République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Abderrahmane MIRA-Bejaia

Faculté des sciences exactes

Département informatique

Mémoire de fin de cycle

En vue d'obtention du diplôme de Master Recherche en Informatique

***O*ption : *R*éseaux et *S*ystèmes *D*istribués**

Thème :

MonPerf : Monitorage Performant des réseaux mobiles ad hoc

Réalisé par :

SAHLI Randja

SAHALI Hayette

Setenu devant le jury composé de :

Présidant :	*M^r AISSANI Sofiane*	**U.A/Mira BEJAIA**
Encadreur :	*M^r BATTAT Nadia*	**U.A/Mira BEJAIA**
Examinatrice :	*M^lle YAHIAOUI Soraya*	**U.A/Mira BEJAIA**
Examinatrice :	*M^lle BELKACEM Nassima*	**U.A/Mira BEJAIA**

Promotion : 2012/2013

Remerciements

Nous remercions Allah le tout puissant, qui nous a donné la force et la patience pourl'accomplissement de ce travail.

nous tenons à remercier chaleureusement notre promotrice, Melle BATTAT Nadia, de nous avoir proposé ce projet, en nous faisant confiance, ainsi pour avoir dirigé ce travail avec ses orientations, ses précieux conseils et remarques. nous vous remercions infiniment Madame pour le temps que vous avez consacré à ce modèste travail, votre gentillesse, votre patience et votre modestie.

Nous remerciements s'adressent également aux membres du jury pour l'immense honneur qu'ils nous ont fait en acceptant d'évaluer ce travail.

Enfin, que tous ceux qui ont contribué de prés ou de loin, par leurs encouragements et conseils à l'accomplissement de ce travail, trouvent ici l'expression de nos profonde reconnaissances.

Dédicaces

Je dédie ce modeste travail aux personnes les plus chères à mes yeux mes parents.

A ces deux grands cœurs qui m'entourent toujours par leur tendresseet leur affection.

A ceux qui m'ont toujours encouragée et soutenue dans mes études et m'ont éclairée et ouvert la vie de l'avenir.

Je vous dédie le fruit de mes efforts, comme un symbole de gratitude.Que Dieu vous me garde et que vous soyez toujours fières de moi.

A tous ceux qui me sont chers, qui m'ont aidée par leur soutien moral , en particulier :

A mes trés chères frères et soeurs

qui occupent une place particulière dans mon cœur

A toute ma famille,particulièrement à mes adorables :Billel, Walid, Zinou, Nadin, Amine, Rayan et Amel.

A tous mes amis, pour leur amitié, leur soutien moral, et leur conseils

A Hizia, Sabah et Khoukha,

A mes trés chères amis : Randja, Samira et Nacira .

en souvenir de nos éclats de rire et des bons moments

en souvenir de tout ce qu'on a vécu enssemble, j'éspère de tout mon cœur que notre amitié durera éternellement.

Hayette

Dédicaces

Je dédie ce modeste travail aux personnes les plus chères à mes yeux mes parents.

A ces deux grands cœurs qui m'entourent toujours par leur tendresseet leur affection.

A ceux qui m'ont toujours encouragée et soutenue dans mes études et m'ont éclairée et ouvert la vie de l'avenir.

Je vous dédie le fruit de mes efforts, comme un symbole de gratitude.Que Dieu vous me garde et que vous soyez toujours fières de moi.

A tous ceux qui me sont chers, qui m'ont aidée par leur soutien moral , en particulier :

A mes trés chères soeurs et frères qui occupent une place particulière dans mon cœur

A tous mes amis, pour leur amitié, leur soutien moral, et leur conseils

A Hizia, Sabah et Khoukha

A mes trés chères amis : Hayette, Samira et Nacira .

en souvenir de nos éclats de rire et des bons moments

en souvenir de tout ce qu'on a vécu enssemble, j'éspère de tout mon cœur que notre amitié durera éternellement.

Randja

Table des matières

Table des figures

Liste des tableaux

Liste d'abréviations

ADMA : Autonomous Decentralized Management Architecture for MANETs

AES : Advanced Encryption Standard

ANMP : Ad hoc Network Management Protocol

AODV : Ad hoc On demand Distance Vector routing

CDS : Connected Dominating Set

CMDB : Configuration and Monitoring Database

CPU : Central Processing Unit

DARPA : Defence Advanced Reseach Agency

DES : Data Encryptions Standard

DHT : Distributed Hash Table

Distmon : Distributed Monitoring in Ad hoc network

DPA : Domain Policy Agent

DRAMA : Dynamic Readdressing And Management for the Army

DSDV : Dynamic destination Sequenced Distance Vector

DoD : Departement of Defense

DSR : Dynamic Routing Source

DSSS : Direct Sequence Spread Packet Radio

GloMo : Global Mobile Information System

GMIB : Guerrilla Management Information Base

GPA : Global Policy Agent

GUI : Graphical User Interface

IDMEF : Intrusion Detection Message Exchange Format

IDS : Intrusion Detection System

IT : Internet Tactique

ITMANET : Information Theory for Mobile Ad hoc networks

ISO : International Organization for Standardization

LACM : Level Access Control Model

LPA : Local Policy Agent

LPDP : Local Policy Decision Point

LPR : Low-cost Packet Radio

MANET : Mobile Ad hoc Network

MD5 : Message Digest

MIB : Management Information Base

MIS : Configuration and Monitoring Database

MMAN : Monitor for Mobile Ad hoc Network

NMCAM : Maximal Independant Set

MPR : MultiPoint Relays

MU : Monitoring Unit

OLSR : Optimized Link State Routing

OLSRM : Optimized Link State Routing Protocol Monitoring

PAI : Protection Against Insider

PEP : Policy Enforcement Point

PRNet : Packet Radio Network

QoS : Quality of Service

QoSMI : Quality of Service Monitoring Infrastructure

RSA : Rivest Shamir Adelman

SF : Smart Firewall plicies

SFR : Smart Firewall Rulls

SHA-1 : Secure Hash Algorithme

SPL : Security Policy Language

SURAN : SURvivable Radio Network

TC : Topology Control

VBB : Virtual Backbone

WANMON : Wireless Ad hoc Network Monitoring

YAP : Yelp Announcement Protocol

ZRP : Zone Routing Protocol

Introduction générale

1. Contexte

Les avancées remarquables de la technologie sans fils ont favorisé le développement des réseaux mobiles de façon prodigieuse. Les réseaux mobiles ad hoc sont l'une des principales catégories de réseaux mobiles. Ils sont des réseaux auto-organisés, formés spontanément à partir d'un ensemble de nœuds mobiles, communicants sans nécessiter d'infrastructure fixe préexistante. Ces nœuds mobiles, peuvent être de formes variées : ordinateurs portables, téléphones mobiles, capteurs et qui présentent par conséquent des capacités non homogènes en termes de communication, de puissance de calcul et de stockage. Ils communiquent, soit directement lorsqu'ils se trouvent dans le même voisinage direct, soit par communication multi-sauts en faisant appel à des nœuds intermédiaires.
Grace aux réseaux mobiles ad-hoc, l'utilisateur peut déployer son propre réseau très facilement et sans coût supplémentaire. Mais l'apparence simpliste du concept cache de nombreux défis . Vu les contraintes spécifiques des réseaux mobiles ad hoc (mobilité, énergie limité, etc) et leurs vulnérabilité, un mécanisme de monitorage doit être mis en oeuvre de manière à contrôler le réseau et à avoir des connaissances sur le fonctionnement de celui-ci.

2. Problématique

Le monitorage est une activité d'observation qui consiste à évaluer l'état opérationnel et le fonctionnement d'un réseau, il permet de déterminer sa topologie, l'usage de ses ressources ainsi que ses performances.
Trois spécificités importantes des réseaux mobiles ad hoc rendent la réalisation du processus de monitorage délicate. La première spécificité est la mobilité fréquente des nœuds. La

seconde réside dans le fait que les nœuds ont une capacité de calcul, de communication et d'énergie très limitée. La troisième spécificité est qu'ils doivent être capables de communiquer entre eux en toute sécurité pour accomplir leurs activités. Afin de surmonter cet obstacle, les nœuds d'un réseau ad hoc s'auto-organisent et coopèrent afin d'assurer toutes les étapes indispensables au monitorage : la collecte des données, l'analyse de données et le stockage.

Plusieurs approches ont été proposée dans le but de réaliser le processus de monitorage le plus convenablement possible, cependant chacune d'elles présentent ses avantages et ses inconvénients.

3. Contribution

Nous avons proposé une nouvelle méthode pour élire les managers en se basant sur l'énergie, la mobilité, la connectivité et la valeur de confiance

Vu la nécessité de l'interaction entre les nœuds lors de monitorage, (comme toutes les activités sont réalisées en collaboration entre ces nœuds), un nœud doit mesurer la fiabilité d'un autre nœuds avant de décider d'interagir ou d'entrer en communication avec lui. Ce qui nécessite un mécanisme d'établissement de confiance entre ces nœuds. Notre deuxième contribution consiste à introduire un nouveau mécanisme d'estimation de degré de confiance des nœuds et la détection des nœuds égoïstes. afin d'assurer le bon fonctionnement de monitorage en rejetant les données colléctées par les non confiant et en évitant les noeuds égoistes.

4. Organisation du mémoire

Le mémoire est divisé en quatre chapitres illustrés ci-dessous :

- **Généralités sur les réseaux mobiles ad hoc**

  Dans ce chapitre nous avons présenté les environnements sans fil en générale et les réseaux mobile ad hoc en particulier, nous avons commencé par une petite historique de ces réseaux, par la suite, nous avons introduit les domaines d'application, les caractéristiques, ainsi que les avantages de ce type de réseau et nous avons achevé ce chapitre par un aperçu des protocoles de routage utilisés dans ces réseaux ainsi que leurs avantages et leurs inconvénients.

– **Le monitorage des réseaux mobiles ad hoc**

Ce deuxième chapitre est consacré au processus de monitorage, nous avons commencé par introduire les concepts de base d'un tel processus, ensuite nous avons présenté un état de l'art sur les principales approches de monitorage existantes dans la littérature, et nous avons terminé ce chapitre par une comparaison de ces différentes approches.

– **Proposition**

Dans ce troisième chapitre, nous avons commencé, en premier lieu, par la définition de quelques notions essentielles pour la description de notre proposition, par la suite nous avons présenté cette dernière. Et nous avons fini ce chapitre par un exemple illustratif.

– **Simulation et évaluation de performances**

Dans ce chapitre nous avons illustré les différents résultats de simulations obtenus en utilisant Matlab, avec une comparaison des performances de l'approche proposée avec deux autres approches vues dans l'état de l'art .

Notre mémoire se termine avec une conclusion génèrale et des perspectives que nous voulons réalisées prochainement.

1

Généralités sur les réseaux mobiles ad hoc

1.1 Introduction

Dans un passé pas très loin, les réseaux filaires étaient la seule solution pour relier les terminaux et périphériques d'une organisation ou d'une entreprise de toute taille. Ainsi, des câbles doivent être utilisés à cet effet. Vu l'absence des autres technologies concurrentes, cette architecture constituait, à cette époque, une révolution. Mais le coût élevé nécessaire pour le déploiement d'une telle solution ainsi que la difficulté de relier certaines régions, pour des raisons géographiques (les zones rurales) ou stratégiques (les champs de batailles), a donné naissance à une autre technologie basée sur les transmissions radio. Cette technologie est basée sur des réseaux appelés réseaux sans fil. Ce type de réseau permet à ses utilisateurs d'accéder à l'information indépendamment du temps et de leur position géographie. Il offre une grande flexibilité d'emploi et, en particulier, permet la mise en réseau des noeuds dont le câblage serait trop onéreux à réaliser, voir même impossible.

Dans ce chapitre nous commençons par la définition des réseaux sans fils et les deux classes qui les constituent (mode infrastructure et mode sans infrastructure). Nous introduisons ensuite le concept des réseaux mobiles ad hoc et les caractéristiques inhérentes à ces réseaux, ainsi que quelques domaines d'application de ce type de réseau. A la fin de ce chapitre, nous donnons un aperçu général sur le routage ad hoc. Nous présentons les types de protocoles de routage ainsi que leurs avantages et leurs inconvénients.

1.2 Les réseaux sans fil

Un réseau sans fil est un ensemble de nœuds mobiles connectés entre eux et qui peuvent s'envoyer et recevoir des données à l'aide des interfaces sans fils [1].

1.3 Les classes des réseaux sans fil

Les réseaux sans fil peuvent être classés en deux classes [2] (voir la figure 1.1) :

- les réseaux avec infrastructure (cellulaire).
- les réseaux sans infrastructure (MANET : Mobile Ad hoc NETwork).

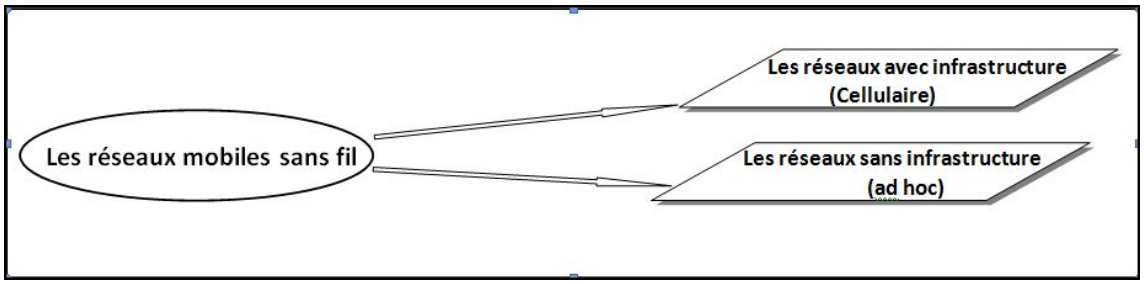

FIGURE 1.1 – Topologie des réseaux sans fil

1.3.1 Les réseaux mobiles avec infrastructure

Les réseaux avec infrastructure sont composés de deux ensembles de nœuds distincts : les nœuds fixes d'un réseau de communication filaire, et les nœuds mobiles (UM : Unités Mobiles). Les nœuds fixes appelés stations de base (SB) sont munis d'une interface de communication sans fil pour permettre la communication directe avec les nœuds mobiles, localisés dans une zone géographique limitée appelée " cellule ". Ainsi, un nœud mobile n'est pas rattaché, à un moment donné, qu'à une seule station de base, qui lui offre tous les services en utilisant la communication filaire (voir la figure 1.2).

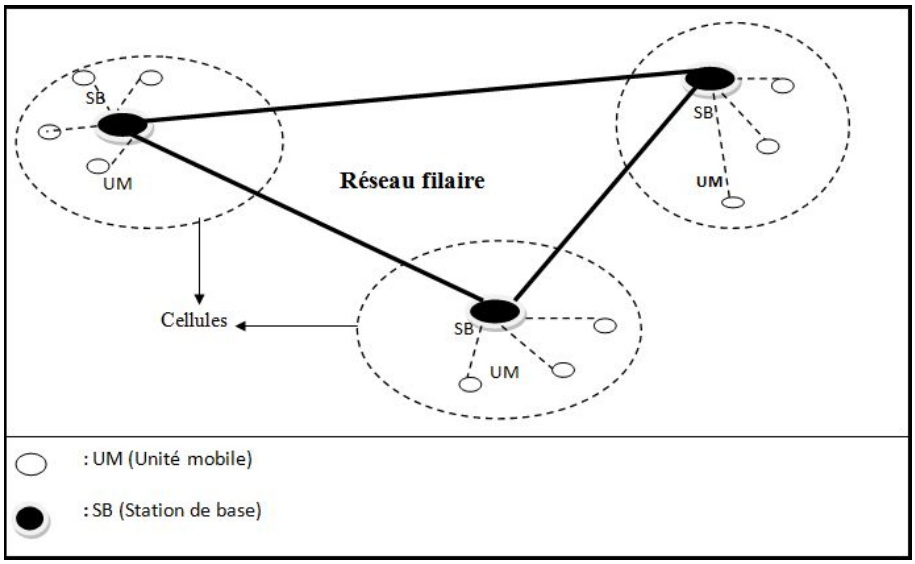

FIGURE 1.2 – Réseau avec infrastructure

1.3.2 Les réseaux mobiles sans infrastructure

Ce type de réseau ne comporte pas de nœuds fixes, tous les nœuds du réseau sont mobiles et communiquent d'une manière directe en utilisant leurs interfaces de communication sans fil (Voir Figure 1.3). L'absence d'infrastructure ou de réseau filaire, composé de 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 .

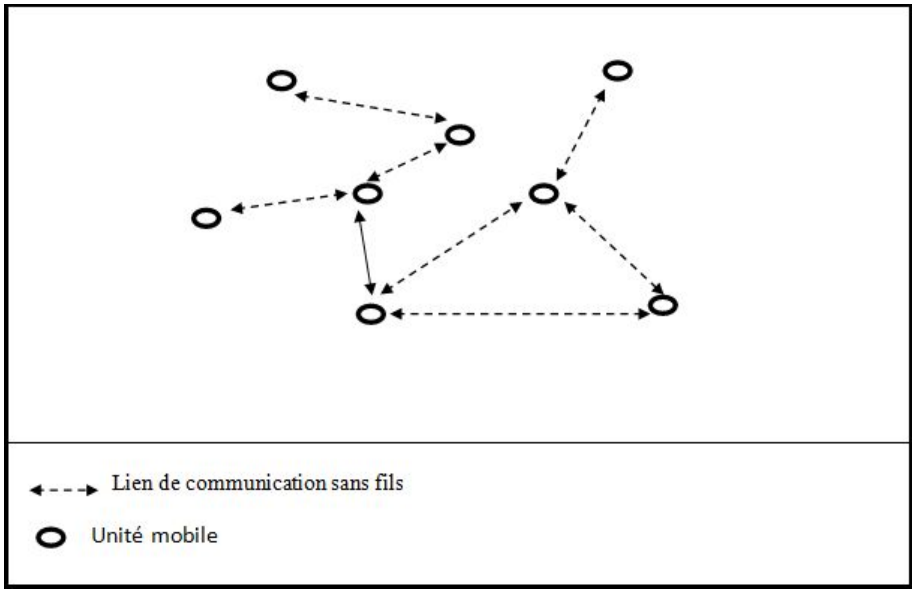

FIGURE 1.3 – Mode sans infrastructure

1.4 Les réseaux mobiles ad hoc

1.4.1 Historique des réseaux mobiles ad hoc

Historiquement, les réseaux mobiles ad hoc ont pour origine, le projet PRNet (Packet Radio Network) du DARPA (Defense Advanced Research Projects Agency) en 1972, qui a été inspiré par l'efficacité de la technologie à commutation de paquets et la possibilité de son utilisation dans les environnements mobiles sans fil.

En 1983, le DARPA crée le projet SURAN (Survivable Radio Networks) pour résoudre les principaux problèmes du projet PRNet (sécurité, passage à l'échelle, capacité de traitement, etc.).

En 1987, la conception de la technologie LPR (Low-cost Packet Radio) a été apparue et qui est doté d'une couche radio DSSS (Direct Sequence Spread Packet Radio) avec un processeur pour la commutation de paquet intégré.

En 1994, le DoD (Department of Defense) lança le programme de DARPA appelé GloMo (Global Mobile) Information Systems. Ce programme visait le développement de réseaux ad hoc mobiles et en particuliers d'appareils sans fil supportant une connectivité multimédia de type Ethernet à tout moment et n'importe où.

En 1997, l'armée américaine a mis en place l'IT (Internet Tactique) qui a permis la plus grande implémentation à large échelle des réseaux mobiles, sans-fil et multi-sauts de radios à commutation par paquets.

Les applications militaires, utilisant les réseaux MANETs, continuent à faire l'objet de projets à la DARPA notamment à travers le projet ITMANET (Information Theory for Mobile Ad hoc Networks) qui a commencé en 2007et dont l'objet est de développer de puissantes technologies [3].

1.4.2 Domaine d'application des réseaux mobiles ad hoc

Le domaine d'application des réseaux mobiles ad hoc couvre un très large spectre, bien que les projets aient souvent débuté dans un cadre purement militaire, le domaine d'application des réseaux mobiles ad hoc s'étend bien au-delà. En effet, la flexibilité et la rapidité ainsi que la facilité d'implémentation de ces réseaux les rendent d'un grand apport lors des opérations de sauvetage, notamment lors des tremblements de terre ou autres catastrophes. Ces réseaux peuvent être rapidement déployés sur des terrains de sinistres pour assurer le relai et la liaison des communications entre sauveteurs.

Ces réseaux intéressent aussi de plus en plus les entreprises. Cela permet d'assurer une grande mobilité des agents, le partage des données et les conférences. Par exemple, lors d'une réunion ou conférence, l'intervenant peut communiquer avec tous les participants et créer un débat interactif.

Il existe d'autres applications des réseaux mobiles ad hoc, comme la communication entre les véhicules. Cette application est prometteuse car elle permet de réduire le risque d'accidents sur les autoroutes, d'assurer la communication des véhicules dans les tunnels, etc [4].

1.4.3 Caractéristiques des réseaux mobiles ad hoc

Les réseaux mobiles ad hoc possèdent de nombreuses caractéristiques non connues dans les réseaux filaires et cellulaires, nous pouvons citer [5] :

- **Absence d'infrastructure**

  Pas de station de base ou de point d'accès, tous les nœuds du réseau se déplace dans un environnement distribué sans point d'accès ou un point de rattachement à l'ensemble du réseau. Un nœud joue le rôle aussi bien d'acteur actif dans le réseau émetteur et récepteur mais aussi de routeur pour relayer la communication des autres nœuds du réseau.

- **Ressources limitées**

  Les nœuds dans les réseaux mobiles ad hoc ont des ressources très limitées, comme la capacité de calcul, de stockage et surtout d'énergie.

- **Interférences**

  Les liens radios ne sont pas isolés, deux transmissions simultanées sur une même fréquence ou utilisant des fréquences proches, peuvent interférer.

- **Topologie dynamique**

  Les nœuds mobiles du réseau se déplacent d'une façon libre et arbitraire, par conséquent, la topologie du réseau peut changer, à des instants imprévisibles, d'une manière rapide et aléatoire.

– **Sécurité physique limitée**

Les terminaux ne sont pas protégés. Ils sont menacés de vol ou de destruction.

– **La vulnérabilité des nœuds** les nœuds ne sont pas physiquement protégés, ils peuvent être capturés par des attaquants (les ennemis), ce qui pose problème au niveau des relations de confiance entre les nœuds. Ainsi, n'importe quel modèle de sécurité dédié aux réseaux mobiles ad hoc doit prendre en compte la compromission des nœuds, ainsi que la résistance à cette attaque

1.5 Le routage dans les réseaux mobiles ad hoc

Le problème de routage consiste à déterminer un acheminement optimal des paquets à travers le réseau.

1.5.1 Protocoles de routage

Nombreux protocoles de routage ont été développés pour les réseaux mobiles ad hoc faisant face aux contraintes spécifiques de ce type de réseau, ces protocoles peuvent être classés en trois grandes classes (voir la figure 1.4) :

- les protocoles proactifs.
- les protocoles réactifs.
- les protocoles hybrides.

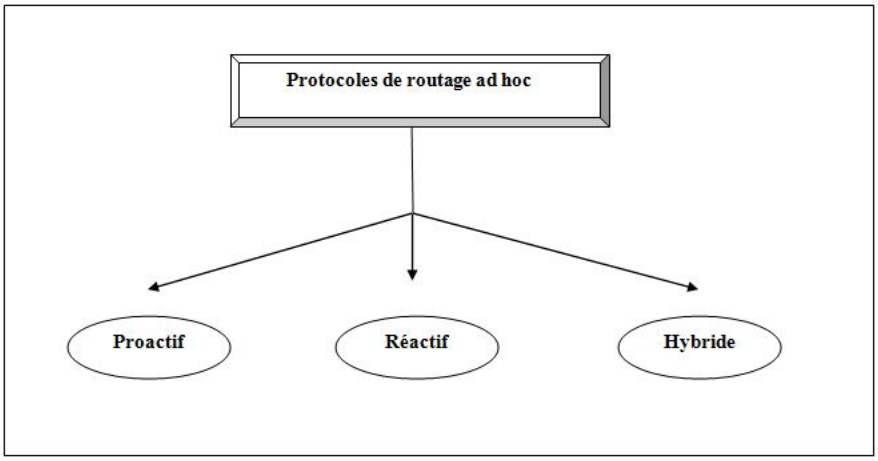

FIGURE 1.4 – Classification des protocoles de routage

1.5.1.1 Protocoles de routage proactifs

Les protocoles de routage proactifs tentent de maintenir, dans chaque nœud, la table de routage qui contient des informations concernant tous les destinataires possibles, tels que, à chaque fois qu'un nœud du réseau souhaite envoyer un message , il consulte sa table de routage pour déterminer la route à suivre jusqu'au destinataire du message. Ces protocoles sont capables de répondre aux changements de topologies du réseau en propageant à chaque voisin les mises à jours des routes afin que chacun puisse maintenir une vue consistante du réseau [6].

Parmi les protocoles de routage proactifs les plus connus nous citons :

- OLSR (Optimized Link State Routing Protocol) [7].
- DSDV (Destination Sequenced Distance Vector) [8].

1.5.1.2 Protocoles de routage réactifs

Les protocoles de routage réactifs créent et maintiennent les routes selon les besoins, c'est-à-dire, lorsqu'un message doit être envoyé, le protocole de routage va rechercher un chemin jusqu'à la destination. Une fois ce chemin trouvé, il est inscrit dans la table de routage et peut être utilisé. En général, cette recherche se fait par inondation (un paquet de recherche de route est transmis de proche en proche dans tout ou partie du réseau) [5]. Parmi les protocoles de routage réactifs les plus connus nous énumérons :

- AODV (Ad hoc On Distance Victor)[9].
- DSR (Dynamic Source Routing) [10].

1.5.1.3 Protocoles de routage hybride

Les protocoles hybrides combinent les deux approches proactif et réactif. Ils utilisent un protocole proactif, pour connaître le proche voisinage (voisinage à deux ou trois sauts). Ils font appel aussi, aux techniques des protocoles réactifs pour chercher des routes. Avec ce protocole, nous disposons immédiatement des routes dans le voisinage proche, et lorsque la recherche doit être étendue plus loin, elle en est optimisée (un nœuds qui reçoit un paquet de recherche de route réactive va, tout de suite, savoir si la destination est dans son propre voisinage. Si c'est le cas, il va pouvoir répondre, sinon il va propager de manière optimisée la demande hors de sa zone proactive) [2].

Parmi les protocoles de routage hybride les plus connus nous mentionnons :

- ZRP (Zone Routing Protocol) [11].

1.5.2 Avantages et inconvénients des protocoles de routages

Le tableau récapitulatif ci-dessous présente les avantages et les inconvénients des différents protocoles de routage dans les réseaux mobiles ad hoc.

	Avantages	**Inconvenients**
Protocoles proactifs	- Une route est toujours disponible entre une source et une destination, rapide ce qui implique le gain du temps.	- Le coût, dû au maintient de la topologie, génère une consommation continuelle de la bande passante.
Protocoles réactifs	- La génération du trafic de contrôle ne se fait que lorsqu'il est nécessaire.	- L'inondation est un mécanisme très coûteux, génération d'un délai important pour ouvrir une route entre deux nœuds.
Protocoles hybrides	- Il s'adapte bien aux grands réseaux.	- Il combine les inconvénients des deux protocoles proactifs et réactifs.

TABLE 1.1 – Avantages et inconvénients des protocoles de routages

1.6 Conclusion

Dans ce chapitre, nous avons donné un aperçu général sur les réseaux mobiles sans fil. En suite, nous avons présenté, les réseaux mobiles ad hoc qui sont un type particulier de réseaux sans fil, ne nécessitant aucune infrastructure fixe pour se créer et s'organiser. Nous avons cité leurs domaines d'application ainsi que leurs caractéristiques, et nous avons fini par une petite description des protocoles de routage utilisés dans ce type de réseau.

2

Monitorage des réseaux mobiles ad hoc

2.1 Introduction

Les réseaux mobiles ad hoc sont d'une part tout à l'heur actuelle, ils devient de plus en plus indispensable dans tout les domaines, mais ils présentent d'autre part des contraintes supplémentaires liées à une topologie dynamique, une bande passante réduite, une durée de vie restreinte due aux limites énergétiques et encore une sécurité limitée. C'est la raison pour laquelle il est nécessaire de mettre en œuvre des mécanismes permettant de surveiller le réseau pour pouvoir maintenir une vue globale de fonctionnement.

Dans ce chapitre, nous allons commencer par présenter la supervision des réseaux mobiles ad hoc, ses étapes et ses buts. Ensuite nous allons nous focaliser sur le monitorage, ses difficultés, les principales approches de monitorage existantes. A la fin de ce chapitre, nous effectuerons une étude comparative sur ces approches.

2.2 Supervision des réseaux mobiles ad hoc

La supervision des réseaux est un ensemble d'activités prenant en charge la surveillance du réseau afin d'avoir une vue globale de fonctionnement et des problèmes pouvant survenir sur celui-ci. Elle a pour objectif la gestion du nombre croissant d'équipements (stations, serveurs, etc.) et la possibilité d'effectuer les réparations nécessaires le plus rapidement possible [12]. Elle regroupe les cinq étapes suivantes :

- **Collecte de données :** c'est l'étape qui consiste à rassembler tout les informations qui participent à la formation des performances du réseau tel que l'adresse IP, la bande passante, le niveau d'énergie, et la capacité de stockage.
- **Analyse de données :** c'est l'étape qui consiste à comparer les données capturées à des intervalles du temps spécifiques et d'étudier le taux d'influence des valeurs de ces données sur le fonctionnement du réseau et ses performances.
- **Déclenchement d'alertes :** après analyse et en cas de problème, des alertes seront lancées pour informer les membres du réseau et provoquer une correction.
- **Stockage de données :** Dans cette étape, on procède à une sauvegarde des données collectées et analysées, ainsi que les alertes, et les rapports de disfonctionnement pour des utilisations ultérieurs.
- **Correction en fonction d'erreur :** c'est l'étape qui consiste à corriger les erreurs détectées lors de l'analyse.

2.2.1 Le but de la supervision

La classification de l'ISO (International Standard Organisation), qui se base sur l'aire fonctionnelle, permet de déterminer les principaux objectifs de la supervision des réseaux mobiles ad hoc. Elle définit cinq aires principales [12] [13] :

- **Gestion des fautes :** Cette aire fonctionnelle a pour but la détection, l'isolation et la correction des anomalies qui affectent le fonctionnement des réseaux et de leurs services. Ces fautes peuvent être causées par la panne d'un équipement physique aussi bien que par un dysfonctionnement d'origine logicielle. La gestion de fautes vise à minimiser l'impact des fautes sur les services tout en limitant les interférences induites par les opérations de détection et de correction elles-mêmes.
- **Gestion de la configuration :** Elle comprend le recensement des ressources du réseau ainsi que leur configuration physique et logicielle. Elle intervient notamment lors de l'intégration de nouveaux équipements ou lors du déploiement de nouveaux services à travers les différentes opérations de configuration.
- **Gestion de la comptabilité :** Elle implique de surveiller l'utilisation de réseau par de divers utilisateurs et groupes. Cette information peut être très utile dans la configuration de réseau et l'attribution des ressources de réseau à de divers groupes dans une organisation.
- **Gestion de la performance :** Son objectif est d'évaluer la qualité du service délivrée par le réseau et de la maintenir grâce à des opérations de contrôle. Elle comprend les opérations de monitorage qui permettent de déterminer l'état de fonctionnement du réseau à travers différents critères de qualité tels que la disponibilité de service, mais aussi les opérations de prévention et de correction qui permettent de garantir le niveau de performance souhaité.
- **Gestion de la sécurité :** Elle vise la protection du réseau en empêchant l'ensemble des activités frauduleuses qui peuvent avoir un impact sur l'intégrité et le bon usage des services. Elle comprend les mécanismes d'authentification, de contrôle d'accès et de confidentialité.

2.3 Monitorage des réseaux mobiles ad hoc

Le monitorage est une activité formée à partir des quatre premières étapes de processus de supervision citées plus haut. Il permet d'effectuer une analyse et une cap-

ture d'information sur le réseau, dans le but d'avoir une vue de plus haut niveau ce qui permettra de déterminer la topologie, l'usage des ressources, ainsi que les performances du réseau en terme de sécurité, disponibilité, et aussi en terme de qualité de service [12] .

2.3.1 Difficulté de monitorage

La tâche du monitorage dans les réseaux mobiles ad hoc s'avère plus complexe que celle des réseaux filaire en raison [14] :

- de la nature dynamique des nœuds dans les réseaux mobiles ad hoc.
- des nœuds non coopératifs ou malicieux qui refusent de fournir des informations, ou bien de les falsifier se qui induit à une réduction de la fiabilité de monitorage (perte d'informations).
- du trafic généré lors du monitorage qui ne doit pas surcharger le réseau.
- des ressources limitées qui ne doivent pas être consommées à cause du processus de monitorage lui-même.

2.4 Le clustering

Le clustering consiste en un découpage virtuel du réseau en groupe de nœuds proches géographiquement. Ces groupes sont appelés clusters, ils sont généralement identifiés par un nœuds particulier, un chef de groupe, aussi nommé cluster-head. Dans la plupart des algorithmes de clustering, les clusters sont construits à partir d'une ou plusieurs métriques qui permettent d'assigner un chef à chaque cluster. Le cluster étant alors constitué de cluster-head et de touts les nœuds qui lui sont rattachés.

Le principal avantage de mécanisme de clustering est qu'il permet une meilleure organisation de réseau et il facilite le partage de ressources entre les différents nœuds [15].

2.5 Les modèles de gestion

Il existe différents modèles de la gestion des réseaux mobiles ad hoc [16], nous pouvons citer :

2.5.1 Le modèle d'information

Le modèle d'information définit un cadre formel commun pour décrire les ressources contrôlées et la structure de l'information de gestion. Il doit offrir un niveau d'abstraction suffisant pour fournir une vue homogène et extensible de toutes les ressources indépendamment de la nature, de l'endroit et des méthodes d'accès de celles-ci.

2.5.2 Le modèle fonctionnel

Ce modèle permet de répartir les opérations de gestion par aire fonctionnelle qui a pour objectif la correction des anomalies, l'évaluation des performances, et la protection du fonctionnement des réseaux .

2.5.3 Le modèle organisationnel

Ce modèle [21][14] vise à définir le rôle et la relation de chacun des nœuds intervenant dans le processus de monitorage :

- **Gestionnaire :** c'est le nœud responsable de l'activité de monitorage.
- **Gestionnaire local :** c'est un nœud intermédiaire, responsable de la collecte des données de monitorage d'un sous ensembles de nœuds du réseau.
- **Agent :** c'est le nœud qui assure l'interface avec les ressources gérées en exicutant les requêtes transmises par le gestionnaire.

La figure ci-dessous illustre un exemple d'un modèle organisationnel.

