Aula 19 - Generais bizantinos

Wednesday, May 18, 2016 13:48

Neste tópico consideramos falhas **bizantinas**. Processos com falha bizantina têm comportamento arbitrário.

Uma aplicação prática disso é **detecção de intrusão**.

O problema

Cidade medieval cercada por um exército.

- Unidades do exército podem **atacar** ou **recuar**.
- Cada unidade tem um **general**.
- Um dos generais é o **comandante**.

Premissas:

- O comandante envia uma ordem para cada general comandado.
- Um general **traidor** pode enviar, aleatoriamente, qualquer ordem (atacar ou recuar).
- As mensagens são entregues corretamente ao destino sem modificações.

Objetivo: atingir duas condições:

IC1: Todos os generais **leais** executam a mesma ação (mesmo que o comandante seja traidor!)

IC2: Se o comandante é leal, então todo comandado leal obedece sua ordem.

(IC = Interactive Consistency)

O algoritmo dos generais bizantinos (GenBiz) é especificado de forma recursiva e recebe como parâmetro o número de traidores. São N generais.

Algoritmo GenBiz (0)

(1) O comandante a ordem para (N-1) comandados

(2) Cada comandado executa a ordem recebida do comandante

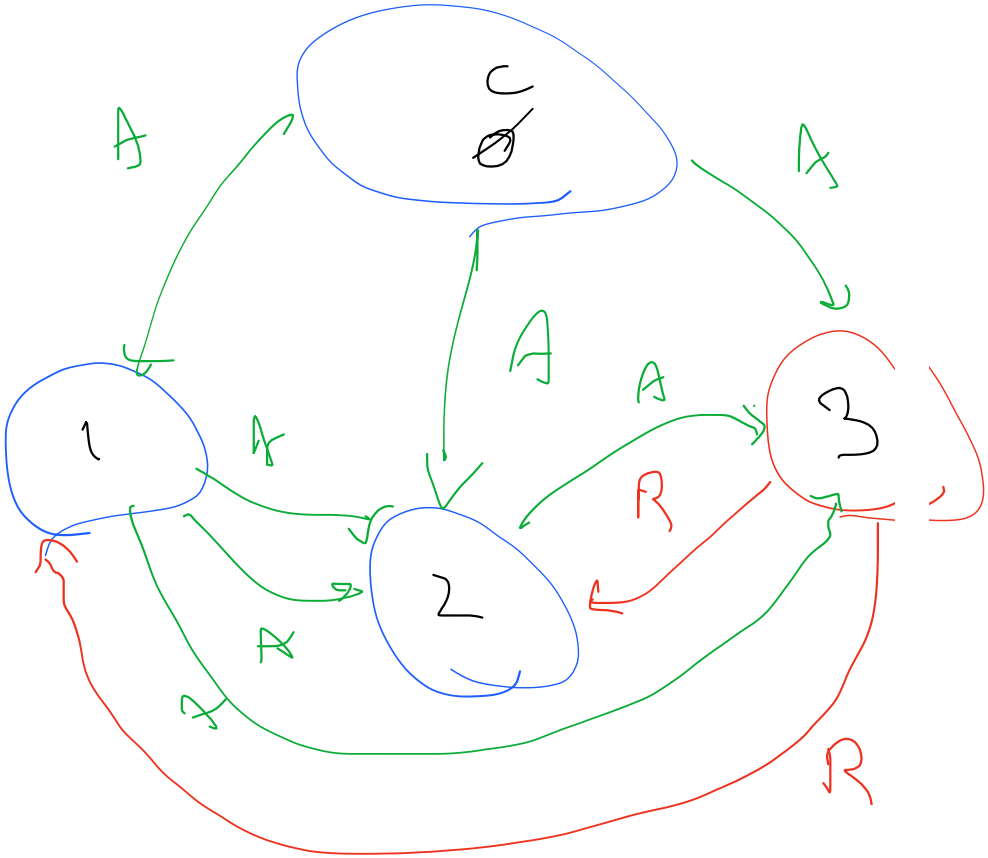
Algoritmo GenBiz $(m), m > 0$

(1) O comandante envia a ordem para cada comandado

(2) Seja v_i o valor da ordem recebida pelo comandado i.
Em seguida, o comandado i se transforma em comandante para a ordem v_i executando GenBiz$(m-1)$ para enviar a ordem aos demais comandados (não manda para comandante original)

(3) Para cada i, considere para $j \neq i$ o valor que o nodo j recebeu do nodo j no passo anterior. O nodo i executa: a

maioria entre $(v_0, v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_n)$.



