3 АВТОМАТИЧЕСКОЕ УПРАВЛЕНИЕ И РОБОТОТЕХНИКА
AUTOMATIC CONTROL AND ROBOTICS

УДК 004.056

ПОСТРОЕНИЕ МОДЕЛИ ДОВЕРИЯ И РЕПУТАЦИИ К ОБЪЕКТАМ МУЛЬТИАГЕНТНЫХ РОБОТОТЕХНИЧЕСКИХ СИСТЕМ С ДЕЦЕНТРАЛИЗОВАННЫМ УПРАВЛЕНИЕМ

И.А. Зикратов[a], Т.В. Зикратова[b], И.С. Лебедев[a], А.В. Гуртов[c, d]

[a] Университет ИТМО, Санкт-Петербург, Россия,zikratov@cit.itmo.ru

[b] Военный институт (военно-морской политехнический) ВУНЦ ВМФ «Военно-морская академия», г. Пушкин, Санкт-Петербург, Россия, ztv64@mail.ru

[c] Хельсинский институт информационных технологий, Хельсинки, Финляндия

[d] Аалто Университет, Аалто, Финляндия, mailto:gurtov@hiit.fi

Рассматривается проблема построения механизмов защиты мультиагентных робототехнических систем от атак со стороны роботов-диверсантов. Проведен анализ функционирования таких систем с децентрализованным управлением. Рассмотрен класс так называемых мягких атак, использующих перехват сообщений, формирование и передачу коллективу роботов дезинформации, а также осуществляющих иные действия, которые не имеют идентифицируемых признаков вторжения роботов-диверсантов. Проведен анализ существующих моделей информационной безопасности мультиагентных информационных систем, основанных на вычислении уровня доверия в процессе взаимодействия агентов. Предложена модель информационной безопасности, в которой роботы-агенты вырабатывают уровни доверия друг к другу на основе анализа ситуации, складывающейся на *k*-м шаге итерационного алгоритма, с использованием бортовых сенсорных устройств. На основе вычисленных уровней доверия осуществляется распознавание объектов категории «диверсант» в коллективе легитимных роботов-агентов. Для увеличения меры сходства (близости) объектов, относящихся к одной категории («диверсант» или «легитимный агент») предложен алгоритм вычисления репутации агентов как меры сформировавшегося во времени общественного мнения о качествах того или иного агента-субъекта. Рассмотрены варианты реализации алгоритмов выявления диверсантов на примере базового алгоритма распределения целей в коллективе роботов.

Ключевые слова: информационная безопасность, коллектив роботов, мультиагентные робототехнические системы, атака, уязвимость, модель информационной безопасности**.**

TRUST AND REPUTATION MODEL DESIGN FOR OBJECTS OF MULTI-AGENT ROBOTICS SYSTEMS WITH DECENTRALIZED CONTROL

I.A. Zikratov[a], T.V. Zikratova[b], I.S. Lebedev[a], A.V. Gurtov[c, d]

[a] ITMO University, Saint Petersburg, Russia, zikratov@cit.itmo.ru

[b] Military Institute (Naval Polytechnic) Military Educational and Scientific Center of the Navy "Naval Academy", Pushkin, Saint Petersburg, Russia, ztv64@mail.ru

[c] Helsinki Institute for Information Technology HIIT, Helsinki, Finland

[d] Aalto University, Aalto, Finland, mailto:gurtov@hiit.fi

The problem of mechanisms design for protection of multi-agent robotics systems from attacks of robots-saboteurs is considered. Functioning analysis of these systems with decentralized control is carried out. The type of the so-called soft attacks using interception of messages, misinformation formation and transmission to group of robots which are also realizing other actions without identified signs of invasion of robots-saboteurs. Analysis of existing information security models of the system based on the trust level computation, calculated in the process of agents' interaction is carried out. Information security model is offered in which robots-agents produce the trust levels to each other on the basis of situation analysis emerging on a certain step of iterative algorithm with usage of onboard sensor devices. On the basis of calculated trust levels, recognition of "saboteur" objects in the group of legitimate robots-agents is done. For measure of likeness (adjacency) increase for objects from the same category ("saboteur" or "legitimate agent"), calculation algorithm for agents reputation is offered as a measure of public opinion about qualities of this or that agent-subject. Implementation alternatives of the algorithms for detection of saboteurs on the example of the basic algorithm for distribution of purposes in the group of robots are considered.

Keywords: information security, group of robots, multi-agent robotics systems, attack, vulnerability, information security model (IT security model).

Введение

Возрастающий интерес к групповой робототехнике приводит к необходимости разработки механизмов обеспечения информационной безопасности (ИБ) мультиагентных робототехнических систем (МРТС). Децентрализация управления, пространственная удаленность агентов, непредсказуемая динамика внешней среды, вплоть до сознательного противодействия, делают мультиагентную среду максимально уязвимой для угроз, основанных на физическом внедрении «инородных» роботов (роботов-диверсантов), задачей которых является недопущение или снижение эффективности действий коллектива роботов [1, 2].

