



République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche
Scientifique
Université des Sciences et de la Technologie HOUARI BOUMEDIENE
Faculté d'Electronique et Informatique
Département Informatique



Mémoire de Projet de Fin d'Etude
Pour l'obtention du Diplôme d'Ingénieur d'Etat en
Informatique

Option : Systèmes et Réseaux.

Sujet :

*La sécurité du routage dans les
réseaux mobiles Ad hoc*

Proposé par :

M^r D. DJENOURI

Présenté par :

**M^r BOUAMAMA Med Nadjib
M^r MAHMOUDI Othmane**

Présenté devant le jury composé de:

Prof. N. BADACHE

M^r B. LAICHI

M^{me} S. MOUSSAOUI

Président

Membre

Membre



Année universitaire 2005/2006

Table des matières

INTRODUCTION	5
--------------------	---

Chapitre 1 : Introduction et généralités

I. INTRODUCTION	7
II. ECHELLE DES RESEAUX SANS FIL	7
II.1. RESEAUX PARSONNELS SANS FIL (WPAN).....	7
II.2. RESEAUX LOCAUX SANS FIL (WLAN)	8
II.3. RESEAUX METROPOLITAINS SANS FIL (WMAN).....	8
II.4. RESEAUX ETENDUS SANS FIL (WWAN)	8
III. MODES OPERATOIRES DES RESEAUX SANS FIL.....	8
III.1. LE MODE AVEC INFRASTRUCTURE	9
III.2. LE MODE SANS INFRASTRUCTURE (LES RESEAUX MOBILES AD HOC).....	10
III.2.1. Caractéristiques des réseaux mobiles Ad hoc.....	10
III.2.2. Domaines d'utilisation des réseaux mobiles Ad hoc.....	11
III.2.3. Le routage des données dans un réseau mobile Ad hoc	12
III.2.3.1. Notions générales.....	12
III.2.3.2. Les protocoles de routage proactifs	13
III.2.3.3. Les protocoles de routage réactifs	14
IV. LES PROBLEMES DE LA SECURITE DU ROUTAGE DANS UN RESEAU MOBILE AD HOC.....	15

Chapitre 2 : Les attaques et les protocoles de routage sécurisés

I. INTRODUCTION	17
II. CONCEPTS DE BASE	17
II.1. DEFINITIONS	17
II.1.1. Cryptographie symétrique	17
II.1.2. Cryptographie asymétrique	17
II.1.3. Signature digitale.....	18
II.1.4. Fonction de hachage.....	18
II.1.5. Nœud malicieux.....	18
II.1.6. Attaquant actif-n-m	18
II.1.7. TESLA	18
II.1.8. Cryptographie à seuil (Threshold cryptography).....	19
II.2. CONDITIONS DE SECURITE	19
II.2.1. Disponibilité	19
II.2.2. Authentification.....	19
II.2.3. Confidentialité des données	19
II.2.4. Intégrité.....	19
II.2.5. Non répudiation	19
II.3. CARACTERISTIQUES DES RESEUX MOBILES AD HOC ET LEUR IMPACT SUR LA SECURITE.....	19
II.3.1. Absence d'infrastructure	20
II.3.2. Utilisation des liens sans fil.....	20
II.3.3. Multi sauts	20
II.3.4. Mouvement autonome des nœuds.....	20
II.3.5. Amorphe.....	20
II.3.6. Limitation d'énergie.....	20

