЫ

2.1. Экспериментальная установка и среда моделирования

Для исследований ИБ процесса КПР рассматривался сценарий коллективного восприятия РРТС [19] внешней среды (сцены).

На абстрактном уровне целью РРТС в данном сценарии является определение выбора наилучшего решения, т.е. альтернативы

$A_{\hat{i}}$ из множества доступных альтернатив A_m. Каждая альтернатива $A_i \in \{A_1, ..., A_m\}$ характеризуется качеством $P_i \in (0,1]$ [20], мерой того, насколько распространён признак внешней среды (сцены). Альтернативами в данном случае являются цвета, в которые окрашены области на сцене, а качеством служит время, в течение которого робот наблюдал определенный цвет. В подавляющем большинстве современных исследований подобные вопросы рассматривают на бинарной черно-белой сцене. В текущем исследовании рассматриваются случаи с большим количеством цветов: от двух до пяти (белый, черный, красный, синий, зеленый). В сценарии коллективного восприятия цель РРТС состоит в том, чтобы принять коллективное решение и выбрать на основе данных о внешней среде одно из нескольких действий A_i (голосование за цвет i) при наличии некоторого количества ВР.

В качестве меры измерения сложности выполнения РРТС задачи используется соотношение между наиболее распространённым цветом и прочими плитками на сцене, данное соотношение выбрано ввиду необходимости сопоставления сложности задачи с двумя цветами задачам с большим числом цветов. 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 распознается алгоритмами работы РРТС. Сложность задачи можно варьировать, изменяя соотношение между процентами белых плиток и других цветов. В простой задаче разница между процентом белых и черных плиток должна быть велика. Например, если $P_1 = 0,72$ и $P_2 = P_3 = P_4 = P_5 = 0,07$, то сложность составит $0,1$. В сложной задаче, напротив, разница невелика. Например, в самой сложной задаче для пяти цветов, при их равновероятном распределении: $P_1 = P_2 = P_3 = P_4 = P_5 = 0,2$, сложность составит единицу.

Для проведения экспериментов использована имитационная среда ARGoS. Разработан модуль для моделирования задач с большим количеством цветов и масштабированием среды, код которого доступен по ссылке [21]. Сцена проведения эксперимента представляет собой комнату, ограниченную 4 стенками и размером $S_{scene} = x \times x$ $м^2$. Группировка РРТС состоит из $R = 20$ роботов e-puck [22], 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 10 см/с, RGB светодиодную подсветку, 8 датчиков приближения, датчик определения цвета поверхности, а также модуль для локального обмена информацией, состоящий из 12 ИК приемопередатчиков. Роботы могут общаться друг с другом только в том случае, если расстояние между роботами меньше, чем $d_n = 22$ см, для имитации физических ограничений РРТС. Траектория движения каждого робота представляет ломаную линию, робот при этом 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.

В начале эксперимента генерируется сцена заданной сложности со случайным расположением цветов, роботы случайным образом размещаются внутри арены. Задача роботов в ходе эксперимента состоит в том, чтобы достичь общего мнения относительно преобладания количества областей, окрашенных в один цвет при наличии некоторого количества ВР с различными стратегиями поведения. В конце успешного запуска все отдельно взятые роботы РРТС будут иметь одинаковое мнение, соответствующее наиболее часто встречающемуся цвету. Условием выхода из эксперимента, т.е. условием ДК, является достижение кворума в 100 % от числа всех роботов, функционирующих нормально. По окончанию эксперимента РРТС достигает коллективного мнения о наиболее частом цвете на сцене (во всех проведенных в рамках этой работы экспериментах – белом цвете).

2.2. Метод выявления вредоносных роботов с использованием технологий машинного обучения

На рис. 1 представлена структура данных сообщений, которые передаются между агентами PPTC в используемой среде моделирования Argos.

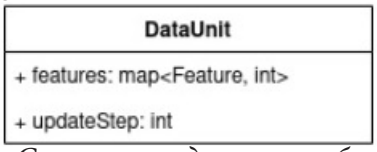

Рис 1. Структура данных сообщений, передаваемых между агентами PPTC [Fig 1. Structure of messages transmitted between agents]

Поле «Признаки» (features) содержит ассоциативный массив, где ключами являются цвета (Feature), которые робот r_i зафиксировал в процессе функционирования с использованием бортовых датчиков и сенсоров, а значениями – продолжительность наблюдений каждого из цветов, т. е. целочисленное количество дискретных моментов времени t, соответствующих интервалам между соседними моментами срабатывания бортовых устройств управления. Остальные поля, представленные на рис. 1, используются в процессе КПР между агентами PPTC.

