République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A/Mira de Béjaia
Faculté des Sciences Exactes
Département d'Informatique

MÉMOIRE DE MASTER RECHERCHE

En
Informatique

Option
Réseaux et Systèmes Distribués

Thème

Incitation des nœuds ad hoc à participer au routage

Présenté par : Mlle OUZAR Lydia
M. SADI Chaouki

Soutenu le 02 Juliet 2016 devant le jury composé de :

Président	**Dr S. Boulefekhar**	**Maître de conf. A**	**U. A/Mira Béjaia.**
Promotrice	**Mme D. Boulahrouz**	**Maître assistante A**	**U. A/Mira Béjaia.**
Copromotrice	**Dr K. Adel**	**Maître de conf. A**	**U. A/Mira Béjaia.**
Examinateur	**Dr N. Rebouh**	**Maître assistante A**	**U. A/Mira Béjaia.**

Béjaia, Juliet 2016.

⁕ Remerciements ⁕

Avant tous, nous remercions le bon Dieu, le tout puissant, qui nous a donné la force et la patience pour réaliser ce travail.
Nous tenons à remercier toutes personne ayant contribué de prés ou de loin à l'élaboration de ce travail.
Ainsi, nous remercions Mr Bounouni Mahdi pour son savoir et sa patience.
Enfin, nous remercions nos promotrices Meme Boulahrouz et Meme Adel d'avoir voulu dirigé ce travail.

⁂ *Dédicaces* ⁂

À mes parents qui me sont les plus chers au monde, dont l'amour et les sacrifices n'ont pas cessé de combler ma vie ; (que Dieu les protège et les garde pour moi),
À mes très chères sœurs,
À mon binôme Chaouki,
À tous mes amis (es),
À tous mes enseignants,
À mes camarades de la promotion,
Et à tous ceux qui m'ont aidée de prés ou de loin.
Je dédie ce modeste travail.

Lydia

⁂ *Dédicaces* ⁂

À mes très chères parents,
À mes chères sœurs et frères,
À ma binôme Lydia,
À tous mes amis (es),
À tous mes enseignants,
À mes camarades de la promotion,
Et à tous ceux qui m'ont aidée de prés ou de loin.
Je dédie ce modeste travail.

Chaouki

Table des matières

Table des figures

Liste des Acronymes

ACK	**A**cknowledgment.
ACKREQ	**A**cknowledgment **R**equest.
AODV	**A**d hoc **O**n demande **D**istance **V**ector.
CANFIDANT	**C**ooperation **O**f **N**odes **F**airnes **I**n **D**ynamic **A**d hoc **N**etworks.
CORE	**CO**llaborative **RE**putation.
DARPA	**D**ifense **A**dvenced **R**esearch **P**rojects **A**gency.
DREAM	**D**istance **R**outing **E**ffect **A**lgorithm for **M**obility.
DSR	**D**ynamic**S**ource **R**outing.
FSR	**F**fisheye **S**tate **R**outing.
IEEE	**I**nstitue of **E**lectrical and **E**lectronic **E**ngeinerie.
LAR	**L**ocation **A**ided **R**outing.
MAC	**M**édium **A**cces **C**ontrol.
MANET	**M**obile **A**d hoc **NET**work.
NS2	**N**etwork **S**imulator **2**.
OCEAN	**O**bservation based **C**ooperation **E**nforcement in **A**d hoc **N**etwork.
OLSR	**O**ptimized **L**ink **S**tate **R**outing.
OSPF	**O**pen **S**hortest **P**ath **F**irst.
OTCL	**O**bject **T**ools **C**ommand **L**anguage.
RErr	**R**oute **Err**or.
RIP	**R**outing **I**nformation **P**rotocol.
RRep	**R**oute **Rep**lay.
RReq	**R**oute **Req**uest.
SORI	**S**ecure and **O**bjective **R**eputation based **I**ncentive.
SrcR	**S**ource and **R**oute.
TCP	**T**ecure and **C**bjective **P**eputation.
TWOACK	**TWO**ecure and **ACK**nowledjement.
ZRP	**Z**one **R**outing **P**rotocol.

Introduction générale

Les réseaux sans fil sont en plein développement du fait de la flexibilité de leur interface, qui permet à un utilisateur de changer facilement de place. Les communications entre équipements terminaux peuvent s'effectuer directement.

La norme 802.11 offre deux modes de fonctionnement des réseaux sans fil. Le premier est le mode infrastructure qui est défini pour fournir aux différentes stations des services spécifiques, sur une zone de couverture déterminée par la taille du réseau. Les réseaux d'infrastructure sont établis en utilisant des points d'accès qui jouent le rôle de station de base pour l'ensemble de stations. L'évolution des technologies de l'information et le penchant vers l'utilisation des machines sans fil qui se sont imposées ces dernières années ont fait émerger le deuxiéme mode de réseaux : les réseaux mobiles ad hoc, ou MANET (Mobile Ad hoc NETwork). Un réseau en mode ad hoc est un ensemble d'entités mobiles libres(nœuds) qui utilisent le médium radio pour communiquer et forment un réseau n'utilisant aucune infrastructure existante. De ces faits, ces réseaux qualifiés de spontanés présentent une architecture originale qui évolue à tout instant [9].

Les utilisations des réseaux ad hoc sont nombreuses et variées. Des scénarios à des fins militaires, d'opérations de secours lors de catastrophes naturelles, ou encore dans des réseaux de capteurs sont aujourd'hui avancés. Du fait de ces différents aspects et des ressources limitées des noeuds mobiles, un routage efficace est crucial dans les réseaux ad hoc car chaque noeud s'appuie sur son voisin pour transmettre ses paquets à la destination. En fait, la plupart des études antérieures sur les MANET ont implicitement supposé que les nœuds sont coopératifs. La coopération des noeuds devient donc très importante dans ces réseaux [8].

Problématique et objectifs

Les réseaux mobiles ad hoc sont connus par la limitation de la portée de transmission par l'interface réseaux sans fil. Il n'existe pas des routeurs ou des stations de base à utiliser pour l'échange d'informations entre les nœuds du réseau, chaque nœud est donc responsable de transmettre les paquets de ses voisins.

À cause de la contrainte rigoureuse des ressources tel que la mémoire, la puissance de calcul et surtout l'énergie, certain nœuds évitent de participer à la transmission des paquets de leurs voisins dans le but de conserver ces ressources.

Les nœuds dans les réseaux ad hoc peuvent avoir de mauvais comportements ce qui induit des pertes d'informations (paquets) et influence ainsi sur les performances du réseau. Un nœud peut se mal comporté de trois façons :

- Avoir un comportement malicieux : le nœud diffuse de fausses informations concernant ses voisins.
- Avoir un comportement opportuniste : le nœud profite des autres et essaye de maximiser son énergie au détriment du réseau.
- Avoir un comportement égoïste : le nœud refuse d'acheminer les paquets de ses voisins et conserve son énergie pour ses propres traitements.

Dans le cadre de ce travail, nous allons nous intéresser au problème de l'égoïsme des nœuds. EN fait, l'égoïsme des nœuds partitionne le réseau ce qui rend l'opération de routage plus difficile et complexe en augmentant le temps de transmission et l'énergie consommée par les nœuds du réseau.

Pour pallier à ce problème, plusieurs techniques existent dans la littérature pour la détection et l'isolation des nœuds égoïstes. Nous distinguons deux catégories : celles à base de réputation où la plus part des traveaux ne permettent pas de pénaliser les nœuds égoïstes ni de les inciter mais uniquement de les détecter. Et celles à base de crédit qui nécessitent un matériel de confiance ou un système centralisé pour gérer les paiments.

Il est donc important de trouver une solution qui remédié à ces problèmes. A cet effet nous proposons une approche qui consiste d'abord à détecter le nœud égoïste, ensuite d'essayer de l'encourager, de l'inciter ou même de l'obliger à transmettre les

paquets qui leur ont été confiés pour acheminer, et cela avant de décider de l'isoler du réseau et de l'éviter dans la création des routes. Enfin, à un certain moment, un nœuds égoïste peut décider d'arrêter de se comporter de façon égoïste et désire de coopérer avec ses voisins. Dans ce cas notre approche doit lui offrir une chance de réintégrer le réseau, ce qui est aussi rentable pour les performances du réseau.

Organisation de mémoire

Ce mémoire est organisé de la manière suivante :

Dans le chapitre 1, nous diffinissans les réseaux mobiles ad hoc, leurs caractéristiques et leurs dommaines d'application.

Dans le chapitre 2, nous présentons les concepts fondamentaux des protocoles de routage ad hoc notamment à travers la présentation d'exemples de protocoles et plus précisément le protocole de routage réactif DSR sur lequel se base notre travail. Nous terminons par les menaces de sécurité auxquels ces protocoles font face.

Le chapitre 3 présente l'état de l'art des mécanismes utilisés pour détecter les noeuds égoistes, leurs avantages ainsi que leurs inconvénients.

Le dernier chapitre (4) présente notre proposition. Après avoir défini l'environnement de simulation ainsi que l'implémentation faite, nous étudions ses performances en analysant les résultats obtenus après simulations pour prouver son efficacité. Ensuite, nous vérifions que cette solution ne dégrade pas les performances du réseau. Enfin, nous testons les limites de notre proposition.

Chapitre 1

Généralités sur les réseaux ad hoc

1.1 Introduction

Les réseaux sans fil traditionnels reposent sur une infrastructure partielle représentée par des stations de base fixe reliées par des liaisons filaires, l'inconvénient de ce type de réseaux c'est qu'ils requièrent le déploiement d'une importante infrastructure fixe. Pour cela, des réseaux qui n'ont besoin d'aucune infrastructure préexistantes ont évolué, appelés réseaux ad hoc qui sont utilisés à l'origine pour les applications militaires afin d'améliorer et de garantir la communication dans les champs de bataille. Ces derniers permettent l'accès rapide à l'information indépendamment du lieu et du temps.

Les nœuds mobiles eux même forment de façon ad hoc une infrastructure du réseau, ils participent ainsi dans le routage afin d'établir la connectivité du réseau.

Dans ce chapitre nous allons présenter ces réseaux, leurs caractéristiques ainsi que leurs domaines d'application.

1.2 Réseaux sans fil mobiles

Un environnement mobile est un système composé de nœuds mobiles et qui permet à ses utilisateurs d'accéder à l'information indépendamment de leurs positions

géographiques. Les réseaux mobiles peuvent être classés en deux classes : les réseaux mobiles basés sur une infrastructure de communication (modèle cellulaire), et les réseaux mobiles sans infrastructure (modèle ad hoc).

La norme la plus utilisée actuellement pour les réseaux sans fil est la norme IEEE 802.11.

1.2.1 Réseaux avec infrastructure

Les réseaux sans fil avec infrastructure sont généralement caractérisés par des sites fixes, appelés stations de base (SB) sont munis d'une interface de communication sans fil pour la communication directe avec les sites mobiles localisés dans une zone géographique limitée, appelée cellule comme le montre la figure 1.1 :

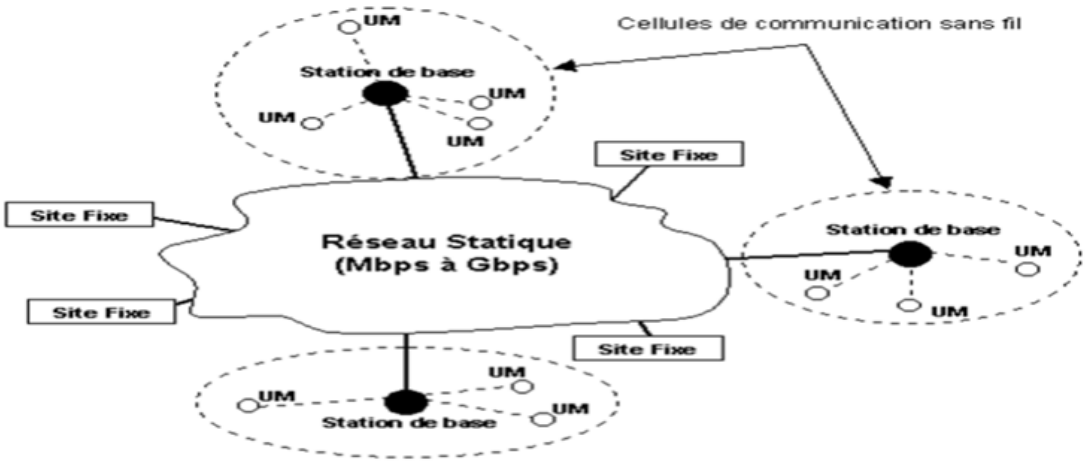

FIG. 1.1 – Exemple de réseau avec infrastructure [14].

UM : unité mobile.

