Sujet de master recherche " Architectures logicielles distribuées " 2005–2006

Etude des protocoles de routage sécurisés et d'une solution mojette dans un réseau 802.11 en mode ad'hoc

Encadrant principal : Salima HAMMA
courriel : Salima.Hamma@univ-nantes.fr
tél. : 02 51 12 58 11

Co-encadrant(s) : Benoît Parrein

Objectif du stage

Un réseau ad hoc est un réseau sans-fil ne disposant pas d'une infrastructure fixe qui permet de gérer la communication entre les noeuds. Tous les noeuds du réseau participent au routage et donc acceptent de jouer le rôle de routeur. Le routage dans les réseaux adhoc manque encore de maturité. Même si aucune technologie sans fil n'a été conçue spécialement pour ce type de réseau, on peut, par exemple, pour le standard IEEE 802.11 ajouter des protocoles de routage appropriés pour faire communiquer les mobiles entre eux. Il faut intégrer une chose sûre est que les protocoles de routage utilisés dans les réseaux filaires ne peuvent être utilisés tels quels dans les réseaux adhoc. En effet, ces derniers ont par définition une topologie complètement dynamique et plus spécialement des ressources limitées (bande passante et l'énergie).

Deux principales approches animent de grands débats : l'approche réactive et l'approche proactive [1, 2]. L'approche proactif permet à chaque noeud de maintenir à jour en permanence la topologie complète du réseau. Il repose sur un échange permanent de paquets de contrôle permettant cette mise à jour. On cite le protocole OLSR (Optimized LinkState Routing), DSDV (Destination Sequenced Distance Vector) et TBRPF (Topology Broadcast Based on Reverse-Path Forwarding). L'approche réactif permet à chaque noeud d'effectuer une découverte de route vers une destination seulement s'il a des paquets à transmettre à celle ci (à la demande). On cite le protocole de routage par la source, DSR (Dynamic Source Routing) et le protocole AODV (Ad'hoc On Demand Vector).

Il existe une autre approche hybride qui combine les deux précédentes approches en gardant que les avantages de chacune d'elles. Le protocole ZRP (Zone-Based Hierarchical Link State Routing protocol).

Ces protocoles font l'hypothèse d'un environnement idéal dans lequel le fonctionnement du réseau n'est pas soumis à des attaques malveillantes concernant la disponibilité des services et l'intégrité des données. Ils font également l'hypothèse que tous les noeuds participent volontairement à l'opération du réseau sans tenir compte de leur tendance naturelle à s'abstenir dans le but de sauvegarder l'énergie de leur batterie. La sécurisation du routage ad hoc est particulièrement difficile en raison du manque d'entité administrative dans le coeur du réseau. Il existe de nombreuses vulnérabilités permettant à des noeuds mal intentionnés de corrompre la configuration des tables de routage, modifier les paquets en transit ou tout simplement de ne pas participer à l'effort routage dans le but d'économiser de l'énergie.

Voici quelques exemples de protocole de routage sécurisé dans un environnement ad'hoc [3, 4, 5, 6] :

- SRP (Secure Routing Protocol), amélioration de DSR, permettant de sécuriser la phase de découverte,

- ARIADNE & TESLA, permettant d'authentifier l'initiateur et chacun des noeuds intermédiaires,
- ARAN, où chaque noeud signe (serveur de certificat) les paquets de découverte et de réponse de routes,
- SEAD, amélioration de DSDV, authentifiant l'émetteur et les noeuds intermédiaires par une chaîne de hachage.

L'objectif du stage est l'étude de ces protocoles de routage et la mise en oeuvre d'un protocole sécurisé basé sur la transformée Mojette. Cette dernière permet de partager l'information à transmettre en morceaux avec une redondance contrôlée.

Travail à réaliser

Le travail à réaliser au cours de ce stage peut se résumer en quelques points :

- État de l'art des réseaux mobiles.
- Etude des protocoles de routage sécurisés dans le mode ad'hoc.
- spécification d'un protocole de routage sécurisé à l'aide de la transformée mojette.
- Modélisation et dimensionnement d'un réseau ad'hoc
- Simulation et étude de performances de ce protocole pour le transport des applications type multimédias
- Etude comparative par rapport aux protocoles non sécurisés.

Plusieurs scénarii seront proposés afin de prendre en compte des situations diverses (mobilité forte, moyenne, consommation de l'énergie, le nombre de noeuds mobiles dans le réseau ad'hoc...). On s'intéressera en particulier aux critères de performances tels que la perte des paquets, le débit effectif, le temps de réponse. Le langage de simulation NS2 sera utilisé pour la partie expérimentations.

Outils de simulation
Le Network Simulator (NS2) est un simulateur à évènements discrets orienté objets. Sa première version a été développée au laboratoire National Lawrence Berkeley aux Etats Unis. C'est un outils de simulation qui est très largement utilisé par la communauté scientifique. Une connaissance préalable de cet outil sera nécessaire pour mener à bien toutes les expérimentations.

Références

[1] H.Labiod and H.Afifi. *De bluetooth à Wifi, sécurité, qualité de service et aspects pratiques.* Hermès, France, 2004.

[2] P. Mühlethaler. *802.11 et les réseaux sans fil.* Eyrolles, France, 2002.

[3] Siddhartha Gupte and Mukesh Singhal. Secure routing in mobile wireless ad hoc networks. *Ad Hoc Networks*, 1 :151–174, 2003.

[4] YC.Hu, DB.Johnson, and A.Perrig. Sead : secure efficient distance vector routing for mobile wireless ad hoc networks. *Ad Hoc Networks*, 1 :175–192, 2003.

[5] P.Papadimitratos and ZJ.Haas. Secure routing for mobile ad hoc networks. In *SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS)*, Proc., San Antonio TX, January 2002.

[6] W.Lou, W.Liu, and Y.Fang. Spread : Enhancing data confidentiality in mobile ad hoc networks. In *IEEE INFOCOM*, Hong Kong, March 7-11 2004.