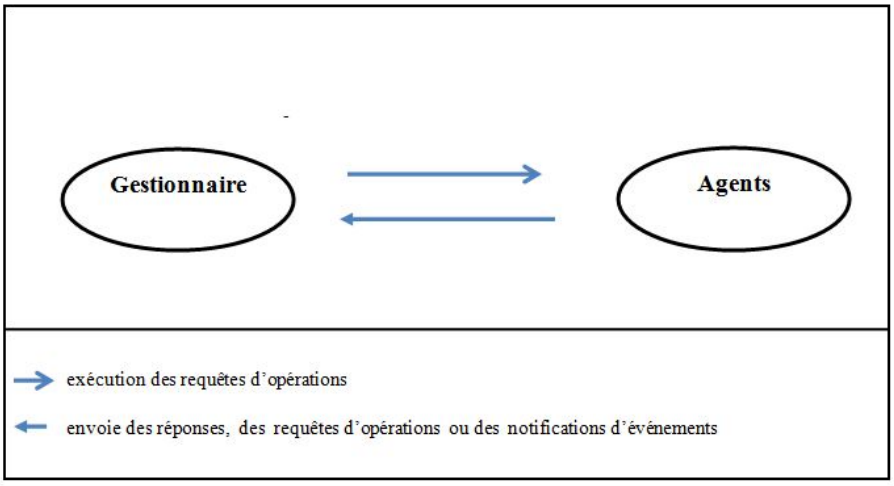

FIGURE 2.1 – Exemple d'un modèle organisationnel

Le modèle organisationnel regroupe quatre types d'organisations distinctes [21] [18] [114] :

2.5.3.1 Organisation centralisée

Cette organisation repose sur un unique gestionnaire qui contrôle l'ensemble de nœuds (agents) formant le réseau lors de la communication entre eux. (voir la figure 2.2).

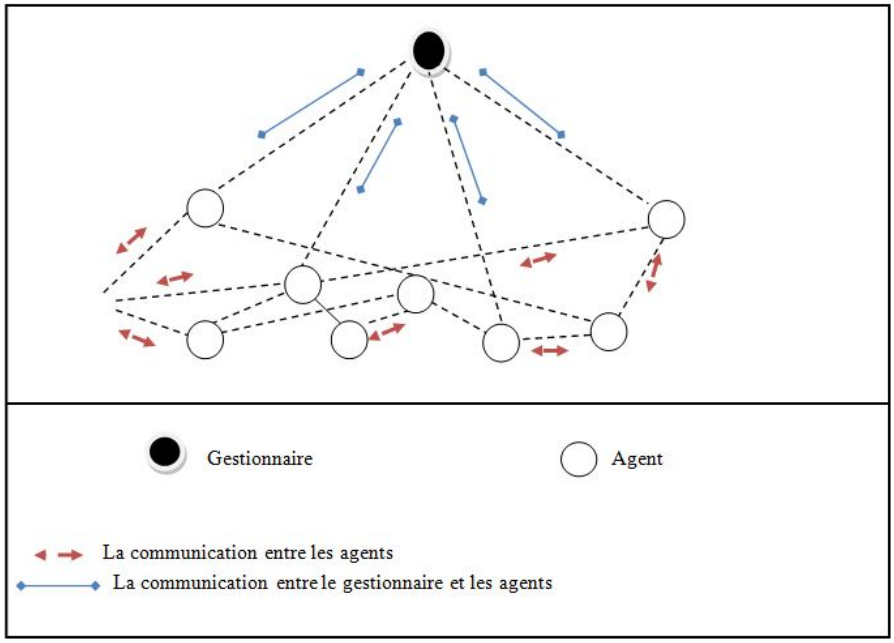

FIGURE 2.2 – Organisation centralisée

2.5.3.2 Organisation centralisée hiérarchique

Cette organisation conserve une autorité centrale mais introduit une hiérarchie de gestionnaires locaux afin d'assurer un meilleur passage à l'échelle. Le gestionnaire utilise des gestionnaires locaux comme intermédiaires afin de répartir les opérations de gestion. Chaque gestionnaire dispose d'un certain niveau de responsabilité dans la tâche de gestion.

Le gestionnaire central reste l'unique point de contrôle et dispose donc du plus haut degré de responsabilité (voir a figure 2.3).

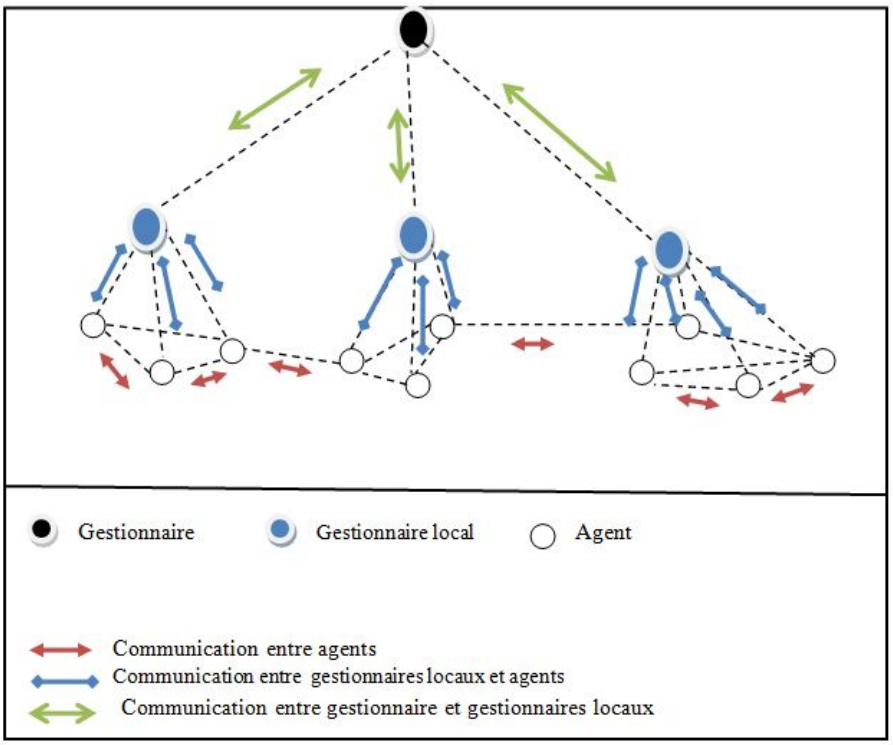

FIGURE 2.3 – Organisation centralisée hiérarchique

2.5.3.3 Organisation distribuée

Cette organisation repose sur un ensemble de gestionnaires, qui collaborent pour effectuer le monitorage total du réseau entier. Ces gestionnaires disposent du même degré de responsabilité. Chacun d'eux est responsable du monitorage d'un sous ensemble de nœuds dans le réseau (voir la figure 2.4).

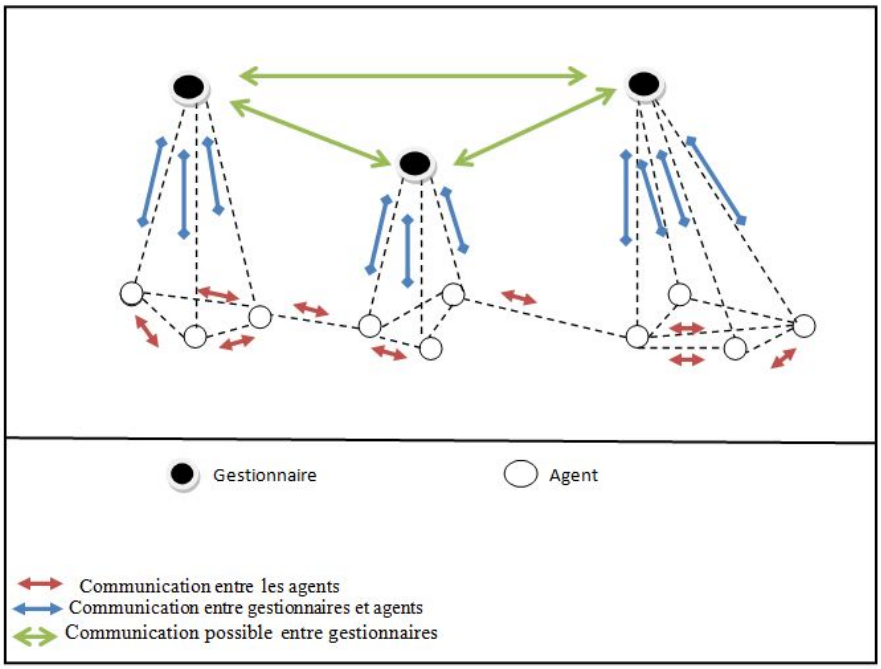

FIGURE 2.4 – Organisation distribuée

2.5.3.4 Organisation distribuée hiérarchique

Dans cette organisation, chaque gestionnaire peut déléguer une partie des tâches de gestion à des gestionnaires locaux qui se chargent de rassembler et traiter les données de leurs domaine, et peuvent passer ces données aux gestionnaires de niveau supérieur au besoin.

Il n'existe pas une communication directe entre les gestionnaires locaux (voir la figure 2.5).

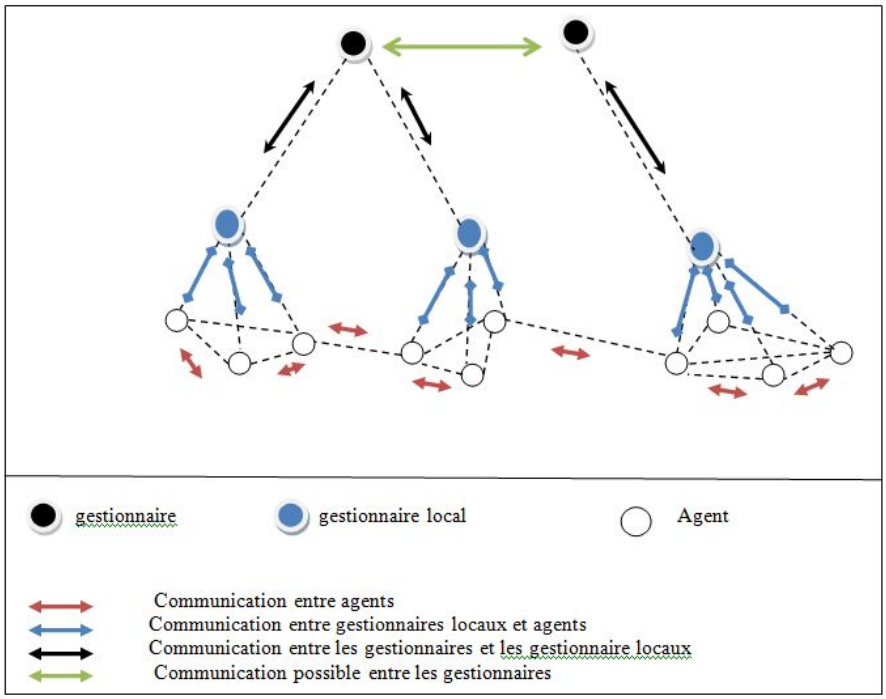

FIGURE 2.5 – Organisation distribuée hiérarchique

2.5.4 Le modèle de communication

Le modèle de communication indique l'architecture de protocole pour échanger des informations de gestion entre les différents noeuds. Il s'agit notamment d'assurer des échanges au niveau applicatif entre le gestionnaire et l'agent [21].

2.6 Classification des approches de monitorage

Plusieurs approches ont été proposées afin de remédier aux problèmes liés au monitorage. Nous avons améloiré la classification citée en [12] par des approches récentes (voir la figure 2.6). Cette classification est effectuée en se basant sur le modèle organisationnel.

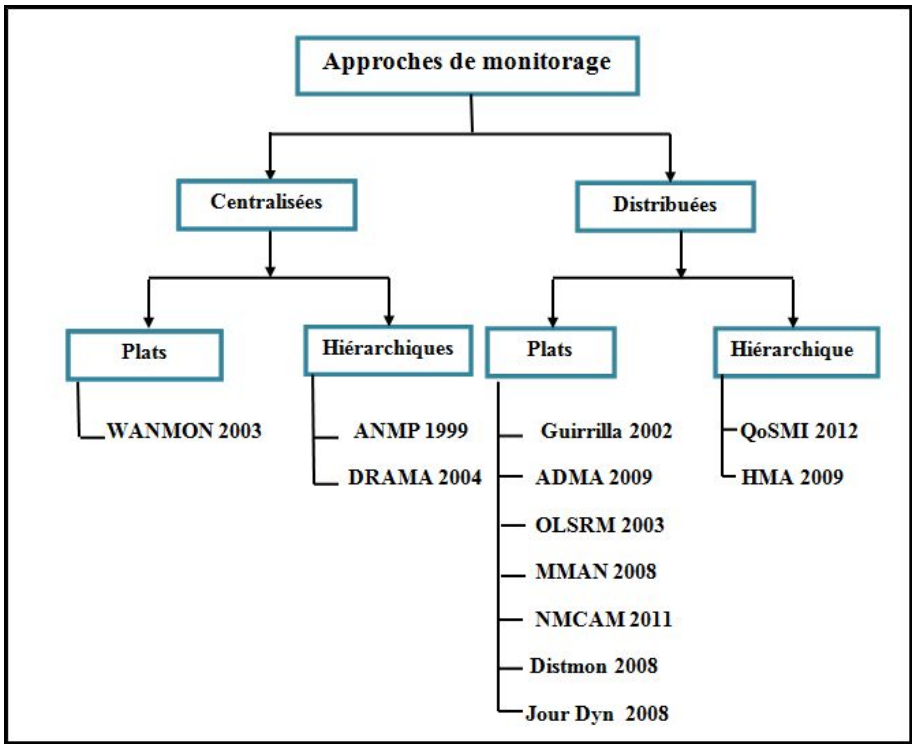

FIGURE 2.6 – Classification des approches de monitorage

2.6.1 Approches centralisées plats

2.6.1.1 WANMon

WANMon (Wireless Ad hoc Network Monitoring Tool) [17] est une approche de monitorage qui permet à un utilisateur de surveiller la consommation de ressources en termes de trafic réseau, consommation d'énergie, occupation mémoire, et charge CPU dans un réseau mobile ad hoc. En particulier, elle vise à distinguer entre les ressources consommées par le nœuds lui-même et les ressources consommées par l'activité de routage au nom des autres noeuds.

L'approche WANMon est décomposée en modules de comptabilité de système qui sont responsables de rassembler des données brutes concernant l'utilisation de ressources, modules de collecte et de traitement de données qui, comme leurs nom l'indique, se chargent du traitement des données venant des modules de comptabilité pour créer l'information utile, ainsi que, des modules d'affichage qui montrent à l'utilisateur les statistiques finales obtenues après traitement au moyen d'une GUI (Graphical User Interface), sous forme d'informations textuelle et/ou graphique.

2.6.2 Approches centralisées hiérarchiques

2.6.2.1 ANMP

ANMP (Ad Hoc Network Management Protocol)[18] est une approche fondée sur le mécanisme de délégation qui permet de confier une partie des opérations de gestionnaire à ses agents, visant ainsi à réduire considérablement le trafic global de la gestion dans le réseau, comparant aux approches centralisées, en favorisant les échanges locaux.

ANMP est décomposé en trois niveaux hiérarchiques comprenant un gestionnaire, des gestionnaires locaux, et des agents. La construction de ces trois niveaux est fondée sur l'utilisation de deux algorithmes de clustering. Le premier repose sur l'identifiant (adresse MAC) des nœuds pour le choix de cluster-head tel que le nœud qui possède le plus petit identifiant sera élu. Le deuxième algorithme, en revanche, repose sur la connectivité des nœuds, tel que le nœud ayant la plus grande connectivité sera le cluster-head (voir la figure 2.7).

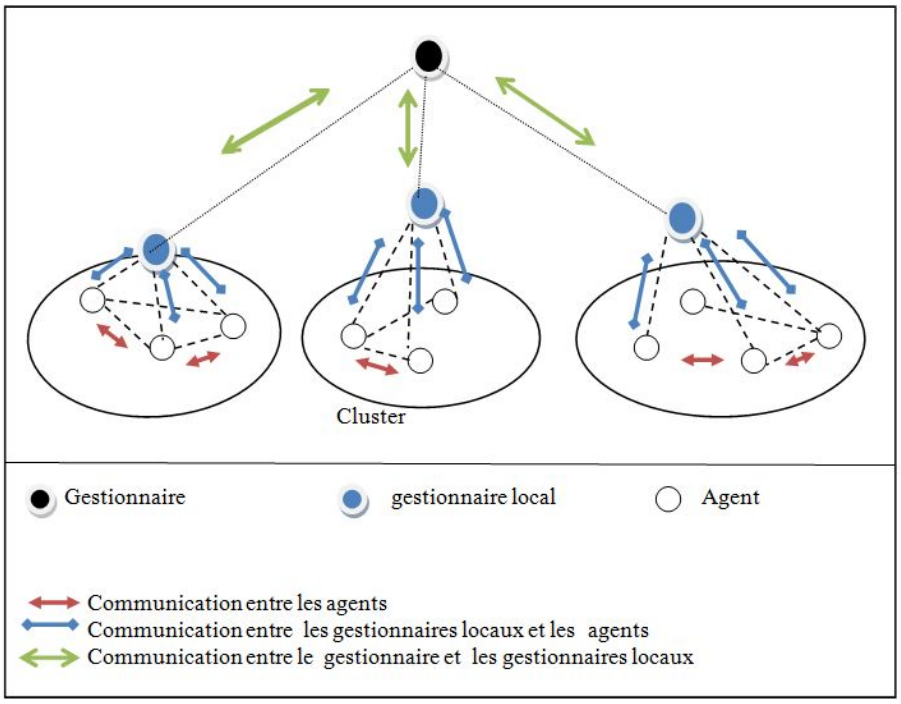

FIGURE 2.7 – L'architecture d'ANMP

Les agents collectent les données spécifiées par le gestionnaire tel que l'énergie restante, nombre de voisins actifs, le taux d'envoie et de réception des paquets, et remplissent la base de données de gestion MIB (Management Informations Base), par la suite, ils envoient une copie de ces informations aux gestionnaires locaux. A la réception de celles-ci, les gestionnaires locaux, les organisent pour former un nouveau message à envoyer au gestionnaire du réseau.

Les informations collectées ainsi que le résultat d'analyse seront stockées par le gestionnaire principal au niveau d'une base de données globale nommée anmpMIB.