O nodo 0, comandante leal, executa atacar.
O nodo 1, leal, executa MAIORIA(A, A, R): atacar
O nodo 2, leal, executa MAIORIA(A, A, R): atacar
O nodo 3, traidor, executa arbitrariamente!

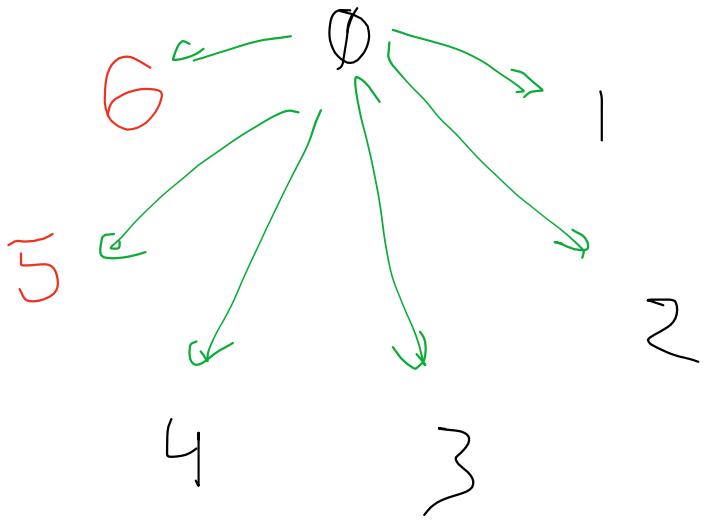
Em síntese:

- Em GenBiz(m), comandante envia ordem para $N-1$ comandados.
- Em GenBiz($m-1$), cada comandante envia ordem para $N-2$ comandados.
- Em GenBiz($m-2$), cada comandante envia ordem para $N-3$ comandados.
- Até chegar em GenBiz(0)

Vamos provar a seguir que, para funcionar, o algoritmo deve ser executado com MAIS de $\frac{2}{3}$ d de generais leais.

1 traidor → $4 = N$
2 traidores → $7 = N$
3 traidores → $10 = N$
Etc.

Antes das provas, exemplo para 2 traidores (traidores sempre enviam R):



Vamos executar:
GenBiz(2)
GenBiz(1)
GenBiz(0)

Quais os valores recebidos pelo nodo 2?

Passo	Valoresssssssssss	Valoresssssssssss	Valoresssssssssss	Valoresssssssssss	Valore	esssssssssss
GB(2)	$v_0 = A$					
GB(1)	$v_{1,0} = A$	$v_{3,0} = A$	$v_{4,0} = A$	$v_{5,0} = R$	$v_{6,0} =$	$= R$
GB(0)	$v_{3,1,0} = A$ $v_{4,1,0} = A$ $v_{5,1,0} = R$	$v_{1,3,0} = A$ $v_{4,3,0} = A$ $v_{5,3,0} = R$	$v_{1,4,0} = A$ $v_{3,4,0} = A$ $v_{5,4,0} = R$	$v_{1,5,0} = R$ $v_{3,5,0} = R$ $v_{4,5,0} = R$	$v_{1,6,0}$ $v_{3,6,0}$ $v_{4,6,0}$	$= R$ $= R$ $= R$

	$v_{6,1,0} = R$	$v_{6,3,0} = R$	$v_{6,4,0} = R$	$v_{6,5,0} = R$	$v_{5,6,0} = R$

Agora executa MAIORIA (A, A, A, A, R, R) = ATACAR

CUIDADO: Fazer uma maioria única para TODAS as mensagens dá errado!
10 As e 16 Rs.

Ordem default é usada no caso de empate: RECUAR.

Um exercício: