V. Экологическая и техногенная безопасность

Мещеряков Р.В.

Подход к защищенному интеллектуальному управлению роботами и их коалициями с использованием интерфейса человек-робот(ы) и робот-робот(ы)

Аннотация: Рассмотрен подход к защите обеспечения каналов управления и формирования коалиции роботов при использовании различных интерфейсов. Предлагается обеспечивать типовые решения за счет введения функций интеллектуализации при принятии решения. Предлагается использование различных интерфейсов для резервирования каналов связи при подаче команд и получения обратной связи от объектов управления.

Ключевые слова: кибербезопасность, защита информации, интерфейсы, коалиция, интернет вещей

Введение

Развитие интеллектуальных робототехнических систем в современном мире оказывает значительное влияние на другие отрасли науки и промышленности. В настоящее время количество роботов, задействованных не только в промышленности, но и в быту, стремительно увеличивается. Современные робототехнические системы зачастую представляют собой распределенные децентрализованные системы, для обеспечения работоспособности которых необходима связь между их отдельными элементами, в том числе беспроводная. Связь между элементами робототехнических систем может быть реализована через межмашинное взаимодействие, в том числе в рамках концепции интернета вещей (Internet of Things, IoT). В настоящее время происходит глубокая интеграция интеллектуальных робототехнических систем и IoT-инфраструктуры. Однако это приводит к появлению проблемы, не имеющей на данный момент полноценного решения. Массовое использование интернета вещей,

как в робототехнике, так и в иных отраслях, затруднено теми проблемами безопасности, которыми обладает данная концепция.

Вмешательство злоумышленников в управление роботами и группами роботов может не только воспрепятствовать выполнению тех задач, для решения которых используются роботы, и в связи с этим привести к финансовым потерям, но и создать угрозы для жизни и здоровья людей. Поэтому крайне актуальной становится проблема формирования защищенных механизмов межмашинного обмена данными при управлении робототехническими системами.

Ситуация осложняется тем, что на сегодняшний день не существует стандартов безопасности для робототехнических систем и типовых систем управления с использованием человеко-машинных интерфейсов. Наследование робототехническими системами уязвимостей, характерных для IoT-инфраструктуры, не позволяет применять традиционные меры обеспечения безопасности, в частности, из-за ограниченной вычислительной мощности и других характерных особенностей исследуемых устройств. В отличие от компьютеров и смартфонов, значительная часть IoT-устройств не способна применять средства защиты от вредоносного программного обеспечения из-за отсутствия инфраструктуры для запуска подобных приложений. С другой стороны, разработка интерфейсов при участии человека требует решения проблем удаленного взаимодействия с реальными и виртуальным робототехническими системами, в частности, ограничения информации по каналу связи устройство-человек. При использовании существующих каналов связи отсутствуют тактильные и ряд звуковых данных, а видео-информация представляется в урезанном виде по сравнению с непосредственным наблюдением как за управляемой системой, так и за другими пользователями, осуществляющими либо управление этой же системой (разделение операторских функций) либо же другими системами в общем пространстве.

Отдельную сложность проблемам безопасности робототехнических систем независимо от используемых технологий связи и методов управления придает увеличение числа одновременно взаимодействующих единиц, обусловленное постоянным технологическим ростом робототехнической отрасли. Это приводит к появлению принципиально новых угроз

безопасности. Для того, чтобы вмешаться в работу коалиции роботов, злоумышленнику достаточно получить возможность управлять отдельными представителями коалиции и за счет этого организовать деструктивное воздействие на систему в целом.

Состояние исследований

Робототехника применяется в различных сферах человеческой деятельности и их количество год от года стремительно увеличивается. Происходит стремительная интеграция роботов в инфраструктуру интернета вещей. Например, в работе [1] предлагается структура, обеспечивающую беспрепятственную связь между интеллектуальными домашними устройствами и роботами.

Большое количество исследований направлено на разработку алгоритмов управления роботами [2-6]. Многие задачи способны эффективно решаться только при групповом взаимодействии роботов. Модели группового поведения, в частности, коалиций роботов, рассмотрены в [7]. Согласно [7], коалиции образуют агенты (роботы), которые могут объединять свои ресурсы для решения сложных задач. В [8] рассмотрена модель координации роботов на основе клеточных автоматов. В [9] с помощью клеточных автоматов моделируется коллективное взаимодействие агентов для совместного преодоления препятствий.