В мультиагентных компьютерных системах (МАС) для предотвращения деструктивных воздействий путем обеспечения подлинности и доверия доступа используются механизмы «жесткой» безопасности, такие как: шифрование канала связи, схемы криптографической аутентификации и авторизации, политики для предоставления полномочий. К числу таких методов можно отнести метод защищенных состояний агентов [3], методы мобильной криптографии [4]. Эти традиционные методы обеспечения безопасности не будут рассматриваться нами далее.

В данной работе рассмотрены механизмы «мягкой» безопасности. Роботы-диверсанты противоборствующей стороны могут предоставлять ложную или вводящую в заблуждение информацию, и традиционные механизмы обеспечения безопасности не могут защитить пользователей от этого вида угроз. Для защиты МАС от подобных скрытых атак могут использоваться метод Ксюдонга [5], «товарищеская» модель безопасности (Buddy Security Model, BSM) [6, 7], которые хорошо согласуется с принципами построения децентрализованных систем. Кроме того, для обеспечения защиты пользователя от таких угроз используют механизмы социального контроля, а именно системы доверия и репутации. Эти механизмы основаны на расчете величины доверия агентов друг к другу, осуществляемой в процессе мониторинга действий агента в системе [8–13]. Различие в подходах к вычислению уровня доверия обусловлено, как правило, особенностями среды, в которой происходит взаимодействие участников. Это могут быть электронные рынки, пиринговые сети, онлайновые социальные сети и т.п. Как следствие, в существующих моделях доверия имеются различные трактовки понятий доверия и репутации, рассматриваются различные субъекты и объекты доверия.

Целью настоящей работы является разработка модели защиты МРТС, основанной на вычислении меры доверия и репутации роботов-агентов в коллективе роботов при децентрализованном управлении.

Функционирование МРТС с децентрализованным планированием действий

Роботы-агенты МРТС, в отличие от агентов МАС, оснащены бортовым сенсорно-измерительным устройством (СУ), от которого робот получает информацию об окружающей среде, а также каналом радиосвязи, предназначенным для обмена информацией в процессе выполнения задачи. Рассмотрим действия МРТС при использовании наиболее распространенной итерационной процедуры оптимизации коллективного решения – распределения целей в группе роботов [14]. Функционирование МРТС в самом общем виде выглядит следующим образом. Пусть имеется M целей и коллектив из N роботов R_j ($j = \overline{1,N}$). На каждую цель должен быть выделен некоторый, заранее известный наряд сил (число роботов, необходимых для выполнения задачи). После того, как какую-нибудь цель выберет необходимое число роботов, она считается обеспеченной. Оставшиеся роботы образуют резервный кластер. Роботу-агенту известны координаты целей, свои координаты и потребный наряд сил для каждой цели. Робот R_j оценивает эффективность своих действий по каждой цели и сообщает массив своих оценок $D_j = [d_{j1},\ d_{j2},\ \ldots,\ d_{jM}]$ остальным членам коллектива. В процессорном устройстве (ПУ) каждого робота формируется матрица **D**, размерностью (N, M), элементами которой являются d_{jl} – оценки эффективности j-го робота для l-й цели. После формирования матрицы **D** начинаются итерационные процедуры формирования коллективного плана, в результате которой для каждой цели $T_l \in \mathbf{T}_c$ обеспечивается максимум функционала

$$\mathbf{Y}_c = \sum_{j,l=1}^{N} d_{jl} n_{jl} \to \max, \qquad (1)$$

при ограничениях

$$\sum_{l=1}^{N} n_{jl} = 1,$$

$$\sum_{j=1}^{N} n_{jl} = n_l^{\max},$$

$$d_{jl} \geq 0,$$

где

$$n_{jl} = \begin{cases} 1, & \text{если } j-\text{й робот выбрал } l-\text{ю цель}, \\ 0, & \text{в противном случае.} \end{cases}$$

Здесь $j = \overline{1,N},\ l = \overline{1,N}$, а $n_l^{\max}$ – необходимое количество роботов, которые должны выбрать l-ю цель.

В основу итерационных процедур положен анализ каждым роботом-агентом массива оценок эффективности и выбора «своей» цели, для которой значение оценки «эффективность» максимально. Затем происходит обмен информацией о выбранных решениях, анализ и «обсуждение» решений, принятых другими роботами, выбор для l-ой цели агента с максимальным значением d_l, «вычеркивание» из матрицы **D** обеспеченных целей и роботов, выбравших цель в соответствии с функционалом (1). Так как в ПУ всех роботов имеются одинаковые матрицы **D**, то и результаты вычислений будут совпадать. Процедура повторяется до тех пор, пока не будут обеспечены все цели множества M. Существуют модификации

этого алгоритма, позволяющие учитывать не только оценки d_{jl}, но и возможные изменения целевого функционала, если робот R_j откажется от выбранной в текущем итерационном цикле цели и выберет другую цель. Ряд модификаций алгоритмов позволяет также рационально разрешить ситуацию, когда имеется несколько агентов с одинаковой эффективностью по одной цели.

