Tópicos em Redes de Computadores

Os Generais Bizantinos

Prof. Elias P. Duarte Jr.
Universidade Federal do Paraná (UFPR)
Departamento de Informática
www.inf.ufpr.br/elias/topredes

Sumário

- Os Generais Bizantinos originais:

  Leslie Lamport, Robert E. Shostak, Marshall C. Pease, “The Byzantine Generals Problem,” *ACM Trans. Program. Lang. Syst*, Vol. 4, No. 3, pp. 382–401, 1982.
- O problema da “consistência interativa”
- Limites no número de traidores
- O algoritmo de Lamport
- Exercícios

Era uma vez…

- Uma cidade medieval, cercada por uma impressionante muralha

Infelizmente sob ataque...

- O exército bizantino está atacando nossa cidade medieval

Infelizmente sob ataque...

- O exército bizantino está atacando nossa cidade medieval
- Múltiplas unidades do exército estão ao redor da cidade
- Cada unidade é comandada por um general
- Entre eles há generais traidores
- Um comandante é o chefe maior que dita as leis que os generais vão executar: atacar ou recuar

Espec.Sistema Distribuído:

- Considere um sistema distribuído assíncrono sujeito a falhas bizantinas
  - há processos que apresentam comportamento “arbitrário” → pode trocar o conteúdo de uma msg
  - um processo falho pode também mandar mensagens diferentes para destinatários diferentes
- Canais de comunicação perfeitos, além disso: mensagens assinadas (autenticação)
- Topologia *fully connected*, cada processo pode comunicar diretamente com qualquer outro

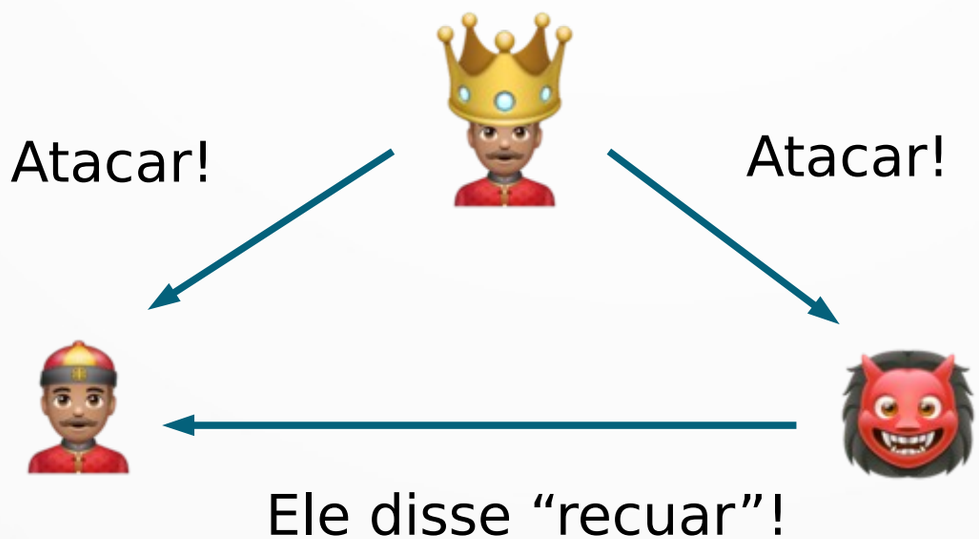
Propriedades IC

- Tendo em vista que os próprios generais sabem que há traidores entre eles...
- ... o objetivo é garantir as 2 seguintes propriedades (IC – *Interactive Consistency*):

1) (IC1) Todos os generais leais executam a mesma ação (atacar ou recuar)
2) (IC2) Se o comandante é leal, todos os generais leais devem executar sua ordem (atacar ou recuar)