2.6.2.2 DRAMA

Cette approche [19] [20] de monitorage est basée sur une gestion par politique qui permet de donner une définition globale des comportements des équipements du réseau à travers un ensemble de règles générique du type " si condition alors action " définies par l'administrateur.

DRAMA(Dynamic Readdressing And Management for the Army) est construite en trois niveaux hiérarchiques sous la forme de clusters. Elle est composée d'un agent global GPA (Global Policy Agent), situé au niveau le plus élevé et qui gère un ensemble d'agents de domaine DPA (Domain Policy Agent), qui à leurs tour prennent en charge des agents locaux LPA (Local Policy Agent)(voir la figure 2.8).

Les politiques de gestion sont disséminées de l'agent global aux agents de domaine et d'agents de domaine aux agents locaux d'une façon hiérarchique.

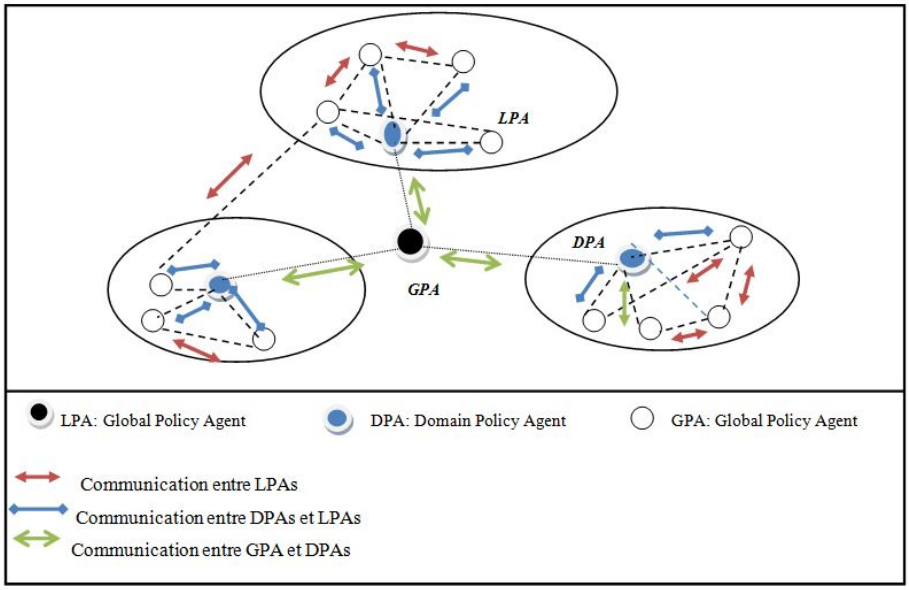

FIGURE 2.8 – L'architecture de DRAMA

Chaque LPA collecte localement les informations de gestion et les envoie au GPA par l'intermédiaire de DPA, en se servant du protocole de gestion YAP (Yelp Announcement Protocol) [19].

Les données collectées seront stockées localement au niveau de chaque nœud dans des bases de données nommées CMDB (Configuration and Monitoring Database) [20].

Divers scénarios d'utilisation de DRAMA ont été évalués à l'aide d'un prototype, tel que le monitorage de la consommation CPU des nœuds ad hoc, la redistribution de serveur lors de l'échec et la reconfiguration d'allocation de la bande passante.

2.6.3 Approches Distribuées plats

2.6.3.1 GUERRILLA

GUERRILLA [21] est une approche distribuée pour le monitorage des réseaux mobiles ad hoc fondée sur le mécanisme de clustering. Elle est décomposée en :

- **Un gestionnaire nomade :** représente le nœud qui a la plus grande capacité (CPU et énergie).
- **Des nœuds Sonde :** représente les nœuds qui ont une capacité (CPU et énergie) suffisante.
- **Des agents :** représentent des nœuds qui ont une capacité (CPU et énergie) minimale.

Le gestionnaire nomade peut décider d'envoyer une sonde active (un scipt spécifiant les opérations de monitorage à réaliser), qui traverse un ensemble de noeuds (nœuds sonde).La sonde active permet à ces derniers de collecter des données de gestion qui seront envoyées au gestionnaire nomade correspondant.

Basé sur les données collectées par les sondes actives, chaque gestionnaire nomade doit construire une vue du secteur de réseau contrôlé. Une fois que celle-ci est établie, le gestionnaire évaluera l'état actuel de son secteur.
Les informations collectées ainsi que les résultats d'analyse seront enregistrés dans une base de données globale nommée GMIB (Guerrilla Management Information Base) au niveau de chaque managers nomade.

2.6.3.2 ADMA

ADMA (Autonomous Decentralized Management Architecture for MANETs) [22] est basée sur la propriété d'auto-configuration qui se rapporte à la capacité des systèmes de se configurer et de se reconfigurer selon des politiques.

Dans cette architecture, chaque nœud contient un ensemble de composants de base : un moniteur, un LPDP (Local Policy Decision Point), un PEP(Policy Enforcement Point) et un dépôt local de politique.

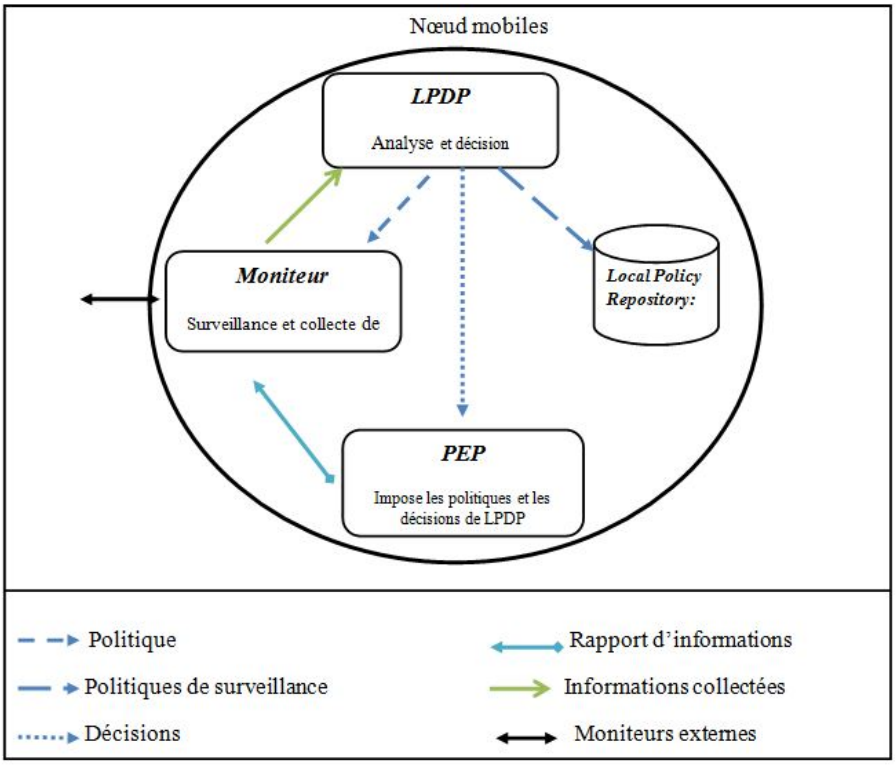

FIGURE 2.9 – L'architecture d'ADMA
[22]

Le moniteur collecte les informations de monitorage (niveau de bruit, taux de perte de paquets, les évènements déclenchés, etc.) et les fournit au LPDP. Ce dernier prend les décisions adéquates, en se basant sur des politiques prédéfinies appropriées et les informations observées par le moniteur. Ces décisions seront ensuite exécutées par le PEP.

2.6.3.3 OLSRM

Cette approche [23] est caractérisée par l'utilisation de protocole OLSR [7] ce qui implique que le concept principal utilisé dans le protocole OLSRM (Optimized Link State Routing Protocol Monitoring) est identique à celui d'OLSR qui est l'utilisation d'un groupe de nœuds choisis pour la diffusion des messages de contrôle de topologie nommés MPRs (MultiPoint Relays).

OLSRM permet de collecter un ensemble de données de la manière suivante :
des nouveaux champs sont inclus dans les messages HELLO(respectivement TC (Topology Control)), tel que le délai entre deux noeuds(respectivement le délai entre MPR et MPR Selector), la consommation de la baterie et la qualité de signal.
Les données échangées via les messages HELLO (respectivement TC), seront stockées

dans les tables de voisins et les tables de MPR Selector(respectivement dans les table de topologie).

2.6.3.4 MMAN

MMAN (Monitor for Mobile Ad hoc Networks) [24] est une approche de monitorage des réseaux mobiles ad hoc, qui se base sur l'utilisation des nœuds de surveillance (MU) ayant une capacité suffisante pour maintenir une vue de la topologie du réseau. L'un de ces nœuds peut jouer le rôle d'un nœuds de gestion.

MMAN comporte trois composants indépendants :

- **Un composant de capture :** il est déployé sur les MUs à travers le réseau, Il permet d'effectuer une observation et une analyse du trafic circulant dans le réseau, et rangés les résultats obtenues dans des dossiers d'information (Info Files).
- **un composant de la livraison de dossier :** il fonctionne sur tout les MUs, ainsi il permet de communiquer les dossiers d'information au composant d'analyse.
- **Un composant d'analyse et GUI (Graphical User Interface) :** il permet d'analyser le contenu des dossiers d'information, les agrégées, et produire des résultats finals (vue globale de topologie).

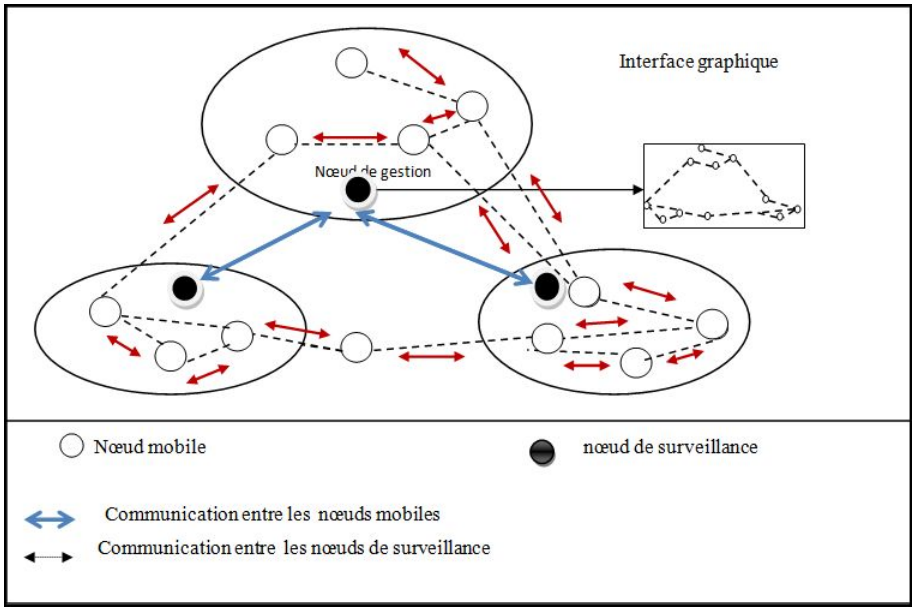

FIGURE 2.10 – L'architecture de MMAN

Les UMs collaborent à la production des vues partielles du réseau en écoutant le trafic et en recueillant les informations nécessaires (l'image de topologie de réseau, le changement des liens, etc). Ces informations seront ensuite envoyées à un nœuds de

gestion, où elles seront analysées et agrégées afin d'obtenir une vue globale du réseau. Cette vue sera, par la suite, présentée sur une interface utilisateur graphique (voir la figure 1.10).

2.6.3.5 NMCAM

NMCAM (Neighborhood Monitoring Based Collaborative Alert Mechanism) [25] est une approche de monitorage qui se base sur le mécanisme de réputation pour la détection des noeuds malveillants dans le voisinage et cela en se servant de protocole du routage DSR [10]. Cette approche repose sur trois composants essentiels qui sont :

- **Le moniteur :** C'est un noeud responsable de l'écoute du trafic et l'enregistrement des paquets envoyés.
- **Le système de réputation :** Il est employé pour maintenir la valeur de confiance pour les nœuds voisins.
- **Le directeur de chemin :** Il est responsable d'apprendre des nouveaux chemins ne contenant pas des nœuds malveillants.

Le moniteur est le composant responsable de la manipulation et de l'enregistrement des paquets envoyés dans le voisinage. A chaque fois qu'un nœud réussit à acheminer un paquet vers la bonne destination, le moniteur enregistre un événement positif à la faveur de ce nœud. Dans le cas contraire, un événement négatif est enregistré. Ces événements seront envoyés par la suite au directeur de confiance (composant interne de système de réputation) qui, en fonction de ces derniers, attribut les valeurs de confiance aux nœuds en incrémentant cette valeur dans le cas positif et en la décrémentant dans le cas négatif.

Une fois qu'une valeur de confiance d'un nœud atteint un seuil donné, le nœud correspondant est ajouté dans la liste défectueuse et n'importe quel paquet venant ou à destination de ce nœud malveillant sera rejeté.

2.6.3.6 Distmon

Distmon (Distributed Monitoring in Ad Hoc Networks)[26] est une approche de monitorage qui permet de rassembler et analyser les traces de trafic de réseau afin d'étudier la conformité de fonctionnement et de propriétés de sécurité du protocole de routage utilisé.

Dans cette approche chaque nœud du réseau rassemble sa trace locale de trafic.

Ces traces serons envoyées à un observateur global.

A la réception de ces traces, l'observateur global procède à la première étape vers l'exécution de l'analyse, qui est la corrélation des traces locales afin de former une trace globale. La deuxième étape consiste à vérifier si les traces sont conformes au fonctionnement prévue et aux propriétés de sécurité du protocole de routage utilisé. Une fois qu'une violation d'une propriété est détectée, une identification du noeud(s) irrégulier qui est derrière cette violation est effectuée.
Le stockage des traces se fait dans des tables crées par l'observateur global nommées tables de traces.

2.6.3.7 Journalisation dynamique de topologie

Cette approche [27] repose sur une architecture distribuée, basée sur des DHT (tables de hachage distribuées) pour le monitorage des réseaux mobiles ad-hoc. Elle permet d'obtenir un journal de l'évolution de la topologie sur des intervalles du temps (slot), qui sera accessible par n'importe quel nœud participant du réseau.

Dans cette approche, au début chaque nœud exécute un agent qui est responsable de capturer la topologie du réseau pour chaque slot de temps. Cet agent commence par initialiser la liste des voisins des noeuds appropriés tel que le premier élément présent dans cette liste est l'adresse MAC du nœud lui-même. Pour la durée du slot de temps, l'agent intercepte des beacons venant des voisins, les analyses, et si leur nombre est au-dessus d'un seuil spécifique, il ajoute l'identifiant (adresse MAC) de ces derniers à sa liste, et cela dans le cas ou ils ne sont pas déjà enregistrés.
A la fin du slot chaque agent crée un enregistrement topologique, en datant la liste de voisinage obtenue avec le slot de temps, et l'ajoute à la DHT.

2.6.4 Approches Distribuées hiérarchique

2.6.4.1 QoSMI

QoSMI (A Novel Quality of Service Monitoring for Mobile Ad hoc Network)[28] est une architecture pour le monitorage de la qualité de service (QoS) dans les réseaux mobiles ad hoc. Elle comprend deux étapes qui sont :

- la construction des nœuds VBB-QoS (Virtuel BackBone-QoS) : cette étape consiste à rassembler les nœuds indépendants qui se caractérisent par leur stabilité dans

un ensemble nommé MIS (Maximal independant set), formant ainsi un domaine comportant des noeuds dominants (MIS) et des nœuds dominés (les autres nœuds qui n'appartiennent pas à la MIS).

Les noeuds de MIS doivent être reliés entre eux (se connecter) pour construire les CDS (connected dominating set)ou VBB.

- l'analyse de QoS et la surveillance de la QoS : cette étape se base sur la logique floue.

Après avoir créé le VBB, chaque nœud dominé devrait mesurer les paramètres de QoS (retard, gigue, perte de paquets) dans son domaine, puis transmet ces mesures à son nœud dominant en utilisant un message unicast. Les valeurs de paramètres collectées par les nœuds dominés seront déployées comme entrées au système de logique floue, qui procède à l'analyse en se servant d'un ensemble de règles, pour produire finalement les résultats sous forme d'une variable linguistique (pauvre, moyen, bon).

2.6.4.2 HMA

HMA (Hierarchy Model for Ad hoc Network Monitoring Based on Clustering) [29] est une approche basée sur un nouveau mécanisme de clustering considérant le degré d'un nœud mobile, le niveau d'énergie, la mobilité et la capacité de transmission pour sélectionner les gestionnaires. Elle consiste en :

- Chaque nœud calcule ses métriques en utilisant la formule suivante :

$$W=w1*Dv+w2*Pv+w3*Mv+w4*Ev$$

Où :

w1,w2,w3,w4 sont des facteurs de poids correspondant aux paramètres :

Dv :le degré, Mv : mobilité, Ev : énergie , Pv : puissance de transmission.

- le nœud ayant une valeur de métrique minimum devient le gestionnaire.
- Le nombre de nœuds dans chaque cluster doit être compris entre une limite supérieur U et une borne inférieur L.
- Lorsque le nombre de membre du cluster est inférieur à la limite inférieur L, ce cluster doit essayer de se fusionner avec un cluster voisin.
- Lorsque le nombre de membre du cluster est plus que la limite supérieure U, ce

cluster doit être scindé en deux clusters.

