

БЕЗОПАСНОСТЬ РЕШЕНИЯ КОМБИНАТОРНЫХ ЗАДАЧ НА ЛОКАЛЬНЫХ СЕТЯХ

М.П. РЕВОТЮК, П.М. БАТУРА

Объект рассмотрения — способ противодействия раскрытия смысла задач комбинаторной оптимизации, решаемых по технологии GRID на вычислительных сетях общего назначения. Невозможность на таких сетях физической и логической изоляции программных компонент проблемно-ориентированной системы агентов создает угрозу раскрытия информации о задаче легитимным пользователем рабочей станции.

Однако для многих вычислительно сложных задач комбинаторной оптимизации шаги процесса поиска решения можно естественным образом связать с требованиями основной теоремы безопасности. Для этого достаточно выбрать подходящие приемы грануляции процесса решения и запутывания представления задачи с секретом, назначаемым агентом-диспетчером на рабочей станции.

Например, решение задачи коммивояжера методом ветвей и границ процесса, как известно, наиболее эффективно проводится с ветвлением на множестве линейных задач назначения. Распараллеливание такой задачи в момент появления доступного процессора рекомендуется проводить в узле с минимальным расстоянием от корня дерева. Скрытие параметров и содержания задачи предлагается выполнять случайно генерируемой перестановкой индексов элементов матриц порождаемых подзадач. Это позволяет сохранить преимущества жадного алгоритма загрузки процессоров сети с минимизацией передачи коррелированных данных о подзадачах.

В результате новый агент получает фактически матрицу квадратичной задачи назначения. Так как последняя относится к классу обобщенных задач коммивояжера, то раскрытие описания задачи в узле порождения становится существенно более сложным.

Реализация предлагаемого подхода не исключает стандартных подходов к обеспечению безопасности работы на сетях.