В работе [10] подробно рассмотрены аспекты группового взаимодействия гетерогенной группы роботов, т.е. роботов с различным устройством, алгоритмами управления и задачами, а также наличием централизованного автоматического управления каждой гомогенной подгруппой. Авторы отмечают, что групповое управление должно осуществляться с минимальным участием человека, поэтому необходимо применение механизмов интеллектуального управления.

Вопросы интеллектуального управления рассмотрены в [11]. В данной работе предлагается подход к взаимодействию пользователей и роботов с помощью онтологий для совместного решения задач. Онтологии публикуются в интеллектуальном пространстве, позволяющем пользователям и роботам осуществлять непрямое взаимодействие. Пользователи и роботы формируют и публикуют задачи, роботы определяют задачу, объединяются в

коалицию для ее выполнения и распределяют подзадачи в рамках этой коалиции.

Авторы [12] сфокусированы на работе нескольких агентов с точки зрения интерактивного интеллектуального пространства. В основе архитектуры управления лежит обеспечение локализации и надежного отслеживания.

Обзор большого числа архитектур интеллектуального управления приводится в статье [13]. Среди них иерархическая, поведенческая и другие архитектуры. В работе [14] представлен частный случай архитектуры интеллектуального управления, основанной на взаимодействии человека с роботом для помощи в детской реабилитации.

Постановка задачи и обсуждение

Для выявления наиболее проблемных участков в информационном взаимодействии элементов робототехнических систем, подверженных отказам, была построена классификация возможных отказов и нарушений в воздействии на данные и команды управления, передаваемые в интеллектуальных робототехнических системах, функционирующих с использованием технологии интернета вещей. В частности, было установлено, что уникальные особенности построения группы роботов затрудняют использование существующих механизмов обеспечения информационной безопасности и предоставляют возможность злоумышленникам для воздействия на роевые алгоритмы (адаптивное поведение) [15].

В качестве основных механизмов реализации атак были выделены физические атаки на группы робототехнических устройств; атаки на каналы связи; затруднение идентификации и аутентификации агентов-роботов в системе; внедрение сторонних устройств в коалицию (в том числе перепрограммированные злоумышленником легитимных роботов) [15].

Было установлено, что интерфейсы взаимодействия роботов с человеком требуют решения проблем удаленного взаимодействия с реальными и виртуальным робототехническими системами, в частности, ограничения информации по каналу связи устройство-человек. При использовании существующих каналов связи отсутствуют тактильные и ряд звуковых данных, а видео

информация представляется в урезанном виде по сравнению с непосредственным наблюдением как за управляемой системой, так и за другими пользователями, осуществляющими либо управление этой же системой (разделение операторских функций), либо же другими системами в общем пространстве [16].

Одним из решений защищенного управления отдельными интеллектуальными роботами и их коалициями представляет собой применение алгоритмов шифрования каналов связи; многофакторной аутентификации; средств управления доступом, мониторинга, защиты от установки вредоносного программного обеспечения (в том числе на этапах инициализации новых версий ПО), локального и централизованного поиска уязвимостей, исправления и управления конфигурациями агентов.

Заключение

Проведенные исследования показали, что требуется разработка модели безопасности интеллектуальных робототехнических систем, функционирующих с использованием интерфейса интернета вещей. Базовые механизмы обеспечения защищенности должны учитывать особенности использования интерфейса интернета вещей при выполнении основных сценариев выполнения индустриальных задач робототехнических комплексов прикладного назначения. Алгоритм для модели управления измерительными компонентами, позволяет получить в необходимые моменты времени совокупность оценок измеряемых физических величин, показателей их точности, а также устранить систематические погрешности. Полученные оценки величин могут быть использованы в качестве априорной информации в принятии управленческих решений. Используемые модели управления для мониторинга, построенные на концепции интернета вещей, обладают преимуществами: взаимодействие измерительных компонент без вмешательства человека и возможность быстрого реагирования при изменениях каких-либо параметров окружающей среды, в частности для задач [17]. Оригинальность разработанной модели заключается в учете таких факторов, как помехоусточивость измерительных каналов, отказоустойчивость системы в целом, воспроизводимость эталонного сигнала, а также единый формат передачи

измерительной информации, который воспринимают все компоненты системы в целом.

