КОДИРОВАНИЕ И ЗАЩИТА ИНФОРМАЦИИ

Юрьева Р.А., Комаров И.И., Масленников О.С.

РАЗРАБОТКА МЕТОДА ОБНАРУЖЕНИЯ И ИДЕНТИФИКАЦИИ СКРЫТОГО ДЕСТРУКТИВНОГО ВОЗДЕЙСТВИЯ НА МУЛЬТИАГЕНТНЫЕ РОБОТОТЕХНИЧЕСКИЕ СИСТЕМЫ

Аннотация: *Увеличение рисков информационной безопасности (ИБ) мультиагентной робототехнической системы (МРТС), к числу которых относятся потеря или недоступность данных, распространения ложных данных о цели группировки и использование искаженной информации, нехватка энергетических ресурсов, обуславливает потребность в оценке известных и новых алгоритмов с точки зрения безопасности. Стоит отметить, что единые подходы к обеспечению ИБ МРТС до настоящего момента не сформированы. Исследование направлено на разработку модели ИБ МРТС, учитывающую специфику технологии. Имеющийся научно-методический аппарат и технические решения обеспечения ИБ мультиагентных систем не применимы для задач обеспечения ИБ МРТС ввиду специфических технологий и особого вида модели угроз и модели нарушителя, связанных с ними. Существующие методы обеспечения ИБ мультиагентных систем не обеспечивают комплексного решения проблем ИБ в МРТС, так как они не учитывают специфику их состава и структуры. Научная новизна заключается в разработке модели обеспечения ИБ МРТС. Преимущество предлагаемого метода заключается в возможности обнаружения атак нового типа без модификации или обновления параметров модели, так как вторжение нарушителя в систему может быть описано как некоторое отклонение от штатного поведения.*

Ключевые слова: *мультиагентная робототехническая система, децентрализованное управление, модель информационной безопасности, роевой интеллект, защита информации, информационная атака, информативные признаки, признаковое пространство, идентификация деструктивного воздействия, скрытое деструктивное воздействие*

Abstract: *Increased information security risks in multi-agent robotic systems create a need for new and known assessment in terms of security algorithms. Such risks include the loss or inaccessibility of data, spreading false information about the purpose of grouping and the use of distorted information, lack of energy resources. Authors note that common approaches to information*

DOI: 10.7256/2305-6061.2016.4.21128

security in multi-agent robotic systems so far are not formed. The research is aimed at developing a model of information security in multi-agent robotic systems taking into account the specifics of the technology. Existing scientific and methodical apparatus and technical solutions of ensuring information security in multi-agent systems are not applicable to the tasks of ensuring information security in multi-agent robotic systems due to the specific technology and a special type of threat models and the offending patterns associated with them. Existing methods of providing information security of multi-agent systems do not provide a comprehensive solution of the problems of information security in the multi-agent robotic systems, since they do not take into account the specificity of their composition and structure. Scientific novelty consists in the development of software models of information security risks in multi-agent robotic systems. An advantage of the method is the ability to detect new types of attacks without having to modify or update the model parameters, since the invasion of the offending system can be described as a deviation from the nominal behavior.

Keywords: *hidden destructive effect, identification of the destructive impact, feature space, informative signs, information attack, data protection, swarm intelligence, information security model, decentralized control, multi-agent robotic system*

Мультиагентные робототехнические системы (МРТС) являются уникальными, благодаря сочетанию физических характеристик с автономным поведением, мобильностью и распределенным управления. Следовательно, «владелец» мультиагентной системы не может знать точное местоположение каждого устройства и нахождения злоумышленников в непосредственной близости.