1.2.2 Réseaux sans infrastructure

Contrairement aux réseaux avec infrastructure, dans ces réseaux, l'entité "site fixe" n'existe pas, tous les nœuds du réseau sont mobiles et se communiquent d'une manière directe en utilisant leurs interfaces de communication sans fil comme le montre la figure 1.2 . L'absence de l'infrastructure ou du réseau filaire composé des stations de base, oblige les nœuds mobiles à se comporter comme des routeurs qui participent à la découverte et la maintenance des chemins pour les autres nœuds du réseau

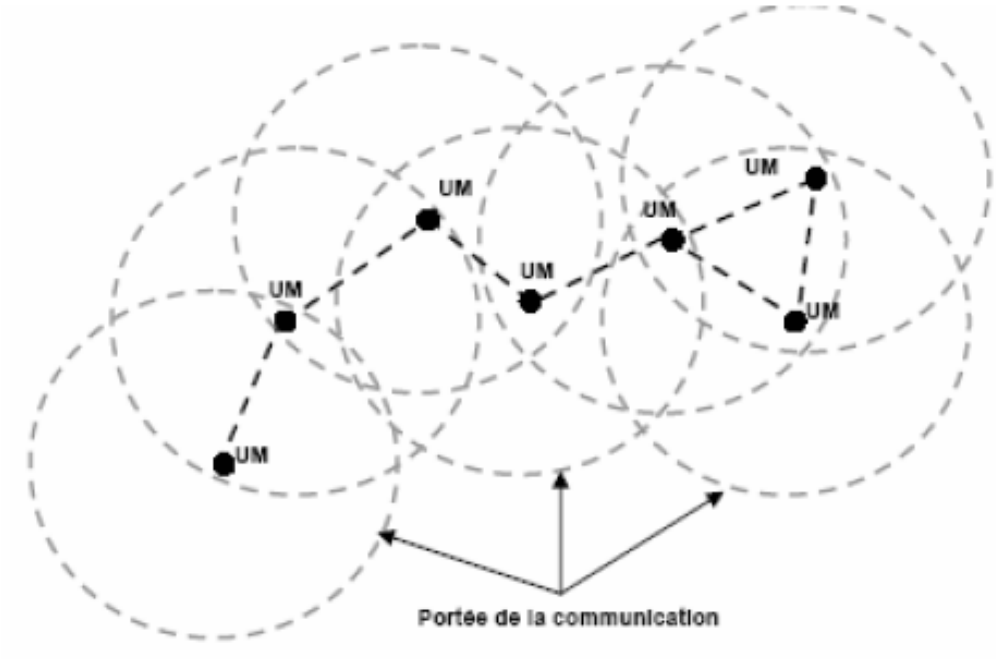

FIG. 1.2 – Exemple de réseau sans infrastructure (ad hoc) [14].

1.3 Réseaux ad hoc

1.3.1 Historique

À l'origine, les réseaux ad hoc sont utilisés pour les applications militaires. Au début des années 70, la première utilisation d'un réseau avec un médium radio au sein de projet DARPA (The Defense Advenced Research Projects Agency), il utilise une architecture distribuée et partage le canal tout en répétant des paquets pour élargir la zone de couverture global.

Par la suite, en 1983, le survival Radio Network (S4/RAN) à été développé, le but était d'attendre le réseau afin de dépasser les limitations (en particulier permettre le passage à des réseaux comportant énormément des nœuds gérant la sécurité, l'énergie,etc). Mais les recherches sur les réseaux ad hoc restent exclusivement militaires.

Pendant les années 90, des recherches dans le monde commercial sont apparus avec l'apparition du protocole 802.11 de l'IEEE (Institue of Electrical and Electronic Engeinerie) [9].

1.3.2 Définition

Un réseau mobile ad hoc, appelé généralement MANET (Mobile Ad hoc NETwork), est une collection de nœuds (terminaux, ordinateur portable, smartphone,etc) connectés via des interfaces sans fil communiquant directement ou reposant sur d'autres nœuds qui jouent le rôle des routeurs sans nécessité d'infrastructure externe ni d'administration centralisée [10].

1.3.3 Modélisation mathématique d'un réseau ad hoc

Un réseau ad hoc peut être modélisé par un graphe Gt = (Vt, Et) où Vt représente l'ensemble des nœuds du réseau et Et modélise l'ensemble des connections qui existent entre ces nœuds. Si e = (u, v) dans Et, cela veut dire que les nœuds u et v sont en mesure de communiquer directement à l'instant t [1].

1.3.4 Caractéristiques des réseaux ad hoc

Les réseaux ad hoc sont caractérisés principalement par [9] :

- **Absence d'infrastructure :** L'absence d'infrastructures préexistante et de tout genre d'administration centralisée est le caractère qui les caractérise le plus. Les nœuds mobiles sont responsables d'établir et de maintenir la connectivité du réseau d'une manière continue.
- **Topologie dynamique :** Les unités mobiles du réseau se déplacent d'une façon libre et arbitraire ce qui change la topologie du réseau à des instants imprévisibles (figure 1.3), d'une manière rapide et aléatoire ce qui provoque des erreurs de transmission.

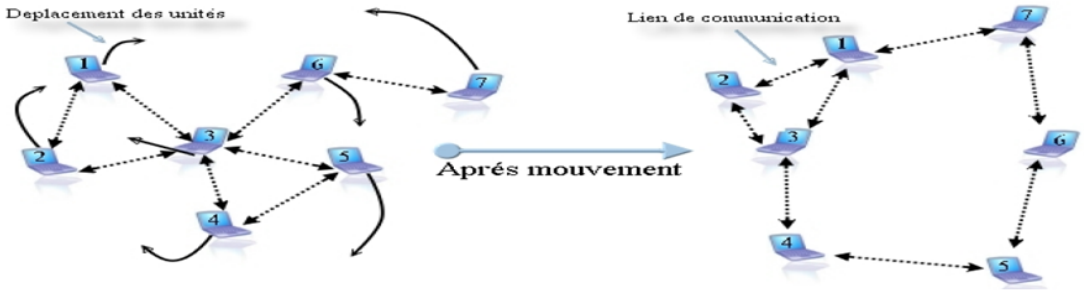

FIG. 1.3 – Mouvement des nœuds qui induit le changement de la topologie [10].

- **Équivalence des noeuds du réseau :** Dans un réseau classique, il existe une distinction nette entre les nœuds terminaux (stations, hôtes) qui supportent les applications et les nœuds internes (routeurs par exemple) du réseau, en charge de l'acheminement des données. Cette différence n'existe pas dans les réseaux ad hoc car tous les nœuds peuvent être amenés à assurer des fonctions de routage.
- **Bande passante limitée :** La bande passante est limitée et restreinte par rapport à celle offerte dans les réseaux filaires cela se justifie par le partage de médium de communication.

- **Contraintes d'énergie :** Les nœuds mobiles dans les réseaux ad hoc sont alimentés par des sources d'énergie autonomes comme les batteries ou les autres sources consommables, la consommation d'énergie devient alors un problème important car il affecte la durée de vie du réseau.
- **Sécurité limitée :** Pour les réseaux ad hoc, le principal problème ne se situe pas au niveau du support physique mais principalement dans le fait que tous les nœuds sont équivalents et potentiellement nécessaires au fonctionnement du réseau. Les possibilités de s'insérer dans le réseau sont plus grandes, la détection d'une intrusion ou d'un déni de service plus délicat et l'absence de centralisation pose un problème de remonter de l'information de détection d'intrusions.
- **Interférences :** Les réseaux ad hoc utilisent les transmissions radio pour transmettre l'information, ce qui rend les communications exposées aux interférences radio, ces derniers sont de nature diverse comme : le rapprochement des fréquences d'émission (interférences entre deux nœuds). Ces interférences font augmenter le taux d'erreurs de transmission, et le rendent incompréhensible par le récepteur.
- **Multi sauts (multihops) :** Plusieurs nœuds mobiles participent dans le routage de l'information.

1.3.5 Applications des réseaux ad hoc

Les réseaux ad hoc offrent une grande flexibilité ainsi qu'une rapidité et une facilité de mise en place, ils sont utilisés d'une façon générale dans toute application où le déploiement d'une infrastructure réseau fixe est trop contraignant, soit parce qu'il est difficile à mettre en place, soit parce que la durée et le cout d'installation du réseau ne le justifie pas [9].

Ces derniers peuvent se révéler trés utiles dans de nombreuses applications :

- **Domaine militaire :** Le domaine militaire a été un moteur initial pour le développement des réseaux ad hoc car l'utilisation d'une infrastructure fixe pour la communication est trés difficile dans un champ de bataille.

- **Cas d'urgences ou catastrophes naturelles (incendies, tremblement de terre, feux,etc) :** Il sera alors indispensable de disposer rapidement d'un réseau qui remplace le réseau détruit pour organiser les secours et les opérations de sauvetage ;

- **Communications dans des entreprises et batiments :**
  - Les batiments : Où il est impossible d'installer des cables convenablement (les vieux batîments, châteaux et monûments historique).
  - Les entreprises : Dans le cadre d'une réunion ou conférence.
- **Applications commerciales :** Pour le paiement électronique distant par exemple ou l'accès mobile à internet.
- **Cadre informatique :** Dans ce cas, on parle non plus de LAN (Local Area Network) mais de PAN (Personnal Area Network) ce qui est valable pour les gares et aéroports pour la communication et la collaboration entre les membres du personnel.

1.3.6 Communications dans les réseaux ad hoc

- La communication se fait directement si le destinataire est à un saut de l'émetteur ou à travers des nœuds intermédiaires qui agissent comme routeurs ;
- Le fonctionnement d'un réseau MANET dépend de la collaboration des différents éléments du réseau dans le routage ;
- Les nœuds peuvent se déplacer librement en restant connectés au réseau ;
- Le réseau subit fréquemment des changements de la topologie en raison de la mobilité des nœuds ;
- Le réseau utilise des ondes radio pour bénéficier ou bien offrir des services ;
- Les nœuds sont autonomes en matière de ressources surtout l'énergie ;
- Tous les nœuds sont équivalents.

1.4 Conclusion

Les réseaux ad hoc sont trés adaptés aux environnements mobiles grace à leur indépendance, leur flexibilité d'emploi, et leur faible coût de déploiement. Mais des mauvaises caractéristiques se présentent comme la limitation d'énergie. L'entité cen-

tralisé qui assure la tache de routage dans les réseaux filaires est absente, ce qui complique alors la fonction de routage pour la communication entre les nœuds.

Chapitre 2

Protocoles de routage dans les réseaux ad hoc

2.1 Introduction

La stratégie (ou le protocole) de routage est utilisée dans le but de découvrir et d'établir des chemins qui soient correctes et efficaces entre une paire quelconque de nœuds, ce qui assure l'échange des messages d'une manière continue.

Le problème qui se pose dans le contexte des réseaux ad hoc est l'adaptation de la méthode d'acheminement utilisée avec le grand nombre de nœuds existant dans un environnement caractérisé par de modestes capacités de calcul et de sauvegarde, c'est pourquoi certaines approches utilisés dans les routages classique sont inadéquates à ce type du réseau.

Mais la question qui se pose, en tenant compte des contraintes des réseaux ad hoc est que ces protocoles de routage permettent d'établir un meilleur acheminement entre les nœuds tout en maintenant le bon fonctionnement (un minimum de contrôle, de consommation de la bande passante, et de l'énergie) et sans dégrader les performance du réseau.

Dans ce chapitre, nous présentons d'abord les protocoles de routage existant selon des classifications, les différents types de protocole et leurs modes de fonction-

nement. En se terminant par la description des attaques et les vulnérabilités que subissent les réseaux ad hoc.

2.2 Définition de routage

Le routage définit l'acheminement d'un paquet envoyé par un émetteur, transmis à travers un ou plusieurs réseaux afin d'atteindre le destinataire. Le processus de routage se réalise grâce au routeur en exploitant les informations contenues dans sa table de routage [14].

La figure 2.1 illustre le chemin optimal reliant la source à la destination.

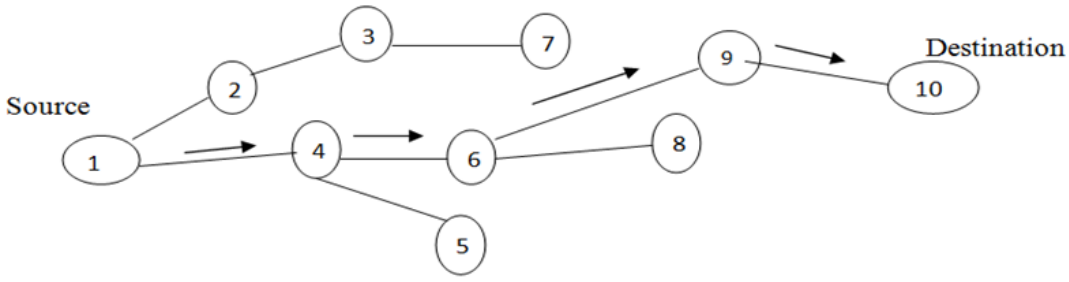

FIG. 2.1 – Chemin optimal entre une source et une destination.

Une bonne stratégie de routage utilise ce chemin pour transmettre les paquets entre les deux noeuds du réseau.

Pour être réellement opérationnel dans un environnement mobile, le protocole de routage prend en compte [12] :

- **Découverte de l'information de routage** : Cette étape permet de connaitre les éléments nécessaires sur la topologie utilisée afin de choisir un chemin qui peut atteindre la Destination.

- **Choix du chemin** : Après la collecte des informations obtenues, le protocole de routage peut choisir une route en se basant sur certains critères, par exemple : le nombre minimum de sauts, économie d'énergie et le cout,etc.
- **Maintenance des routes** : La topologie des réseaux ad hoc n'arrête pas d'évoluer avec le temps. Les routes sont dans l'obligation de changer à cause de la mobilité des nœuds, le protocole de routage doit prendre en considération ces changements et met à jour les nouvelles routes qui apparaissent et d'autres qui disparaissent.

