Sistemas Distribuídos - MIEEC **16 de Novembro de 2016**
Teste (Com consulta de "cheat sheet") **Duração: 120 min**

---

1. **Justifique todas as respostas.**

2. **Responda às perguntas 1 e 2 numa folha e às restantes noutra.**

---

1 [3v] - Sobre sistemas distribuídos.
1.1- Diga por que razão se faz **sincronização de relógios lógicos** em sistemas distribuídos e dê um exemplo de aplicação em que esse tipo de sincronização seja útil.
1.2- Explique o modelo de interação **Produtor-Consumidor** e dê um exemplo de uma situação em que este modelo é particularmente adequado.
1.3- Refira algumas vantagens e desvantagens de utilizar uma camada de **middleware de distribuição**.

2 [7v] - Um sistema de limpeza de grandes superfícies é composto por uma equipa de robôs autónomos cooperantes. A cooperação é efetuada através de um computador central que recebe informação dos robôs sobre as áreas já cobertas e faz a respetiva fusão para representar o estado global atual do processo de limpeza. Os robôs estão sempre em ligação direta com o computador central e escolhem as suas áreas de intervenção consultando o estado do processo de limpeza.
2.1- Indique qual o **modelo de interação mais adequado** entre os robôs, Cliente-Servidor, Produtor-Consumidor, Publicador-Subscritor ou Memória Partilhada, para suportar a aplicação referida. Justifique.
2.2- Qual a **topologia da rede** constituída pelos robôs e computador central e que **protocolo de transporte** (TCP/IP ou UDP/IP) será mais adequado? Justifique.
2.3- Considere que o processo de limpeza beneficia da existência de um **relógio global** que permite aos robôs sincronizar as suas ações entre si. Para obter tal relógio o sistema utiliza o **protocolo NTP** que usa uma técnica comum para medição dinâmica do **atraso de rede**. Como se chama essa técnica e como funciona? (Faça um esboço)
2.4- Suponha que o sistema conta com 10 robôs e que cada um tem um relógio local perfeito, i.e., sem *drift*. Contudo, os atrasos de rede são aleatórios, variando entre 500 μs e 10 ms. Qual a **melhor precisão absoluta**, numa abordagem determinística, que se consegue obter?
2.5- Suponha agora que o protocolo de rede foi alterado para permitir **topologias em malha (mesh)**, de modo que as comunicações com o computador central podem agora ter de ser reencaminhadas por vários robôs. Para a propagação de informação na rede está a considerar a utilização ou de uma **árvore lógica dinâmica** ou de uma técnica de **disseminação epidémica**. Caracterize as duas possibilidades sumariamente e discuta a sua aplicabilidade neste contexto, considerando as comunicações dos robôs para o computador central e deste para os robôs.

3 [2v]- Considere o algoritmo do **Bully** para a eleição de *leader*.
Explique as possíveis consequências da perda de algumas mensagens HALT na execução desse algoritmo.

4 [2v]- Considere o protocolo **two-phase commit**. Para que seja possível **recuperação**, em caso de falhas, os processos registam as suas ações num *log* em *stable storage* **antes** de enviar mensagens.
Apresente uma execução que mostre que: se as mensagens forem enviadas antes do registo do seu envio no *log*, as ações de recuperação apresentadas nas aulas podem conduzir à violação de algumas propriedades que uma solução para o problema do *atomic commitment* tem que satisfazer. Justifique.
Dica- Use um diagrama temporal de mensagens.

5 [3v] - View synchronous (VS) multicast foi definida com base em duas propriedades **View Synchrony** e **Self-Delivery**.
5.1- Explique o conceito de **stable message** usado na implementação de VS multicast.
5.2- Explique as **duas alternativas** apresentadas na aula para implementar **view synchrony** com base no conceito de **stable message**, e para cada uma dessas alternativas apresente uma vantagem em relação à outra.

6 [3v] - Na implementação de um **canal de comunicação segura** optou-se pelo uso dos seguintes mecanismos criptográficos (apenas estes e mais nenhum):

(a) Protocolo de Diffie-Hellman

(b) HMAC com SHA256

(c) AES com CBC

Para cada uma das seguintes afirmações indique se é verdadeira ou falsa. Justifique cada uma das suas respostas.

1. Este canal **garante a autenticação** das entidades que o estabelecem.
2. Este canal **garante a integridade** das mensagens por ele transportadas.
3. Este canal **garante a confidencialidade** das mensagens por ele transportadas.
4. Este canal **garante a autenticidade** das mensagens por ele transportadas.

Nota: Por **garantia da autenticidade** entende-se a deteção duma mensagem enviada por um processo diferente dos que estabeleceram o canal seguro.