ДОВЕРИТЕЛЬНАЯ МОДЕЛЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СРЕДЫ МНОГОАГЕНТНЫХ РОБОТОТЕХНИЧЕСКИХ СИСТЕМ

Степенкин А.А.[1]

Аннотация

Возможности робототехнических систем стремительно возрастают. Способы эксплуатации таких систем с каждым днем возрастают. Сенсорные сети, Интернет вещей, киберфизические системы обладают аналогичными свойствами, как и многоагентные робототехнические, что позволяет рассматривать использующиеся в них подходы и методы обеспечения безопасности.

***Цель работы**: повышение безопасности эксплуатации многоагентных систем в условиях неконтролируемой среды, разработка методов оценки доверия к среде.*

***Методы исследования:** анализ существующих моделей угроз для многоагентных роботизированных систем, а также систем, обладающих аналогичными свойствами: киберфизические системы и интернет вещей. Анализ результатов исследования существующих подходов обеспечения безопасности многоагентных систем.*

***Результаты исследования:** проведен анализ угроз безопасности и существующих способов обеспечения безопасности для роботизированных многоагентных систем, а также систем, обладающих аналогичными свойствами. Разработано расширение для методов безопасности на основе доверия и репутации, учитывающее среду эксплуатации системы как часть информационного взаимодействия. Предложен способ локализации субъекта внешнего нарушителя в среде. Предложено использование результатов оценки доверия среды внутри системы группового управления агентами для повышения эффективности и защищенности системы. Проведено моделирование эффективности использования энергии при достижении целей агентами с использованием показателя доверия к среде и без него.*

***Ключевые слова:** многоагентные системы, системы группового управления, системы доверия и репутации, обнаружение вторжения.*

DOI:10.21681/2311-3456-2020-06-23-31

Введение

Возможности робототехнических систем возрастают с каждым днем. Удешевление производства устройств и повышение их вычислительных мощностей привело к созданию многоагентных систем. Многоагентные системы (МАС) позволяют комбинировать возможности более простых устройств для решения более комплексных задач. Агенты могут быть представлены не только как информационные, но и как физические субъекты. Робототехнические МАС могут применяться для перевозки грузов и людей, проведения разведки труднодоступных и опасных для человека мест, для контролирования территории. Агенты могут быть реализованы как наземные, воздушные, наводные или подводные беспилотные аппараты.

Основное назначение применения МАС – эффективное решение задач при помощи кооперации агентов. Эффективность является важным критерием таких систем, т. к. агенты являются автономными, время их работы ограничивается доступными энергетическими ресурсами. Следовательно, можно рассматривать эффективность как отношение решенных задач к количеству затраченной агентами энергии.

Для повышения эффективности МАС применяются системы группового управления роботами (СГУР). Задачи СГУР – получение списка задач, распределение задач между агентами, контроль перемещения агентов, разрешение коллизий между агентами [1, 2].

Угрозы информационной безопасности МАС

Каждый агент является самостоятельным робототехническим устройством и наименьшей частью МАС. Следовательно многие воздействия на МАС начинаются с воздействий на отдельных агентов. [3, 4]

Отличительными чертами МАС от прочих информационных систем [5] является большая изменчивость системы: агенты могут входить и выходить из состава системы, кооперироваться в разные группы при решении разных задач; сложность взаимодействия: большое

1 Степенкин Андрей Анатольевич, аспирант, Южный Федеральный Университет, Инженерно-технологическая академия, Институт компьютерных технологий и информационной безопасности, Кафедра Безопасности информационных технологий, Таганрог, Россия. Email: stepen927@gmail.com

количество протоколов, внедрение новых протоколов или отсутствие единого для всех агентов протокола [6, 7]. Как и любая информационная система, информационная безопасность МАС обеспечивается свойствами: конфиденциальности, целостности и доступности. Нарушение конфиденциальности в условиях применения МАС может привести к обнаружению действующих агентов и их свойств, несанкционированному доступу к агенту, раскрытию информации. Нарушение целостности может привести к повреждению или изменению информации, используемой МАС, введению дезинформации. Нарушение целостности может привести к изменению процессов, происходящих внутри МАС. Нарушение доступности может быть представлено отказом в обслуживании [8, 9].

Изменчивость МАС приводит к возникновению угроз, специфичных для данного класса систем – внедрение поддельных или вредоносных агентов. Таким образом МАС обладает еще одним свойством безопасности – подлинность. Внедрение поддельных агентов может приводить к нарушению любой из характеристик информационной безопасности. Поддельный агент может обладать дополнительными каналами связи, посредством которых будет нарушена конфиденциальность. Некорректное выполнение задач приведет к нарушению целостности. Робототехнические агенты могут быть похищены, подвергнуты несанкционированной модификации и повторному внедрению. Внедренный поддельный агент может нарушать процессы кооперации других агентов и распределения задач между ними, срывать выполнение задач. Внедренный агент может навязывать остальным агентам собственные задачи. [10-12]

Методы обеспечения безопасности

Для поддержания конфиденциальности, целостности и доступности могут применяться традиционные для прочих информационных систем методы: контроль целостности на нижних уровнях модели OSI, применение шифрования и распределения ключей, методы на основе сигнатур для определения сетевых атак.

