ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.896 : 004.056 ISSN 1995-5499
DOI: https://doi.org/10.17308/sait/1995-5499/2022/4/23-38
Поступила в редакцию 26.04.2022
Подписана в печать 05.12.2022

ПРОТОКОЛ ДЕЛЕГИРОВАННОЙ АУТЕНТИФИКАЦИИ НОВЫХ АГЕНТОВ ПРИ МАСШТАБИРОВАНИИ ЧИСЛЕННОСТИ АГЕНТОВ В РОЕВЫХ РОБОТОТЕХНИЧЕСКИХ СИСТЕМАХ

© 2022 А. С. Павлов✉[1], Н. Ю. Свистунов[1], В. И. Петренко[1], Ф. Б. Тебуева[1], В. В. Копытов[1], Е. Н. Тищенко[2]

1Северо-Кавказский федеральный университет
пр-т Кулакова, 2, 355029 Ставрополь, Российская Федерация
2Ростовский государственный экономический университет (РИНХ)
ул. Большая Садовая, 69, 344002 Ростов-на-Дону, Российская Федерация

Аннотация. Интенсивное развитие групповой робототехники, в том числе роевых робототехнических систем (РРТС), актуализирует вопросы обеспечения информационной безопасности. Известные подходы к аутентификации агентов роевых робототехнических систем не учитывают свойство масштабируемости системы, что вызывает «лавинный эффект» при значительном увеличении численности агентов. Целью данной работы является повышение эффективности выполнения таких заданий агентами РРТС, которые требуют увеличения численности агентов, за счет уменьшения времени, необходимого для аутентификации новых агентов. В рамках решения поставленной задачи разработано расширение протокола для делегированной аутентификации новых агентов при масштабировании численности агентов РРТС на базе схемы идентификации Фейга — Фиата — Шамира с нулевым разглашением знаний. Элементом научной новизны является разработанный набор продукционных правил, представленных в виде дерева решений, позволяющих путем информационного обмена агентов с использованием распределенного реестра выполнить делегированную аутентификацию агентов, которые ранее прошли успешно эту процедуру. К отличительным особенностям представленного решения относятся возможность использования любого базового протокола аутентификации, удовлетворяющего аппаратным ограничениям вычислительной платформы робототехнических устройств, входящих в состав РРТС, а также возможность агентов «переключаться» между наиболее приоритетными задачами и взаимодействовать с другими агентами без повторной аутентификации, находясь в области видимости по меньшей мере одного соседнего агента. Представленный протокол реализован в виде программного обеспечения на языке программирования Python, которое может быть использовано при моделировании систем управления РРТС.

Ключевые слова: роевые робототехнические системы, информационная безопасность, внедрение вредоносных агентов, аутентификация, доказательство с нулевым разглашением знаний.

✉ Павлов Андрей Сергеевич
e-mail: anspavlov@ncfu.ru

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. Наличие большого количества прикладных задач, решение которых характеризуется высокой трудоемкостью, неопределенностью и требованием работы в масштабе реального времени в условиях воздействия противоречивых, а также часто меняющихся факторов обуславливает непрерывно растущий интерес к роевой робототехнике.

Одним из наиболее значимых барьеров к широкому использованию роевых робототехнических систем (РРТС) является наличие уязвимостей с точки зрения информационной безопасности (ИБ) [1]. В ряде исследований отечественных и зарубежных авторов рассматривается вопрос ИБ в РРТС. Так, в работе [2] представлен подробный обзор актуальных вопросов ИБ в РРТС, в работе [3] выполнен анализ потенциальных атак на РРТС, а в работах [10, 11] разработаны модели угроз и нарушителя ИБ РРТС. В работе [4] приведен анализ и исследование основных угроз актуальных для различных принципов, методов и особенностей группового управления РРТС.

Основные уязвимости ИБ РРТС обусловлены следующими особенностями систем данного вида [6]:

– высокая масштабируемость: система управления РРТС строится таким образом, чтобы обеспечить требуемое качество выполнения задания с неограниченным количеством роботов;

– децентрализованная система управления: ожидаемое поведение роботов достигается за счет использования принципов самоорганизации;

– простота технической реализации роботов: все роботы, входящие в состав РРТС, имеют ограниченные возможности вычислительных устройств, а также бортовых датчиков и сенсоров, что делает невозможным выполнить поставленную задачу с использованием только одного робота;

– локальное взаимодействие роботов: выполнение поставленной перед РРТС задачи возможно только путем взаимодействия роботов друг с другом с использованием различных средств связи, при этом дальность их действия ограничена некоторой областью видимости;

– гомогенность: роботы имеют идентичные структурные и функциональными характеристики;

– автономность: каждый робот самостоятельно принимает решение о своих дальнейших действиях, опираясь на доступную ему информацию.

К основным механизмам атак на РРТС, формирующим угрозы, относят [7]:

– атаки на каналы связи;

– сложность идентификации и аутентификации агентов в системе;

– внедрение в систему «вредоносных» роботов.

Однако, несмотря на наличие указанных исследований в области обеспечения ИБ РРТС, большинство исследований не рассматривают проблему аутентификации агентов в системе в процессе масштабирования системы. В работах [2, 3] представлен анализ проблем обеспечения информационной безопасности в РРТС. Авторы работ отмечают, что основная часть исследований в области идентификации и аутентификации агентов РРТС направлена на адаптацию классических методов и протоколов с учетом специфических свойств систем данного вида. В зарубежных литературных источниках наибольшей популярностью пользуются криптосистемы с симметричным и ассиметричным шифрованием. Так, в работе [8] исследование авторов направлено на повышение эффективности выполнения задания группой беспилотных летательных аппаратов (БПЛА) путем модификации инерциальной системы навигации и обеспечения защищенной передачи измерений данной системы другим БПЛА. Данный подход позволяет оптимально осуществлять планирование пути перемещения агентов в

динамических средах с множеством препятствий, а также в агрессивных средах, которые предполагают возможность воздействия злоумышленника на информационный обмен между БПЛА. Авторы предложили гибридную криптосистему, включающую процедуру аутентификации по подписи с использованием алгоритма RSA. Основной акцент в работе авторами сделан на модификацию инерциальной системы навигации БПЛА, вследствие чего оценка эффективности обеспечения информационной безопасности не приведена. Также авторами упоминается, что обеспечение работы предложенного решения в реальном масштабе времени возможно при использовании дополнительного аппаратного обеспечения, что требует проведения экспериментальных исследований, направленных на оценку возможности применения данного решения в условиях ограниченных ресурсов вычислительных платформ агентов РРТС.

Авторы работы [9] провели исследование и оценку эффективности обеспечения информационной безопасности РРТС, состоящей из 3 БПЛА, при наличии внешних информационных воздействии в процессе коммуникации каждого из агентов с центром управления. Эксперимент был проведен в среде моделирования Gazebo [10] с использованием средств аутентификации, встроенных в фреймворк ROS2 (англ. «Robotic operation system» — робототехническая операционная система) [11]. Результаты проведенных исследований подтвердили эффективность применения данного инструмента, однако, его использование вызвало задержку при передаче данных между сторонами, что существенно увеличило время симуляции.

