ДОВЕРИТЕЛЬНАЯ МОДЕЛЬ БЕЗОПАСНОСТИ В МУЛЬТИАГЕНТНЫХ СИСТЕМАХ

Н. А. Савицкий, К. В. Козадаев, В. А. Чуйко, Е. И. Козлова

Белорусский государственный университет, Минск, РБ
E-mail: chuykovladislav611@gmail.com

В работе рассматривается доверительная модель в мультиагентных системах и предлагается вариант с накоплением бонусов к изменению репутации. Изменение репутации напрямую зависит от количества и последовательности неправильных сведений.

Ключевые слова: *агент, мультиагентная система, доверительная модель, репутация, угроза.*

МУЛЬТИАГЕНТНЫЕ СИСТЕМЫ

Мультиагентная система (МАС) – это компьютерная среда, состоящая из нескольких взаимодействующих интеллектуальных агентов. МАС предпочтительнее использовать при решении задач, которые являются трудными для отдельного агента.

В последние годы многие исследователи указывают на насущную необходимость включения разработки безопасности проектируемых открытых распределенных информационных систем в этап их проектирования и анализа. К таким системам можно отнести и МАС. Основой информационной безопасности являются конфиденциальность, целостность и доступность [1]. Доверие также является фундаментальной проблемой в крупномасштабных открытых распределенных системах. Оно лежит в основе всех взаимодействий между сущностями, которым приходится действовать в неопределенной и постоянно меняющейся среде. Агенты системы должны понимать, кому из окружения можно доверять и в какой степени.

В теории и практике мультиагентных систем агент определяется как автономная сущность, программная или аппаратно-программная, выполняющая определенные действия и при этом не подверженная влиянию внешнего управления. Агенты могут быть разработаны по принципу «снизу вверх» и способны обрабатывать информацию, обмениваясь ею с другими агентами посредством индивидуального взаимодействия, которое не подвергается контролю «сверху вниз». Это делает необходимым перевод вопроса доверия в системах взаимодействующих сущностей на нижний, собственно, агентный, уровень.

Для минимизации угроз и решения некоторых проблем безопасности в мультиагентной системе представляется необходимым обеспечить следующие требования на уровне агента: безопасность идентификации и

аутентификации агента, безопасность общения между агентами, предотвращение несанкционированного доступа к агентам. Требования на уровне системы: защитить систему от угроз из внешней сети, обеспечить безопасную связь между различными платформами на системном уровне, для защиты основной хост-системы от мобильных агентов обеспечить возможность изоляции части системы в аварийной ситуации. Существует и должна быть устранена и такая угроза, как физическое внедрение в систему извне агентов-«диверсантов» и/или захват ими агентов под свой контроль. Наличие в системе «диверсантов», говорит о том, что «жесткая» безопасность не смогла защитить систему. Это приводит к таким проблемам, как утечка данных, передача фальшивой информации, приводящим к сбою в работе системы. Такой сценарий требует создания слоя «мягкой» безопасности –алгоритмов, которые будут определять потенциальных «диверсантов» и по возможности выводить их из системы до того, как они нанесут значительный урон. Одним из способов обеспечения «мягкой» безопасности является использование механизма доверия [2].

АЛГОРИТМ НАКОПИТЕЛЬНОЙ РЕПУТАЦИИ С ИСПОЛЬЗОВАНИЕМ ДОВЕРИТЕЛЬНОЙ МОДЕЛИ

Доверие – это убеждение агента в том, что другой агент сделает то, что обещает. Высокая степень доверия к агенту будет означать, что он с высокой вероятностью, будет выбран в качестве партнера по взаимодействию. Таким образом, модели доверия направлены на то, чтобы направлять агента при принятии решений о возможности и целесообразности взаимодействия с другими агентами [3].

Предлагаемое решение проблемы доверительного общения состоит в реализации системы агентов, работающих в определенном «поле». Поле разделено на сектора, каждый из которых в свою очередь разделен на подсектора. В поле работают N агентов, из них M – «диверсанты». В пределах одного сектора агенты могут реагировать на запросы других агентов. Агенты, находящиеся в одном секторе, могут слышать действия друг друга, в одном подсекторе – еще и видеть, тем самым имея возможность подтвердить или опровергнуть полученную информацию и изменить репутацию других агентов.

Целью агентов является поиск определенных «точек интереса» (ТИ), которых может быть несколько. Находя такую точку, агенты будут запрашивать о ней других агентов для сбора информации.