Основная идея метода-прототипа заключается в получении сообщения с описанной структурой данных от соседнего агента и расчета показателя степени уверенности Y_{r_i} аналитически по формуле [15]. Недостатком данного подхода является отсутствие нормализации данных, которые используются в расчетах. Например, возможна ситуация, когда в среде цвета распределены неравномерно, вследствие чего агент № 1 зафиксировал несколько цветов, а агент № 2 – только один. Тогда показатель степени уверенности робота r_1 относительно робота r_2 может превысить допустимый порог и робот № 2 ложно будет считаться ВР и окажется заблокированным. С целью минимизации влияния подобных аномалий в данной работе предлагается использование ИНС в качестве классификатора ВР.

Подготовку обучающей выборки предлагается осуществлять путем сбора данных, полученных в результате проведения серии экспериментов с использованием разработанного ранее метода-прототипа при следующих параметрах экспериментов:

1) стратегия вредоносного поведения;

2) масштаб M исследуемой внешней среды;

3) устойчивость случайного мнения;

4) количество признаков внешней среды;

5) процентное соотношение ВР к обычным роботам.

Под стратегией ВР понимается правило, по которому ВР считывают признаки внешней среды и выбирают альтернативу для голосования в процессе КПР. Наиболее часто в качестве ВР в литературе рассматриваются роботы, голосующие против большинства в задачах с бинарным выбором. Вместе с тем в реальной практике применения PPTC возможны разнообразные стратегии воздействий ВР на процесс КПР. Предлагается к рассмотрению три типа ВР:

1) ВР с случайной стратегией поведения (ССП) – голосование за случайную альтернативу;

2) ВР с оппозиционной стратегией поведения (ОСП) – голосование против большинства;

3) ВР с координированной стратегией поведения (КСП) – голосование за определённую альтернативу.

В качестве масштаба среды используется характеристика – плотность покрытия сцены M роботами, характеризующаяся соотношением размера арены и площади покрытия сенсоров роботов и рассчитываемая как:

$$M = \frac{S_{scene}}{R_m \times S_{d_n}},$$

где M – плотность покрытия сцены роботами; S_{scene} – площадь сцены; R_m – количество роботов; $S_{d_n} = \pi \times d_n^2$ – площадь покрытия сцены сенсорами 1 робота.

Таким образом, $M \sim 1$ – означает достаточность количества роботов для равномерного заполнения всей сцены, $M < 1$ – означает высокую плотность покрытия сцены сенсорами роботов, а $M > 1$ – низкую. Плотность

сцены $M = 1,32$ является стандартной (аналогично другим исследованиям по данной тематике) для данной работы плотности роботов: 20 роботов на сцене 2×2.

Устойчивость случайного мнения представляет собой периодичность, с которой обновляется массив данных. В случае, если этот шаг равен 0, то массив обновляется только один раз при генерации сцены и имеет максимально возможную устойчивость; если шаг равен 1, то массив обновляется каждый ход (получается более случайные результаты); если шаг равен 10, то массив обновляется раз в 10 ходов.

Количество признаков внешней среды показывает число альтернатив A_i (цветов), доступных для выбора роботам при ДК. В работах-аналогах применяется бинарный выбор. Вместе с тем, в реальной практике применения РРТС возможны задачи, связанные с выбором из большого числа доступных альтернатив. Настоящее исследование проводилось на задачах от 2 до 5 альтернатив для выбора не только задач с бинарным выбором, но и задач с большим количеством альтернатив.

Варьирование значений описанных параметров проведения экспериментов в процессе подготовки обучающей выборки позволяет обеспечить универсальность выявления ВР, в том числе при динамическом изменении этих параметров в процессе функционирования РРТС.

В качестве ИНС предлагается использовать многослойный персептрон с двумя скрытыми слоями по 128 нейронов в каждом. Архитектура ИНС представлена на рис. 2.

