УДК 004.056

СОВЕРШЕНСТВОВАНИЕ POLICE OFFICE MODEL ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ РОЕВЫХ РОБОТОТЕХНИЧЕСКИХ СИСТЕМ

И.А. Зикратов[a], А.В. Гуртов[b, c], Т.В. Зикратова[d], Е.В. Козлова[a]

[a] Университет ИТМО, 197101, Санкт-Петербург, Россия, zikratov@cit.itmo.ru

[b] Хельсинский институт информационных технологий, 00014, University of Helsinki, Finland

[c] Аалто Университет, FI-00076, Aalto, Finland

[d] Военный институт (Военно-морской политехнический) ВУНЦ ВМФ «Военно-морская академия», 196602, г. Пушкин, Россия

Аннотация. Рассматриваются аспекты информационной безопасности групповых мобильных робототехнических комплексов с роевым интеллектом. Обсуждаются способы осуществления скрытых атак противоборствующей стороны на роевой алгоритм. Выполнено численное моделирование возможных деструктивных информационных воздействий на муравьиный алгоритм поиска кратчайшего пути. Приведена демонстрация последствий атак на муравьиный алгоритм при различной концентрации в рое роботов-диверсантов. Предложены подходы к обеспечению информационной безопасности в роевых робототехнических системах, основанные на реализации принципов централизованного управления безопасностью мобильных агентов. Разработан метод формирования самоорганизующейся системы управления информационной безопасностью роботов-агентов в роевых коллективах, реализующий Police Office Model – модель обеспечения безопасности на основе полицейских участков, которая применяется для обеспечения информационной безопасности мультиагентных систем. В основу метода положено использование в узлах графа сети полицейских участков, на которые возложены функции идентификации и аутентификации агентов, а также выявления диверсантов как по их формальным признакам, так и по их поведению в рое. Предложен перечень программно-аппаратных компонентов полицейских участков, состоящий из каналов связи между роботами-полицейскими, реестра узлов, базы данных агентов и механизмов шифрования и дешифрования. Предложены варианты логики функционирования механизма информационной безопасности роевых систем, отличающиеся временными диаграммами обмена данными между полицейскими участками. Представлен сравнительный анализ реализаций защищенных роевых систем в зависимости от логики функционирования полицейских участков, интегрированный в роевую систему. Показано, что модель безопасности сохраняет способность функционирования в условиях помех при длительности помехи, сопоставимой со временем преодоления агентом пути между полицейскими участками.

Ключевые слова: информационная безопасность, робототехнический комплекс, рой роботов, муравьиный алгоритм, групповая робототехника, модель Police Office Model, защищенный рой, уязвимость, атака.

POLICE OFFICE MODEL IMPROVEMENT FOR SECURITY OF SWARM ROBOTIC SYSTEMS

I.A. Zikratov[a], A.V. Gurtov[b, c], T.V. Zikratova[d], E.V. Kozlova[a]

[a] ITMO University, 197101, Saint Petersburg, Russia, zikratov@cit.itmo.ru

[b] Helsinki Institute for Information Technology (HIIT), 00014 Helsinki, Finland

[c] Aalto University, FI-00076 Aalto, Finland

[d] Military Institute (Naval Polytechnic) Military Educational and Scientific Center of the Navy "Naval Academy", 196602, Pushkin, Saint Petersburg, Russia

Abstract. This paper focuses on aspects of information security for group of mobile robotic systems with swarm intellect. The ways for hidden attacks realization by the opposing party on swarm algorithm are discussed. We have fulfilled numerical modeling of potentially destructive information influence on the ant shortest path algorithm. We have demonstrated the consequences of attacks on the ant algorithm with different concentration in a swarm of subversive robots. Approaches are suggested for information security mechanisms in swarm robotic systems, based on the principles of centralized security management for mobile agents. We have developed the method of forming a self-organizing information security management system for robotic agents in swarm groups implementing POM (Police Office Model – a security model based on police offices), to provide information security in multi-agent systems. The method is based on the usage of police station network in the graph nodes, which have functions of identification and authentication of agents, identifying subversive robots by both their formal characteristics and their behavior in the swarm. We have suggested a list of software and hardware components for police stations, consisting of: communication channels between the robots in police office, nodes register, a database of robotic agents, a database of encryption and decryption module. We have suggested the variants of logic for the mechanism of information security in swarm systems with different temporary diagrams of data communication between police stations. We present comparative analysis of implementation of protected swarm systems depending on the functioning logic of police offices, integrated in swarm system. It is shown that the security model saves the ability to operate in noisy environments, when the duration of the interference is comparable to the time necessary for the agent to overcome the path between police stations.

Keywords: IT security, robotic complex, swarm of robots, ant algorithm, group robotics, Police Office Model, protected swarm, vulnerability, attack.

Введение

В работе исследуются вопросы применимости механизма безопасности мультиагентных информационных систем (МАС), основанного на модели полицейских участков – Police Office Model (POM) – для решения задач информационной безопасности (ИБ) в мультиагентных робототехнических системах

(МРТС) с роевым интеллектом. В отличие от механизмов жесткой безопасности, таких как шифрование канала связи, схемы криптографической аутентификации и авторизации, политики для предоставления полномочий, использование цифровых подписей и сертификатов и т.д., метод РОМ относят к механизмам мягкой безопасности [1], которые противостоят вредоносным информационным воздействиям, осуществляемым со стороны роботов-диверсантов. Под вредоносным информационным воздействием (атакой) будем понимать деятельность робота-диверсанта, направленную на реализацию угрозы ИБ в отношении роботов-агентов и осуществляемую с использованием информационных средств и технологий, в результате которой выбранное агентами новое действие не будет способствовать приращению целевого функционала МРТС в имеющихся условиях [2]. Иначе говоря, механизмы мягкой безопасности позволяют дать ответ на вопрос: а действительно ли робот-агент, получивший доступ в систему, выполняет действия, направленные на решение стоящих перед МАС (МРТС) задач?

Наиболее распространенными механизмами мягкой безопасности в МАС являются метод защищенных состояний агентов [3], метод Ксюдонга [4], «товарищеская» модель безопасности (Buddy Security Model, BSM) [5, 6], которые хорошо согласуются с принципами построения децентрализованных систем. Условно эти механизмы можно разделить на две группы – основанные на принципах децентрализованного и централизованного управления ИБ соответственно.

