Etude de cas Sureté de Fonctionnement SAR 2017-2018

I. Disponibilité d'un réseau en anneau (20 pts)

Dans cet exercice nous allons étudier la topologie réseau en anneau. On parle ici de topologie physique et donc de « câblage ».

Le but de cet exercice est de vous amener à utiliser les outils découverts en TD pour analyser et résoudre un problème.

Le modèle du système et ses défaillances.

Le principe d'une topologie en anneau est la suivante. Pour un ensemble de N machines nommées m_0,... m_{N-1}. Chaque machine m_i est connectée à m_{i-1} et m_{i+1} modulo N (ceci est la version simple qui fait abstraction de certains détails dans la constitution d'un tel réseau). En l'absence de connexions défaillantes (câbles rompus), les données circulent de machine en machine par le chemin le plus court. Ce modèle suppose que les câbles permettent des communications bi-directionnnelles. La pile réseau en charge du transport est munie de moyens de détection pour la perte de connexions. En cas de perte de connexion chaque nœud met à jour une table indiquant pour chaque nœud destination d'un message le prochain nœuds sur le plus court chemin pour l'atteindre. On supposera que cette table se met à jour instantanément et sans erreur. Le réseau est déclaré défaillant pour les nœuds (m_i, m_j) si il est impossible d'établir un chemin de i à j.

Question 1 (3 pts)

Supposons N=10, combien de câbles peuvent être rompus sans empêcher la transmission de donnée de la machine 0 vers la machine 4

- dans le pire cas (du point de vue de l'ingénieur en sureté de fonctionnement)
- dans le meilleur des cas

Question 2 (5 pts)

En supposant que

- la date de rupture d'un câble dans cette architecture suit une loi exponentielle de paramètre L=0.00001 (pour une unité de temps correspondant à 1h),
- la rupture de chaque câble doit être vue comme un événement indépendant

Calculez la probabilité que les nœuds 0 et 4 restent connectés pendant 5 mois à partir d'un système totalement fonctionnel.

Processus de maintenance

Le processus de maintenance est modélisé de la manière suivante. La réparation d'un câble rompu suit une loi exponentielle de paramètre m=0,001 (même unité temps qu'auparavant). La détection de défaillance étant instantanée, le processus de maintenance est engagé dès qu'un câble se rompt. On supposera qu'il y a au moins autant d'équipes de maintenance que de câbles. Une connexion entre deux machines (mi, mj) est jugée défaillante si aucun des deux chemins possibles pour communiquer

entre ces machines n'est totalement fonctionnel (aucun câble rompu). Le système est défaillant à partir du moment où il existe une connexion défaillante dans le système.

Question 3 (5 pts)

Quelle est la probabilité maximale qu'une connexion soit défaillante pour un couple de machine et le reste pour au moins 24h d'affilées.

Question 4 (4 pts)

Supposons que L vaillent désormais 0.0001. Est il possible que le système soit défaillant pendant 2h avec une probabilité supérieure ou égale à 0.001 ? En quoi la valeur de m affecte-t-elle votre réponse ?

Question 5 (3 pts) **(difficile)**

Déterminer la même probabilité dans le cas où il y a une seule équipe de maintenance (la durée aléatoire du processus de maintenance est liée à la réparation d'un câble donné). On attend de vous que vous fournissiez le modèle de votre système.

II. Placement de répliques actives sur un anneau (6pts)

Nous devons réaliser un système critique reposant sur une fonctionnalité implémentée de trois manières différentes. Nous appellerons ces versions C1, C2, C3. Pour chaque exécution ces variantes ont les probabilités suivantes de fournir un résultat numérique faux :

C1 : 0.001 ; C2 : 0.01 ; C3 : 0,0025

De plus, ces composants peuvent entraîner l'arrêt du calculateur sur lequel ils s'exécutent avec les probabilités suivantes pour chaque exécution (on suppose les deux défaillances comme étant des événements disjoints)

C1 : 0.0001 ; C2 :0.000001 ; C3 : 0,00025.

Les algorithmes utilisés pour C1 et C2 sont déterministes (deux répliques avec les mêmes entrées engendrent des résultats et flux d'exécution identiques). En revanche C3 possède une partie aléatoire : les défaillances lors de l'exécution de deux répliques de C3 sur des calculateurs différents doivent être jugées indépendantes.

Question 6 :

Évaluer la fiabilité des réponses pour l'architecture (|| veut dire « en parallèle avec) C1 || C2 || C3, C3||C3||C3, C3||C3||C1.

Question 7 :

Evaluer la disponibilité de l'architecture en supposant que le système est jugé disponible tant qu'au moins 2 répliques sont capables de s'exécuter. (i.e. temps moyen avant défaillance).

Question 8 :

En utilisant l'architecture ayant la meilleur disponibilité, quelle est la probabilité que l'architecture produise un résultat correcte pendant 10000 exécutions consécutives.