Входной слой ИНС будет принимать закодированные численные значения полей «Признаки» агента, который отправил сообщение, и агента, который получил сообщение. Тогда, например, при наличии в среде 5 цветов, на вход ИНС будет подано два вектора размерности 5×2, для чего потребуется входной слой из 20 нейронов. Выходной слой состоит из двух нейронов, значения которых определяют вероятность того, насколько агент, пославший сообщение, относится к классу обычных или вредоносных роботов. Получаемая в результате работы нейросетевого алгоритма вероятность вредоносности агента может быть в дальнейшем использована для оценки необходимости блокирования агента, что приведет к уменьшению времени, необходимого для ДК.

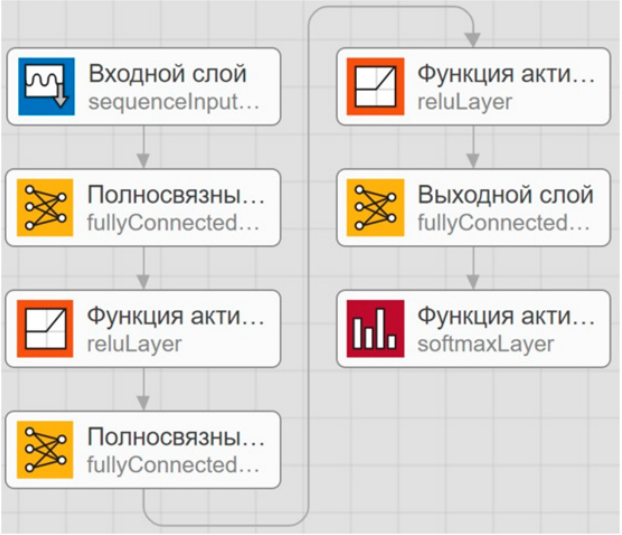

Рис 2. Архитектура нейронной сети
[Fig 2. Artificial neural network architecture]

Схематическое представление предлагаемого метода показано на рис. 3. Стоит отметить, что этапы № 1–2 выполняются до тех пор, пока не будет достигнут требуемый минимальный порог ложных срабатываний (точность выявления ВР). Результат обучения

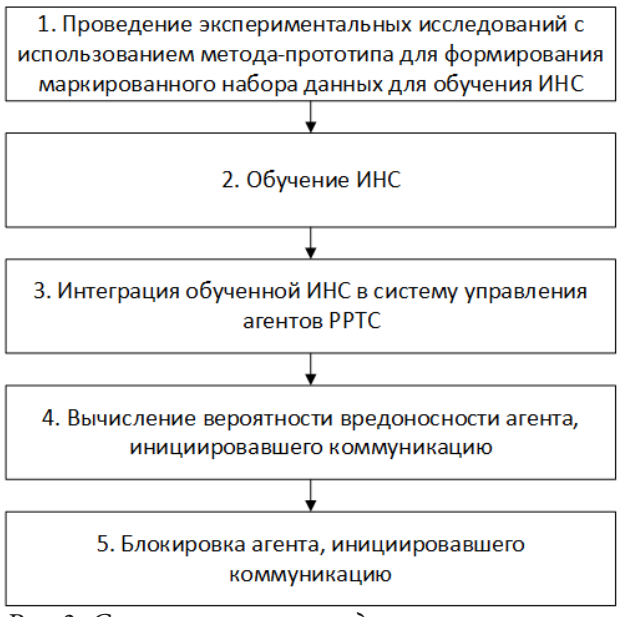

Рис 3. Схематическое представление этапов предлагаемого метода
[Fig 3. Stages of the proposed method]

ИНС может зависеть как от объема обучающей выборки, так и от выбранного алгоритма обучения с учителем.

Этапы № 4 и 5 после этапа интеграции обученной ИНС в систему управления агентов РРТС выполняются каждый раз при инициализации коммуникации любым соседним агентом, находящимся в области видимости.

Данный подход позволяет осуществлять выявление ВР и его блокировку в режиме реального времени.

3. РЕЗУЛЬТАТЫ И ИХ ОБСУЖДЕНИЕ

Для апробации предложенного метода была выполнена программная реализация на языке программирования C++ с использованием библиотеки tiny-dnn [23] и последующей интеграцией со скриптом Argos, содержащим систему управления агентов РРТС. Формирование графиков для оценки эффективности предложенного метода выполнены с помощью библиотеки Matplotlib на языке программирования Python. При проведении симуляции был использован компьютер с характеристиками: процессор Intel Core i7-8550U с тактовой частотой 1,8 ГГц, 8 ГБ оперативной памяти. Использованы параметры моделирования, указанные в табл. 1.