В работе [12] предложен протокол аутентификации для мультиагентных систем на основе технологии JWT (JSON Web Token) и асимметричного шифрования. Это решение отличается простотой реализации и относительно низкой вычислительной сложностью. Однако, авторы работы не представили результатов оценки эффективности протокола, что требует проведения дополнительных исследований.

В работе [13] представлен протокол взаимной аутентификации на основе алгоритма с открытым ключом для создания цифровой подписи ECDSA (Elliptic Curve Digital Signature Algorithm). Протокол разработан для использования в беспроводных сенсорных сетях, поэтому может быть достаточно легко модифицирован для использования в РРТС. К достоинствам протокола относятся высокая криптографическая стойкость и низкие требования к ресурсам вычислительной платформы. К недостаткам можно отнести относительно высокое время взаимной аутентификации сторон, что может снизить эффективность выполнения задания РРТС при высокой численности нарушителей.

В результате анализа литературы отечественных исследователей можно отметить, что большинство работ по обеспечению информационной безопасности в групповой робототехнике строится на основе доверительной модели [1]. Например, в работе [14] предложен протокол аутентификации на основе использования доверительной модели, что делает возможным использование этого решения в РРТС ввиду низкой вычислительной сложности. Основная идея протокола заключается в том, что все агенты составляют «таблицы доверия», в которых на основе анализа поведения каждого агента рассчитывается показатель доверия. После каждого обновления таблицы, например, при аутентификации нового агента, обновленная версия таблицы рассылается всем агентам группы. Представленный подход согласуется с децентрализованной стратегией управления агентами РРТС, а также позволяет актуализировать уровень доверия к агентам группы и своевременно выявить нарушителя. Авторы работы продемонстрировали эффективность предложенного решения при моделировании группы, состоящей из 5 беспилотных летательных аппаратов. Однако, авторами не рассматривается вопрос функционирования группы агентов большой численности в недетерминированной среде, характеризующейся нестабильностью каналов связи, что затрудняет своевременность обновления таблиц

доверия. Исходя из этого, применимость данного протокола аутентификации для обеспечения масштабирования РРТС и выполнения задания требует дополнительных исследований. Также к особенностям данного протокола можно отнести обязательное требование наличия индивидуальных идентификаторов у агентов, что затрудняет использование данного решения без его модификации. К подобной модификации можно отнести, например, использование технологии блокчейн [15] для закрепления идентификатора за каждым агентом РРТС. Такой подход, с одной стороны, позволит использовать методы и протоколы аутентификации с обязательным наличием идентификаторов для РРТС, а с другой стороны, необходимость использования алгоритмов достижения консенсуса и согласования актуальной версии цепочек блоков данных увеличит вычислительную сложность решения [16].

В работе [17] предложено решение проблемы взаимной аутентификации пользователей в децентрализованных системах обмена сообщениями, в рамках которого представлена схема групповой аутентификации на основе доказательства с нулевым разглашением. Это решение позволяет аутентифицировать пользователей децентрализованной сети без установки общего секрета по стороннему каналу, опираясь на существующие в сети цепочки доверия. В основе метода лежит механизм групповой подписи с нулевым разглашением [18], позволяющий членам аутентифицированных групп подписывать сообщения от их имени и обеспечивающий невозможность подделки групповой подписи участниками, не являющимися членами группы. С точки зрения применимости данного решения в РРТС стоит отметить, что протокол требует наличия информации у каждого агентов обо всех агентах системы, а также возможности коммуникации агентов по принципу «каждый с каждым», что затруднительно ввиду специфических ограничений агентов РРТС.

1. ПОСТАНОВКА ЗАДАЧИ

В результате проведенного литературного анализа, можно заключить, что большая часть исследований в области аутентификации агентов в групповой робототехнике направлена на увеличение быстродействия алгоритмов и уменьшения их вычислительной сложности, что особенно актуально для РРТС. С другой стороны, ключевым преимуществом РРТС, в отличии от других видов групповой робототехники, является такое свойство как масштабируемость системы. Так, например, если говорить о задаче аутентификации агентов при «слиянии» двух и более РРТС, то использование известных протоколов, удовлетворяющих возможности использования в РРТС, может вызвать «лавинный эффект», то есть такую ситуацию, когда агенты начнут осуществлять аутентификацию по принципу «каждый с каждым». При этом необходимо учитывать высокую динамику изменения структуры системы и ограниченную область видимости агентов. Это может вызвать такую ситуацию, когда в процессе функционирования агенты «расходятся» на расстояние превышающее область видимости друг друга. В результате при повторной встрече через некоторый промежуток времени агенты снова должны осуществить процедуру аутентификации. Описанная проблема требует дополнительных исследований, направленных на минимизацию количества процедур аутентификации агентов в процессе масштабирования их численности, при этом в идеальном случае это количество должно стремиться к удвоенному общему числу агентов, то есть должна обеспечиваться единая точка входа агентов системы.

Согласно классическому подходу проектирования РРТС агенты не имеют собственных идентификаторов [6]. Однако, для реальных приложений РРТС и обеспечения защиты информации этот параметр имеет ключевое значение. С этой точки зрения, использование протоколов с нулевым разглашением знаний позволяет использовать открытый ключ агентов в качестве их идентификаторов. Если же отойти от канонов проектирования РРТС

путем, например, назначения оператором уникального идентификатора каждому агенту, то выбор того или иного протокола аутентификации зависит только от аппаратных ограничений робототехнических устройств, используемых в составе РРТС. При этом актуальной остается проблема «лавинного эффекта» при аутентификации агентов в процессе масштабировании их численности. Стоит отметить, что авторы данной работы являются приверженцами классического варианта проектирования и реализации РРТС, поэтому в данном исследовании в качестве базового протокола аутентификации будет использоваться семейство протоколов с нулевым разглашением знаний.

Таким образом, целью данной работы является повышение эффективности выполнения задания агентами РРТС, требующего увеличения численности агентов, за счет уменьшения времени аутентификации агентов. Исходя из этого, формальная постановка научной задачи имеет следующий вид. Необходимо найти такой протокол P, что:

$$P: A, O, E, Q \to \{\Delta q_1, \ldots, \Delta q_l\} \big| \forall \Delta q_l < 0, q_l \in Q,$$

$$l = 1, 2, \ldots, h,$$

где $A = \{a_1, a_2, \ldots, a_m\}$ — РРТС численностью m агентов; $O = \{o_1, o_2, \ldots, o_j\}$ — задание агентов РРТС, состоящее из j задач, E — множество параметров среды и условий функционирования агентов РРТС, $Q = \{q_1, \ldots, q_l\}$ — множество показателей эффективности функционирования РРТС, h — количество показателей эффективности выполнения задания агентами РРТС, $\Delta q_l = q_l^{П} - q_l^{Д}$, где индекс «д» значит «до использования протокола», индекс «п» — «после использования протокола».

