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

Université A. Mira de Béjaïa
Faculté des Sciences Exactes
Département d'Informatique

MÉMOIRE DE FIN D'ÉTUDE

En vue de l'Obtention du Diplôme de Master Recherche en Informatique

THÈME

MONITORAGE SÉCURISÉ POUR LES RÉSEAUX MOBILES AD HOC

Réalisé par :

M^{lle} : AIT – OUAZZOUG Nadia
M^{lle} : MEDJAHED Sabrina

Soutenu devant le jury composé de :

Président :	M^{me}	ALOUI	Soraya	U.A/Mira BEJAIA
Encadreur :	M^{lle}	BATTAT	Nadia	U.A/Mira BEJAIA
Examinateur :	M	SAADI	Mustapha	U.A/Mira BEJAIA

Promotion 2015

REMERCIEMENTS

En premier lieu, nous remercions Dieu qui nous a procuré ce succès, et qui nous a donné le courage et la volonté pour accomplir ce modeste travail.

Nos sincères remerciements s'adressent à notre promotrice Melle battat Nadia d'avoir accepter de nous encadré, pour sa disponibilité, son suivi, et ses critiques constructives.

Nos remerciements vont également aux membres de jury pour l'honneur qu'ils nous ont fait en acceptant d'evaluer ce modeste travail.

Nous présentons nos remerciements à tous ceux qui ont aidés de prés ou de loin, chacun à sa manière dans la réalisation de ce travail.

TABLE DES MATIÈRES

TABLE DES FIGURES

LISTE DES TABLEAUX

LISTE DES ABRÉVIATIONS

ADMA	:	Autonomous Decentralized Management Architecture for MANETs
ANMP	:	Ad hoc Network Management Protocol
AODV	:	AdhOc Distance Vector
CBA	:	Case-Based Agents
CBR	:	A General Case-Based Reasoning System
DAMON	:	A Distributed Architecture for Monitoring Multi-hop Mobile Networks
DARPA	:	The Defense Advanced Research Projects Agency
DPA	:	Domain Policy Agent
DSDV	:	Destination Sequence Distance Vector
DSR	:	Dynamic Source Routing
EDRAMA	:	Extension of Dynamic Re-Addressing and Management for the Army
ELB ACTD	:	Extending the Littoral Battle-space Advanced Concept Technology Demonstration
ETSI	:	European Telecommunications Standards Institute
hiperLAN	:	HIgh Performance Radio LAN
HMA	:	Hierarchy Model for Ad hoc Network Monitoring Based on Clustering
HomeRF	:	HomeRadio Frequency
IDS	:	Intrusion Detection System
IEEE	:	Institute of Electrical and Electronics Engineers
GPA	:	Global Policy Agent
GPS	:	Global Positioning System
GUI	:	Graphique User Interface
LACM	:	Level-based Access Control Model
LPA	:	Local Policy Agent

LPDP	:	Local Policy Decision Point
LPR	:	Low-cost Packet Radio
MANET	:	Mobile ad hoc Network
MBCR	:	Minimum Battery Cost Routing
MMAN	:	Monitor for Mobile Ad hoc Networks
MMBCR	:	Min-Max Battery Cost Routing
MMWN	:	Multimedia Mobile Wireless Network de GTE Internetworking
MPRs	:	MultiPoint Relays
MIB	:	Management Information Base
MIS	:	Maximal Independent Set
NMCAM	:	Neighborhood Monitoring Based Collaborative Alert Mechanism to Thwart the Mis
OLSR	:	Optimized Link State Routing
OLSRM	:	Optimized Link State Routing Protocol monitoring
PEP	:	Policy Enforcement Point
PRNet	:	projet Packet Radio Network
QOSMA	:	A Quality of Service MONITORING AGENT IN MOBILE AD-HOC NETWORKS
QOSMI	:	Quality of Service Monitoring for Mobile Ad hoc Network
SCN	:	Survivable Communication Network
SURAN	:	le Survivable Radio Networks
TDD	:	time dependent digests
TID	:	time Independent Digests
VBB	:	Virtuel BackBones
WANMON	:	A Resource Usage Monitoring Tool for Ad Hoc Wireless Networks
WING	:	Wireless Internet Gateways
WLAN	:	Wireless Local Area Networks projet Packet Radio Network