Цель проведенных экспериментов состояла в оценки числа ложных срабатываний обнаружения ВР. Была проведена серия экспериментов из 1000 экспериментальных запусков со случайными параметрами моделирования в пределах значений, указанных в табл. 1.

Таблица 1. Параметры моделирования
[Table 1. Simulation parameters]

Параметр	Значение	Ед. измерения
1	ОСП; КСП; ССП	Тип ВР
2	0,33–11,32	Масштаб сцены
3	0–1000	Шаг процесса КПР
4	2–5	Кол-во альтернатив
5	20	Число ВР
6	0,45–0,85	Сложность сцены
7	100	(%) кворум для ДК

Оценка эффективности предложенного метода обнаружения нарушений информационной безопасности коллективного принятия решений в роевых робототехнических системах на основе машинного обучения по сравнению с методом-прототипом осуществлялась путем выявления ВР в сценарии с заданным (фиксированным) количеством ВР, равным 20 % от числа корректно функционирующий роботов, для наибольшей объективности. При этом для сравнения использовано два критерия: количество ложных срабатываний при выявлении ВР (рис. 4), а также процентное соотношение количества ложных срабатываний и истинных срабатываний методов выявления ВР (рис. 5). Данные измерения представлены только с позиции наблюдателя, так как оценка результата выявления ВР отдельного агента не может дать целостного представления для оценки эффективности из-за сложных характеристик и ограничений РРТС [24]. На рис. 4 и 5 аббревиатуры РМ и МП означают «разработанный метод» и «метод-прототип» соответственно.

При функционировании РРТС необходимо за минимальное количество шагов обеспечить возможность обнаружения и блокировки ВР при их наличии. Недостатком метода-прототипа является тот факт, что при его функционировании на малом количестве шагов для сбора данных о поведении роботов РРТС происходит большое число неправильно отнесенных к ВР роботов, что существенно замедляет работу РРТС. Основная сложность при этом заключается в том, что разработчи-

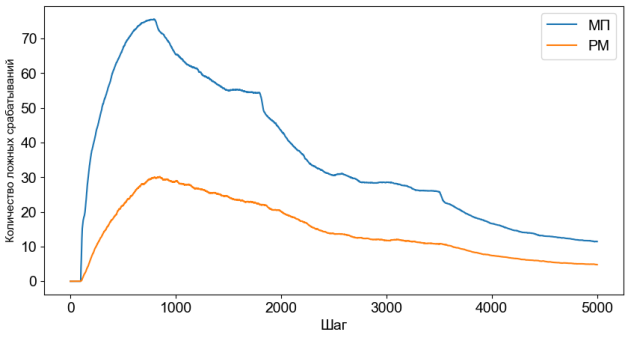

Рис 4. Результат оценки количества ложных срабатываний при обнаружении ВР
[Fig 4. Number of false positive results of Byzantine robots detection]

ку необходимо экспериментально определить значения порога аномальности отдельно для каждого типа ВР с определенной стратегией поведения и конкретных внешних условий при функционировании РРТС. С другой стороны, разработанный метод за счет использования ИНС, обученной на множестве различных сценариев, позволяет автоматически устанавливать этот порог независимо от условий и типа ВР.

На рис. 4 на оси абсцисс показано время (шаг – итерация процесса КПР) начала выявления ВР при использовании сравниваемых методов. Критерий количества ложных срабатываний непосредственно связан с целью данной работы. Полученные численные значения приведены в табл. 2.

Таблица 2. Оценка абсолютного количества ложных срабатываний при обнаружении ВР
[Table 2. Number of false positive results of Byzantine robots detection]

Шаг	Значения (количество срабатываний)		
	МП	РМ	Прирост
1000	65,43	30,29	35,14
2000	43,49	17,89	25,60
3000	28,56	10,56	18,00
4000	16,61	5,58	11,03
5000	11,45	4,13	7,32
Среднее 0–5000	35,93	14,76	21,17

Из проведенных экспериментальных исследований можно заключить, что разработанный метод позволяет снизить количество ложных срабатываний при малом количестве шагов для сбора данных о поведении роботов РРТС на 35,14 срабатывания (46,29 %). Среднее уменьшение количества ложных срабатывания по всем шагам процесса КПР по сравнению с прототипом составило 41,07 %.