2. МАТЕРИАЛЫ И МЕТОДЫ

2.1. Базоый протокол аутентификации агентов РРТС

Многие протоколы, в том числе протоколы на основе систем с открытым ключом, требуют сложных вычислений. Однако при этом обладают значимым преимуществом: для полной проверки доказываемого знания достаточно одной итерации. Вычисления протоколов с нулевым разглашением более просты, но требуют большого количества итераций, прежде чем проверяющая сторона сможет убедиться в том, что доказывающая сторона знает секрет. Сравнительно простые устройства с небольшим объемом памяти не могут осуществлять сложные вычисления. В таких устройствах и находит применение протокол Фейга — Фиата — Шамира [19, 20].

Стойкость протокола аутентификации Фейга — Фиата — Шамира основывается на сложности извлечения квадратного корня по модулю большого числа с неизвестным разложением на простые множители. Рассмотрим основную схему идентификации Фейга — Фиата — Шамира. Сначала выбирается случайный модуль, рассчитываемый по формуле $n = pq$. Для генерации открытого и закрытого ключей стороны А выбирается k случайных различных чисел $v_1, v_2, \ldots, v_k$, где каждое v_i, $i = 1, 2, \ldots, k$ является квадратичным остатком по модулю n. При этом выполняется условие, что $1 \le v_i \le n-1$. Последовательность $v_1, v_2, \ldots, v_k$ служит открытым ключом. Затем вычисляются наименьшие s_i по формуле $s_i \equiv \sqrt{v_i^{-1}} \bmod n$.

Последовательность $s_1, s_2, \ldots, s_k$ служит закрытым ключом. Основная схема идентификации включает в себя следующие этапы:

1. Сторона А выбирает случайное число r, где $1 \le r \le n-1$, и случайный бит e, где $e = 1$ или $e = 0$. Затем вычисляет x по формуле $x = (-1)^e r^2 \bmod n$. Результат вычисления отправляется стороне В.

2. Сторона В отправляет стороне А последовательность из k случайных битов: $b_1, b_2, \ldots, b_k$, где $b_i = 1$ или $b_i = 0$.

3. Сторона А вычисляет значение y по формуле $y = r \prod_{i=1}^{k} s_i^{b_i} \bmod n$. Результат вычисления отправляется стороне В.

4. Сторона В вычисляет значение z по формуле $z = y^2 \prod_{i=1}^{k} v_i^{b_i} \bmod n$. А затем проверяет $z = \pm x$ и $z \ne 0$.

Стороны исполняют этот протокол t раз, пока сторона В не убедится, что сторона А знает последовательность $s_1, s_2, \ldots, s_k$. Веро-

ятность обмана стороны В стороной А t раз составляет $1/2^{kt}$.

В классическом понимании РРТС агенты не имеют идентификаторов, поэтому преимущество данного протокола заключается в том, что генерируемый каждым агентом открытый ключ должен обязательно пересылаться проверяющему агенту, а значит может быть использован в качестве уникального идентификатора доказывающего агента.

2.2. Расширение протокола аутентификации агентов РРТС

Основная суть предлагаемого решения заключается в следующем. При встрече двух множеств агентов РРТС в заданной точке два «первых» агента разных множеств, попадающих в область видимости друг друга, осуществляют аутентификацию. Каждая пара последующих агентов разных множеств также должна пройти аутентификацию, но не только друг с другом, но и с другими агентами другого множества, которые находятся в области видимости.

Вместо того, чтобы последовательно осуществлять аутентификацию новых агентов в данной работе предлагается использовать принцип «круговой поруки» или делегированной аутентификации. Пусть у «первого» агента в постоянной памяти хранится список открытых ключей агентов в его области видимости, которые прошли аутентификацию успешно — доверенный список, а также тех, которые не прошли проверку — список нарушителей. Тогда, в случае если «первый» агент прошел аутентификацию успешно, данный агент может «поручиться» за последующего агента. Таким образом, пока любой агент системы находится в области видимости хотя бы одного другого агента, он всегда сможет получить подтверждение того, что аутентификация ранее была пройдена успешно. Аналогичный принцип может быть применен и к нарушителям. В случае, если один из агентов доверенного списка уже обнаружил подозрительного агента, то эта информация может быть передана другим агентам, что исключит дополнительную процедуру аутентификации с нарушителем. Представим данную процедуру в виде дерева решений (рис. 1).

Рассмотрим пошаговое описание предлагаемого протокола аутентификации, в основе которого будет использована схема идентификации Фейга — Фиата — Шамира. Генерация параметров базового протокола подразумевает следующую последовательность действий.

1. Для каждого нового задания $O = \{o_1, o_2, \ldots, o_j\}$ оператор выбирает пару больших простых чисел p и q, а также рассчитывает основание модуля $n = pq$. Полученное значение n является открытым и передается по каналу связи всем агентам РРТС в виде идентификатора задания вместе со всей необходимой служебной информацией для выполнения задания. Также эта информация должна включать параметры базового протокола k и t. Это предполагает, что что в зависимости от сложности и важности задания стойкость базового протокола может быть изменена.

2. После получения задания O каждый агент системы a_c, $c = 1, 2, ..., m$ в соответствии с параметрами базового протокола формирует открытый $V_c = v_1, v_2, \ldots, v_k$ и секретный $S_c = s_1, s_2, \ldots, s_k$ ключи.

Основная схема аутентификации включает в себя следующие этапы (правая ветвь дерева на рис. 1):

1. Аналогично первому шагу базового протокола, сторона А выбирает случайное число r, случайный бит e и вычисляет x. Результат вычисления отправляется стороне В. Помимо этого, передаваемое сообщение должно содержать открытый ключ V_A.

2. Сторона В, получив открытый ключ стороны А, выполняет запрос на делегированную аутентификацию соседним агентам. Каждый агент имеет список доверенных агентов T_c и нарушителей M_c, которые обновляются при каждом акте коммуникации с соседними агентами.

В том случае, если открытый ключ уже хранится в одном из списков любого соседнего агента, то он возвращает в ответ 1 или –1 (если V_A входит в список доверенных агентов T_c или нарушителей M_c соответственно).

