УДК 004.056

# ПРОБЛЕМЫ МАСКИРОВАНИЯ УПРАВЛЯЮЩИХ СИГНАЛОВ АГЕНТОВ МОБИЛЬНЫХ РОБОТОТЕХНИЧЕСКИХ ГРУПП

**О.О. Шумская**
*Санкт-Петербургский институт информатики и автоматизации РАН*
Россия, 199178, Санкт-Петербург, 14-я линия В.О., 39
E-mail: shumskaya.oo@gmail.com

**А.О. Исхакова**
*Институт проблем управления им. В.А. Трапезникова РАН*
Россия, 117997, Москва, Профсоюзная ул., 65
E-mail: iao@ipu.ru

**Ключевые слова:** многоагентные робототехнические системы, робототехнические комплексы, взаимодействие роботов, управление роботами, информационная безопасность, стеганографические методы защиты информации.

**Аннотация:** В работе рассматривается актуальная научная проблема формирования защищенных механизмов межмашинного обмена данными между агентами, коммуникации между которыми осуществляются вне зоны контролируемой территории. Автором рассматриваются работы российских и зарубежных ученых в данной области, выделяются недостатки и недоработанные вопросы. Отмечается, что существующие подходы по обеспечению защиты информации в таких системах не могут быть применены для экстремальных условий такого приоритетного направления как робототехника в связи с массовой интеграцией специфических технологий, а также отсутствием адаптированных моделей угроз и моделей нарушителя. Разработка концепции безопасного управления интеллектуальными роботами и коалициями роботов, создание соответствующих алгоритмов и протоколов защищенного взаимодействия позволит решить актуальную задачу создания единого подхода к управлению робототехническими комплексами, а также повышения эффективности данного процесса.

## 1. Введение

Создание сетецентрических систем управления на базе сетевых технологий открывает новый этап в развитии как теории Интернета вещей, так и практики удаленного управления различными объектами. Сетецентрические системы управления, характеризующиеся общей открытостью и подразумевающие принятие решений внутри системы, находят широкое применение в актуальной проблеме эффективного группового управления взаимодействием между роботами. Объективный взгляд на мировые тенденции развития робототехники в мире позволяет утверждать, что одиночный робот способен решать достаточно узкий класс задач, в то время как решение сложных, комплексных проблем возможно только в результате группового применения роботов, обладающих различными функциональными возможностями. Применение сетецентрических систем предполагает возможность коммуникации не только агентов с операторами, но и между

роботами как частями системы, что позволяет лучше оценивать имеющиеся ресурсы и принимать решения в условиях неопределенности. Кроме того, коммуникация между автономными устройствами отвечает современному тренду киберфизических систем.

Разработка многоагентных робототехнических систем требует решения целого ряда научно-технических проблем, связанных с реализацией технологий «распределенного» искусственного интеллекта, коллективного взаимодействия роботов в группе и адаптации существующих методов защиты информации, циркулирующей между агентами подобных систем.

Использование инфраструктуры Интернета вещей как платформы для взаимодействия интеллектуальных робототехнических систем помимо очевидного преимущества в виде получения эффективного инструмента для управления множеством гетерогенных устройств приводит к наследованию ряда существенных уязвимостей, характерных для данной концепции. В связи с тем, что эксплуатация этих уязвимостей может поставить под угрозу безопасность жизни и здоровья человека, приоритетной задачей становится решение проблемы формирования защищенных механизмов межмашинного обмена данными. В частности, несмотря на указанные выше преимущества, децентрализованный характер построения информационных систем и потенциальная возможность коммуникации между любыми роботами делают мультиагентную среду максимально уязвимой для таких угроз, как несанкционированный перехват сообщений в процессе межагентных коммуникаций, нарушение целостности передаваемых по сети данных, отказ в обслуживании (DDoS-атаки), перехват запросов с последующей их модификацией и воспроизведением и т.д.

Важным отличительным аспектом коммуникации агентов в мобильной робототехнической группировке подобного рода является то, что взаимодействие элементов осуществляется вне зоны контролируемой территории. Данное обстоятельство повышает вероятность как несанкционированного доступа злоумышленников к каналам информационного обмена, так и непосредственного физического воздействия. Этим обусловлена необходимость адаптации существующих методов защиты передаваемых данных применительно к группам мобильных роботов.

