

REPUBLICQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE
SCIENTIFIQUE

UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE
HOUARI BOUMEDIENE

**FACULTE DE GENIE ELECTRIQUE ET
INFORMATIQUE**

Département d'informatique

**Mémoire de fin d'études pour l'obtention du diplôme
d'ingénieur d'état en informatique**

Organisme d'accueil: C.E.R.I.S.T

Thème

Conception et Réalisation d'un protocole de détection de
nœuds égoïstes dans les réseaux mobiles ad hoc

Promoteurs:

M^r Djamel Djenouri

M^{me} Samira Moussaoui

Soutenu le :

Les membres du jury:

Président: M^{me} Kadri

Examineur : M^r Benchaiba

Examineur : M^{elle} Benzaid

Réalisé par:

M^r Ahmed Mahmoudi

M^r Nabil Ouali

Table des matières

INTRODUCTION	4
--------------------	---

Chapitre 1 : Introduction et généralité

1.1. INTRODUCTION.....	6
1.2. CATEGORIES DE RESEAUX	6
1.2.1. LES RESEAUX FILAIRES	6
1.2.1.1. La topologie en bus.....	7
1.2.1.2. La topologie en étoile.....	7
1.2.1.3. La topologie en anneau.....	7
1.2.2. LES RESEAUX SANS FIL	7
1.2.2.1. Le mode avec infrastructure.....	8
1.2.2.2. Le mode sans infrastructures	9
1.3. COMMUNICATION SANS FIL.....	10
1.3.1. LA TECHNIQUE DE SAUT DE FREQUENCE	10
1.3.2. ÉTALEMENT DE SPECTRE A SEQUENCE DIRECTE	10
1.3.3. LA TECHNIQUE INFRAROUGE.....	10
1.4. LES RESEAUX AD HOC	11
1.4.1. DEFINITION	11
1.4.2. CARACTERISTIQUES	11
1.4.3. UTILISATION	12
1.4.4. LE ROUTAGE DE DONNEE	13

Chapitre 2 : Les solutions existantes pour la détection des nœuds égoïstes

2.1. INTRODUCTION.....	15
2.2. NOTIONS DE BASE	15
2.2.1. CRYPTOGRAPHIE SYMETRIQUE	15
2.2.2. CRYPTAGE A CLE PUBLIQUE:(LE CHIFFREMENT ASYMETRIQUE).....	16
2.2.3. SIGNATURE DIGITALE	16
2.3. EFFETS DU COMPORTEMENT EGOÏSTE	16
2.4. ACQUITTEMENT DE BOUT EN BOUT (END TO END FEEDBACKS)	17
2.5. WATCHDOG AND PATHRATHER	18
2.5.1. WATCHDOG	18
2.5.2. PATHRATHER :	19
2.6. TWO-HOP ACK.....	19
2.6.1. DEFINITION	19
2.6.2. DISCUSSION	20
2.7. JETON SIGNE (SIGNED TOKEN)	21

2.7.1. LA VERIFICATION DES VOISINS.....	21
2.7.2. LE PROTOCOLE DE ROUTAGE SECURISE.....	22
2.7.3. LE CONTROLE DE L'ENTOURAGE.....	22
2.7.4. LA REACTION A LA DETECTION D'INTRUSION.....	22
2.8. SOLUTIONS BASEES SUR LA REPUTATION.....	23
2.8.1. CORE (COLLABORATIVE REPUTATION MECHANISM TO ENFORCE NODE COOPERATION IN MANETS).....	23
2.8.1.1. Composants.....	24
2.8.1.2. Mise à jour de table de réputation.....	24
2.8.1.3. Application.....	24
2.8.1.3.1 L'application de « CORE » au protocole de routage DSR.....	25
2.8.1.3.2 Application pour l'expédition des données.....	25
2.8.1.4. Discussion.....	25
2.8.2. CONFIDANT (COOPERATION OF NODES FAIRNESS IN DYNAMIC AD HOC NETWORKS).....	25
2.8.2.1. Le contrôleur (Le contrôle du voisinage).....	26
2.8.2.2. Le gestionnaire de confiance.....	26
2.8.2.3. Le système de réputation.....	26
2.8.2.4. Le gestionnaire de routage.....	27
2.8.2.5. Description du protocole.....	27
2.8.2.6. Discussion.....	27
2.8.3. FRIENDS AND FOES (AMIS ET ENNEMIS).....	27
2.8.3.1. Modèle du système :.....	28
2.8.3.2. La structure :.....	28
2.8.3.3. Discussion.....	30
2.9. L'APPROCHE BAYESIAN MODIFIEE POUR LE SYSTEME DE REPUTATION.....	30
2.9.1. STRUCTURE DU BAYESIAN.....	31
2.9.2. L'APPROCHE « BAYESIAN » MODIFIEE.....	31

