MATA88 - Fundamentos de Sistemas Distribuídos

Professor: Raimundo José de Araújo Macêdo
Aluno: Reynan da Silva Dias Paiva

Questão 1. Como o mascaramento de falhas é abordado em sistemas distribuídos quando se trata de garantir a confiabilidade da comunicação ?

2.4 Modelos Fundamentais

Um modelo fundamental para sistemas distribuídos deve considerar interação, falha e segurança. Os sistemas são compostos por processos que se comunicam através de mensagens, enfrentando desafios como atrasos na comunicação, falhas nos computadores e na rede, e ataques de agentes internos e externos. A precisão da coordenação é limitada pelos atrasos de comunicação. O modelo de falha classifica e define falhas, enquanto o modelo de segurança identifica formas de ataques. Um modelo fundamental para sistemas distribuídos deve considerar interação, falha e segurança. Os sistemas são compostos por processos que se comunicam através de mensagens, enfrentando desafios como atrasos na comunicação, falhas nos computadores e na rede, e ataques de agentes internos e externos. Um modelo fundamental para sistemas distribuídos deve considerar interação, falha e segurança. Os sistemas são compostos por processos que se comunicam, enfrentando desafios como atrasos na comunicação, falhas nos computadores e na rede, e ataques de agentes internos e externos.

2.4.1 Modelo de interação

Em sistemas distribuídos, a interação envolve muitos processos complexamente interligados, como servidores cooperando para fornecer um serviço ou conjuntos de processos peer-to-peer. Um algoritmo distribuído define os passos a serem executados por cada processo, incluindo a transmissão de mensagens. O desempenho da comunicação, um fator crítico, é limitado. Latência, largura de banda e jitter são considerações essenciais. A latência, por exemplo, é o atraso entre o início da transmissão de uma mensagem e o início da recepção pelo processo destinatário. Cada computador possui seu próprio relógio interno, o que torna difícil manter uma noção global de tempo única. Existem estratégias

para corrigir os tempos em relógios de computador, como o uso de receptores de rádio para obter leituras de tempo GPS ou sincronização entre computadores. Existem duas variantes do modelo de interação em sistemas distribuídos. Os sistemas distribuídos síncronos têm limites conhecidos para o tempo de execução de cada etapa de um processo, a recepção de mensagens e a taxa de desvio do relógio. Já os sistemas distribuídos assíncronos não fazem nenhuma consideração sobre os intervalos de tempo envolvidos em qualquer tipo de execução. A execução de um sistema distribuído pode ser descrita em termos da ocorrência e ordem dos eventos, mesmo na ausência de uma noção global de tempo. Às vezes, é necessário tratar o problema de demoras e atrasos de execução. Por exemplo, embora a Web nem sempre possa fornecer uma resposta específica dentro de um limite de tempo razoável, os navegadores são projetados para permitir que os usuários façam outras coisas enquanto esperam.

2.4.2 Modelo de Falhas

O modelo de falhas em sistemas distribuídos considera falhas de processos e canais de comunicação. As falhas podem ser por omissão, arbitrárias ou de temporização. As falhas por omissão incluem falhas de processo (quando um processo para inesperadamente) e falhas de comunicação (quando uma mensagem se perde no caminho). Falhas arbitrárias são as piores, incluindo comportamentos inesperados nos processos ou na comunicação. Falhas de temporização incluem atrasos na resposta ou na entrega de mensagens. Mascaramento de falhas e confiabilidade na comunicação são estratégias para lidar com falhas.

2.4.3 Modelo de Segurança

O modelo de segurança em sistemas distribuídos visa proteger processos, canais de comunicação e objetos, garantindo autenticidade, integridade e privacidade das interações. Isso é alcançado através de direitos de acesso aos objetos e canais seguros baseados em criptografia e autenticação. As ameaças incluem ataques aos processos, canais de comunicação, negação de serviço e código móvel. A eficácia das medidas de segurança deve ser ponderada em relação às ameaças identificadas.