Institut National des Sciences Appliquées de Lyon

Département Informatique, 4ème année, 2013-2014

Réseaux avancés et sécurité

(Documents manuscrits et copies des supports de cours autorisés)

A. Question d'ordre général (2 points)

Qu'est-ce que le chiffre de César ? Quels sont les moyens qu'un attaquant qui ne connaît pas les paramètres de chiffrement, peut utiliser pour « casser » un texte chiffré par cette méthode (c'est-à-dire découvrir le texte initial (non-chiffré) sans autre information que le texte chiffré) ?

B. Exercice : Administration réseaux (10 points)

Cf. fiche annexe.

C. Problème : Pic de pollution sur Hypsis (*mobile crowd sourcing*) (11 points + 2 points)

La belle ville d'Hypsis vient de lancer un ambitieux programme de ville intelligente dont l'un des projets vise à surveiller en temps réel le niveau de plusieurs polluants via la collecte de données issues de capteurs intégrés aux téléphones portables (*smartphones*) des habitants volontaires.

Par souci de simplification, les hypothèses suivantes seront considérées :

- les smartphones ont la capacité de se découvrir et de se reconnaître
- un serveur de la mairie, nommé Valérian, abrite l'application de collecte et d'analyse des données de pollution transmises par les smartphones

Note importante : vous êtes libre, dans vos réponses aux questions ci-dessous, de faire des hypothèses additionnelles dès lors que vous les justifiez.

C.1 Dans cette question, on considère que, toutes les *m* minutes, chaque smartphone transmet au serveur central Valérian, via le réseau de téléphonie mobile (GSM/3G/4G), la valeur instantanée de l'ensemble des mesures de polluants qui remontent de ses capteurs. Décrivez le fonctionnement de cette opération (protocole (envoi-réception des données) entre le smartphone et le serveur central Valérian ; opérations effectuées localement par le smartphone et par le serveur central Valérian).

C.2 Certaines zones d'Hypsis ne sont malheureusement pas couvertes par le réseau de téléphonie mobile. Dans ces zones, le système fonctionne alors de la manière suivante. Spontanément (en fait, quand il estime qu'il va bientôt se déplacer vers une zone couverte par le réseau mobile (rq : le calcul de cette estimation est en-dehors du sujet)), un smartphone (localisé dans une zone non-couverte) diffuse autour de lui, en WiFi, une annonce précisant qu'il va bientôt se connecter au serveur central et qu'il est à même

de recevoir les données de pollution de *k* autres smartphones. Cette diffusion se fait à 2 sauts (*hops*): le smartphone diffuse en WiFi à tous ses voisins qui, eux-mêmes, diffusent en WiFi à tous leurs voisins. Le smartphone à l'initiative de cette annonce est appelé « smartphone collecteur ». Tout smartphone qui n'a pas pu transmettre ses données depuis plus de *p* minutes va essayer d'utiliser la possibilité offerte par le smartphone collecteur pour faire remonter ses données au serveur central.

Décrivez le fonctionnement de l'ensemble de cette procédure (de la diffusion de l'annonce à l'envoi, par le smartphone collecteur, des données collectées vers le serveur central Valérian).

Notes : (i) n'oubliez pas : un smartphone collecteur ne peut récupérer que les données de *k* smartphones (=> comment traiter cette limite pour éviter les « famines » (smartphone qui n'arrive jamais à envoyer ses données à un collecteur) ?) ; (ii) n'oubliez pas que l'annonce concerne tous les nœuds situés à moins de deux sauts du smartphone collecteur : pensez à traiter le cas des nœuds n'ayant pas de lien direct avec le smartphone collecteur ; (iii) pensez que plusieurs smartphones peuvent se déclarer « smartphone collecteur » en même temps ! ; (iv) quel mécanisme proposez-vous de mettre en place pour utiliser de manière optimale les smartphones situés sur la limite de couverture du réseau mobile ?

Conseil : commencez par traiter le cas le plus simple (une seule annonce en même temps, pas de famine possible, pas de smartphone sur la limite de couverture…) puis considérez les éléments de complexité un par un en vérifiant que les solutions que vous apportez ne se contredisent pas. Proposez des solutions simples (même si elles ne sont pas tout à fait optimales (discutez alors leur non-optimalité)) !

Remarques : (i) on suppose, dans cette question, que tous les smartphones se comportent de manière dite « altruiste », c'est-à-dire qu'ils font tout ce qu'il est possible pour faciliter le fonctionnement du système (même si cela nuit à leur fonctionnement propre (sur-utilisation de la batterie par exemple)) ; (ii) on suppose également que la prévision initiale du smartphone collecteur est juste : il va effectivement se déplacer vers une zone couverte par le réseau mobile dans le délai prévu (en clair : ne traitez pas le cas où cette estimation est erronée).

C.3 (question subsidiaire – 2 points) Malheureusement, tous les smartphones collecteurs ne sont pas fiables : certains, pour différentes raisons que l'ont n'abordera pas ici, ne font pas remonter les données collectées au serveur central :

- imaginez un mécanisme (simple !) pour faire savoir à un smartphone qui a utilisé un collecteur *C* si les données qu'il lui a transmises ont effectivement été remontées par *C* au serveur central dans un délai « raisonnable ». Grâce à cette information, on supposera, dans la suite du problème, qu'un smartphone est capable de calculer son « avis » personnel sur la fiabilité du collecteur *C*

- un smartphone, avant d'envoyer ses données à un collecteur *C* veut savoir si, dans le passé, *C* a bien fait remonter les données qu'il avait reçues des autres smartphones. On propose de déterminer cette information (on parlera de « réputation » de *C*) en agrégeant les avis sur *C* (cf. point précédent : avis personnels sur la fiabilité d'un collecteur) des smartphones disponibles dans l'environnement. Imaginez un mécanisme de détermination de cette réputation. Conseil : privilégiez une solution simple et efficace (minimisez le nombre de messages échangés) même si elle n'est pas absolument optimale (identifiez alors en quoi elle n'est pas optimale)

Excellentes vacances largement méritées (et très bon stage) (en clair : faites-vous plaisir et revenez-nous en forme) !!!