INTRODUCTION GÉNÉRALE

L'évolution dans le domaine de la communication sans fil et l'informatique mobile gagne de plus en plus de popularité, et les unités mobiles deviennent de plus en plus fréquentes (laptops, téléphone...) ceci a permis l'apparition des réseaux mobiles ad-hoc qui représentent une composante de cette évolution et leurs fondements seront inévitablement intégrés au générations futures de réseaux sans-infrastructure , ces réseaux auto-organisés sont formés spontanément a partir d'un ensemble d'entités mobiles communicantes, sans nécessiter d'infrastructure, les entités mobiles constituent en elles-mêmes le réseau. Elles peuvent être de formes variées présentent par conséquent des capacités non homogènes en termes de communication, de puissance de calcul et de stockage,elles sont libres de se déplacer de manière aléatoire et de s'organiser arbitrairement, si bien que la topologie du réseau est fortement dynamique dans le temps et dans l'espace, bien que ces caractéristiques soient parmi des avantages de réseaux ads-hoc, elles présentent également des défis dans la surveillance et la gestion, c'est pourquoi un certain nombre d'outils sont nécessaires pour que ces réseaux s'adaptent aux nouveaux besoins de sécurité ,dans notre mémoire nous intéressons à un de ces outils qui est le monitorage .

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 des ressources ainsi que ses performances, et son niveau de sécurité, les contraintes spécifiques des réseaux mobiles ad hoc et leurs vulnérabilités rendent la réalisation du processus de monitorage délicate donc une approche de monitorage pour les réseaux ad-hoc doit être capable de prendre en compte leurs nature dynamique et leurs ressources limitées et particulièrement les problèmes de sécurité puisque le processus de monitorage lui-même est vulnérable aux attaques ,de se fait il est très utile de prendre en compte le niveau de sécurité des nœuds lors de l'élection des moniteur puisque la vulnérabilité de moniteur peut perturber

tous le fonctionnement de réseau et non pas seulement le processus de monitorage et les effets pervers sont catastrophiques dans les domaine sensible ou à temps réel par exemple une fausse politique de moniteur dans le domaine militaire peut causer l'attaque d'un partenaire au lieu d'attaquer un ennemi.

Dans ce mémoire nous avons proposé une nouvelle approche de monitorage sécurisé pour les réseaux ad-hoc permet la détection de tout comportement malveillant ou égoïste d'un moniteur après son élection, nous avons aussi proposé pour cette approche une nouvelle topologie pour le monitorage qui améliore les topologies existantes en terme de sécurité et de performances.
Notre mémoire est structuré de la façon suivante :

Le premier chapitre donne un aperçu général sur les réseaux mobile ad hoc, présente ses caractéristiques, ses applications et ces différentes technologies, Nous discuterons également le principe de routage dans ce type de réseau.

Le deuxième chapitre est consacré à définir le concept de monitorage dans le réseau ad hoc ainsi son processus et ces difficultés, nous présenterons également les différentes approches de monitorage dédiés aux réseaux mobiles ad hoc en citons pour chacune son but de gestion, ensuite nous citerons les critères pour évaluer ces approches. Par la suite, nous présenterons une étude comparative de ces approches en ce basant sur les critères définis.

Le troisième chapitre offre une analyse détaillée des approches présentées dans le chapitre 2 qui garantient un niveau de sécurité, en détaillons pour chacune ses services et ses mécanismes de sécurité que nous allons tous d'abord rappeler, finalement nous présenterons notre proposition qui est élaborée d'après cette analyse et en détaillons son principe et ses déférentes étapes ainsi notre nouvelle topologie qui sera comparée avec deux autres topologies(les clusters et le CDS) qui seront aussi présentées.

Dans le dernier chapitre, nous présenterons la simulation de notre solution pour la sécurisation de monitorage dans les réseaux mobiles ad hoc et nous implémenterons notre proposition sur la nouvelle topologie et sur le CDS afin de les comparer , dans ce chapitre nous détaillerons les étapes de simulation et nous discuterons les résultats obtenus.

En fin, notre mémoire s'achève par une conclusion générale résumant les grands points qui ont été abordés dans ce mémoire, ainsi que des perspectives.

CHAPITRE 1

GÉNÉRALITÉS SUR LES RÉSEAUX MOBILES AD HOC

1.1 Introduction

Les réseaux sans-fil connaissent un engouement saisissant,leurs flexibilité d'utilisation a fait que de tels réseaux ont été rapidement adoptés. Durant la dernière décennie, un nouveau type de réseau sans fil a suscité un grand intérêt auprès de la communauté scientifique, il s'agit des réseaux mobiles ad hoc.

