



Рисунок 1 – Взаимодействие подсистем БПЛА

В случае смены роли БПЛА с ведомого на ведущего на блок «Управляющих правил, активируемых контекстом» может резко возрасти нагрузка в зависимости от количества БПЛА в рою и сложности обстановки. Для снижения нагрузки при большом количестве БПЛА ведущий может дать команду на разбиение роя на звенья по три-четыре БПЛА, назначив в каждом из них по ведущему.

Литература

1. Беспилотный летательный аппарат [Электронный ресурс] – Режим доступа: URL: https://bigenc.ru/technology_and_technique/text/4087725 (22.02.2019).
2. Система Touring Machine [Электронный ресурс] – Режим доступа: URL: <https://dl.acm.org/citation.cfm?id=151239> (22.02.2019).
3. Руководство по GUID. Часть 1 [Электронный ресурс]: Режим доступа: <https://blogs.msdn.microsoft.com/ruericlippert/2012/07/31/guid-1> (22.02.2019).

Р.М. Дунин, Д.А. Яковлева

МОДЕЛИ ЗАЩИЩЁННОЙ МУЛЬТИАГЕНТНОЙ СИСТЕМЫ И ИНТЕЛЛЕКТУАЛЬНОГО АГЕНТА

(Тамбовский государственный технический университет)

Аннотация: Многоагентные системы широко применяются в различных сферах. Компрометация хотя бы одного агента может подорвать к ней доверие и привести к значительным финансовым потерям. В статье описана модель защищённой мультиагентной системы и модель интеллектуального агента для такой системы.



Ключевые слова: защищённая мультиагентная система, интеллектуальный агент, конфликт, доверие, репутация.

Abstract: *Multi-agent systems are widely used in various fields. Discrediting at least one agent can undermine its credibility and lead to significant financial losses. The article describes a model of a secure multi-agent system and an intelligent agent model for such a system.*

Keywords: *protected multi-agent system, intelligent agent, conflict, trust, reputation.*

Многоагентные системы нашли широкое применение в различных сферах деятельности: транспорте, логистике, робототехнике, компьютерных играх, фильмах [1] и многих других. Увеличение числа агентов способствует увеличению эффективности принятия решений [2] и сокращению времени промежуточных вычислений. Компрометация или взлом хотя бы одного из них снижает доверие к мультиагентной системе и может способствовать к последующему отказу от неё в пользу другой, что приводит к значительным финансовым потерям, поэтому разработка защищённой мультиагентной системы является актуальной задачей.

Мультиагентная система должна быть защищена как от внешних, так и от внутренних источников угроз целостности, доступности и конфиденциальности. Модель такой системы может быть описана как $MAS = \{AG, ST, ENV, SEC, SAF\}$ – защищённая мультиагентная система, где:

– $AG = \{ag_i | i = 2, \dots, n\}$ – непустое конечное множество интеллектуальных агентов, n – количество агентов;

– $ST = \{st_j | j = 1, \dots, m\}$ – непустое конечное множество состояний внешней среды, m – количество состояний внешней среды;

– $ENV: ST \times A_{ag_1} \times \dots \times A_{ag_n} \rightarrow 2^{ST}$ – функция, описывающая возможную реакцию внешней среды на действия всех агентов системы, A – непустое конечное множество действий агента;

– $SEC: R(T_{IN}^{EXT}, T_{AV}^{EXT}, T_{CON}^{EXT}) \rightarrow 0$ – функция, описывающая защищённость мультиагентной системы, где R – риск, вероятность реализации внешних угроз целостности, доступности и конфиденциальности;

– $SAF: R(T_{IN}^{INT}, T_{AV}^{INT}, T_{CON}^{INT}) \rightarrow 0$ – функция, описывающая безопасность мультиагентной системы, где R – риск, вероятность реализации внутренних угроз целостности, доступности и конфиденциальности.

Под защищённостью понимается способность мультиагентной системы противостоять несанкционированному доступу к данным, а также их случайному искажению или разрушению. Под безопасностью понимается способность мультиагентной системы сохраняться при разрушающих воздействиях.

$IN = \{IN_{TRD}, IN_{STD}, IN_{AG}\}$ – целостность данных, где:

– $IN_{TRD} = \{ES, TCP\}$ – целостность передаваемых данных, которая обеспечивается путём использования электронной подписи и протокола управления передачей TCP ;



– $IN_{STD} = \{H\}$ – целостность хранимых данных достигается благодаря хешированию;

– $IN_{AG} = \{H, OB\}$ – целостность агента достигается путём хеширования и проверки перед запуском ПО, а также обфускацией кода.

