Подход к обнаружению новых кибератак на киберфизические системы на основании метода обнаружения аномалий

Р.А. Юрьева, И.И. Викснин, А.Р. Мурадов, О.С. Масленников, И.И. Комаров, И.С. Пантюхин (Университет ИТМО)

Представлены результаты исследований, направленных на повышение кибербезопасности распределенных мультиагентных киберфизических систем (КФС). Основные этапы работ связаны с анализом скрытых деструктивных информационных воздействий (СДИВ), не нарушающим штатные режимы работы элементов системы; формированием пространства косвенных признаков функционирования КФС, позволяющих сделать вывод о наличии информационных атак.

Результатом исследования является расширяемый подход к обнаружению новых кибератак на КФС, основанный на анализе косвенных признаков функционирования сложной системы при выполнении репрезентативных алгоритмов. Он обеспечивает возможность для разработки робастных алгоритмов автоматической идентификации информационных атак на КФС, методов противодействия им, а также пополнению функциональности систем Business Intelligence.

Ключевые слова: кибербезопасность, мультиагентные распределенные киберфизические системы, скрытое деструктивное информационное воздействие, идентификация атак.

Введение

В основе Industry 4.0, с которой связывают ожидания очередной технологической революции, лежит концепция распределенных агентов-вычислителей (мультиагентные системы [1]). К частному случаю таких систем можно отнести киберфизические системы (КФС), представляющие собой симбиоз компонентов информационного и физического уровней [2]. Уже сейчас использование КФС является одним из перспективных направлений решения целого ряда специфических задач, к которым принято относить, прежде всего, задачи с минимальным априорным и минимальным оперативным информационным обеспечением, решаемые в ограниченном временном интервале [3], а также трудно формализуемые задачи с «взрывообразным» ростом сложности, возникающем при увеличении числа агентов или данных.

Вместе с тем задача развития компонентов Industry 4.0, и КФС в частности, зачастую решается в отрыве от задачи обеспечения информационной безопасности (кибербезопасности) новых информационных технологий. Такая несогласованность только увеличивает противоречие между усилением зависимости всех сфер жизни общества от информационных технологий и незащищенностью самих этих технологий, особенно обеспечивающих функционирование критически важных, опасных и транснациональных технологических процессов. Таким образом, задача обеспечения кибербезопасности выходит в перечень первоочередных задач мирового масштаба.

Сложность решения задач обеспечения кибербезопасности перспективных технологий осложняется, как минимум, двумя факторами:

1) безопасность нельзя просто «наложить» на уже реализованные процессы, зачастую они требуют кардинального пересмотра самих технологических компонентов;

2) модели и методы «классической» защиты информации слабо применимы в перспективных технологиях, а методы и средства непосредственного получения данных об информационных атаках требуют расширения моделями анализа системы косвенных признаков скрытых информационных атак.

Industry 4.0 — отложенная угроза

Традиционная ориентация нефтегазовой промышленности на самые современные технологические решения в области производственной автоматизации обеспечила предпосылки для опережающего внедрения компонентов Industry 4.0 с использованием эволюционной стратегии, то есть без разрушения апробированных методов, средств и организационных структур. Сдержанный оптимизм вызывает состояние кибербезопасности операционной деятельности в краткосрочной перспективе (https://www2.deloitte.com).

В частности, например, в рамках нефтеперерабатывающего завода (НПЗ) могут быть использованы такие свойства КФС, как самоорганизация/самоадаптация, автоматическое решение математически сложных задач, самовосстановление, в том числе в условиях, не предусмотренных штатными режимами эксплуатации. Эти имманентные свойства мультиагентных КФС, развивающих концепцию Internet of Things (IoT), но под управлением единого целеполагающего центра, обеспечивают решение целого

ряда задач на новых принципах, а именно: опережающий (предиктивный) контроль параметров сложных технологических процессов, выявление причин нарушения технологических этапов на ранних стадиях возникновения, интеллектуальный контроль производственной безопасности, распределенный контроль параметров и анализ возможных ошибок (преднамеренных фальсификаций) операторов. Кроме того, использование КФС позволяет на новом уровне эффективности организовать применение промышленных автономных роботов [4].