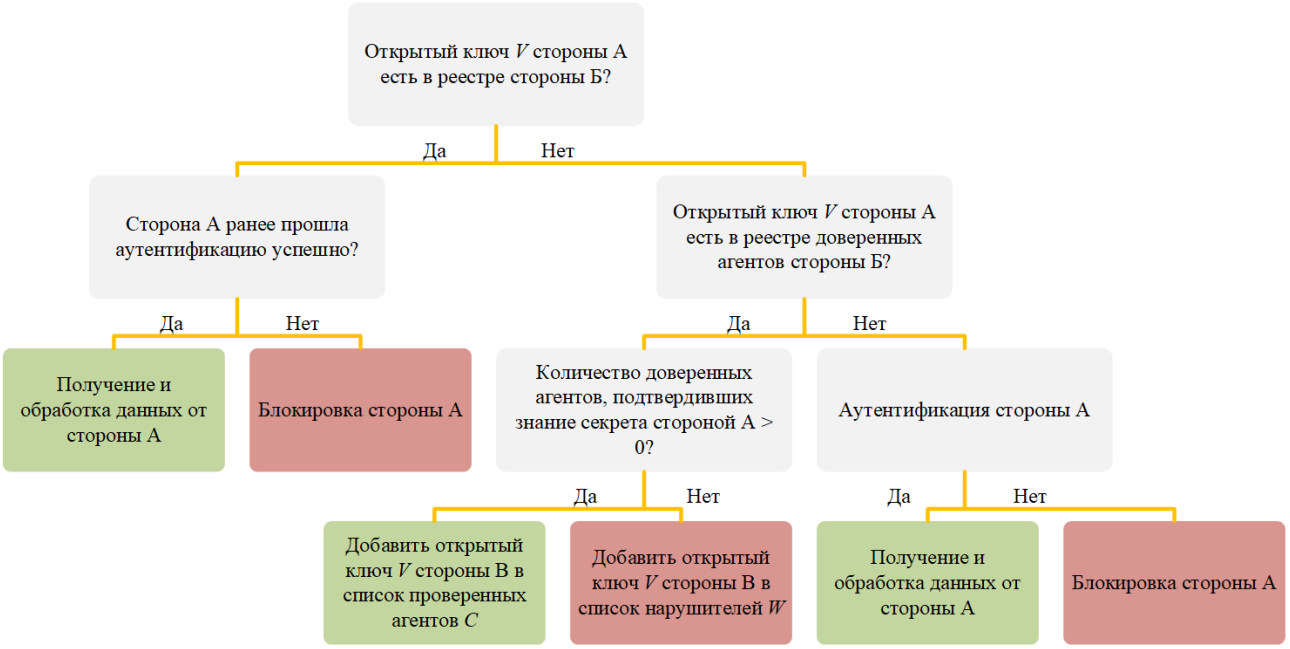

Рис. 1. Представление протокола аутентификации агентов в процессе масштабирования в виде дерева решений
[Fig. 1. Representation of the agent authentication protocol during scaling in the form of a decision tree]

Если же V_A не входит ни в один из списков соседних агентов, то они возвращают 0. Отсутствие ответа на запрос от любого соседнего агента также приравнивается к 0.

Если множество ответов R_B на запрос стороны В содержит неотрицательные элементы, то открытый ключ V_A добавляется в список T_B, делегированная аутентификация считается пройденной. В противном случае, агент считается нарушителем и его открытый ключ добавляется в список M_B. Если же все элементы множества R_B равны 0 или ответ на запрос от соседних агентов не последовал, то выполняется процедура аутентификации согласно пунктам 2–4 базового протокола. В зависимости от результата проверки знания секрета открытый ключ V_A добавляется в один из списков T_B или M_B.

Также необходимо отметить, что при удалении агентов на расстояние, превышающее область видимости, открытый ключ этого агента удаляется из списка T_B. В результате этого, при повторной встрече агентов будет запущена повторная процедура аутентификации. Но в том случае, пока агент находится в области видимости хотя бы одного агента, он всегда сможет пройти делегированную аутентификацию.

3. РЕЗУЛЬТАТЫ И ИХ ОБСУЖДЕНИЕ

Для проведения эксперимента была выполнена программная реализация предложенного решения на языке программирования Python. Визуализация взаимодействия агентов РРТС, а также формирование графиков для оценки эффективности предложенного решения выполнены с помощью библиотеки Matplotlib. При проведении моделирования был использован компьютер со следующими характеристиками: процессор Intel Core i7-8550U с тактовой частотой 1,8 ГГц, 8 ГБ оперативной памяти. Использованы параметры моделирования, указанные в табл. 1.

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

Наименование параметра	Значение
Количество агентов РРТС, m	10, 50, 100
Количество вредоносных агентов	0, 1, 25 %, 50 %
Количество экспериментов для каждого соотношения агентов / нарушителей	100
Количество задач, j	10, 50, 100
Скорость перемещения агентов	1,5 м/с
Размер карты	60×60 м

На рис. 2 представлен пример исходных данных для проведения эксперимента. Два множества агентов (синие и зеленые круги в левом и правом нижнем углах карты) должны встретиться друг с другом в центре карты (черными крестиками обозначены позиции агентов, которые генерируются случайным образом в окрестности центра карты).

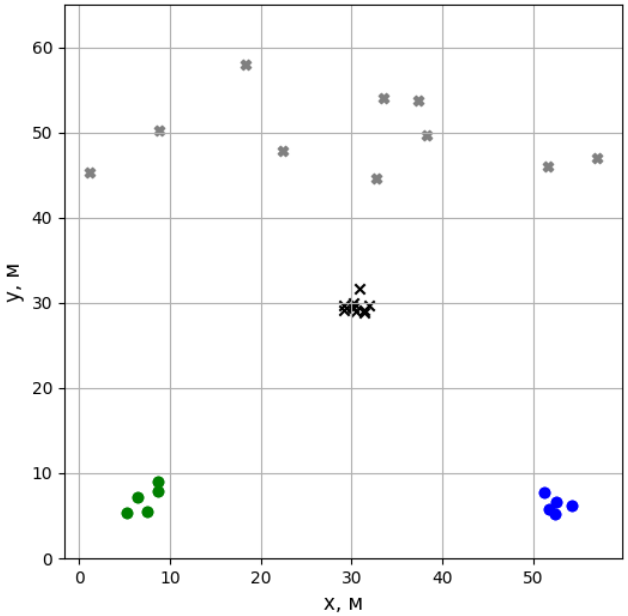

Рис. 2. Пример задания РРТС численностью 10 агентов
[Fig. 2. Example of a SRS task with 10 agents]

Для масштабирования системы агенты должны убедиться в том, что новые агенты являются «своими», и только после этого все агенты системы могут приступить к процедуре распределения задач (позиции которых обозначены серыми жирными крестиками) и их выполнения. Дополнительным допущением является то, что каждый агент может закрепить за собой не более двух задач для выполнения.

Для оценки результатов моделирования использованы следующие показатели эффективности выполнения задания РРТС: количество шагов симуляции, максимальная длина пути агентов, количество актов аутентификации.

Показатель количества шагов симуляции использован по следующей причине. Независимо от того, какая криптосистема будет использоваться на практике, для аутентификации агентов необходимо по меньшей мере два раунда коммуникации агентов (запрос — ответ). Для простоты расчетов будем полагать, что стандартный информационный обмен агентов требует один шаг симуляции, а процедура аутентификации — два. Основная сложность использования времени выполнения задания в качестве явного показателя эффективности заключается в том, что используемый в данной работе протокол Фейга — Фиата — Шамира имеет низкую вычислительную сложность, а максимальные трудозатраты заключаются только в поиске k чисел, взаимно-простых с n для формировании закрытого ключа. Эта процедура выполняется каждым агентом только один раз (для конкретного задания), а ее продолжительность зависит непосредственно от вычислительной платформы робототехнического устройства, поэтому в данной работе этим временем можно пренебречь. С другой стороны, если при инициализации процедуры аутентификации агенты находятся в движении, то необходимо уменьшить скорость перемещения или остановиться, чтобы не прервать выполнение процедуры в случае выхода агентов из области видимости друг друга. Необходимость коррекции скорости движения агентов требует учета их кинематической схемы, а также использования процедур планирования пути и траектории движения. Такой подход избыточно усложнит условия проведения эксперимента и возможность его воспроизведения другими исследователями. Исходя из этого, в данной работе сделано допущение, что каждый акт аутентификации двух агентов требует два шага симуляции, а агенты при этом полностью останавливаются.

