ВикипедиЯ

Задача византийских генералов

Материал из Википедии — свободной энциклопедии

Задача византийских генералов (англ. *Byzantine fault tolerance (BFT), Byzantine agreement problem, Byzantine generals problem, Byzantine failure*) — в криптологии задача взаимодействия нескольких удаленных абонентов, которые получили приказы из одного центра. Часть абонентов, включая центр, могут быть злоумышленниками. Нужно выработать единую стратегию действий, которая будет выигрышной для абонентов.

Содержание

Формулировка

Византия. Ночь перед великим сражением с противником. Византийская армия состоит из n легионов, каждым из которых командует свой генерал. Также у армии есть главнокомандующий, которому подчиняются генералы.

В то же самое время, империя находится в упадке, и любой из генералов и даже главнокомандующий могут быть предателями Византии, заинтересованными в её поражении.

Ночью каждый из генералов получает от предводителя приказ о варианте действий в 10 часов утра (время одинаковое для всех и известно заранее), а именно: «атаковать противника» или «отступать».

Возможные исходы сражения:

1. Если все верные генералы атакуют — Византия уничтожит противника (благоприятный исход).
2. Если все верные генералы отступят — Византия сохранит свою армию (промежуточный исход).
3. Если некоторые верные генералы атакуют, а некоторые отступят — противник уничтожит всю армию Византии (неблагоприятный исход).

Также следует учитывать, что если главнокомандующий — предатель, то он может дать разным генералам противоположные приказы, чтобы обеспечить уничтожение армии. Следовательно, генералам лучше не доверять его приказам.

Если же каждый генерал будет действовать полностью независимо от других (например, сделает случайный выбор), то вероятность благоприятного исхода весьма низка.

Поэтому генералы нуждаются в обмене информацией между собой, чтобы прийти к единому решению.

Определение

n «белых» генералов возглавляют армии в горах и готовятся атаковать «черных» в долине. Для связи атакующие используют надёжную связь (например, телефон). Однако из n генералов m являются предателями и активно пытаются воспрепятствовать согласию лояльных генералов. Согласие состоит в том, чтобы все лояльные генералы узнали о численности всех лояльных армий и пришли к одинаковым выводам (пусть и ложным) относительно состояния предательских армий. (Последнее условие важно, если генералы на основании полученных данных планируют выработать стратегию и необходимо, чтобы все генералы выработали одинаковую стратегию.)

Формализация

По результатам обмена каждый из лояльных генералов должен получить вектор целых чисел длины n, в котором i-й элемент либо равен истинной численности i-й армии (если её генерал лоялен), либо содержит дезинформацию о численности i-й армии (если её генерал не лоялен). При этом векторы, полученные всеми лояльными командирами должны быть полностью одинаковы.

Алгоритмы решения

Частный случай

Рекурсивный алгоритм решения для частного случая, когда количество генералов ограничено и не может динамически изменяться, был предложен в 1982 г. Лесли Лампортом. Алгоритм сводит задачу для случая m предателей среди n генералов к случаю $m-1$ предателя.

Для случая $m=0$ алгоритм тривиален, поэтому проиллюстрируем его для случая $n=4$ и $m=1$. В этом случае алгоритм осуществляется в 4 шага.

1-й шаг. Каждый генерал посылает всем остальным сообщение, в котором указывает численность своей армии. Лояльные генералы указывают истинное количество, а предатели могут указывать различные числа в разных сообщениях. Генерал 1 указал число 1 (одна тысяча воинов), генерал 2 указал число 2, генерал 3 (предатель) указал трём остальным генералам соответственно x, y, z, а генерал 4 указал 4.

2-й шаг. Каждый формирует свой вектор из имеющейся информации.

Получается:

Вектор 1 (1,2,x,4);

Вектор 2 (1,2,y,4);

Вектор 3 (1,2,3,4);

Вектор 4 (1,2,z,4).

3-й шаг. Каждый посылает свой вектор всем остальным (генерал 3 посылает опять произвольные значения).