Желание оставаться на лидирующих позициях рынка, в частности оперативно внедряться в расширенную производственную цепочку партнера (как клиента, так и поставщика), приводит к отношению к кибербезопасности «по остаточному» принципу, когда вопросы ИБ или отходят на задний план, либо игнорируются полностью. (Справедливости ради следует заметить, что это вызвано не только халатностью или недальновидностью разработчиков, зачастую система хозяйственных отношений и используемых технологий даже в масштабах одного ведомства слишком противоречива и многогранна для того, чтобы быть формализованной в системе кибербезопасности).

Вместе с тем, увеличение степени проникновения КФС во все сферы социальных отношений и, особенно, в архитектуру опасных производств и критически важных инфраструктур влечет рост рисков, определяемых состоянием именно информационной безопасности внедряемых технологий. Интуитивно результаты деструктивного воздействия на КФС ассоциируются с кадрами техно-апокалипсических фильмов. Однако использование апробированных методов и средств «классической» защиты информации в «классической» технологии управления бизнесом до некоторой степени гарантируют его безопасность, но препятствует его эволюционному развитию в контексте развития Industry 4.0.

Цели исследования

Согласно прогнозам (https://www2.deloitte.com), следует ожидать увеличение темпов роста маргинального ущерба от деструктивного воздействия, а наибольшую опасность представляют деструктивные информационные воздействия новых типов, особенности реализации и защита от которых еще не изучена в достаточной степени. Продекларированные [5] группы специфических угроз безопасности КФС требуют конкретизации, а главное — разработки методов обнаружения и противодействия атакам, использующим имманентные уязвимости КФС.

Поэтому в работе рассматривается один из видов информационных атак — скрытое деструктивное информационное воздействие (СДИВ), характеризующееся отсутствием ярко выраженных признаков атаки, то есть элементы системы и каналы связи не выводятся из штатного режима работы. Это не позволяет вовремя обнаружить нарушителей в системе классическими способами, что может привести к разрушению технологических процессов. В работе рассматриваются принципы обнаружения СДИВ на ограниченном классе КФС — динамические КФС. Это КФС, элементы которой меняют свое местоположение, исходя из временных принципов и решаемых задач.

Авторы предлагают подход к обнаружению СДИВ на КФС на основе анализа косвенных признаков ее функционирования. Полученные результаты обеспечивают решение целого ряда прикладных задач в области автоматизации промышленных процессов, например, но не ограничиваясь:

— разработка робастных алгоритмов автоматического обнаружения факта СДИВ на возможно ранних этапах выполнения технологических задач производства;

— разработка алгоритмов получения количественных характеристик СДИВ на основе обнаружения аномалий в эталонных «портретах» поведения системы, где под портретом понимается набор специальным образом преобразованных информативных параметров функционирования КФС;

— разработка методов противодействия СДИВ;

— получение дополнительной функциональности аналитических сервисов предприятия за счет выявления новых закономерностей между параметрами производства и параметрами КФС.

Для разработки общего решения поставленной задачи будет рассматриваться одна из возможных реализаций динамической КФС — промышленные роботы. Такой выбор обусловлен присущей им возможностью и необходимостью менять свое местоположение или оставаться в одной точке. Изменение позиции элемента позволяет говорить об использовании набора стандартных алгоритмов перемещения, на основе которых можно анализировать наличие атаки на систему. Актуальность данной темы подтверждается увеличением числа подходов к решению задач обеспечения функционирования распределенных систем на базе автономных транспортных средств [6, 7], являющихся частным случаем реализации КФС.

Техника исследования

В силу сложности аналитического описания эффекта синергии групповой робототехники, а также трудностями учета технической реализации большого числа агентов, связанных с разбросом параметров, в качестве методологической основы исследования использовано имитационное моделирование (ИМ).