Для противодействия угрозам информационной безопасности, связанными с внедрение поддельных агентов применяются механизмы мягкой информационной безопасности. Данные механизмы направлены на определение и предотвращения воздействий, которые не нарушают строгие правила протоколов взаимодействия агентов, но являются деструктивными для системы или снижают ее эффективность [13].

Механизмы обеспечения мягкой информационной безопасности могут быть реализованы посредством добавления роли валидатора поведения, например police office model, системы доверия и репутации между агентами. Валидаторы – это роль, исполняемая некоторыми агентами. Валидаторы получают лог действий агентов, могут выполнять моделирование поведения агентов, анализировать передаваемую агентом информацию. В результате валидатор может оценить действия агента и обнаружить отклонения в поведении у ложных агентов [14, 15].

Модель доверия и репутации вводит оценку, позволяющую характеризовать качество кооперации между агентами. Каждый агент вычисляет доверие ко всем остальным агентам на основе доказательств, полученных в результате непосредственного взаимодействия с этими агентами [16, 17]. Репутация – это коллективная оценка доверия к агенту, рассчитываемая с помощью механизма распределения доверия между агентами. Применение репутации позволяет сократить взаимодействие ложного агента с системой. [18 - 20]

Робототехнические МАС как киберфизические системы

В работах на тему роботизированных, автоматизированных систем существует термин киберфизических систем. Киберфизические системы – это системы, объединяющие в себе физические и информационные системы, а также системы, существующими на их пересечении. Киберфизические системы применяются для управления и автоматизации физических процессов: энергетика, мониторинг здоровья, доставка грузов [21, 22]. Робототехнические МАС соответствуют определению киберфизических систем. Агенты являются информационными субъектами, осуществляющие информационное взаимодействие для автономного выполнения задач. Агенты являются физическими субъектами, т. к. робототехнические могут реализовываться как наземные, воздушные, надводные, подводные или прочие автономные устройства. Робототехнические субъекты обладают набором сенсорных и исполнительных устройств, посредством которых осуществляется взаимодействие физической и информационной среды.

Информационные потоки

Рассмотрим информационные потоки МАС. Агент при присоединении к системе обменивается с остальными агентами идентификаторами, ключевой информацией, списком используемых протоколов и прочими характеристиками. Агент становится частью системы группового управления. Система группового управления способна получать задачи от операторов, авторизованных пользователей или других информационных субъектов. При работе системы группового управления агенты обмениваются обновлениями своего состояния, рассылается информация о задачах. В процессе распределения задач используется информация о текущем состоянии агентов, информация о задачах, а также информация о среде. Информация о среде может быть предопределенна при размещении агента, а также быть получена посредством сенсорной системы агентов.

Сенсорная система агентов имеет ограниченную дальность и сектор наблюдений. Следовательно, можно предположить, что наблюдаемая область среды много меньше области среды, где осуществляется деятельность МАС. Реальные сенсоры робототехнических средств подвержены зашумлению, имеют ограниченную разрешающую способность, следовательно наблюдаемые характеристики среды отличаются от реальных. Сенсорная система подвержена повреждению и за-

грязнению, что также снижает точность ее работы. В реальной физической среде происходят процессы, не являющиеся частью многоагентной системы, следовательно среда обладает свойством недетерминированности.

$$E'_{part}(t) = \left\{ F\left(E(t), a\right),\ a \in A \right\} \quad (1)$$

$$E'(t) = E'(t-1) \setminus E'_{part}(t) \bigcup E'_{part}(t) \quad (2)$$

где: E(t) – реальная среда в момент времени t, E'(t) – информация о среде в момент времени t, a – агент A – многоагентная система, F(e, a) – функция наблюдения среды сенсорной системой агента a

Следовательно, система группового управления обладает неточными, неполными и устаревшими характеристиками среды.

Неконтролируемая среда

Робототехнические МАС могут решать широкий спектр задач. Вследствие этого закономерно предположить, что среди этих задач могут существовать такие, которые потребует развертывание многоагентной системы в неконтролируемой среде. Неконтролируемая среда – это среда, в которой происходят процессы, которые не управляются многоагентной системой, или ее операторами. Ограничение доступа неавторизованных лиц к неконтролируемой среде затруднено или невозможно. Таким образом процессы, происходящие в неконтролируемой среде, могут приводить к ее изменению. Т. к. система группового управления для своей деятельности использует информацию о среде, то внешние процессы оказывают косвенное воздействие на результаты работы. В работах [23, 24] рассматриваются алгоритмы управления, адаптирующиеся к изменяемой среде.

Изменения в среде, возникшие в результате процессов в ней, с точки зрения применяемой МАС можно классифицировать по следующим признакам: естественные и преднамеренные, направленные и ненаправленные. Возникновение естественных изменений не связано с конкретными субъектами, преднамеренные – наоборот являются результатом деятельности некоторого субъекта. Направленные изменения – это такие изменения, которые вовлекают агентов МАС, ненаправленные – не оказывают существенного влияния на агентов.