В методах первой группы функции ИБ возлагаются на агентов МАС. При этом выявление действий злоумышленника осуществляется в процессе интенсивных межагентных коммуникаций, что предъявляет относительно высокие требования к аппаратной составляющей МАС и приводит соответственно к удорожанию всей системы.

При централизованном управлении решение задач ИБ возлагается на специально созданные структуры, которые в некоторых моделях называются полицейскими участками, Police Office (PO). Суть централизованных механизмов ИБ в МАС состоит в том, что мультиагентная система разбивается на несколько областей (участков), в каждом из которых имеется модуль, осуществляющий функции идентификации и аутентификации агентов, а также анализирующий их деятельность. Очевидно, что правила выделения областей и МАС, а также порядок взаимодействия членов коллектива с РО будут иметь особенности для различных роевых алгоритмов.

Цель настоящей работы – разработка механизма ИБ роевых робототехнических систем, предназначенных для выявления и нейтрализации угроз, связанных с осуществлением скрытых атак на рой. В данной работе предложена модель, основанная на модели Ксюдонга, предназначенная для выявления роботов-диверсантов в роевых робототехнических системах. Показано использование модели РОМ в МРТС на основе численного моделирования широко известного классического муравьиного алгоритма поиска кратчайшего пути [7, 8]. Понимание сути модели РОМ позволит легко реализовать этот механизм в других популярных роевых алгоритмах – пчелином, рое частиц и т.д.

Атаки на муравьиный алгоритм

Муравьиный алгоритм – метаэвристический алгоритм, в котором колония искусственных муравьев в кооперации находит хорошее решение сложных дискретных задач оптимизации. Используя этот алгоритм при выборе направления следования, агенты не только выбирают кратчайший путь, но и ориентируются на опыт предшественников, оставляющих за собой на пути особый фермент – феромон. В работе [9] приведены описание и результаты моделирования атак на муравьиный алгоритм в задаче выбора кратчайшего пути, а также выполнен анализ их уязвимостей (рис. 1).

Исследуемым параметром являлась вероятность выбора P агентом кратчайшего маршрута для следующих исходных данных. N роботов, образующих рой, последовательно перемещается из узла i в узел o в условиях агрессивной среды (при атаках противоборствующей стороны). Количество агентов в рое N=2000, одновременно на участке находятся 50 агентов. Цель роя – выбрать кратчайший путь следования из узла i в узел o (маршрут A, рис. 1). Целью противоборствующей стороны является создание условий для увеличения времени на поиск оптимального маршрута или для выбора неоптимального маршрута (маршрут B, C или D, рис. 1), но который рой будет принимать за оптимальный. Выполнение замысла злоумышленника приведет к увеличению расхода энергии агентами, что, в свою очередь, ограничит их радиус действия и (или) будет способствовать невыполнению группировкой конечной задачи.

Несмотря на очевидную простоту примера, ему присущи типовые элементы более сложных графов, таких как наличие нескольких вершин и ребер, однозначно определяемый кратчайший (маршрут A) и альтернативные маршруты (маршруты B, C и D), типовые действия роя при выборе кратчайшего пути, что позволяет моделировать атаки на уязвимости классического муравьиного алгоритма Ant System.

Для моделирования использовался полигон моделей Kilobot в среде V-REP [10, 11]. Моделировались действия роя в штатном режиме и при атаке путем «внедрения» одного или нескольких роботов.

В штатном режиме изменения вероятностей выбора маршрутов A, B, C и D при последовательном прохождении N роботами – членами роя представлены на рис. 2. На рисунке видно, что процесс выбора пути условно можно разбить на две части – переходный процесс, когда количество отложенного феромо-

на на ребрах в значительной степени носит случайный характер (в данной реализации он закончился примерно при прохождении узла двухсотым роботом), и установившийся режим, когда длинные пути «исчезают» вследствие все большей привлекательности кратчайшего пути (более высокой концентрации феромона на маршруте А), а вероятность выбора кратчайшего пути асимптотически приближается к 1. Так, на рис. 2 видно, что при прохождении участка последним агентом, вероятность выбора им маршрута А составляет 0,93.

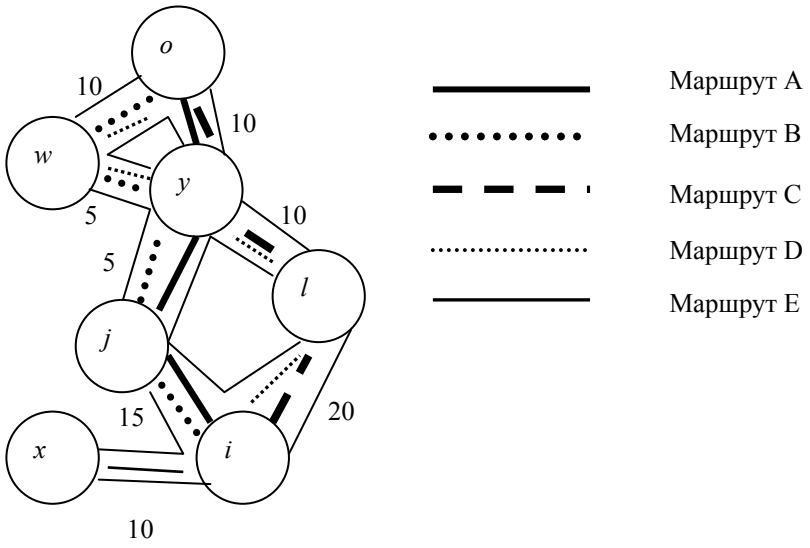


Рис. 1. Муравьиный алгоритм в задаче выбора кратчайшего пути (маршрут А) при наличии иных путей (маршруты B,C,D) и ложного маршрута (маршрут E)