Dans le présent chapitre, nous allons commencer par introduire le concept de réseau mobile ad-hoc et nous allons citer ses différentes applications, puis nous présenterons ses caractéristiques et ses technologies et dans la dernière partie nous intéresserons au routage.

1.2 Réseaux mobiles ad hoc

Avant de définir les réseaux mobiles ad hoc nous commencerons d'abord par un historique de la communication sans fil.

1.2.1 Historique de la communication sans fil

La première forme de réseaux sans infrastructure remonte aux années 1970 avec le projet DARPA PRNET (Packet Radio Network). L'objectif consistait à mettre au point un système de communication multi-sauts sans fil dans le cadre d'applications militaires.

Le système était capable de s'auto-organiser sans le support d'une infrastructure fixe, à travers la détection de la connectivité radio et l'établissement de stratégies de routage. Une extension de ces travaux de recherche ont abouti au projet DARPA SURAN (Survival Radio Network) qui visait à expérimenter des équipements de taille plus réduite et à définir des protocoles robustes offrant une meilleure tolérance aux fautes ainsi qu'un meilleur passage à l'échelle. La commercialisation des premiers réseaux ad-hoc s'est faite discrètement à travers le développement du Bluetooth . Initialement proposée par Ericsson en 1994, puis reprise dans le cadre du groupe d'intérêt Bluetooth SIG regroupant différents industriels majeurs tels qu'IBM, Microsoft et Motorola, cette technologie permet de transmettre des données entre des équipements périphériques sur une faible distance avec une moindre consommation électrique. Elle peut ainsi former des réseaux particuliers appelés scatternet qui requièrent l'utilisation de protocoles de routage multi-sauts. La nécessité de développer des standards ouverts a conduit à la création du groupe de travail MANET (Mobile Ad-Hoc Networks) de l'IETF (Internet Engineering Task Force) en 1998. Ce groupe est chargé de standardiser les protocoles de routage IP unicast pour les réseaux ad-hoc. La lenteur du processus de normalisation a abouti à une standardisation relativement tardive des protocoles de routage[1].

1.2.2 Définition d'un réseau mobile ad hoc

Un réseau mobile ad hoc, appelé généralement MANET (Mobile ad hoc NETwork), consiste en une grande population, relativement dense, d'unités mobiles qui se déplacent dans un territoire quelconque et dont le seul moyen de communication est l'utilisation des interfaces sans fil, sans l'aide d'une infrastructure préexistante ou administration centralisée ,Un réseau Ad-Hoc est une collection de périphériques équipés d'une technologie de transmission sans fil et doté de protocoles permettant la mise en réseaux de ceux-ci. La particularité de ce type de réseau est que chaque nœud peut communiquer avec n'importe quel autre nœud du réseau. En effet, si un nœud A veut communiquer avec un nœud B qui n'est pas a porter radio, alors il passera par une série de nœuds intermédiaires qui joueront le rôle de relais entre la source et la destination[2].

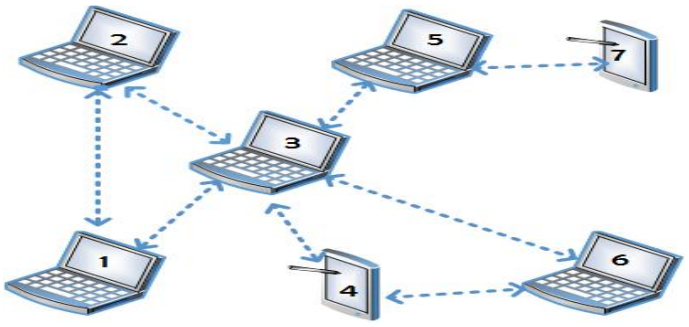

FIGURE 1.1 – Modélisation d'un réseau mobile ad hoc.

1.2.3 Applications des réseaux mobiles ad hoc

Les réseaux mobiles Ad hoc ont réussi à s'imposer en tant que technologie prometteuse. Leurs caractéristiques et en particulier la mobilité et l'absence d'infrastructure élargissent leurs domaines d'application.