2.3 Inadaptation des protocoles de routage Internet aux réseaux ad hoc

Les protocoles de routage exige un très grand nombre de trafic (l'échange des informations topologiques) afin d'établir la communication entre les nœuds du réseau. Cela consomme beaucoup de ressources.

Dans le cas des réseaux mobiles ad hoc sans fil, le besoin de minimiser la consommation des ressources réseau par le protocole de routage est de plus en plus pressant.

D'abord il n'existe pas d'infrastructure de routage, et le routage est effectué par les nœuds mobiles eux-mêmes.

Ensuite ces nœuds n'ont pas les capacités de traitement, de stockage et leurs sources d'énergie ne leur permettront pas d'assurer un échange périodique récurent de données de routage.

Enfin le fait que le canal radio soit partagé pose des soucis de sécurité quand à l'intégrité des tables de routage échangées entre les différents nœuds de routage.

Il en découle que les protocoles de routage dans internet ne sont pas tous adaptés aux MANET [9].

2.4 Classification des protocoles de routage dans les réseaux ad hoc

Il existe deux grandes familles de protocoles de routage : les protocoles basés sur l'état des liens, et ceux basés sur le vecteur de distance. Les deux méthodes exigent une mise à jour périodique des données de routage qui doivent être diffusées par les différents noeuds de routage du réseau. Les algorithmes de routage basés sur ces deux méthodes, utilisent la même technique qui est la technique des plus courts chemins, et permettent à un nœud donné, de trouver le prochain nœud pour atteindre la destination en utilisant le chemin le plus cours existant dans le réseau.

Plusieurs classifications ont été proposées pour les protocoles de routage ad hoc selon divers critères : la façon de création et de maintenance des routes, la façon d'acheminement des données, la façon dont les rôles sont accordés aux nœuds mobiles, etc.

2.4.1 Routage par localisation géographique, hiérarchique et plat

2.4.1.1 Protocoles plats

La décision d'un nœud de router des paquets d'un autre nœuds dépondra de sa position car tous les nœuds sont considérés égaux [13].

2.4.1.2 Protocoles hiérarchiques

La caractéristique du protocole de routage hiérarchique est le groupement multi niveaux et la division logique des nœuds mobiles. Le réseau est divisé en groupes (clusters), et un représentant (cluster head) pour chaque groupe est élu. Les nœuds d'un groupe physique diffusent leurs informations de liens entre eux et le chef de groupe récapitule l'information de son groupe et l'envoie aux chefs de groupe voisins [13].

2.4.1.3 Protocoles avec localisation géographique

Le routage géographique met l'accent sur le fait que chaque nœud connait ses coordonnées géographiques et utilise celles de la destination finale d'un paquet pour les décisions de routage, donc l'idée est d'envoyer le trafic à l'emplacement géographique d'un nœud plutôt qu'à son adresse IP. Ceci peut s'avérer intéressant dans la mesure où l'on n'a plus besoin d'une route vers la destination. Plusieurs protocoles de routage géographique ont été proposés dans la littérature, dont LAR (Location Aided Routing), DREAM (Distance Routing Effect Algorithm for Mobility), etc [13].

2.4.2 Routage à état de liens, à vecteur de distance et par la source

2.4.2.1 Protocoles à état de liens

L'état de lien est l'ensemble des liens vers les voisins d'un nœud. Des informations ont été rassemblées sur l'état des liens du réseau, ce qui permet aux nœud de construire un graphe complet du réseau. Ces protocoles peuvent calculer des chemins multiples ce qui augmente la répartition de la charge et de la tolérance aux pannes dans le réseau. (le protocole OSPF (Open Shortest Path First) est le plus connu) [7].

2.4.2.2 Protocoles à vecteur de distance

Ici, chaque nœud envoie à ses voisins la liste des destinations qui lui sont accessibles et le cout correspondant. Le nœud récepteur met à jour sa liste locale avec les couts minimums. (le protocole RIP (Routing Information Protocol) est le plus connu) [7].

2.4.2.3 Protocoles par la source

Le nœud source introduit dans l'entête du paquet les adresses des nœuds construisant le chemin à traverser par le paquet pour atteindre la destination. Le nœud qui ne s'agit pas de la destination, en recevant le paquet, supprime son adresse

et retransmet le paquet au nœud suivant qui est identifié dans la route source. Le même scenario se répète au niveau de chaque nœud traversé jusqu'à l'arrivé à la destination. (le protocole DSR (Dynamic Source Routing) est le plus connu)

2.4.3 Routage proactif, réactif, hybride

2.4.3.1 Protocoles proactifs

Les protocoles de routage proactif appelé aussi routage Table Driven sont basés sur le même principe de routage que les réseaux filaires. Les routes dans ce type de routage sont calculées à l'avance et tout nœud dispose à tout moment d'une route vers toute destination accessible du réseau. Chaque nœud met à jour sa table de routage par échange de paquets de contrôle entre voisins. En effet, si un nœud veut communiquer avec un autre, il a la possibilité de consulter localement la table de routage et de créer le chemin dont il a besoin.

Le besoin de conserver et de contrôler la validité des tables de routage en permanence (comprenant en outre des informations qui ne seront sans doute pas utilisées) est le principal inconvénient des protocoles proactifs. Par contre, ils présentent l'important avantage de ne nécessiter aucun délai avant de transmettre un paquet puisque la route est déjà connue. OLSR (Optimized Link State Routing) et FSR (Ffisheye State Routing) sont deux exemples de protocoles proactifs [7].

2.4.3.2 Protocoles réactifs

Les protocoles de routage réactifs représentent les protocoles les plus récents proposés dans le but d'assurer le service du routage dans les réseaux sans fil. La majorité des solutions proposées pour résoudre le problème de routage dans les réseaux ad hoc, et qui sont évaluées actuellement par le groupe de travail MANET, appartiennent à cette classe de protocoles de routage [13].

Contrairement aux protocoles proactifs, les protocoles réactifs ne calculent la route que sur demande d'où la dénomination (routage à la demande). A un instant donné, un nœud peut ne pas disposer d'une route vers un nœud de destination (car

aucun nœud ne connait la topologie du réseau). Dans ce cas, si un nœud S souhaite envoyer du trafic à un nœud D, alors S lance une procédure de recherche d'une route vers D. le plus souvent, le nœud S demande aux autres nœuds du réseau si quelqu'un connait une route vers D. les nœuds qui en connaissent lui répondront. Le nœud S enverra son trafic à un de ces nœuds qui se changera de l'acheminer à D [9].

Ces protocoles disposent généralement de deux mécanismes de base :

- Mécanisme de découverte de route (Route Discovery), grâce auquel un nœud cherche une route vers une destination ;
- Mécanisme de maintenance de route (Route Maintenance), grâce auquel un nœud maintient ses routes vers une destination ;

Cependant, le routage à la demande génère une lenteur à cause de la recherche des routes. Cela peut entraîner une dégradation des performances des applications. Ce type de protocole présente l'inconvénient d'être très coûteux en transmission de paquets lors de la détermination des routes mais a l'avantage de ne pas avoir à maintenir des informations inutilisées dans les tables de routage. AODV (Ad hoc On demande Distance Vector) et DSR sont deux exemples de protocoles réactifs.

2.4.3.3 Protocoles hybrides

Certains protocoles, dits hybrides tentent de combiner les meilleures caractéristiques de protocole proactif et réactif.

2.5 Protocole de routage DSR

DSR est un protocole de routage réactif se basant sur le principe de routage par la source, simple et efficace, dédié aux réseaux mobile ad hoc car il peut réagir aux changements topologique rapidement. Chaque nœud rassemble des informations sur la topologie du réseau à travers l'écoute des transmissions des autres nœuds. DSR est composé principalement (comme tous les protocoles réacifs) de deux mécanismes : La découverte des routes et la maintenance des routes. Le premier permet de déterminer automatiquement les routes nécessaires à la communication entre nœuds, tandis que

le second permet de s'assurer de la correction des routes tout au long de leur utilisation. Nous allons décrire ces deux mécanismes dans les sous sections suivantes.

2.5.1 Mecanisme de découverte de routes

La découverte des routes a pour but de trouver, au sein du réseau, les routes entre les nœuds désirant communiquer. Ainsi, DSR étant un protocole réactif, un nœud source S va rechercher une route uniquement s'il veut émettre un paquet vers un nœud destination D, et qu'il ne possède aucune route vers celui-ci dans son cache. Pour trouver la route depuis S, DSR initie un Route Discovery en émettant un paquet en diffusion (broadcast) d'en-tête RREQ, qui va inonder le réseau. Chaque nœud intermédiaire entre S et D qui reçoit un RREQ non dupliqué va concaténer son adresse à la liste contenue dans le RREQ et le diffuser à son tour.

Quand le nœud destinataire D reçoit le paquet, il retourne à la source un paquet d'en-tête RREP. En outre, dans le réseau, les noeuds peuvent enregistrer dans leur cache des informations de routage obtenues au travers des différents paquets Route Discovery reçus et des paquets de données. De plus, si un noeud intermédiaire qui recoit un RREQ possède en cache une route vers la destination D, alors il envoie un RREP à S en ajoutant la route connue. Finalement, le nœud source obtient plusieurs routes pour atteindre le destinataire. Une fois ces routes connues, le nœud va pouvoir envoyer des paquets de données.

2.5.2 Mecanisme de maintenance des routes

Dans un réseaux ad hoc, les noeuds étant mobiles, il faut vérifier, après l'envoi d'une donnée, que la topologie est toujours la même et que la source S peut utiliser une route pour atteindre la destination D. Pour ce faire, DSR utilise le mécanisme de maintenance de routes qui est une succession de trois procédures conditionnelles. Tout d'abord DSR interroge la couche liaison de données pour savoir si elle assure la maintenance des liens. Si cette dernière ne le fait pas, DSR va écouter tous les paquets dans sa portée radio. Chaque paquet est examiné pour savoir si c'est le paquet retransmis par le nœud suivant ou un autre paquet. Dans le premier cas

cela signifie que le lien était valide. Si finalement les deux premiers tests échouent, alors DSR va réémettre le paquet originel en y ajoutant une option de demande d'acquittement ou (Acknowledgment Request) (ACKREQ) auquel le noeud suivant devra répondre par un paquet d'acquittement (ACK).

En cas d'échec total de la maintenance de routes, le nœud détectant la rupture du lien mettra à jour son cache de route et enverra un paquet de type Route Error (RERR) en direction de la source. Celle-ci pourra choisir une nouvelle route ou recommencer une procédure de Route Discovery le cas échéant.

Soit l'exemple dans les figures 2.2 et 2.3 dont on veut établir une route entre le nœud source S et le nœud destination D en utilisant le protocole de routage DSR :

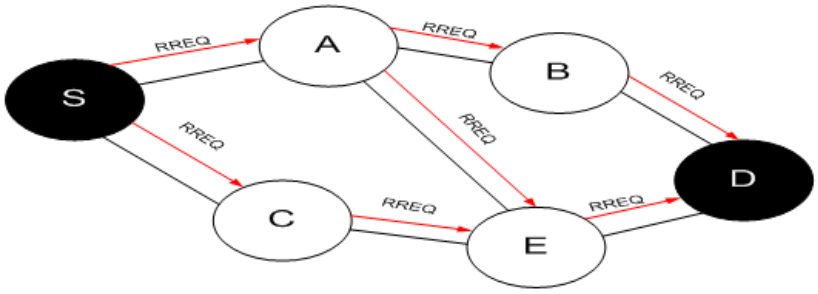

FIG. 2.2 – Diffusion de RREQ pour l'établissement d'un chemin entre les nœuds S et D.

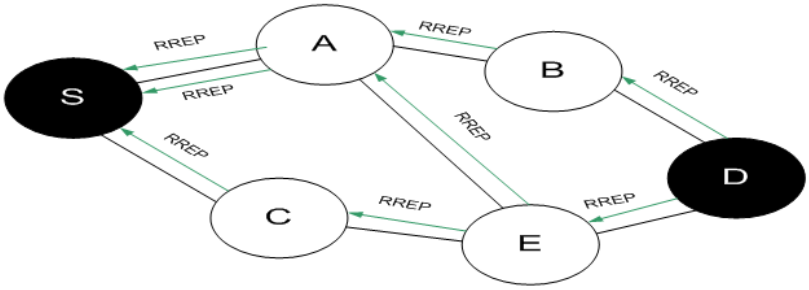

FIG. 2.3 – Le nœud D répond par RREP.

2.5.3 Avantages du protocole DSR

Ce type de routage présente certains avantages particulièrement intéressants :

- Autorise la source à conserver dans son cache plusieurs chemins valides vers une même destination ;
- Le choix de chemin emprunté pourra être fait indépendamment pour chaque paquet ;
- Permet un meilleur équilibrage de la charge du réseau ;
- Permet une meilleure réactivité aux pannes et le changement de la topologie (quand une route est brisée, la source a d'autres à disposition immédiate).

2.6 Attaques et vulnérabilités sur des réseaux ad hoc

Il existe plusieurs raisons qui rendent les réseaux mobiles ad hoc vulnérables aux attaques :

- **Mobilité des nœuds** : Cela qui induit le changement dynamique de la topologie du réseau. Ces attaques interviennent sur le service de transport des paquets d'un point à un autre qui est le but principal des protocoles de routage.