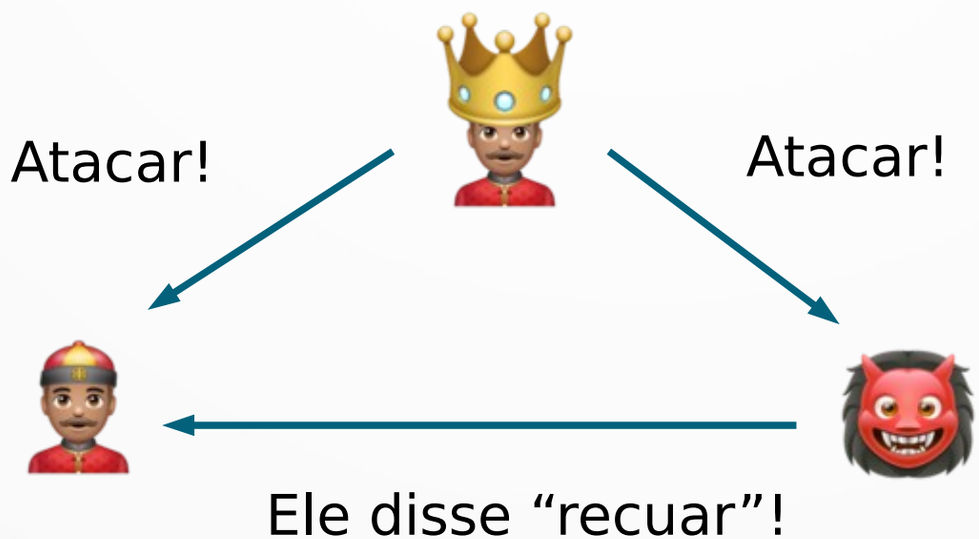
Será que é sempre possível?

- Veja este caso em que há um total de 3 generais sendo 1 deles traidor (e 2 leais, portanto):



Será que é sempre possível?

- Veja este caso em que há um total de 3 generais sendo 1 deles traidor (e 2 leais, portanto): impossível garantir nem IC1, nem IC2!



Solução com Mensagens Orais

- No caso anterior vimos que para N=3 sendo m=1 traidor não é possível garantir as propriedades
- Após vermos o algoritmo, vamos provar que para suportar m falhas N = 3m+1 (no mínimo)
- O algoritmo é chamado no artigo original de “uma solução com mensagens orais”

Antes do Algoritmo

- No algoritmo os generais vão comunicar entre si para decidir o que fazer
- Inicialmente o comandante manda a ordem inicial, que os generais vão comunicar entre si
- Um traidor pode ficar em silêncio (não mandar mensagem) mas isso é detectado
- É preciso definir uma ordem default: em caso de ordem não recebida ou empate, a decisão é por recuar

O Algoritmo GenBiz

- O algoritmo inicialmente é definido para m = zero traidores :-)

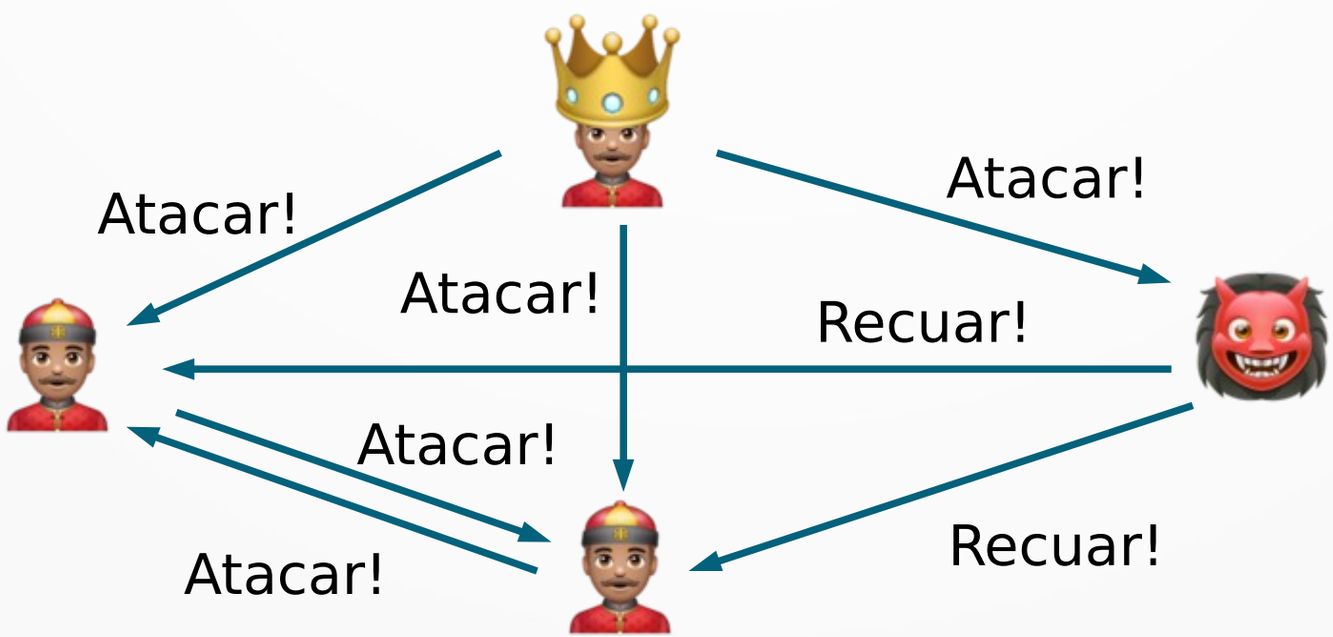
```
Algoritmo GenBiz(m=0)
(1)O comandante envia a ordem para N-1
comandados
(2)Cada comandado e o comandante
executam a ordem recebida
```