Также важным показателем является процентное соотношение количества ложных срабатываний и корректных срабатываний методов обнаружения ВР. Так, на рис. 5 показано соотношение в процентах ложных и корректных срабатываний по сравнению с методом-прототипом.

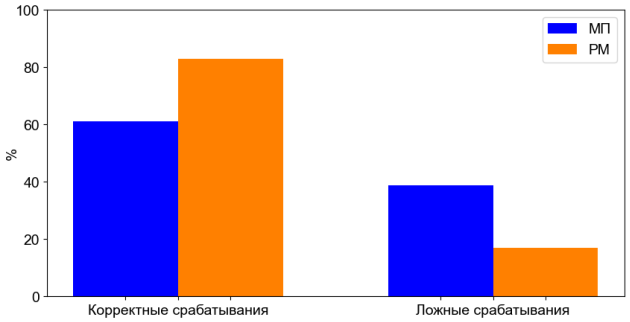

Рис 5. Результат оценки процентного соотношения количества ложных и истинных срабатываний
[Fig 5. Percentage of true and false positives]

Можно заключить, что использование разработанного метода позволяет осуществлять выявление ВР с лучшим соотношением корректных (83 %) и ложных срабатываний (17 %), значительно снизив количество ложных срабатываний.

ЗАКЛЮЧЕНИЕ

Представленный метод обнаружения нарушений ИБ в РРТС на основе машинного обучения позволяет осуществлять выявление ВР в процессе КПР с учетом ограниченной производительности бортовых датчиков и вычислительных устройств агентов, а также специфики децентрализованного управления.

Элементом новизны предложенного решения является использование классификатора на основе ИНС для выявления ВР при ДК. Отличительными особенностями данной работы являются, во-первых, возможность использования метода как для задач с бинарным выбором, так и для задач с большим количеством альтернатив. Во-вторых, разработанный метод позволяет выявлять ВР независимо от их стратегии поведения. Данные особенности позволяют считать разработанный метод универсальным для выявления ВР, в том числе при динамическом изменении условий среды в процессе функционирования РРТС.

Проведенные экспериментальные исследования подтвердили эффективность предложенного решения. Дальнейшая работа будет направлена на разработку испытательного стенда для апробации предложенного ме-

тода и его модификаций. Одним из наиболее перспективных путей модификации является исследование и разработка процедуры блокировки ВР, позволяющей контролировать время, в течение которого не будут учитываться данные, поступающие от ВР.

БЛАГОДАРНОСТИ

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

КОНФЛИКТ ИНТЕРЕСОВ

Авторы декларируют отсутствие явных и потенциальных конфликтов интересов, связанных с публикацией настоящей статьи.

СПИСОК ЛИТЕРАТУРЫ

1. *Higgins, F.* Threats to the swarm: Security considerations for swarm robotics / F. Higgins, A. Tomlinson, K. M. Martin // International Journal on Advances in Security. – 2009. – Vol. 2, № 2. – P. 288–297.

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

3. *Комаров, И. И.* Исследование деструктивного воздействия роботов-злоумышленников на эффективность работы мультиагентной системы / И. И. Комаров, Р. А. Юрьева, А. Л. Дранник, О. С. Масленников, М. Е. Коваленко, Д. А. Егоров // Процессы управления и устойчивость. – 2014. – Т. 1, № 1. – С. 336–340. DOI: 10.7256/2305-6061.2016.1.17946.

4. *Басан, А. С.* Модель угроз для систем группового управления мобильными роботами / А.С. Басан, Е.С. Басан // VIII Всероссийская научная конференция «Системный синтез и прикладная синергетика»: сб. научных тр. (п. Нижний Архыз, 18–20 сентября 2017 г.). – 2017. P. 205–212.

5. *Юрьева, Р. А.* Построение модели нарушителя информационной безопасности для мультиагентной робототехнической системы с децентрализованным управлением / Р. А. Юрьева, И. И. Комаров, Н. А. Дородников // Программные системы и вычислительные методы. –2016. – Т. 1, № 1. – С. 42–48.

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

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

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

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

10. *Носиров, З. А.* Анализ блокчейн-технологии: основы архитектуры, примеры использования, перспективы развития, проблемы и недостатки / З. А. Носиров, В. М. Фомичев // Системы управления, связи и безопасности. – 2021. – № 2. – С. 37–75.

11. *Hamann, H.* Swarm Robotics: A Formal Approach / H. Hamann. – Springer International Publishing, 2018. – 210 p. DOI: https://doi.org/10.1007/978-3-319-74528-2.11.

12. *Canciani, F.* Keep calm and vote on: Swarm resiliency in collective decision making [Электронный ресурс] / F. Canciani, M. S. Talamali, A. R. Marshall J., A. Reina // International Conference on Robotics and Automation. – 2019. – Режим доступа: https://www.cl.cam.ac.uk/~asp45/icra2019/papers/Canciani.pdf (Дата обращения: 07.11.2021).

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

14. *Зикратов, И. А.* Построение модели доверия и репутации к объектам мультиагентных робототехнических систем с децентрализованным управлением / И. А. Зикратов, Т. В. Зикратова, И. С. Лебедев, А. В. Гуртов // Научно-технический вестник информационных технологий, механики и оптики. – 2014. – Т. 3, № 91. – С. 30–38.

15. *Tebueva, F. B.* A method of counteracting Byzantine robots with a random behavior strategy during collective design-making in swarm robotic systems / F. B. Tebueva, S. S. Ryabtsev, I. V. Struchkov // E3S Web of Conferences. – 2021. – Vol. – 270. – P. 1–8. DOI:10.1051/e3sconf/202127001034.

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

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

18. *Петренко, В. И.* Метод глубокого мультиагентного обучения с подкреплением для мобильных киберфизических систем с повышенными требованиями к функциональной безопасности / В. И. Петренко // Системы управления, связи и безопасности. – 2021. – № 3. – С. 179–206.

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

20. *Valentini, G.* Self-organized collective decision making: The weighted voter model / G. Valentini, H. Hamann, M. Dorigo // Proceedings of the 13th international conference on autonomous agents and multiagent systems, AAMAS'14. – 2014. – P. 45–52.

21. Ncfu pmkb, swarm-robotics GitLab. – Режим доступа: https://gitlab.com/pmkb/swarm-robotics. – (дата обращения: 05.11.2021).

22. Проект e-puck. Сайт разработчиков робота e-puck. – Режим доступа: http://www.e-puck.org/. – (дата обращения: 28.10.2021).

23. Библиотека tiny-dnn. – Режим доступа: https://github.com/tiny-dnn/tiny-dnn. – (дата обращения: 29.11.2021)

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

Петренко Вячеслав Иванович – канд. техн. наук, доцент, и.о. директора института цифрового развития Северо-Кавказского федерального университета.
E-mail: vipetrenko@ncfu.ru
ORCID iD: https://orcid.org/0000-0003-4293-7013

Тебуева Фариза Биляловна – д-р физ.-мат. наук, доцент, заведующая кафедрой компьютерной безопасности Северо-Кавказского федерального университета.
E-mail: ftebueva@ncfu.ru
ORCID iD: https://orcid.org/0000-0002-7373-4692

Рябцев Сергей Сергеевич – старший преподаватель кафедры компьютерной безопасности Северо-Кавказского федерального университета.
E-mail: nalfartorn@yandex.ru
ORCID iD: https://orcid.org/0000-0002-1428-6711

Павлов Андрей Сергеевич – старший преподаватель кафедры компьютерной безопасности Северо-Кавказского федерального университета.
E-mail: losde5530@gmail.com
ORCID iD: https://orcid.org/0000-0002-8413-8706

Гурчинский Михаил Михайлович – аспирант 4-го года обучения кафедры компьютерной безопасности Северо-Кавказского федерального университета.
E-mail: gurcmikhail@yandex.ru
ORCID iD: https://orcid.org/0000-0002-1739-2624

DOI: https://doi.org/ ISSN 1995-5499
Received 30.11.2021
Accepted 22.04.2022

MACHINE LEARNING-BASED DETECTION OF INFORMATION SECURITY VIOLATIONS IN SWARM ROBOTIC SYSTEMS

© 2022 V. I. Petrenko, F. B. Tebueva, S. S. Ryabtsev✉, A. S. Pavlov, M. M. Gurchincky