Задача управления мультиагентной системой R состоит в том, чтобы определить такую последовательность действий (вектор-функцию действий) $A(t)$ на интервале времени $[t_0, t_f]$, выполнение которых при заданных связях, начальных условиях и ограничениях обеспечивало бы экстремум функционала [1]

$$Y = \widehat{\Phi}(R^f, E^f, t_f) + \sum_{t_0}^{t_f} F(A(t), R(t), E(t), g(t), t)dt \qquad (1)$$

При наличии организованного противодействия со стороны объектов среды достижение группой цели можно описать следующей формулой:

$$Y_c = \sum_{t_0}^{t_f}[F\left(\zeta(t), E(t), A_c(t)\right)dt - \sum_{t_0}^{t_f} D(\widetilde{A_c(t)}\,dt \to max, \qquad (2)$$

где $\zeta(t), E(t)$ - вектор-функции процесса перехода «группа роботов-среда», $A_c(t)$ - функция действий роботов, $D\left(\widetilde{A_c(t)}, k(t)\right)$ - функция организованного противодействия.

Физический захват робота может привести к немедленному нарушению доступности защищаемой информации. Злоумышленник также может использовать устройство для манипулирования передачей данных и может напасть на аппаратное устройство для извлечения защищаемой информации.

В худшем случае злоумышленник может изменить устройство и вновь ввести его в рой,

DOI: 10.7256/2305-6061.2016.4.21128

что влечет за собой ряд других атак, более опасных. Также устройство злоумышленника может работать с данными о передвижении роя к новым местам, перехватить передачу данных во время коммуникаций, представить вредоносный код или ложные команды для устройств. Злоумышленник может изменить поведение роя, не обличив своего появления. Подобные виды атак являются в некотором роде уникальными для МРТС.

Принцип работы предлагаемого метода состоит в обнаружении несоответствия между текущим режимом работы МРТС и режимом работы, который отвечает штатной модели поведения данного алгоритма, так называемым «поведенческим портретом». Несоответствие «портрету» рассматривается как информационная атака. Дляидентификации деструктивного воздействия на МРТС необходимо сгенерировать поведенческий портрет, который содержит как нормальные данные, циркулирующие в системе в штатном рабочем режиме, так и портреты, содержащие информацию об атаках. Причем последние должны быть четко определены и произведены в объеме, сравнимом с нормальными данными. Портрет нормальной активности будет построен в виде набора косвенных признаков, а также будут определены интервалы, в которых данные признаки считаются нормальными. Выход за интервалы считается аномалией.

Отличие в «портрете» определим как множество точек, удовлетворяющих условию:

$$R(f,g) = \{x \in X \| f(x) - g(x)| > T \text{ или } |f(x) - g(x)| > T\} \qquad (3)$$

где $f(x)$ – функция изменения значения информативного признака на каждом шаге итерации при отсутствии скрытого деструктивного информационного воздействия (СДИВ), $g(x)$ - функция изменения значения информативного признака на каждом шаге итерации при наличии СДИВ, x – шаг итерации, T – некоторое пороговое значение.

Признаковое пространство для идентификации отклонения от безопасной модели поведения формируется из числа доступных измерению характеристик объекта или группировки объектов, которые отражают наиболее существенные свойства в ходе выполнения репрезентативных алгоритмов. К признакам предъявляются требования: объективность, доступность (возможность получения), достаточность. Определение совокупности и/или преобразования (минимально) достаточных признаков обеспечивает возможность для синтеза формальных алгоритмов обнаружения деструктивного воздействия, которые, в свою очередь могут применяться для решения первой и второй частной задачи.

Таким образом, гипотеза о наличии функциональной связи между (2) и (3), представляемая, как

$$Y(\bar{F},\bar{D}) \leftrightarrow R(\bar{f},\bar{g}), \qquad (4)$$

в условиях введения формальных метрик в пространстве информативных признаков и реализации серий экспериментов для получения значений отклонения от безопасной модели, обеспечивает формирование множества векторов количественных значений косвенных признаков СДИВ на МРТС в пространстве времени, что, в свою очередь, позволяет формализовать и определять пути решения прямой и обратной задачи обеспечения информационной безопасности (ИБ) МРТС, а именно:

DOI: 10.7256/2305-6061.2016.4.21128

в условиях введения формальных метрик в пространстве информативных признаков и реализации серий экспериментов для получения значений отклонения от безопасной модели, обеспечивает формирование множества векторов количественных значений косвенных признаков СДИВ на МРТС в пространстве времени, что, в свою очередь, позволяет формализовать и определять пути решения прямой и обратной задачи обеспечения информационной безопасности (ИБ) МРТС, а именно:

– прямая: $R(\bar{f},\bar{g}) \to Y(t)$, «определить ожидаемое *значение показателя качества* (вероятности, времени, стоимости…) решения задачи МРТС при заданных *значениях параметров группировки* (избыточность агентов МРТС, радиус информационного взаимодействия, степень информированности о цели…) и уровне СДИВ»;
– обратная: $R(\bar{f},\bar{g}) \to D(t)$, «определить уровень СДИВ на основании данных *об отклонении реального и эталонного портретов* и при известных *значениях параметров группировки*».

Кроме того, эти задачи трансформируются во множество приводимых задач, например: определение уровня ресурсов группировки для заданного достижения цели на основании данных о СДИВ; определить необходимые силы для усиления группировки для достижения цели по результатам выявленного СДИВ, и т.п (рис.1, рис.2).

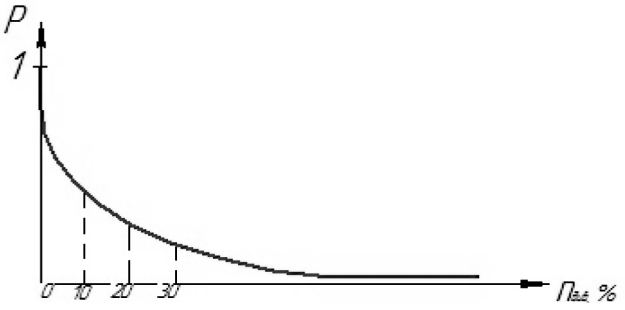

Рисунок 1 – Зависимость вероятности достижения системой цели от процента внедренных в нее злоумышленников

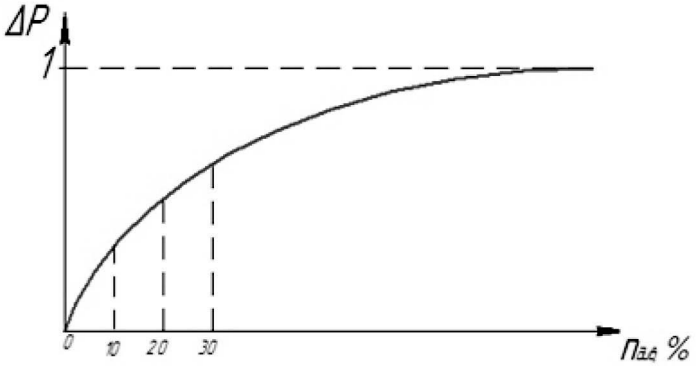

Рисунок 2 – Зависимость вероятности недостижения цели системой от процента внедренных в нее злоумышленников

DOI: 10.7256/2305-6061.2016.4.21128

Опыт исследования лабораторных образцов и программных прототипов МРТС демонстрирует существенное влияние состояния информационной безопасности группировки на результативность ее функционирования. Можно предположить, что с увеличением маргинального вклада МРТС в обеспечение технологических процессов высокой степени важности эта зависимость будет только увеличиваться. В то же время нерешенные проблемы ИБ МРТС создают предпосылки к росту рисков ИБ. Таким образом, учет состояния информационной безопасности группировки мобильных агентов должен быть включен в обобщенную модель строения и функционирования группировки.