2.7 Etude comparative

Dans cette partie nous allons effectuer une comparaison entre les différentes approches citées ci-dessus en se basant sur les critères suivants :

- **La distribution de la charge de traitement (Dist trait) :** désigne le fait qu'une approche de monitorage puisse distribuer la charge de traitement sur un grand nombre de nœuds.
- **La distribution de la charge de stockage (Dist stock) :** désigne le fait de pouvoir procurer des mécanismes permettant de garantir la disponibilité des données collectées lors du monitorage pour tous les nœuds aux besoins.
- **Trafic de monitorage (Trafic monit) :** une bonne approche de gestion doit permettre de diminuer le trafic généré lors de processus de monitorage.
- **Consommation d'énergie (Cons Bp et energ) :** une bonne approche de monitorage doit permettre de diminuer au maximum la consommation d'énergie.
- **Scalabilité (Scalab) :** il interprète la capacité de l'approche à s'adapter à l'évolution des utilisateurs dans le système.
- **Robustesse (Robust) :** une approche de monitorage doit éliminer la possibilité de faire face à une situation où un seul point réalise la tâche de collecte et d'analyse de données.
- **Intégrité (Intég) :** une bonne approche de monitorage doit assurer que le trafic n'a pas été altéré ou modifié sans autorisation préalable pendant sa transmission.
- **Confidentialité (Confid) :** une bonne approche de monitorage doit assurer une protection contre les menaces qui peuvent causer la divulgation non autorisée d'informations alors qu'il faut veiller au caractère privé de l'information
- **Détction de nœuds égoïste (Detect nœuds égïstes) :** une bonne approche de monitorage doit permettre la détection des nœuds ayant un comportement égoïste.

2.7.1 Comparaison

Dans cette section nous allons présenter un tableau comparatif des différentes approches étudiées en se basant sur les critères de comparaison cités dans la section

Critères	Dist trait	Dist stock	Trafic monit	cons Bp et energ	Scalab	Robust	Intég	Confid	Detect nœuds égïstes
ANMP	X	X			X			X	
DRAMA	X	X			X				
GUIRRILLA	X	X			X	X			
OLSRM	X	X	X			X			
ADMA	X	X			X	X			
NMCAM	X				X	X			X
MMAN	X	X			X	X			X
J.Dynam	X	X			X	X	X		
Distmon					X	X			
QoSMI	X				X	X			
HMA	X		X			X			

TABLE 2.1 – Etude comparative des approches de monitorage

précédante.

2.7.2 Discussion

Les approches de monitorage présentées précédemment assurent plusieurs critères, mais, présentent de nombreuses limites.

Si nous visualisons la comparaison effectuée dans le tableau 2.1, nous remarquons qu'il existe des critères assurés par la majorité des approches, et des critères assurés par quelques une seulement, et cela dépend de l'objectif de l'approche et du mécanisme utilisé pour l'atteindre.

Nous remarquons que OLSRM assure les critères de la distribution de la charge de trafic et de stockage, et la robustesse, mais elle n'assure aucun critères de sécurité (intégrité, confidentialité et détection des nœuds égoïstes), elle permet, par exemple, d'obtenir une vue de la topologie sans engendrer un trafic additionnel et cela parce qu'elle inclut ses requêtes dans les messages Hello et TC du protocole de routage OLSR. Elle réduit également la consommation d'énergie et de bande passante.

Contrairement à OLSRM, ANMP, NMCAM, journalisation dynamique, et MMAN, assurent un certain niveau du sécurité, en utilisant des mécanismes différents, en plus, ces approches permettent de distribuer la charge de traitement sur le réseau.

On remarque aussi que hormis ANMP et DRAMA, toutes les autres approches sont robustes.

En plus de OLSRM, la seule autre approche qui permet de réduire le trafic du monitorage est HMA.

2.8 Conclusion

Dans ce chapitre, nous avons introduit les notions de base du monitorage, qui est une activité importante pour la gestion des réseaux mobiles ad hoc. Nous avons illustré la nécessité d'une telle activité dans un environnement où nous attendons beaucoup de services mais, nous confrontons aussi de divers obstacles. Par la suite, nous avons cités quelques approches de monitorage, nous avons effectué une comparaison entres elles dans le but de déterminer le manque qui peut être présent dans ce processus.

3

Approche proposée : MonPerf (Monitorage Performant)

3.1 Introduction

Nous allons consacrer ce chapitre à la description de notre proposition, qui consiste à diviser le réseau en groupes de nœuds, tout en évitant ceux ayant un comportement égoïste d'être des gestionnaires.
Notre approche constitue deux phases, la première définit le mécanisme qui permet le calcul des estimations de la valeur de confiance des nœuds dans le réseau. Les estimations obtenues seront exploitées dans la deuxième phase, où, nous proposons un algorithme de clustering multicritères pour partitionner le réseau en groupes.

Dans la première partie de ce chapitre nous donnons quelques définitions nécessaires pour la description de notre proposition. La deuxième partie sera consacrée à description de l'approche proposée.

3.2 Motivation

Dans le chapitre précédent, nous avons présenté plusieurs approches de monitorage qui tentent de répondre aux défis des réseaux mobiles ad hoc.

La plupart de ces approches se basent soit sur des protocoles de routage, offrant ainsi la possibilité de réduire le trafic de monitorage, mais elles sont uniquement destinées à l'amélioration de routage. En plus, la mise en place de ces approches sur des réseaux à grand échelle augmente considérablement la taille des tables de routage.
Les autres approches utilisent des mécanismes de clustering, qui offrent des solutions simples et extensibles. L'élection des cluster-head, dans ces solutions, se base sur un critère ou une combinaison de paramètres. Cependant, ces critères ne prennent pas en considération toutes les caractéristiques des réseaux mobiles ad hoc, à titre d'exemple, la mobilité des nœuds, leur énergie limité, la sécurité, etc.
Parmi les algorithmes de clustering utilisés dans les approches de monitorage vues précédemment nous pouvons citer : l'algorithme basé sur l'identifiant minimal et la connectivité des nœuds. Cet algorithme permet de stabiliser les gestionnaires, mais un tel choix peut être loin de l'optimum, si un nœud à identifiant minimal est très mobile ou si sa réserve d'énergie est faible, ou bien encore, s'il a un comportement malhonnête .

Notre intérêt principal est de construire une topologie divisée en groupe, où les cluster-heads seront c'eux qui possèdent l'énergie maximales, les plus confiants, et qui sont moins mobiles possibles. Notre proposition doit, également, prendre en charge la détection

et la sanction des nœuds qui ont un comportement égoïste.

3.3 Quelques définitions

Avant de procéder à l'explication de notre proposition, nous allons donner quelques définitions nécessaires pour conprendre notre approche.

3.3.1 La confiance

Il existe plusieurs définitions de la confiance dans la littérature :

Selon **Mcknightet et Chervany**[30] : " La confiance est la dépendance qu'une entité est prête à accepter vis-à-vis d'une chose ou d'une personne dans une situation donnée avec un sentiment de sécurité relative, même si des conséquences négatives sont possibles.".

Dans [31], La confiance est définit comme étant une relation unidirectionnelle entre deux entités participant à un protocole. Cette relation est basée sur l'évaluation des informations reçues ou sur l'évaluation des interactions passées entre ces deux entités dans le cadre de l'exécution du protocole. La relation de confiance dépend du domaine d'application dans lequel elle est utilisée.

Selon [32] le terme " confiance " est définit comme suite : " On dit qu'une entité fait confiance à une autre entité si et seulement si cette dernière se comporte exactement comme la première le prévoit ". Ceci signifie qu'un nœud ne peut faire confiance à un autre nœud seulement si ce dernier se comporte d'une façon correcte.

3.3.2 Nœud égoïste

Un nœud égoïste est un nœud économiquement rationnel dont l'objectif est de maximiser son propre bien-être, qui est définit comme le bénéfice de ses action moins leurs coûts, et que la transmission d'un message inflige un coût(énergie et autre ressources) à un nœud ; le nœud égoïste aurai besoin d'incitation en vue de transmettre les messages des autres [34].

3.4 Description de l'approche proposée : MonPerf

3.4.1 Le choix du modèle organisationnel

Nous proposons une approche de monitorage distribuée pour les réseaux mobile ad hoc, qui intègre un mécanisme de clustering et un modèle de confiance, et qui est basée sur le modèle organisationnel.

Notre choix pour ce modèle se réfère à sa simplicité, sa facilité à mettre en œuvre, et la possibilité de déterminer le rôle et la relation de chaque nœud mobile intervenant dans le réseau.

Nous proposons une architecture qui intègre le mécanisme de clustering qui prend en considération la notion de confiance.

3.4.2 Format des messages

Dans notre proposition, nous allons considérer que chaque nœud du réseau diffuse périodiquement des messages 'hello' qui inclus aussi les champs suivants : P et CH, qui représentent respectivement le poids des nœuds et l'identifiant de cluster-head.

3.4.3 Election des gestionnaires

Dans l'algorithme d'élection que nous proposons, le gestionnaire représente le nœud ayant un poids P maximal parmi ses voisins, tel que :

$$P=W1*P1+W2*P2+W3*P3+W4*P4 \qquad (1)$$

Où :

W1, W2, W3 et W4 représentent les coefficients des métriques (le degré d'implication des métriques). Ils se varient en fonction des besoins de l'application.

Et P1,P2,P3,P4 appartiennent à l'intervalle [0,1].

- **P1 : la valeur de confiance**

  Notre algorithme de clustering utilise la confiance comme l'un des critères de partitionnement. La confiance est fondamentale pour maintenir un certain niveau de sécurité. C'est un aspect important pour l'élection d'un gestionnaire, et par lequel les relations entre les nœuds peuvent se développer ou cesser.

Nous proposons d'attribuer initialement à chaque nœud une valeur de confiance qui est égale à 0,5 pour ne pas considérer un nœud, au préalable, comme étant égoïste où confiant.

Pour établir une première estimation de la valeur de confiance, nous proposons d'utiliser le taux d'activité (R), qui est calculé en fonction de nombre de paquets correcte et de nombre de paquets total.

Si on considère deux nœuds i et j, le nœud i calcule le R de j de la manière suivante :

Le nœud i doit enregistrer le nombre de paquets correcte avec j (pos(i, j)), et le nombre d'interactions totales (total(i, j)), puis calcule le taux d'activité comme suit :

$$R=\text{pos}(i,j)/\text{total}(i,j) \quad (2)$$

Le taux d'activité est sauvegardé et recalculé à chaque sycle de monitorage par les nœuds du réseau.

La valeur de confiance évalue dans le temps en fonction des changements dans le taux d'activité, tel que si ce dernier diminue, la valeur de confiance sera également diminuée d'un 0,1, et s'il augmente, la valeur de confiance augmentera aussi de la même valeur.

Ces estimations de confiance directes peuvent être renforcées par les rapports de confiance distribués qui permettent aux nœuds de partager leurs estimations dans le réseau.

Pour distribuer les rapports de confiance, chaque nœud i diffuse un paquet à ses voisins directs, contient son identifiant et la liste de ses voisins (identifiant des voisins). Il attend une période T pour la réception des estimations, puis il calcule la valeur de confiance de chacun de ses voisins, compris la sienne, en utilisant la formule suivante :

$$Vcj = (\sum_{k=1}^{n} Vc(k,j)) + Vc(i,j))/n \quad (3)$$

Où :

n est le nombre de nœud qui ont envoyé leurs estimation de confiance sur le nœud j au nœud i .

v(k,j) est l'estimation du nœud k sur le nœud j.

si jamais la valeur de confiance baisse à une valeur spécifique Vmin , le nœud sera

sanctionné.

– **P2 : l'énergie restante**

Dans notre approche, nous considèrons l'énergie comme une probabilité qu'un nœud i à un taux d'énergie total.

L'énergie est mise à jour après un envoi ou une réception de message hello, par le modèle de consommation d'énergie de Heinzelman et al [33] défini comme suit : Heinzelman et al proposent un modèle radio de consommation d'énergie (voir figure 3.1). avec ce modèle, les énergies nécessaires pour émettre ETx(s,d) et recevoir ERx(s)des messages sont définies comme suit :

– Pour émettre un message de 's' bits vers un récepteur loin de 'd' mètres, l'émetteur consomme :

$$\begin{aligned} \text{ETx(s, d)} &= \text{ETxelec(s)} + \text{ETx (amp(s, d))} \qquad (4) \\ \text{ETx(s, d)} &= (\text{Eelec} * \text{s}) + (\text{Eamp} * \text{s} * \text{d}^2) \end{aligned}$$

– Pour recevoir un message de s bits, le récepteur consomme :

$$\begin{aligned} \text{ERx(s)} &= \text{ERxelec(s)} \qquad (5) \\ \text{ERx(s)} &= \text{Eelec} * \text{s} \end{aligned}$$

Eelec et Eamp représentent respectivement l'énergie de transmission électronique et d'amplification tels que :

Eelec=10^{-10}nJ ;

Eamp = 5^{*-8}nJ.

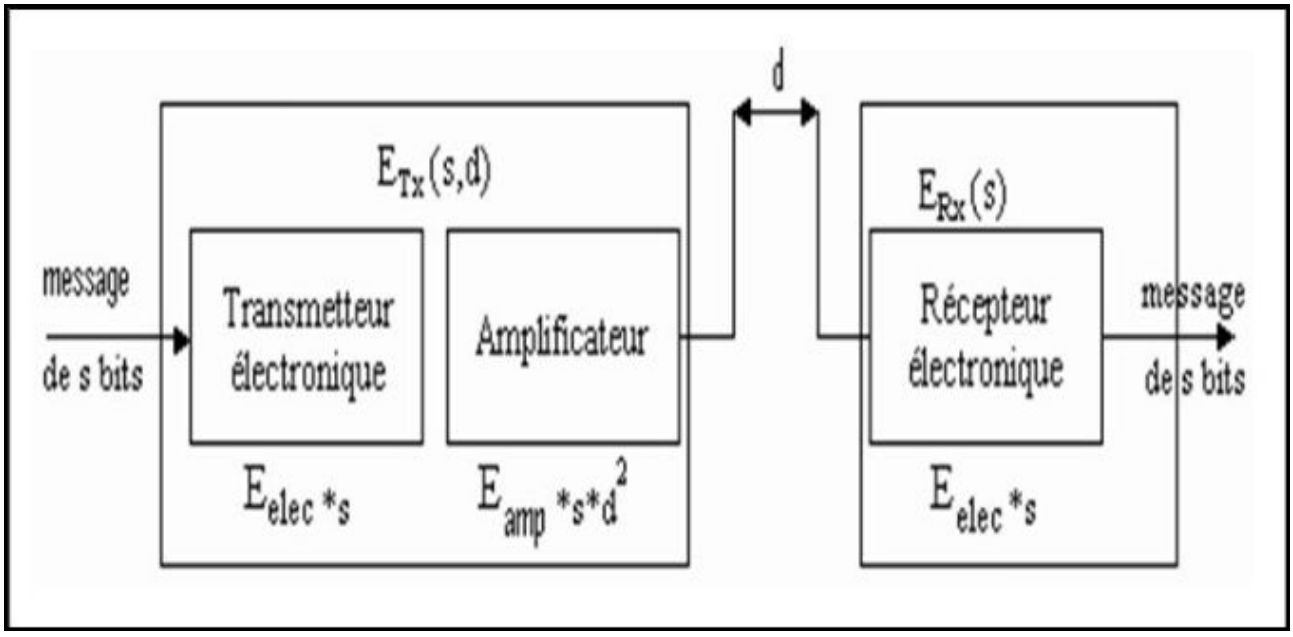

FIGURE 3.1 – le modèle de consommation d'énergie de Heinzelman

– **P3 : la connectivité**

Dans notre approche, nous considèrons la connectivié comme une probabilité qu'un nœud i à un nombre de voisins égale n-1.

– **P4 : la mobilité**

Pour déterminer la mobilité, nous proposons d'estimer la probabilité qu'un nœud se déplace pendant le cycle actuel de monitorage.

Notre choix est basé sur le fait qu'un manager, doit avoir un niveau d'énergie acceptable pour réaliser la tâche de monitorage, il doit découvrir le maximum de voisins, il ne doit pas se déplacer souvant, pour réduire le nombre d'élection, et il doit, également, avoir un niveau de confiance important.

3.4.3.1 Description de l'algorithme d'élection

Chaque nœud vérifie d'abord son poids et celui de ses voisins direct, et choisit le nœud ayant le poids maximal. Par la suite, il vérifie le poids de ses voisins à deux saut, et sélectionne, également, le nœud qui possède la valeur maximal. Ensuite il vérifie ces deux valeurs pour désigner finalement, le gestionnaire comme étant celui ayant le poids maximal à un ou à deux sauts. Dans le cas d'un même poids maximal, le gestionnaire sera le nœud qui a les meilleurs critères selon leurs importances (P1, P2 P4, puis P3).
pour mieux comprendre le principe d'élection, nous allons expliquer son fonctionnement sous forme d'algorithmes :

Algorithme

var : n nombre de nœuds du réseau ;

var : n1 nombre de voisins à un saut ;

n2 nombre de voisins à deux sauts ;

v1 l'ensemble des poids d'un nœud et ses voisins à un saut ;

v2 l'ensemble des poids des voisins à deux saut ;

P1max le poids maximal des poids des voisins à un saut ;

P2max le poids maximal des poids des voisins à deux saut ;

i, j, id1, id2, CH : entier ;

debut

j=0 ;

tanque(j<n) **faire**

pour(i allant de 1 à n1) **faire**

P1max < − max(V1) ;

id1 < − id(P1max) ;

finpour

pour(i allant de 1 à n2) **faire**

P2max < − max(V1) ;

id2 < − id(P2max) ;

finpour

j=j+1 ;

fin tantque

si (P1max >P2max)**alors**

CH < − id1 ;

sinon

CH < − id2 ;

finsi

fin

3.4.3.2 Maintenance des clusters

Plusieurs situations peuvent impliquer l'élection d'un nouveau gestionnaire. Nous nous concentrons sur les situations suivantes :

- Si un gestionnaire tombe en panne, ses membres ne reçoivent plus ses messages hello périodiques. Dans ce cas, les membres ré-initialisent le champ CH de leurs messages hello à null pour désigner un autre gestionnaire.
- Si un gestionnaire veut se déplacer , il doit déléguer un autre gestionnaire parmis ses voisins à un saut ou à deux sauts qui a le poids maximal.
- A l'arrivée d'un nouveau nœud à un cluster, ce dernier reçoit les messages hello venant des nœuds à sa portée.Il vérifier l'identité du gestionnaire qui se trouve dans les messages hello, s'il trouve que ce dernier est un voisin direct, ou à deux sauts, il lui envoi sa demande d'ajout. A la réception de la demande par le gestionnaire, ll vérifie le nombre de son membre, s'il trouve que ce nombre est superieur ou égal à une limite superieur S, il rejette la demande.