Любое изменение в среде можно рассматривать как воздействие на систему. Как было отмечено выше – основной критерий работы многоагентной системы – эффективность применения ресурсов. Следовательно, величину любого воздействия можно оценивать на основе изменения эффективности системы. Определение классов естественных и преднамеренных воздействий является сложной задачей, требующей большого количества информации о среде и возможности выявление признаков с высоким уровнем абстракции. Классификация по направленности, наоборот, может быть определена на основе влияния на эффективность системы.

Как следует из определения, неконтролируемая среда может содержать нарушителей. Нарушитель может быть характеризован по следующим параметрам: цель и потенциал. Целью нарушителя может быть раскрытие конфиденциальности, отказ в обслуживание, навязывание своих задач. Потенциал нарушителя определяет доступные средства, количество и интенсивность воздействий, совершаемых для реализации своих целей. Любой нарушитель обладает конечным потенциалом. Можно предположить, что для нарушителя с высоким потенциалом в качестве наиболее эффективного воздействия будет массовая физическая атака на агентов. Нарушители со средним потенциалом могут быть ограничены методами физического перехвата агента, последующей модификации и внедрения; внедрения ложных сообщений; нарушение каналов связи; изменение среды с целью создания помех перемещения агентов.

Детектирование воздействий

Сенсорная система робототехнического агента включает большое количество сенсоров, таких как лазерные и ультразвуковые дальномеры, лидары, камеры с системами оптического распознавания, микрофоны, приемники GPS, расхода энергии, оставшейся энергии, инерционные датчики: акселерометры, гироскопы, магнетометры, пройденного пути, барометры; и др. Для датчиков могут быть определены профили допустимых показаний для различных режимов работы. Возникновение отклонений может определяться как наличие внешнего воздействия. Важной характеристикой среды является карта местности, которая обозначает положения и форму известных препятствий. Данная карта используется при построении маршрутов к цели. На основе известного маршрута и параметров агента может быть рассчитано теоретическое значение необходимой энергии для выполнения задачи. Значительное отклонение реального расхода от расчетного значения может определяться как наличие внешнего воздействия. В ходе выполнения задач агенты должны выполнять обновление информации о среде, для минимизации неточностей и актуализации устаревших сведений. Каждое обновление информации о среде должно быть распространено среди всех агентов. Для определения значимости таких изменений может применяться два метода: простая разность, показывающая изменившиеся значения; влияние новых изменений на используемые агентами маршруты и эффективность. Агенты в ходе решения задач поддерживают связь. В качестве каналов связи обычно выступает радиоканал и оптический канал. Каждый агент может отслеживать соотношение сигнала и шума в канале. Возникновение высокого параметра шума может определяться как внешнее воздействие. Для эффективного функционирования МАС важным является оперативная доставка сообщений. Для обеспечения связи могут применяться различные методы, например централизованная и децентрализованная сеть. При использовании централизованной связи существует одна или несколько точек доступа, обеспечивающих связь. Низкий уровень сигнала с точкой доступа или полная его потеря может свидетельствовать о внешнем воздействии. Децентрализованная

связь позволяет агентам передавать сообщения непосредственно друг другу. В случае высокой рассредоточенности агентов мощности передатчиков для прямого взаимодействия может не хватать. Для таких случаев применяются протоколы маршрутизации, позволяющие доставить сообщение агенту через цепочку других агентов. Свидетельствовать о наличии внешнего воздействия может несоответствие между уровнем сигнала и известным положением агента, снижению количества доступных агентов, увеличения длины маршрута для доставки сообщения, потеря связи со всеми агентами. Каждое наблюдаемое отклонение *d* определяется вектором параметров воздействий и добавляется в историю наблюдений за средой V системы группового управления как *v*, которое определяется, где *a* – агент, наблюдавший отклонение, *t* – временная метка наблюдения, *l* – геолокационная метка наблюдения. Если наблюдаемое отклонение приводит к нарушению выполнения существующей задачи, то такое наблюдение должно быть помечено как инцидент воздействия на систему. Например, система содержит агентов A1, A2, A3, между которыми распределены задачи. Для решения задач на основе имеющихся сведений о среде определены траектории p1, p2, p3. В случае, если все агенты являются подлинными, а в среде нет нарушителей, чья деятельность направлена против системы, то задачи будут выполнены согласно плану. Предположим, что в группе существует ложный агент, например A2, то для нарушения работы системы возможны следующие сценарии: отказ от движения; движение по траектории, создание ложного наблюдения препятствия на своей траектории и выбор другой траектории; создание ложного наблюдения о препятствии на траектории другого агента, что принудит его выбрать новый энерго-неэффективный маршрут; создание ложного наблюдения о отсутствие препятствия на маршруте другого агента, для принуждения его выбора некорректного пути. При размещении в области ложного наблюдения подлинного агента, будет создано новое наблюдение, противоречащее дезинформации. Предположим, что все агенты подлинные, в среде существует нарушитель, способный манипулировать средой. Тогда после распределения целей и начала движения, нарушителем может быть создано препятствие на одной из выбранных траекторий. Таким образом нарушитель навяжет агенту выбор альтернативного энерго-неэффективного маршрута. При размещении в области наблюдения другого агента, будет создано новое наблюдение, подтверждающее наличие препятствия.

