Секция 3

МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

УДК 519.7 + 519.8 + 004.8

МУЛЬТИАГЕНТНАЯ ЗАДАЧА О РОБОТАХ В ПРОСТРАНСТВЕ: ИНФОРМАЦИОННЫЙ И КРИПТОГРАФИЧЕСКИЙ АСПЕКТЫ[1]

А. Ю. Бернштейн, Н. В. Шилов

Распределённая система — это группа децентрализованных взаимодействующих исполнителей [1]. *Распределённый алгоритм* — это протокол работы и взаимодействия исполнителей в распределённой системе, превращающий децентрализованную группу в коллектив, совместно решающий некоторую задачу [2]. *Параметрический* алгоритм (или протокол) — это масштабируемый алгоритм для исполнителя в распределённой системе (протокол распределённой системы соответственно), в котором множество исполнителей в системе использовано как константа-параметр.

Мультиагентная система — это распределённая система, состоящая из агентов [3]. *Агент* — это автономный (воспринимающий мир разделённым на *себя* и *среду*, включающую всё остальное), реагирующий (способный взаимодействовать со средой и отвечать на воздействия среды) объект (в объектно-ориентированном смысле), внутреннее состояние которого можно характеризовать в терминах *мнений* или *веры* (Believes), *целей* (Desires) и *намерений* (Intentions) агента. *Мультиагентный алгоритм* — это распределённый алгоритм для мультиагентной системы. *Анонимный протокол* — это протокол мультиагентной системы, одинаковый для всех агентов.

В работе исследуется следующая задача о **роботах в пространстве** (RinS — Robot in Space). В евклидовом пространстве $\mathbb{R}^k$ ($k \geqslant 2$) находятся $n > 1$ автономных роботов и столько же укрытий в общем положении (т. е. никакие три объекта не лежат на одной прямой). Местоположение всех укрытий фиксировано и известно каждому роботу. Каждому роботу изначально назначено индивидуальное укрытие, о котором робот знает. Каждый робот знает свои координаты в пространстве, знает о существовании всех остальных роботов, но не знает их координаты, и знает, что всем роботам изначально назначены и известны индивидуальные укрытия. В некоторый момент времени все роботы останавливаются, фиксируют свои текущие позиции, и затем они все должны выбрать укрытия, чтобы двинуться к ним по прямолинейному маршруту. Ясно, что роботам нельзя сталкиваться. Роботы могут взаимодействовать каждый с каждым попарно, вести переговоры в парах и обмениваться укрытиями. Задача: разработать анонимный параметрический мультиагентный алгоритм переговоров, гарантирующий, что каждый робот когда-нибудь будет точно знать, что его маршрут к укрытию, которое он выбрал в результате переговоров, не пересекается и никогда не будет пересекаться с маршрутами остальных роботов. Эта задача «выросла» из ранее рассмотренной задачи о роботах на Марсе (Mars Robot Puzzle — MRP) [4]: MRP является частным случаем RinS на плоскости.

[1]Работа выполнена в рамках проекта СО РАН 15/10 на 2012–14 гг.

Протоколом распределения укрытий будем называть любой мультиагентный алгоритм, решающий задачу RinS. Такой протокол может состоять из алгоритма переговоров для индивидуальных роботов и алгоритма-планировщика общения между роботами мультиагентной системы. Будем говорить, что алгоритм-планировщик общения между роботами удовлетворяет условию *справедливости*, если в любой момент времени для любого робота, желающего контактировать в этот момент с каким-либо другим роботом-партнёром, обязательно наступит в будущем момент времени, когда партнёр будет готов к общению с данным роботом. Варианты алгоритма-планировщика можно найти в работе [4].

Щелчок — это алгоритм переговоров между двумя роботами, который позволяет этим роботам проверить, нужно ли им обмениваться укрытиями, и удовлетворяет следующим двум условиям:

— если текущие пути роботов пересекаются, то они должны совершить обмен;
— после обмена укрытиями суммарная длина путей строго уменьшается.

Два крайних случая щелчка — это *простой щелчок*, при котором обмен укрытиями выполняется тогда и только тогда, когда пути пересекаются, и *щелчком со сравнением*, при котором обмен укрытиями выполняется тогда и только тогда, когда сумма длин путей уменьшается. В рамках данного исследования неважно, как именно устроен щелчок, но существенно то, что при исполнении этого протокола роботы сообщают друг другу что-либо о своём положении.

