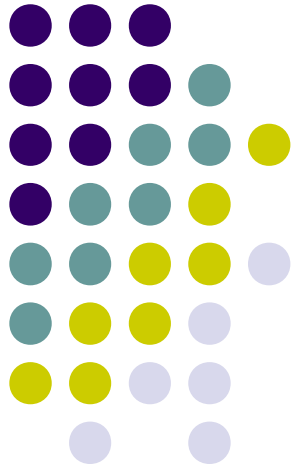
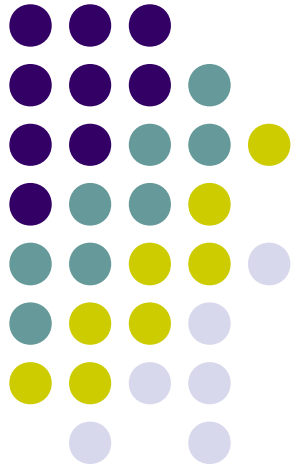
Sistemas Distribuídos

Professora: Ana Paula Couto
DCC 064

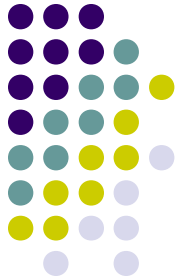


Tolerância a Falha

Capítulo 8



Agenda



- Conceitos Básicos
- Modelos de Falhas
- Mascaramento de Falhas por Redundância
- Estratégias de Tolerâncias a Falha
- Resiliência de Processos

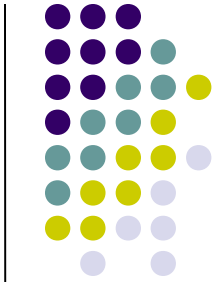
Conceitos Básicos

- Existe uma forte relação entre ser tolerante a falhas e sistemas confiáveis
- Confiabilidade abrange uma série de requisitos úteis para sistemas distribuídos (Kopetz e Veríssimo, 1993):
  - Disponibilidade
  - Confiabilidade
  - Segurança
  - Capacidade de Manutenção

Disponibilidade

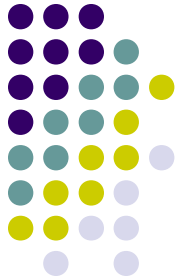
- Propriedade de um sistema estar pronto para ser usado imediatamente
- Probabilidade do sistema estar funcionando corretamente em qualquer momento determinado e estar disponível para executar suas funções em nome de seus usuários
- Alta Disponibilidade →Mais provável de estar funcionando em dado instante de tempo

Confiabilidade



- Propriedade de um sistema poder funcionar continuamente sem falha
- É definida em termos de um intervalo de tempo em vez de um instante de tempo
- Alta confiabilidade → Mais provável de continuar a funcionar sem interrupção durante um período de tempo relativamente longo
- Se um sistema ficar fora do ar por um milissegundo a cada hora, terá uma disponibilidade de mais de 99.99999%, mas sua confiabilidade ainda será muito baixa.

Segurança

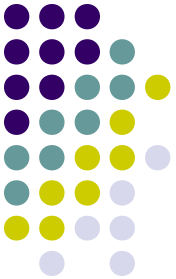


- Se um sistema deixar de funcionar corretamente durante um certo tempo, nada de catastrófico acontecerá
- Ex.: Sistemas de controle de processos usados em usinas de energia nuclear

Capacidade de Manutenção

- Facilidade com que um sistema que falhou possa ser consertado
- Sistemas de alta capacidade de manutenção também pode mostrar alto grau de disponibilidade, em especial se as falhas puderem ser detectadas e reparadas automaticamente

Conceitos Básicos

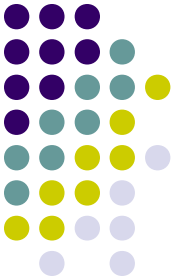


- Defeito: Sistema não pode cumprir o que foi especificado ou prometido
- Erro: Estado de um sistema causado por uma falha
  - Meio de transmissão errado ou ruim pode danificar pacotes → fácil reconhecer a falha
  - No entanto, alguns erros de transmissão podem ser causados por más condições atmosféricas, como redes sem fio → difícil remover a falha

Tipos de Falhas

- Transiente
  - Ocorre uma vez e depois desaparece
  - Se a operação for repetida, a falha não acontecerá novamente
- Intermitente
  - Ocorre e desaparece por “sua própria vontade”. Ex.: conector com problemas
  - Difícil de diagnosticar
- Permanente:
  - Continua a existir até que o componente faltoso seja substituído Exs: bugs de software, chips queimados

Modelos de Falhas Cristian (1991); Hadzilacos e Toueg (1993)



Tipo de falha	Descrição
Falha por queda	O servidor pára de funcionar, mas estava funcionando corretamente até parar.
Falha por omissão	O servidor não consegue responder a requisições que chegam
Omissão de recebimento	O servidor não consegue receber mensagens que chegam
Omissão de envio	O servidor não consegue enviar mensagens
Falha de temporização	A resposta do servidor se encontra fora do intervalo de tempo
Falha de resposta	A resposta do servidor está incorreta
Falha de valor	O valor da resposta está errado
Falha de transição de estado	O servidor se desvia do fluxo de controle correto
Falha arbitrária	Um servidor pode produzir respostas arbitrárias em momentos arbitrários

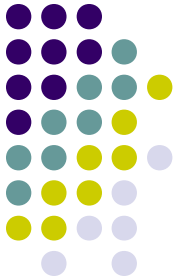
Tabela 8.1 Diferentes tipos de falhas.

Mascaramento de Falha por Redundância

Técnica para mascarar falhas

- Redundância de informação
  - Bits extras são adicionados para permitir recuperação de bits deteriorados
- Redundância de tempo
  - Uma ação é realizada e, então, se for preciso, ela é executada novamente.
- Redundância física
  - Componentes físicos replicados são usados

Estratégias de Tolerância a Falhas



- Resiliência de Processos
  - Replicação de processos em grupos
  - Grupos Simples ou Hierárquicos
- Comunicação Confiável Cliente-Servidor
  - Falhas de Comunicação
  - Canal de Comunicação pode exibir falhas por queda, por omissão, arbitrárias
  - TCP(ponto-a-ponto); RPC
- Comunicação Confiável de Grupo
  - Como implementar entrega confiável de mensagens a todos os processos?
- Comprometimento Distribuído
  - Envolve a realização de uma operação por cada membro de um grupo de processos ou por absolutamente nenhum
  - Exs: Entrega de msg.