Доверие к среде

О каждом обнаруженном воздействие должно сообщаться остальным агентом. Сообщение должно включать вид и параметры обнаруженного воздействия, время и место обнаружения, идентификатор агента, обнаружившего воздействие. Повторные обнаружения воздействий могут позволить определить положение источника. На основе количества агентов, обнаруживших воздействие, может быть определен источник воздействий: субъект среды, воздействующий на многих агентов, либо несанкционированно модифицированный агент. Так как модификация не может быть проведена без физического взаимодействия, то на основе истории сообщений агента может быть определено время и место атаки. Воздействия, обнаруживаемые разными агентами, могут позволить отслеживать положение и активность источника воздействий.

Из вышесказанного следует, что по причине того, что среда активно влияет на процессы системы, среда является субъектом информационного взаимодействия. Следовательно, как и прочие субъекты информационного взаимодействия, среда может обладать характеристикой доверия. Для назначения доверия следует выбрать точку и область ее влияния в среде. Выбор точки и области влияния может осуществляться на основе кластеризации обнаруженных воздействий.

Так, из наблюдений *V*, можно выделить те наблюдения, которые были помечены как воздействия на систему. Для них можно составить матрицу подобности воздействий. Определять подобность воздействия можно функцией *S*:

$$S\left(v_1, v_2\right) = \frac{t_1 - t_2}{l_1 - l_2}\left(d_1, d_2\right) \quad (3)$$

Информация о доверии к среде должна учитываться системой группового управления при принятии решений. Можно определить два сценария использования доверия: сокращение использования областей с низким доверием; мониторинг областей с низким доверием. Для решения задачи может существовать множество путей решения. Различные пути могут использовать различные маршруты перемещений, следовательно включать или не включать области, имеющие низкое доверие. Следовательно каждый путь помимо энергетической стоимости может иметь метрику риска, связанного с использованием данного пути, а система группового управления, выполняющая распределения задач, должна быть соответствующим образом модифицирована для управления рисками и реализации сценариев обработки областей с низким доверием. Так, для реализации сценария мониторинга областей с низким доверием, система группового управления при выборе узла для назначения задачи может отдать приоритет узлу, предлагающему выполнение с большой энергетической стоимостью, поскольку данное решение позволит выполнить дополнительное наблюдение за средой и осуществить ротацию агентов. Система группового управления может генерировать задачи наблюдения за средой. Для реализации сценария сокращения взаимодействия с областями низкого доверия система группового управления должна обеспечивать управление рисками: при оценке решений добавлять штрафы, пропорциональные рискам; выполнять резервирование агентов для гарантирования решения задач с высоким приоритетом, при котором реализуется несколько путей решений с различной стоимостью и рисками.

Эксперименты

Окружающая среда, в которой существуют и осуществляют деятельность агенты, описывается в виде графа. Каждый узел представляет некоторую точку ин-

тереса. Каждый агент может располагаться на любом узле. На любом узле может располагаться произвольное количество агентов. Узлы, между которыми возможны переходы, соединены ребрами. Воспользоваться ребром для осуществления перехода может произвольное количество агентов. Каждое ребро обладает следующими характеристиками: длина ребра, вес ребра, направленность, график активности внешних факторов. Длина ребра характеризует расстояние между соединяемыми узлами. Вес ребра характеризует сложность перемещения по данному ребру. Направленность характеризует возможность двухстороннего перемещения. График активности внешних факторов характеризует изменение состояния ребра во времени. Активность внешних факторов может рассматриваться как штраф к весу, для упрощения модели для активности определены два крайних значения: отсутствие активности и полная блокировка ребра. Каждый агент имеет набор целей, которые необходимо посетить. Очередность целей зафиксирована. Каждый агент выбирает маршрут для достижения цели самостоятельно. Каждое движение агента увеличивает его счетчик затраченной энергии. При попытке осуществления перехода через заблокированное ребро, агент тратит такое же количество энергии, которое было бы затрачено для осуществления энергии, но перемещение не осуществляется, и агент оповещается о неудачном перемещении. Симуляция выполняется пошагово. На каждом шаге каждый агент попытку одного перемещения. Также, на каждом шаге все ребра изменяют свое состоянии в соответствии со своим графиком активности внешних факторов.

Для эксперимента поместим двух агентов S и *T* в один начальный узел. Оба агента получат одинаковый набор целей. Каждый агент выполняет цели в том порядке, как они указаны в наборе целей. При достижении целевого узла агент извлекает следующую цель. Если достигнута последняя цель из списка, агент останавливает свою деятельность. В случае неудачного перехода через ребро, агент помещает это ребро в черный список до окончания выполнения текущей цели, строит новый маршрут до цели, учитывая ребра, помещенные в черный список.