Applications militaires : Les réseaux mobiles Ad hoc sont conçus à la base pour des applications et des opérations à caractère militaire. Ces réseaux sont adaptés aux environnements hostiles, car ils sont dynamiques et rapidement déplorables. Les nœuds du réseau ne sont que des équipements militaires communiquant : soldats, véhicules blindés, . . .etc Cependant, l'application de ces réseaux a dépassé le domaine militaire grâce au développement technologique des réseaux sans fil tel que le Bluetooth.

Opérations de sauvetage : Les réseaux mobiles Ad hoc sont aussi utilisés lors des opérations de sauvetage, notamment lors de 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.

Domaine commercial : Les réseaux mobiles Ad hoc peuvent étendre un réseau avec infrastructure pour offrir un service tel que l'accès à Internet à moindre coût. De plus, ils permettent de relier plusieurs ordinateurs entre eux pour partager des fichiers, des jeux, la tenue des réunions, la communication entre agents, . . .etc 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

Réseau d'entreprise : La facilité à déployer ces réseaux et leur coût réduit intéressent 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[3].

1.2.4 Caractéristiques et contraintes des réseaux ad hoc

Les réseaux mobiles ad hoc possèdent des caractéristiques particulières que nous citons dans ce qui suit :

La topologie dynamique : Les réseaux mobiles ad hoc se caractérisent par la mobilité des nœuds. En effet, ces derniers sont libres de se déplacer d'une manière aléatoire. A tout moment, de nouveaux nœuds peuvent joindre le réseau ou le quitter donc, la topologie du réseau peut changer rapidement à des instants imprévisibles. La figure 1.2 présente un exemple illustratif du changement de la topologie suite à la mobilité des nœuds ainsi, les techniques de routage des réseaux classiques basées sur des routes préétablies ne peuvent plus fonctionner correctement.

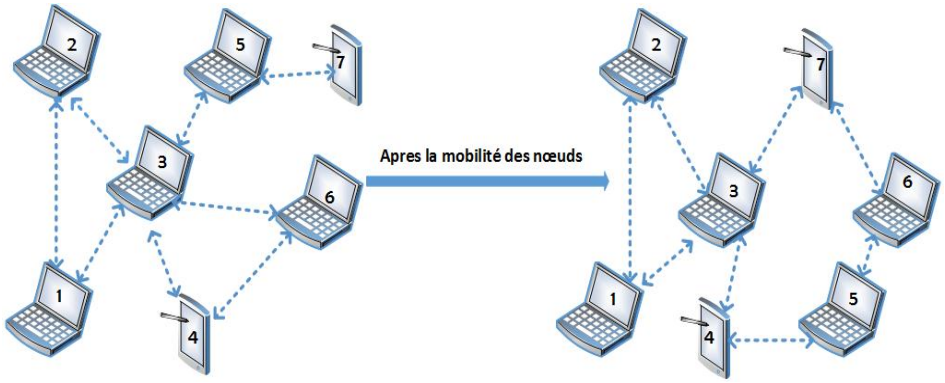

FIGURE 1.2 – Topologie dynamique.

L'absence d'infrastructure : Les réseaux mobiles ad hoc sont formés spontanément à partir des neouds mobiles. Ils se distinguent des autres réseaux par la propriété d'absence d'infrastructure fixe ou préexistante et de tout genre d'administration centrale. Ainsi, les neouds mobiles sont responsables d'établir la connectivité et de la maintenir d'une manière continue. Ils peuvent donc être facilement déployés.

La bande passante limitée : Les réseaux mobiles ad hoc sont basés sur les technologies de la communication sans fil. En effet, les nœuds utilisent un support sans fil pour communiquer entre eux. Ils partagent ainsi le même média lors des échanges d'informations. De ce fait, ce partage fait que la bande passante réservée à un nœud est modeste.

Les contraintes d'énergie : La consommation d'énergie constitue un problème important pour les nœuds dont leur alimentation se repose sur des sources d'énergie autonomes comme les batteries. En effet, la durée de vie des différents nœuds est

fortement liée à la durée de vie limitée de leurs batteries. De ce fait, le paramètre d'énergie doit être pris en considération dans tout contrôle effectué par le système.

L'équivalence des nœuds du réseau : Dans le contexte des réseaux mobiles ad hoc, tous les nœuds sont capables d'assurer des fonctions de routage. Contrairement aux réseaux classiques, les routeurs présentent le seul moyen capable de prendre en charge l'acheminement des informations.

