Institut National des Sciences Appliquées de Lyon

Département Informatique, 4ème année, 2012-2013

Réseaux avancés et sécurité

(Documents manuscrits et copies des supports de cours autorisés)

A. Questions d'ordre général (4 points)

A1. Qu'est-ce qu'un équilibre de Nash ?

A2. Décrivez les mécanismes de création et de vérification d'une signature numérique.

B. Exercice : Administration réseaux (7 points)

Cf. fiche annexe.

C. Problème : Rébellion au Rakmanistan (réseaux tolérant les délais) (9 points + 2 points)

La guerre en République de Rakmanistan oppose rebelles et armée gouvernementale. Tous les moyens de télécommunication (téléphone filaire, GSM/3G…) sont contrôlés par le gouvernement. Le seul moyen restant aux forces rebelles pour communiquer de manière confidentielle est l'échange de données de personne à personne en WiFi. Les dispositifs des rebelles (en abrégé : dispositifs rebelles) forment ainsi un réseau dit « tolérant les délais » dans lequel les échanges se font de dispositif mobile à dispositif mobile. En pratique, en l'absence de connexion de bout en bout, un message *m* émis à destination d'un dispositif destinataire D va transiter de dispositif mobile en dispositif mobile jusqu'à ce qu'un dispositif mobile porteur de *m* se trouve suffisamment proche du dispositif destinataire D (c'est-à-dire dans le rayon de communication WiFi de D) pour lui remettre directement le message *m*.

Tout message est muni d'une estampille (date/heure de départ du message) et d'une durée de validité (ou d'une heure/date limite de validité, à votre choix) (notée TTL : Time To Live), définissant l'instant au-delà duquel le message devient obsolète.

On supposera dans l'ensemble du problème que les dispositifs rebelles savent se reconnaître entre eux (et donc, corollairement, reconnaître les dispositifs gouvernementaux) de manière fiable et sécurisée.

Soit S le dispositif source d'un message *m* à destination du dispositif D. Deux protocoles de routage de base peuvent être considérés :

- « Direct » : dans ce protocole, S attend d'être suffisamment proche de D pour lui transmettre *m* ; si le TTL est atteint avant que S rencontre D, S supprime le message *m* qui n'est donc pas transmis à D. Le point fort de « Direct » est qu'il ne génère qu'un seul message (son coût en nombre de messages est donc optimal). Son point faible est que la probabilité de transmettre *m* avant que le TTL expire peut, dans certaines configurations, être très faible

- « Epidémie » : dans ce protocole, S transmet (une copie de) *m* à tous les dispositifs rebelles qu'il rencontre, ceux-ci retransmettent (une copie de) *m* à tous les dispositifs rebelles qu'ils rencontrent, et ainsi

de suite jusqu'à ce que le message (une copie du message) *m* atteigne D ou que le TTL expire. A l'opposé de « Direct », le point fort d' « Epidémie » est qu'il garantit une probabilité de transmission du message optimale ; son point faible est son coût en nombre de messages générés qui peut, dans certaines configurations, être exorbitant.

Note importante : vous êtes libre, dans vos réponses aux questions ci-dessous, de faire des hypothèses additionnelles sur l'environnement, les dispositifs, etc. dès lors que vous les justifiez et les discutez.

C.1 Décrivez une implémentation d'« Epidémie » (note : à un instant donné, un dispositif mobile peut être porteur de plusieurs (copies de) messages à router).

C.2 Imaginez un protocole limitant à q=10 le nombre total de copies d'un message *m* (source S, destination D) présentes à tout instant dans le réseau.

C.3 On suppose, dans cette question, que chaque dispositif mobile calcule sa fréquence de contact avec chacun des autres dispositifs mobiles. Imaginez des modifications des protocoles décrits en C.1 et C.2 utilisant cette information (idée de base : il vaut mieux passer le message *m* à un dispositif qui rencontre fréquemment D qu'à un dispositif qui ne le rencontre jamais ; note : pensez qu'un message à une durée de vie limitée (TTL)).

C.4 On suppose, dans cette question, que les dispositifs rebelles disposent d'un mécanisme dit de « partage de secret » fonctionnant ainsi :

- à partir d'un message *m*, n sous-messages sont générés
- il suffit de posséder p ≤ n sous-messages pour être en mesure de reconstituer le message *m* dans sa totalité

Notes :

- afin d'assurer la confidentialité du message *m*, tous les sous-messages sont cryptés
- afin de renforcer la sécurité, on cherche à éviter que plusieurs sous-messages transitent par le même dispositif

Décrivez un mécanisme d'envoi d'un message utilisant le partage de secret (création, gestion de clefs, échanges de clefs, protocole de routage…). Etudiez la sécurité de votre protocole. Etudiez la mise en œuvre pratique de votre protocole et son efficacité. Note : l'objectif est, évidemment, de rendre la lecture des messages par les forces gouvernementales aussi difficile que possible.

C.5 (question subsidiaire notée hors barème – 2 points) On suppose que chaque dispositif rebelle fait confiance à chacun des autres dispositifs rebelle avec un certain niveau de confiance (*trust level*) :

- imaginez une modification du protocole décrit en C.4 utilisant cette information
- décrivez un mécanisme d'échange sécurisé des informations de confiance entre dispositifs rebelles

Bonnes vacances (et bon stage) !!!