

SECURITE DES COMMUNICATIONS SANS FIL PAR L'ETUDE DE LA COUCHE PHYSIQUE

Type de contenu : Texte

Titre(s) : SECURITE DES COMMUNICATIONS SANS FIL PAR L'ETUDE DE LA COUCHE PHYSIQUE ; CHORTI, Arsenia ; ERHEL, Yvon ; SLT GUICHARD, Robin

Autre(s) responsabilité(s) : CHORTI, Arsenia (Directeur de thèse)
ERHEL, Yvon (Directeur de thèse)
SLT GUICHARD, Robin Promotion Chef de bataillon Bulle (2010-2013) (Secrétaire)

Editeur, producteur : Ecoles Militaires de Saint-Cyr Coëtquidan

Description matérielle : 1 CD

Note sur le contenu : mémoire

Note de thèses et écrits académiques : Filière Scientifique - Option Electronique Promotion Chef de bataillon Bulle Date de soutenance : 01/01/2013

Résumé ou extrait : Etude : INTRODUCTION : Les communications sans fil jouent un rôle majeur au sein de nombreuses applications civiles et militaires. Néanmoins, la sécurité de l'échange d'information via un réseau sans fil demeure une question de premier plan ; l'objectif est de réaliser une communication en s'assurant que le message confidentiel soit compris uniquement par le destinataire. Elle est alors dite sécurisée. Etablir la sécurité d'une communication par l'utilisation de la couche physique du modèle OSI est un procédé de plus en plus utilisé. Ce procédé explore la possibilité d'atteindre un niveau de confidentialité parfaite lors d'une transmission de messages, au sein du réseau permettant la communication. L'idée majeure est d'exploiter en effet les caractéristiques physiques (amplitude, déphasage) des messages traversant des canaux de communications bruités pour créer la clef de cryptage. La sécurité n'est alors pas assurée par des algorithmes mathématiques complexes mais par les caractéristiques physiques des messages reçus, sans bien même que cette clef ne voyage de l'émetteur vers le récepteur. Dans cette étude, nous montrerons comment l'originalité de la couche physique permet de répondre aux questions de sécurité des communications sans fil. En particulier, nous démontrerons comment créer des clefs secrètes au travers des canaux sans fil et leurs possibles implications dans la sécurité de relais de communication. RESUME : Ce rapport présente les fondations théoriques et les aspects pratiques d'un nouveau procédé de sécurité appliqué aux réseaux relais : la sécurité par la couche physique. Nous exploiterons les caractéristiques du gain propre à chaque canal pour générer des clefs secrètes afin de réaliser une communication sécurisée par un codage symétrique. Dans la première partie de cette étude, nous nous pencherons sur la sécurité par la couche physique. En outre nous présenterons un mécanisme qui permet de générer des clefs à partir des caractéristiques physiques du message reçu. Dans un deuxième temps, nous discuterons du problème de la sécurité des communications réalisées à l'aide de relais de type amplify-and-forward (AF) et dont la sécurité est incertaine. Enfin, nous proposerons un nouveau mécanisme hybride afin de sécuriser la communication entre deux noeuds, A et

B. En particulier, nous exploiterons la transmission d'un message codé du noeud A vers le noeud B pour établir une transmission sécurisée supplémentaire du noeud B vers le noeud A en exploitant des résultats sur les interférences et la sécurité de la couche physique. CONTRAINTES : L'étude de la théorie de l'information est nécessaire pour comprendre et conduire des recherches sur la sécurité par la couche physique. Une publication classique traitant des questions de cryptographie et de sécurité débute couramment par une discussion sur la notion de confidentialité parfaite au sens de Shannon. Ce pourquoi nous faisons un tour d'horizon des concepts basiques de la théorie de l'information en lien avec la sécurité afin de comprendre comment ils diffèrent de la cryptographie classique. Qui plus est, l'implémentation des nouveaux mécanismes, fruit de recherches théoriques, au travers de logiciel ou de plateformes physiques est une réelle problématique. C'est pourquoi nous proposons de tester nos mécanismes par des simulations informatiques et physiques, en laboratoire, afin de réunir les conditions de transmissions réelles. OUTILS : L'exploitation de Matlab nous permet de vérifier les principales hypothèses au travers de simulations algorithmiques. De plus, il permet l'utilisation de la GNU Radio, un logiciel de développement qui permet de faire le lien entre Matlab et l'USRP (Universal Software Radio Peripheral), la plateforme utilisée pour réaliser les tests. CONCLUSION : Bien qu'un grand nombre de recherches aient été réalisées dans le domaine de la cryptographie, un petit nombre seulement traitent de la génération de clés secrètes par l'analyse de la réponse d

Sujet(s) : communication sans fil
confidentialité
cryptographie
message
système de sécurité
traitement de l'information
transmission de données