$AV = \{AV_{TRD}, AV_{STD}\}$ – доступность данных, где:

– $AV_{TRD} = \{RT, DUP\}$ – доступность передаваемых данных, обеспечиваемая таблицей маршрутизации и дублированием информации (передачей информации от агента i (при необходимости) на главный узел, если агент j недоступен);

– $AV_{STD} = \{BKP, REP\}$ – доступность хранимых данных благодаря резервному копированию и репликации баз данных.

$CON = \{CON_{TRD}, CON_{STD}\}$ – конфиденциальность данных, где:

– $CON_{TRD} = \{EN_D\}$ – конфиденциальность передаваемых данных обеспечивается использованием шифрования данных;

– $CON_{STD} = \{EN_D, EN_{F/DIR}\}$ – конфиденциальность хранимых данных обеспечивается шифрованием данных и файла/директории.

В мультиагентной системе находятся несколько агентов (от 2 до n). У каждого агента есть глобальная цель W (например, задание, взятое из доски объявлений), которая может совпадать с глобальными целями других агентов, и одна или несколько локальных (которые ведут к осуществлению глобальной цели) W_i .

Цели W, W_1, W_2, \dots, W_n измеримы и существуют вещественные функции (функции полезности) $q(ag), q_1(ag), q_2(ag), \dots, q_n(ag)$ такие, что если $ag_i \succ^W ag_j$ (\succ^W – лучше в смысле W), то $q(ag_i) > q(ag_j)$ для всех $i, j = 1, \dots, n$ ($i \neq j$). Соответственно, $ag_i \succ^{W_k} ag_j$, если $q_k(ag_i) > q_k(ag_j)$ ($k = 1, \dots, n$) [3].

Если у нескольких агентов совпадают глобальные цели и функция полезности при взаимодействии агентов:

– уменьшается ($q(ag_1, ag_2, \dots, ag_n) < q(ag_1) + q(ag_2) + \dots + q(ag_n)$), то агенты конфликтуют ($ag_i \succ I ag_j$, где ag_i – множество агентов, функция полезности которых больше нуля, ag_j – множество агентов, функция полезности которых меньше нуля, причём $S_i \cap S_j = \emptyset$ (противоположная ситуация – $\succ \bar{I}$));

– не изменяется ($q(ag_1, ag_2, \dots, ag_n) = q(ag_1) + q(ag_2) + \dots + q(ag_n)$), то агенты нейтральны друг к другу, то есть не оказывают никакого взаимодействия друг на друга ($ag_i \succ \bar{I}_n ag_j$);

– увеличивается ($q(ag_1, ag_2, \dots, ag_n) > q(ag_1) + q(ag_2) + \dots + q(ag_n)$), то агенты сотрудничают ($ag_i \succ \bar{I}_c ag_j$ (ag_i – множество агентов с высокой функцией полезности, ag_j – с низкой)).

Устранение конфликта связано с изменением окружения, с формированием (генерированием) условий $\{U\}$ ($\{U\}$ – структурные, функциональные, параметрические и другие преобразования), позволяющих обеспечить выполнение



$U(ag_i > I ag_j) = ag_i > \bar{I} ag_j$, где ag_i и ag_j – конфликтующие агенты, например:

- путём воздействия на оба агента ($U(ag_i) > \bar{I} U(ag_j)$);
- на одного из них ($U(ag_i) > \bar{I} ag_j$ или $ag_i > \bar{I} U(ag_j)$).

Примером разрешения конфликта может быть назначение других агентов для решения задачи, с которой не справились конфликтующие агенты, или исключение какого-либо агента (или группы агентов).

Легитимные агенты могут конфликтовать, сотрудничать или быть нейтральными. Нелегитимные агенты конфликтуют с легитимными или нейтральны к ним (например, если нет связи между ними по какой-либо причине).

Агент ag_i на основании информации о состоянии каждого агента и их текущих действиях вырабатывает текущее действие, при котором значение ΔW максимально, и посылает информацию об этом другим агентам. Если агент ag_k ($k \neq i$) в результате проверки получил положительное заключение, он подаёт положительный голос за ag_i и сообщает об этом остальным агентам. Каждый агент, получив сведения о результатах проверки агента другими агентами, подсчитывают количество положительных и отрицательных голосов, поданных за него, вычисляет доверие к ag_i . Доверие – мера, характеризующая готовность агента ag_i взаимодействовать с агентом ag_j ($i \neq j$) в данной ситуации [4].

