Résumé

Le protocole Mobile IPv4 est un protocole de niveau réseau permettant à un mobile d'être joint et de communiquer (avec d'autres mobiles ou terminaux fixes) quelle que soit sa position géographique. Néanmoins, autoriser une machine à se connecter sur un réseau puis à se déplacer de réseau en réseau entraîne de nombreux risques de sécurité: vol de sessions, l'écoute, la localisation, etc. Il sera nécessaire de s'assurer de l'authenticité des mobiles avant de leurs permettre de s'enregistrer auprès d'un réseau étranger.

Beaucoup de travaux ont été proposés pour améliorer la sécurité de l'authentification du protocole Mobile IP, mais qui restent insuffisants en matière de sécurité et de performance : L'authentification standard s'est avérée insuffisante à cause de la non scalabilité et l'absence d'une entité digne de confiance qui se préoccupe de la gestion des clés entre ces acteurs. L'utilisation des cryptosystèmes à clé publique a été proposé pour résoudre le problème de la scalabilité, mais ça reste une solution théorique en particulier pour les nœuds mobiles puisque les algorithmes à clé publique nécessitent une grande puissance en capacité et en temps de calcul. Le schéma d'authentification Mobile IP/AAA est venu remédier à l'absence de l'outil de gestion de clés dans l'authentification standard mais il comporte deux points faibles qui sont : la centralisation de l'outil de gestion de clés et le non-renouvellement des clés de communication lors d'un intra-domaine handoff.

Cette thèse présente un nouveau schéma d'authentification pour Mobile IP qui propose des améliorations à l'ancien modèle d'authentification Mobile IP/AAA. L'idée de base est de re-générer de nouvelles clés pour l'authentification en local en évitant de contacter le domaine mère à chaque changement de cellule. En effet, les clés seront régénérées par les serveurs locaux certifiés et non pas par le home server. Ce nouveau schéma améliore l'authentification des nœuds mobiles dans le protocole Mobile IPv4 tout en diminuant la latence du handover.