Агенты *S* и *T* имеют различные функции оценки маршрута. Агент S выбирает маршрут с наименьшей суммарной стоимостью перехода, стоимость перехода рассчитывается как произведение веса ребра на его длину: *C* – оценка маршрута *P*, *w* – вес ребра, *l* – длина ребра.

$$C = \sum_{i}^{P} w_i l_i \qquad (4)$$

где: i – ребро, $i \in P$.

Агент T при расчете стоимости перехода учитывает степень доверия к переходам. Предполагается, что за активностью среды было проведено наблюдение, и агент *T* считает доверие, как отношение времени, когда ребро было доступно для перемещения, к общему вре-

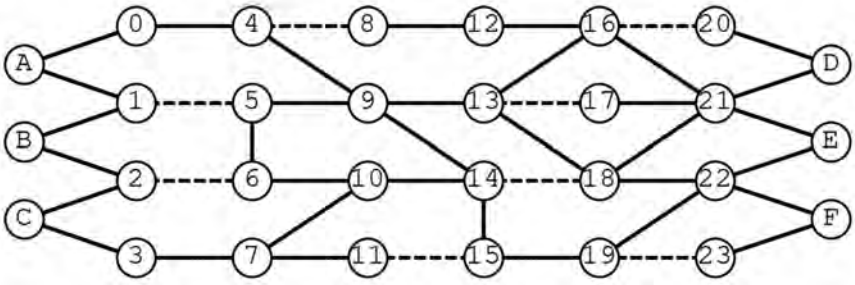

Рис. 1. Изображение графа для случая 1

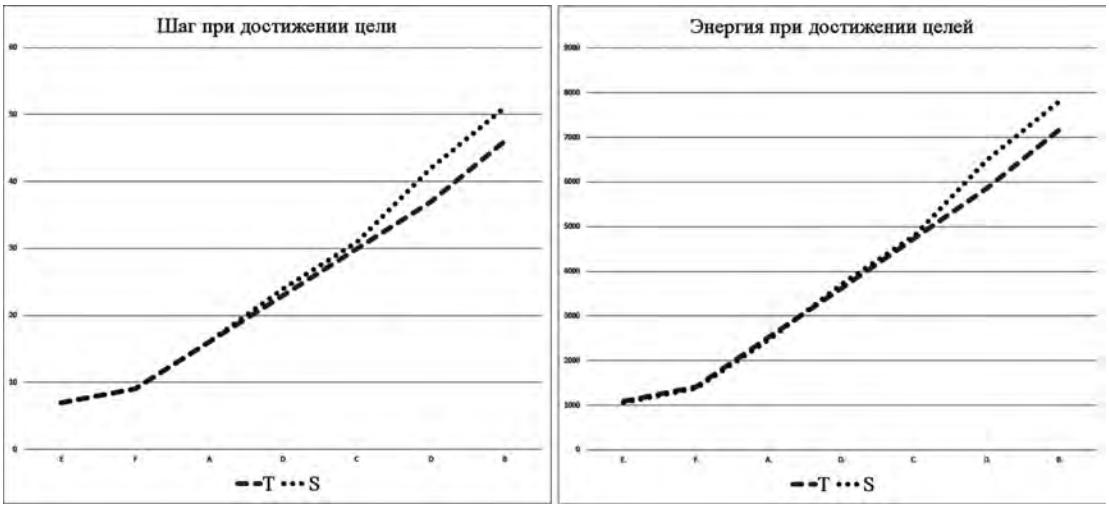

Рис. 2. Графики результатов симуляции случая 1

DOI:10.21681/2311-3456-2020-06-23-31

мени наблюдения. Пусть t – время наблюдения за средой, t'_i – время, в течение которого ребро i было открыто для перемещения, тогда оценка маршрута агентом T:

$$C = \sum_{i}^{P} \left(w_i + 1 - \frac{t'_i}{t} \right) l_i \qquad (5)$$

где: i – ребро, $i \in P$.

Случай 1

Граф среды включает 29 вершин. Вершины *A*, *B*, *C*, *D*, *E*, *F* используются как цели. На (Рис. 1) представлено изображение графа, где ребра, отмеченные сплошными линиями доступны всегда, линии, отмеченные пунктирной линией – изменяют свое состояние. В начале агенты размещены в узле *B*. Агенты имеют следующий набор задач, выбранных случайно: *E*, *F*, *A*, *D*, *C*, *D*, *B*. На (Рис. 2) изображен процесс выполнения задач агентами: количество энергии, израсходованной агентом при достижении каждой цели, и шаг симуляции, на котором была достигнута каждая цель.

