

N° d'ordre :

Université des Sciences et de la Technologie Houari Boumediene

Faculté d'Electronique et Informatique
Département d'Informatique

THÈSE

Présentée pour l'obtention du grade

Magister

En : INFORMATIQUE

Spécialité : Programmation et Systèmes

Par

Lynda Aliouane

Intitulée

L'authentification dans les réseaux ad hoc

Soutenue le 02/07/05, devant le Jury composé de :

Mr. A. AISSANI	Professeur, USTHB,	Président de jury
Mme Z. ALIMAZIGHI	Professeur, USTHB,	Examineur
Mr S. LARABI	Maître de conférences, USTHB	Examineur
Mr. N. BADACHE	Professeur, USTHB,	Directeur de thèse
Mr. D. TANDJAOUI	Attaché de recherche, CERIST,	Invité

Sommaire

Introduction générale	6
------------------------------------	----------

Chapitre 1: Les réseaux mobiles ad hoc et le problème de routage.....	9
--	----------

1.1	Introduction	9
1.2	L'environnement mobile	9
1.3	Les Réseaux Mobiles Ad Hoc	11
1.3.1	Définition	11
1.3.2	Les domaines d'application des réseaux ad hoc.....	12
1.3.3	Caractéristiques des réseaux Ad hoc	13
1.4	Le problème de Routage dans les réseaux Ad Hoc	13
1.4.1	Définition de routage.....	14
1.4.2	La difficulté du routage dans les réseaux Ad Hoc	14
1.4.3	La conception de stratégie de routage	15
1.5	Classification des protocoles de routage pour les réseaux Ad Hoc.....	16
1.5.1	Les protocoles de routage proactifs.....	16
1.5.2	Les protocoles de routage réactifs.....	17
1.6	Conclusion.....	17

Chapitre 2 : La sécurité réseau : notions et techniques	20
--	-----------

2.1	Introduction	20
2.2	Les services de la sécurité	20
2.3	Les types d'attaques	20
2.4	Les outils cryptographiques	21
2.4.1	Le cryptage symétrique (ou à clé secrète).....	21
2.4.2	Le cryptage asymétrique (ou à clé publique)	22
2.4.3	Les fonctions de hachage	23
2.4.4	La signature numérique.....	23
2.4.5	Les certificats numériques.....	24
2.4.6	La notion de partage de secret.....	24
2.5	Mécanismes de sécurité.....	25
2.5.1	Algorithme d'échange de clé (Diffie Hellman).....	25
2.5.2	Infrastructure à clé publique (PKI).....	26
2.5.3	PGP (Pretty Good Privacy)	27
2.6	Conclusion.....	28

Chapitre 3 : L'authentification dans les réseaux ad hoc.....	30
---	-----------

3.1	Introduction	30
3.1	Autorité de certification partiellement distribuée.....	30
3.1.1	Introduction	30
3.1.2	Description du système	31
3.2.3	Utilisation de la cryptographie à seuil.....	32
3.2.4	La gestion des certificats	33

3.2.5	Analyse de la solution	35
3.3	L'autorité de certification entièrement distribuée	35
3.3.1	Description du système	36
3.3.2	La maintenance du système.....	36
3.3.3	Analyse de la solution	41
3.4	Certificats délivrés individuellement (Self issued certificates).....	42
3.4.1	Introduction	42
3.4.2	Principe de la solution	42
3.4.3	Les chaînes de certificats.....	43
3.4.4	Graphe de modélisation.....	43
3.4.5	Analyse.....	44
3.5	Accord de clé dans un groupe (Key agreement)	45
3.5.1	Introduction	45
3.5.2	Description de la solution.....	45
3.5.3	Le protocole Hypercube	45
3.5.4	Le protocole d'échange de clé (EKE)	46
3.5.5	Analyse.....	47
3.6	Conclusion.....	47
Chapitre 4 : Présentation d'un nouveau schéma d'authentification		49
4.1	Introduction	49
4.2	Les chaînes de hachages.....	50
4.2.1	Introduction	50
4.2.2	Définition de la chaîne de hachage	50
4.2.3	Application des chaînes de hachage.....	51
4.3	Description du système	52
4.3.1	Supposition.....	52
4.3.2	Buts du protocole	52
4.3.3	Les étapes de l'authentification.....	53
4.3.4	Entretien du réseau	57
4.3.5	Remarques	58
4.3.6	Protocole proposé.....	58
4.3.7	Les avantages de cette solution	64
4.3.8	Inconvénients	64
4.4	Conclusion.....	64
Chapitre 5 : Etude de performance des algorithmes cryptographiques utilisés dans notre protocole		66
Partie 1 : Comparaison de performances des algorithmes cryptographiques .		66
5.1	Introduction	66
5.2	Consommation d'énergie des protocoles de sécurité	66
5.2.1	Introduction	66
5.2.2	Analyse de l'énergie des algorithmes cryptographiques symétriques	66
5.2.3	Les fonctions de hachage	67
5.2.4	Les algorithmes asymétriques	68
5.2.5	Analyse de cette étude.....	68
5.3	Nombre d'opérations cryptographiques exécutées par seconde	68

5.3.1 Introduction	69
5.3.2 Résultats de tests	69
5.3.3 Conclusion de l'analyse	69
5.4 Temps d'exécution des algorithmes cryptographiques	70
5.4.1 Paramètres des expériences	70
5.4.2 Résultats de tests	70
5.4.3 Conclusion de cette étude.....	70
Partie2 : Etude de performance du protocole proposé.....	71
5.5 Introduction	71
5.6 Le choix des algorithmes cryptographiques.....	71
5.7 Capacité de stockage	71
5.8 Temps d'exécution	72
5.9 La consommation d'énergie	73
5.10 Conclusion.....	73
Conclusion générale	74
Références	75