  Si le nouveau nœud est rejeter par plusierurs gestionnaire, dont il a envoyé des demandes, il crie son propre cluster.

3.4.4 La détection des nœuds égoïstes

La détection des nœuds égoïstes se rapporte à la diminution de taux d'activité R.

Nous proposons de considérer un nœud comme égoïste si sa valeur de confiance baisse au dessus d'une valeur minimale Vmin=0,1, mais, il sera suspecté dés que sa valeur de confiance atteint la valeur 0,3. Un nœud détecté comme égoïste sera ajouté à une liste comportant ce type de nœuds. Pour ne pas suspecter un nœud à tort, nous proposons d'attribuer aux nœud un nombre maximum de fautes à toléré, et de vérifier son énergie, avants de l'ajouter à la liste.

Pour mieux formaliser le processus de détection de nœuds égoïste, nous proposons l'algorithme suivant :

```
Algorithme
    var : Vcn la valeur de confiance d'un nœud n
          Nbref nombre de faute ;
debut
  si(Vcn<=0,3)
    si (P2<>0) alors
      si (nbref>=nbref-max) alors
        si(membre)alors
          Ajouter le nœud à la liste ;
        finsi
        si (gestionnaire)alors
          Ajouter le nœud à la liste ;
          Répétition de clustering ;
        finsi
      sinon
        Vcn=Vcn-0,1 ;
        Nbref=nbref+1 ;
      finsi
    finsi
  finsi
fin
```

3.4.5 Monitorage

Après avoir décomposé le réseau en cluster et déterminer les nœuds égoïstes, les nœuds du réseau peuvent entamer le processus de monitorage.

- **La collecte d'informations**

  Pour la collècte de données, nous se référons au travail réalisé dans [34], qui se base sur la théorie des jeux pour la mise en place d'une collecte optimisée, permettant de réduire l'énergie consommée et le nombre de messages pour effectuer cette collècte.

- **L'analyse des informations**

  Chaque cluster-head analyse les informations venant des nœuds de son cluster

et en cas d'anomalies lancent des alertes. A la fin de cette analyse, il construit un rapport de monitorage sur l'état de son cluster.

– **Le stockage des informations**

Au niveau de chaque cluster-head, il existe une base de données pour le stockage des données collèctées et les rapports d'analyse.

3.4.6 Exemple illustratif

Dans ce qui suit, nous allons donner un exemple illustrant notre approche, en exploitant le réseau modélisé dans la figure suivante :

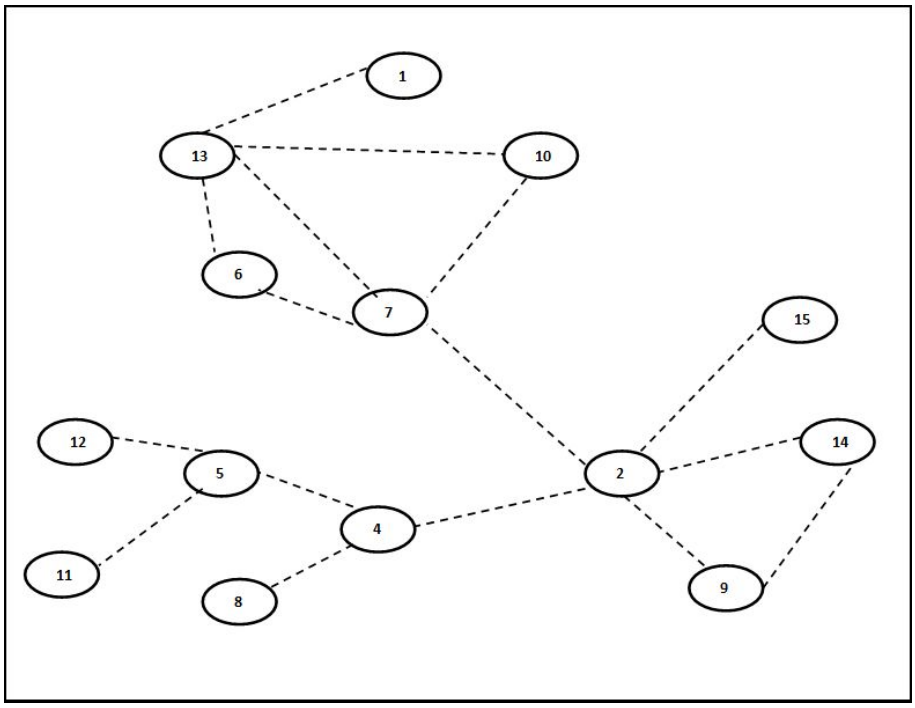

FIGURE 3.2 – Le réseau modélisé

– **Etape 1 : Le calcul de la valeur de confiance**

Dans cet exemple, nous allons supposer que chaque nœud à déjà calculer ses première estimations en fonction du taux d'activité.

Si nous considérons le nœud 13 qui veut renforcer ses estimations de ses voisins alors :

Le nœud 13 envoie un paquet, soit par exemple Req(13, 1,6,7,10) à ses voisins.

A la réception du Req par :

- Le nœud 7, il prépare une réponse, soit ResReq(7, (13, 0,5), (10, 0,7),(6, 0,5)) destiné à 13, qui comporte les estimations qui possède sur les nœuds 13, 10 et 6.
- Le nœud 6, il prépare une réponse, ResReq(6, (13, 0,5), (7, 0,8)) destiné à 13, qui comporte les estimations qui possède sur les nœuds 13 et 7.
- Le nœud 10, il prépare une réponse, ResReq(10, (13, 0,5), (7, 0,4)) destiné à 13, qui comporte les estimations qui possède sur les nœuds 13 et 7.
- Le nœud 1, il prépare une réponse, ResReq(1, (13, 0,5)) destiné à 13, qui comporte les estimations qui possède sur le nœud 13.

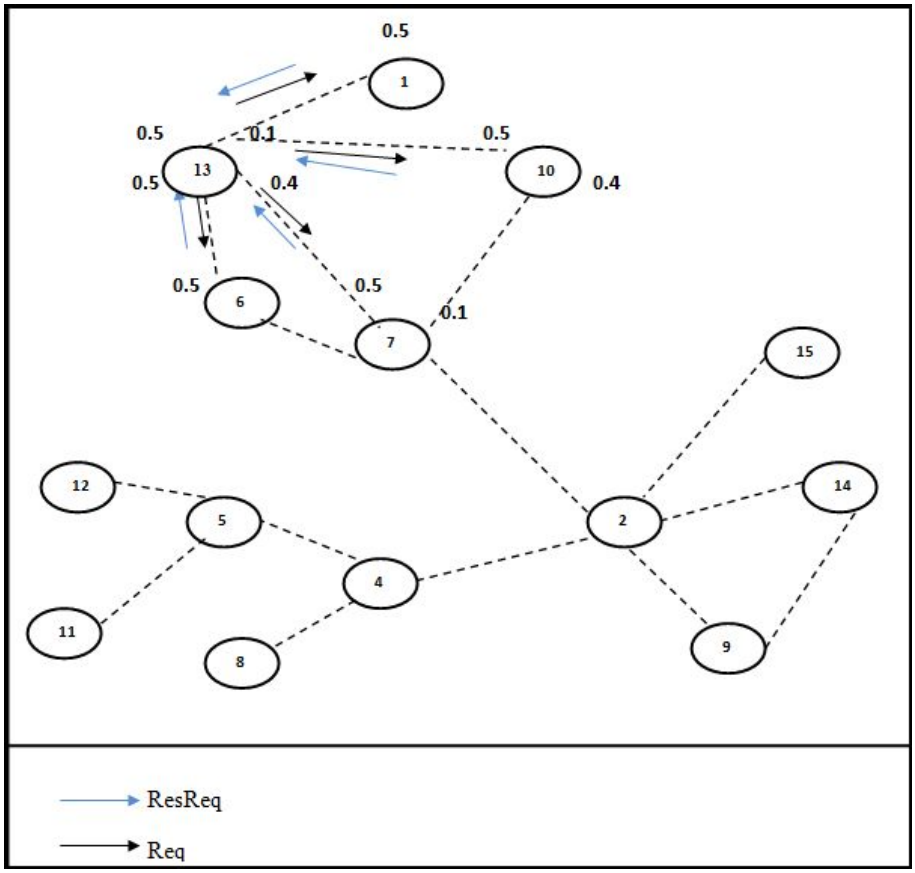

FIGURE 3.3 – envoie du Req et réception des ResReq

A la réception de ResReq par le nœud 13, il procède au calcule des valeurs de confiance de ses voisins :

- Pour le nœud 1 : le nœud 13 n'a pas reçu d'estimation sur ce nœud, alors le 1 aura comme valeur de confiance celle estimée par 13, c-à-d : Vc1=0,5.

- Pour le nœud 6 : Vc=0,2+0,5= 0,7

- Pour le nœud 10 : Vc= 0,1+0,1= 0,2

- Pour le nœud 7 : Vc= 1/2*(0,8+0,4+0,4)= 0,8

- Pour le 13 : Vc=1/4*(0,5+0,7+0,2+0,8)=0,5

De cette façon, le nœud 13 aura les valeurs de confiance de tous ses voisins directs (voir la figure 3.4).

Dans notre exemple le nœud 10 sera suspecté d'être égoïste puisqu'il a une valeur inférieur à 0,3.

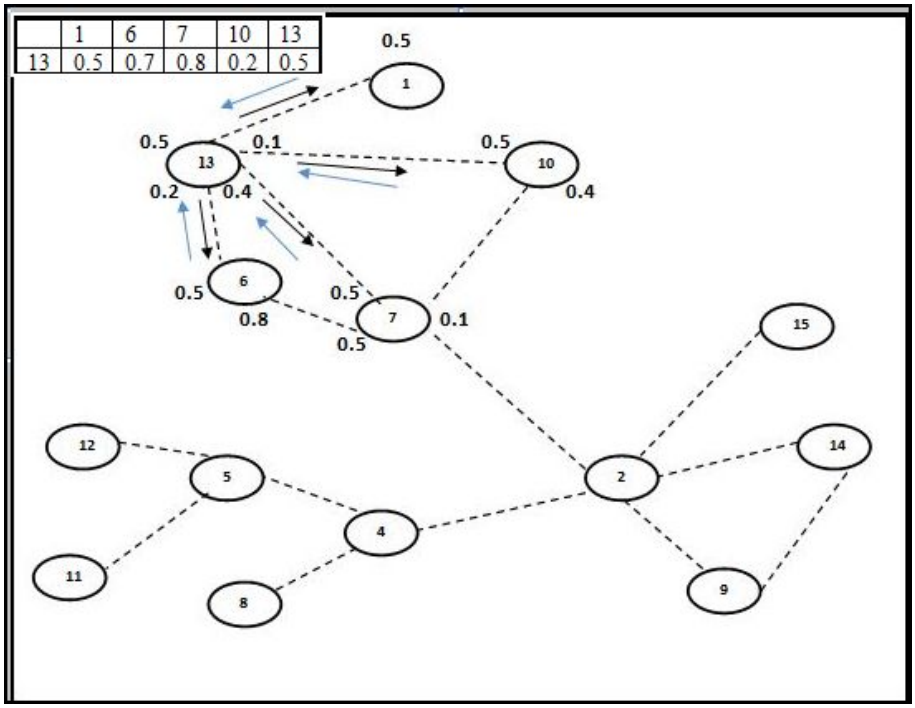

FIGURE 3.4 – Le calcul de la valeur de confiance

– **Etape 2 : La division du réseau en groupes**

En appliquant l'algorithme d'élection sur le réseau présenté dans la figure 3.2, nous aurons le réseau de la figure3.5, où les nœuds appartiennent à des clusters, tel que chacun d'eux est contrôlé par un cluster-head.

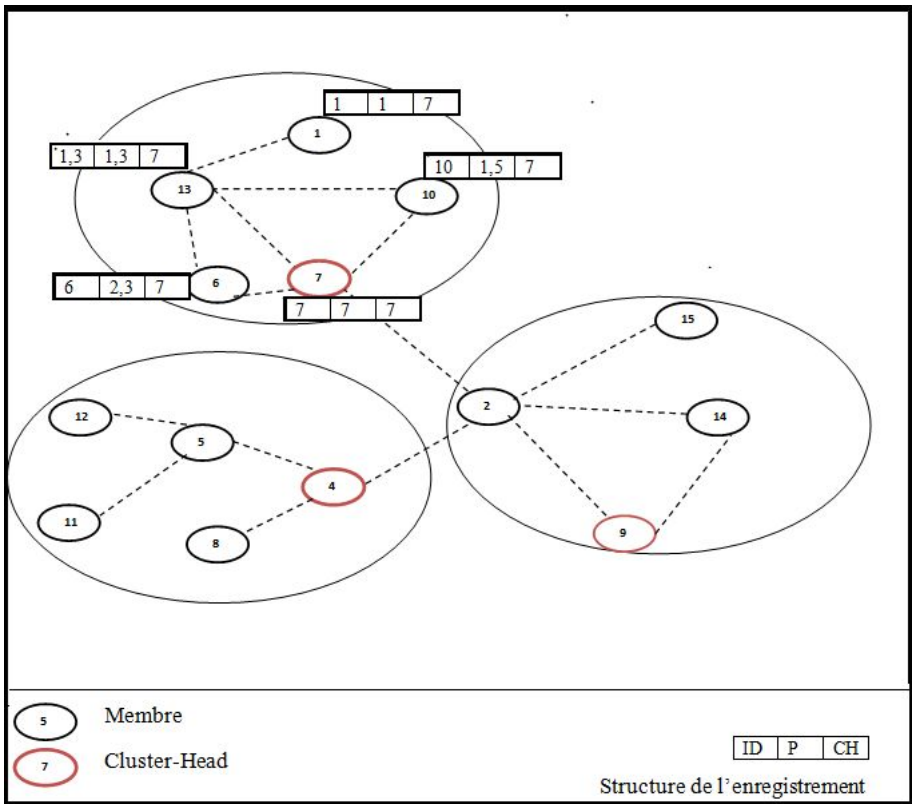

FIGURE 3.5 – Division du réseau en clusters

– **Etape 3 : Le monitorage**

La figure suivante montre un exemple du processus de monitorage de l'énergie restante dans un réseau organisé en cluster : Les nœuds 1, 6,10 et 13 collectent les données de monitorage (id et énergie) et les envois à leurs gestionnaire, qui est dans notre exemple le nœud 7. A la réception de ces données, le gestionnaire les analyse en se basant sur des règles de gestion définies selon la nature de l'application.

Exemple : Nous supposons que le seuil minimal pour l'énergie est 0,2. Le gestionnaire trouve que l'énergie du nœud 6 est inferieur à 0,2, donc il lance une alerte.

Les données collectées et les rapports résultants seront stockés au niveau du gestionnaire 7.

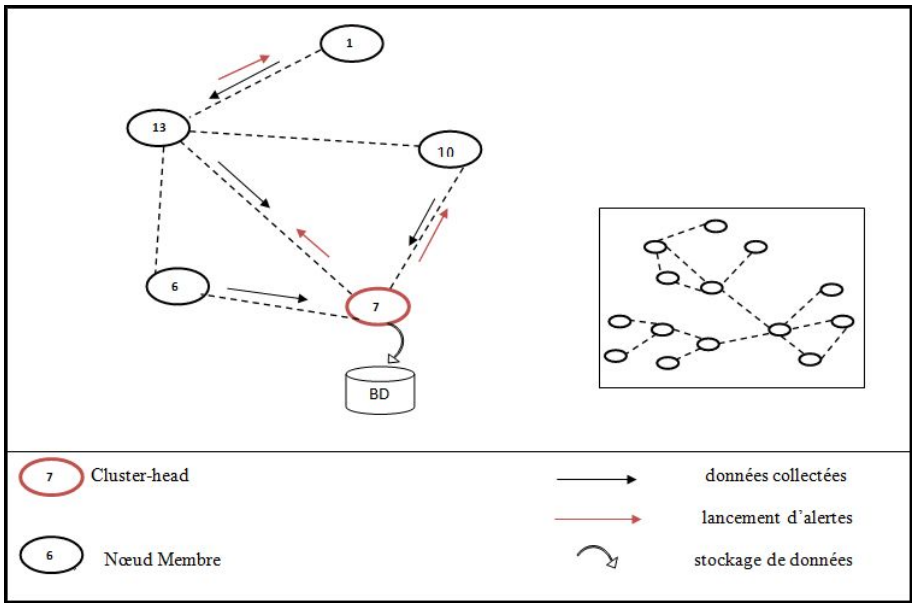

FIGURE 3.6 – Le monitorage

3.5 Conclusion

Dans ce chapitre nous avons présenté une solution pour un monitorage performant des réseaux mobiles ad hoc, basée sue un modèle de confiance et un algorithme de clustering, puis nous avons donné un exemple illustratif pour bien expliquer le fonctionnement de notre approche.

4

Simulation et étude des performances

4.1 Introduction

Dans le chapitre précédent, nous avons présenté une nouvelle approche pour le monitorage des réseaux mobile ad hoc, basée sur un modèle de confiance et un nouveau mécanisme de clustering. Afin d'évaluer ses performances, nous l'avons comparé avec l'approches HMA [29] et l'approche NMCAM [25]. La première approche propose un mécanisme de clustering multicritère. L'autre approche utilise un modèle de confiance pour assurer un acheminement fiable des paquets.