Случай 2

Граф среды включает 45 вершин. Вершины *A*, *B*, *C*, *D*, *E*, *F*, *G*, *H*, *I* используются как цели. На (Рис. 3) представлено изображение графа, где ребра, отмеченные сплошными линиями доступны всегда, линии, отмеченные пунктирной линией – изменяют свое состояние. В начале агенты размещены в узле *B*. Агенты имеют следующий набор задач, выбранных случайно: *E*, *F*, *A*, *I*, *D*, *C*, *I*, *D*, *H*, *B*, *I*, *G*, *F*, *I*, *H*, *B*, *I*. На (Рис. 4) изображен процесс выполнения задач агентами: количество энергии, израсходованной узлом при достижении каждой цели, и шаг симуляции, на котором была достигнута каждая цель.

Как следует из результатов симуляции, при решении некоторых задач агент *S* используя кратчайшие маршруты решает задачу эффективнее. Однако в долгосрочной перспективе, агент *T* имеет меньший итоговый расход энергии на решение всех задач. Дополнительно, агент *T* решил поставленные задачи за меньшее количество шагов.

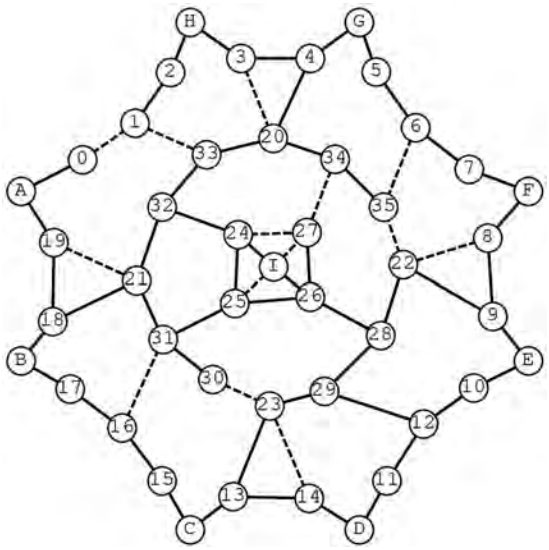

Рис. 3. Изображения графа для случая 2

Вывод

В работе был проведен анализ существующих моделей угроз и средств обеспечения безопасности в роботизированных многоагентных системах. При проведении анализа также рассматривались системы, обладающие схожими свойствами: киберфизические системы и интернет вещей. Значительную роль в обеспечении безопасности этих систем имеют подходы на основе доверия и репутации. Субъектами доверия выступают агенты, являющиеся частью информационного взаимодействия. В работе предложено рассмотрение роли процессов, происходящих в среде, в деятельности многоагентных систем. Предложен метод детектирования воздействий и оценки их влияния. Предложено расширение для методов обеспечения безопасности на основе доверия, учитывающее существование внешнего нарушителя, оказывающего непрямое воздействие на систему. Рассмотрено использование доверия к среде как элемента системы группового управления, проведено моделирование, отражающее повышение эффективности работы системы.