North-Caucasus Federal University
1, Pushkin Street, 355017 Stavropol, Russian Federation

Annotation. Intensive development of swarm robotic systems actualizes the need to ensure their information security. Known approaches to information protection of the collective decision-making process in swarm robotic systems use physical parameters that strongly depend on operating environment and hardware implementation of the system. Thus, it is difficult to identify universal indicators of abnormal behavior of an agent, that are able to provide accurate rejection threshold and low false positive rate. The aim of the work is to improve the efficiency of consensus achievement in swarm robotic systems in the presence of faulty or Byzantine robots. Detection of Byzantine robots is carried out by the use of machine learning methods. To classify the robots as normal or Byzantine, we used an artificial neural network trained on a dataset generated with a previously developed analytical method. The novelty of the proposed solution lies in the choice of parameters for carrying out simulations in order to form a dataset for training the classifier. Simulation of a swarm consisting of 100 robots has been carried out. In the presence of 20 % of robots with incorrect behavior, the number of false positives is reduced by 41,07 % relative to the prototype method. The proposed approach is capable of detecting Byzantine robots regardless of their number or behavioral strategy. The method is implemented as a C++ program.
Keywords: swarm robotic systems, information security, Byzantine robot, collective decision-making, consensus achievement, machine learning.

✉ Ryabtsev Sergey S.
e-mail: nalfartorn@yandex.ru

CONFLICT OF INTEREST

The authors declare the absence of obvious and potential conflicts of interest related to the publication of this article.

REFERENCE

1. *Higgins F., Tomlinson A. and Martin K. M.* (2009) Threats to the swarm: Security considerations for swarm robotics. *International Journal on Advances in Security*. 2(2), P. 288–297.

2. *Sargeant I. and Tomlinson A.* (2018) Review of Potential Attacks on Robotic Swarms. *Proceedings of SAI Intelligent Systems Conference*. P. 628–646. Available at: doi:10.1007/978-3-319-56991-8_46.

3. *Komarov I. I., Iureva R. A., Drannik A. L., Maslennikov O. S., Kovalenko M. E. and Egorov D. A.* (2014) 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*. 1(1). P. 336–340. (In Russian)

4. *Basan E. A. and Basan E. S.* (2017) Model' ugroz dlya sistem gruppovogo upravleniya mobil'nymi robotami [A threat model for group control systems for mobile robots]. *Procedings of All-Russian Scientific Conference «Sistemnyy sintez i prikladnaya sinergetika»*, 18–20 september 2017, Nizhny Arkhyz, Russia. Rostov-on-Don, SFEDU, P. 205–212. (In Russian)

5. *Iureva R. A., Komarov I. I. and Dorodnikov N. A.* (2016) Postroyeniye modeli narushitelya informatsionnoy bezopasnosti dlya mul'tiagentnoy robototekhnicheskoy sistemy c detsentralizovannym upravleniyem [Building the violent model information security for multi-agent robot systems with decentralized management]. *Software systems and computational methods*. 1 (1). P. 42–48. Available at: doi: 10.7256/2305-6061.2016.1.17946. (In Russian)

6. *Zikratov I. A., Zikratova T. V. and Lebedev I. S.* (2014) Trust model for information security of multi-agent robotic systems with a decentralized management. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*. 2 (90). P. 47–52. (In Russian)

7. *Strobel V., Ferrer C. and Dorigo M.* (2020) Blockchain Technology Secures Robot Swarms: A Comparison of Consensus Protocols and Their Resilience to Byzantine Robots. *Front. Robot. AI. Frontiers Media S. A*. 7, 54. Available at: doi:10.3389/frobt.2020.00054.

8. *Strobel V. Ferrer C. and Dorigo M.* (2018) Managing Byzantine Robots via Blockchain Technology in a Swarm Robotics Collective Decision Making Scenario: Robotics track. I*nternational Conference on Autonomous Agents and Multiagent Systems*. 1. P. 541–549.

9. *Lamport L., Shostak R. and Pease M.* (1982) The Byzantine Generals Problem. *ACM Transactions on Programming Languages and Systems*. 4 (3). P. 382–401.