Пусть группе из семи роботов (N=7) необходимо распределить две цели (M=2). Известно, что каждая цель должна быть обеспечена двумя агентами. Показателем эффективности цели будем считать расстояние от робота до нее. Таким образом, чем ближе робот расположен к цели, тем выше ее эффективность. Пусть матрица **D** оценок эффективности имеет следующий вид:

	A	B
D_1	3,2	1,0
D_2	1,9	2,5
D_3	0,7	5,4
D_4	3,6	3,5
D_5	5,8	3,4
D_6	4,2	5,6
D_7	5,8	1,4

В результате работы алгоритма цель А будет обеспечена агентами R_2 и R_3, а цель В – агентами R_1 и R_7. Очевидно, что деструктивные информационные воздействия внедренных роботов-диверсантов могут заключаться в передаче членам коллектива ложного вектора оценок (предоставление членам коллектива завышенных или заниженных показателей эффективности), в нарушении правил, принятых при «обсуждении» решений (необоснованные заявления о выборе целей и т.д.). Последствиями проведения таких атак может являться недостижение максимума функционалом (1), и (или) появление фактически необеспеченных целей – когда в составе наряда сил, предназначенных для цели, имеются диверсанты, которые не будут выполнять требующихся от легитимного агента действий в отношении цели. Например, если окажется, что робот R_5 является диверсантом, то он может осуществить «мягкое» воздействие, которое заключается в предоставлении неверной информации о расстоянии до цели А:

D_1	3,2	1,0
D_2	1,9	2,5
D_3	0,7	5,4
D_4	3,6	3,5
D_5	**0,8**	3,4
D_6	4,2	5,6
D_7	5,8	1,4

В результате этой атаки на цель А будут назначены роботы R_5 и R_3, и цель А не будет обеспечена потребным количеством легитимных агентов.

Таким образом, опасность «мягких» атак состоит в том, что, в отличие от «жестких» атак, МРТС не обнаруживает деструктивные воздействия, так как роботы, их системы и каналы связи функционируют в штатном режиме. Коллектив роботов «думает», что цель, стоящая перед ним, достигнута, так как формально все критерии принятия решения выполнены. Предлагаемая в работе модель информационной безопасности для МРТС на основе вычисления репутации и доверия предназначена для обнаружения и нейтрализации роботов-диверсантов, осуществляющих подобные атаки.

Модель ИБ для МРТС на основе вычисления репутации и доверия

Идея, положенная в основу модели, состоит в следующем [15].

После запуска итерационного цикла j-й робот (робот-объект доверия) ($j = \overline{1,N}$), имеющий текущее состояние S_j^0, получает в активной фазе текущей итерации в свое распоряжение канал связи и доступ к ПУ роботов – членов своего коллектива. На основании имеющейся у него информации о состояниях $S_1^0, S_2^0, \ldots, S_{j-1}^0, S_{j+1}^0, \ldots, S_N^0$ и текущих действиях $A_1^{k+1}, A_2^{k+1}, \ldots, A_{j-1}^{k+1}, A_{j+1}^k, \ldots, A_N^k$ объект вырабатывает действие A_j^{k+1}, при котором значение ΔY максимально, и осуществляет доступ на запись w информации о A_j^{k+1} в ПУ роботов-субъектов. Остальные роботы-агенты (субъекты доверия), получив эту информацию, проверяют полученную информацию на предмет соответствия действительности, а также «полезность» выбранного роботом-объектом действия с точки зрения приращения целевого функционала ΔY.

Если i-й робот (робот-субъект) ($i \neq j$) в результате проверки получил положительное заключение, он подает положительный голос за j-й робота-объекта и сообщает об этом остальным субъектам. Каждый субъект, получив сведения о результатах проверки объекта другими субъектами, подсчитывает количество положительных и отрицательных голосов, поданных за него, вычисляя доверие j-го объекта.

Определение 1. *Под доверием в данном случае понимается мера, характеризующая готовностью субъекта взаимодействовать в данной ситуации с объектом*. В соответствии с принятой в коллективе политикой безопасности возможно блокирование или игнорирование роботов-агентов, доверие к которым

меньше некоторого заданного порогового значения. Таким образом, низкий уровень доверия не позволит диверсанту оказывать деструктивное воздействие на принятие решения агентами. Из этого следует, что действия диверсанта по повышению доверия предполагают участие робота в достижении цели МРТС, что, в свою очередь, противоречит логике его использования с точки зрения противника.