В качестве инструментального средства ИМ выбрана среда V-REP в режиме моделирования поведения робота Kilobot компании K-team [8], обеспечивающая поддержку модельного эксперимента, как с физическими реализациями агентов, так и с их программными моделями. Существенными достоинствами среды являются: декларируемая взаимная переносимость параметров физической модели и компьютерного эксперимента; поддержка широкого спектра лабораторных роботов и свободная расши-

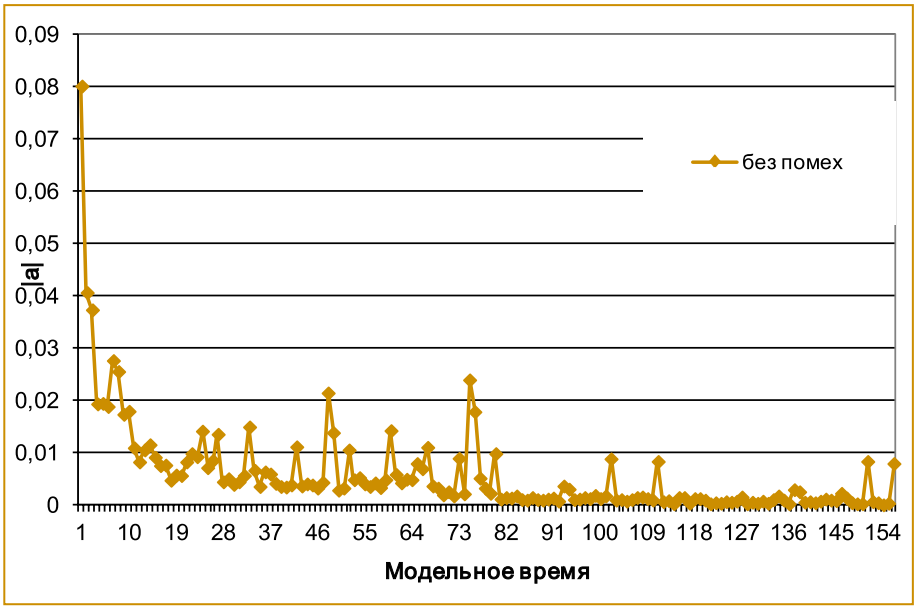

Рис. 1. Динамика суммы модулей ускорения агентов при выполнении задачи без помех – для алгоритма распределения по поверхностям

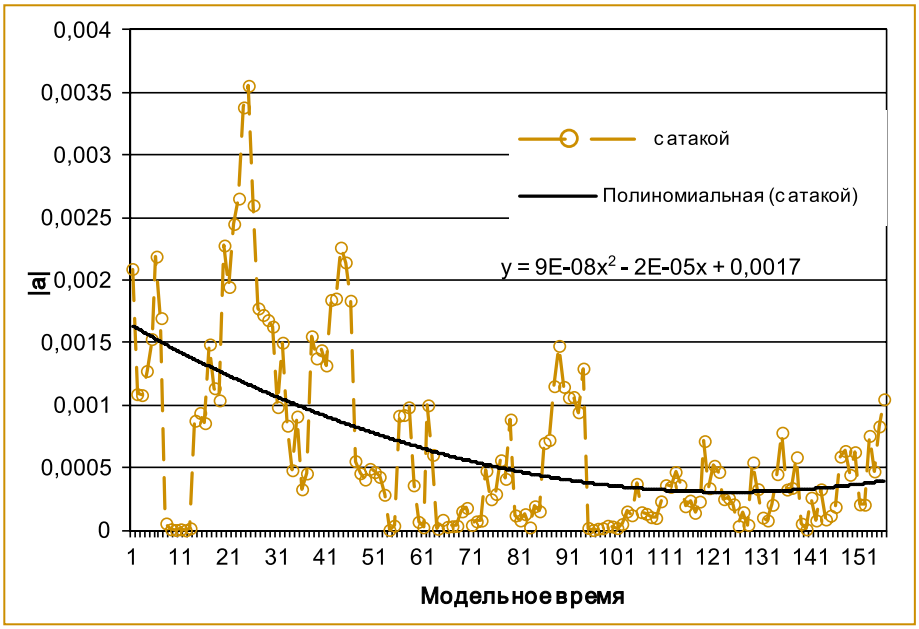

Рис. 2. Зависимость математического ожидания суммы модулей ускорения всех объектов от времени решения задачи – для алгоритма распределения по поверхностям в условиях ДИВ

ряемость программного кода; одна из самых низких стоимостей исследовательского полигона; возможность использования свободного программного обеспечения.