В работе [4] поставлен вопрос об оценке сложности алгоритмов назначения укрытий, основанных на щелчках. Сейчас мы готовы дать очень простой ответ на этот вопрос.

Теорема 1. Любой алгоритм назначения укрытий, основанный на протоколе щелчка, не может совершить более $\dfrac{L-l}{\Delta} \cdot n$ щелчков, где L и l — максимальное и минимальное расстояния между роботом и укрытием в системе, а Δ — минимальный декремент суммы длин путей при щелчке (который не равен 0, так как никакие три объекта не лежат на одной прямой).

Сужением протокола распределения укрытий на множество S будем называть протокол, отличающийся только тем, что входные данные для него (положения роботов и укрытий) должны принадлежать множеству S.

В рамках исследования информационного аспекта задачи RinS в качестве входных данных рассматриваются действительные числа. При этом неважно, как роботы хранят их в памяти; будем интересоваться общим количеством битов (сообщений), переданных участниками друг другу в ходе исполнения протокола. Будем называть протокол *финитным*, если при любых допустимых значениях входных данных его работа завершается после передачи конечного количества битов.

Теорема 2. Существует финитный параметрический анонимный мультиагентный алгоритм распределения укрытий, основанный на протоколе щелчка и справедливом планировщике общения между агентами.

Будем называть протокол *ограниченным*, если существует такая константа N, что при любых допустимых значениях входных данных его работа завершается после передачи не более N битов. Будем называть протокол *ограниченным по сообщениям*, если существует такая константа N, что при любых допустимых значениях входных данных его работа завершается после передачи не более N сообщений.

Теорема 3. Пусть бесконечное множество точек $S \subseteq \mathbb{R}^k$, $k \geqslant 2$, лежащих в общем положении, обладает следующим свойством: существует непрерывная замкнутая плоская кривая, содержащая S и ограничивающая выпуклое плоское множество. Тогда сужение любого протокола распределения укрытий между $n \geqslant 2$ участниками на множество S не может быть ограниченным. Кроме того, если множество S более чем счётно, то сужение любого протокола распределения укрытий между $n \geqslant 2$ участниками на множество S не может быть ограниченным по сообщениям.

В рамках исследования криптографического аспекта задачи RinS будем считать, что входные данные (координаты роботов и укрытий) берутся из некоторого конечного множества точек в пространстве $\mathbb{R}^k$, $k \geqslant 2$, все координаты которых — числа, заданные конечным числом разрядов в какой-либо (фиксированной) позиционной системе счисления. Заметим, что в этом случае смысл протокола распределения укрытий состоит в вычислении некоторой функции координат роботов и укрытий, значением которой является искомое распределение. В силу теоремы о конфиденциальных вычислениях (Oblivious Transfersecure multi-party computation) [5, 6] существует способ вычисления этой функции, при котором участники не получат никаких дополнительных сведений о входных данных друг друга.

Теорема 4. Пусть $S \subset \mathbb{R}^k$ — произвольное конечное множество точек, все координаты которых — числа с фиксированным числом разрядов в некоторой фиксированной позиционной системе счисления. Тогда

1) существует сужение на множество S основанного на простом щелчке протокола распределения укрытий, в котором агенты не сообщают друг другу свои координаты;
2) существует сужение на множество S основанного на щелчке со сравнениями протокола распределения укрытий, в котором агенты не сообщают друг другу свои расстояния до укрытий.

ЛИТЕРАТУРА

1. *Таненбаум Э., ван Стеен М.* Распределённые системы. Принципы и парадигмы. СПб.: Питер, 2003.
2. *Тель Ж.* Введение в распределённые алгоритмы. М.: МЦНМО, 2009.
3. *Wooldridge M.* An Introduction to Multiagent Systems. John Willey & Sons Ltd, 2002.
4. *Бодин Е. В., Гаранина Н. О., Шилов Н. В.* Задача о роботах на Марсе (мультиагентный подход к задаче Дейкстры) // Моделирование и анализ информационных систем. 2011. Т. 18. № 2. С. 113–128.
5. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2002.
6. *Goldreich O.* Foundations of Cryptography — A Primer // Foundations and Trends in Theoretical Computer Science. 2005. V. 1. No. 1. P. 1–116.

УДК 004.056.53

ПОИСК МОСТОВ В МОДЕЛИ БЕЗОПАСНОСТИ TAKE-GRANT

Д. М. Бречка

В настоящее время для разработки и исследования защищённых компьютерных систем широко используются дискреционные модели безопасности. Такие модели основаны на субъектно-объектном подходе, согласно которому система представляется