Nous présentons en premier lieu l'environnement de simulation utilisé avec les métriques de performances mesurées, les scénarios de simulations adoptés, puis nous donnons l'interprétation des résultats obtenus à l'issue de ces simulations.

4.2 Environnement de simulation

Pour tester les performances d'une solution apportée à un problème de communication dans un réseau, il n'est pas toujours possible d'accéder aux infrastructures nécessaires en raison de leurs coûts élevés. De plus, les expérimentations réelles n'offre souvent pas une grande souplesse. Rappelons que les réseaux mobiles ad hoc sont des réseaux qui englobent plusieurs unités mobiles qui se déplacent dans un territoire quelconque et dont le seul moyen de communication est l'utilisation des interfaces radio. En effet, il serait très coûteux voir impossible de mettre en place un réseau à des fins de tests de certains critères.Pour remédier à ce problème et afin de tester les performances d'un nouveau protocole, on a recours à la simulation qui met à la disposition de l'utilisateur un environnement d'expérimentation. Parmi les simulateurs les plus utilisés dans la communauté des réseaux mobile ad hoc, nous citons le simulateur MATLAB.

4.2.1 Le choix de MATLAB

MATLAB est un logiciel de calcul numérique produit par MathWorks. Il est disponible sur plusieurs plateformes.

MATLAB est un langage simple et très efficace, optimisé pour le traitement des matrices, d'où son nom. Pour le calcul numérique, MATLAB est beaucoup plus concis que les anciens langages (C, Pascal, Fortran, Basic) et pour la programmation, il optimise le code des programmes en utilisant des fonctions prédéfinies. On peut traiter la matrice

comme une simple variable. MATLAB contient une interface graphique puissante, et on peut l'enrichir en ajoutant des "boites à outils" (toolbox) qui sont des ensembles de fonctions supplémentaires, profilées pour des applications particulières (traitement de signaux, analyses statistiques, optimisation, etc.). Il permet aussi la création de fonctions et distingue les données locales des données globales. Ces avantages ont rendus de MATLAB, un langage de programmation et de simulation très sollicité.

4.3 Les paramètres de simulation

Le tableau suivant contient les paramètres du réseau sur lequel les simulations ont été effectuées.

Paramètres	**Valeur initiale**	**Type**	**Unité de mesure**
Nombre de nœuds	100	Entier positif	
nombre de nœuds égoïstes	$30 - 80$	Entier positif	
Portée des nœuds	20	Entier	Mètre
Temps de simulation	6000	Seconde	
Taille du réseau	$100 * 100$	Surface	m^2

TABLE 1.1-Paramètres de simulation

– **L'échéancier**

Les évènements détectés dans le réseau sont rangées dans un échéancier (voir le tableau 1.2).

Numéro d'évènement	1	2	3	4	5
Nœud émetteur	4	1	5	2	3
Nœud récepteur	2	1	4	3	5
Temps d'arrivé	1.67	2.20	2.89	3.23	3.56

TABLE 1.2- Table d'echancier

4.4 Les étapes de réalisation du simulateur

Les étapes décrivant la réalisation de notre simulateur sont illustrées par l'algorithme ci-dessous :

Début

Initialisation des variables de simulation

Déploiement des nœuds dans le réseau

Initialisation de l'échéancier

Clusterisation

Monitorage

Affichage des résultats

Fin

4.4.1 Initialisation des variabes de simulation

Cette phase est exécutée automatiquement au début du programme de simulation. Elle inclut la déclaration des variables globales (nombre de nœuds, zone de déploiement simulée, temps max de simulation, etc) et leur initialisation, ainsi que la création des nœuds sous forme d'une structure qui comporte (identité du nœud, leur coordonnées).

Structure d'un nœu
identité du nœud : id
Coordonnées du nœud (x,y) : cord
Energie : e
Nombre de voisins : nb
Valeur de confiance : vc
Mobilité : m
Poids : P
Id de Cluster-head : ch
Nombre de fautes d'un nœuds : Nbrefaut
Nombre de messages reçus : NbreMR
Nombre de messages envoiés : NbreME
Tablenoire : tabln

TABLE 1.3- Structure d'un nœud

4.4.2 Déploiement du réseau

Les nœud constituants notre réseaux sont déployés d'une manière aléatoire sur une surface de (100*100) m^2. Chaque nœud dans le réseau est représenté par ses coordonnées (x,y).

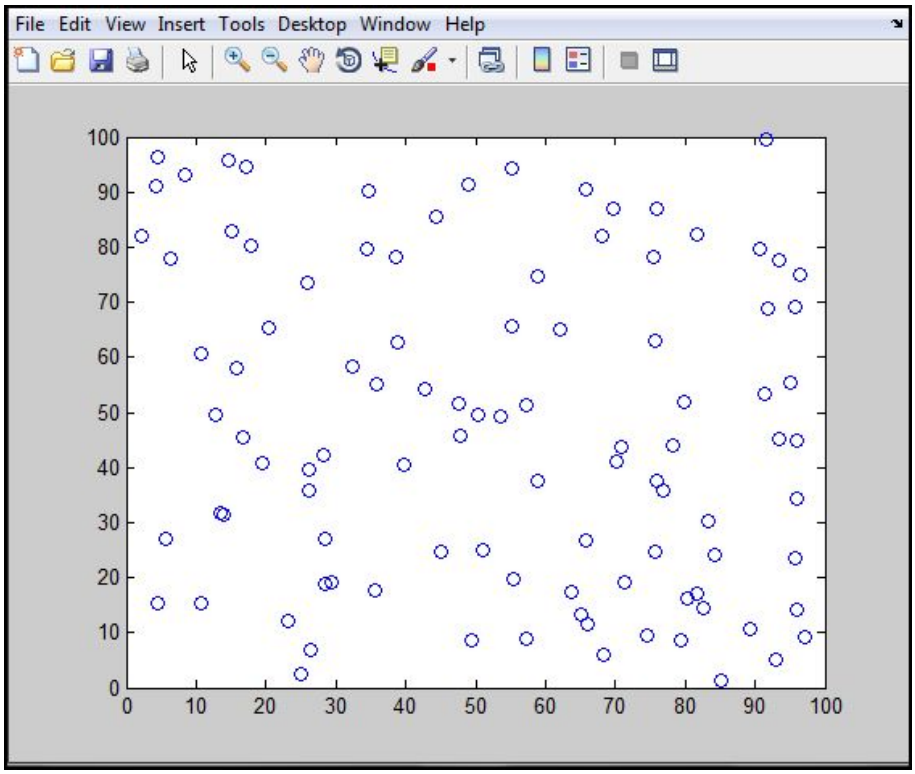

FIGURE 4.1 – Déploiement du réseau

4.4.3 Application de l'algorithme d'élection

Dans notre approche de clusterisation, l'élection d'un cluster-head se base sur le calcule de poids de chaque nœud, en suivant la formule (1) citée dans le chapitre 3. Le cluster-head élu représente le nœud ayant la valeur du poids maximale parmi ses voisins à un saut ou à deux sauts.

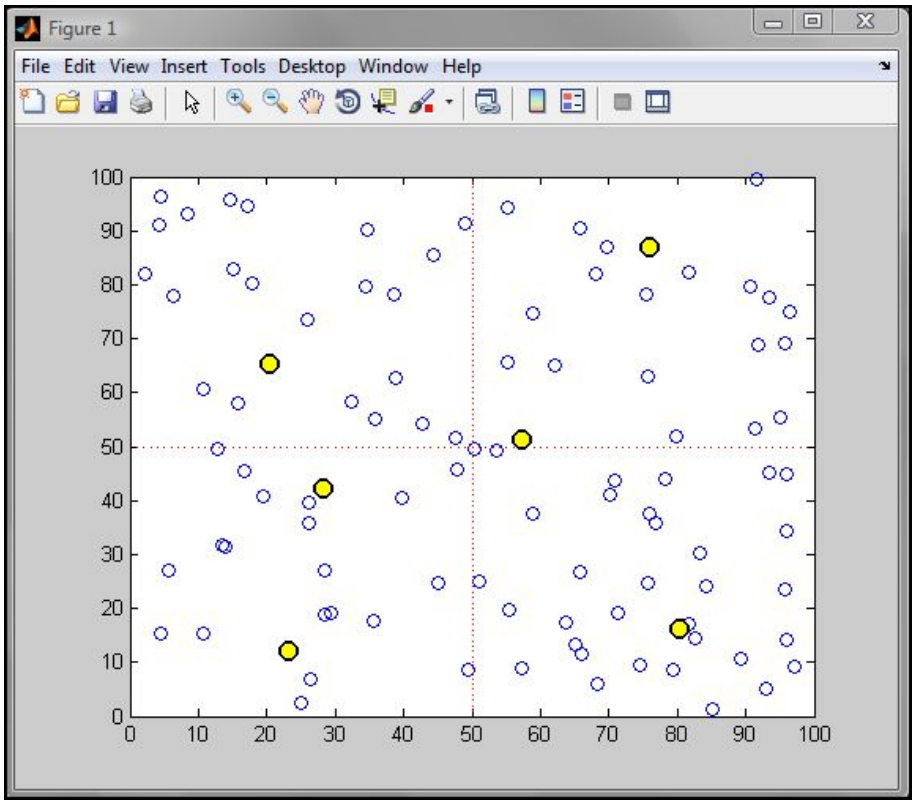

FIGURE 4.2 – Eléction des gestionnaires

4.4.4 Détection des nœuds égoïstes

La détection des nœuds égoïstes se base sur l'échange des données entre les nœuds (émetteurs/récepteurs), tel que à chaque échange nous procèdons à une vérification du nœud demandeur en calculant sa nouvelle valeur de confiance à partir du taux d'activité, et en vérifiant sa présence dans la liste.

4.5 Les métriques d'évaluation de performances

Nous allons évaluer notre solution en utilisant les métriques de performances suivantes :

- Le taux de détection des nœuds égoïste

Pour montrer l'efficacité de notre proposition, nous mesurons le taux de détection des nœuds égoïste en se basant sur le rapport entre le nombre de nœuds égoïstes détecté par au moins un nœud divisé par le nombre total des nœuds égoïstes.

- Les nœuds égoistes élus comme des managers

Cette métrique permet d'examiner les fonctionnalités des managers.

- Le taux de paquets reçus avec succès

C'est le nombre de paquets de données reçus avec succès par la destination par rapport au nombre de paquets de données émis par la source, Il nous permet de vérifier si l'approche proposée a un impact sur le transfert de paquets de données avec succès.

- le taux de perte de paquets Il est mesuré en termes de rapport de données non livrés aux destinations.

4.6 Simulation : résultats et interprétations

Pour étudier l'efficacité de notre approche après avoir pris en considération la notion de confiance , nous allons la comparée avec les deux approches HMA [] et NMCAM []. En se basant sur les paramètres d'évaluation cités précédemment, nous analysons les résultats de simulation obtenus dans les figures ci-dessus comme suit :

1. Le taux de détection des nœuds égoïstes

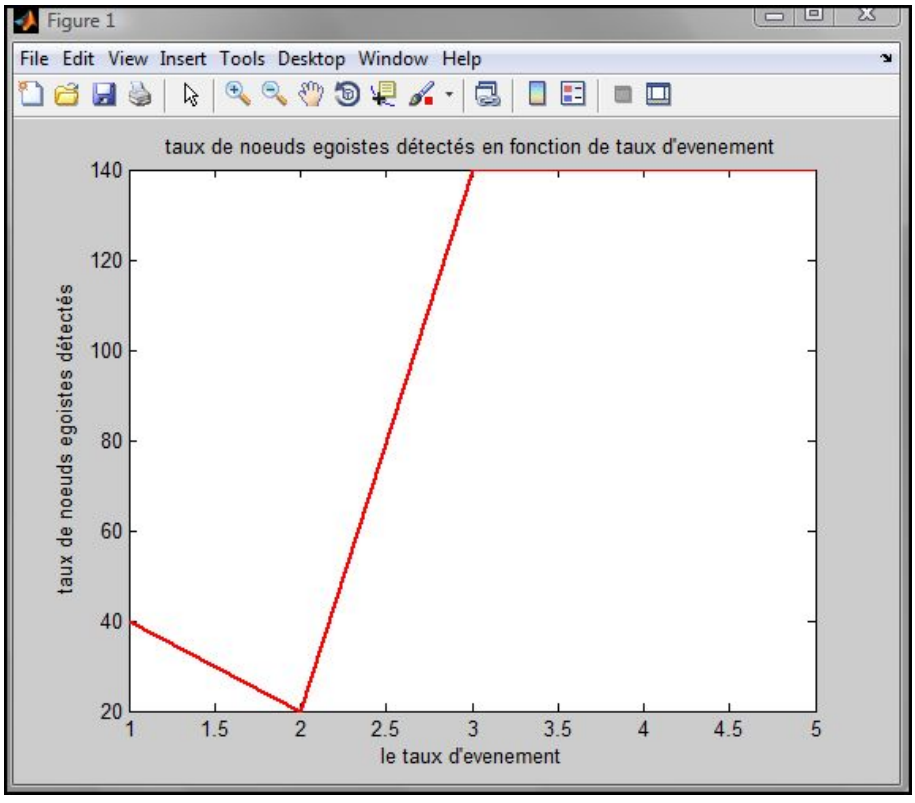

FIGURE 4.3 – Détection de nœuds égoïste

Cette figure montre l'évolution du taux de détection en fonction de nombre d'événement. Les résultats de cette figure montrent un taux de détection important durant certain événement après avoir été égal à 0.

2. Les nœuds égoïstes élus comme des managers

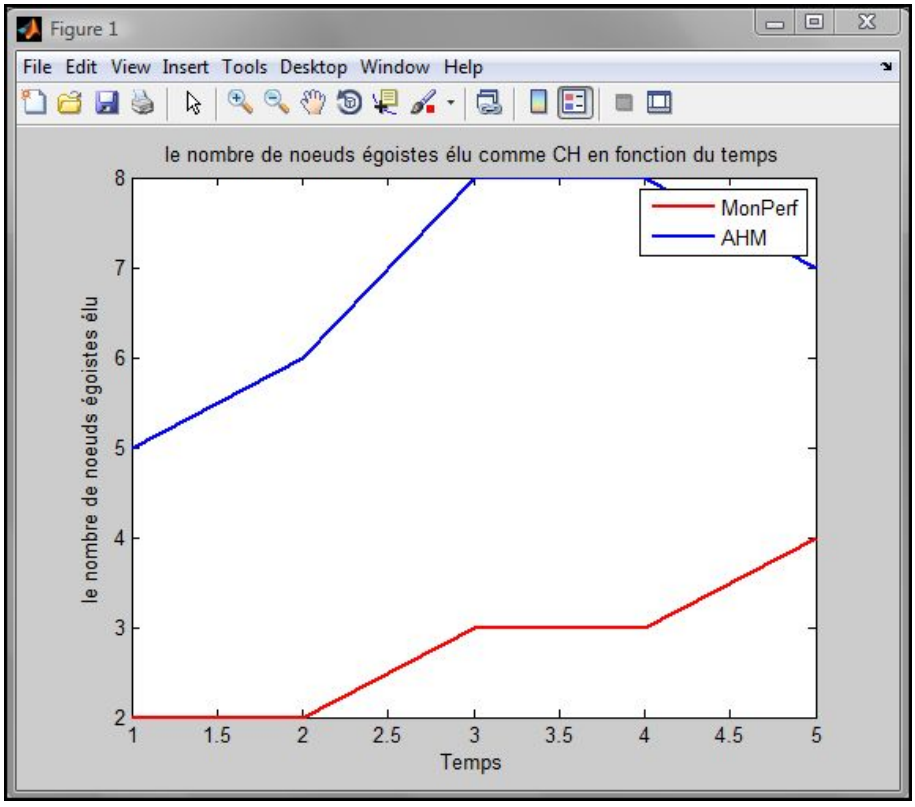

FIGURE 4.4 – Les nœuds égoistes élus comme des managers

La figure ci-dessus représante le nombre de nœuds égoistes élus comme clustr-head en fonction de temps.

Dans cette figure, nous avons comparé notre approche à l'approche HMA Pour pouvoir analyser les performances des fonctionalités des gestionnaire.

Les résultats obtenus montre que notre approche diminue le nombre de managers égoistes. Contrairement à HMA qui présente un nombre croissant de gestionnaire égoistes.

3. Le taux de paquets reçus avec succès

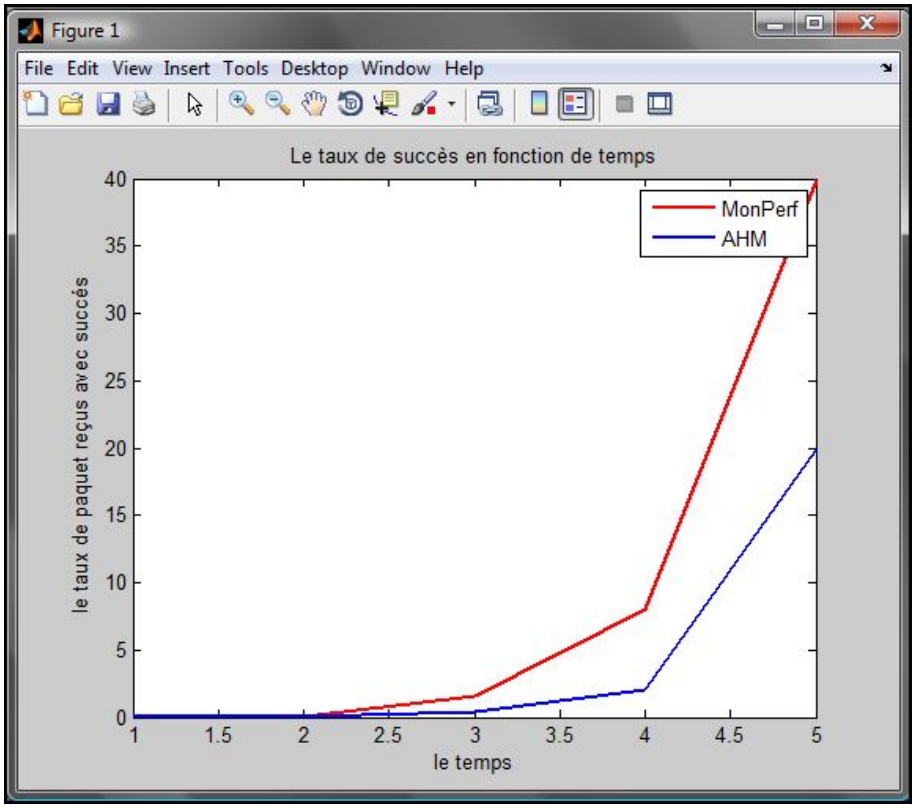

FIGURE 4.5 – Le taux de paquets reçus avec succès

Cette figure illustre le taux de paquets reçus avec succès mesuré en utilisant notre approche comparée à HMA.