В настоящее время получены существенные результаты в области организации МРТС на основе формализованных и адаптированных алгоритмов живой природы [2]. МРТС, состоящие из достаточно простых агентов, использующих такие алгоритмы, действительно способные решать сложные и, что наиболее интересно с практической точки зрения, трудно формализуемые задачи, проявляя эмерджентный эффект. Вместе с тем следует учитывать, что калькирование поведения живых существ в сферу современных IT не совсем корректно: как правило, в живой природе не происходит внезапных и преднамеренных деструктивных информационных воздействий на стаю, в то время как современные искусственные системы подвергаются целенаправленным полиморфным атакам, причем эта тенденция усиливается.

Спецификой обеспечения ИБ МРТС является то, что группировка состоит из автономных агентов, «роевое» информационное обеспечение распределено между ними, а достижение цели группировки обеспечивается за счёт множества параллельных воздействий агентов друг на друга и окружающую среду [3-8]. Незащищённые роевые роботы могут оказаться не только индивидуально бесполезными при СДИВ, но и привести к нарушению безопасности информационной среды МРТС в целом, что в конечном итоге приведёт к невыполнению задачи группировкой, может стать причиной материального ущерба, угрозой безопасности человека [9-11].

Выявление СДИВ на основе косвенных признаков состоит из следующих этапов:

- Определение информативности косвенных признаков;
- Формирование «поведенческого портрета» при отсутствии помех и/или информационной атаки на систему;
- Формирование «поведенческих портретов» при наличии помех и/или информационной атаки на систему;
- Получение портрета в ходе выполнения задачи и его сравнение с имеющимися типовыми.

Такой подход наиболее эффективен для обнаружения атак на этапе выполнения типовых маневров, поскольку получаемые портреты не содержат влияния других типовых маневров.

DOI: 10.7256/2305-6061.2016.4.21128

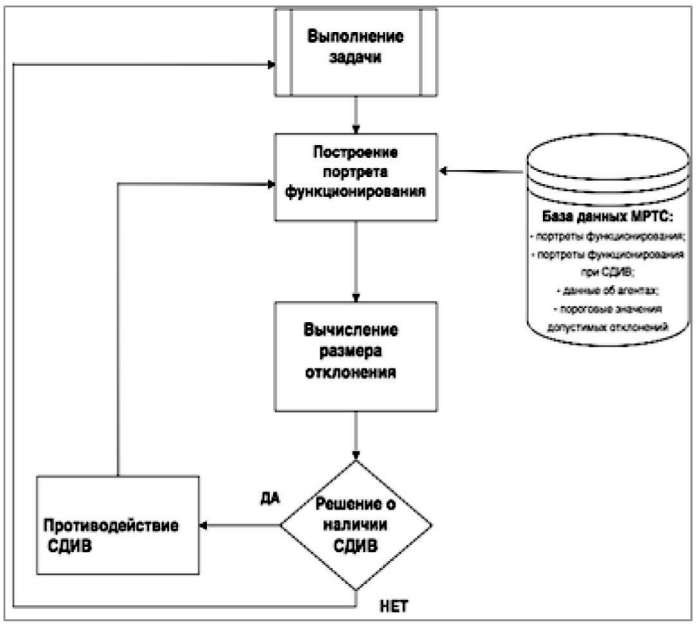

Рисунок 3 – Структура обеспечения ИБ МРТС, основанная на поведенческих процессах

Согласно предложенной структуре для обеспечения ИБ МРТС необходимо:

- Выявить специфические черты технологии.
- Создать базу портретов поведенческих процессов при наличии и отсутствия СДИВ на МРТС.
- Создать базу идентифицированных атак.

Преимущество предлагаемого метода заключается в возможности обнаружения атак нового типа без модификации или обновления параметров модели, так как вторжение нарушителя в систему может быть описано как некоторое отклонение от штатного поведения. Основополагающим элементом метода обнаружения деструктивного воздействия на МРТС является база данных, которая представляет собой набор поведенческих портретов системы при реализации различных репрезентативных алгоритмов. Накопленная база данных, включающая в себя портреты выполнения репрезентативных алгоритмов роем при наличии скрытого деструктивного воздействия, позволит не только выявить наличие атаки на систему, но и идентифицировать ее [12-13].