- **Technologie sans fil** : Quiconque possédant le récepteur adéquat peut potentiellement écouter ou perturber les messages échangés.
- **Comportement des nœuds** : Les nœuds eux mêmes sont des points de vulnérabilités du réseau car un attaquant peut compromettre un élément laissé sans surveillance.
- **Absence d'infrastructure fixe** : Pénalise l'ensemble du réseau dans la mesure où il faut faire abstraction de toute entité centrale de gestion pour l'accès aux ressources.
- **Mécanismes de routage** : Sont d'autant plus critiques dans les réseaux ad hoc que chaque entité participe à l'acheminement des paquets à travers le réseau. De plus, les messages de routage transitent sur les ondes radio.

2.6.1 Attaques fréquentes sur les réseaux ad hoc

Nous allons maintenant classer et décrire quelques attaques possibles sur les MANET et le protocoles de routage [23] [17] [11].

2.6.1.1 Attaques passives

- **Eavesdropping :** L'attaque la plus simple sur un réseau sans fil est l'écoute ; il nécessite un minimum de préparation et ne peut pas être détecté. Eavesdropping peut être subdivisé comme suit :
  - Le contenu de la communication. Comme il existe différentes techniques pour chiffrer le contenu, ce qui garantit sa confidentialité. Comme le cryptage est coûteux, les utilisateurs des clients mobiles peuvent choisir de ne pas chiffrer afin d'économiser les ressources énergétiques.
  - Infrastructure méta-données, y compris les options de protocole utilisées et en particulier des informations de routage. Le chiffrement de cette communication est possible, mais généralement pas nécessaire parce qu'il faudrait avoir une gestion des clés sophistiquée.
  - Le montant et la distribution de la communication ou de l'emplacement des nœuds. Même sans connaître le contenu, un indiscret peut encore détecter

les modèles de trafic entre les nœuds. En théorie, cela pourrait être évité en envoyant au hasard un message entre les nœuds, mais dans des environnements mobiles cela est impossible en raison des contraintes d'énergie. dépendamment sur l'utilisation et la politique de MANET même la divulgation de l'emplacement d'un nœud peut être considérée comme un succès de violation de la sécurité.

- **non participation :** Après avoir rejoint le réseau mobile, un nœud pourrait tout simplement refuser de transmettre les données d'un autre nœud. Il existe deux alternatives :

– Le noeud répond aux messages (route request) de demande de chemin, mais en devenant partie de la route, il rejette silencieusement les données qu'il est censé transmettre.

– Le noeud ne répond pas pour acheminer des messages de requête.
Ces deux altérnatives représentent un comportement égoïste auquel s'intéresse notre travail.

2.6.1.2 Attaques actives

- **Déni de service :** Avec suffisamment de ressources un attaquant peut toujours envoyer plus de données que les autres nœuds peuvent traiter. Les clients mobiles sont particulièrement vulnérables à des attaques de déni de service, car il draine rapidement leur énergie réservée. Une autre approche possible n'a même pas besoin pour envoyer de grandes quantités de données, mais simplement d'envoyer suffisamment de paquets pour empêcher un nœud d'entrer dans le mode sommeil pour l'économie d'énergie ; ce qu'on appelle la privation de sommeil.
- **Manipuler des données transmises :** Ceci est une attaque potentiellement dangereuse, mais assez simple pour prévenir en utilisant un message d'authentification.
- **Manipuler le routage des méta-données :**
  – Simple déni de service : Certains protocoles de routage permettre des

attaques très simples, comme l'envoi de données pour des cibles non-existantes, créant ainsi une voie d'enquête diffuser.

- Trou noir : Un nœud peut s'annoncer comme ayant le chemin le plus court vers tous les autres nœuds, ce qui perturbe les routes existantes et attire beaucoup de trafic. Obtenir une grande quantité de données conduit à de nouvelles opportunités comme la transmission de manière sélective ou l'abandon de paquets (parfois appelé trou gris).
- Wormhole : En collaboration, les attaquants peuvent créer deux ou plus de trous noirs et les connecter. Cela leur donne un contrôle sur de grandes parties du MANET et ses paquets.
- Eclipse : En collaboration, les attaquants peuvent partitionner le réseau, contrôlant ainsi toutes les données circulant entre les partitions. En fonction du nombre d'attaquants, un d'entre eux peut séparer les nœuds simples, obtenir entre une station de base et ses clients ou même bipartition de réseau.
- Sybil attaque : Un seul nœud malveillant peut simuler un certain nombre de nœuds indépendants. Ceci est une base pour beaucoup de manipulations : il favorise le client dans l'allocation de la bande passante, ce qui influence sur les décisions de routage.

2.7 Conclusion

Dans ce chapitre, nous avons défini les différentes techniques qui existent pour le routage d'informations dans les réseaux ad hoc ainsi que les différentes attaques qui peuvent intervenir sur ces protocoles en empêchant la bonne transmission des données. Parmi ces attaques, nous avons parlés sur celles passives tel que l'égoïsme des nœuds. Divers solution sont été proposées pour régler ce problème et elles sont détaillées dans le chapitre suivant.

Chapitre 3

Etat de l'art sur les solutions existantes

3.1 Introduction

Les réseaux mobiles ad hoc sont connus par la limitation de la portée de transmission par l'interface réseaux sans fil. Il n'existe pas des routeurs ou des stations de base à utiliser pour l'échange d'informations entre les nœuds du réseau, chaque nœud est donc responsable de transmettre les paquets de ses voisins.

À cause de la contrainte rigoureuse des ressources tels que la mémoire, la puissance de calcul, le temps et surtout l'énergie, certain nœuds évitent de participer à la transmission des paquets de leurs voisins dans le but de conserver ces ressources.

La présence de comportement égoïste de certains nœuds produit un impact négatif qui est le partitionnement du réseau.

Plusieurs mécanismes de détection et d'isolation des nœuds égoïstes ont été alors développés et sont classées en deux catégories : les systèmes à base de réputation [21] [20] [16] [19] [18] [8] et les systèmes à base de crédit [15] [4].

3.2 caractéristiques des nœuds égoïstes

Un nœud égoïste se caractérise par :

- Ne pas participer dans le processus de routage : Un nœud égoïste détruit les messages de routage.
- Ne pas répondre ou envoyer des messages hello : Un nœud égoïste peut ne pas répondre à des messages hello, donc les autres nœuds peuvent ne pas être en mesure de détecter sa présence quand ils en ont besoin.
- Retarder intentionnellement le paquet RREQ : Un nœud égoïste peut retarder le paquet de RREQ jusqu'à un maximum de temps limité. Il va certainement s'éviter de chemins de routage.
- Abandon du paquet de données : Un nœud égoïste peut participer à l'acheminement des messages, mais pas à la transmission des paquets de données.

La littérature fournit diverses stratégies pour faire face à un tel comportement.

Ces stratégies peuvent être classées en deux catégories de base : approche de motivation et d'incitation et approche de détection et d'exclusion [5].

3.3 Types des nœuds égoïstes

L'égoisme d'un nœud paut être définie de trois manières :

- Le nœud participe dans la découverte et la maintenance des routes mais il refuse d'acheminer les paquets de données dans le but de réserver ses ressources ;
- Le nœud ne participe jamais dans la phase de découverte des routes ni dans la phase d'acheminement des paquets de données, il utilise ses ressources seulement pour la transmission de ses propres paquets ;
- Le nœud se comporte soit comme le premier type soit comme le deuxième selon son énergie [4].

Le type d'égoïsme dans notre travail est le premier type : les nœuds dans ce cas coopèrent dans la phase de découverte des routes avant qu'ils deviennent égoïstes dans la phase de transmission des paquets de données.

3.4 Problèmes dus à la présence de nœuds égoïstes dans un réseau ad hoc

- **Partitionnement de réseau :** En raison de la présence de nœuds égoïstes, le partitionnement de réseau se produit plus souvent dans les MANET. le partitionnement de réseau est un problème grave lorsque le serveur qui contient les données requises est isolé dans une partition séparée, réduisant ainsi l'accessibilité des données à une large mesure.
- **Disponibilité des données :** La perte d'une partie des liens et des nœuds considérés comme critiques peut diviser le réseau en plusieurs partitions disjointes, en présence des nœuds égoïstes. Les nœuds mobiles dans l'une des partitions ne peuvent pas accéder aux données détenues par les nœuds mobiles dans l'autre partition. Cette situation réduit considérablement la disponibilité des données.
- **Durée de vie du réseau :** Dans MANET, la performance du réseau devient très dépendante de la collaboration de tous les nœuds membres. Un nœud à volonté égoïste ne coopère pas généralement à la transmission des paquets pour sauver ses ressources, il affecte sérieusement la durée de vie du réseau.
- **Débits :** Le pourcentage des paquets reçus par la destination au nombre de paquets envoyés par la source est affecté par la disposition des nœuds égoïstes dans MANET.
- **Nombre de sauts :** Un saut est un segment de chemin entre la source et la destination. Chaque nœud le long de chemin de routage de données comprend un bond. Si le nombre de nœuds égoïstes augmente, le nombre de sauts intermédiaires de la source à la destination accru ce qui pourrait diminué les performances de réseau.
- **Ratio d'abandon des paquets :** Nombre des paquets abandonnés par les routeurs en raison des nœuds qui agissent comme égoïstes pour sauver leurs ressources.
- **Ratio de livraison des paquets :** Est la fraction du nombre de paquets

de données délivrés au nœud destination à partir d'un nœud source. Elle est affectée par les nœuds égoïstes.

- **Délai End-to-End :** Est le temps consommé par un paquet de données pour être transférés à travers le MANET d'un nœud source au nœud destination. Il est augmenté par la présence des nœuds égoïstes.

Ces caractéristiques pourraient potentiellement conduire au partitionnement de réseau et correspondant à une dégradation de ses performances. Pour minimiser ces situations dans les MANET, de nombreuses études ont exploré des techniques basées sur la réputation ou sur le crédit [22].

3.5 Techniques à base de réputation

La réputation étant la perception qu'un nœud a d'un autre nœud à propos de ses intentions, au vu d'un ensemble d'anciennes actions (observations antérieures) et qui peut être combinée à d'autres points de vue (recommandations). Ainsi, par son comportement un nœud ne pourra pas décider de sa réputation mais pourra influencer sa propre réputation. Une valeur numérique est associée à la réputation d'un noeud dont le calcul diffère d'une solution à une autre mais qui se base essentiellement sur la surveillance du voisinage.

Dans une technique basée sur la réputation, chaque nœud est responsable de la surveillance de la transmission d'un paquet au nœud voisin, ou de l'obtention de l'état des autres nœuds à partir d'un nœud centralisé sur le réseau. Si un nœud contribue avec succès la transmission en transmettant les paquets de données, sa réputation est augmentée ; si le nœud rejette le paquet, sa réputation est diminuée. Après que la réputation des nœuds tombe au-dessous d'un certain seuil, le nœud est soit puni ou ignoré.

La figure 3.1 ci-dessous représente le classement des différentes techniques de détection des nœuds égoïstes basées sur la réputation.

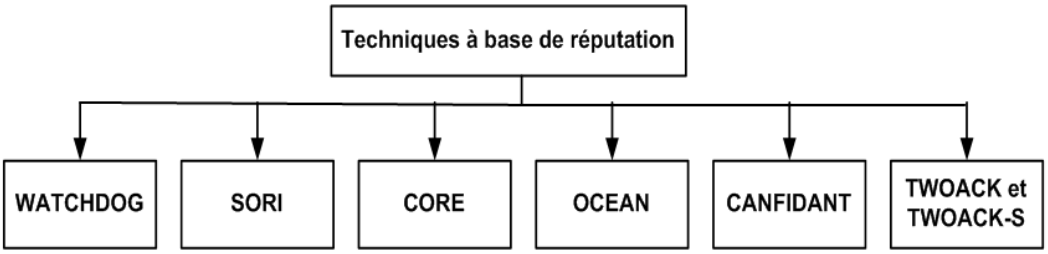

FIG. 3.1 – Techniques à base de réputation.

3.5.1 Watchdog

Dans [21], Marti, Giuli, Lai et Baker proposent la technique de chien de garde. Chaque nœud a un mécanisme qui surprend le moyen de vérifier si le nœud de saut suivant a fidèlement transmis le paquet ou non. Chaque nœud maintient un tampon des paquets récemment transmis et compare chaque paquet entendu avec ceux dans le tampon pour voir s'il y a une égalité. Si ce dernier surprend l'acheminement, il enlève le paquet à partir de la mémoire tampon et détermine que ce nœuds a un comportement normal. Si un paquet a séjourné dans la table pendant une certaine période, le nœud incrémente un compteur de défaillance pour le nœud responsable de la transmission de paquet. Si ce compteur dépasse un certain seuil, il détermine que le nœuds est infidèle (a une mauvaise conduite) et envoie un message à la source en lui avisant du ce nœud malveillant.

Avantages et Inconvénients

La force de ce mécanisme est de détecter le nœud égoïste avec précision et à maintenir le débit du système à un niveau adéquat même avec un nombre important des nœuds malveillants et il peut identifier le nœud égoïste dans la couche liaison et la couche réseau.

Parmi les inconvénients de ce mécanisme nous citons :

- Il ne peut pas détecter les nœuds égoïstes en cas d'une puissance d'émission limitée, ambigüité de collision, collision au niveau récepteur, etc.
- Il ne convient que pour les protocoles de routage à source tels que DSR.
- Cette technique ne pénalise pas les nœuds égoïstes non coopérants et les omet réellement de la charge d'acheminement des autres. Par conséquent, étant égoïste devient une bénédiction pour les nœuds mobiles eux même.
- Le watchdog ne peut fonctionner que lorsque les liens sont bidirectionnels. En pratique, des liens unidirectionnels peuvent exister dans MANET.
- Chaque nœud mobile nécessite une certaine quantité d'espace mémoire pour conserver les paquets jusqu'à ce qu'une bonne transmission par son voisin est confirmée. Par conséquent, cette technique consomme un volume de stockage élevé.