II.3.7. Limitation de mémoire et de capacité de traitement.....	20
II.3.8. Vulnérabilité physique des appareils mobiles.....	20
II.4. MENACES	21
II.4.1. Attaques.....	21
II.4.1.1. Attaques externes.....	21
II.4.1.2. Attaques internes.....	21
II.4.1.3. Attaques passives.....	21
II.4.1.4. Attaques actives.....	21
II.4.2. Mauvais comportement	21
III. LES PROBLEMES DE SECURITE DU ROUTAGE	22
III.1. PRESENTATION DES PROTOCOLES DE ROUTAGE DSR ET AODV.....	22
III.1.1. Le protocole DSR.....	22
III.1.2. Le protocole AODV.....	23
III.2. LES DIFFERENTS TYPES D'ATTAQUES (AVEC UNE PROJECTION SUR LES DEUX PROTOCOLES DSR ET AODV).....	23
III.2.1. Attaques en utilisant des modifications.....	23
III.2.1.1. Redirection en modifiant le numéro de séquence de route.....	23
III.2.1.2. Redirection en modifiant le nombre de sauts.....	24
III.2.1.3. Modification de la route source.....	24
III.2.1.4. Attaque par le trou de ver.....	25
III.2.2. Attaques par personifications (Spoofing attacks).....	25
III.2.3. Attaques en utilisant la fabrication.....	26
III.2.3.1. Falsifier les paquets RERR.....	26
III.2.3.2. Diffusion des routes falsifiées.....	27
III.2.4. Attaques par précipitation (Rushing attacks).....	27
III.2.5. Attaques de type trou noir (Blackhole attacks).....	27
III.3. LES SOLUTIONS.....	28
III.3.1. Authentification pendant toutes les phases du routage.....	28
III.3.2. Métrique du niveau de confiance.....	28
III.3.3. Sécurisation de la vérification du voisinage.....	29
III.3.4. Rendre aléatoire l'expédition des messages.....	29
III.3.5. Chiffrement en oignon.....	29
IV. LES PROTOCOLES DE ROUTAGE SECURISES	31
IV.1. LE PROTOCOLE SAR	31
IV.2. LE PROTOCOLE SRP	32
IV.3. LE PROTOCOLE ARAN.....	34
IV.4. LE PROTOCOLE ARIADNE.....	36
IV.4.1. ARIADNE basé sur le mécanisme TESLA.....	36
IV.4.2. ARIADNE basé sur le calcul des MACs.....	38
IV.4.3. ARIADNE basé sur les signatures numériques.....	40
IV.5. LE PROTOCOLE ENDAIRA.....	41
IV.5.1. Le protocole endairA de base.....	41
IV.5.2. Extensions du protocole endairA de base.....	42
V. CONCLUSION	44

Chapitre 3 : Conception et implémentation

I. INTRODUCTION	46
II. MECANISMES UTILISES CONTRE LE COMPORTEMENT EGOÏSTE DES NŒUDS	46
II.1. LA METHODE DE LA DEVISE VIRTUELLE (NUGLETS).....	46
II.2. LE WATCHDOG.....	47
II.3. LE MECANISME CORE	48
II.4. LE MECANISME CONFIDANT	49
II.5. PROTOCOLE BASE SUR LE TEMOIGNAGE	49
LE MECANISME DE REDEMPTION	50

II.5.1. La surveillance.....	50
II.5.1.1. Les paquets de contrôle à diffusion (RREQ).....	50
II.5.1.2. Les paquets de contrôle dirigés (RREPs, RERRs).....	51
II.5.1.3. Les paquets de données.....	53
II.5.2. Le jugement	55
II.5.2.1. Les paquets de contrôle à diffusion (RREQ).....	55
II.5.2.2. Les paquets de contrôle dirigés (RREPs, RERRs).....	55
II.5.2.3. Les paquets de données.....	56
II.5.3. Preuve de mauvais comportement et isolation.....	57
II.5.3.1. Les paquets de contrôle à diffusion (RREQ).....	57
II.5.3.2. Les paquets de contrôle dirigés et les paquets de données	58
III. INTEGRATION DU PROTOCOLE ENDAIRA AVEC EXTENSION DANS GLOMOSIM.....	59
III.1. ENVIRONNEMENT D'IMPLEMENTATION	60
III.1.1. PARSEC.....	60
III.1.2. GloMoSim	60
III.2. MISE EN ŒUVRE DU PROTOCOLE ENDAIRA AVEC EXTENSION	61
DEFINITION DU SYSTEME RSA	61
III.2.1. Rappel sur le fonctionnement général du protocole endairA avec extension	63
III.2.2. Détails d'intégration du protocole endairA avec extension dans GloMoSim.....	66
IV. RENFORCEMENT DU PROTOCOLE ENDAIRA.....	71
IV.1. EXTENSION DE ENDAIRA AVEC LA METHODE BASE SUR LE PRINCIPE DE PROMISCUITE	72
IV.2. EXTENSION DE ENDAIRA AVEC LE MECANISME TWO HOPS ACK DOTE DU MECANISME DE REDEMPTION	73
IV.2.1. Au niveau de la couche réseau.....	74
IV.2.2. Au niveau de la couche MAC.....	75
IV.3. EXTENSION DE ENDAIRA AVEC LE MECANISME RANDOM TWO HOPS ACK	75
IV.3.1. Au niveau de la couche réseau.....	75
IV.3.2. Au niveau de la couche MAC.....	76
V. CONCLUSION	77