Agora GenBiz(m), m>0

Algoritmo GenBiz(m, m>0)
(1)O comandante envia a ordem para os comandados
(2)Para cada i, seja Vi o valor que o comandado i recebeu do comandante: o comandado i vira comandante executando GenBiz(m-1) para os demais comandados
(3)Ao final: o comandado i vai ter ordens de todos os demais generais e executa Maioria(V0, V1, V2, …, V_{N-1})

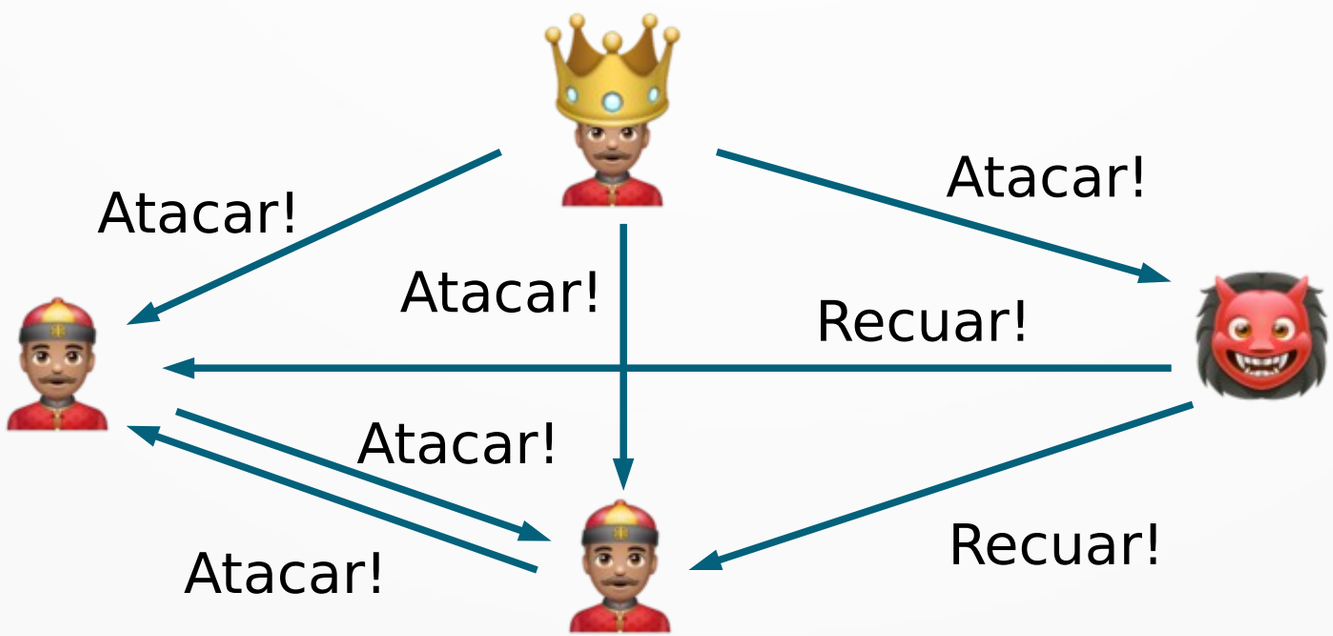
Entendendo o Algoritmo

- Veja um exemplo de execução para N=4, m=1 e o comandante leal
- Vamos sempre usar o identificador zero para o comandante



Entendendo o Algoritmo