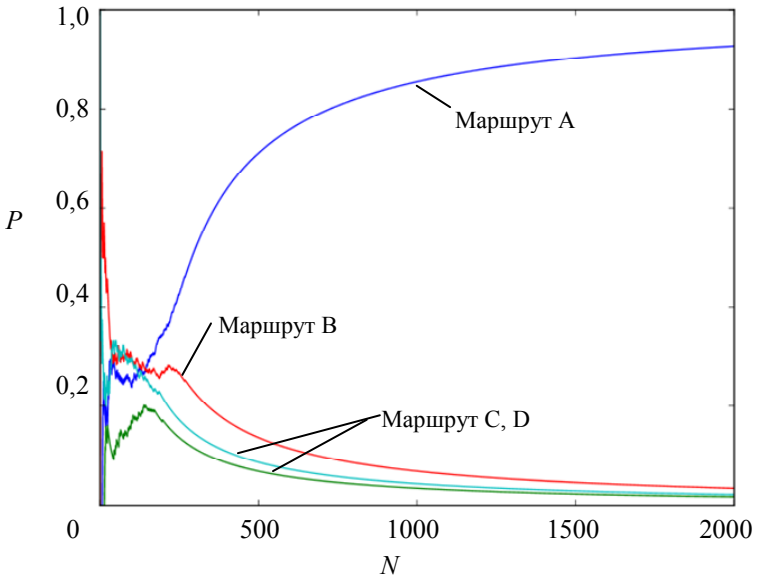


Рис. 2. Зависимость вероятности *P* выбора роем рационального пути от количества *N* роботов, прошедших по ребру без воздействия злоумышленников

При реализации атаки злоумышленником внедряются роботы, являющиеся для данной системы «инородными». Эти роботы начинают свой путь по нерациональному для роя маршруту – ребру (i, l). В зависимости от технических возможностей злоумышленника и от количества времени, в течение которого требуется направить систему по ложному пути, количество роботов-диверсантов может быть различным. Целью фланирования роботов-диверсантов по маршруту является создание более высокой концентрации феромона на ребре (i,l).

На рис. 3 представлены графики, иллюстрирующие влияние роботов-диверсантов, действующих на ребрах (i, l), (l, y), (y, w) и (w, o) (рис. 1), при различных значениях их концентрации по отношению к числу агентов, находящихся на рассматриваемом участке. Так, при наличии на «длинных» ребрах пяти диверсантов (концентрация 1:10, рис. 3, а) видно, что переходный процесс становится более продолжительным, а вероятность выбора маршрута А последним агентом снизилась до 0,59. Увеличение концентрации диверсантов на маршруте приводит практически к равновероятному выбору кратчайшего и иных

маршрутов (рис. 3, б), а уже при концентрации 1:2 возможно снижение вероятности выбора кратчайшего маршрута до пренебрежимо малого значения (рис. 3, в).

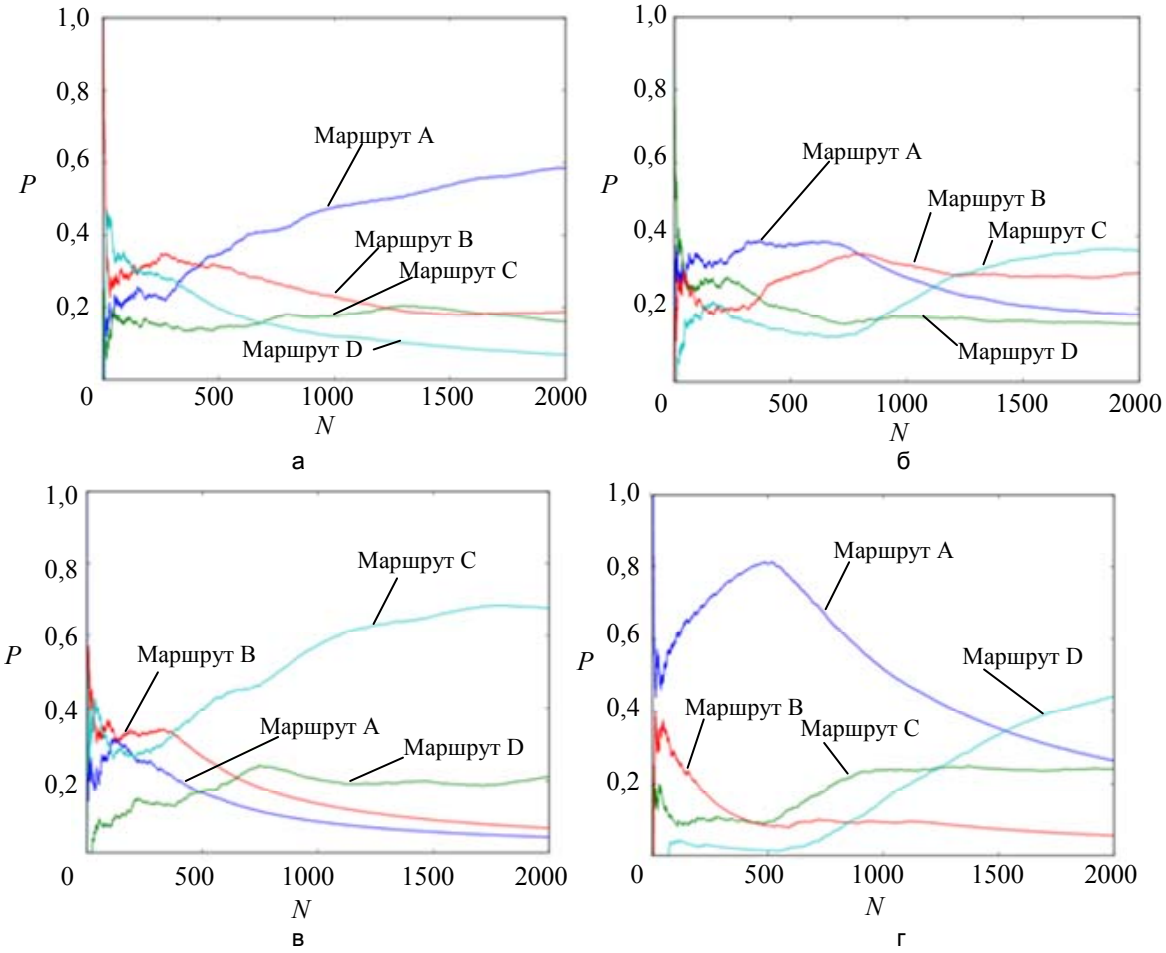


Рис. 3. Значения вероятности *P* выбора роем из *N* агентов рационального пути при действиях диверсантов на этапе поиска кратчайшего пути (примеры реализации) при разной концентрации диверсантов в составе роя: 1:10 (а); 3:10 (б); 1:2 (в); 1:2. Внедрение диверсантов в установившемся режиме (г)

Следует обратить внимание, что внедрение диверсантов в установившемся режиме также приводит к резкому снижению эффективности алгоритма. Так, на реализации, представленной на рис. 3, г, видно, что инъекция в рой 25 диверсантов в установившемся режиме (после прохождения участка пятью-стами агентами) привело к тому, что вероятность выбора кратчайшего маршрута стала меньше вероятности выбора агентами нерационального маршрута С.

Из представленных результатов видно, что уязвимости, присущие муравьиному алгоритму, позволили осуществить деструктивное воздействие на рой путем информационной воздействия через сенсоры агентов без атаки на физическую и (или) программную компоненту робота. Физическое внедрение в рой роботов-диверсантов способно оказать дестабилизирующее влияние на процесс движения группировки как на этапе переходного процесса (в процессе поиска кратчайшего пути), так и в установившемся режиме, когда кратчайший путь движения уже найден. Следовательно, механизмы обеспечения ИБ должны осуществляться непрерывно на всех этапах выполнения задачи, быть масштабируемыми по пространству и обеспечивать устойчивость функционирования во времени.

Метод формирования системы информационной безопасности роботов-агентов в роевых коллективах, реализующий POM

Очевидно, что для предотвращения указанных выше атак роевые робототехнические комплексы должны оснащаться механизмами ИБ, отвечающими некоторым специфическим требованиям по сравнению с аналогичными механизмами защиты МАС [12–17]. Для обеспечения ИБ МАС систем различают два подхода к реализации таких механизмов – централизованный и децентрализованный. В частности, децентрализованный подход основан на принципе обеспечения взаимной безопасности и представляет собой такую систему безопасности, в которой агенты отвечают за безопасность друг друга, отслеживая происходящие в системе события и взаимодействуя между собой и внешней средой. В ходе межагентных

коммуникаций агенты системы обмениваются по каналам связи информацией о своем состоянии и выполняемых действиях, а также специальными сообщениями, которые несут в себе секретную информацию о состояниях известных им агентов и о возможных угрозах с их стороны либо со стороны узлов сети. Таким образом, все агенты системы получают информацию о потенциальных угрозах их безопасности. Информируя своих соседей о возможной опасности (например, при появлении «чужого» агента в системе), каждый из агентов несет ответственность за безопасность своего окружения и всей системы в целом. Привлекательность этой модели состоит в отсутствии какого-либо единого центра безопасности, что приводит к невозможности разрушения модели. Однако применение подобных систем для роевых коллективов, не оснащенных каналами связи, может быть сопряжено с трудностями технического характера и удорожанием системы.

В настоящей работе рассмотрены варианты построения самоорганизующегося механизма ИБ роевых систем, основанного на модели РО и предназначенного для предотвращения скрытых атак на роевые алгоритмы со стороны роботов-диверсантов. Самоорганизация в данном случае заключается в автоматическом формировании полицейских участков в узлах графа маршрутов (рис. 1) в результате работы муравьиного алгоритма. Централизация предусматривает освобождение роботов-агентов от функций ИБ и возложение этих функций на интегрированные в роевую модель специальные аппаратно-программные комплексы, реализующие функции РО и обеспечивающие поддержку межагентного взаимодействия и самоорганизации роя.

В состав каждого РО входят:

- агенты-полицейские по числу выходящих из узла (вершины графа) маршрутов (дуг);
- реестр узлов;
- база данных роботов-агентов;
- модуль шифрования данных (при необходимости).

Соседние РО связаны между собой каналами связи. Логика функционирования такой системы может быть основана на известной логике функционирования системы безопасности мобильных агентов информационных систем, предложенной в работе [18]. Применительно к рассматриваемой модели защищенного роя логика взаимодействия роботов-агентов с полицейскими участками РО может быть следующей.

Способ 1. Пусть некоторый робот-агент R_k, находящийся в узле *i*, выбрал согласно описанному выше алгоритму путь движения в направлении узла *j*. Агент R_k, отправляет запрос *Z*1 агенту-полицейскому AP_i участка PO_i на разрешение осуществления миграции на соответствующий узел. Агент-полицейский AP_i выполняет запрос, проверяет в своем реестре узлов существование узла *j* и в случае положительного ответа формирует и выдает роботу-агенту R_k уникальный сертификат, который содержит идентификатор агента, остаток энергоресурса, информацию о точке отправления и выбранном маршруте и время выдачи сертификата. При необходимости осуществляется шифрование данных убывающего робота-агента. После этого агент-полицейский дает разрешение на миграцию R_k. Прибыв в узел *j*, робот-агент R_k предъявляет агенту-полицейскому AP_j этого узла свой сертификат. Агент-полицейский AP_j участка PO_i на основе информации, содержащейся в предъявленном сертификате, осуществляет проверку в своем реестре узлов существования в системе узла *i* и робота-агента R_k в удостоверяющем центре полицейских участков. Если информация подтверждается, то AP_j обращается к агенту-полицейскому AP_i участка PO_i, с которого мигрировал агент R_k, который и выполняет функции удостоверяющего центра роботов-агентов, с запросом на подтверждение существования агента R_k и того факта, что ему было разрешено мигрировать на узел *j*. Если агент AP_i подтверждает факт существования и миграции агента R_k на узел *j*, агент-полицейский AP_j осуществляет расчеты временных и энергетических параметров движения робота-агента из узла *i* в узел *j* с целью проверки соответствия:

- фактического времени прихода агента и остатка энергоресурса расчетному времени прибытия и остатку энергоресурса, которые могут быть вычислены исходя из времени выхода из узла убытия и расстояния до него, а также величины остатка энергии в момент убытия робота из узла *i*;
- соответствия фактического пути следования и пути, заявленного в сертификате.

При отсутствии противоречивых данных агент-полицейский AP_j заносит в свою базу данных агентов робота-агента R_k и предоставляет ему доступ к ресурсам узла, необходимым для решения стоящей перед роем задачи. Например, это может быть информация о длине путей, выходящих из узла, которая потребуется для реализации алгоритма поиска кратчайшего пути. При необходимости на участке PO_i производится дешифрование данных прибывшего агента.

Если AP_j не получил соответствующего подтверждения о существовании агента R_k в системе или обнаружено несоответствие по одному из пунктов проверки (фактические изменения остатка энергии, скорость и направление следования не соответствуют заявленным в сертификате значениям), то агент R_k блокируется, а доступ к ресурсам узла для него запрещается. Агент-полицейский AP_j в этом случае заносит агента R_k в «черный список» и информирует о присутствии «инородного» агента в системе всех ему известных полицейских участков. Аналогичные действия агент-полицейский AP_j осуществляет, если робот-агент R_k в качестве дальнейшего пути следования выбирает тот маршрут, по которому он прибыл в узел *j*, так как это служит признаком осуществления атаки.

Для предотвращения атак типа «ложный путь» [9] на агентов-полицейских возлагается функция блокирования выбора роботами-агентами тех маршрутов, на которых прибывающие на участок роботы-агенты имеют сертификат, выданный этим же полицейским участком.

Оценка производительности защищенного роевого алгоритма

Оценку производительности защищенного роевого алгоритма произведем путем сравнения времени выполнения задачи защищенным роем и незащищенным роем [18]. Для этого рассмотрим особенности работы систем на этапе выбора дуги маршрута, на этапе перемещения по дуге и на этапе прибытия в узел маршрута.

Способ 1. Этап выбора пути следования. Для незащищенной системы работное время $T_1^{\text{н}}$ робота-агента будет состоять из времени T_{RV} – времени, потребного для вычисления кратчайшего маршрута согласно муравьиному алгоритму. Для защищенной системы добавляется время переговоров с агентом-полицейским – T_{RAP}, время работы агента-полицейского с реестром узлов – T_{APU}, время формирования сертификата для робота-агента – T_{RU}, и, возможно, шифрования данных агента – T_{KR}. Тогда для защищенной системы работное время агента на первом этапе будет равно

$$T_1^{\text{з}} = T_{RV} + T_{RAP} + T_{APU} + T_{RU} + T_{KR}. \quad (1)$$

Этап движения по пути следования. На данном этапе работное время незащищенной и защищенной роевых систем совпадает и равно времени перемещения робота агента из узла *i* в узел *j*:

$$T_2^{\text{н}} = T_2^{\text{з}} = T_{ij}. \quad (2)$$

Этап прибытия на узел назначения. По прибытии в вершину графа робот-агент приступает к выбору дальнейшего пути следования. Следовательно, работное время робота-агента $T_3^{\text{н}}$ для незащищенного алгоритма в узле будет состоять из времени T_{RV}.

Для защищенной системы временные затраты будут определяться следующим соотношением:

$$T_3^{\text{з}} = T_{RV} + T_{RAP} + T_{DKR} + T_{APU} + T_{UU} + T_{CalcR} + T_{BD} + T_{AR}, \quad (3)$$

где T_{RAP} – время переговоров с агентом-полицейским; T_{DKR} – время дешифрования данных (при необходимости); T_{APU} – время обращения агента-полицейского к реестру узлов; T_{UU} – время обращения к удостоверяющему центру (полицейскому участку узла убытия робота-агента); T_{CalcR} – время, затрачиваемое на расчет параметров движения робота-агента по данным сертификата; T_{BD} – время обращения к базе данных агентов; T_{AR} – время принятия решения в отношении робота-агента по результатам аутентификации.

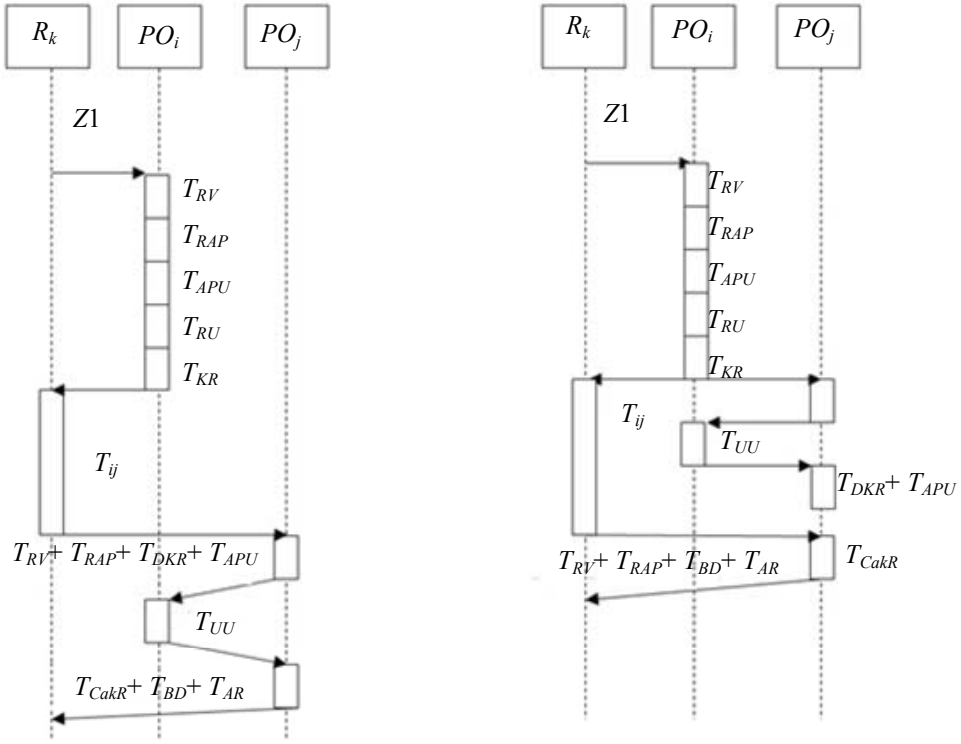
Очевидно, что общее время работы зависит как от сложности маршрута и потребного количества узлов размещения РО соответственно, так и от количества агентов в рое. Однако из формул (1)–(3) следует, что наибольшие затраты времени в защищенном роевом алгоритме падают на проведение процедур, связанных с вопросами обеспечения ИБ в узле прибытия робота-агента: T_{UU}, T_{CalcR}, T_{BD} и T_{AR}. Вместе с тем следует учесть, что время, затрачиваемое роботом-агентом на преодоление расстояния между узлами T_{ij}, всегда превышает величину $T_{UU} + T_{CalcR} + T_{BD} + T_{AR}$.

