ACI SI MOSAIC

29/09/2005

Yves Roudier – Institut Eurécom

1) Collaboration

- Observation de la collaboration ?
  - Immédiate : e.g. routage MANETs (service immédiat)
  - Non immédiate dans notre cas (promesse de service selon [Obreiter, Nimis])
    - Incitation économique (crédit contre service) ou par réputation (comportement observé “conforme aux normes”)
    - initialisation du mécanisme ?? (nb de crédits p. ex. ?)
- Faut-il forcer les noeuds à adopter un comportement équitable dans toutes les situations ?
    - Surtout si beaucoup de ressources sont disponibles ?
- In fine, problème d’évaluation des ressources disponibles ?

2) Sécurité

élimination des malveillances

- Disponibilité du service: éviter le DoS
  - comment empêcher un noeud de remplir l'espace de stockage de tous ses voisins ?
  - comment empêcher un noeud de bloquer un voisin en lui laissant ses données sans les récupérer ?
- Accountability: comment empêcher un noeud de cacher sa responsabilité dans la non résolution du protocole de sauvegarde ?
  - Protection des incitations à la collaboration: TPH ?
  - optimistic fair exchange: situations non décidables en distribué tranchées par un TTP
    - TTP centralisé / distribué? (peut nécessiter un service d'horodatage centralisé)
    - Log sur TPH / sécurisé sur terminal ?
- Confidentialité et Contrôle d'accès: comment empêcher un noeud d'accéder les données d'un autre noeud ou de les faire supprimer de leur lieu de stockage temporaire?
  - Chiffrement
  - Équivalent au "key escrow" ? (perte d'appareil)
  - Authentification de l'origine de la sauvegarde

3) Sûreté / Vivacité / QoS

- Disponibilité des données (suffisamment redondée) ?
  - Criticité des données
  - Comportement collaboratif à estimer
    - Incitation économiques: un noeud “riche” a participé à l’infrastructure – mais a pu détruire beaucoup de données qui lui ont été confiées
      - Possibilité de pénalités (amendes)
    - Réputation autoportée : conformité au processus complet de sauvegarde
- Gestion des problèmes réseaux
  - Pertes de paquets / de connexion ?
- Performance ?
  - Délais de récupération d’une sauvegarde ? (primes?)
  - Situations de bloquage ?
  - Priorités ?

Optimistic Fair Exchange: quelques références

- **Optimistic Fair Exchange protocols**
  - [ASW97] N. Asokan, M. Schunter, and M. Waidner. Optimistic Protocols for Fair Exchange. In Proceedings of 4th ACM Conference on Computer and Communications Security, Zurich, April 1997. http://citeseer.ist.psu.edu/article/asokan96optimistic.html
  - [PSW98] Birgit Pfitzmann, Matthias Schunter, and Michael Waidner. Optimal efficiency of optimistic contract signing. In 17th Symposium on Principles of Distributed Computing (PODC), ACM, New York, 1998. http://citeseer.ist.psu.edu/article/pfitzmann98optimal.html
  - [ZG96] Jianying Zhou and Dieter Gollmann. A fair non-repudiation protocol. In Proceedings of the IEEE Symposium on Research in Security and Privacy (IEE96), pages 55--61. http://citeseer.ist.psu.edu/62704.html
  - [PVG+00] Henning Pagnia, Holger Vogt, Felix C. Gärtner, and Uwe G. Wilhelm. Solving fair exchange with mobile agents. In ASA/MA. http://citeseer.ist.psu.edu/article/pagnia00solving.html

- **Optimistic Fair exchange et TPH**
  - [TIH+04] M. Terada, M. Iguchi, M. Hanadate, and K. Fujimura. An Optimistic Fair Exchange Protocol for Trading Electronic Rights. In 6th Smart Card Research and Advanced Application conference (CARDIS'2004), 2004.
  - [VPG01] H. Vogt, H. Pagnia, and F. C. Gärtner. Using Smart cards for Fair-Exchange. WELCOM 2001, LNCS 2232, Springer, pp. 101-113, 2001. http://citeseer.ist.psu.edu/vogt01using.html

Mécanismes : résumé

- Malveillance: politique de sécurité à définir, mise en application assurée par la cryptographie et TPH utilisés dans le protocole
    - Association fonctions de sauvegarde – crypto/TPH à préciser (cf. rôle du TPH vis-à-vis du packet forwarding dans les nuglets)
- Collaboration : incitations
    - économiques plus faciles et plus sûres que la réputation
    - “Trop” équitables?
- Sûreté/vivacité : estimations
    - Déterminer les caractéristiques du processus de sauvegarde

- Peut-on faire l’économie de plusieurs mécanismes ?
  – i.e. les incitations à la collaboration peuvent-elles servir à l’estimation de la sûreté/vivacité (et aussi comme mécanisme pour contrer la malveillance) ?