- Neste exemplo de execução tudo começa com GenBiz(1) sendo executado pelo comandante
- Em seguida os demais generais executam GenBiz(0) – (sem msgs recebidas pelo traidor)

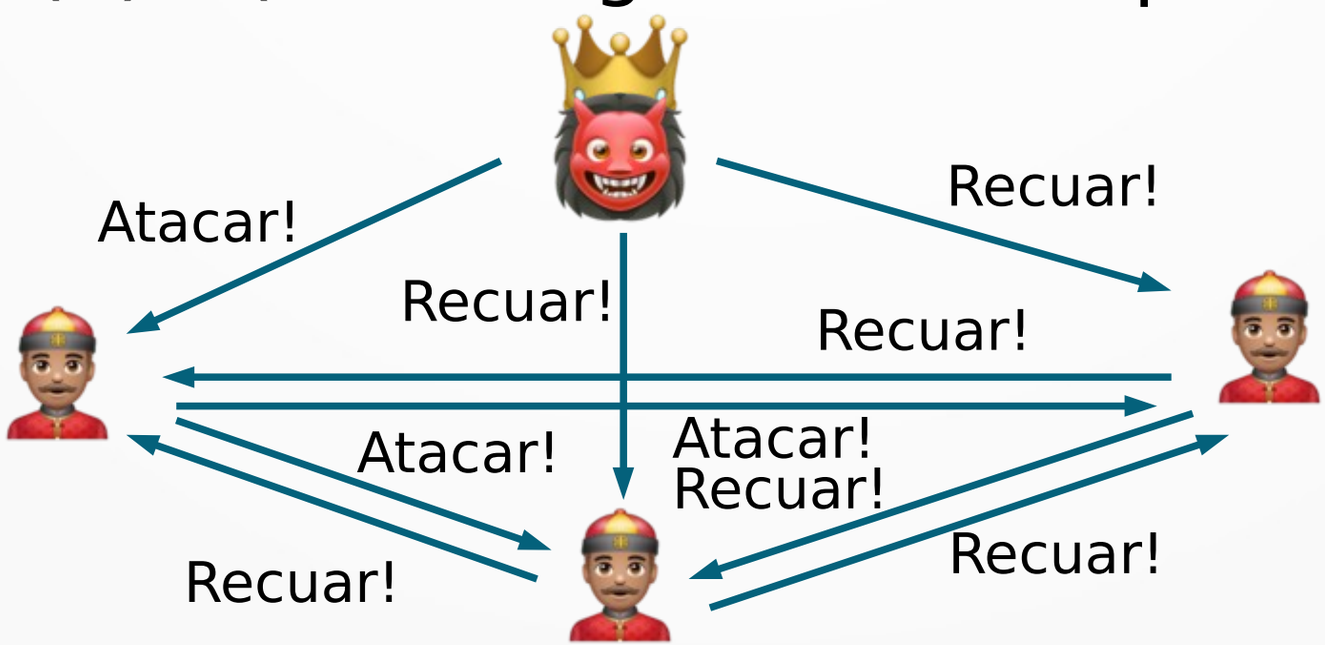


Entendendo o Algoritmo

- Seja V_0 a ordem original recebida do comandante (0 - zero); $V_0 = A$
  - Os identificadores sendo 1, 2 e 3 da esquerda para a direita
- Seja Vij a ordem que o general i recebeu do general j: no exemplo, apenas para os leais:
- General 1: $V_{20} = A$; $V_{30} = R$; Maioria(A,A,R) = A
- General 2: $V_{10} = A$; $V_{30} = R$; Maioria(A,A,R) = A