Во всех проведенных экспериментах расчет количества нарушителей соответствует следующим сценариям:

– константное значение нарушителей: 0, 1 агент;

– динамически вычисляемое значение: 25 % и 50 % от общей численности агентов.

В табл. 2 представлены усредненные результаты количества шагов симуляции при выполнении задания РРТС, численностью 10, 50 и 100 агентов.

Сравнение эффективности выполнения задания РРТС проводится с использованием базового и предложенного протоколов аутентификации (обозначены в табл. 2–5 как БП и РП соответственно). Помимо этого, в сравнении приводятся результаты выполнения задания без использования средств аутентификации (сокращение в таблицах — БЗИ) для объективной оценки полученных результатов, а также демонстрации необходимости обеспечения информационной безопасности в РРТС.

Таблица 2. Усредненные показатели количества шагов симуляции [Table 2. Averaged number of simulation steps]

Количество агентов РРТС / из них нарушителей	РП	БП	БЗИ
10 / 0	60,3	67,0	47,8
10 / 1	65,3	72,1	51,9
10 / 3	67,2	73,9	62,5
10 / 5	71,9	78,6	74,3
50 / 0	133,4	213,5	50,0
50 / 1	136,8	218,4	53,2
50 / 13	138,2	220,5	64,2
50 / 25	136,1	202,9	80,1
100 / 0	256,1	443,3	50,4
100 / 1	253,9	454,1	53,8
100 / 25	240,4	428,0	67,1
100 / 50	234,7	414,4	80,9

Так, согласно результатам, представленным в табл. 2, количество шагов симуляции при использовании расширенного протокола аутентификации уменьшено от 8,52 % (71,9 против 78,6) до 10 % (60,3 против 67,0) по сравнению с базовым протоколом при моделировании РРТС численностью 10 агентов. При 50 агентах в РРТС значение рассматриваемого критерия уменьшено от 32,92 % (136,1 против 202,9) до 37,52 % (133,4 против 213,5), а при 100 агентах — от 42,23 % (256,1 против 443,3) до 44,09 % (253,9 против 454,1).

Данное преимущество достигается за счет уменьшения количества актов аутентификации агентов, которые замещаются простым запросом, который может быть встроен в стандартный протокол информационного обмена между агентами. В табл. 3 показаны усредненные результаты оценки количества актов аутентификации (аббревиатуры РП-А и БП-А для предложенного и базового протоколов) и запросов на делегированную аутентификацию (РП-З).

Таблица 3. Усредненные показатели количества актов аутентификации [Table 3. Average indicators of the number of authentication acts]

Количество агентов РРТС / из них нарушителей	РП-А	РП-З	БП-А
10 / 0	20,3	71,8	92,1
10 / 1	20,7	72,0	92,7
10 / 3	21,8	71,4	93,2
10 / 5	22,3	70,3	92,6
50 / 0	134,5	2643,8	2778,3
50 / 1	126,4	2623,0	2749,4
50 / 13	141,5	2634,2	2775,7
50 / 25	153,0	2615,7	2768,7
100 / 0	269,0	12381,7	12650,7
100 / 1	273,1	12331,4	12604,5
100 / 25	278,3	11711,3	11989,6
100 / 50	302,3	11243,0	11545,3

Согласно результатам, представленным в табл. 3, предложенное решение позволило уменьшить количество шагов симуляции за счет уменьшения количества актов аутентификации: от 68,28 % (22,3 против 70,3) до 71,73 % (20,3 против 71,8) при моделировании РРТС из 10 агентов, от 94,15 % (153,0 против 2615,7) до 95,18 % (126,4 против 2623,0) при 50 агентах и от 97,31 % (302,3 против 11243,0) до 97,83 % (269,0 против 12381,7) в случае РРТС, состоящей из 100 агентов. Стоит также отметить, что, несмотря на то, что количество актов аутентификации существенно уменьшено, единая точка входа агентов в систему оказалась не достигнута. Это объясняется тем, что в самом начале функционировании агенты имеют пустые списки доверенных агентов

и нарушителей. Поэтому каждый агент начинает осуществлять аутентификацию по принципу «каждый с каждым» до тех пор, пока у агентов не будут сформированы собственные реестры, что и позволит заменить акт аутентификации на запрос делегированной аутентификации.

Согласно табл. 2, использование предложенного протокола увеличивает количество шагов симуляции при выполнении задания агентами РРТС до 190,11 % (234,7 против 80,9). Этот результат является ожидаемым. Однако, для сравнения более наглядным будет использование такого показателя эффективности выполнения задания РРТС как максимальная длина пути, пройденная агентами РРТС при выполнении задания (табл. 4).

Таблица 4. Усредненные показатели максимальной длины пути, м
[Table 4. Average indicators of the maximum path length, m]

Количество агентов РРТС / из них нарушителей	РП	БП	БЗИ
10 / 0	68,4	68,4	68,7
10 / 1	74,85	74,85	73,8
10 / 3	77,85	77,85	89,25
10 / 5	84,0	84,0	106,8
50 / 0	71,7	71,7	72,0
50 / 1	71,55	71,55	75,6
50 / 13	86,25	86,25	91,8
50 / 25	85,8	85,8	115,65
100 / 0	73,2	73,2	72,6
100 / 1	76,5	76,5	76,2
100 / 25	88,2	88,2	96,15
100 / 50	87,6	87,6	116,85

Согласно полученным результатам, независимо от того, используется ли базовый или предложенный протоколы, максимальная длина пути сокращается до 25,81 % (85,8 м против 115,65 м) по сравнению с результатами моделирования без использования средств аутентификации агентов. Дело в том, что в последнем случае агенты предполагают, что в процессе распределения задач каждый из агентов возьмет ровно по одной задаче с минимальным расстоянием до нее и выполнит ее. Однако, модель нарушителя, рассматриваемая в данной работе, предполагает, что нарушитель выберет задачу, наиболее удаленную от собственной позиции, сообщит другим агентам, но не станет ее выполнять. В результате этого первый агент, выполнивший закрепленную за ним задачу, должен выбрать новую задачу для выполнения. В результате этого длина пути существенно возрастает.