10. *Nosirov Z. A. and Fomichev V. M.* (2021) Analysis of Blockchain Technology: Architectural Basics, Application Examples, Future Trends, Problems and Disadvantages. *Systems of Control, Communication and Security*. (2). P. 37–75. Available at: doi: 10.24412/2410-9916-2021-2-37-75. (In Russian)

11. *Hamann H.* (2018) Swarm Robotics: A Formal Approach. *Springer International Publishing*, 210 p. Available at: doi: https://doi.org/10.1007/978-3-319-74528-2.11.

12. *Canciani F., Talamali M. S., Marshall A. R. and Reina A.* (2019) Keep calm and vote on: Swarm resiliency in collective decision making [Electronic resource]. *International Conference on Robotics and Automation*. Available at: https://www.cl.cam.ac.uk/~asp45/icra2019/papers/Canciani.pdf [Accessed 07th Nowember 2021].

13. *Iureva R. A., Komarov I. I. and Maslennikov O. S.* (2016) 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*. (4). P. 375–382, Available at: doi: 10.7256/2305-6061.2016.4.21128. (In Russian)

14. *Zikratov I. A., Zikratova T. V., Lebedev I. S. and Gurtov A. V.* (2014) 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. 3 (91). P. 30–38. (In Russian)

15. *Tebueva F. B., Ryabtsev S. S. and Struchkov I. V.* (2021) A method of counteracting Byzantine robots with a random behavior strategy during collective design-making in swarm robotic systems. *E3S Web of Conferences*. 270. P. 1–8. Available at: doi:10.1051/e3sconf/202127001034.

16. *Petrenko V. I., Tebueva V. I., Ryabtsev S. S., Gurchinsky M. M. and Struchkov I. V.* (2021) 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*. 1069(1). P. 1–8. Available at: doi:10.1088/1757-899X/1069/1/012044.

17. *Petrenko V. I., Tebueva F. B., Ryabtsev S. S., Gurchinsky M. M. and Struchkov I. V.* (2020) Consensus achievement method for a robotic swarm about the most frequently feature of an environment. *IOP Conference Series: Materials Science and Engineering*. 919 (4). P. 1–8. Available at: doi: 10.1088/1757-899x/919/4/042025.

18. *Petrenko V. I.* (2021) Multi-agent Deep Reinforcement Learning Method for Mobile Cyber-Physical Systems with Increased Functional Safety Requirements. *Systems of Control, Communication and Security*. (3). P. 179–206. Available at: doi: 10.24412/2410-9916-2021-3-179-206. (In Russian)

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

20. *Valentini G., Hamann H. and Dorigo, M.* (2014) Self-organized collective decision making: The weighted voter model. *Proceedings of the 13th international conference on autonomous agents and multiagent systems, AAMAS'14*. P. 45–52.

21. Ncfu pmkb, swarm-robotics GitLab [Electronic resource]. URL: https://gitlab.com/pmkb/swarm-robotics (accessed: 28.11.2021).

22. E-puck education robot [Electronic resource]. URL: http://www.e-puck.org/ (accessed: 19.11.2019).

23. GitHub - tiny-dnn/tiny-dnn: header only, dependency-free deep learning framework in C++14 [Electronic resource]. URL: https://github.com/tiny-dnn/tiny-dnn (accessed: 29.11.2021).

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

Petrenko Vyacheslav I. – PhD in Engineering Sciences, Associate Professor. Head of the department of organization and technology of information security. North-Caucasian Federal University.
E-mail: vipetrenko@ncfu.ru
ORCID iD: https://orcid.org/0000-0003-4293-7013

Tebueva Fariza B. – advanced doctor in physics and mathematics sciences, Head of the Department of Computer Security, North-Caucasus Federal University. E-mail: ftebueva@ncfu.ru
ORCID iD: https://orcid.org/0000-0002-7373-4692

Ryabtsev Sergey S. – senior lecturer of the department of computer security. North-Caucasus Federal University. E-mail: nalfartorn@yandex.ru
ORCID iD: https://orcid.org/0000-0002-1428-6711

Pavlov Andrey S. – senior lecturer of the department of computer security. North-Caucasus Federal University. E-mail: losde5530@gmail.com
ORCID iD: https://orcid.org/0000-0002-8413-8706

Gurchincky Mickhail M. – postgraduate student of the Department of Computer Security. North-Caucasus Federal University. E-mail: gurcmikhail@yandex.ru
ORCID iD: https://orcid.org/0000-0002-1739-2624