3.5.2 Pathrater

Les auteurs dans [21] proposent cette technique pour la sélection des chemins fiables de la source jusqu'à la destination. Dans ce mécanisme, chaque nœud du réseau conserve une note pour tous les autres nœuds mobiles. Il calcule les métriques de chemin en faisant la moyenne des notes des nœuds sur les chemins et la métrique donne une comparaison de la fiabilité globale des différents chemins. Après le calcul des métriques pour chaque chemin d'un emplacement particulier, le chemin qui a la plus haute métrique sera choisi comme un chemin fiable et il est décidé par le pathrater. Si un nœud obtient une très faible note, il devrait être considéré comme un nœud égoïste et donc il est exclu du routage.

Avantages et inconvénients

L'avantage de pathrater est l'augmentation de débit avec l'augmentation de la mobilité des nœuds.

Les principaux inconvénients de cette approche sont qu'il ne punit pas les nœuds égoïstes et si la mobilité des nœuds augmente, les frais généraux augmentent également.

Il se concentre pour sélectionner le chemin fiable mais ne traite pas la récupération du nœud égoïste.

3.5.3 Confident

Est une technique efficace pour la détection des nœuds égoïstes proposée par Buchegger et Le Boudec dans [20]. L'objectif de cette approche est de détecter et isoler ces nœuds. Dans cette approche, les valeurs de réputation et de confiance sont calculées à base d'observation et d'expérience sur le comportement des autres nœuds.

La figure 3.2 représente les composants de mécanisme de Confident tel qu'un moniteur, système de réputation, gestionnaire de confiance et gestionnaire de chemin.

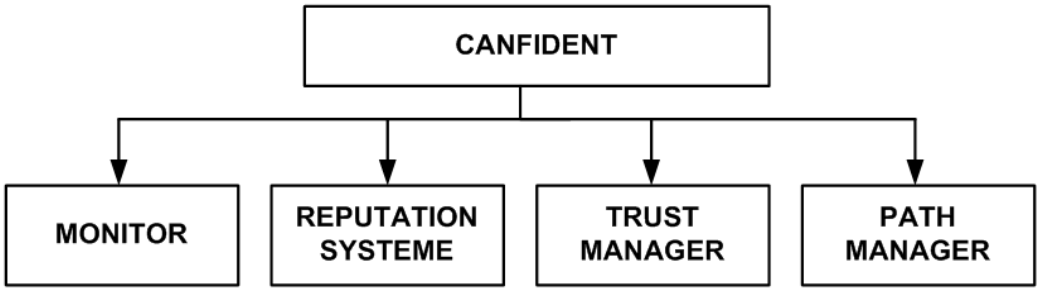

FIG. 3.2 – Composants de mécanisme de Confident.

- Moniteur : Il est responsable de l'observation et l'enregistrement de l'égoïsme des nœuds voisins.
- Système de Réputation : Chaque nœud maintient une liste locale des notes de chacun de ses nœuds voisins, ce qui pourrait être échangé avec ses voisins non égoïstes.
- Gestionnaire de confiance : Il est responsable de l'envoi des avertissements sur les nœuds qui se comportent mal.
- Gestionnaire de chemin : Il est responsable de la punition des chemins contenant des nœuds mal comportés en fonction de leurs réputation, et de décider

ce qui devrait être quand un nœud malveillant demande le chemin ou un nœud bien comporté demande un chemin qui contient des nœuds malveillants.

Avantages et inconvénients

Les avantages de cette approche est l'évitement des mauvaises routes et il y a une possibilité d'augmentation de débit si la mobilité augmente. Mais cette approche pose aussi des problèmes :

- problème d'incohérence : chaque nœud a des évaluations différentes pour un même nœud lors de la détection des nœuds égoïstes.
- L'espionnage n'est pas abordé.
- Les nœuds de la liste noire sont ignorés.
- Le besoin d'une plus grande consommation d'énergie pour les nœuds situés au centre du réseau en comparaison avec ceux situés à la périphérie du réseau.
- L'évolutivité est un autre problème en raison de la validation de la clé et de la certification au niveau de gestionnaire de confiance.

3.5.4 CORE

Dans [16], Michiardi et Molva proposent ce mécanisme pour détecter et isoler les nœuds égoïstes, il améliore également la coordination entre les nœuds en utilisant la réputation et la surveillance collaborative. CORE classe trois types de réputation qui sont combinés pour former une valeur commune de réputation pour un nœud mobile.

Chaque mesure est normalisée de telle sorte que la réputation varie de -1 (mauvais) à +1 (bon). 0 représente une vue neutre utilisé quand il n'y a pas assez d'observations pour faire une évaluation de la réputation d'un nœud.

- Réputation Subjective [-1, 1] est basée sur le calcule des observations passées.
- Réputations indirectes sont observées par le nœud X à travers Z à propos de Y, seules les valeurs positives de réputation sont utilisées pour éliminer une attaque où un nœud égoïste transmet des informations négatives de réputation dans le but de causer un déni de service.

- La fonction de réputation qui combine les deux types de réputations subjectives et indirectes qui est progressivement diminuée à une valeur nulle s'il n'y a pas d'interaction avec le nœud observé.

Avantages et inconvénients

Ce mécanisme permet d'éviter les attaques de déni de service, il est impossible pour un nœud de diminuer malicieusement la réputation d'un autre nœud car il n'y a pas un écart négatif entre les nœuds. Toutefois, CORE souffre des attaques spoofing, il ne peut pas empêcher les nœuds de distribuer une réputation négative, la limitation de la puissance de transmission et les antennes directionnelles ne sont pas abordées.

3.5.5 OCEAN

Proposé par S. Bansal et M. Baker dans [19], c'est une extension du protocole DSR. Ce mécanisme se base également sur la surveillance et la réputation.

Chaque nœud contient cinq composants :

- **Neighbor watch module :** Il surveille le comportement des voisins d'un nœud.
- **Route Ranker Module :** Calcule et maintient un rapport pour chacun des nœuds voisins.
- **Rank-based Routing :** Il aide à omettre les routes contenant des nœuds de la liste bloquée.
- **Malicious Traffic Rejection :** Rejette tout le trafic des nœuds qu'il décide qu'ils sont trompeurs.
- **Second Chance Mechanism :** Il est prévu de donner une autre possibilité d'opérer en tant que nœuds normaux après qu'étaient considérés comme malveillant auparavant.

  La figure 3.3 représente l'ensemble de ces composants

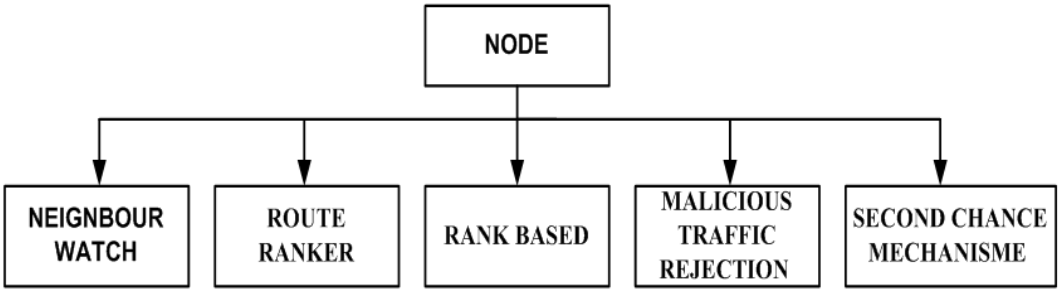

FIG. 3.3 – Composants de mécanisme OCEAN.

Avantages et inconvénients

Cette approche a les avantages suivants :

- Elle distinguera les nœuds égoïstes et trompeurs.
- Elle maintient le débit du réseau global avec l'existence des nœuds égoïstes à la couche réseau.

Néaumoins, elle ne parvient pas à punir sévèrement des nœuds de mauvais comportement.

3.5.6 SORI

Proposé par He, Wu, et Khosla dans [18], c'est une approche d'encouragement du transfert de paquets et de faire discipliné le comportement égoïste en utilisant le mécanisme de punition à base de réputation. La valeur de réputation d'un nœud se base sur le taux de transfert des paquets des autres nœuds.

Cette approche dispose de trois modules : la surveillance des voisins, la propagation de la réputation et la punition.

- Système de surveillance des voisins : chargé de recueillir des informations sur le comportement des paquets de transmission des voisins, le nœud N compte le nombre des paquets envoyés par le nœud N au nœud X, appelé RFN (X) (requête de transmission), et le nombre des paquets actuellement transmis par

le nœud X au nœud N, appelée HFN (X). la Réputation d'un nœud est calculée à partir de ces valeurs. La valeur de confiance d'un nœud est directement proportionnelle au nombre des paquets transmis par le nœud (RFN (X)). cette valeur de confiance est utilisée pour donner une haute priorité à la valeur de réputation reçue par le nœud.

- Système de propagation de la réputation est responsable de la communication de réputation des nœuds entre les voisins quand il y a des changements significatifs dans la réputation de certains nœuds. Une façon de hachage est utilisée pour l'authentification des messages contenant les informations de réputation et des paquets de données.
- Système de punition est responsable de décider de la probabilité d'abandon de paquets provenant d'un nœud malveillant en proportion de son égoïsme.

Avantages et inconvénients

Il est efficace par rapport aux autres méthodes car il réduit le nombre de communications.

Il ne parvient pas à différencier les nœuds malveillants et égoïstes. Il dispose également d'une mauvaise performance dans le cas de la coopération des nœuds.

3.5.7 TWOACK

TWOACK est une technique proposée par Balkrishnan et al dans [8] qui visent à résoudre la collision au niveau de récepteur et la puissance de transmission limitée des problèmes de Watchdog, il permet de détecter rapidement les nœuds égoïstes ou non coopératifs dans un réseau ad hoc puis de chercher à atténuer le problème en avertira le protocole de routage afin d'éviter les routes dans l'avenir. Comme il peut aussi détecter les liens de mauvaise conduite par reconnaissance de tous les paquets de données transmis sur chaque trois nœuds consécutifs le long du chemin depuis la source à la destination. Lors de la récupération d'un paquet, chaque nœud le long de la route est tenu de renvoyer un paquet (TWOACK) au nœud qui est à une distance

de deux sauts vers la source. TWOACK est requis pour travailler sur des protocoles de routage tel que DSR.

Le principe de ce modèle est simple, il est représenté sur la figure 3.4. Le nœud A transmis premièrement le paquet 1 au nœud B qui le transmis à son tour au nœud C. Lorsque le nœud C reçoit le paquet 1, il est endetté à créer un paquet TWOACK contenant le chemin inverse (celui empreinté par le paquet l) et le renvoyé au nœud A. cette procédure se répète pour tous les triplets de nœuds consécutifs qui constituent le chemin qu'empreinte le message.

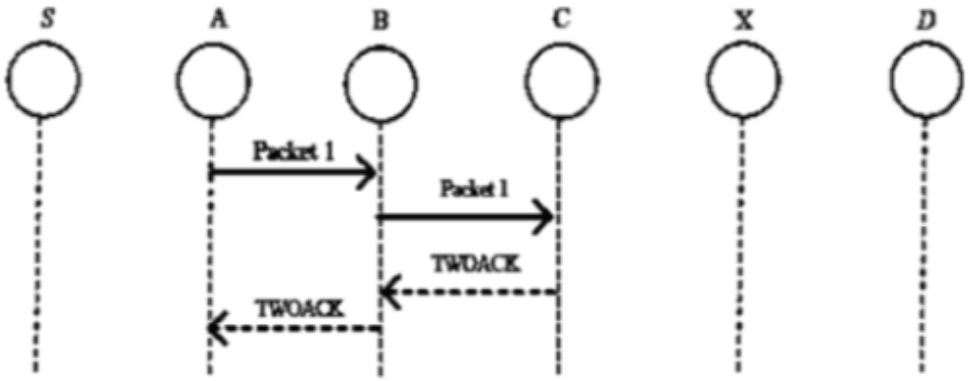

FIG. 3.4 – Fonctionnement de l'approche TWOACK.

Afin de détecter le mauvais comportement d'un nœud, l'émetteur maintient à son niveau une liste d'ID des messages dont il n'a pas encore reçu de paquet TWOACK d'un nœud à deux sauts, et chaque élément dans cette liste contient les champs informations suivants :

- Les récepteurs du message dans les deux prochains sauts
- Un compteur de nombre de détection de mal comportement noté Cmis.
- LIST : une liste d'ID des paquets de données qui ne sont toujours pas acquittée d'un paquet TWOACK.

Prenons un autre exemple (figure 3.5), Supposons qu'un nœud A veuille envoyer un paquet en empruntant le chemin (A,n1,n2), il ajoute l'ID du paquet à LIST dans la liste correspondantes au lien (n1,n2). Quand A reçoit un paquet TWOACK, il

vérifie l'ID et le retire de LIST. Si après un temps dit TimeOut, A ne reçoit pas un paquet TWOACK pour un certain paquet, alors le lien (n1,n2) sera suspecté, et le compteur Cmis de ce lien sera incrémenté. Lorsque le Cmis dépasse un certain seuil noté tresh déclare le lien (n1,n2) come égoïste, et envoie un paquet pour informer la source. Tout nœud recevant ce message mettra ce lien come égoïste. Ainsi chaque nœud sera en possession des informations concernant les liens égoïstes et pourra les éviter dans la sélection du chemin de routage de paquet.