Однако в МРТС возможно внедрение групп диверсантов, которые оценивают друг друга высоко, а других членов коллектива – низко. Последствием таких действий может быть дискредитация легитимных агентов [16]. Для решения этой проблемы целесообразно использовать в механизме ИБ понятие *репутации.*

Определение 2. *Под репутацией будем понимать сформировавшееся во времени общественное мнение о качествах того или иного агента-субъекта.* Тогда при подсчете положительных и отрицательных голосов, поданных за объект, будет учитываться репутация голосующих субъектов путем взвешенного суммирования их оценок. В этом случае влияние агентов с низкой репутацией на процесс вычисления доверия к объекту будет меньшим, чем субъектов с высокой репутацией. Отметим, что значение репутации зависит от истории взаимодействия агента в коллективе и от времени пребывания в нем.

Таким образом, понятия доверия и репутации в мультиагентных системах фактически используются для распознавания в коллективе роботов внедренных злоумышленником роботов-диверсантов. Тогда для решения задачи распознавания объектов вводимые понятия (признаки) доверия и репутации должны обеспечить, с одной стороны, наибольшую похожесть объектов в пределах группы (кластера) и, с другой стороны – наибольшее расстояние между группами (кластерами). В простейшем случае будем говорить о двух кластерах: «легитимные агенты» и «роботы-диверсанты».

Реализация модели ИБ на основе вычисления уровня доверия

Покажем реализацию модели на примере рассмотренной выше задачи распределения целей в группе роботов.

Алгоритм 1.

Пусть в группу роботов, представленную на рис. 1, внедрены два диверсанта – роботы №№ 5 и 8, целью которых является – не допустить обеспечение целей нарядом сил.

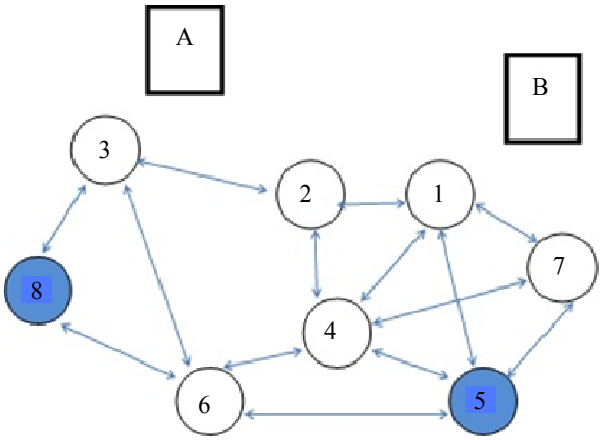

Рис. 1. Задача распределения целей при наличии диверсантов

На рис. 1 показано взаимное расположение роботов и целей, а также стрелками обозначены межагентные связи, осуществляемые посредством бортовых сенсорно-измерительных устройств (например, визуальная связь). В качестве ограничения задачи полагаем, что все агенты имеют доступ к каналу радиосвязи для обмена информацией.

Шаг 1. Каждый робот-агент сформировал вектор оценок эффективности и сообщил свои оценки всем членам коллектива. Роботами-диверсантами проведена атака, которая заключается в дезинформации агентов относительно своего расстояния до цели: $D_5 = [\mathbf{0,8}\quad 3{,}4]$, $D_8 = [3{,}1\quad \mathbf{0,2}]$. Сформирована матрица оценок эффективности **D** которая имеет вид

D_1	3,2	1,0
D_2	1,9	2,5
D_3	0,7	5,4
D_4	3,6	3,5
D_5	**0,8**	3,4
D_6	4,2	5,6
D_7	5,8	1,4
D_8	3,1	**0,2**

Начиная со второго шага, выполняются мероприятия ИБ, направленные на выявление деструктивных воздействий.

Шаг 2. Агенты при помощи бортовых сенсорно-измерительных устройств выполняют проверку данных массива **D**. Результаты проверки j-й робот записывает в массив оценок $V_j = [v_{j1},\ v_{j2},\ \cdots,\ v_{jM}]$ и сообщает его членам коллектива. Здесь $v_{ji} = -1$, если информация, переданная i-м роботом, не подтверждается данными СУ j-го робота; $v_{ji} = 1$ в противном случае. Если i-й робот не наблюдает j-го робота посредством СУ, то $v_{ji} = 0$. Например, для ситуации, представленной на рис. 1, робот R_1 составит следующий массив: $V_1 = [1,1,0,1,-1,0,1,0]$. Так как робот-диверсант R_5 находится в зоне действия бортового сенсорно-измерительного блока, то R_1 обнаружил, что R_5 находится от цели А на удалении, превышающем указанную в массиве D_5 величину. Агенты R_3, R_6 и R_8 находятся вне зоны действия СУ R_1, что обусловило появление нулей на соответствующих позициях массива. Следует обратить внимание, что диверсанты R_5 и R_8 могут действовать согласованно. В этом случае они могут осуществлять следующие действия:

1. выставлять друг другу оценки «1», подтверждающие достоверность переданных сведений, даже в случае, когда они не находятся в зоне действия своих СУ;
2. с целью дискредитации остальных членов коллектива выставлять им оценки «-1» в случае наблюдения их СУ.