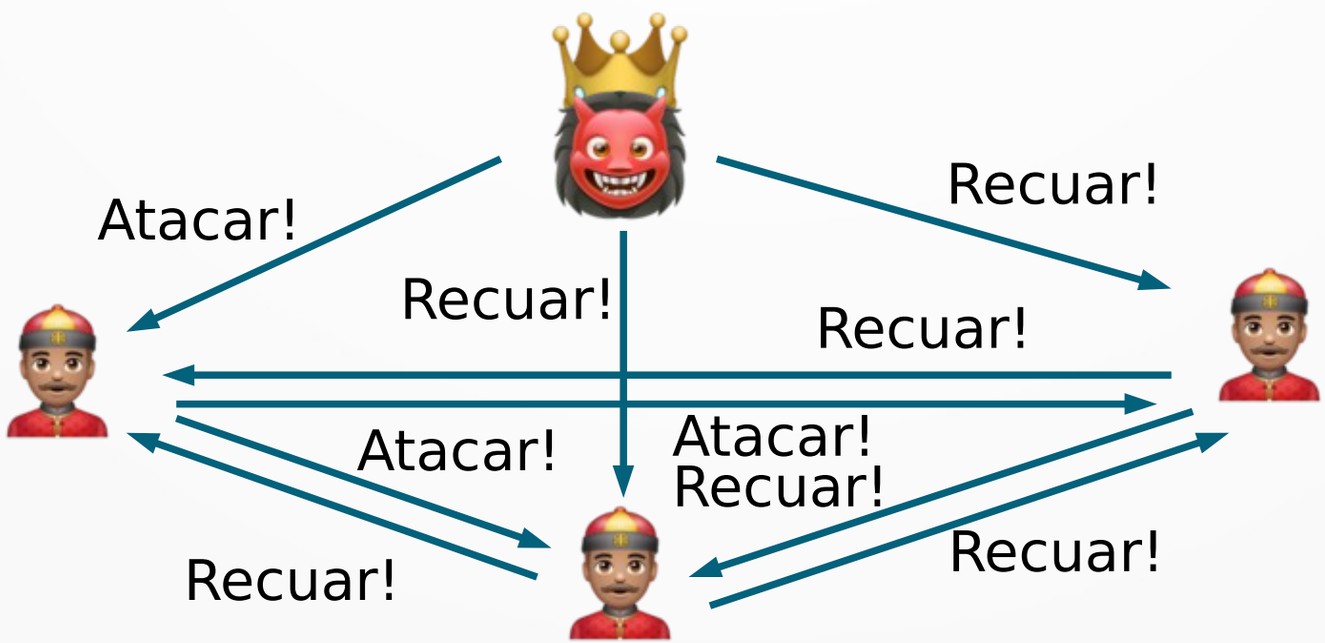
Agora com Comandante Traidor

- Neste exemplo o comandante manda Atacar! para 1, e Recuar! para 2 e 3
- Em seguida os demais generais executam GenBiz(0) – (sem msgs recebidas pelo traidor)