Исходя из этого, можно предложить следующую логику функционирования РО в составе защищенного роя.

Способ 2. Первый этап – выбор маршрута. Пусть некоторый робот-агент R_k, находящийся в узле *i*, выбрал путь движения в направлении узла *j*. Агент R_k отправляет запрос агенту-полицейскому AP_i участка PO_i на разрешение миграции на соответствующий узел. Агент-полицейский AP_i проверяет в своем реестре узлов и базе данных агентов существование узла *j* и уникального идентификатора робота-агента R_k соответственно. После этого агент-полицейский дает разрешение на миграцию R_k. Время, необходимое для выполнения этих процедур, равно

$T_1^з = T_{RV} + T_{RAP} + T_{APU} + T_{BD}$.

Второй этап – движение агента по маршруту. Во время физического перемещения робота-агента из узла в узел на полицейских участках узла убытия PO_i и узла PO_j прибытия робота-агента выполняются следующие процедуры.



а б

Рис. 4. Диаграмма взаимодействия основных компонентов РОМ: организация взаимодействия при способе 1 (а); организация взаимодействия при способе 2 (б)

Агент-полицейский AP_i составляет сертификат убывшего робота-агента R_k, в котором содержится информация об остатке энергоресурса, о точке отправления, выбранном маршруте и времени убытия R_k. После этого осуществляется шифрование сертификата и передача его по каналам связи на полицейский участок узла назначения робота R_k. Время, потребное для выполнения этих действий, составляет

$T_{RU} + T_{KR} + T_{UU} << T_{ij}$.

Агент-полицейский AP_j участка PO_j получает сертификат, дешифрует его и на основе информации, содержащейся в сертификате, осуществляет проверку в своем реестре узлов существования в системе узла *i*. При положительном результате агент-полицейский AP_j осуществляет расчеты временных и энергетических параметров движения робота-агента из узла *i* в узел *j* с целью прогнозирования времени прихода агента и остатка энергоресурса, которые могут быть вычислены исходя из времени выхода из узла убытия и расстояния до него. Полученные результаты расчетов, а также идентификатор и сертификат агента R_k агент-полицейский AP_j вносит в базу данных агентов участка PO_i.

Время работы PO_j по обработке данных ожидаемого агента R_k составляет

$T_{UU} + T_{DKR} + T_{APU} + T_{CalcR} << T_{ij}$.

Таким образом, на данном этапе работное время защищенной системы равно времени перемещения робота агента из узла *i* в узел *j*:

$T_2^з = T_{ij}$.

Третий этап – прибытие в вершину графа. На третьем этапе, прибыв в узел *j*, робот-агент R_k предъявляет агенту-полицейскому AP_j этого узла свой идентификатор. Агент-полицейский AP_j проверяет наличие идентификатора в базе данных агентов своего участка PO_j. Если таковой имеется, то AP_j сверяет фактическое время прибытия робота, его маршрут следования и остаток энергоресурса с данны-

ми, имеющимися в базе данных участка PO_j в отношении агента R_k. При отсутствии противоречивых сведений AP_j предоставляет агенту R_k доступ к ресурсам узла, необходимым для решения стоящей перед роем задачи. При несоответствии сведений агент-полицейский AP_j осуществляет в отношении робота R_k процедуры блокировки, описанные ранее.

Таким образом, работное время на третьем этапе составляет (рис. 4)

$$T_3^3 = T_{RV} + T_{RAP} + T_{AR} + T_{BD},$$

что на величину $T_{DKR} + T_{APU} + T_{UU} + T_{CalcR}$ меньше, чем при реализации защищенного метода обеспечения ИБ роевой системы по способу 1 (формула (3)).

Следует учесть, что при выполнении роем задач на пересеченной местности, а также в условиях воздействия дестабилизирующих факторов естественного и искусственного происхождения, существенную роль приобретают вопросы помехоустойчивости группировки.

Анализ помехоустойчивости защищенного роевого алгоритма

Рассмотрим различия в работе систем, организованных по описанным выше способам при воздействии помехи на каналы связи между РО.

Пусть путь от *i*-го к *j*-му участку состоит из *n* элементарных дистанций (рис. 5). Предположим, что при перемещении агента по этому пути в произвольный момент времени на каналы связи между полицейскими участками PO_i и PO_j воздействовала помеха. Предположим также, что за время воздействия помехи робот-агент преодолел *m* элементарных дистанций, которые на рисунке выделены желтым цветом. На рис. 5 проиллюстрированы возможные ситуации воздействия помехи на каналы связи между полицейскими участками во время преодоления агентом элементарных дистанций, которые отличаются временем начала постановки помех $t_1, t_2, ..., t_n$. Например, при варианте № 3 (рис. 5) воздействие помехи наблюдалось во время передвижения роботом-агентом по дистанциям 2 и 3. Из рисунка видно, что при использовании способа 1 неблагоприятными событиями являются варианты, когда помеха воздействует на каналы связи во время прибытия робота-агента в *n*-й участок, в котором расположен полицейский участок PO_j (варианты *n*+*m*–2 и *n*+*m*–1 рис. 5). В соответствии с диаграммой (рис. 4, а) для выполнения процедур безопасности, доступа R_k к ресурсам системы и выдачи квитанции агенту на продолжение движения PO_j должен установить связь с PO_i, что будет возможно только после прекращения воздействия помехи на каналы связи.

