KAA : Knowledge Authentication for Ambient

ACI SECURITE

Modélisation et gestion de la confiance dans les réseaux spontanés

Objectif : conception d'un modèle de confiance dans les réseaux spontanés

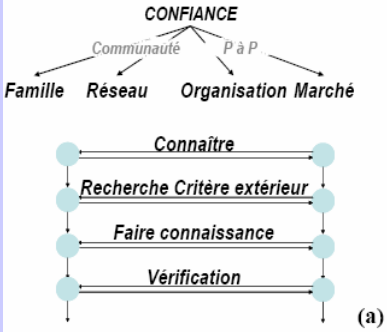
- **Réseaux spontanés :** Composés d'entités ou nœuds sans infrastructure

  - •Capables de rencontrer des objets anonymes
  - •Gestion de relations déjà existantes et de nouvelles relations
  - •Organisés en communautés en perpétuelle évolution mais capable de constituer des services d'accès coûte que

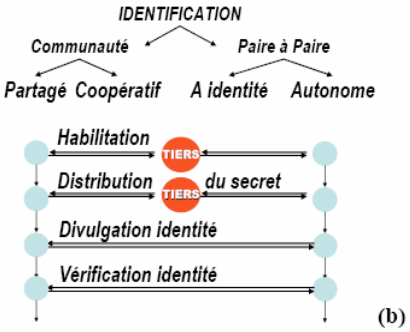
=> **Besoin graduel de confiance** selon les services demandés, la topologie du réseau,…

- **Problème de l'identification : état de l'art**

- **Modèle social**



- **Modèle électronique**



Proposition : le projet KAA

- **Stations d'imprégnation : fournit un package KAA** qui donne aux nœuds KAA un **germe de confiance** composée de matériel cryptographique, d'une identité et d'une paire de clé publique/clé secrète. Elles définissent des domaines

imprinting station

Common knowledge : trust level

- **Chaque nœud KAA** construit au fur et à mesure de ses rencontres un historique (publique/secret)

- **Deux modes de fonctionnement :**

  - **Mode fermé :** deux nœuds imprégnés par la même station ou le même domaine se rencontrent

    => **confiance établie** (modèle de la famille)

  - **Mode ouvert :** les nœuds n'appartiennent pas au même domaine. Pour communiquer, ils doivent avoir dans leur historique respectif, suffisamment de **nœuds rencontrés en commun.**

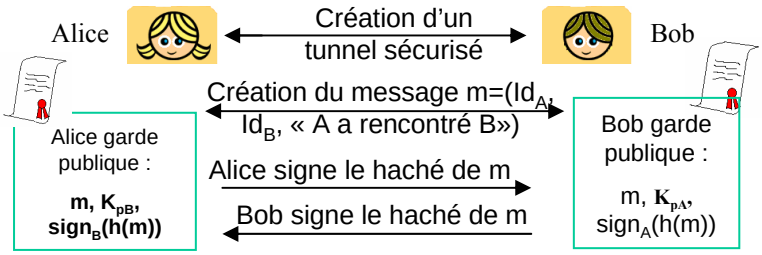
- **L'historique** peut également contenir la sémantique des interactions réalisées avec les autres nœuds.

Proposition de protocole cryptographique ou comment prouver les rencontres

- **Problématique :** Alice rencontre Bob, Bob rencontre Charlie => Alice veut ensuite prouver à Charlie qu'elle a bien rencontré Bob.

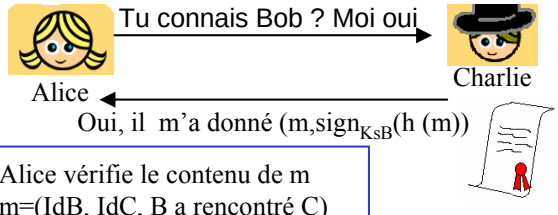
- **Protocole fondé sur des identités cryptographiques**

- **Première rencontre : Alice/Bob (de même Bob/Charlie)**



- **Rencontre entre Alice et Charlie (deux nœuds inconnus)**

veulent se prouver réciproquement qu'ils connaissent Bob



LIP

le Centre de Sociologie des Organisations

CITI

CERCRID

MAPLY

Laboratoire d'Économie des Transports