Таким образом, в результате выполнения шага 2 в ПУ каждого робота формируется массив **V**, который для рассматриваемого примера представлен в табл. 1.

	1	2	3	4	5	6	7	8
1	1	1	0	1	–1	0	1	0
2	1	1	1	1	0	0	0	0
3	0	1	1	0	0	1	0	–1
4	1	1	0	1	–1	1	1	0
5	–1	0	0	–1	1	–1	–1	**1**
6	0	0	1	1	–1	1	0	–1
7	1	0	0	1	–1	0	1	0
8	0	0	–1	0	**1**	–1	0	1

Таблица 1. Массив оценок действий членов коллектива

Как видно из табл. 1, i-й столбец представляет собой совокупность оценок всех членов коллектива i-го агента, величина доверия к которому w_i в простейшем случае может рассчитываться как отношение числа положительных голосов γ^+ к общему количеству голосов $\gamma = \gamma^+ + \gamma^-$ [8]:

$$w_i = \frac{\gamma^+}{\gamma^+ + \gamma^-}\ . \qquad (2)$$

Для рассматриваемого примера уровни доверия агентов будут иметь следующие значения: $\mathbf{W} = [0{,}8;\ 1{,}0;\ 0{,}75;\ 0{,}83;\ 0{,}33;\ 0{,}6;\ 0{,}75;\ 0{,}33]$.

Шаг 3. На заключительном шаге осуществляется обработка результатов вычисления уровня доверия агентов. Следует отметить, что конечной целью вычисления уровня доверия агентов является принятие решения – относится агент к легитимным членам коллектива либо к диверсантам. Иначе говоря, шаг 3 можно рассматривать как двухклассовую задачу распознавания образов, которая в простейшем случае может заключаться в выборе значения порога w^p, ниже которого агенты считаются недостаточно доверенными и исключаются из работы алгоритма. В нашем случае, если принять $w^p = 0{,}5$, то матрица оценок эффективности **D** в ПУ каждого агента примет следующий вид:

D_1	3,2	1,0
D_2	1,9	2,5
D_3	0,7	5,4
D_4	3,6	3,5
D_6	4,2	5,6
D_7	5,8	1,4

Дальнейшие шаги алгоритма распределения целей не отличаются от известных [14].

Анализ этого алгоритма показывает, что ему присущи следующие уязвимости:

1. уровень доверия зависит от соотношения в зоне действия СУ роботов-диверсантов и легитимных агентов;
2. уровень доверия не зависит от предыстории взаимодействия агентов в МРТС.

Следовательно, возможно проведение организованной атаки роботов-диверсантов при формировании ими простого большинства на локальном участке действий, когда легитимные агенты будут дискредитированы путем выставления им отрицательных голосов, при положительном оценивании диверсантами самих себя. Для устранения этой угрозы предлагается дополнить существующий алгоритм введения меры репутации агента.

Алгоритм 2.

Первый и второй шаг совпадают с шагами 1 и 2 алгоритма 1.

Шаг 3. Вычисление репутации агентов.

Если на шаге 2 агенты оценили действия тех объектов, которые оказались в зоне действия их бортовых СУ, т.е. непосредственные взаимодействия агентов, то действия на шаге 3 можно расценивать как анализ взаимодействия агентов с остальными членами коллектива.

Рассмотрим массив оценок **V** (табл. 1). Анализ таблицы показывает, что существуют объекты оценки, которые наблюдаются СУ нескольких роботов. Тогда, если оценка *i*-го робота в отношении действий *k*-го объекта совпадает с оценкой, выставленной *j*-го роботом в отношении того же действия *k*-го объекта, то это будет являться основанием повышения уровня репутации; в противном случае – уменьшения. Относительно рассматриваемого примера анализ табл. 1 показывает, что взаимодействия робот № 1 и робота № 2 можно оценить следующим образом:

1. значение увеличивается на «1», так как робот № 1 и робот № 2 находятся в зоне действия своих бортовых СУ и выставили друг другу положительные оценки;
2. значение увеличивается на «1», так как робот № 1 и робот № 2 наблюдали своими СУ действия робота № 4, и их оценки его действий совпали;
3. итоговая оценка действий робота № 2, полученная при взаимодействии с роботом № 1, и робота № 1, при взаимодействии с роботом № 2, равна 2.

Оценка действий, рассчитанная по аналогии при анализе взаимодействия робота № 3 и робота № 1, будет равна 1, так как, не наблюдая друг друга, эти агенты вместе наблюдали действия робота № 2, и их оценки его действий совпали. Проведя подобный анализ массива **V**, каждый робот формирует в своем ПУ массив оценок действий агентов **S** (табл. 2).