D'après la figure, nous constatons que le taux de paquets reçus avec succès est plus important dans notre approche par apport à l'autre. Ceci est interprété par le fait que AHM ne prend pas en considération les nœuds égoïstes ce qui diminue le taux de paquets reçus avec succés.

4. Le taux de perte de paquets

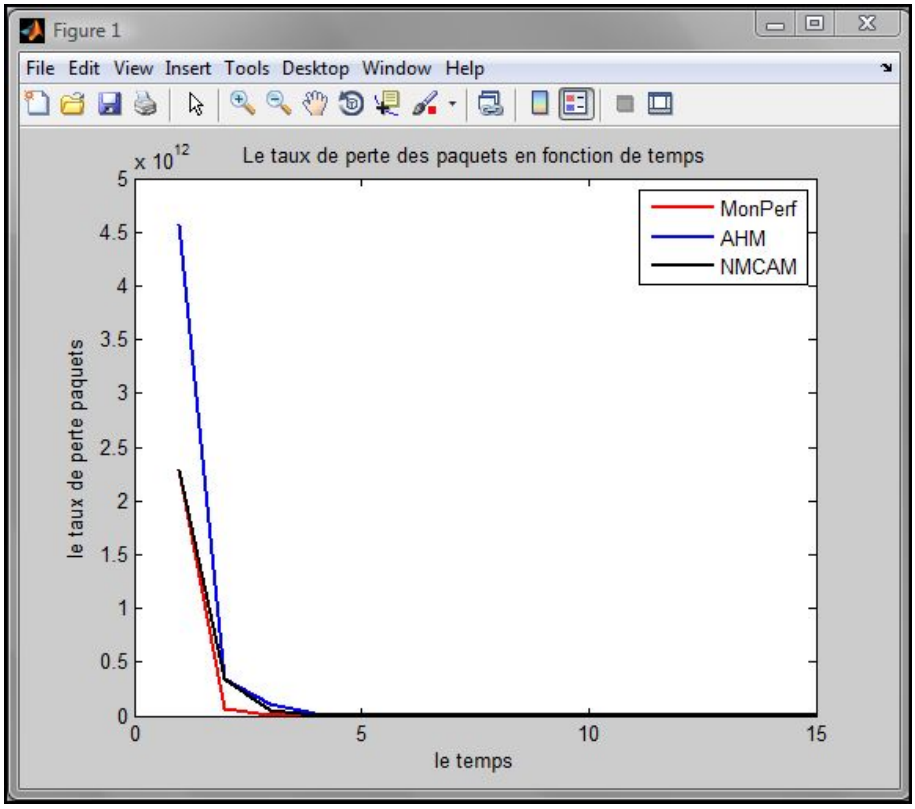

FIGURE 4.6 – Le taux de perte de paquets

Nous avons effectué une comparaison de notre approche par rapport à HMA et NMCAM, en prenant comme critère d'évaluation le taux de perte de paquets, qui est définit comme étant le rapport entre le nombre de paquet non livrés au destination et le nombre de paquets total. Les résultat obtenus (voir la figure 4.6) montre un taux de perte de paquet élevé pour HMA, et qui est diminué pour les deux autres approches. Et cela est interpréter par le fait que notre approche et NMCAM prend en charge la détection des nœuds égoïstes.

4. nombre de CH élus

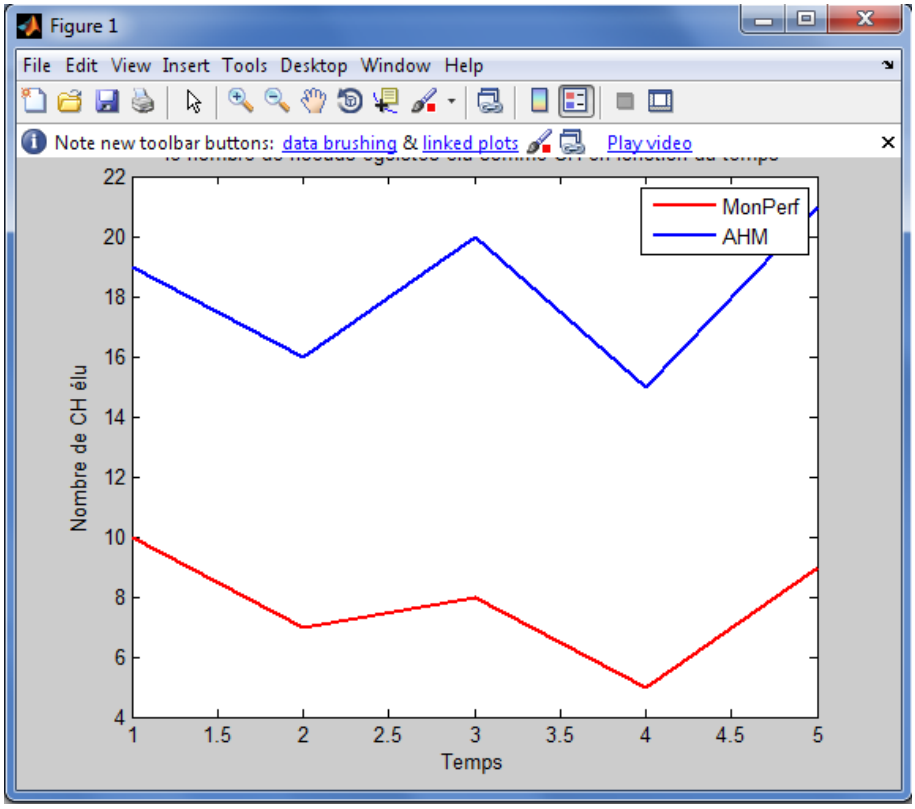

FIGURE 4.7 – Le nombre de CH élus

Cette figure illustre le nombre de gestionnaires élus comme en fonction du temps. D'aprés la figure ci dessus, nous remarquons que le nombre de cluster-head élus dans notres approche est moins que celui de HMA. cela est interprété par le fait que l'algorithme d'élection proposé est à deux sauts.

5. L'énergie consommée

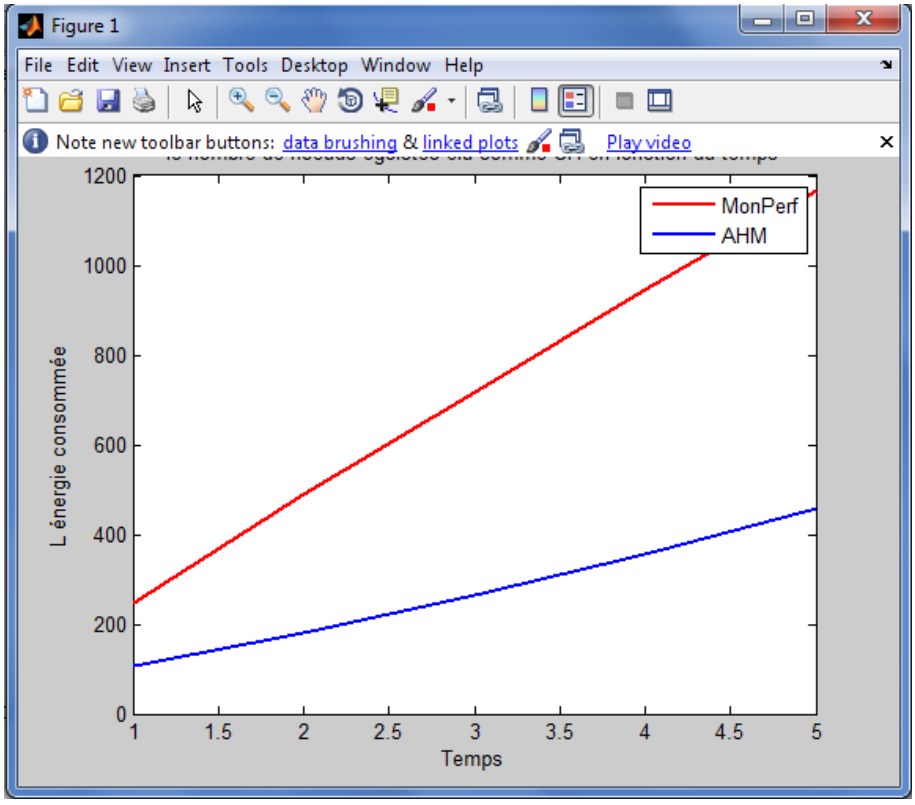

FIGURE 4.8 – l'énergie consommée

Dans cette partie, nous avons effectué une comparaison entre l'énergie consommée par notre approche comparé à AHM. les résultats obtenus montre une consommation d'énergie importante par notre approche par rapport à HMA, et cela est dû au fait que notre algorithme d'élection est à deux sauts contrairement à celui d'HMA qui est à un saut.

4.7 Conclusion

Dans cette partie nous avons évalué les performances de notre approche en la comparant aux deux autres approches HMA et NMCAM. A travers les figures obtenues, nous remarquant bien l'efficacité de la prise en charge de la notion de confiance dans l'élection de gestionnaire.

La solution proposée semble offrir une possibilité réelle pour contrer les nœuds égoïstes et non confiants dans le réseau.

Conclusion générale et perspectives

Ce mémoire traite le problème du monitorage dans les réseaux mobiles ad hoc, il a comme objectif de proposer une nouvelle approche basée sur un modèle de confiance et un algorithme de clustering multicritères.

En premier lieu, nous avons présenté les réseaux sans fils en général et les réseaux ad hoc en particulier. Nous avons cité les caractéristiques de ces derniers et leurs domaines d'application.

En deuxième lieu, nous avons étudié le monitorage dans ce type de réseaux, nous avons cité son utilité et ses difficultés. Par la suite, nous avons énuméré les principales approches existantes dans la littérature, et nous avons achevé cette partie par une étude comparative.

A base de cette étude, nous avons proposé une nouvelle approche pour un monitorage performant des réseaux mobiles ad hoc fondée sur un algorithme de clustering qui prend en considération plusieurs critères pour l'élection d'un gestionnaire (mobilité, énergie, connectivité et confiance). Notre approche comporte, également, un modèle de calcule de confiance des nœuds basée sur le taux d'activité. Elle donne aussi la possibilité de détecter les nœuds égoïstes et non confiant, en se basant sur ces valeurs de confiance.

En perspective, il parait important de comparer notre approche avec d'autres approche de monitorage en considérant d'autres critère d'évaluation et de prendre en considération d'autres paramètres de sélection comme les nœuds malveillants.

Bibliographie

[1] C.Perkins, P.Bhagwat, Highly Dynamic Destination Sequenced Distance Vector Routing (DSDV) for Mobile Computers, ACM SIGCOMM Conference on Communications Architectures, Protocols and Applications, 1994.

[2] W. Chen, N. Jain, S. Singh. ANMP : Ad Hoc Network Management Protocol, IEEE journal on selected areas in communications.1999.

[3]W. Heinzelman, A. Chandrakasan, H. Balakrishman. Energy efficient communication protocol for wireless microsensor networks. proceding of the 33rd hawaii internationelconference on system science. 2000.

[4] N.Badache, D.Djenourf , A. Derhab, T.Lemlouma, Les protocoles de routage dans les réseaux mobiles Ad Hoc, Laboratoire des logiciels de base CERIST, 2002.

[5] N.Beijar, Zone Routing Protocol (ZRP), Networking Laboratory, Helsinki University of Technology P.O. Box 3000, FIN-02015 HUT, Finland, 2002.

[6] T.C. Shen, C. Jaikaeo, C. Srisathapornphat, Z. Huang ,The Guerrilla Management Architecture for Ad hoc Networks, Computer and Information Sciences University of Delaware Newark,2002 .

[7] N.L Chervany et D.H Knight, what trust means in e commerce customer relation ships :an interdisciplinary conceptual typologie, International Journal of Electronic Commerce, 2002.

[8] S. Zhong, J.Chen, Y.R. Yang, Sprite : A Simple, Cheat-Proof, Credit-Based System for Mobile Ad-Hoc Networks, Computer Science Department, Yale University, 2002.

[9] T.Clausen and P.Jacqeut,Optimized Link State Routing Protocol (OLSR), Network Working Group,Project Hipercom, 2003.

[10] D.Ngo ,N.Hassan, J.Wu,WANMON :A Ressource Usage Monitoring Tool for Ad

Hoc Wireless Network,Proceedings of the 28 th Annual IEEE International Conference on Local Computer Network, 2003.

[11] R. Chadha, Y. H. Cheng, J. Chiang, G. Levin, S. W. Li, A. Poylisher, POLICY-BASED MOBILE AD HOC NETWORK MANAGEMENT FOR DRAMA, Telcordia Technologies, One Telcordia Drive, Piscataway NJ 08854.

[12] S. C. Chung, C. Srisathapornphat, L. Rui, H. Zhuochuan, C. Jaikaeo, and E. Lloyd.CLTC, a Cluster-Based Topology Control for Ad-Hoc Networks,IEEE Transaction-son Mobile Computing, 2004.

[13]R. Badonnel, R. State, O. Festor, Management of Mobile Ad-hoc Networks :Evaluating the Network Behavior, MADYNES Research Team, LORIA-INRIA Lorraine.

[14] S.YAHIAOUI,Topologies Dynamiques pour la Découverte de Services dans les Réseaux Ad hoc Peer-to-Peer, mémoire de magistère, Université Abderrahmane Mira de Bejaia, 2005

[15] B.Abderrahmene, Sécurité du routage dans les réseaux mobiles ad hoc, mémoire de magistère, 2005 .

[16] R. Badonnel ,Supervision des réseaux et services ad hoc,Thèse de doctorat, université Henri Poincaré-Nancy, 2006.

[17] R. Badonnel, Radu State, Olivier Festor , Management of Ad-Hoc Networks,MADYNES Research Team, 2006 .

[18] K.CHEBIRA ,Etude et analyse de la stabilité des protocoles de routage dans les réseaux ad-hoc,mémoire de magistère, Université Hadj Lakhdar de Batna, 2007.

[19] B.S.HAGGAR ,Les protocoles de routage dans les réseaux ad hoc,mémoire de magistère, Université de Reims, 2007.

[20] H. Kazemi, G. Hadjichristofi, L. A.DaSilva ,MMAN : A Monitor for Mobile Ad hoc Networks : Design, Implementation, and Experimental Evaluation, 2008.

[21] W. Mallouli, B. Wehbi, A. Cavalli, Distributed Monitoring in Ad Hoc Networks : Conformance and Security Checking, Institut Telecom/Telecom SudParis, 2008.

[22] C. Popi , O. Festor, Monitorage et journalisation dynamiques des topologies dans les réseaux ad-hoc, Research Center, 2008.

[23] Z. Yanping, J. Yuehui, C. Yidong, Q. Xirong, THE REASEARCH OF HIERARCHY MODEL FOR AD HOC NETWORK MONITORING BASED ON CLUSTERING, Beijing University of Posts and Telecommunications, 2009.

[24] M.Frikha,Réseaux ad hoc, routage, qualité de service et optimisation, Lavoisier, 2010.

[25] R. AOUDJIT, Répartiton et équilibrage de charges dans les hôtes mobiles, thèse de Doctorat, université Mouloud Mammeri de Tizi Ouzou, 2010.

[26] M. AYARI, Z. MOVAHEDI, G. PUJOLLE, F. KAMOUN, ADMA : Autonomous Decentralized Management Architecture for MANETs -A Simple Self-Configuring Case Study, Guy PUJOLLE LIP6, University of Paris-VI, CRISTAL lab, National School of Computer Sciences, University of Manouba, 2010.

[27] S. Ghannay, S. M. Gammar, F. Kamoun, The Monitoring of Ad Hoc Networks Based on Routing, CRISTAL Laboratory ENSI,2010.

[28] M.Claire, S.LARAFA,Services AAA dans les réseaux ad hoc mobiles, thèse de Doctorat, l'école doctorale S-I, SudParis, 2011.

[29] S. El brak, M. Bouhorma, A.A. Boudhir, Network Management Architecture Approaches Designed for Mobile Ad hoc Networks, International Journal of Computer Applications (0975 - 8887) Volume 15- No.6, 2011.

[30] K. Gopalakrishnan, V. Rhymend Uthariaraj, Neighborhood Monitoring Based Collaborative Alert Mechanism to Thwart the Misbehaving Nodes in Mobile Ad Hoc Net-

works, European Journal of Scientific Research ISSN, 2011.

[31] B. AIT-SALEM, Sécurisation des Réseaux Ad hoc : Systèmes de Confiance et de Détection de Répliques, thèse de Doctorat, université de LIMOGES, 2011

[32] A. RACHEDI, Contributions à la sécurité dans les réseaux mobiles ad Hoc,thèse de Doctorat,Université d'Avignon et des Pays de Vaucluse, 2012.

[33] y.Al-Sbou, A Novel Quality of Service Monitoring for Mobile Ad Hoc Networks, Départaient of Computer Engineering, Mu'tah Umversity,,2012.

[34]N. Sadoui, S. Heddar, Monitorage avec qualité de service des réseaux mobiles ad hoc, mémoire de master, Université Abderrahmane MIRA-Bejaia,2013.