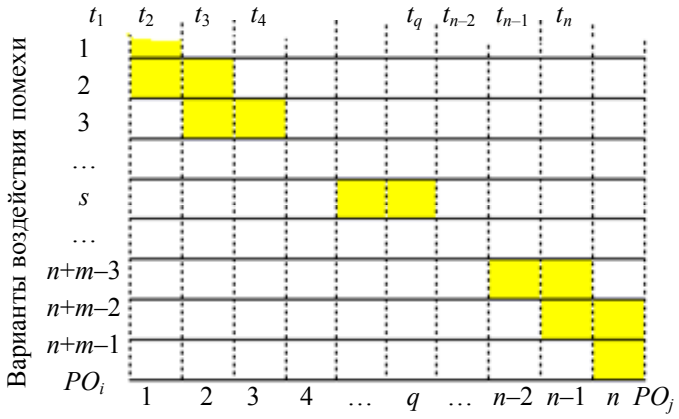


Рис. 5. Варианты воздействия помехи на каналы связи между полицейскими участками во время передвижения робота-агента между *i*-м и *j*-м РО при *m*=2

Исходя из этих рассуждений, вероятность отказа РО в обслуживании агента при организации полицейских участков по способу 1 будет равна

$$P_1 = \frac{m}{n+m-1}. \qquad (4)$$

Очевидно, что при использовании способа 2 ситуации, показанные на рис. 5, не представляют сложности для работы системы, так как PO_i начинает устанавливать связь между полицейскими участками сразу после выхода R_k к пункту назначения PO_i. Как видно из рисунка, при таком способе организации взаимодействия неблагоприятное событие (неустановление связи между полицейскими участками)

возможно только при длительности помехи, превышающей время агента в пути ($m > n$), и вероятность его наступления будет равна

$$P_2 = \frac{m-n+1}{n+m-1}. \quad (5)$$

Несложно показать преимущества взаимодействия между РО, организованного по способу 2, по сравнению с организацией по способу 1. Обозначим $k = \frac{m}{n}$. Тогда формулы (4) и (5) примут следующий вид:

$$P_1 = \frac{m}{n+m-1} = \frac{kn}{n(k+1)-1},$$

$$P_2 = \frac{m-n+1}{n+m-1} = \frac{n(k-1)+1}{n(k+1)-1}.$$

Задавшись константой n, построим графики зависимости вероятности отказа РО в зависимости от отношения k (рис. 6).

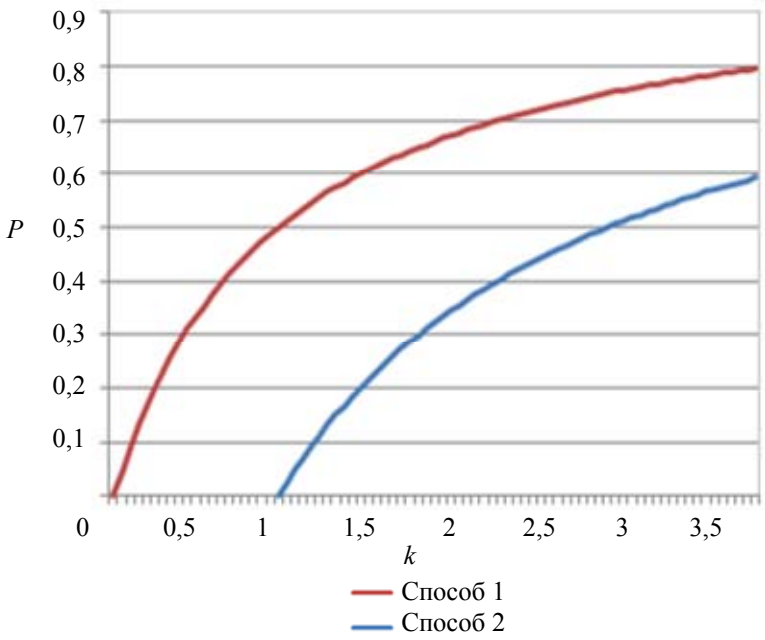


Рис. 6. Зависимость вероятности отказа РО в обслуживании агента от длительности воздействия помехи на канал связи между полицейскими участками

Из рис. 6 видно, что при реализации РОМ способом 2 помеха не влияет на работу защищенного алгоритма при выполнении условия $m < n$. При увеличении времени воздействия помехи, когда $m >> n$, кривые асимптотически сближаются и приближаются к 1, что свидетельствует о необходимости использования средств радиоэлектронной борьбы в сложной помеховой обстановке.

При моделировании на полигоне Kilobot в среде V-REP предложенная модель безопасности позволила обнаружить и нейтрализовать скрытые атаки на рой со стороны роботов-диверсантов, в том числе в условиях воздействия на каналы связи активных помех. Моделирование скрытых атак на муравьиный алгоритм при наличии системы РОМ показало, что значения вероятности P выбора роем из N агентов рационального пути при действиях диверсантов на этапе поиска кратчайшего пути при разной концентрации диверсантов стремятся к 1 (рис. 2) при различных концентрациях роботов-диверсантов.

Недостатком предлагаемого метода, как указывалось выше, является уязвимость МРТС при выводе из строя полицейских участков. Очевидно, что при практической реализации защищенных роевых алгоритмов будет необходимо использование дополнительных систем контроля их работоспособности.

Заключение

В работе проанализированы виды скрытых атак на робототехнические системы с роевым интеллектом. Рассмотрены современные подходы, ориентированные на решение задач, связанных с обеспечением информационной безопасности агентов робототехнических мультиагентных систем.

В ходе проведенных исследований были получены следующие основные результаты.

1. Выполнено численное моделирование возможных деструктивных информационных воздействий на муравьиный алгоритм поиска кратчайшего пути. Продемонстрированы атаки на муравьиный алгоритм при различной концентрации в рое роботов-диверсантов. Показана зависимость вероятности выбора кратчайшего пути от различной концентрации диверсантов в рое.
2. Обоснованы требования к мягким механизмам обеспечения информационной безопасности роевых робототехнических систем. Рассмотрены достоинства и недостатки подходов к обеспечению информационной безопасности в роевых робототехнических системах, основанных на реализации х централизованного и децентрализованного управления безопасностью мобильных агентов.
3. Разработан метод формирования самоорганизующейся системы управления информационной безопасностью роботов-агентов в роевых коллективах, реализующий модель полицейских участков, которая применяется для обеспечения информационной безопасности мультиагентных систем. Метод заключается в интеграции в коллектив роботов программно-аппаратных компонентов, выполняющих функции выявления и пресечения скрытых атак на роевые алгоритмы.
4. Проведен анализ логики функционирования системы управления информационной безопасностью роботов-агентов в роевых коллективах. Представлен сравнительный анализ реализаций защищенных роевых систем в зависимости от логики функционирования полицейских участков, интегрированных в роевую систему.
5. Проведен численный эксперимент, имитирующий работу защищенного алгоритма в помеховой обстановке.

