УДК 004.75

ПРИМЕНЕНИЕ ТЕОРИИ КОДИРОВАНИЯ ДЛЯ ВЫСОКО-ПРОИЗВОДИТЕЛЬНОГО РАСПРЕДЕЛЕННОГО БРОДКАСТА

Шашуловский А.В. (Университет ИТМО, г. Санкт-Петербург)
Научный руководитель – к.т.н, доцент Кузнецов П.В.
(Университет ИТМО, г. Санкт-Петербург)

Введение. В современных реалиях активно растет интерес к распределенным системам, поскольку задачи хранения и обработки данных требуют все больше ресурсов. Эти системы известны своей сложностью реализации и отладки даже самых простых алгоритмов. Некоторые задачи требуют значительно больше ресурсов, чем может показаться на первый взгляд. Одной из таких задач является надежный распределенный бродкаст в системе, где фиксированное число узлов может отказывать произвольным образом. Ее суть заключается в следующем: один из узлов должен отправить сообщение всем остальным таким образом, чтобы либо все корректно работающие процессы получили одно и то же сообщение, либо не получили никакого сообщения вовсе.

Классическое решение этой задачи предполагает квадратичный объем передаваемых по сети данных, относительно исходного сообщения. Однако в научных работах были представлены теоретически более оптимальные методы решения задачи, использующие для этого теорию кодирования информации, практическая полезность которых остается неизвестной. Целью данного исследования является реализация как классического, так и оптимизированных алгоритмов, их оптимизация для практического применения, а также сравнение и выявление преимуществ одного алгоритма над другими.

Эта проблема востребована в широком множестве приложений, включая распределенные базы данных, блокчейн и другие системы, где отказ узлов или злонамеренное поведение являются ожидаемыми.

Основная часть. Для анализа было выделено три подхода к решению задачи:

Double-Echo Broadcast [1] – базовый алгоритм. Его основная идея заключается в использовании двух дополнительных фаз рассылки сообщений между узлами, что позволяет корректно работающим процессам прийти к соглашению о принятии сообщения. В этих фазах каждый процесс отправляет всем остальным свою версию сообщения, что приводит к квадратичной асимптотике как передачи, так и хранения данных.

Алгоритм Cachin-Tessaro [2] – основывается на той же идее, что и предыдущий, но использует стирающий код, чтобы разбить сообщение на блоки, части которых достаточно для восстановления исходного сообщения. Таким образом, вместо того чтобы отправлять все сообщение, каждый процесс отправляет только свой кусок данных, а также доказательство его корректности с помощью деревьев Меркля. Для достаточно больших сообщений достигается большой выигрыш в объеме как передачи, так и хранения данных.

Алгоритм Das-Xiang-Ren [3] – дальнейшая оптимизация идеи предыдущего алгоритма. Ее суть заключается в применении кодирования, исправляющего ошибки, что позволяет не отправлять доказательства каждого блока по отдельности, а отправлять только хэш всего сообщения в целом, что еще больше оптимизирует объем передачи и хранения данных.

Эти алгоритмы были реализованы на языке программирования Go, оптимизированы для практического использования и протестированы на различных конфигурациях, для выявления оптимального алгоритма для разных сценариев использования: в зависимости от размера сообщения, количества узлов в сети и сетевых задержек.

Выводы. В ходе работы был проведен сравнительный анализ трех алгоритмов, реализующих протокол распределенного бродкаста в системах с возможным произвольным отказом узлов. Были предложены и реализованы оптимизации для этих алгоритмов.

Полученные результаты показали, что использование теории кодирования позволяет существенно улучшить производительность решений данной задачи. Однако, оптимальный выбор алгоритма зависит от характеристик конкретной сети и размера передаваемого сообщения.

Результаты исследований могут быть использованы для таких распространенных систем, как распределенные базы данных, блокчейн и другие системы, где отказ узлов или злонамеренное поведение могут привести к сбоям и потере данных.

Список использованных источников:

1. Bracha G. Asynchronous byzantine agreement protocols // Inf. Comput. - 1987. - №75. - С. 130-143.
2. Cachin C, Tessaro S. Asynchronous Verifiable Information Dispersal // 24th IEEE Symposium on Reliable Distributed Systems. - 2005. - С. 7-8.
3. Das S., Xiang Z., Ren L. Asynchronous Data Dissemination and its Applications // ACM SIGSAC Conference on Computer and Communications Security. - 2021. - С. 4-5.

Шашуловский А.В. (автор) Подпись

Кузнецов П.В. (научный руководитель) Подпись