Disciplina: Sistemas Distribuídos
Professora: Ana Cristina Barreiras Kochem Vendramin

Avaliação (valor 2,0)
Protocolo de Consenso,
Comunicação em Grupo e Segurança.

Um problema de consenso requer um acordo entre um número de processos para um único valor. Desses processos, alguns podem falhar ou não serem confiáveis. Então, protocolos de consenso devem ser tolerante a falhas. Em um protocolo de consenso, os processos devem, de alguma forma, fornecer seus valores candidatos, se comunicar uns com os outros e entrar num acordo em relação a um único valor. Um caso especial do problema de consenso, chamado de **consenso binário,** restringe o número de valores na entrada e, consequentemente, o domínio da saída para um único dígito binário {0,1}. Um exemplo de protocolo de consenso binário tolerante a falhas é o algoritmo *Phase King* proposto por Berman e Garay.

Siga as instruções abaixo para desenvolver e testar o protocolo de consenso binário Phase-King.

1. Considere o algoritmo apresentado em: https://www.cs.uic.edu/~ajayk/Chapter14.pdf (slide 17);
2. Considere um conjunto de cinco processos (n = 5), no máximo um processo malicioso será tolerado (f = 1), duas fases (com duas rodadas em cada fase) e identificação única para cada nó no intervalo [1,5];
3. Ao invés da comunicação broadcast, utilize a comunicação em grupo (*multicast*) para os processos se conhecerem, trocarem suas chaves públicas e trocarem as mensagens necessárias para chegarem em um consenso seguindo o algoritmo Phase King. Lembrando que o protocolo desenvolvido deve satisfazer quatro propriedades: término (todo processo não defeituoso deve escolher um valor), validação (se todos os processos propuserem um mesmo valor v, então todos os processos não defeituosos devem escolher v), integridade (todo processo não defeituoso deve escolher no máximo um valor, e se ele escolher algum valor v, então v deve ter sido proposto por algum processo), acordo

(todo processo não-defeituoso deve concordar com o mesmo valor) (valor 1,5).

4. O rei de cada fase deve usar sua chave privada para assinar digitalmente sua mensagem e o receptor deve checar a autenticidade dessa mensagem com a chave pública do rei correspondente (valor 0,5).
5. É obrigatório documentar todo o código e a equipe é de dois programadores.

Profª. Ana Cristina Barreiras Kochem Vendramin
DAINF/UTFPR