После этого у каждого генерала есть по четыре вектора:

g1	g2	g3	g4
(1,2,x,4)	(1,2,x,4)	(1,2,x,4)	(1,2,x,4)
(1,2,y,4)	(1,2,y,4)	(1,2,y,4)	(1,2,y,4)
(a,b,c,d)	(e,f,g,h)	(1,2,3,4)	(i,j,k,l)
(1,2,z,4)	(1,2,z,4)	(1,2,z,4)	(1,2,z,4)

4-й шаг. Каждый генерал определяет для себя размер каждой армии. Чтобы определить размер i-й армии, каждый генерал берёт три числа — размеры этой армии, пришедшие от всех командиров, кроме командира i-й армии. Если какое-то значение повторяется среди этих трех чисел как минимум дважды, то оно помещается в результирующий вектор, иначе соответствующий элемент результирующего вектора помечается неизвестным (или нулём и т. п.).

Все лояльные генералы получают один вектор $(1, 2, f(x, y, z), 4)$, где $f(x, y, z)$ есть число, которое встречается как минимум два раза среди значений (x, y, z), или «неизвестность», если все три числа (x, y, z) различны. Поскольку значения x, y, z и функция f у всех лояльных генералов одни и те же, то согласие достигнуто.

Общий случай

При помощи технологии цепочки блоков и майнинга, впервые использовавшейся в первой децентрализованной системе электронной наличности Bitcoin, решён более общий случай данной задачи, когда количество генералов (узлов сети) неограниченно и может динамически изменяться.

Результаты исследования задачи

Лампорт доказал, что в системе с m неверно работающими процессорами («нелояльными генералами») можно достичь согласия только при наличии $2m + 1$ верно работающих процессоров («лояльных генералов»), то есть строго больше двух третей от общего числа процессоров.

Применение

- Синхронизация часов
- Биткойн — пиринговая платёжная система[1].

См. также

- Надёжность
- Network Time Protocol (NTP)
- Задача двух генералов
- Алгоритм Паксос
- Алгоритм Raft

Примечания

1. *Marc Andreessen.* Why Bitcoin Matters (http://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/) (англ.). The New York Times (21.01.2014). Проверено 2 октября 2015. (*Марк Андрессен.* Почему Биткоин так важен? = Why Bitcoin Matters (http://habrahabr.ru/company/host-tracker/blog/210126/) (рус.). Habrahabr.ru. Проверено 2 октября 2015. — вариант перевода).

Ссылки

- Крюков В. А. Курс лекций «Распределенные ОС» (http://parallel.ru/krukov/lec7.html)

- The Byzantine Generals Problem (with Marshall Pease and Robert Shostak) ACM Transactions on Programming Languages and Systems 4, 3 (July 1982), 382—401." (http://research.microsoft.com/users/lamport/pubs/pubs.html#byz) (англ.)
- Решение задачи о византийских генералах (http://cryptowiki.net/index.php?title=%C2%AB%D0%97%D0%B0%D0%B4%D0%B0%D1%87%D0%B0_%D0%BE_%D0%B2%D0%B8%D0%B7%D0%B0%D0%BD%D1%82%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D1%85_%D0%B3%D0%B5%D0%BD%D0%B5%D1%80%D0%B0%D0%BB%D0%B0%D1%85%C2%BB._%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%C2%AB%D0%B2%D0%B8%D0%B7%D0%B0%D0%BD%D1%82%D0%B8%D0%B9%D1%81%D0%BA%D0%BE%D0%B3%D0%BE_%D1%81%D0%BE%D0%B3%D0%BB%D0%B0%D1%88%D0%B5%D0%BD%D0%B8%D1%8F%C2%BB._%D0%9E%D0%B1%D0%B5%D1%81%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%B8%D0%B5_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D0%B8_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%BD%D1%8B%D1%85_%D0%B2%D1%8B%D1%87%D0%B8%D1%81%D0%BB%D0%B5%D0%BD%D0%B8%D0%B9) (рус.)
- Доказательство невозможности решения задачи о византийских генералах в случае N<3m+1 (http://blog.artlives.ru/programming/%D0%B2%D0%B8%D0%B7%D0%B0%D0%BD%D1%82%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B5-%D0%B3%D0%B5%D0%BD%D0%B5%D1%80%D0%B0%D0%BB%D1%8B-%D0%B4%D0%BE%D0%BA%D0%B0%D0%B7%D0%B0%D1%82%D0%B5%D0%BB%D1%8C%D1%81%D1%82/) (рус.)

Источник — https://ru.wikipedia.org/w/index.php?title=Задача_византийских_генералов&oldid=94259440