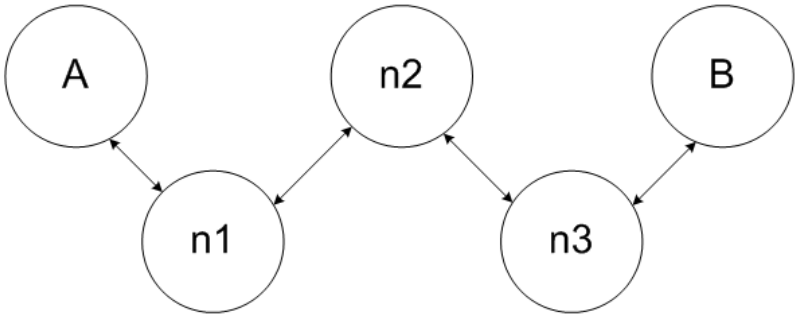

FIG. 3.5 – Ilustration de l'exemple.

Avantages et inconvénients

Cette approche a les avantages suivant :

- TWOACK vise à résoudre la collision au niveau de récepteur et la puissance de transmission limitée des problèmes de Watchdog.
- Détecter rapidement les nœuds égoïstes ou non coopératifs dans un réseau ad hoc puis chercher à atténuer le problème en avertira le protocole de routage afin d'éviter les routes dans l'avenir.
- Détecter les liens de mauvaise conduite.

Cependant cette technique pose certains problème :

- La surcharge du réseau par les messages TWOACK.
- Ce régime ne peut pas distinguer exactement quel nœud particulier est égoïste.
- Les nœuds normaux peuvent devenir une partie d'une liaison infidèle et par

conséquent on ne peut pas utiliser largement le réseau ce qui provoque la congestion du trafic sur le réseau

3.5.8 S-TWOACK

Les paquets TWOACK peuvent contribuer à la congestion du trafic sur le chemin de routage, pour remédier à ce problème, les auteures ont proposé S-TWOACK. Ici, au lieu de renvoyer un TWOACK par paquets à chaque fois qu'un paquet de données est reçu, un nœud attend jusqu'à ce qu'un certain nombre de paquets de données (par le biais du même triplet) arrivent. Le nœud renvoie alors un paquet TWOACK reconnaître plusieurs paquets de données qui ont été reçue. Donc, dans cette approche, une réduction significative des frais généraux de routage est atteinte [8].

3.6 Techniques à base de crédit

Cette approche essaie de motiver les utilisateurs du réseau à participer activement aux activités de transfert. Un tel système implique certaine transfert d'argent aux nœuds intermédiaires, au nom de la source ou de destination, pour les inciter à transférer des messages.

3.6.1 Nuglets

Cette approche proposée par Jamal N. Al-Karaki Ahmed E. Kamal dans [15] se base sur une monnaie virtuelle appelée nuglet. Chaque nœud de réseau a un stock initial de nuglets. La source ou la destination utilisent ces nuglets à payer les nœuds qui participent dans l'acheminer de trafic.

Par rapport au paiement à partir de la source ou de la destination, on distingue deux modèles.

3.6.1.1 The Packet Purse Model

Dans ce modèle, l'expéditeur du paquet paie pour le service de transfert de paquets. Les frais de service sont distribués parmi les nœuds de transfert. L'initiateur est chargé avec le nombre de grains suffisants pour atteindre la destination. Chaque nœud de transfert acquiert un ou plusieurs grains de paquet et donc, augmente le stock de ses grains. Si le paquet n'a pas assez de grains pour être transmis, il sera débarrassé [4].

Le problème fondamental de cette approche est qu'il pourrait être difficile d'estimer le nombre de grains nécessaires pour atteindre une destination donnée.

3.6.1.2 The Packet Trade Model

Ici, le paquet ne porte pas des grains, mais cela est négocié par les nœuds intermédiaires. Chaque nœud intermédiaire les achète du précédent et les vend au nœud suivant pour plus de grains. Le coût total de l'acheminement du paquet est couvert par la destination [4].

Un avantage de cette approche est que le créateur de paquet n'a pas à connaître à l'avancer le nombre de grains nécessaires pour le livrer.

Le coût d'un paquet peut dépendre de plusieurs paramètres, tels que la puissance d'émission totale et de l'état de charge des nœuds intermédiaires. Les paquets envoyés par ou destinés à des nœuds qui ne disposent pas d'une quantité suffisante de nuglets seront débarrassés.

Avantages est inconvénients

Cette technique permet d'encourager les nœuds égoïstes à participer au routage en les payant à chaque participation, mais elle pose quelques problèmes :

- La demande de matériel de confiance pour sécuriser et maintenir le dossier de la monnaie au niveau central.
- Le nombre de messages qui doivent être échangés dans le but de trouver la route vers la destination est très élevé.

3.6.2 Sprite

Dans [15],Jamal N. Al-Karaki Ahmed E. Kamal proposent ce protocole qui utilise un service de compensation de crédit (CCS : Compensation Credit Service) qui gère les récompenses et les paiements de crédit pour chaque nœud. Un nœud qui tente de transmettre un message est compensé, mais le crédit qu'un nœud reçoit dépend de son action de transmission (si sa transmission est réussite, il gagne plus de crédit). Le transfert est considéré comme réussi si et seulement si le nœud suivant sur le chemin rapporte un reçu valide aux CCS .

3.6.2.1 Avantages et inconvénient

Le problème avec cette approche est qu'elle a besoin d'un système centralisé (serveur) pour gérer les récompenses et le paiement de crédit pour chaque nœud du réseau. Mais elle permet d'inciter les nœuds égoïstes à participer dans la fonction d'acheminement des paquets.

3.7 conclusion

Ce chapitre porte sur un résumé de quelques techniques qui existent dans la littérature permettant de détecter les nœuds égoïstes dans un réseau ad hoc, il y a ceux qui se base sur la réputation des nœuds et d'autres sur le crédit (argents virtuel). Ces techniques malgré leurs avantages dans l'évaluation des performance de réseau, posent certains inconvénients. Le chapitre qui suit présente une solution que nous avons proposé en essayant de remédier à ces inconvénients.

Chapitre 4

Proposition et implémentation

4.1 Introduction

Nous avons vu dans le chapitre précédent quelques techniques existantes qui permettent de détecter les nœuds égoïstes dans le réseau ad hoc et puis soit de les isoler soit de les encourager à participer au routage et faire ainsi acheminer les paquets de leurs voisins. Suite à l'étude de ces techniques, nous avons pus penser à une proposition qui se base sur la réputation des nœuds. Cette technique permet de détecter un nœud égoïste et de l'inciter à transférer les paquets. Notre proposition sera alors détaillée dans ce chapitre.

4.2 Hypothèses

Nous avons pris quelques hypothèses par rapport à l'environnement d'exécution, nous considèrons que :

- Il n y a pas d'autres types d'attaques à part l'égoïsme ;
- Les liens sont bidirectionnels ;
- Chaque nœud possède un identifiant (ID) unique ;
- Les nœuds sont mobiles et le temps de pause est égal à zéro ;
- Si un nœud A peut transmettre des paquets au nœud B directement (sans

nécessité des nœuds intermédiaires) alors le nœud B est à portée de nœud A et inversement.

- Si un nœud B est à portée du nœud A alors A peut entendre les communications vers le nœud B et celles à partir de nœud B.

Ces hypothèses ne sont pas compliquées et sont des paramètres qu'on trouve généralement dans la plupart des MANET ce qui rend notre système plus libre.

4.3 Principe de notre proposition

Cette solution permet de détecter les nœuds égoïstes et de les encourager à participer dans l'acheminement des paquets en introduisant une information supplémentaire à l'approche TWOACK [8] qui existe déjà (voir chapitre 3) en utilisant le protocole de routage DSR. Cette information est une valeur de réputation REP(N) (N est un nœud Intermédiaire)que possède chaque nœud à propos des autres. À base de cette valeur, un nœud peut décider si le nœud suivant (succésseur) dans le chemin de transmission des paquets est coopératif (se comporte normalement) ou égoïste (se comporte mal).

Cette valeur de réputation variée entre 0 et 100 et elle est initialement égale à 50 pour tous les nœuds du réseau.

En se basant sur l'approche TWOACK, dans notre approche un nœud constate si son suivant dans le chemin de transmission des paquets a bien complété sa tâche en faisant acheminer le paquet ou non, selon quoi il va mettre à jour la réputation de ce dernier comme suit :

- Le nœud suivant a acheminé le paquet, sa valeur de réputation sera alors incrémenté de 1 ;
- Le nœud suivant n'a pas acheminé le paquet, sa valeur de réputation sera alors décrémenté de 2 ;

Quand cette réputation sera inférieur ou égale à 0, le nœud constate que son suivant est égoïste et il réagit comme suit :

- Il met ce nœud dans une liste noire qu'il possède déjà ;

– Il rédige un rapport déclarant que ce nœud est égoïste tout en introduisant son identifiant ;
– Il envoie le paquet rapport dans le chemin inverse (vers la source) de paquet de données informant les autres du comportement de ce dernier ;

La source, les nœuds intermédiaires (entre le nœud détectant le nœud égoïste et la source) et les nœuds entendant le paquet rapport vont à leurs tours mettrent ce nœud égoïste dans leurs listes noires.

La valeur de réputation est alors une information locale qui traduit la vision d'un nœud envers un autre, et reste privée avant que cette dernière atteint le seuil (0).

Ces valeurs de réputation sont une manière d'incitation car un nœud a une connaissance que les autres nœuds le jugent selon sa réputation donc il essaye d'acheminer les paquets de ses voisins avant que sa réputation atteigne le zéro induisant ainsi son isolation (ignorance) du réseau.

Le protocole de routage utilisé est DSR (voir chapitre 2) qui est adapté aux réseaux ad hoc et supporte la mobilité des nœuds et le changement de la topologie de réseau. Le fonctionnement de ce protocole est détaillé dans le deuxième chapitre.

4.3.1 Exemple

L'exemple de la figure 4.1 illustre un scénario sur lequel on applique notre approche :

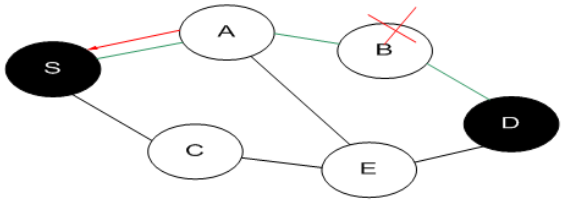

FIG. 4.1 – Exemple d'acheminement des données entre une source S et une destination D à la présence d'un nœud égoïste B.

Les lignes en vert dans la figure 4.1 représentent le chemin etabli entre S et D, et celui en rouge représente le chemin de paquet rapport.

Supposant que le nœud source (S) possède un paquet à transmettre à la destination (D), et que chaque nœud a une réputation égale à 50.

- Le nœud S initie la procédure de découverte de routes en utilisant le protocole DSR ;
- Une fois la route est établie (supposons que c'est le chemin S,A,B,D), le nœud S transmet son paquet au nœud A ;
- A étant un nœud coopératif, achemine le paquet au nœud B ;
- En appliquant la technique TWOACK le nœud S constate que le nœud A a transmis le paquet et met à jour REP(A)(en l'incrémentant de 1) : REP(A)= REP(A)+1=50+1=51 ;
- B étant un nœud égoïste, n'achemine pas le paquet au nœud D ;
- En se basant sur TWOACK, A constate la non réémission du paquet par B ;
- A met à jour REP(B)(en la décrémentant de 2) : REP(B)= REP(B)-2=50-2=48.

Si le nœud B continu toujours à se comporter comme égoïste alors le nœud A décrémente sa réputation qui peut atteindre la valeur 0 ou même une valeur négative. Une fois la réputation de B, REP(B) sera inférieur ou égale à zéro, le nœud A met le nœud B dans sa liste noire puis il rédige un rapport signalant B comme égoïste qui sera envoyé vers la source S (le rapport prend le chemin A,S). Dans ce cas, le nœud S et tous les nœuds qui sont capables d'entendre le paquet rapport mettent le nœud B dans leurs listes noires (le nœud est isolé du réseau).

4.3.2 Formalisation algorithmique

Pour détailler notre approche et mieux comprendre son fonctionnement, nous l'avons organisé sous forme d'instructions algorithmiques.