	1	2	3	4	5	6	7	8
1		2	1	4	–3	2	3	–1
2	2		1	2	–2	2	2	–2
3	1	1		2	–1	2	0	–2
4	4	2	2		–4	2	3	–1
5	–3	–2	–1	–4		–2	–3	1
6	2	2	2	2	–2		2	–2
7	3	2	0	3	–3	2		0
8	–1	–2	–2	–1	2	–2	0	

Таблица 2. Массив оценок действий агентов **S**

Отсюда можно вычислить уровень репутации каждого агента q_j как результат отношения к нему всех членов коллектива как в процессе их непосредственного взаимодействия и при взаимодействии с соседями. Здесь q_i может рассчитываться как отношение числа положительных голосов s^+ к общему количеству голосов $s = s^+ + s^-$:

$$q_i = \frac{s^+}{s^+ - s^-} \ . \qquad (3)$$

Например, из табл. 2: $q_1 = \frac{12}{12+4} = 0{,}75$. Массив значений репутаций всех агентов, вычисленный по формуле (3) будет равен

$\mathbf{Q} = [0{,}75;\ 0{,}69;\ 0{,}66;\ 0{,}72;\ 012;\ 0{,}77;\ 0{,}11]$.

На рис. 2 приведены графики нормированных значений векторов **W** и **Q.** Из рис. 2 видно, что разброс положительных оценок репутации существенно меньше разброса значений положительных оценок уровня доверия:

$$\sigma^2_{\mathbf{Q}} = 0{,}003, \sigma^2_{\mathbf{W}} = 0{,}038,$$

где $\sigma^2_{\mathbf{Q}}$ и $\sigma^2_{\mathbf{W}}$ – дисперсии векторов **Q** и **W** соответственно.

Шаг 4. Учет изменения уровня репутации с течением времени.

Можно заметить, что значения вектора **Q** нельзя полагать соответствующим понятию репутации, данным в определении 2, так как компоненты вектора учитывают «мнение» коллектива об объектах, сформировавшееся в результате анализа только одной ситуации. Для учета фактора времени в работах [11, 17] предлагается использовать монотонно возрастающие функции времени. Известно, что функцию и плотность распределения случайной величины, характеризующей длительность функционирования сложной системы, предприятия, живого существа и т.д. можно описывать функцией Вейбулла–Гнеденко, которая имеет вид

$$F(t) = 1 - e^{-at^k}, \quad (4)$$

где a определяет масштаб, а k – вид плотности распределения. Так, при постоянной интенсивности итерационных процедур в алгоритме распределения целей можно положить $k = 1$. Например, если в качестве параметра времени положить номер итерации, то вид функции времени будет иметь вид рис. 3.

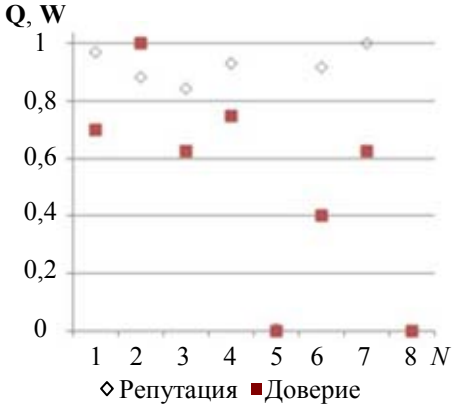

Рис. 2. Нормированные значения уровней доверия и репутации *N* агентов

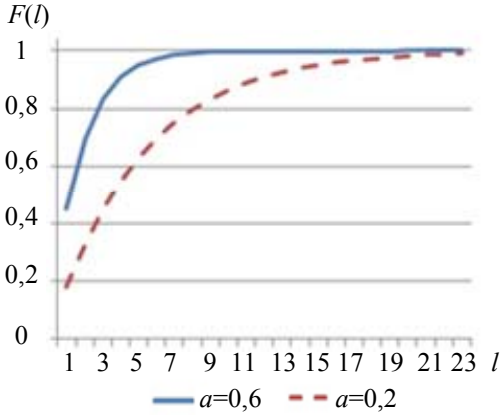

Рис. 3. Влияние параметра *a* на уровень репутации с увеличением числа итераций

Из рис. 3 видно, что, устанавливая в соответствии с политикой безопасности, принятой в системе, величину параметра a, можно контролировать рост скорости репутации объекта.

Таким образом, скалярное умножение вектора **Q** на величину $F(l)$, где l – номер текущей итерации алгоритма распределения целей, позволит контролировать влияние новичков с малым уровнем репутации на процесс оценивания уровня доверия агентов в текущей ситуации.