Технология адаптации полученных результатов к условиям функционирования реальных систем включает следующие этапы:

1) на основании данных, полученных в ходе теоретических и экспериментальных исследований [9, 10], формулируется перечень репрезентативных алгоритмов выполнения типовых операций КФС;

2) определяется информативность элементов признакового пространства;

3) формируется «портрет» выполнения этих алгоритмов в определенном признаковом пространстве;

4) анализ возможных методов и средств скрытого ДИВ, то есть не рассматриваются случаи физического уничтожения, силового электромагнитного подавления, DDoS- атаки и т. п.;

5) получение «портретов» выполнения репрезентативных алгоритмов при СДИВ;

6) проверка информативности элементов признакового пространства с точки зрения различимости процесса достижения основной цели КФС в условиях без помех и при ДИВ.

Адаптация к самоорганизующейся сети мобильных датчиков

Проверка разработанного решения проведена на примере сети мобильных датчиков, выполняющих задачу в двумерном изотропном пространстве в соответствии с этапами 1–6.

В результате выполнения первого этапа выделены четыре алгоритма, которые используются в качестве типовых шагов при решении задач КФС: *распределение по поверхности, распределение по укрытиям, группирование* (по парам), *покрытие площади* (обход) круга. Гомогенные агенты реализуют одинаковые алгоритмы решения задач, формализованное изложение которых представляются в [3].

На *втором этапе* в качестве кандидатов на информативные косвенные признаки анализировались две группы признаков, первая из которых связана с механическим перемещением агентов, а вторая — с информационным взаимодействием агентов. В первую группу входили упомянутые выше алгоритмы; во вторую – алгоритмы *обмена идентификаторами*, алгоритмы *выбора лидера*, алгоритмы *выбора цели* в локальной группе.

По результатам предварительного анализа наиболее перспективным признаком оказалась *сумма модулей ускорения* элементарных агентов.

По результатам *третьего этапа исследования* — формирование портрета выполнения репрезентативных алгоритмов в выбранном определенном признаковом

пространстве без ДИВ — получены соответствующие зависимости. На рис. 1 приведены усредненные результаты серии экспериментов в осях «модельное время — средний модуль ускорения всех агентов» для алгоритма распределения по поверхности. Несколько забегая вперед, следует отметить, что такие, казалось бы, очевидные показатели функционирования группировки роботов, как перемещение центра масс, средняя скорость, суммарный вектор перемещения, применявшиеся в исследованиях отдельных авторов, оказались совершенно неинформативны в условиях эксперимента. Тогда как такой неочевидный показатель (*сумма модулей ускорения*) обеспечил не только решение поставленной задачи, но и позволил выявить специфические фазы работы роботов конкретного типа: характерные всплески на спадающей кривой оказались связаны с этапами *взаимной* корректировки положения агентов в пространстве и связанного с этим «перетоптывания» и уточнением выбора направления не одного, а целой группы агентов.

Четвертый этап — анализ возможных методов и средств скрытого ДИВ — реализовывалась с использованием методов структурного и функционального анализа сложных систем [11], основных положений ГОСТ Р 51275-2006. «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» и подхода, изложенного в «Методике определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (ФСТЭК России, 2008 г.). По результатам работы получены модель угроз и модель нарушителя информационной безопасности КФС, обсуждение которых выходит за рамки настоящей статьи [12].

Один из типовых способов реализация СДИВ является «введение в заблуждение» элементарных агентов. Для этого используется агент-диверсант, который сообщает заведомо ложную информацию о своем состоянии, окружающей среде или степени выполнения задачи. Напомним, что у аутентичного агента нет возможности проверить истинность получаемой информации. В зависимости от компрометируемого (атакуемого) алгоритма могут использоваться различные сценарии атак. Например, при попытке срыва задачи группирования может использоваться внедрение некоторого числа неподвижных роботов-злоумышленников, которые имитируют вступление в пару с роботами-агентами и тем самым снижают эффективность выполнения задачи. Техническая реализация агента-диверсанта осуществляется по той же технологии, что и остальные агенты, отличаясь только своей программой, что может переводить СДИВ из класса преднамеренных воздействий в класс случайных — при возникновении нарушений в работе аутентичных роботов.