## 2. Анализ состояния вопроса и существующих проблем

Мультиагентные робототехнические системы активно разрабатываются и широко исследуются в отечественной и мировой научной среде. Известно множество научных исследований, направленных на увеличение эффективности мобильных робототехнических группировок, способных взаимодействовать друг с другом при выполнении сложных миссий, в том числе при решении исследовательских, разведывательных, а также тактических боевых задач. Аспекты обеспечения безопасности межмашинного взаимодействия в мультиагентных робототехнических системах находят свое отражение в работах И.И. Комарова, А.П. Жука, И.А. Зикратова, L.V. Qiuyun, R.C. Luo, P.K. Wang и др. Данные авторы в разное время предпринимали попытки формулирования требований к перспективным механизмам обеспечения информационной безопасности роевых систем [1-5].

Увеличение рисков информационной безопасности обусловливает острую потребность в оценке известных и новых алгоритмов именно с точки зрения безопасности. Так, в работе [6] рассматриваются вопросы защиты мультиагентных робототехнических систем от атак со стороны роботов-диверсантов. Авторами предлагается модель информационной безопасности, в которой роботы-агенты вырабатывают уровни доверия друг к другу на основе анализа событий, происходящих в системе. Идея довери-

тельной модели состоит в анализе каждым роботом переданной информации и выполненных действий других членов коллектива и сопоставлении выбранного ими на $k$-м шаге итерации решения с целевой функцией коллектива. Однако, данная модель рассчитана на исключительно децентрализованную систему и не может быть применена в мобильных робототехнических группах с сетецентрическим управлением (при использовании центра управления безопасностью). Ещё одним недостатком децентрализованной модели информационной безопасности являются определенные затраты канальных и вычислительных ресурсов членами мультиагентной робототехнической системы.

Обеспечение безопасности беспроводных каналов передачи данных между элементами гетерогенной системы роботов исследуется в [7]. Беспроводной канал связи является одним из наиболее уязвимых элементов робототехнического комплекса. Несанкционированный доступ (просмотр, подмена, перехват и подавление помехами), направленный на нарушение работы робота, может привести к критическим последствиям. Для обеспечения безопасности авторами предлагается использование хаотически широкополосных сигналов.

Актуальным направлением решения задачи защищенной передачи управляющих сигналов является развитие стеганографических методов, однако они имеют ряд недостатков и недоработок для применения в данной предметной области и требуют значительной адаптации.

Например, в работе [8] предлагается циркулярное симметричное вложение водяного знака, а именно – формировать цифровой водяной знак (ЦВЗ) с помощью псевдослучайной ключевой последовательности в виде амплитудного Фурье-спектра, значения элементов которого принадлежат множеству {–1, 1}. Элементы Фурье-образа образуют кольцо в области средних частот. Круговая симметрия генерируемой ЦВЗ обеспечивает устойчивость перед геометрической атакой «поворот изображения». Схожий алгоритм описан в [9], однако авторы формируют цифровой водяной знак в виде окружности с оптимальным радиусом внедрения, а не кольца, и все элементы принимают значения из множества {0, 1}. Чтобы определить наличие конкретного водяного знака в изображении, авторы используют обратный встраиванию алгоритм и находят корреляцию между извлеченными значениями и значениями предполагаемого водяного знака. В случае если величина корреляции превышает предопределенный порог, авторы принимают решение, что искомый знак скрыт в данном изображении. Недостатком подхода является малая емкость передаваемой информации, ограниченной половиной круга установленного радиуса, а также неустойчивость перед атаками типа размытие и изменение яркости, которые могут возникнуть при преобразовании контейнера, в том числе округлении данных.

В работе [10] изложена схема аутентификации JPEG-изображений на основе цифровой подписи и полухрупкого ЦВЗ. Алгоритм использует инвариантность отношения порядка между двумя коэффициентами ДКП до и после сжатия JPEG для встраивания водяного знака, поэтому водяной знак может выдержать сжатие JPEG с потерями. В то же время авторы [11] предлагают использовать для аутентификации изображений схему обратимого встраивания ЦВЗ, основанную на разложении сингулярных значений, с дополнительным применением цифровой подписи. Подпись формируется на основе данных изображения, уже содержащего ЦВЗ, а затем также встраивается в подписываемое изображение.

