Sistemas Distribuídos

Rui Raposo

Saturday 23rd May, 2020
21:30

1 Modelos Fundamentais

Os sistemas distribuídos podem ainda ser analisados segundo **3 aspetos travensais a todos os sistemas**:

- Modelo de Interação (ou de sincronismo);
- Modelo de Falhas (ou avarias);
- Modelo de Segurança.

1.1 Modelo de Interação

Interação é a ação (comunicação e sincronização) entre as partes para realizar um qualquer trabalho.

É afetada por **dois** aspetos:

1. Performance dos canais de comunicação;
2. Inexistência de um tempo global.

1.1.1 Performance dos canais de comunicação

- **Latência** – Intervalo de tempo que medeia entre o início da transmissão de uma mensagem por um processo e o início da sua receção pelo outro processo.
  Depende de :
  - Tempo requerido pelo sistema operativo em ambos os lados da comunicação;
  - Demora no acesso aos recursos da rede;
  - Demora (*delay*) de transmissão pela rede.
- Largura de banda (*bandwidth*) – Total de informação que pode ser transmistida pela rede num dado intervalo de tempo;

- Jitter – Variação no tempo necessário para enviar grupos de mensagens consecutivos constituintes de uma informação transmitida de um ponto para outro na rede (**importante na transmissão de som e imagem**).

1.1.2 Inexistência de um tempo global

- Cada computador tem um relógio interno;
- Cada relógio tem um ***drift*** (um desvio) do **tempo de referência**;
- Os *drifs* de dois relógios distintos são também distintos (o que significa que entre eles o tempo será sempre divergente).

Uma solução passa por obter o tempo fornecido por GPS e enviar aos participantes do sistema distribuído, mas existe um **problema** : o envio dessa mensagem!

Duas variantes no modelo de interação:

1.1.2.1 Sistemas distribuídos síncronos .

Sistemas onde podem existir limites máximos de tempo conhecidos para:

- Tempos de execução dos processos;
- Atrasos na comunicação;
- Variação;
- O tempo necessário para executar cada passo de um processo tem um limite inferior e um limite superior conhecidos;
- Cada mensagem transmitida por um canal é recebida dentro de um limite de tempo conhecido;
- Cada processo tem um relógio cujo desvio máximo para o tempo de referência é conhecido.

Podem definir-se *timeouts* para detetar falhas.

Dificuldade em contrar os limites para os tempos, mais difícil ainda, provar a sua correção.

1.1.2.2 Sistemas distribuídos assíncronos .

Não possui limites para:

- Tempo de execução dos processos – cada passo de execução pode levar um tempo arbitrariamente longo;
- Tempo de transmissão de mensagems – uma mensagem pode chegar rapidamente ou demorar dias;

- O desvio para o tempo de referência pode ser um qualquer;

Exemplos de um sistema assíncrono: Internet.
Como lidar com longos tempos de espera:

- O sistema pode avisar o utilizador que o tempo de espera pode ser longo e solicitar uma alternativa;
- O sistema pode dar oportunidade ao utilizador para fazer outras coisas;

Este tipo de sistema, **pode levar a problemas da ordenação de eventos**.

1.2 Modelo de Avarias

Uma avaria é qualquer alteração do comportamento do sistema em relação ao esperado.

Avarias podem acontecer e atingir **processos ou canais de comunicação**.

1.2.1 Tipos de Avarias

- Avarias por omissão;
- Avarias arbitrárias;
- Avarias em tempo.

1.2.1.1 Avarias por omissão.

- Quando um processo deixa de funcionar em algum ponto do sistema distribuído;
- Quando o canal de comunicação falha.

Tipos de avarias por omissão:

- *Fail-stop* – o processo bloqueou (*crashed*) e esse facto pôde ser detetado por outros processos.
  Crash – o processo aparentemente bloqueou, mas não é possível garantir que apenas deixou de responder por estar muito lento, ou porque as mensagens que enviou não chegaram;
- *Omission* – uma mensagem colocada no buffer de emissão nunca chega ao buffer de recepção (pode ocorrer por falta de espaço no buffer);
- *Send-omission* – uma mensagem perde-se entre o emissor e o buffer de emissão;
- *Receive-omission* – uma mensagem perde-se entre o buffer de receção e o recetor.

1.2.1.2 Avarias arbitrárias.

- Qualquer tipo de erro pode aparecer:
  1. Nos processos:
     - Processo não responde;
     - Estado do processo é corrompido;
     - Responde de forma errada;
     - Responde fora de tempo.
  2. Nos canais de comunicação.
     - Mensagens corrompidas;
     - Mensagens não entregues;
     - Mensagens duplicadas;
     - Mensagens inexistentes são entregues.

São raras de ocorrer nos canais de comunicação porque o software de comunicação protege as mensagens com somas de verificação (*checksums*), números de sequenciamento, etc.

1.2.1.3 Avarias em tempo.

- Ocorrem quando o tempo limite para um evento ocorrer é ultrapassado;
- Em sistemas eminentemente síncronos é um indicativo seguro de falha;

1.3 Modelo de Segurança

- Proteção das entidades do sistema, processo/utilizador;
- **Direitos de acesso** especificam que **entidades** podem aceder, e de **que forma, a que recursos**.
- O servidor é responsável por verificar a **identidade** de quem fez o pedido, e verificar se essa entidade tem **direitos de acesso** para realizar a **operação pretendida**;
- O cliente deverá verifica a identidade de **quem lhe enviou a resposta**, para ver se a resposta veio da entidade esperada.

Que ameaças?
Suponde que existe um processo inimigo capaz de:

- Enviar qualquer mensagem para qualquer processo;
- Intercetar (ler/copiar) qualquer mensagem trocada entre 2 processos.

Classificação das ameaças:

- Aos processos;
- À comunicação;
- Negação de serviço.

1.3.1 Ataques a processos

- Ao projetar um servidor, ter consciência de que:
  - Os protocolos de rede não oferecem proteção para que o servidor saiba a identidade do emissor (IP inclui o endereço do computador origem da mensagem, mas um processo inimigo pode forjar esse endereço);
  - Um cliente também não dispõe de métodos para validar as respostas de um servidor;

1.3.2 Ataques a canais de comunicação

- Um processo inimigo pode copiar, alterar ou injetar mensagens numa rede;
- A comunicação pode ser violada por processos que observam a rede à procura de mensagens significativas (essas mensagens podem posteriormente ser reveladas a terceiros).

1.3.3 Negação de Serviço

Um processo intruso **captura** uma mensagem de solicitação de serviço e **retransmite-a** inúmeras vezes ao destinatário, fazendo-o executar sistematicamente o mesmo serviço e **ultrapassando** a sua capacidade de resposta. Como lidar com estas ameaças? **Utilização de canais seguros**.

Canal Seguro – Canal utilizado para comunicação entre dois processos com as seguintes características:

- Cada processo pode identificar com 100 por cento de confiança a entidade responsável pela execução de outro processo;
- As mensagens que são transferidas de um processo para outro são garantidas do ponto de vista da integridade e da privacidade;
- As mensagens têm garantia de não repetibilidade ou reenvio por ordem distinta (cada mensagem inclui um tempo físico ou lógico).