Реализация *пятого этапа* — получение «портретов» выполнения репрезентативных алгоритмов при ДИВ — выполнена аналогично этапу 3 путем проведения серии модельных экспериментов, обработанные результаты которых представлены на рис. 2. Характерными чертами этого портрета являются: общее снижение значения анализируемого показателя $\leqslant 0{,}0036$ ед/t^2 (по сравнению 0,8 ед/t^2 на рис. 1); наличие этапов неизменных скоростей (рис. 2, в районе отметки 10), резкие изменения показателя в смежных интервалах (например]15;25 [,]82;92 [); немонотонное поведение аппроксимирующей кривой.

Этап шесть — проверка информативности элементов признакового пространства с точки зрения различимости процесса достижения основной цели КФС в условиях без помех и при ДИВ демонстрирует различимость поведения группировки. Различия выражаются как в величине абсолютных значений модулей ускорения агентов, времени выполнения задачи, так и в характере изменения показателей (рис. 1 и 2 — для алгоритма распределения по поверхности).

Систематическое наблюдение указанных различий в поведении системы, находящей под кибератакой и без нее, позволяют утверждать о выявлении новой закономерности, которая может быть использована в прикладных задачах. Наиболее очевидным методом динамического контроля кибербезопасности КФС представляется использование апробированного аппарата карт Шухарта согласно ГОСТ Р 50779.42-99 (ИСО 8258-91) «Статистические методы. Контрольные карты Шухарта» (переиздание, июль, 2004 г.).

Таким образом, результаты исследования подтверждают работоспособность авторского подхода по разработке решений для защиты мультиагентных распределенных КФС от скрытого деструктивного информационного воздействия.

Заключение

В работе получены экспериментальные подтверждения предлагаемого подхода, который может быть адаптирован не только для решения частных задач выявления СДИВ на целевые системы, но и расширен для получения дополнительной функциональности системы комплексной автоматизации производства.

Основным результатом работы является методика выявления новых скрытых атак на киберфизические системы, реализующая подход, основанный на получении косвенных характеристик функционирования КФС при выполнении репрезентативных алгоритмов. Она может использоваться при исследовании групп, состоящих из других агентов, и обеспечивает формирование портретов процессов, зависящих от конструктивных особенностей элемента системы.

Основные направления развития результатов исследования связаны с пожеланиями заказчика по решению целого семейства прямых и обратных задач выявления скрытого кибервоздействия. А именно, но, не ограничиваясь:

— разработка формальных алгоритмов обнаружения ДИВ на КФС на возможно ранних этапах выполнения основной задачи с использованием эталонных и динамически формируемых портретов частных задач;

— разработка методик количественной оценки ДИВ на КФС;

— получение оценок числа роботов-диверсантов;

— оценка вероятности выполнения основной задачи с учетом нанесенного ущерба;

— необходимое/достаточное число аутентичных роботов для выполнения задачи группировкой с заданной вероятностью с учетом данных о наличии/возможностях роботов-диверсантов.

Кроме того, полученные результаты могут использоваться при разработке методов и средств противодействия ДИВ на КФС и, в частности, устойчивых к компрометации алгоритмов взаимодействия.

Список литературы

1. *Jazdi N.* Cyber physical systems in the context of Industry 4.0//Automation, Quality and Testing, Robotics, 2014 IEEE International Conference on. IEEE, 2014. С. 1-4.
2. *Akella R., Tang H., McMillin B.M.* Analysis of information flow security in cyber–physical systems //International Journal of Critical Infrastructure Protection. 2010. Т. 3. №. 3. С. 157-173.
3. *Каляев И.А., Гайдук А.Р., Капустян С.Г.* Модели и алгоритмы коллективного управления в группах роботов. М.: Физматлит. 2009. Т. 280.
4. *Lee E.A.* Cyber physical systems: Design challenges //Object Oriented Real-Time Distributed Computing (ISORC). 11th IEEE International Symposium on. IEEE. 2008. С. 363-369.
5. *Higgins F., Tomlinson A., Martin K. M.* Threats to the swarm: Security considerations for swarm robotics //International Journal on Advances in Security. 2009. Т. 2. №. 2&3.
6. *Зикратов И.А., Викснин И.И., Зикратова Т.В.* Мультиагентное планирование проезда перекрестка дорог беспилотными транспортными средствами // Научно-технический вестник информационных технологий, механики и оптики. 2016. Т. 16. № 5(105). С. 839-849.
7. *Viksnin I. I., Iureva, R. A., Komarov I. I., Drannik A. L* Assessment of stability of algorithms based on trust and reputation model // FRUCT. 2016. С. 364-369.
8. *Rubenstein M., Hoff N., Nagpal R.* Kilobot: A low cost scalable robot system for collective behaviors // Robotics and Automation (ICRA), 2012 IEEE International Conference on. IEEE, 2012, С. 3293-3298.
9. *Дранник А.Л., Комаров И. И., Юрьева Р. А.* Моделирование проблем информационной безопасности мультиагентных систем//В мире научных открытий. 2014. № 4 (52). 418 с. С. 61-71.
10. *Юрьева Р.А., Комаров И.И., Дранник А.Л., Масленников О.С., Егоров Д.А., Елисеев Ю.М.* Учет конструктивных особенностей стайных роботов в решении задач моделирования проблем информационной безопасности // Наука и бизнес: пути развития. 2015. № 3(45). С. 63-67.
11. *Коваль Е.Н., Лебедев И.С.* Общая модель информационной безопасности робототехнических систем // Научно-технический вестник информационных технологий, механики и оптики. 2013. № 4(86). С. 153-154.
12. *Юрьева Р.А., Комаров И.И., Дородников Н.А.* Построение модели нарушителя информационной безопасности для мультиагентной робототехнической системы с децентрализованным управлением//Программные системы и вычислительные методы. 2016. № 1. С. 42-48.

Мурадов Александр Романович *– старший лаборант,* ***Викснин Илья Игоревич*** *– ассистент,*
Пантюхин Игорь Сергеевич *– ассистент,* ***Масленников Олег Сергеевич*** *– ассистент,*
Комаров Игорь Иванович *– канд. физ.-мат. наук, доцент кафедры проектирования и безопасности компьютерных систем,* ***Юрьева Радда Алексеевна*** *– ассистент кафедры систем и технологий техногенной безопасности Университета ИТМО.*
Контактный телефон +7 (812) 232-97-04.

Сетевой пакетный симулятор для моделирования динамических свойств коммуникационной сети

Г.М. Антонова (ИПУ РАН), А.П. Титов (МФЮА)

Показано, что известные сетевые пакетные симуляторы помогают решать многочисленные задачи исследования и совершенствования телекоммуникационных систем, но не предназначены для имитации динамических свойств сети. Описана структура сетевого пакетного симулятора, учитывающего динамические свойства сети, а также алгоритм его работы.

Ключевые слова: сетевой пакетный симулятор, коммуникационные сети, динамические свойства, имитационное моделирование.

Введение

Создание динамической модели коммуникационной сети — актуальная задача современного этапа развития рынка промышленной автоматизации. Компьютерная модель необходима при тестирование новых протоколов передачи данных, при выборе оптимальной сетевой архитектуры и компонентов коммуникационной инфраструктуры и др. Для систем передачи данных (СПД), работающих с большими потоками информации [1], пользователи должны понимать влияние на работу сети таких характеристик, как коэффициент готовности, полоса пропускания, среднее время передачи сообщения или пакета, задержки, вероятность потери сообщения или пакета и др. Предварительное определение оценок качества СПД по модели требуется как при проектировании, так и в процессе эксплуатации с целью мониторинга функционирования.

Цель работы состоит в обосновании выбора модулей ПО для моделирования динамических свойств коммуникационной сети. Процессы в СПД имеют очень высокую скорость. Даже совершенные компьютерные модели не способны имитировать реальные процессы, протекающие в коммуникационных устройствах передачи данных и отследить изменения текущих характеристик во времени. Однако обобщенные интегральные характеристики сети могут быть успешно исследованы, если будет создана адекватная модель. Имитационные эксперименты позволят проверить изменения значений интегральных характеристик сети в реальных условиях эксплуатации и сделать вывод о пригодности СПД для внедрения.