Несмотря на наличие отдельных исследований по обеспечению безопасности робототехнических систем, в данной области имеется ряд проблем:

– отсутствуют исследования, направленные на сокрытие управляющего сигнала между группировками различных роботов в условиях невозможности устранения демаскирующих признаков роботов-разведчиков;

– не сформированы универсальные подходы к комплексному обеспечению безопасности мультиагентных робототехнических систем с сетецентрическим управлением;

– существующие модели верификации агентов не могут быть применены в мобильных робототехнических группах с сетецентрическим управлением (при использовании центра управления безопасностью);

– возможностей контроля ограничена, особенно при решении трудно формализуемых задач (в настоящее время не известен универсальный научно-методический аппарат выявления скрытых информационных атак на исследуемые системы).

## 3. Подходы к решению задач маскирования управляющих сигналов агентов мобильных робототехнических групп

В задаче сокрытия управляющих сигналов от роботов-разведчиков к роботам-исполнителям перспективно использовать технологию цифровых водяных знаков. Незаметность встраивания цифровых водяных знаков и устойчивость к искажениям, возникающим при формировании, хранении и передаче цифрового объекта, достигается путем выбора области сокрытия в цифровом объекте. Наиболее емкими и распространенными контейнерами являются видеопотоки, представляющие собой последовательность цифровых изображений. Встраивание в частотную область изображения позволяет добиться устойчивости к ряду атак за счет свойств таких преобразований как дискретное преобразование Фурье (ДПФ), дискретное косинусное преобразование (ДКП), дискретное вейлет-преобразование (ДВП) и др. вне зависимости от конкретного алгоритма встраивания.

Общим слабым местом алгоритмов, описанных в перечисленных работах, является возможность возникновения ошибок при извлечении встроенной информации. Это недопустимо, если информация перед встраиванием была сжата или преобразована с помощью криптографического алгоритма. Ошибка в одном бите хеш-кода или электронной подписи приведет к компрометации соответствующего ЦВЗ даже при отсутствии внешних деструктивных воздействий и попыток подделки. Полноценное решение данной проблемы в настоящее время отсутствует. Например, в работе [12] явно отмечается, что при извлечении информации может возникнуть ситуация, при которой часть извлеченных битов попадает в зону неопределенности, и требуется дополнительный перебор всех возможных вариантов, чтобы определить, было ли изображение модифицировано или нет. В некоторых других исследованиях данный вопрос обходится стороной, однако проблема от этого не становится менее актуальной.

Например, в работе [13] представлен метод встраивания цифровых водяных знаков (ЦВЗ), основанный на двухуровневом контурном преобразовании. Для повышения незаметности встраивания авторы при сокрытии информации отдают предпочтение более «сложным» блокам изображения, где «сложность» определяется высокой концентрацией границ, обнаруженных с помощью детектора Кэнни. При этом в статье [14] вводится схема внедрения ЦВЗ вдоль краев изображения, основанная на концепции психовизуального порога. Встраивание происходит в коэффициенты ДКП тех блоков, в которых с помощью оператора Кэнни обнаружено более десяти границ.

Авторы [15] утверждают, что для изображений, содержащих прежде всего края и гладкие области, водяной знак изображения должен быть встроен именно в краевые области. В работе предлагается адаптивный алгоритм, маскирующий искажения, вносимые на этапе сокрытия ЦВЗ, в границы на изображении, определяемые сочетанием сегментации изображения и детектора Кэнни. В работе [16] наоборот предлагается иг-

норировать края и соседние с ними области при встраивании информации. Это объясняется тем, что извлеченный из краевых зон водяной знак подвергается большим искажениям.

Данные примеры иллюстрируют, что детектирование границ на изображении успешно применяется для повышения эффективности стеганографического встраивания. Однако в существующих на данный момент работах учет границ изображения применяется исключительно для улучшения незаметности встраивания либо устойчивости к внешним воздействиям. Поэтому перспективным направлением исследования является использование информации о границах объектов на изображении для внедрения ее в защищаемое изображение наряду с ЦВЗ или вместо него. Данный подход позволит обеспечить контроль целостности изображения и выявить внесенные в него изменения, если контуры объектов будут модифицированы.

