**Проблема византийских генералов**

ЛЕСЛИ ЛАМПОРТ, РОБЕРТ ШОСТАК и МАРШАЛ ПИЗ СРИ International

Надежные компьютерные системы должны справляться с неисправными компонентами, которые дают противоречивую информацию различным частям системы. Эта ситуация может быть абстрактно выражена в терминах группы генералов византийской армии, расположившихся со своими войсками вокруг вражеского города. Общаясь только через посланников, генералы должны согласовать общий план битвы. Однако один или несколько из них могут быть предателями, которые попытаются запутать остальных. Проблема заключается в том, чтобы найти алгоритм, который обеспечит достижение согласия среди лояльных генералов. Показано, что, используя только устные сообщения, эта проблема разрешима, если и только если более двух третей генералов лояльны; таким образом, один предатель может сбить с толку двух лояльных генералов. С использованием не подделываемых письменных сообщений проблема разрешима для любого количества генералов и возможных предателей. Затем обсуждаются применения решений к надежным компьютерным системам.

: Надежность -- устойчивость к сбоям

Общие термины: Алгоритмы, Надежность

Дополнительные ключевые слова и фразы: Интерактивная согласованность

1. ВВЕДЕНИЕ

Надежные компьютерные системы должны быть способны справляться с отказом одного или нескольких своих компонентов. Неисправный компонент может проявлять такой тип поведения, который часто игнорируется, а именно, отправляя противоречивую информацию различным частям системы. Проблема справления с таким типом отказа абстрактно выражается как Проблема византийских генералов. Мы посвящаем основную часть статьи обсуждению этой абстрактной проблемы и завершаем, указывая, как наши решения могут быть использованы для реализации надежной компьютерной системы. Мы представляем, что несколько дивизий византийской армии расположены вне вражеского города, каждая дивизия под командованием своего генерала. Генералы могут общаться друг с другом только через посланника. После наблюдения за врагом они должны решить общий план действий. Однако некоторые из генералов

может быть предателями, пытающимися помешать лояльным генералам достичь соглашения. Генералы должны иметь алгоритм, чтобы гарантировать, что

A. Все лояльные генералы принимают одно и то же решение о плане действий. Лояльные генералы будут делать то, что говорит алгоритм, но предатели могут делать все, что захотят. Алгоритм должен гарантировать условие A независимо от того, что делают предатели. Лояльные генералы должны не только достичь соглашения, но и согласовать разумный план. Поэтому мы также хотим гарантировать, что

B. Небольшое количество предателей не может заставить лояльных генералов принять плохой план. Условие B трудно формализовать, поскольку оно требует точного определения того, что такое плохой план, и мы не пытаемся это сделать. Вместо этого мы рассматриваем, как генералы принимают решение. Каждый генерал наблюдает за врагом и передает свои наблюдения другим. Пусть v(i) будет информацией, переданной i-м генералом. Каждый генерал использует какой-то метод для объединения значений v(1) ... v(n) в единственный план действий, где n — это количество генералов. Условие A достигается тем, что все генералы используют один и тот же метод для объединения информации, а условие B достигается с помощью надежного метода. Например, если единственное решение, которое нужно принять, — это атаковать или отступить, то v(i) может быть мнением генерала i о том, какой вариант лучше, и окончательное решение может основываться на голосовании большинства среди них. Небольшое количество предателей может повлиять на решение только в том случае, если лояльные генералы были почти поровну разделены между двумя возможностями, в этом случае ни одно из решений нельзя назвать плохим. Хотя этот подход может быть не единственным способом удовлетворить условия A и B, это единственный, о котором мы знаем. Он предполагает метод, с помощью которого генералы передают свои значения v(i) друг другу. Очевидный метод — это когда i-й генерал отправляет v(i) курьером каждому другому генералу. Однако это не сработает, потому что для удовлетворения условия A требуется, чтобы каждый лояльный генерал получил одни и те же значения v(1) ... v(n), а предательский генерал может отправить разные значения разным генералам. Чтобы условие A было выполнено, должно быть верно следующее:

1. Каждый лояльный генерал должен получить одну и ту же информацию v(1) ..., v(n). Условие 1 подразумевает, что генерал не может обязательно использовать значение v(i), полученное непосредственно от i-го генерала, поскольку предательский i-й генерал может отправить разные значения разным генералам. Это означает, что, если мы не будем осторожны, при выполнении условия 1 мы можем ввести возможность того, что генералы используют значение v(i), отличное от того, что отправил i-й генерал, даже если i-й генерал лоялен. Мы не должны позволять этому происходить, если условие B должно быть выполнено. Например, мы не можем позволить нескольким предателям заставить лояльных генералов основывать свое решение на значениях "отступить", ..., "отступить", если каждый лояльный генерал отправил значение "атаковать". Поэтому у нас есть следующее требование для каждого i:
2. Если i-й генерал лоялен, то значение, которое он отправляет, должно использоваться каждым лояльным генералом как значение v(i).

Мы можем переписать условие I как условие, что для каждого i (независимо от того, лоялен ли i-й генерал), 1'. Любые два лояльных генерала используют одно и то же значение v(i). Условия 1' и 2 являются условиями на единственное значение, отправленное i-м генералом. Мы можем, следовательно, ограничить наше рассмотрение проблемой того, как один генерал отправляет свое значение другим. Мы формулируем это в терминах командующего генерала, отправляющего приказ своим лейтенантам, получая следующую задачу.

IC2. Если командующий генерал лоялен, то каждый лояльный лейтенант подчиняется приказу, который он отправляет.

Условия IC1 и IC2 называются условиями интерактивной согласованности. Обратите внимание, что если командир лоялен, то IC1 следует из IC2. Однако командир не обязательно должен быть лоялен. Чтобы решить нашу исходную задачу, i-й генерал отправляет свое значение v(i), используя решение проблемы византийских генералов, чтобы отправить приказ "используйте v(i) как мое значение", при этом другие генералы действуют как лейтенанты.

1. Проблема византийских генералов кажется обманчиво простой. Ее сложность указывает на удивительный факт, что если генералы могут отправлять только устные сообщения, то ни одно решение не будет работать, если более двух третей генералов не лояльны. В частности, с только тремя генералами ни одно решение не может работать в присутствии одного предателя. Устное сообщение — это сообщение, содержание которого полностью контролируется отправителем, поэтому предательский отправитель может передать любое возможное сообщение. Такое сообщение соответствует типу сообщения, который компьютеры обычно отправляют друг другу. В разделе 4 мы рассматриваем подписанные, письменные сообщения, для которых это не так.

Теперь мы показываем, что с устными сообщениями ни одно решение для трех генералов не может справиться с одним предателем. Для простоты мы рассматриваем случай, в котором единственные возможные решения — это "атаковать" или "отступить". Сначала рассмотрим сценарий, изображенный на рисунке 1, в котором командир лоялен и отправляет приказ "атаковать", но лейтенант 2 является предателем и сообщает лейтенанту 1, что он получил приказ "отступить". Чтобы IC2 было выполнено, лейтенант 1 должен подчиниться приказу атаковать. Теперь рассмотрим другой сценарий, показанный на рисунке 2, в котором командир является предателем и отправляет приказ "атаковать" лейтенанту 1 и приказ "отступить" лейтенанту 2. Лейтенант 1 не знает, кто предатель, и он не может сказать, какое сообщение командир на самом деле отправил лейтенанту 2. Следовательно, сценарии на этих двух картинках выглядят совершенно одинаково для лейтенанта 1. Если предатель последовательно лжет, то у лейтенанта 1 нет способа различить эти две ситуации, поэтому он должен подчиниться приказу "атаковать" в обоих случаях. Следовательно, всякий раз, когда лейтенант 1 получает приказ "атаковать" от командира, он должен ему подчиниться.

Проблема византийских генералов

. Используя этот результат, мы можем показать, что ни одно решение с менее чем 3m + 1 генералами не может справиться с m предателями. Доказательство идет методом противоречия - мы предполагаем, что такое решение существует для трех или более генералов, поскольку проблема тривиальна для двух генералов. ACM Transactions on Programming Languages and Systems, Т. 4, № 3, Июль 1982.