Максимальная длина пути при использовании предложенного и базового протоколов одинаковы. Это объясняется тем, что после соотнесения нарушителей в соответствующий список, доверенные агенты распределяют задачи между собой с учетом меньшего количества агентов, чем задач. Таким образом, на первой итерации распределения задач агенты выбирают по одной задаче из общего списка. На второй итерации агенты наблюдают такую ситуацию, когда часть задач остаются свободными. Соответственно, агенты выбирают дополнительные задачи по критерию минимальной дистанции от первой выбранной задачи. В результате полного распределения задач и полной детерминированности процедуры выполнения задания максимальная длина пути агентов сокращается.

Представленные результаты по показателям количества шагов симуляции и максимальной длины пути можно рассматривать как наилучший и наихудший варианты выполнения задания при следующем допущении. Пусть в наилучшем варианте время информационного обмена агентов при аутентификации является настолько малым, что им можно пренебречь. Тогда время, затраченное на выполнение задания агентами РРТС будет зависеть непосредственно от показателя максимальной длины пути при равноускоренном движении агентов. А для наихудшего варианта можно считать, что время информационного обмена при аутентификации является постоянным и равно времени, за которое агент проезжает расстояния между двумя дискретными моментами времени срабатывания вычислительного устройства агента. В этом случае количество шагов симуляции

также можно считать максимальной длиной пути агентов, а среднее значение этих показателей позволит получить среднее время выполнения задания агентами РРТС. Полученные результаты отражены в табл. 5.

Таким образом, с учетом всех допущений, приведенных в данной работе, прирост среднего значения эффективности выполнения задания составляет:

– от 4,12 % (51,97 с против 54,2 с) до 4,95 % (42,9 с против 45,13 с) при РРТС из 10 агентов;

– от 23,14 % (73,97 с против 96,23 с) до 28,14 % (69,45 с против 96,65 с) при РРТС из 50 агентов;

– от 35,8 % (107,43 с против 167,33 с) до 37,73 % (110,13 с против 176,87 с) при РРТС, состоящей из 100 агентов.

Таблица 5. Среднее расчетное время выполнения задания, с
[Table 5. Average estimated time to complete the task, s]

Количество агентов РРТС / из них нарушителей	РП	БП	БЗИ
10 / 0	42,9	45,13	38,83
10 / 1	46,72	48,98	41,9
10 / 3	48,35	50,58	50,58
10 / 5	51,97	54,2	60,37
50 / 0	68,37	95,07	40,67
50 / 1	69,45	96,65	42,93
50 / 13	74,82	102,25	52,0
50 / 25	73,97	96,23	65,25
100 / 0	109,77	172,17	41,0
100 / 1	110,13	176,87	43,33
100 / 25	109,53	172,07	54,42
100 / 50	107,43	167,33	65,92

Также стоит отметить, что использование средств аутентификации агентов увеличивает время выполнения задания до 62,98 % (107,43 с против 65,92 с). Однако, в данной работе введено допущение, согласно которому каждый агент может выполнить две задачи. Таким образом, при равном количестве агентов и задач и при наличии 50 % нарушителей задание РРТС в любом случае будет выполнено. Но на практике, у агента может не хватать уровня заряда аккумуляторной батареи для выполнения дополнительной задачи, а также не исключено возникновение неисправностей, что делает выполнение задания невозможным, так как агенты РРТС должны вернуться на базу для заряда аккумулятора (ремонта) и последующего выполнения оставшихся задач. Если же рассматривать такие задания, для которых оперативность их выполнения является критически важным показателем [21, 22], то подобное задание можно считать невыполненным, что и обуславливает необходимость использования средств информационной безопасности.

ЗАКЛЮЧЕНИЕ

В данной работе рассмотрен вопрос аутентификации РРТС в процессе масштабирования численности агентов. В рамках представленного протокола сложность угадывания множителей основания модуля остается такой же, как и в оригинальной схеме Фейга — Фиата — Шамира. Аналогично при использовании любого другого протокола в качестве базового — криптографическая стойкость протокола зависит непосредственно от выбранных параметров протокола. При этом выбор того или иного протокола аутентификации и его параметров в случае РРТС зависит как от требований к обеспечению информационной безопасности, так и от ограничений вычислительной платформы, на которой этот протокол будет выполняться.

Предложенный подход делегированной аутентификации новых агентов стремится обеспечить единую точку входа агентов системы, что значительно уменьшает общее время, необходимое для выполнения задания, за счет уменьшения количества актов аутентификации. С другой стороны, предложенный подход привносит необходимость отслеживания поведения доверенных агентов, так как агент, являющийся доверенным, может искажать результаты ответов, тем самым блокируя доверенных агентов и поручаясь за нарушителей. Эта особенность требует использования соответствующих методов,

например, разграничения доступа или определении уровня доверия к тому или иному агенту.

Таким образом, авторы считают наиболее актуальными следующие направления дальнейших исследований:

1. Расстояние, пройденное агентами в ходе выполнения задания, уменьшается в случае использования средств обеспечения информационной безопасности. При этом увеличивается время, необходимое для коммуникации агентов. В рамках проведения компьютерного моделирования функционирования агентов получение полной картины о результатах эффективности РРТС является достаточно сложной задачей. Поэтому необходимо проведение натурных экспериментов.

2. В текущей работе рассмотрена только модель внешнего нарушителя. В том случае, если доверенный агент начнет демонстрировать некорректное поведение, например, «поручаться» за агентов-нарушителей или наоборот, помечать доверенных агентов как нарушителей, необходимо проведение дополнительных исследований, направленных на выявление внутренних нарушителей, участвующих в процедуре аутентификации новых агентов РРТС.

БЛАГОДАРНОСТИ

Исследование выполнено при финансовой поддержке Минцифры России (грант ИБ), проект № 45/21-к.

КОНФЛИКТ ИНТЕРЕСОВ

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

СПИСОК ЛИТЕРАТУРЫ

1. *Петренко, В. И.* Анализ технологий обеспечения информационной безопасности мультиагентных робототехнических систем с роевым интеллектом / В. И. Петренко, Ф. Б. Тебуева, М. М. Гурчинский, С. С. Рябцев // Наука и бизнес: пути развития. – 2020. – № 4(106). – С. 96–99.

2. *Higgins, F.* Threats to the swarm: Security considerations for swarm robotics / F. Higgins, A. Tomlinson, K. M. Martin // Int. J. Adv. Secur. – 2009. – Vol. 2, No 2. – P. 288–297.

3. *Sargeant, I.* Review of Potential Attacks on Robotic Swarms / I. Sargeant, A. Tomlinson // IntelliSys 2016: Proceedings of SAI Intelligent Systems Conference (IntelliSys). – 2018. – P. 628–646.

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. – С. 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. – № 1(1). – С. 42–48.

6. *Zakiev, A.* Swarm Robotics: Remarks on Terminology and Classification / A. Zakiev, T. Tsoy, E. Magid // Interactive Collaborative Robotics (ICR 2018). – 2018. – P. 291–300.

7. *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. – № 2(90). – С. 47–52.

8. *Madhu, A.* Positioning Optimization of Drones using IMU and Securing UAV Communication by implementing Hybrid Cryptosystem / A. Madhu, M. B.-H. Prajeesha // 5th International Conference on Trends in Electronics and Informatics (ICOEI). – 2021. – P. 681–686.

9. *Sandoval, S.* Cyber Security Assessment of the Robot Operating System 2 for Aerial Networks / S. Sandoval, P. Thulasiraman // IEEE International Systems Conference (SysCon). – 2019. – P. 1–8.

10. Gazebo. – Текст: электронный // Режим доступа: http://gazebosim.org/ (дата обращения: 17.02.2022).

11. ROS2. – Текст: электронный // Режим доступа: https://github.com/ros2/ros2/wiki/DDS-and-ROS-middlewareimplementations/ (дата обращения: 17.02.2022).

12. *Sabir, B. E.* Authentication and load balancing scheme based on JSON Token For Multi-Agent Systems / B. E. Sabir, M. Youssfi, O. Bouattane, H. Allali // Procedia Computer Science. – 2019. – Vol. 148. – P. 562–570.

13. *Moon, A.* Mutual Entity Authentication Protocol Based on ECDSA for WSN / A. Moon, U. Iqbal, G. Bhat // Procedia Computer Science. – 2016. – Vol. 89. – P. 187–192.

14. *Khanh, T. D.* TRA: Effective Authentication Mechanism for Swarms Of Unmanned Aerial Vehicles / T. D. Khanh, I. Komarov, L. D. Don, R. Iureva and S. Chuprov // IEEE Symposium Series on Computational Intelligence (SSCI). – 2020. – P. 1852–1858.

15. *Chen, A.* ToAM: a task-oriented authentication model for UAVs based on blockchain / A. Chen, K. Peng, Z. Sha // EURASIP J. Wirel. Commun. Netw. – 2021. – Vol. 1. – P. 166–171.

16. *Иванов, Д. Я.* Перспективы применения блокчейн-технологии в групповой робототехнике / Д. Я. Иванов // Робототехника и техническая кибернетика. – 2019. – Т. 7, № 4. – С. 300–305.

17. *Шляхтина, Е. А.* Схема групповой аутентификации на основе доказательства с нулевым разглашением / Е. А. Шляхтина, Д. Ю. Гамаюнов // ПДМ. – 2021. – № 51. – С. 68–84.

18. *Manulis, M.* Democratic group signatures: on an example of joint ventures / M. Manulis // Proceedings of the 2006 ACM Symposium on Information, Computer and Communications Security. – 2006. – P. 365–372.

19. *Алферов, А. П.* Основы криптографии: Учебное пособие. 2-е изд. М.: Гелиос АРВ. – 2002. – 480 с.

20. *Fiat, A.* How To Prove Yourself: Practical Solutions to Identification and Signature Problems / A. Fiat, A. Shamir // Advances in Cryptology. – 1987. – P. 186–194.

21. *Sujit, P. B.* Cooperative forest fire monitoring using multiple UAVs / P.B. Sujit, D. Kingston, R. Beard // IEEE Conference on Decision and Control. – 2007. – P. 4875–4880.

22. *Чжай, М.* Многоагентная робототехническая система спасения при землетрясениях: дис. ... канд. техн. наук // Москва: Московский Государственный Технический Университет имени Н. Э. Баумана. – 2019. – 158 с.

Павлов Андрей Сергеевич — старший преподаватель кафедры компьютерной безопасности Института цифрового развития Северо-Кавказского федерального университета.
E-mail: anspavlov@ncfu.ru
ORCID iD: https://orcid.org/0000-0002-8413-8706

Свистунов Николай Юрьевич — ассистент кафедры компьютерной безопасности Института цифрового развития Северо-Кавказского федерального университета.
E-mail: nusvistunov@ncfu.ru
ORCID iD: https://orcid.org/0000-0002-3277-1120

Петренко Вячеслав Иванович — канд. техн. наук, доцент, заведующий кафедрой организации и технологии защиты информации 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 Института цифрового развития Северо-Кавказского федерального университета.
E-mail: ftebueva@ncfu.ru
ORCID iD: https://orcid.org/0000-0002-7373-4692

Копытов Владимир Вячеславович — д-р техн. наук, профессор, профессор базовой кафедры «Инфоком-С» Института цифрового развития Северо-Кавказского федерального университета.
E-mail: v.kopytov@infocom-s.ru
ORCID iD: https://orcid.org/ 0000-0002-3053-1641

Тищенко Евгений Николаевич — д-р экон. наук, профессор, декан факультета компьютерных технологий и информационной безопасности Ростовского государственного экономического университета (РИНХ).
E-mail: celt@inbox.ru
ORCID iD: https://orcid.org/ 0000-0003-1527-4904

DOI: https://doi.org/10.17308/sait/1995-5499/2022/4/23-38 ISSN 1995-5499
Received 26.04.2022
Accepted 05.12.2022

PROTOCOL FOR THE DELEGATED AUTHENTICATION OF NEW AGENTS WHEN THE NUMBER OF AGENTS IS SCALING IN SWARMING ROBOT SYSTEMS

© 2022 A. S. Pavlov✉[1], N. U. Svistunov[1], V. I. Petrenko[1], F. B. Tebueva[1], V. V. Kopytov[1], E. N. Tishchenko[2]

[1]North-Caucasus Federal University
2, Kulakov Avenue, 355029 Stavropol, Russian Federation
[2]Rostov State University of Economics (RINH)
69, Bolshaya Sadovaya Street, 344002 Rostov-on-Don, Russian Federation

Annotation. The intensive development of group robotics, including swarm robotic systems (SRS), actualizes the issues of information security. Known approaches to agent authentication of swarm robotic systems do not take into account the scalability properties of the system, which contributes to the «avalanche effect» with a significant number of agents used. The purpose of this work is to increase the efficiency of performing such tasks by SRS agents, which require an increase in the concentration of agents, by taking into account the time required to authenticate new agents. In accordance with the task set, the task of extending the protocol for delegated authentication of new agents while scaling the coverage of SRS agents based on Feige — Fiat — Shamir identification scheme with zero knowledge has been developed. An element of scientific innovation is an impressive set of production rules presented in image selections that allow the use of agent information exchange algorithms using a distributed registry of delegated authentication protocols for agents that have previously successfully passed this test. The specific features of the presented approach include solutions to use any basic authentication protocol determined by the hardware distribution of the computing platform of robotic devices that are part of the SRS. Also agents have ability to «switch» between the highest priority tasks and, in interaction with other agents of painless authentication, in the search area for identified at least one neighbor agent. The presented protocol is implemented in

✉ Pavlov Andrey S.
e-mail: anspavlov@ncfu.ru

the form of software in the Python programming language, which can be used in modeling SRS control systems.
Keywords: swarm robotic systems, information security, introduction of malicious agents, authentication, zero-knowledge proof.

