Sécurité dans les réseaux Ad-hoc

Enseignants : Yves GERARD
Laure GONNORD

Etudiants : Mehdi HADDAD
Robleh WAIS

Introduction (1)

- Réseaux Ad-Hoc constitué de stations mobiles
- Pouvoir diffuser de manière sécurisée
- Deux catégories « stateless » et « stateful »
- Les réseaux Ad-Hoc ont des caractéristiques particulières
- Cryptage des données est rendu difficile

Introduction (2)

- Proposer un protocole de diffusion
- Permettre aux stations les plus éloignées de récupérer les messages et (ou) clés
- Permettre aux stations qui ne sont pas en ligne de récupérer les messages et (ou) clés

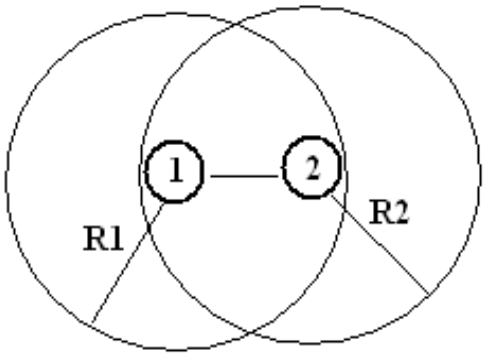
Introduction (3)

- 3 approches évoquées
- Approche interactive
- Approche « naïve »
- Approche non interactive

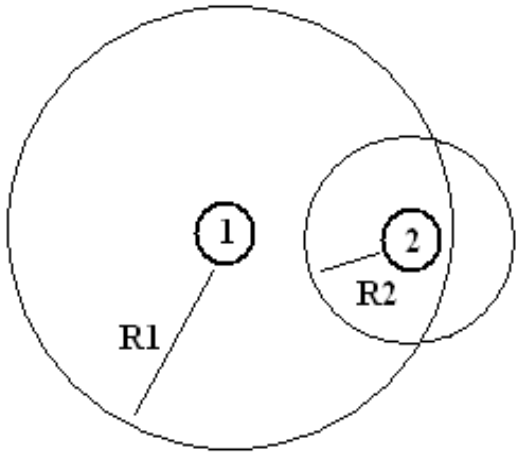
Présentation des réseaux Ad-hoc(1)

- Réseau Ad-hoc ou MANET (Mobil Ad-hoc Network)
- Collection d'unités mobiles
- Unités équipées d'émetteur/récepteur (cartes Wi-Fi)
- Qui forment d'une manière spontanée un réseau
- Topologie du réseau changeante

Présentation des réseaux Ad-hoc(2)



Lien Bi-directionnel



Lien unidirectionnel

R1 : rayon de la portée du noeud 1
R2 : rayon de la portée du noeud 2

Caractéristiques des réseaux Ad-hoc

- Liens asymétriques
  - Déphasage du aux réflexion du signal sur les obstacles
  - Route inverse peut être différente de la route directe
- Sécurité limitée
- Contraintes sur la bande passante

Protocoles(1)

- Approche interactive
  - Message manqué par une station
  - Demande au serveur de répéter le message manqué
- Intéressantes pour des réseaux de taille réduites
- Surcharge le serveur dès que le réseau devient important

Protocoles(2)

- Approche « naïve »
  - Chaque station stocke tous les messages
  - Une station qui a manqué un message interroge ses voisines et récupère le(s) message(s)
- Surcharge du serveur est évitée
- Mais sollicite beaucoup de mémoire au niveau des stations

Protocoles(3)

- Approche non interactive
  - Chaque station stocke un morceau du message manqué
  - La station interroge ses voisines et peut reconstituer le message
- Pas de surcharge du serveur
- Mémoire sollicité au niveau des stations est moins important

Code correcteur (Approche non interactive)

- Utilisation d'un code correcteur

- Code correcteur (C=(Encode, Decode))
  - Combinaison de 2 algorithmes
  - L'émetteur utilise « Encode »
  - Le récepteur utilise « Decode »

Code correcteur (Exemple)

- L'émetteur veut envoyer un message m composé de « l » symboles
- Calcule c=Encode(m) et obtient un nouveau message de longueur λ
- c est envoyé au récepteur
- Le récepteur calcule Decode(c) et obtient le message m
- Pas besoin de tous les symboles pour reconstituer m

Récupération de message (1) (Approche non interactive)

- Définissons
- N : l'ensemble des nœuds du réseau
- ON(t) : les nœuds en ligne (connectés) à l'instant t
- OFF(t) : les nœuds hors ligne (déconnectés) à l'instant t
- m(t) : message envoyer à l'instant t
- u : durée qu'un nœud dans ON(t) stock une partie du message qu'il a reçu

Récupération de message (2) (Approche non interactive)

- La source S veut envoyer le message m(t) et le nœud $v \in OFF(t)$
- S diffuse c(t)= Encode (m(t))= (s(t,1), s(t,2), ..., s(t, λ))
- Pour chaque nœud dans ON(t) :

  Si (t>u) alors $\forall$ x $\in$ [1, λ] supprimer s(t-u, x)

  Stocker s(t, y) avec y=Random(1, λ)

  Si à l'instant t' > t le nœud v veut récupérer m(t), il demande les symboles de c(t) à ses voisins jusqu'à en avoir assez de parties s(t,i) pour reconstituer c(t).
- v récupère m(t) = Decode(c(t)). Puis c(t)= Encode (m(t))= (s(t,1), s(t,2), ..., s(t, λ)). Et stock un symbole s(t, y) avec y = Random (1 , , λ)

Récupération d'un seul message (Approche non interactive)

- Déterminons le nombre de station à interroger pour reconstituer un message
- Avec l'utilisation d'un code correcteur on a juste besoin de λ-d+1 symbole de c(t) (avec d est la distance du code correcteur)
- Ce problème peut donc se réduire au problème du coupon collecteur

Récupération d'un seul message (Approche non interactive)

- On cherche donc E[X] l'espérance de la variable aléatoire X correspondant au problème
- D'après la formule donnée par le problème des coupons collecteurs

$$E[X] \leq \lambda(\ln \lambda - \ln (d-1)) \leq \lambda \ln \left(\frac{\lambda}{d-1}\right) \leq \frac{l}{\rho} \ln \left(\frac{l}{\rho.(d-1)}\right)$$

- On a donc un ordre de grandeur de O(l.ln(l)) (avec l = longueur du message m)

Utilisation du protocole

- Un réseau Ad-hoc où les stations auront chacune leur clé individuelle avec le serveur
- Le serveur aura mis en place une clé de groupe
- Quand un nœud est inclus dans le groupe
  - Mise en place de sa clé individuelle
  - Le serveur change de clé de groupe
  - Le serveur diffuse la clé de groupe en la cryptant via la clé individuelle pour le nouveau nœud et via l'ancienne clé pour les nœuds déjà existant

Récupération de la clé mise à jour

- Une clé est considérée comme un message particulier
- Le mécanisme utilisé est donc le même que précédemment

Conclusion

- Réseau Ad-Hoc de plus en plus répandus
- Pouvoir communiquer en sécurité
- Mécanisme plutôt robuste aux attaques
- L'utilisation du code correcteur le rend sensible aux « pollution attacks »
- L'utilisation de de « distilation code » peut permettre de contrer ce genre d'attaque

Questions?