Алгоритм определения степени доверия к агенту предлагается следующим:

- Если в координате нет ТИ, агент может перейти в другой подсектор, либо в другой сектор;

• Если агент в своей координате заметил ТИ, он сообщает об этом тем, кто находится рядом. Как описывалось выше, это услышат только агенты, находящиеся в том же секторе.

• Агенты в секторе слышат сообщение и перемещаются в нужный подсектор.

• При (не)нахождении в переданной координате ТИ и оценки совпадения заявленной ценности ТИ, агент соответственно «составляет» репутацию агента-заявителя.

Агенты-«диверсанты» могут решить соврать о позиции, чтобы не дать другим агентам взаимодействовать с ТИ и перехватить информацию себе. Кроме того, агент может случайно передать ошибочную информацию. У агента есть право на ошибку, т. е. если агент передал ошибочную информацию в одном сообщении, а следующие несколько сообщений оказались верными, его репутация вернется в область доверительной.

Рассмотрена работа системы репутации в двух режимах: упрощенном централизованном и распределённом по агентам. Первый концентрирует подсчет в контрольном пункте, тем самым позволяя быстро вывести «диверсантов» из сети. Поскольку мультагентные системы часто работают децентрализовано, второй подход прорабатывает возможность предупреждения других агентов о возможных «диверсантах».

Для оценки продуктивности алгоритма на данном этапе исследований решено оценить процент успешности симуляции относительно числа агентов и «диверсантов» (устанавливаемое число «диверсантов» не входит в число агентов) в упрощенных условиях – число точек интереса – 1, число агентов – от 10 до 15, агентов-«диверсантов» – от 1 до 3.

Централизованный режим: так как агентам позволено ошибаться, симуляция считается успешной, если агенты-«диверсанты» определены первыми. Процент успешности рассчитывался по результатам запуска нескольких симуляций (Таблица 1). Достигнутые результаты показывают, что определение агента-«диверсанта» на ранних стадиях проходит вполне успешно. Отмечено снижение точности при увеличении числа агентов и агентов-«диверсантов». Установлено, что отдельной проблемой является вероятность, что несколько диверсантов донесут лживое сообщение о репутации. Агрегация сообщений помогает это обойти, но только в случае, если верных оценок оказалось больше.

Распределенный режим: так как каждый агент высчитывает репутации самостоятельно, не следует ожидать, что каждый агент определит «диверсанта». За критерий успешности на этот раз примем случай, когда половина агентов примет решение игнорировать «диверсантов» в течении 2-х минут симуляции. Как и в первом опыте, процент успешности работы алгоритма рассчитывался по нескольким симуляциям (Таблица 2).

Таблица 1

Работоспособность централизованного алгоритма

Кол-во агентов	Кол-во диверсантов	Процент успешности
10	1	90%
10	2	85%
10	3	70%
15	1	80%
15	3	70%

Таблица 2

Работоспособность распределительного алгоритма

Кол-во агентов	Кол-во диверсантов	Процент успешности
10	1	90 %
10	2	85 %
15	1	80%
15	3	80%

Результаты показывают, что агенты справляются с задачей определения «диверсантов» в обоих режимах функционирования алгоритма. Предупреждение других агентов позволяет быстро скорректировать работу системы на игнорирование проблемных агентов. Риск отметить ошибавшихся агентов, как «диверсантов», минимизирован путем введения инструмента «прощения», как описано выше.

Представленный подход показал способность справиться с проблемой вычисления «диверсантов» в мультиагентной среде. Изменение репутации в результате постоянного обновления результатов помогает в определении часто врущих/ошибающихся агентов, при этом одиночные ошибки влияют на репутацию незначительно. В ходе дальнейших исследований планируется провести ряд модельных экспериментов по установлению зависимостей корректности работы алгоритма от числа агентов, агентов-«диверсантов», числа непредумышленных ошибок, числа точек интереса и пр. в разных режимах работы.

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ

1. Bishop M. Introduction to Computer Security // Boston: Pearson Education Inc. 2013. 747 p.
2. Jung Y., Kim M., Masoumzadeh A. et al. A survey of security issue in multi-agent systems // Artificial Intelligence Review. 2012. V. 37.3 P. 239-260. DOI: 10.1007/s10462-011-9228-8.
3. Jurca R., Faltings B. Towards incentive-compatible reputation management // In Workshop on Deception, Fraud and Trust in Agent Societies. 2002.