Библиография :

1. Каляев И.А., Гайдук А.Р., Капустян С.Г. Модели и алгоритмы коллективного управления в группах роботов. М.: ФИЗМАТЛИТ, 2009. 280 с.
2. Couzin, I.D., Krause, J., Franks, N.R. & Levin, S.A. Effective leadership and decision making in animal groups on the move. Nature 433, 513-516, 2005

DOI: 10.7256/2305-6061.2016.4.21128

3. Rubenstein M., Hoff N., Nagpal R. Kilobot: A Low Cost Scalable Robot System for Collective Behaviors. Computer Science Group Harvard University Cambridge, Massachusetts URL: ftp://ftp.deas.harvard.edu/techreports/tr-06-11.pdf (режим доступа: открытый; дата обращения: 13.02.2014).
4. Gjondrekaj E., Loreti M., Pugliese R., Tiezzi F., Pinciroli C., Brambilla M., Birattari M., Dorigo M. Towards a Formal Verification Methodology for Collective Robotic Systems. In Formal Methods and Software Engineering, Proceedings of the 14th International Conference on Formal Engineering Methods, ICFEM 2012, volume 7635 of Lecture Notes in Computer Science, pages 54-70. Springer, Berlin, Germany, 2012. [электронный ресурс], http://code.ulb.ac.be/dbfiles/GjoLorPug-etal2012icfem.pdf, режим доступа свободный.
5. Higgins F., Tomlinson A., Martin K. M., Survey on security challenges for swarm robotics, in Proceedings of the 5th International Conference on Autonomic and Autonomous Systems (ICAS '09), pp. 307–312, IEEE Computer Society, Los Alamitos, CA, USA, April 2009.
6. Knowledge Driven Planning and Modeling. NIST Laboratory. [электронный ресурс], http://www.nist.gov/el/isd/ps/knowdrivenplanmodel.cfm, режим доступа свободный.
7. Kolling A., Nunnally S., Lewis M. Towards Human Control of Robot Swarms (2012). [электронный ресурс], http://faculty.cs.byu.edu/~mike/mikeg/papers/MOSC/LewisIros11swarm.pdf), режим доступа свободный.
8. Navarro I., Matía F. An Introduction to Swarm Robotics. ETSI Industriales, Universidad Politécnica de Madrid, c/José Gutiérrez Abascal, 2, 28006 Madrid, SpainReceived 18 April 2012; Accepted 19 June 2012 [электронный ресурс], http://www.hindawi.com/isrn/robotics/2013/608164/, режим доступа свободный.
9. Станкевич Л.А. Нейрологические средства систем управления интеллектуальных роботов. Научная сессия МИФИ-2004. VI Всероссийская НТК «Нейроинформатика-2004»: Лекции по нейроинформатике, ч. 2. М.: МИФИ, 2004. С. 57-110.
10. Станкевич Л.А. Адаптивные поведенческие системы на нейрологических сетях. 11-я Национальная конференция по искусственному интеллекту с международным участием (КИИ-08), 29.09-3.10.2008, Дубна. 7 с.
11. Юревич Е.И. Основы робототехники. 2-е изд., перераб. и доп. СПб.: БХВ-Петербург, 2005. 416 с.
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(14). С. 42-48
13. Комаров И.И., Юрьева Р.А., Дранник А.Л., Масленников О.С. Постановка задачи обеспечения информационной безопасности роевых робототехнических систем // Наука и бизнес: пути развития. 2015..№ 3(45). С. 66-72.