Chapitre 4 : Simulations et résultats

I. INTRODUCTION	79
II. PARAMETRES ET MODELES UTILISES POUR LES SIMULATIONS	79
II.1. MODELE DE MOBILITE	79
II.2. MODELE DE PROPAGATION	79
II.3. PROTOCOLE DE LA COUCHE MAC.....	79
II.4. LA COUCHE APPLICATION	80
II.5. DEMARCHE DE LA SIMULATION.....	80
III. METRIQUES DE COMPARAISONS.....	80
III.1. TAUX DE BONNE DETECTION	81
III.2. TAUX DE MAUVAISE DETECTION	81
III.3. DELAI DU BOUT EN BOUT (END TO END DELAY)	82
III.4. LE SURPLUS (OVERHEAD).....	82
IV. RESULTATS ET ANALYSES.....	82
IV.1. EVALUATION POUR LE MECANISME DE REDEMPTION	82
IV.1.1. Réseau à taux de mauvais comportement faible.....	83
IV.1.2. Réseau à taux de mauvais comportement moyen	83
IV.1.3. Réseau à taux de mauvais comportement élevé	84
IV.2. OBTENTION DES MEILLEURS PARAMETRES POUR LE PROTOCOLE ENDAIRA.....	85
IV.2.1. Meilleurs paramètres pour contrer le comportement égoïste	85
IV.2.1.1. Détection du meilleur seuil de tolérance.....	85
IV.2.1.1.1. Réseau à taux de mauvais comportement faible	85

IV.2.1.1.2. Réseau à taux de mauvais comportement moyen.....	86
IV.2.1.1.3. Réseau à taux de mauvais comportement élevé.....	86
IV.2.1.2. Détection du meilleur nombre de témoins.....	87
IV.2.1.2.1. Réseau à taux de mauvais comportement faible.....	87
IV.2.1.2.2. Réseau à taux de mauvais comportement moyen.....	87
IV.2.1.2.3. Réseau à taux de mauvais comportement élevé.....	88
IV.2.2. Meilleurs paramètres pour contrer le comportement malicieux.....	88
IV.2.2.1. Détection du meilleur pas de rédemption.....	88
IV.2.2.1.1. Réseau à taux de mauvais comportement faible.....	89
IV.2.2.1.2. Réseau à taux de mauvais comportement moyen.....	89
IV.2.2.1.3. Réseau à taux de mauvais comportement élevé.....	90
IV.2.2.2. Détection du meilleur seuil de tolérance.....	90
IV.2.2.2.1. Réseau à taux de mauvais comportement faible.....	90
IV.2.2.2.2. Réseau à taux de mauvais comportement moyen.....	91
IV.2.2.2.3. Réseau à taux de mauvais comportement élevé.....	91
IV.2.2.3. Détection du meilleur nombre de témoins.....	91
IV.2.2.3.1. Réseau à taux de mauvais comportement faible.....	92
IV.2.2.3.2. Réseau à taux de mauvais comportement moyen.....	92
IV.2.2.3.3. Réseau à taux de mauvais comportement élevé.....	93
IV.3. COMPARAISON ENTRE LES PROTOCOLES DSR, ENDAIRA DE BASE ET ENDAIRA RENFORCE.....	94
IV.3.1. Le surplus.....	94
IV.3.1.1. Réseau à taux de mauvais comportement nul.....	94
IV.3.1.2. Réseau à taux de mauvais comportement maximal.....	95
IV.3.2. Le délai du bout en bout.....	95
IV.3.2.1. Réseau à taux de mauvais comportement nul.....	95
IV.3.2.2. Réseau à taux de mauvais comportement maximal.....	96
IV.3.3. L'énergie consommée.....	96
IV.3.3.1. Réseau à taux de mauvais comportement nul.....	96
IV.3.3.2. Réseau à taux de mauvais comportement maximal.....	97
V. CONCLUSION	97
 CONCLUSION	 99
 BIBLIOGRAPHIE.....	 100
 ANNEXE.....	 106