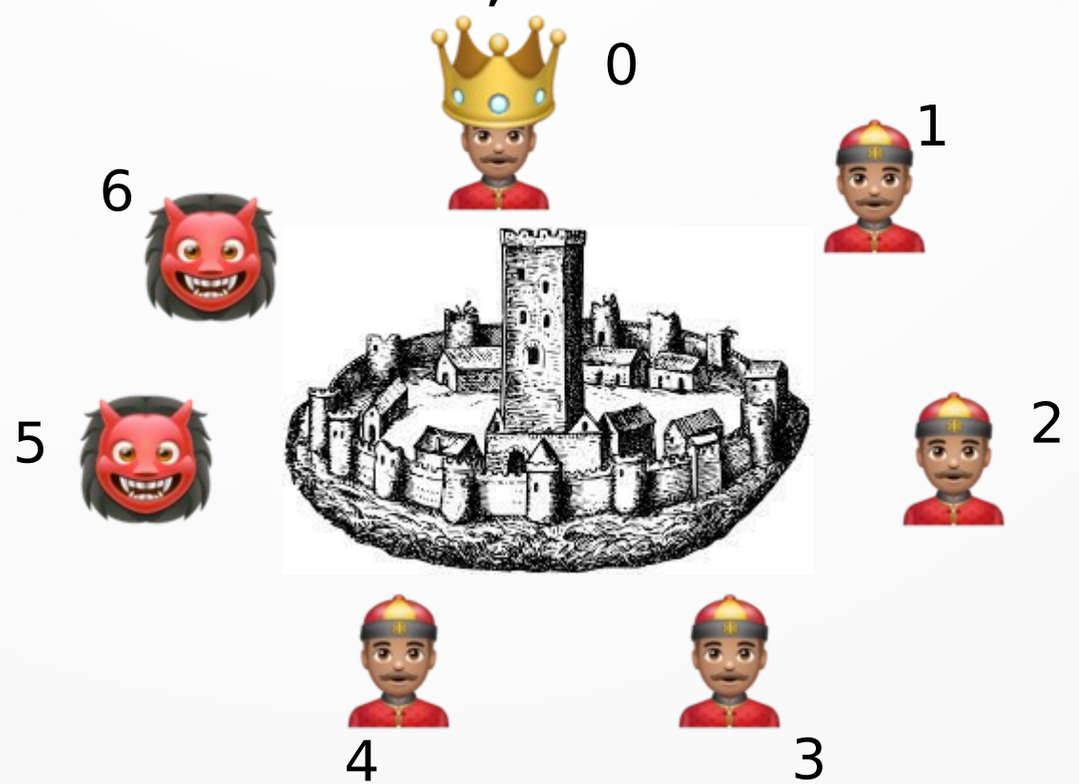
Agora com Comandante Traidor

- Veja como as maiorias executadas por todos os generais (que são leais) são idênticas!
- Todos executam Maioria sobre R, R, A



Em Seguida: 2 Traidores

- Considere um sistema com 2 generais traidores
- Neste caso m=2, portanto N = 2*m+1 = 7
- Considere que a ordem é A, os traidores só mandam R



2 traidores: 5 e 6

- O comandante leal executa GenBiz(2) enviando V_0=A para todos
- Todos recebem e executam GenBiz(1) com os seguintes valores: V_{10}=A, V_{20}=A, V_{30}=A, V_{40}=A, V_{50}=R, V_{60}=R
- Qual a ordem executada pelo General 2?
- V1: V_{10}=A, V_{310}=A, V_{410}=A, V_{510}=R, V_{610}=R → Maioria: A
- V3: V_{30}=A, V_{130}=A, V_{430}=A, V_{530}=R, V_{630}=R → Maioria: A
- V4: V_{40}=A, V_{140}=A, V_{340}=A, V_{540}=R, V_{640}=R → Maioria: A
- V5: V_{50}=R, V_{150}=R, V_{350}=R, V_{450}=R, V_{650}=R → Maioria: R
- V6: V_{60}=R, V_{160}=R, V_{360}=R, V_{460}=R, V_{560}=R → Maioria: R
- Maioria(V0,V1,V3,V4,V5,V6) = Maioria(A,A,A,A,R,R) = ATACAR!

Exercício

- Considere a execução do algoritmo de Lamport dos Generais Bizantinos para m=2 traidores
- O general 3 bem como o comandante (0 – zero) são traidores
- Eles estão mancomunados e mandam “Atacar” para 1 e 2 & “Recuar” para 4, 5 e 6
- Mostre a ordem executada pelo General 2

Conclusão

- Nesta aula estudamos o algoritmo dos Generais Bizantinos de Lamport
- Executamos para 1 e 2 traidores
- Na próxima aula: vamos ver a prova de que realmente são necessários N = 3m + 1 generais no total (no mínimo) para tolerar m falhas bizantinas

Obrigado!

Lembrando: a página da disciplina é:
https://www.inf.ufpr.br/elias/topredes