References:

1. Kalyaev I.A., Gaiduk A.R., Kapustyan S.G. Modeli i algoritmy kollektivnogo upravleniya v gruppakh robotov. M.: FIZMATLIT, 2009. 280 s.
2. Couzin, I.D., Krause, J., Franks, N.R. & Levin, S.A. Effective leadership and decision making in animal groups on the move. Nature 433, 513-516, 2005
3. Rubenstein M., Hoff N., Nagpal R. Kilobot: A Low Cost Scalable Robot System for Collective Behaviors. Computer Science Group Harvard University Cambridge, Massachusetts URL: ftp://ftp.deas.harvard.edu/techreports/tr-06-11.pdf (rezhim dostupa: otkrytyi; data obrashcheniya: 13.02.2014).

DOI: 10.7256/2305-6061.2016.4.21128

4. Gjondrekaj E., Loreti M., Pugliese R., Tiezzi F., Pinciroli C., Brambilla M., Birattari M., Dorigo M. Towards a Formal Verification Methodology for Collective Robotic Systems. In Formal Methods and Software Engineering, Proceedings of the 14th International Conference on Formal Engineering Methods, ICFEM 2012, volume 7635 of Lecture Notes in Computer Science, pages 54-70. Springer, Berlin, Germany, 2012. [elektronnyi resurs], http://code.ulb.ac.be/dbfiles/GjoLorPug-etal2012icfem.pdf, rezhim dostupa svobodnyi.
5. Higgins F., Tomlinson A., Martin K. M., Survey on security challenges for swarm robotics, in Proceedings of the 5th International Conference on Autonomic and Autonomous Systems (ICAS'09), pp. 307–312, IEEE Computer Society, Los Alamitos, CA, USA, April 2009.
6. Knowledge Driven Planning and Modeling. NIST Laboratory. [elektronnyi resurs], http://www.nist.gov/el/isd/ps/knowdrivenplanmodel.cfm, rezhim dostupa svobodnyi.
7. Kolling A., Nunnally S., Lewis M. Towards Human Control of Robot Swarms (2012). [elektronnyi resurs], http://faculty.cs.byu.edu/~mike/mikeg/papers/MOSC/LewisIros11swarm.pdf), rezhim dostupa svobodnyi.
8. Navarro I., Matía F. An Introduction to Swarm Robotics. ETSI Industriales, Universidad Politécnica de Madrid, c/ José Gutiérrez Abascal, 2, 28006 Madrid, SpainReceived 18 April 2012; Accepted 19 June 2012 [elektronnyi resurs], http://www.hindawi.com/isrn/robotics/2013/608164/, rezhim dostupa svobodnyi.
9. Stankevich L.A. Neirologicheskie sredstva sistem upravleniya intellektual'nykh robotov. Nauchnaya sessiya MIFI-2004. VI Vserossiiskaya NTK «Neiroinformatika-2004»: Lektsii po neiroinformatike, ch. 2. M.: MIFI, 2004. S. 57-110.
10. Stankevich L.A. Adaptivnye povedencheskie sistemy na neirologicheskikh setyakh. 11-ya Natsional'naya konferentsiya po iskusstvennomu intellektu s mezhdunarodnym uchastiem (KII-08), 29.09-3.10.2008, Dubna. 7 s.
11. Yurevich E.I. Osnovy robototekhniki. 2-e izd., pererab. i dop. SPb.: BKhV-Peterburg, 2005. 416 s.
12. Yur'eva R.A., Komarov I.I., Dorodnikov N.A. Postroenie modeli narushitelya informatsionnoi bezopasnosti dlya mul'tiagentnoi robototekhnicheskoi sistemy s detsentralizovannym upravleniem // Programmnye sistemy i vychislitel'nye metody. 2016. № 1(14). S. 42-48.
13. Komarov I.I., Yur'eva R.A., Drannik A.L., Maslennikov O.S. Postanovka zadachi obespecheniya informatsionnoi bezopasnosti roevykh robototekhnicheskikh sistem // Nauka i biznes: puti razvitiya. 2015..№ 3(45). S. 66-72.

DOI: 10.7256/2305-6061.2016.4.21128