Литература

1. Губанов Д.А. Обзор онлайновых систем репутации/доверия [Электронный ресурс]. 2009. Режим доступа: http://mtas.ru/bitrix/components/bitrix/forum.interface/show_file.php?fid=1671, свободный. Яз. рус. (дата обращения 24.03.2014).
2. Зикратов А.А., Зикратова Т.В., Лебедев И.С. Доверительная модель информационной безопасности мультиагентных робототехнических систем с децентрализованным управлением // Научно-технический вестник информационных технологий, механики и оптики. 2014. № 2 (90). С. 47–52.
3. Neeran K.M., Tripathi A.R. Security in the Ajanta MobileAgent system. Technical Report. Department of Computer Science, University of Minnesota, 1999. 28 p.
4. Xudong G., Yiling Ya., Yinyuan Y. POM-a mobile agent security model against malicious hosts // Proc. 4th International Conference on High Performance Computing in the Asia-Pacific Region. 2000. V. 2. P. 1165–1166.
5. Page J., Zaslavsky A., Indrawan M. A buddy model of security for mobile agent communities operating in pervasive scenarios // Proc. 2nd Australasian Information Security Workshop (AISW2004). ACS, Dunedin, New Zealand, 2004. V. 32. P. 17–25.
6. Page J., Zaslavsky A., Indrawan M. Countering security vulnerabilities using a shared security buddy model schema in mobile agent communities // Proc. of the First International Workshop on Safety and Security in Multi-Agent Systems (SASEMAS 2004), 2004. P. 85–101.
7. Dorigo M., Maniezzo V., Colorni A. Ant system: optimization by a colony of cooperating agents // IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics. 1996. V. 26. N 1. P. 29–41.
8. Wooldridge M. Introduction to MultiAgent Systems. John Wiley & Sons Ltd, 2002. 368 p.
9. Зикратов И.А., Козлова Е.В., Зикратова Т.В. Анализ уязвимостей робототехнических комплексов с роевым интеллектом // Научно-технический вестник информационных технологий, механики и оптики. 2013. № 5 (87). С. 149–154.
10. Комаров И.И., Дранник А.Л., Юрьева Р.А. Моделирование проблем информационной безопасности мультиагентных систем // В мире научных открытий. 2014. № 4 (52). С. 61–70.
11. Дранник А.Л. Использование программ-симуляторов поведения роевых робототехнических систем для исследования вопросов безопасности // Материалы VIII Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России (ИБРР-2013)». Санкт-Петербург, 2013. С. 240–251.
12. Schillo M., Funk P., Rovatsos M. Using trust for detecting deceitful agents in artificial societies // Applied Artificial Intelligence. 2000. V. 14. N 8. P. 825–848.
13. Golbeck J., Parsia B., Hendler J. Trust networks on the semantic web // Lecture Notes in Artificial Intelligence. 2003. V. 2782. P. 238–249.
14. Garcia-Morchon O., Kuptsov D., Gurtov A., Wehrle K. Cooperative security in distributed networks // Computer Communications. 2013. V. 36. N 12. P. 1284–1297.
15. Бешта А.А., Кирпо М.А. Построение модели доверия к объектам автоматизированной информационной системы для предотвращения деструктивных воздействий на систему // Известия Томского политехнического университета. 2013. Т. 322. № 5. С. 104–108.

16. Ramchurn S.D., Huynh D., Jennings N.R. Trust in multi-agent systems // Knowledge Engineering Review. 2004. V. 19. N 1. P. 1–25.
17. Gorodetski V., Kotenko I., Karsaev O. Multi-agent technologies for computer network security: Attack simulation, intrusion detection and intrusion detection learning // Computer systems science and engineering. 2003. N 4. P. 191–200.
18. Маслобоев А.В., Путилов В.А. Разработка и реализация механизмов управления информационной безопасностью мобильных агентов в распределенных мультиагентных информационных системах // Вестник МГТУ. 2010. Т. 13. № 4–2. С. 1015–1032.

Зикратов Игорь Алексеевич – доктор технических наук, профессор, заведующий кафедрой, Университет ИТМО, 197101, Санкт-Петербург, Россия, zikratov@cit.itmo.ru

Гуртов Андрей Валерьевич – PhD, главный научный сотрудник, Хельсинский институт Информационных Технологий University of Helsinki P.O. Box 33 (Yliopistonkatu 4) 00014, University of Helsinki Finland; адъюнкт-профессор, Аалто Университет, P.O. Box 11000, FI-00076 Aalto, Finland, mailto:gurtov@hiit.fi

Зикратова Татьяна Викторовна – преподаватель, Военный институт (военно-морской политехнический) ВУНЦ ВМФ «Военно-морская академия», 196602, г. Пушкин, Россия, ztv64@mail.ru

Козлова Екатерина Владимировна – студент, Университет ИТМО, 197101, Санкт-Петербург, Россия, kekvlad@gmail.com

Igor A. Zikratov – D.Sc., Professor, Department head, ITMO University, 197101, Saint Petersburg, Russia, zikratov@cit.itmo.ru

Andrei V. Gurtov – PhD, Principal Scientist, Helsinki Institute for Information Technology (HIIT), 00014 Helsinki, Finland; Adjunct Professor, Aalto University, FI-00076 Aalto, Finland, gurtov@hiit.fi

Tatyana V. Zikratova – tutor, Military Institute (Naval Polytechnic) Military Educational and Scientific Center of the Navy "Naval Academy", 196602, Pushkin, Saint Petersburg, Russia, ztv64@mail.ru

Ekaterina V. Kozlova – student, ITMO University, 197101, Saint Petersburg, Russia, kekvlad@gmail.com

Принято к печати 08.05.14
Accepted 08.05.14