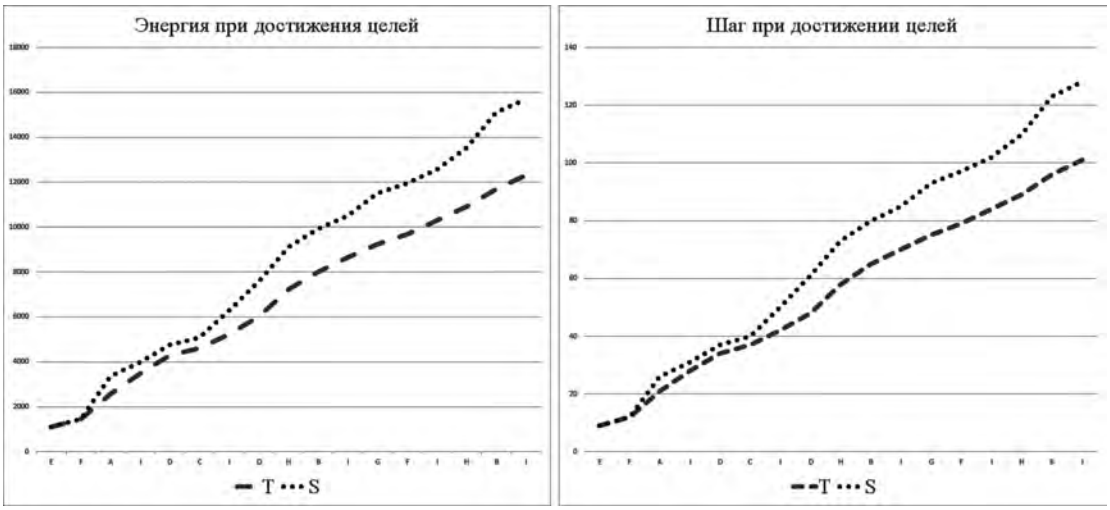

Рис. 4. Графики результатов симуляции случая 2

Литература

1. Ismail Z. H., Sariff N. A survey and analysis of cooperative multi-agent robot systems: challenges and directions //Applications of Mobile Robots. IntechOpen, 2018.
2. Sotzing C. C., Evans J., Lane D. M. A multi-agent architecture to increase coordination efficiency in multi-auv operations // CEANS 2007-Europe. IEEE, 2007. С. 1-6.
3. Uluagac A. S., Subramanian V., Beyah R. Sensory channel threats to cyber physical systems: A wake-up call // 2014 IEEE Conference on Communications and Network Security. IEEE, 2014. С. 301-309.
4. Parkinson S. et al. Cyber threats facing autonomous and connected vehicles: Future challenges // IEEE transactions on intelligent transportation systems. 2017. Т. 18. №. 11. С. 2898-2915.
5. Makhdoom I. et al. Anatomy of threats to the internet of things // IEEE Communications Surveys & Tutorials. 2018. Т. 21. №. 2. С. 1636-1675.
6. Li M. et al. Robot swarm communication networks: architectures, protocols, and applications //2008 Third International Conference on Communications and Networking in China. IEEE, 2008. С. 162-166.
7. Quenum J. G. et al. Dynamic protocol selection in open and heterogeneous systems //2006 IEEE/WIC/ACM International Conference on Intelligent Agent Technology. IEEE, 2006. С. 333-341.
8. Ahmad Yousef K. M. et al. Analyzing cyber-physical threats on robotic platforms //Sensors. 2018. Т. 18. №. 5. С. 1643.
9. Loukas G. et al. A taxonomy and survey of cyber-physical intrusion detection approaches for vehicles //Ad Hoc Networks. 2019. Т. 84. С. 124-147.
10. Archibald C., Schwalm L., Ball J. E. A survey of security in robotic systems: vulnerabilities, attacks, andsolutions //International Journal of Robotics and Automation. 2017. Т. 32. №. 2.
11. Bijani S., Robertson D. A review of attacks and security approaches in open multi-agent systems // Artificial Intelligence Review. 2014. Т. 42. №. 4. С. 607-636.
12. Dorri A., Kanhere S. S., Jurdak R. Multi-agent systems: A survey //Ieee Access. 2018. Т. 6. С. 28573-28593.
13. Bezemskij A. et al. Detecting cyber-physical threats in an autonomous robotic vehicle using Bayesian Networks // 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, 2017. С. 98-103.
14. Afanasyev I. et al. Blockchain solutions for multi-agent robotic systems: Related work and open questions //arXiv preprint arXiv:1903.11041. 2019.
15. Danilov K. et al. Towards blockchain-based robonomics: autonomous agents behavior validation // 2018 International Conference on Intelligent Systems (IS). IEEE, 2018. С. 222-227.
16. Wang Y., Singh M. P. Formal Trust Model for Multiagent Systems //JCAI. 2007. Т. 7. С. 1551-1556.
17. Wang Y., Singh M. P. Evidence-based trust: A mathematical model geared for multiagent systems // ACM Transactions on Autonomous and Adaptive Systems (TAAS). 2010. Т. 5. №. 4. С. 1-28.
18. Jung Y. et al. A survey of security issue in multi-agent systems // Artificial Intelligence Review. 2012. Т. 37. №. 3. С. 239-260.
19. Granatyr J. et al. Trust and reputation models for multiagent systems //ACM Computing Surveys (CSUR). 2015. Т. 48. №. 2. С. 1-42.
20. Zikratov I. et al. Dynamic trust management framework for robotic multi-agent systems // Internet of Things, Smart Spaces, and Next Generation Networks and Systems. Springer, Cham, 2016. С. 339-348.
21. Shi J. et al. A survey of cyber-physical systems // 2011 international conference on wireless communications and signal processing (WCSP). IEEE, 2011. С. 1-6.
22. Gunes V. et al. A survey on concepts, applications, and challenges in cyber-physical systems // KSII Transactions on Internet & Information Systems. 2014. Т. 8. №. 12.
23. Wong L. H., Looi C. K. Swarm intelligence: new techniques for adaptive systems to provide learning support // Interactive Learning Environments. 2012. Т. 20. №. 1. С. 19-40.
24. Li X., Branke J., Blackwell T. Particle swarm with speciation and adaptation in a dynamic environment // Proceedings of the 8th annual conference on Genetic and evolutionary computation

DOI:10.21681/2311-3456-2020-06-23-31

TRUST MODEL OF INFORMATION SECURITY OF THE ENVIRONMENT OF MULTI-AGENT ROBOTIC SYSTEMS

Stepenkin A.A.[2]

Abstract:

The capabilities of robotic systems are growing rapidly. The ways of operating such systems are increasing every day. Sensor networks, the Internet of Things, cyber-physical systems have similar properties as multi-agent robotic systems, which allows us to consider the approaches and methods of ensuring security used in them.