Исследование выполнено при частичной финансовой поддержке гранта РФФИ № 19-08-00331

Литература:

1. *S.M. Nguyen, C. Lohr, P. Tanguy, Y. Chen.* Plug and Play your Robot into your Smart Home: Illustration of a New Framework // KI – Künstliche Intelligenz. – 2017. – Vol. 31. № 3. – P. 283-289.

2. *Павловский В.Е.* Эвристический алгоритм обнаружения изолированных препятствий мобильным роботом по дальномерным данным // Искусственный интеллект и принятие решений. – 2016. – №4. – С. 93-105.

3. *Филимонов А.Б., Филимонов Н.Б.* Некоторые аспекты автоматизации систем управления беспилотными мобильными средствами // Мехатроника, автоматика и робототехника. – 2018. – № 2. – С. 35-38.

4. *Атакищев О.И., Титенко Е.А., Скорняков К.С., Заичко В.А., Риос А.П.* Модель и методы управления сложными техническими объектами на основе продукционной парадигмы // Известия ЮФУ. Технические науки. – 2012. – №3(128). – С. 181-187.

5. *Визильтер Ю.В., Вишняков Б.В., Выголов О.В., Горбацевич В.С., Князь В.А.* Технологии интеллектуальной обработки информации для задач навигации и управления беспилотными летательными аппаратами // Труды СПИИРАН. – 2016. – №2(45). – С. 26-44.

6. *Лохин В.М., Манько С.В., Романов М.П.* Развитие технологий применения аппарата теории автоматов для управления многоагентными робототехническими системами // Робототехника и техническая кибернетика. – 2016. – №2(11). – С. 3-7.

7. *Карпов В.Э.* Модели социального поведения в групповой робототехнике // Управление большими системами: сборник трудов. – 2016. – № 59. – С. 165-232.

8. *C.R. Tinoco, D.A. Lima, G.M.B. Oliveira.* An improved model for swarm robotics in surveillance based on cellular automata and repulsive pheromone with discrete diffusion // International Journal of Parallel, Emergent and Distributed Systems. – 2017 (2019). – Volume 34. Issue 1. – P. 53-77. doi: 10.1080/17445760.2017.1334886

9. *Kuznetsov A.V.* A Model of the joint motion of agents with a three-level hierarchy based on a cellular automaton // Computational Mathematics and Mathematical Physics. – 2017. – Vol. 57. № 2. – P. 340-349.

10. *Васильев И.А., Половко С.А., Смирнова Е.Ю.* Организация группового управления мобильными роботами для задач специальной робототехники // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. – 2013. – № 1 (164). – С. 119-123.

11.*Петров М.П., Кашевник А.М.* Онтолого-ориентированный подход к непрямому взаимодействию пользователей и роботов для совместного решения задач // Научный вестник НГТУ. – 2017. – Т. 66. №1. – С. 133-146.

12.*D. Kim, K.H. Jeong, B.H. Lee.* An approach to multi-agent interactive control in an intelligent space // International Journal of Control, Automation and Systems. – 2015. – Vol. 13. № 3. – P. 697-708.

13.*Tzafestas S.G.* Mobile robot control and navigation: a global overview // Journal of Intelligent & Robotic Systems. – 2018. – Vol. 91. – P. 35-58. doi: 10.1007/s10846-018-0805-9

14.*S.F. dos Reis Alves, H. Ferasoli.* Intelligent control architecture for assistive mobile robots // Journal of Control, Automation and Electrical Systems. – 2016. – Vol. 27. № 5. – P. 515-526.

15.*Туровский Я.А., Харченко С.С., Мещеряков Р.В., Исхаков А.Ю., Исхакова А.О.* Алгоритмическое обеспечение интерфейса управления робот-человек при выделении зрительных вызванных потенциалов на основе многомерного индекса синхронизации // Известия ЮФУ. Технические науки. – 2020. – № 1 (211). – С. 66-78.

16.*Мещеряков Р.В., Исхаков А.Ю., Евсютин О.О.* Современные методы обеспечения целостности данных в протоколах управления киберфизических систем // Информатика и автоматизация. – 2020. – Т. 19. № 5. – С. 1089-1122.

17.*Ананьев П.П., Плотникова А.В., Тимофеев А.С., Мещеряков Р.В., Беляков К.О.* Проблемы тестирования робототехнических систем для перемещения по космическим объектам // Робототехника и техническая кибернетика. – 2021. – Т.3. № 9. – 180-185.