Debut

1. Le noeud S initie la phase de découverte de routes en utilisant le protocole de routage DSR (plusieurs chemins peuvent être établis entre la source et la destination et ils sont mis dans le cache de la source pour des utilisations futures) ;
2. Le nœud S choisit le chemin le plus court ;
3. Le nœud S transmet le paquet de données à son successeur (N) dans le chemin choisi ;
4. Si Le nœud N achemine le paquet à son successeur (Le nœud S constate cela à travers la technique TWOACK) alors
   - Le nœud S incrémente la réputation de N : REP(N)= REP(N)+1 ;
   - S :=N ;
   - Aller à 3 ;
5. Sinon
   - Le nœud S décrémente la réputation de nœud N : REP(N)= REP(N)-2 ;
     (a) Si (REP(N)inférieur ou égale à 0) ou (Le nœud S reçoit ou écoute un paquet rapport) alors
         - Le nœud S met le nœud N dans sa liste noire ;

         i. Si le nœud S est le nœud source alors
            - Le nœud S supprime ce chemin de son cache ;
            - Si cache n'est pas vide alors aller à 2 ;
            - Sinon aller à 1 ;

         ii. Sinon
            - Le nœud S envoie un rapport signalant N comme égoïste à son prédécesseur ;

     (b) Sinon
         - aller à 3 ;

Fin ;

4.4 Implémentation et simulation de notre approche

La simulation est nécessaire pour la mise en place d'une topologie qui n'a pas encore été testée et de pouvoir modifier ses paramètres ainsi de tester de nouveaux protocoles avant de les utilisés réellement. Pour cet effet, nous avons éffectué notre simulation sous le simulateur NS2.

4.4.1 Network Simulator NS2

Le simulateur du réseau NS2 est un outil logiciel de simulation de réseaux informatiques. Il est principalement bâti avec les idées de la conception par objets, de réutilisation du code et de modularité. NS2 est écrit en C++ et utilise le langage OTCL dérivé de TCL. A travers OTCL, l'utilisateur décrit les conditions de la simulation :

- La topologie du réseau ;
- Les caractéristiques des liens physiques ;
- Les protocoles utilisés ;
- Les communications qui ont lieu.

La simulation doit d'abord être saisie sous forme de fichier que NS utilise pour produire un fichier contenant les résultats. Mais l'utilisation de l'OTCL permet aussi à l'utilisateur de créer ses propres procédures (par exemple s'il souhaite enregistrer dans un fichier l'évolution d'une variable caractéristique du réseau au cours du temps)[3].

4.4.1.1 Le modèle de réseau sous NS

Un modèle de réseau sous NS est constitué :

- De nœuds de réseau : endroit où est généré le trafic, ou nœuds de routage ;
- Des liens de communication entre les réseaux ;
- D'agents de communication, représentant les protocoles de niveau transport

(TCP, UDP) ; ces agents sont attachés aux nœuds et connectés l'un à l'autre, ce qui représente un échange de données (connexion TCP, flux UDP) ;
- D'applications qui génèrent le trafic de données selon certaines lois (CBR, VBR), et se servent des agents de transport.

4.4.1.2 Le choix de NS2

NS2 contient les fonctionnalités nécessaires à l'étude des protocoles de routage unicast ou multicast, des protocoles de transport, de réservation, des services intégrés, des protocoles d'application. De plus le simulateur possède déjà une palette de systèmes de transmission, d'ordonnanceurs et de politiques de gestion de files d'attente pour effectuer des études de contrôle de congestion. Ce dernier possède plusieurs avantages qui facilitent notre travail :

- Observation des états du système ;
- Etudes des points de fonctionnement de système ;
- Etudes de systèmes à échelle de temps variables ;
- Etudes de l'impact des variables sur les performances du système ;
- Etude d'un système sans les contraintes matérielles.

4.4.2 Description de réseau implémenté

Pour tester notre approche nous avons mis en œuvre un réseau qui contient 40 nœuds mobiles dont le temps de pause égale à zéro ce qui induit un changement permanant de la topologie du réseau. Pour le routage des paquets de donnée, nous avons choisi d'utiliser le protocole de routage réactif DSR qui permet d'établir des routes entre une source désirant transmettre des données à une destination quelconque auquelle nous avons introduit notre approche. Ce protocole permet aussi la maintenance des routes découvertes. Les paramètres de simulation sont cités dans le tableau 4.1 :

Paramètre	**Valeur**
Nombre de nœuds	40
Temps de simulation	600 s
Dimension du réseau	700*700
Type de file d'attente	Queue/Droptail/ProQueue
Couche mac utilisée	Mac/802.11
Type des cannaux	Channel/Wireless/Channel
Nombre maximum de paquets dans la file d'attente	200
Temps de pause des nœuds mobiles	0 s
Protocole de routage	DSR

Tab. 4.1 – Les paramètres de simulation utilisés.

L'implémentation et la simulation sont faites sur un micro ordinateur qui a les caractéristiques décrite dans le tableau 4.2 suivant :

Caractéristiques	**Valeur**
Nom de l'ordinateur	Accer
Procésseur	Core i3, 1.98 GHz
Type de système	64 bits
RAM	4 Go
Plateforme utilisé	Ubunto

Tab. 4.2 – Caractéristiques de l'ordinateur utilisé.

4.4.3 Evaluation des performances

Après l'implémentation de notre approche, nous devons l'évaluer afin de constater une amélioration par rapport à ce qui existe. Pour ce faire nous l'avons comparé avec le fonctionnement de protocole DSR utilisant l'approche TWOACK dans un réseau avec la présence de nœuds égoïstes.

Cette comparaison est faite selon les métriques : le taux de succès du réseau, le taux des paquets perdus en variant le nombre de nœuds égoïstes et selon la durée de vie du réseau en variant le temps.

4.4.3.1 Taux de succès

Définition 4.4.1. *Taux de succès est le rapport entre les paquets émis et les paquets délivrés. Sa valeur est en pourcentage.*

*Le rapport de paquets délivrés=(le nombre total de paquets reçues/le nombre total de paquets émis)*100.*

Définition 4.4.2. *Paquets émis est le nombre de paquets qu'un nœud source a transmis à un nœud destination.*

Définition 4.4.3. *Paquets délivrés est le nombre de paquet bien reçu par cette destination.*

Ce taux nous permet d'évaluer le nombre de paquets perdus dûs à la présence des nœuds égoïstes.

On dit que les résultats sont parfaits quand on aura la formule suivante :

((Le nombre total des paquets reçues+le nombre total des paquets perdues)/le nombre total des paquets émis)==1.

La simulation nous donne les résultats présentés dans le tableau 4.3 ci dessous et cela en faisant varier le nombre de nœuds égoïstes dans le réseau où nous avons implémentés notre approche et de la même façon dans celui de DSR avec TWOACK.

Nous avons fait varier le nombre de nœuds égoïstes de 2 jusqu'à 10.

Nombre de nœuds égoïstes	2	4	6	8	10
Taux de succès (cas : DSR)	90.47	82.86	75.15	70.90	69.24
Taux de succès (cas : notre approche)	96.07	92.50	91.88	91.82	90.63

Tab. 4.3 – Résultats de simulation : taux de succès.

Les résultats sont aussi interprétés sous forme de graphe comme le montre la figure 4.2 :

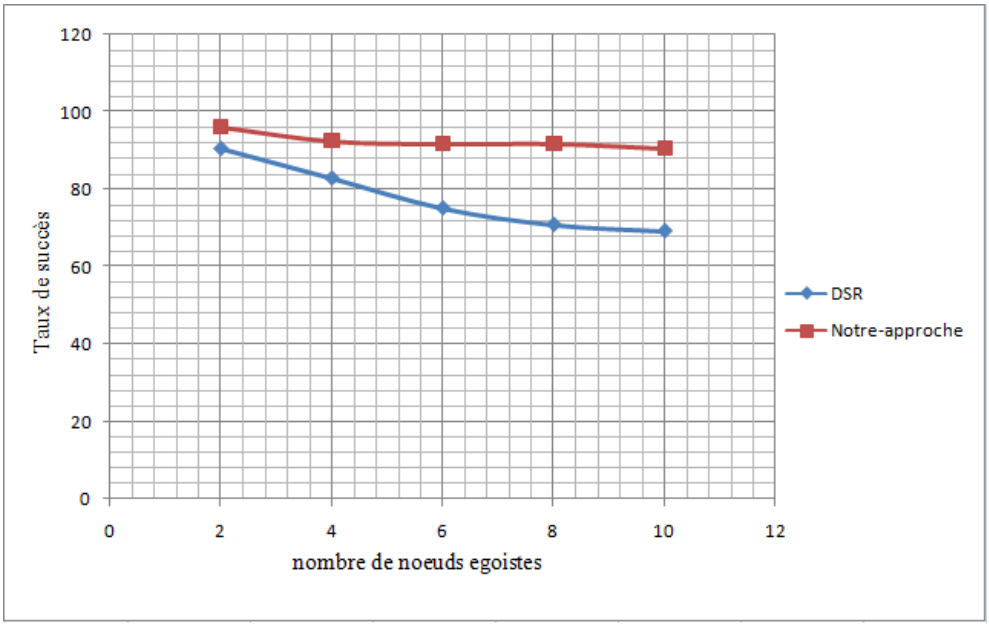

FIG. 4.2 – Résultats de simulation : taux de succès.

À partir du graphe nous remarquons qu'avec la présence de deux nœuds égoïstes, le taux de succès du réseau de notre approche est égal à 96.07%, par contre celui de DSR avec TWOACK égal à 90.47%, la différence entre les deux est alors 5.6%. En augmentant ce nombre de nœuds égoïstes dans le réseau, les deux courbes décroissent jusqu'elles arrivent aux valeurs de 90.63% et 69.24% dans notre approche et DSR respectivement et cela à la présence de dix nœuds égoïstes avec une différence de 21.39%. Les vitesses de décroissance des deux courbes sont alors différentes :

– Dans notre approche la courbe décroisse avec une vitesse de 0.68 ;
– Dans DSR avec TWOACK la courbe décroisse avec une vitesse de 2.65.

Cette vitesse est meilleure dans notre approche (le taux de succès dans DSR diminue rapidement en fonction de nombre de nœuds égoïstes).

4.4.3.2 Taux de paquets perdus

On peut traduire le graphe précédent pour obtenir un autre résultat par rapport au taux de paquets perdus en fonction de nombre de nœuds égoïstes qui existent dans le réseau.

Le tableau 4.4 contient les valeurs correspondantes.

Nombre de nœuds égoïstes	2	4	6	8	10
Taux de paquets perdus (cas : DSR)	9.53	17.14	24.85	29.1	30.76
Taux de paquets perdus (cas : notre approche)	3.93	7.5	8.12	8.18	9.37

Tab. 4.4 – Résultats de simulation : taux des paquets perdus.

Les résultats sont aussi interprétés sous forme de graphe comme le montre la figure 4.3 :

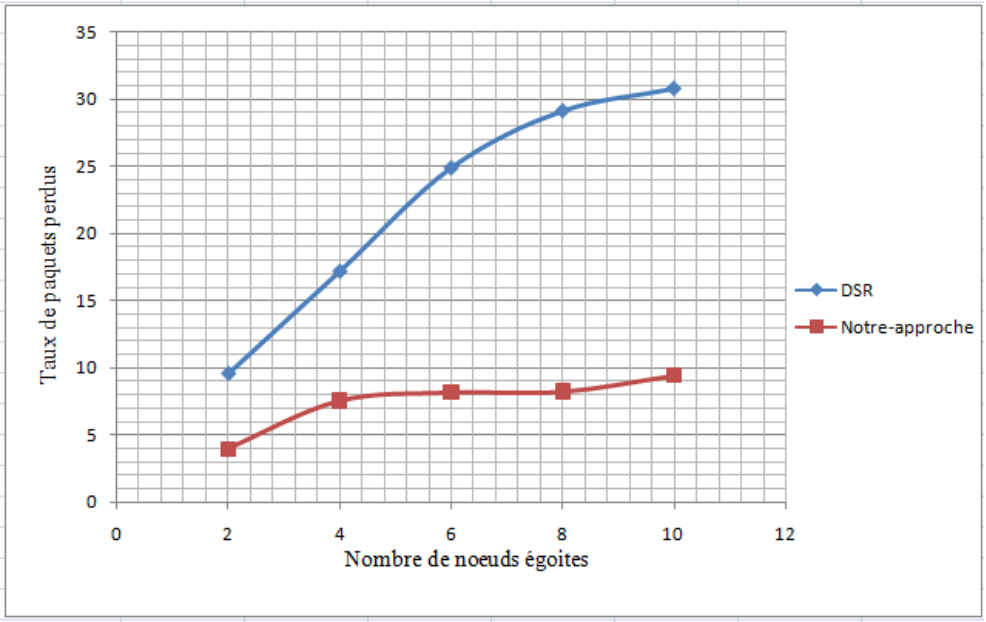

FIG. 4.3 – Résultats de simulation : taux des paquets perdus.

Comme le montre la figure 4.3, notre approche donne d'excellents résultats par rapport à DSR utilisant TWOACK, en effet le taux de paquets perdus n'excède pas les 10% et qui dépasse les 30% dans l'autre approche bien que le nombre de nœuds va jusqu'à 10 nœuds égoïstes d'un total de 40 nœuds.

Cela peut être justifié par le fait que notre approche introduit le paquet rapport qui informe les autres nœuds de la présence d'un nœuds égoïstes qui sera évité dans l'acheminement des paquets de données minimisant ainsi leurs pertes.

4.4.3.3 Durée de vie du réseau

Comme notre approche est incitative, le nombre de nœuds isolés de réseau est alors moins comparant à DSR ce qui augmente la durée de vie de réseau. Les résultats par rapport à cette contrainte de durée de vie sont représentés dans le tableau 4.5 :

Temps (en seconde)	0	50	100	150	200	250	300	350	400	450	500	550	600
Nombre de nœuds vu (cas : DSR)	40	35	25	15	10	5	5	3	0	0	0	0	0
Nombre de nœuds vu (cas : notre approche)	40	37	32	27	23	19	14	9	4	2	0	0	0

Tab. 4.5 – Résultats de simulation : durée de vie du réseau.