Purpose of the article: *improving the security of multi-agent systems in an uncontrolled environment, developing methods for assessing trust of the environment.*

Research methods: *analysis of existing threat models for multi-agent robotic systems, as well as systems with similar properties: cyber-physical systems and the Internet of things. Analysis of the research results of existing approaches to ensuring the security of multi-agent systems.*

The results: *an analysis of security threats and existing methods of ensuring security for robotic multi-agent systems, as well as systems with similar properties, was carried out. An extension for security methods based on trust and reputation has been developed, taking into account the operating environment of the system as part of information interaction. A method for localizing the subject of an external intruder in the environment is proposed.*

Keywords: *multi-agent systems, group management systems, trust and reputation systems, intrusion detection.*

References

1. Ismail Z. H., Sariff N. A survey and analysis of cooperative multi-agent robot systems: challenges and directions //Applications of Mobile Robots. – IntechOpen, 2018.
2. Sotzing C. C., Evans J., Lane D. M. A multi-agent architecture to increase coordination efficiency in multi-auv operations //OCEANS 2007-Europe. – IEEE, 2007. – С. 1-6.
3. Uluagac A. S., Subramanian V., Beyah R. Sensory channel threats to cyber physical systems: A wake-up call //2014 IEEE Conference on Communications and Network Security. – IEEE, 2014. – С. 301-309.
4. Parkinson S. et al. Cyber threats facing autonomous and connected vehicles: Future challenges //IEEE transactions on intelligent transportation systems. – 2017. – Т. 18. – №. 11. – С. 2898-2915.
5. Makhdoom I. et al. Anatomy of threats to the internet of things //IEEE Communications Surveys & Tutorials. – 2018. – Т. 21. – №. 2. – С. 1636-1675.
6. Li M. et al. Robot swarm communication networks: architectures, protocols, and applications //2008 Third International Conference on Communications and Networking in China. – IEEE, 2008. – С. 162-166.
7. Quenum J. G. et al. Dynamic protocol selection in open and heterogeneous systems //2006 IEEE/WIC/ACM International Conference on Intelligent Agent Technology. – IEEE, 2006. – С. 333-341.
8. Ahmad Yousef K. M. et al. Analyzing cyber-physical threats on robotic platforms //Sensors. – 2018. – Т. 18. – №. 5. – С. 1643.
9. Loukas G. et al. A taxonomy and survey of cyber-physical intrusion detection approaches for vehicles //Ad Hoc Networks. – 2019. – Т. 84. – С. 124-147.
10. Archibald C., Schwalm L., Ball J. E. A survey of security in robotic systems: vulnerabilities, attacks, andsolutions //International Journal of Robotics and Automation. – 2017. – Т. 32. – №. 2.
11. Bijani S., Robertson D. A review of attacks and security approaches in open multi-agent systems //Artificial Intelligence Review. – 2014. – Т. 42. – №. 4. – С. 607-636.
12. Dorri A., Kanhere S. S., Jurdak R. Multi-agent systems: A survey //Ieee Access. – 2018. – Т. 6. – С. 28573-28593.
13. Bezemskij A. et al. Detecting cyber-physical threats in an autonomous robotic vehicle using Bayesian Networks //2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). – IEEE, 2017. – С. 98-103.
14. Afanasyev I. et al. Blockchain solutions for multi-agent robotic systems: Related work and open questions //arXiv preprint arXiv:1903.11041. – 2019.
15. Danilov K. et al. Towards blockchain-based robonomics: autonomous agents behavior validation //2018 International Conference on Intelligent Systems (IS). – IEEE, 2018. – С. 222-227.
16. Wang Y., Singh M. P. Formal Trust Model for Multiagent Systems //IJCAI. – 2007. – Т. 7. – С. 1551-1556.
17. Wang Y., Singh M. P. Evidence-based trust: A mathematical model geared for multiagent systems //ACM Transactions on Autonomous and Adaptive Systems (TAAS). – 2010. – Т. 5. – №. 4. – С. 1-28.
18. Jung Y. et al. A survey of security issue in multi-agent systems //Artificial Intelligence Review. – 2012. – Т. 37. – №. 3. – С. 239-260.
19. Granatyr J. et al. Trust and reputation models for multiagent systems //ACM Computing Surveys (CSUR). – 2015. – Т. 48. – №. 2. – С. 1-42.

2 Andreiy Stepenkin, Postgraduate, Department of Information Security Southern Federal University, Taganrog, Russia. E-mail: stepen927@gmail.com

20. Zikratov I. et al. Dynamic trust management framework for robotic multi-agent systems //Internet of Things, Smart Spaces, and Next Generation Networks and Systems. – Springer, Cham, 2016. – С. 339-348.
21. Shi J. et al. A survey of cyber-physical systems //2011 international conference on wireless communications and signal processing (WCSP). – IEEE, 2011. – С. 1-6.
22. Gunes V. et al. A survey on concepts, applications, and challenges in cyber-physical systems //KSII Transactions on Internet & Information Systems. – 2014. – Т. 8. – №. 12.
23. Wong L. H., Looi C. K. Swarm intelligence: new techniques for adaptive systems to provide learning support //Interactive Learning Environments. – 2012. – Т. 20. – №. 1. – С. 19-40.
24. Li X., Branke J., Blackwell T. Particle swarm with speciation and adaptation in a dynamic environment //Proceedings of the 8th annual conference on Genetic and evolutionary computation