Шаг 5. С учетом вышеизложенного формула для расчета уровня доверия (2) окончательно примет следующий вид:

$$w_i = \frac{p_i}{p_i + n_i}, \quad (5)$$

$$p_i = \sum_{j=0}^{N} h_{ij} \cdot q_j \cdot F(l),$$

$$n_i = \sum_{j=0}^{N} g_{ij} \cdot q_j \cdot F(l).$$

Здесь: q_i – уровень репутации i-го агента, вычисленный по формуле (3) из табл. 2, значения h_{ij} и g_{ij} определяются из анализа оценок v_{ij} массива **V**:

$$h_{ij} = \begin{cases} 1, & \text{если } j-\text{й робот положительно оценил действия } i-\text{го робота,} \\ 0, & \text{в противном случае.} \end{cases}$$

$$g_{ij} = \begin{cases} 1, & \text{если } j-\text{й робот отрицательно оценил действия } i-\text{го робота,} \\ 0, & \text{в противном случае.} \end{cases}$$

Тогда для рассматриваемого примера окончательно получим значения компонентов вектора уровня доверия $\mathbf{W} = [0{,}96;\ 1{,}0;\ 0{,}94;\ 0{,}97;\ 0{,}071;\ 0{,}9;\ 0{,}95;\ 0{,}08]$ (рис. 4).

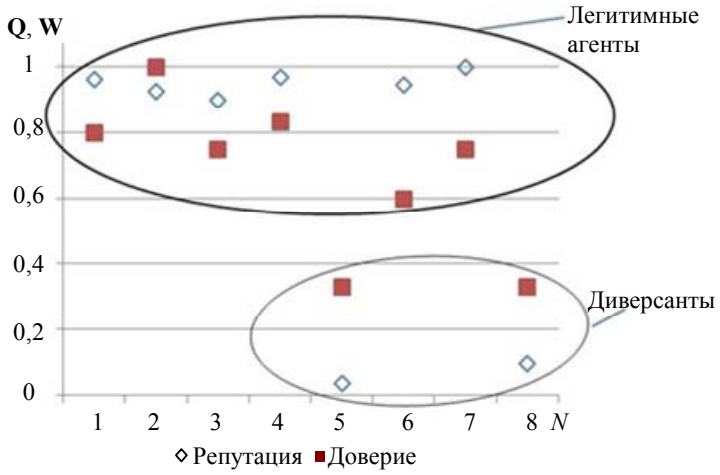

Рис. 4. Сравнение результатов работы алгоритмов 1 и 2

Из рис. 4 и расчетов видно, что при использовании формул (4) и (5) объекты кластера X_{la} – «легитимные агенты», к которым относятся роботы №№ 1–4, 6 и 7, находятся на большем межкластерном расстоянии от роботов кластера X_d – «диверсанты» (№№ 5 и 8), нежели при использовании алгоритма 1:

$$\left|X^1_{цla} - X^1_{цd}\right| = 0{,}45 < \left|X^2_{цla} - X^2_{цd}\right| = 0{,}88,$$

где $X^i_{цla}$ и $X^i_{цd}$ – центры кластеров, вычисляемые как $X_{ц} = \sum w_i / n$ с использованием формулы (2) или формул (4)–(5). В результате выполнения шага 5 происходит выявление диверсантов по принятому в системе критерию распознавания, и дальнейшие шаги направлены на выполнение базового алгоритма распределения целей.

Можно показать, что предлагаемые модели работоспособны при появлении новых агентов, появлении коллектива диверсантов, действующих в сговоре, и в других ситуациях, типовых для МРТС.

Очевидно, что более высокое качество распознавания агентов, совершающих деструктивные информационные воздействия, присущее алгоритму 2, сопровождается возрастающим объемом вычислительных ресурсов. Так, если при работе штатного алгоритма в ПУ агента необходимо сформировать матрицу оценок эффективности **D** размерностью (*N*, *M*), то при использовании алгоритма 1 необходимо дополнительно к этому формирование массива оценок действий членов коллектива **V** размерностью (*N*, *N*), а при использовании алгоритма 2 – еще и массив оценок уровня репутации **S** такой же размерности.

Заключение

Разработанная модель представляет собой модель информационной безопасности мультиагентных робототехнических систем, в которой разграничение доступа агентов к коллективу осуществляется на основе показателя уровня доверия *w* по отношению друг к другу, вырабатываемому членами коллектива при анализе ситуации, сложившейся на *l*-м шаге итерационного процесса, с учетом предыдущей истории их взаимодействия. При этом члены коллектива, впервые попавшие в область действия бортового сенсорного устройства робота-агента, обладают минимальной репутацией. Для повышения уровня доверия агенту необходимо выполнять не только рациональные (с точки зрения других членов коллектива) действия, но и функции по обеспечению информационной безопасности. Авторами предложены способы вычисления метрик доверия и репутаций применительно к функционированию типового алгоритма мультиагентной робототехнической системы.

Разработанный подход позволяет обеспечить более высокое качество распознавания образов за счет минимизации дисперсии параметров объектов одного класса (кластера) и увеличению межклассового (межкластерного) расстояния.

Литература

1. Higgins F., Tomlinson A., Martin K.M. Threats to the swarm: Security considerations for swarm robotics // International Journal on Advances in Security. 2009. V. 2. N 2&3. P. 288–297.
2. Зикратов И.А., Козлова Е.В., Зикратова Т.В. Анализ уязвимостей робототехнических комплексов с роевым интеллектом // Научно-технический вестник информационных технологий, механики и оптики. 2013. № 5 (87). С. 149–154.
3. Karnik N.M., Tripathi A.R. Security in the Ajanta mobile agent system // Software - Practice and Experience. 2001. V. 31. N 4. P. 301–329.
4. Sander T., Tschudin Ch.F. Protecting mobile agents against malicious hosts // In Giovanni Vigna (ed.) Mobile Agents and Security, LNCS, Springer, 1998. P. 44–60.