Ситуация, когда внедряется группа нелегитимных агентов, оценивающих друг друга положительно, а легитимных агентов отрицательно, ведёт к компрометации легитимных агентов. Для решения этой проблемы используется репутация – сформировавшееся во времени общественное мнение об агенте. При подсчёте голосов будет учитываться репутация голосующих агентов путём взвешенного суммирования их оценок. Значение репутации зависит от истории взаимодействия и от времени пребывания в нём.

Примером решения конфликта может быть следующее решение. Если репутация какого-то агента ниже определённого порога, то взаимодействие других агентов с ним прекращается, такой агент заносится в «чёрный список».

Модель интеллектуального агента для защищённой мультиагентной системы выглядит как $AG = \{ST, A, ENV, I, REF, ACT\}$ – интеллектуальный агент, где:

- $ST = \{st_j | j = 1, \dots, m\}$ – непустое конечное множество состояний внешней среды, m – количество состояний внешней среды;
- $A = \{a_k | k = 1, \dots, q\}$ – непустое конечное множество действий агента;
- $ENV: S \times A \rightarrow 2^S$ – функция поведения внешней среды, сопоставляющая текущему состоянию внешней среды и выбранному агентом действию непустое конечное множество возможных следующих состояний внешней среды (то есть действия агента могут влиять на окружающую среду, но не контролировать её полностью);
- $I = \{COM, RCT, PCT, DI, PI\}$ – непустое конечное множество внутренних состояний агента:



- $COM: I \times W \rightarrow I'$ (W – цель, которую агент стремится достичь) – свойство коммуникативности;
- $RCT: I \times ENV \rightarrow A$ – свойство реактивности;
- $PCT: I \times ST \times W \rightarrow A$ – свойство проактивности;
- $DI = \{DI_{self}, DI_{env}, DI_{ag}\}$ – декларативная информация;
- $PI = \{PI_{self}, PI_{env}, PI_{ag}\}$ – процедурная информация;
- $REF: I \times S \rightarrow I'$ – функция обновления состояния, сопоставляющая предыдущему внутреннему состоянию и новому состоянию внешней среды новое внутреннее состояние агента;
- $ACT: I \times S \times A \rightarrow A'$ – функция принятия решения, сопоставляющая текущему внутреннему состоянию агента некоторое действие.

Литература

1. Massive Software [Электронный ресурс] – Режим доступа: URL: <http://web.archive.org/web/20080415081617/http://www.massivesoftware.com/showcase/film/> (23.02.2019).
2. Информационные мультиагентные технологии в экономике [Электронный ресурс] – Режим доступа: URL: <https://cyberleninka.ru/article/n/informatsionnye-multiagentnye-tehnologii-v-ekonomike> (дата обращения: 23.02.2019).
3. Сысоев, В.В. Формирование конфликта в структурном представлении систем // Информационные технологии и системы. – Воронеж: Воронеж, отд. Междун. акад. информатизации, 1996 г. – 30 с.
4. Зикратов, И.А. Построение модели доверия и репутации к объектам мультиагентных робототехнических систем с децентрализованным управлением. / И.А. Зикратов, Т.В. Зикратова, И.С. Лебедев, А.В. Гуртов. – Научно-технический вестник информационных технологий, механики и оптики, 2014 г. – 9 с.

И.С. Казанцева, О.П. Солдатова

РЕШЕНИЕ ЗАДАЧИ ДЕТЕКТИРОВАНИЯ ИЗОБРАЖЕНИЙ ПРИ ПОМОЩИ КАСКАДНЫХ КЛАССИФИКАТОРОВ

(Самарский университет)

Целью данной работы является решение задачи детектирования изображения с помощью каскадного классификатора Хаара и каскадного классификатора LBP применительно к детектированию оптимальных мест для измерения толщины комплекса интим-медиа артериальной стенки сонной артерии.

Каскадные алгоритмы, известные так же, как классификаторы со скользящим окном, получили широкое распространение. Паул Виола и Майкл Джонс первыми предложили метод для обнаружения лиц на фотографиях. Для реше-