Les résultats sont aussi interprétés sous forme de graphe qui représente le nombre de nœud actif vu dans le réseau en fonction du temps comme le montre la figure 4.4 :

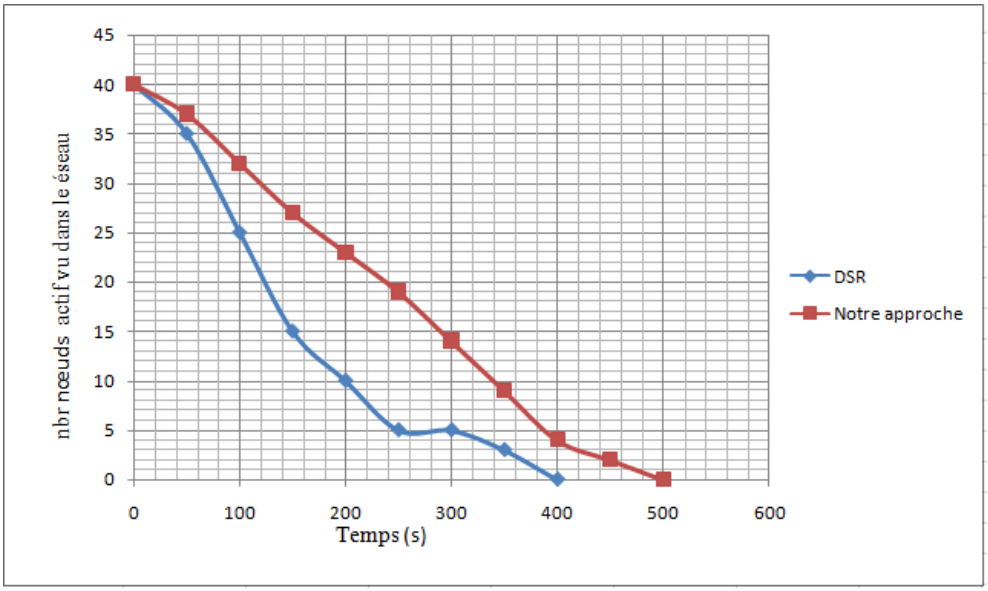

FIG. 4.4 – Résultats de simulation : durée de vie du réseau.

Nous constatons qu'à chaque fois que le temps augmente, le nombre de nœuds actifs dans le réseau se diminue mais la vitesse de diminution dans DSR est plus grande que celle de notre approche. à t=0 s, le nombre de nœuds pour les deux approches égal à 40, ensuite à t=50 s, le nombre de nœuds actifs dans DSR est 35 (donc 5 nœuds égoïstes sont isolés) par contre, 3 nœuds égoïstes sont isolés dans notre approche ce qui fait 37 nœud actifs. À t=400 s, le réseau est mort dans DSR (aucun nœud actif), mais pour notre approche il reste encore 4 nœuds actifs et il ne devient mort qu'après 100 s (à t=500).

4.5 Conclusion

Ce chapitre est consacré à notre approche proposée, sa description, son implémentation et sa simulation. Les résultats de simulation ont été satisfaisants

en matière de taux de succès du réseau et de taux de paquets pardus à la présence d'un certain pourcentage de nœuds égoïstes et en matière de durée de vie du réseau ce qui preuve son efficacité.

La plus part des techniques qui existes et plus précisément celles qui utilisent le principe de la réputation sur lequel se base aussi notre approche, le nœud détectant un nœud égoïste est le seul qui vas l'ignorer du réseau ce qui n'est pas le cas dans notre proposition : un nœud constatant que son voisin est égoïste le mis dans une liste noire et le signal au nœud source en lui envoyant un rapport, ce qui implique que les nœuds intermédiaires et les nœuds entendant le rapport vont aussi l'ignorer et éviter ainsi les routes contenant ce nœud égoïste, ie, si un nœud veut transmettre un paquet à une destination donnée vers laquelle il possède des chemins dans son cache, parmi ces chemins, il évite ceux qui contient le nœud égoïste minimisant de cette façon le temps de transmission et le taux des paquets perdus.

Conclusion générale et perspectives

Un réseau ad hoc a plusieurs contraintes qui rendent l'acheminement des paquets très difficile telle que l'absence d'infrastructure, topologie dynamique, équivalence des nœuds du réseau, bande passante limitée et la contrainte d'énergie. En effet, le problème du routage est le défi le plus difficile à réaliser, car il s'agit de trouver une route optimale multi-sauts et fiable qui relie deux nœuds quelconques du réseau sachant que des nœuds à comportement égoïste qui refuse d'acheminer les paquets de leurs voisins peuvent exister dans le réseau. Le principal objectif visé dans ce mémoire est de proposé un mécanisme ou une technique pour inciter les nœuds ad hoc à participer à cette tache de routage.

Nous avons introduit notre mémoire par les réseaux sans fil qui peuvent être classifiés en deux catégories : les réseaux avec infrastructures (réseaux cellulaires utilisant des stations de base), et les réseaux sans infrastructures (réseaux ad hoc). Nous nous sommes basés sur ce dernier type, qui est une collection de nœuds mobiles interconnectés formant un réseau temporaire sans l'aide de toute administration centralisée ou de tout support fixe.

Nous avons commencé par présenter les réseaux ad hoc et les notions relatives au fonctionnement et au rôle du protocole de routage. Ensuite les différents types d'attaque que peut subir un tel protocole, en empêchant le bon fonctionnement du réseau. Nous nous sommes principalement focalisés sur les caractéristiques, les types des nœuds égoïstes et les problèmes que posent ces nœuds dans les réseaux ad hoc. Puis étudier les différentes techniques existantes pour détecter ces nœuds et les inciter

a participé au routage, qui sont classées en techniques a basent de réputation et d'autres sur le crédit. Dans la dernière partie de notre travail, nous avons opté pour une proposition qui se base sur la notion de réputation pour encourager les nœuds à participer au routage, cette dernière est intégrée dans le protocole de routage DSR qui utilise l'approche TWOACK pour détecter les nœuds refusant de participer au routage des paquets de données.

Notre approche est implémentée puis évaluée en utilisant le simulateur NS2 (Network Simulator), les résultats de simulation ont été satisfaisants en matière de taux de succès du réseau, le nombre de paquet perdus et la durée de vie du réseau à la présence d'un certain pourcentage de nœuds égoïstes ce qui prouve son efficacité.

La plupart des objectifs visés au départ de ce travail sont atteint par l'approche proposée tels que détecter les nœuds égoïstes et les encourager à participer au routage en se basant sur la notion de réputation qui leurs donne des chances de coopérer avec leurs voisins avant de les ignorer du réseau en les mettant dans des listes noires. Cependant un nœud égoïste peut décider d'arrêter de se comporter de façon égoïste et désirer coopérer avec ses voisins. Dans ce cas, cette technique ne lui offre pas une chance de réintégrer le réseau une fois il est met dans une liste noire.

En guise de perspectives, nous souhaitons atteindre ce dernier objectif cité et enrichir notre travail par l'implémentation de notre approche dans d'autres protocoles de routage autre que DSR (AODV par exemple) et de la comparer à d'autres techniques existantes.

Bibliographie

[1] A. Bouzaher, *Approche agent mobile pour l'adaptation des réseaux mobiles ad hoc*, mémoire de magister en informatique, Université Mohamed Khider Biskra, 2010.

[2] A. Lopez-Fernandez , *Routing Protocol Performance Evaluation for Mobile Adhoc Networks*, Theses and Dissertations Student Scholarship, University of North Florida, 2008.

[3] B. David , D. Johnson , A. Maltz and J. Broch,*DSR : The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks*, Charles E. Perkins, 2001.

[4] D. Koshti and S. Kamoji, *Comparative study of Techniques used for Detection of Selfish Nodes in Mobile Ad hoc Networks*, International Journal of Soft Computing and Engineering, Vol. 1, Issue 4, September 2011.

[5] G. Shailender, C. K. Nagpal and S. Charu, *Impact of selfish node concentration in MANETS* , International Journal of Wireless and Mobile Networks Vol. 3, No. 2, April 2011.

[6] J. Bernard and J-M Percher, *Détection d'intrusions dans les réseaux ad hoc*, Ecole Supérieure d'électronique de l'Ouest (ESEO), France, Mars 2004.

[7] K. Beydoun, *Conception d'un protocole de routage hiérarchique pour les réseaux de capteurs*, Thèse de doctorat, Université de Franche Comté, 2009.

[8] K. Balakrishnan, J. Deng and P. Varshney, *TWOACK :Preventing selfishness in Mobile Ad Hoc Networks*, Proc. IEEE Wireless Comm. and Networking Conf.(WCNC'05),Mar. 2005.

[9] M. Frikha, *Réseau ad hoc, routage, Qualité de service et optimisation*, Lavoisier, Paris, 2010.

[10] M. Germain, *Introduction aux réseaux sans infrastructure dédée*, Atena, 2011.

[11] M. Schutte, *Detecting Selfish and Malicious Nodes in MANETs*, Seminar : Sicherheit in selbstorganisierenden netzen, Univercity Potsdam, 2006.

[12] N. Aiane and S. Chebel , *Application des jeux de formation de Coalition dans L'Etude de la Sécurité de la Couche Phisique des Réseaux Ad-hoc*, Mémoire de master en informatique, Université de Béjaia, Juin 2014.

[13] N. Badache, D. Djenourf , A. Derhabj and T. Lemlouma, *Les protocoles de routage dans les réseaux mobiles Ad Hoc*, Laboratoire des logiciels de base, Vol 12, No. 02, 2002, pp. 77-112.

[14] N. Benouaret and M. Mehdaoui, *Routage dans les réseaux de moyenne dimension*, Mémoire de fin d'études, Université de Béjaia, Juin 2012.

[15] N. Jamal and A. Al-Karaki, *Stimulating Node Cooperation in Mobile Ad hoc Networks*, Wireless Personal Communications, Vol 44, Issue 2, pp 219-239.

[16] P. Michiardi and R. Molva, *CORE : A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks*, The 6th IFIP Conf on Security Communications, and Multimedia, Porotoz, Slovenia, 2002.

[17] P. Muhlethaler, *802.11 et Les Réseaux Sans Fil*, Projet Hipercom ,Eyrolles, Août 2002.

[18] Q. He, D. Wu, and P. Khosla, *SORI : A Secure and Objective Reputation-based Incentive Scheme for Ad- Hoc Networks*, Proc.IEEE Wireless Communications and Networking Conf, March 2004, vol. 2, pp. 825-830.

[19] S. Bansal and M. Baker, *Observation-Based Cooperation Enforcement in Ad hoc Networks*, Research Report, Stanford University, 2003.

[20] S. Buchegger and J. Y. Le Boudec, *Performance Analysis of the CONFIDANT Protocol : Cooperation Of Nodes- Fairness In Dynamic Ad-hoc NeTworks*, Proc. 3rd IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing, Lausanne, CH,9-11 June 2002, pp.226-236.

[21] S. Marti, T. Giuli, K. Lai and M. Baker, *Mitigating Routing Misbehavior in Mobile Ad Hoc Networks*, Proc. 6th, Annual ACM/IEEE Mobile Computing and Networking, Boston, MA, Aug. 2000, pp.255-265.

[22] S. Senthilkumar and 2J. William, *A Survey on reputation based selfish node detection technoques in mobile ad hoc network*, Journal of Theoretical and Applied Information Technology 20th February 2014. Vol. 60 No.2.

[23] Y. Po-wah, H. Shenglan and M. Chris , *Malicious attacks on ad hoc network routing protocol*, Information Security Group, Royal Rolloway, University of London egham.

RÉSUMÉ

Dans les réseaux mobiles ad hoc, les protocoles de routage joue un rôle crucial pour une communication efficace entre les nœuds mobiles et fonctionnent sur l'hypothèse de base que les nœuds sont entièrement coopératifs. Cependant, un nœud peut se conduire mal pour plusieurs raisons, la plus évidente est l'économie d'énergie. Un des différents types de mauvaise conduite d'un nœud qui peuvent êtres présentés est l'égoïsme. Plusieurs approches ont été développées pour faire face à ce problème. En analysant ces approches de coopération classées en deux catégories à savoir les systèmes à base de réputation et les systèmes à base de crédit, nous avons proposé une approche d'incitation des nœuds ad hoc à participer au routage qui est intégrée dans l'approche TWOACK utilisant le protocole de routage DSR en se basant sur la réputation. Les résultats de simulations de l'approche proposée indiquent le renforcement des performances du réseau en terme de taux de paquets perdus, la durée de vie du réseau et de son taux de succé.

Mots clés : réseaux mobiles ad hoc, routage, nœud égoïste, incitation.

ABSTRACT

In a mobile ad hoc networks, routing protocols is critical for effective communication between mobile nodes and work on the basic assumption that the nodes are fully cooperative. However, a node can misbehave for many reasons, the most obvious is the energy savings. One of the various types of misconduct of a node that can beings presented is selfishness. Several approaches have been developed to address this problem. By analyzing these cooperative approaches classifies on two categories namely the reputation-based systems and credit-based systems, we proposed an incentive approach of ad hoc nodes participate in routing that is integrated into the approach TWOACK using the DSR routing protocol based on reputation. The results of the proposed approach simulations indicate strengthening network performance in terms of packet loss rate, the life of the network and its meers rates.

Key words : mobile ad hoc networks, routing, selfish node, incentive.