5. Xudong G., Yiling Ya., Yinyuan Y. POM-a mobile agent security model against malicious hosts // Proceedings of the 4th International Conference on High Performance Computing in the Asia-Pacific Region. 2000. V. 2. P. 1165–1166.
6. Page J., Zaslavsky A., Indrawan M. A buddy model of security for mobile agent communities operating in pervasive scenarios // Proceedings of 2nd Australasian Information Security Workshop (AISW2004). ACS, Dunedin, New Zealand, 2004. V. 32. P. 17–25.
7. Page J., Zaslavsky A., Indrawan M. Countering security vulnerabilities using a shared security buddy model schema in mobile agent communities // Proc. of the First International Workshop on Safety and Security in Multi-Agent Systems (SASEMAS 2004), 2004. P. 85–101.
8. Schillo M., Funk P., Rovatsos M. Using trust for detecting deceitful agents in artificial societies // Applied Artificial Intelligence. 2000. V. 14. N 8. P. 825–848.
9. Golbeck J., Parsia B., Hendler J. Trust networks on the semantic web // Lecture Notes in Artificial Intelligence (Subseries of Lecture Notes in Computer Science). 2003. V. 2782. P. 238–249.
10. Garcia-Morchon O., Kuptsov D., Gurtov A., Wehrle K. Cooperative security in distributed networks // Computer Communications. 2013. V. 36. N 12. P. 1284–1297.
11. Бешта А.А., Кирпо М.А. Построение модели доверия к объектам автоматизированной информационной системы для предотвращения деструктивных воздействий на систему // Известия Томского политехнического университета. 2013. Т. 322, № 5. С. 104–108.
12. Ramchurn S.D., Huynh D., Jennings N.R. Trust in multi-agent systems // Knowledge Engineering Review. 2004. V. 19. N 1. P. 1–25.
13. Gorodetski V., Kotenko I., Karsaev O. Multi-agent technologies for computer network security: Attack simulation, intrusion detection and intrusion detection learning // Computer systems science and engineering. 2003. N 4. P. 191–200.
14. Каляев И.А., Гайдук А.Р., Капустян С.Г. Модели и алгоритмы коллективного управления в группах роботов. М.: ФИЗМАТЛИТ, 2009. 280 с.
15. Зикратов А.А., Зикратова Т.В., Лебедев И.С. Доверительная модель информационной безопасности мультиагентных робототехнических систем с децентрализованным управлением // Научно-технический вестник информационных технологий, механики и оптики. 2014. № 2(90). С. 47–52.
16. Коваль Е.Н., Лебедев И.С. Общая модель безопасности робототехнических систем // Научно-технический вестник информационных технологий, механики и оптики. 2013. № 4(86). С. 153–154.
17. Carter J., Bitting E., Ghorbani A.A. Reputation formalization for an information-sharing multi-agent system // Computational Intelligence. 2002. V. 18 (2). P. 515-534.

Зикратов Игорь Алексеевич – доктор технических наук, профессор, зав. кафедрой, Университет ИТМО, Санкт-Петербург, Россия, zikratov@cit.itmo.ru

Зикратова Татьяна Викторовна – преподаватель, Военный институт (военно-морской политехнический) ВУНЦ ВМФ «Военно-морская академия», г. Пушкин, Санкт-Петербург, Россия, ztv64@mail.ru

Лебедев Илья Сергеевич – доктор технических наук, доцент, Университет ИТМО, Санкт-Петербург, Россия, lebedev@cit.ifmo.ru

Гуртов Андрей Валерьевич – адъюнкт-профессор, главный научный сотрудник, Хельсинский институт информационных технологий, Хельсинки, Финляндия; Аалто Университет, Аалто, mailto:gurtov@hiit.fi

Igor A. Zikratov – Department head, D.Sc., Professor, ITMO University, Saint Petersburg, Russia, zikratov@cit.itmo.ru

Tatyana V. Zikratova – tutor, Military Institute (Naval Polytechnic) Military Educational and Scientific Center of the Navy "Naval Academy", Pushkin, Saint Petersburg, Russia, ztv64@mail.ru

Ilya S. Lebedev – Associate professor, D.Sc., Associate professor, ITMO University, Saint Petersburg, Russia,lebedev@cit.ifmo.ru

Andrei V. Gurtov – Principal Scientist, Helsinki Institute for Information Technology HIIT, Helsinki, Finland; Adjunct Professor, PhD, Aalto University, Aalto, Finland, mailto:gurtov@hiit.fi

Принято к печати 21.03.14
Accepted 21.03.14