Chapitre 3 : Environnement de simulation

3.1. INTRODUCTION.....	34
3.2. GENERALITES SUR LA SIMULATION.....	34
3.2.1. SYSTEME REEL ET OBJECTIF DE SIMULATION.....	34
3.2.2. LIMITE DE L'EXPERIMENTATION DIRECTE.....	35
3.2.3. SYSTEMES DISCRETS ET CONTINUS.....	35
3.2.4. MODELES DE SIMULATION.....	35
3.2.5. GESTION DU TEMPS.....	36
3.2.6. SIMULATION PAR EVENEMENTS DISCRETS.....	36
3.2.7. SIMULATEUR.....	37
3.3. PARSEC.....	37
3.3.1. INTRODUCTION.....	37
3.3.2. ENTITE.....	37
3.3.3. MESSAGE.....	37
3.3.4. EVENEMENT.....	38
3.3.5. EXECUTION DE PARSEC.....	38
3.4. GLOMOSIM.....	39
3.4.1 INTRODUCTION.....	39
3.4.2. AGREGATION DES NŒUDS.....	41
3.4.3. STRUCTURE DES REPERTOIRES DE GLOMOSIM.....	41
3.4.4. EXECUTION DE GLOMOSIM.....	42
3.4.5. LES APIS DE GLOMOSIM.....	43
3.4.6. DESCRIPTION DU FICHIER D'ENTREE (DE CONFIGURATION).....	43
3.4.6.1. Le terrain.....	43
3.4.6.2. Domaine de puissance.....	43

3.4.6.3. Temps de simulation.....	43
3.4.6.4. Nombre de nœuds.....	44
3.4.6.5. L'emplacement initial des nœuds.....	44
3.4.6.6. La bande passante.....	44
3.4.6.7. Protocoles et modèles à utiliser.....	44
3.4.6.8. Mobilité.....	45
3.4.6.9. Applications.....	46
3.4.6.10. Type statistique.....	46
3.4.7. LES STATISTIQUES OBTENUES DANS GLOMOSIM.....	47

Chapitre 4 : Conception et simulation

4.1. INTRODUCTION.....	52
4.2. CONCEPTION.....	52
4.2.1 DESCRIPTION DE LA SOLUTION.....	52
4.2.2. ALGORITHME.....	53
4.2.2.1 Composant de la couche réseau.....	53
4.2.2.2. Composant de la couche MAC.....	54
4.3. SIMULATION.....	55
4.3.1. ENVIRONNEMENT DE SIMULATION.....	56
4.3.1.1. Extension de GloMoSim.....	56
4.3.1.1.1. Implémentation du protocole Watchdog.....	56
4.3.1.1.2. Implémentation du protocole « Random Two-Hop ACK ».....	56
4.3.1.2. Métriques de comparaison.....	56
4.3.1.2.1. Taux de bonne détection.....	56
4.3.1.2.2. Taux de fausse accusation.....	57
4.3.1.2.3. Délai de bout en bout (End to end delay).....	57
4.3.1.2.4. Nombre de « Two-Hop ACK » (Overhead):.....	57
4.3.1.3. Paramètres et modèles utilisés.....	58
4.3.1.3.1. Modèle de mobilité.....	58
4.3.1.3.2. Modèle de propagation.....	58
4.3.1.3.3. Protocole de la couche MAC.....	58
4.3.1.3.4. La couche Application.....	58
4.3.1.4. Démarche de la simulation.....	59
4.4. RESULTATS ET ANALYSES.....	60
4.4.1. TAUX DE BONNE DETECTION.....	60
4.4.2. TAUX DE FAUSSE ACCUSATION.....	60
4.4.3. DELAI DE BOUT EN BOUT (END TO END DELAY).....	61
4.4.4. NOMBRE DE « 2 HOPS ACK ».....	61
4.5. CONCLUSION.....	62
CONCLUSION.....	63
BIBLIOGRAPHIE.....	64