# 4. Заключение

Без решения перечисленных в работе проблем нельзя рассчитывать на повсеместное и эффективное внедрение многоагентных интеллектуальных робототехнических систем. Таким образом, разработка методов, алгоритмов маскирования управляющих сигналов и верификации агентов в мобильных робототехнических группах с сетецентрическим управлением является актуальной и перспективной научной задачей. Создание решений в части безопасного управления интеллектуальными роботами и коалициями роботов, а также создание соответствующих алгоритмов и протоколов защищенного взаимодействия позволят решить актуальную задачу создания единого подхода к управлению робототехническими комплексами, а также повышения эффективности данного процесса.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 19-01-00767.

# Список литературы

1. Celikkanat H., Sahin E. Steering self-organized robot flocks through externally guided individuals // Neural Computing and Applications. 2010. Vol. 19, No.(6. P. 849-865.
2. Dorigo M., Birattari M., Stutzle T. Ant colony optimization: Artificial ants as a computational intelligence technique // IEEE Computational Intelligence Magazine. 2006. Vol. 1, No. 4. P. 28-39.
3. Higgins F., Tomlinson A., Martin K.M. Survey on security challenges for swarm robotics // Proceedings of the 5th International Conference on Autonomic and Autonomous Systems (ICAS '09). IEEE Computer Society, 2009. P. 307-312.
4. Navarro I., Matha F. An Introduction to Swarm Robotics // ETSI Industriales, Universidad Politicnica de Madrid. 2012. www.hindawi.com/isrn/robotics/2013/608164
5. Navarro I., Matha F. Survey of Collective Movement of Mobile Robots // International Journal of Advanced Robotic Systems. 2013. Vol. 10, No. 73 cdn.intechopen.com/pdfs/42383/InTech-A_survey_of_collective_movement_of_mobile_robots.pdf
6. Зикратов И.А., Козлова Е.В., Зикратова Т.В. Анализ уязвимостей робототехнических комплексов с роевым интеллектом // Научно-технический вестник информационных технологий, механики и оптики. 2013. № 5 (87). С. 149-154.
7. Жук А.П., Осипов Д.Л., Гавришев А.А., Бурмистров В.А. Анализ методов защиты от несанкционированного доступа беспроводных каналов связи робототехнических систем // Наукоемкие технологии в космических исследованиях земли. 2016. Т. 8, № 2. С. 38-42.
8. Solachidis V., Pitas I. Circularly Symmetric Watermark Embedding in 2-D DFT Domain // IEEE Transactions on Image Processing. 2001. Vol. 10. P. 1741-1753.
9. Poljicak A., Mandic L., Agic D. Discrete Fourier Transform-based Watermarking Method with an Optimal Implementation Radius // Journal of Electronic Imaging. 2011. Vol. 20. P. 033008-1–033008-8.

10. Zhang H.-B., Yang C., Quan X.-M. Image authentication based on digital signature and semi-fragile watermarking // Journal of Computer Science and Technology. 2004. Vol. 19, No. 6. P. 752-759.
11. Singh S.K., Poria N., Palanisamy P. Reversible watermarking with embedded digital signature // Proceedings of 2014 International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC). 2014. Chennai, India. P. 478-481.
12. Zhu X.-w., Xiao L. Research of Multiple Watermarks Algorithm in E-commerce Copyright Protection and Tracking // Proceedings of 2008 International Conference on Computational Intelligence and Security. 2008. P. 300-304.
13. Fazlali H.R., Samavi S., Karimi N., Shirani S. Adaptive blind image watermarking using edge pixel concentration // Multimedia Tools and Applications. 2017. Vol. 76, No. 2. P. 3105-3120.
14. Abu N.A., Ernawan F., Suryana N., Sahib S. Image Watermarking Using Psychovisual Threshold over the Edge // Proceedings of ICT-EurAsia: Information and Communication Technology - EurAsia Conference. 2013. P. 519-527.
15. Guo J., Zhang Y., Zhi S., Cosman P. Adaptive edge masking based on TV decomposition and adjacent similarity for digital watermarking // Proceedings of 2015 IEEE International Conference on Progress in Informatics and Computing (PIC). 2015. P. 142-147.
16. Morshed A.B.M.M., Amornraksa T. Pixel-wise based image watermarking by ignoring edges and its neighbor pixels // Proceedings of the 10th International Symposium on Communications and Information Technologies. 2010. P. 475-480.