Переход между уровнями ветвления дополняется операциями в рассматриваемом классе для синхронной обработки прерываний. Альтернативы ветвления представимы инкрементом вектора состояния на предыдущем уровне. Возврат процесса в предшествующее состояние реализуется операцией декремента. Сохранение состояния процесса решения удобно синхронизировать с моментом обработки листа дерева вариантов.

Таким образом, состояние процесса решения оказывается представленным удобным для его миграции и дальнейшего распараллеливания системно-независимым и проблемно-ориентированным способом. Иллюстрация применения предлагаемой технологии проводится на примере динамической задачи о назначении [1] и задачи многих коммивояжеров.

Литература

1. Zlot R., Stentz A. Market-based multirobot coordination for complex tasks // International Journal of Robotics Research. 2006. № 25 (1). P. 1–25.

ПРОАКТИВНЫЙ АЛГОРИТМ КООРДИНАЦИИ СИСТЕМ АГЕНТОВ

М.П. Ревотюк, А.К. Пушкина

В процессе координации систем взаимодействующих агентов необходимо регулярно решать задачу о динамическом назначении свободным агентам новых возникающих задач [1] с учетом реальных ограничений и возможной коррекции плана назначения с учетом текущего состояния. Традиционно задачи координации агентов сводятся к известным задачам дискретной оптимизации, таким как линейная задача о назначении или задача нескольких странствующих коммивояжеров. Однако необходимость учета реальных отношений между агентами и задачами приводит к экспоненциальной сложности алгоритма формирования оптимального назначения и часто делает их практически не реализуемыми.

Используя понятия наиболее раннего и позднего срока начала решения задачи, можно проводить жадный упреждающий поиск окончательного назначения. Так как процедура назначения дополняет граф оптимального паросочетания при поступлении новых заявок, то время реакции на заявку определяется сложностью обработки последней группы заявок. Предлагается дополнить такую процедуру накоплением на интервалах ожидания заявок информации о множествах альтернативных кратчайших путей для дальнейшего сокращения задержки на обработку прогнозируемых заявок.

Реализация предлагаемой схемы проактивного управления возможна на рекуррентных сетевых моделях, состояние которых соответствует графу текущего паросочетания с выделением оптимального решения. Переход между состояниями сети реализуется инкрементальными версиями алгоритмов решения линейных задач о назначении, задачи коммивояжера и поиска кратчайших путей на графах. На параметры таких задач проецируются особенности процессов обслуживания, включая векторные критерии и разнообразные отношения вложенности.

Литература

1. Gerkey B.P., Mataric M.J. A Formal Analysis and Taxonomy of Task Allocation in Multi-Robot Systems // The International Journal of Robotics Research, 2004. Vol. 23, no. 9. P. 939–954.

КВАДРАТИЧНО-ВЫЧЕТНЫЕ КОДЫ КАК КОДЫ ХЕММИНГА И ОБОБЩЕННЫЕ КОДЫ БОУЗА-ЧОУДХУРИ-ХОКВИНГЕМА

Е.В. Реентович, В.А. Липницкий

Квадратично-вычетные коды являются обобщением кодов Боуза-Чоудхури-Хоквингем. В настоящее время БЧХ коды являются наиболее распространенными по сравнению с остальными видами кодов. Они нашли свое применение в различных областях информатики и радиоэлектроники, таких как сети и системы телекоммуникаций, системы радионавигации, радиолокации, телевидения, вычислительные машины и системы, компьютерных сетях, связана с теорией групп, колец и полей, теорией чисел и полиномов и т.д. Однако, в общем случае, с ростом длины, параметры БЧХ кодов (скорость, минимальное расстояние) становятся хуже.

В свою очередь, известно, что с ростом длины параметры КВ-кодов становятся только лучше или, как минимум, не ухудшаются, что сделало множество КВ-кодов популярным объектом для исследований. Однако процесс исследования этих объектов весьма затруднителен, КВ-коды плохо поддаются декодированию.

В данной работе строится способ декодирования квадратично-вычетных кодов при помощи теории норм синдромов, основанной на инвариантности норменных и полиномиальных орбит ошибок. Были изучены квадратично-вычетные коды длины 31 и 73. Для них были построены норменные, полиномиальные орбиты, построен алгоритм декодирования данных кодов в системе компьютерной алгебры Wolfram Mathematica. Данный алгоритм отличается своей простотой, скоростью и эффективностью.

ОСОБЕННОСТИ ПРИМЕНЕНИЯ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ ДЛЯ АУТЕНТИФИКАЦИИ В СИСТЕМАХ IoT

Н.С. Руденко, Г.А. Власова

Тенденция массового перехода от интернета персональных компьютеров к интернету вещей (Internet of Things, IoT) ставит новые задачи по обеспечению надежности и безопасности работы сетей. Одним из основных средств защиты информации для IoT является использование криптографических алгоритмов. В связи с тем, что многие приспособления в сети мобильны и зачастую имеют небольшие размеры, существуют общие ограничения на ресурсы времени и памяти. Эти ограничения распространяются и на криптографические схемы, открывая новое направление – разработки и исследования алгоритмов малоресурсной криптографии (Lightweight Cryptography, LWC).

В настоящее время наиболее «легковесными» являются алгоритмы асимметричной криптографии, работающие с эллиптическими кривыми (ECC – Elliptic Curves Cryptography). Типичными значениями параметров различных процессоров, предназначенных для вычислений с эллиптическими кривыми, являются величины энергопотребления в пределах 10–40 μW и размеров микросхемы 10,000–20,000 GE (условных логических элементов, Gate Equivalent). Известные реализации алгоритма RSA значительно превышают 15,000 GE. По сравнению с симметричной криптографией, асимметричная криптография с безопасной длиной ключа, реализованная на аппаратном уровне, по прежнему требует значительно больших ресурсов (по крайней мере 10000 дополнительных логических элементов), при этом реализуется вполне приемлемая скорость работы. Для криптографии с открытым ключом верхняя граница на размер микросхемы устанавливается в 15,000 GE. Что касается программной реализации, то тщательная оптимизация алгоритмов позволяет микроконтроллерам выполнять операции ассиметричной криптографии менее чем за 1 секунду, что вполне достаточно для большинства приложений. При этом программно-аппаратная реализация, создает наилучший баланс между размером и скоростью для многих распространенных вычислительных приложений.

Одним из наиболее надежных симметричных алгоритмов является ГОСТ 28147-89. Результаты сравнений популярных симметричных шифров показывают, что ГОСТ 28147-89 при аналогичной криптостойкости обладает достаточным для IoT быстродействием. Также хорошие результаты показывают отечественные алгоритмы, собранные в библиотеке bee2.

В результате можно сделать вывод о том, что использование малоресурсных криптографических алгоритмов для аутентификации в сетях IoT вполне возможно и не практически не влияет на удобство их эксплуатации пользователем.

ЛЕГКОВЕСНАЯ КРИПТОГРАФИЯ С ОТКРЫТЫМ КЛЮЧОМ

Т.Х. Рустамов

Легковесная криптография – раздел криптографии, имеющий своей целью разработку алгоритмов для применения в устройствах, которые не способны обеспечить большинство существующих шифров достаточными ресурсами (память, электропитание, размеры) для функционирования. Области блочного шифрования наиболее популярными легковесными алгоритмами считаются CLEFIA и PRESENT. Оба алгоритма известны еще с 2007 г. В 2012 г. организации ISO и IEC включили алгоритмы PRESENT и CLEFIA в международный стандарт