CONFLICT OF INTEREST

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

REFERENCE

1. *Petrenko V. I. Tebueva F. B., Gurchinsky M. M. and Ryabtsev S. S.* (2020) Analiz tehnologij obespechenija informacionnoj bezopasnosti mul'tiagentnyh robototehnicheskih sistem s roevym intellektom [Analysis of information security technologies for multi-agent robotic systems with swarm intelligence]. *Science and business: ways of development*. 4(106). P. 96–99. (in Russian)

2. *Higgins F., Tomlinson A. and Martin K. M.* (2019) Threats to the swarm: Security considerations for swarm robotics. *Int. J. Adv. Secur*. 2(2). P. 288–297.

3. *Sargeant I. and Tomlinson A.* (2018) Review of Potential Attacks on Robotic Swarms. *Proceedings of SAI Intelligent Systems Conference (IntelliSys)*. P. 628–646.

4. *Basan A. S. and Basan E. S.* (2017) Model' ugroz dlja sistem gruppovogo upravlenija mobil'nymi robotami [Threat model for group control systems for mobile robots]. *VIII All-Russian Scientific Conference "System Synthesis and Applied Synergetics"*. P. 205–212. (in Russian)

5. *Yurieva R. A., Komarov I. I. and Dorodnikov N. A.* (2016) Postroenie modeli narushitelja informacionnoj bezopasnosti dlja mul'tiagentnoj robototehnicheskoj sistemy c decentralizovannym upravleniem [Building an information security violator model for a multi-agent robotic system with decentralized control]. *Program systems and computational methods*. 1(1). P. 42–48. (in Russian)

6. Zakiev A., Tsoy T. and Magid E. (2018) Swarm Robotics: Remarks on Terminology and Classification. *Interactive Collaborative Robotics (ICR 2018)*. P. 291–300.

7. *Zikratov I. A., Zikratova T. V. and Lebedev I. S.* (2014) Doveritel'naja model' informacionnoj bezopasnosti mul'tiagentnyh robototehnicheskih sistem s decentralizovannym upravleniem [Confidence model of information security of multi-agent robotic systems with decentralized control]. *Scientific and technical bulletin of information technologies, mechanics and optics*. 2(90). P. 47–52. (in Russian)

8. *Madhu A. and Prajeesha M. B.-H.* (2021) Positioning Optimization of Drones using IMU and Securing UAV Communication by implementing Hybrid Cryptosystem. *5th International Conference on Trends in Electronics and Informatics (ICOEI)*. P. 681–686.

9. *Sandoval S. and Thulasiraman P.* (2019) Cyber Security Assessment of the Robot Operating System 2 for Aerial Networks. *IEEE International Systems Conference (SysCon)*. P. 1–8.

10. Gazebo – Text: electronic. http://gazebosim.org/. Accessed 17.02.2022.

11. ROS2 – Text: electronic. https://github.com/ros2/ros2/wiki/DDS-and-ROS-middleware-reimplementations/. Accessed 17.02.2022.

12. *Sabir B. E., Youssfi M., Bouattane O. and Allali H.* (2019) Authentication and load balancing scheme based on JSON Token For Multi-Agent Systems. *Procedia Computer Science*. 148. P. 562–570.

13. *Moon A., Iqbal U. and Bhat G.* (2016) Mutual Entity Authentication Protocol Based on ECDSA for WSN. *Procedia Computer Science*. 89. P. 187–192.

14. *Khanh T. D., Komarov I., Don L. D., Iureva R. and Chuprov S.* (2020) TRA: Effective Authentication Mechanism for Swarms Of Unmanned Aerial Vehicles. *IEEE Symposium Series on Computational Intelligence (SSCI)*. P. 1852–1858.

15. *Chen A., Peng K. and Sha Z.* (2021) ToAM: a task-oriented authentication model for UAVs based on blockchain. *EURASIP J. Wirel. commun. netw.* 1. P. 166–171.

16. *Ivanov D. Ya.* (2019) Perspektivy primenenija blokchejn-tehnologii v gruppovoj roboto-

tehnike [Prospects for the use of blockchain technology in group robotics]. *Robotics and technical cybernetics*. 7(4). P. 300–305. (in Russian)

17. *Shlyakhtina E. A. and Gamayunov D. Yu.* (2021) Shema gruppovoj autentifikacii na osnove dokazatel'stva s nulevym razglasheniem [Group authentication scheme based on zero-knowledge proof]. *PDM*. 51. P. 68–84. (in Russian)

18. *Manulis M.* (2006) Democratic group signatures: on an example of joint ventures. *Proceedings of the 2006 ACM Symposium on Information, Computer and Communications Security*. P. 365–372.

19. *Alferov A. P.* (2002) Osnovy kriptografii [Fundamentals of cryptography]: Textbook. 2nd ed. *Moscow : Helios ARV*. 480 p. (in Russian)

20. *Fiat A. and Shamir A.* (1987) How To Prove Yourself: Practical Solutions to Identification and Signature Problems. *Advances in Cryptology*. P. 186-194.

21. *Sujit P. B., Kingston D. and Beard R.* (2007) Cooperative forest fire monitoring using multiple UAVs. *IEEE Conference on Decision and Control*. P. 4875–4880.

22. *Zhai M.* (2019) Mnogoagentnaja robototehnicheskaja sistema spasenija pri zemletrjasenijah [Multi-agent robotic rescue system during earthquakes]: Ph.D. Tesis. Moscow: Moscow State Technical University named after N. E. Bauman. 158 p. (in Russian)

Pavlov Andrey S. — Senior Lecturer, Department of Computer Security, Institute of Digital Development, North-Caucasus Federal University
E-mail: anspavlov@ncfu.ru
ORCID iD: https://orcid.org/0000-0002-8413-8706

Svistunov Nikolay Yu. — Assistant of the Department of Computer Security of the Institute of Digital Development of the North-Caucasus Federal University
E-mail: nusvistunov@ncfu.ru
ORCID iD: https://orcid.org/0000-0002-3277-1120

Petrenko Vyacheslav I. — Candidate of Technical Sciences, Associate Professor, Head of the Department of Organization and Technology of Information Protection, Institute of Digital Development of the North-Caucasus Federal University
E-mail: vipetrenko@ncfu.ru
ORCID iD: https://orcid.org/0000-0003-4293-7013

Tebueva Fariza B. — Doctor of Physical and Mathematical Sciences, Associate Professor, Head of the Department of Computer Security, Institute for Digital Development, North-Caucasus Federal University
E-mail: ftebueva@ncfu.ru
ORCID iD: https://orcid.org/0000-0002-7373-4692

Kopytov Vladimir V. — Doctor of Technical Sciences, Professor, Professor of the Basic Department «Infocom-S» of the Institute for Digital Development of the North-Caucasus Federal University
E-mail: v.kopytov@infocom-s.ru
ORCID iD: https://orcid.org/ 0000-0002-3053-1641

Tishchenko Evgeniy N. — Doctor of Economic Sciences, Professor, Dean of the Faculty of Computer Technologies and Information Security, Rostov State University of Economics (RINH)
E-mail: celt@inbox.ru
ORCID iD: https://orcid.org/ 0000-0003-1527-4904