L'hétérogénéité des nœuds : Les réseaux mobiles ad hoc sont formés par un ensemble de nœuds hétérogènes ayant des capacités différentes. En effet, un nœud peut être équipé d'une ou plusieurs interfaces radio ayant des capacités de transmission variées. Cette hétérogénéité de capacité peut engendrer des liens asymétriques dans le réseau. De plus, les nœuds peuvent avoir des différences en termes de capacité de traitement (mémoire, CPU).

La sécurité limitée : Les réseaux sans fil mobiles sont généralement plus sensibles aux problèmes de sécurité. En effet, n'importe quel nœud peut faire partie du réseau juste en se plaçant dans une zone de propagation, où il pourra écouter tout ce qui se passe par le médium physique. De ce fait, ce type de réseau pose un problème lié à la confidentialité ce qui réduit d'avantage la sécurité[4].

1.2.5 Technologies de réseaux mobiles ad hoc

1.2.5.1 IEEE 802.11

Cette norme concerne la transmission radio et la transmission infrarouge. Elle a pour but de définir des normes sans fil permettant l'interopérabilité entre produits de différents constructeurs Le protocole 802.11 de l'Institute of Electrical and Electronics Engineers (IEEE), parfois nommé Wi-Fi, définit plusieurs couches physiques et une couche d'accès au medium pour les réseaux locaux sans fil (Wireless Local Area Networks - WLAN) . Dans sa première version définie en 1997, les transmissions infrarouges étaient envisagées. Les versions les plus récentes du standard telles que IEEE 802.11b pour un débit partagé de 11Mbps, IEEE 802.11g avec un débit de 22Mbps ou encore IEEE 802.11a pour un débit de 56 Mbps sur la base desquelles sont construites l'essentiel des cartes d'interface commercialisées, s'adressent principalement à des transmissions radio fréquences[5].

1.2.5.2 HiperLAN

HiperLAN (HIgh Performance Radio LAN), norme européenne élaborée par l'ETSI (European Telecommunications Standards Institute), permet d'obtenir un débit théorique de 54 Mbps sur une zone d'une centaine de mètres dans la gamme de fréquence comprise entre 5150 et 5300 MHz[6].

1.2.5.3 Bluetooth

La norme Bluetooth a été conçue pour présenter une faible consommation et permettre de réduire le coût de conception des communications sans fil à courte distance. Originalement conçue comme une alternative aux liaisons câblées, le Bluetooth est utilisé pour connecter différents types d'équipements comme les périphériques informatiques tels que souris et clavier, ou bien audio (écouteur sans fil).

La norme Bluetooth exploite les fréquences ISM 2.4 GHz et utilise 79 canaux présentant une bande passante de 1MHz. La portée du Bluetooth est de 10 m environ. En augmentant la puissance d'émission, la portée peut atteindre 100 m [7].

1.2.5.4 Zigbee

Beaucoup moins connue aujourd'hui que Bluetooth, ZigBee est une norme de transmission de données sans fil permettant la communication de machine a machine. Sa très faible consommation électrique et son faible cout ouvre la voie à des applications domotiques également. ZigBee, utilisant les couches MAC et PHY du standard de communication IEEE 802.15.4, est le prolongement de la norme HomeRF (HomeRadio Frequency) qui a, depuis son lancement en 1998, et dépassée par Wifi. Les débits autorises sont relativement faibles, entre 20 et 250 Kbits/s, mais sa très faible consommation énergétique en fait son atout principal. ZigBee fonctionne dans le monde entier sur la bande de fréquences des 2,4 GHz et sur 16 canaux. Sa portée est de plusieurs dizaines de mètres. Un réseau ZigBee peut contenir jusqu'à 254 nœuds par cellule en plus d'un nœud qui en assure la gestion, nommé coordinateur. Le protocole ZigBee est optimisé pour permettre une durée de vie de plusieurs mois à plusieurs années aux dispositifs alimentés par batterie. La pile protocolaire est suffisamment petite pour tenir dans la mémoire interne d'un microcontrôleur actuel (quelques dizaines de KOctets)[8].

1.3 Routage dans les réseaux mobiles ad hoc

Le routage est une méthode d'acheminement des informations à la bonne destination à travers un réseau de connexion donné. Le problème de routage consiste à déterminer un acheminement optimal des paquets à travers le réseau au sens d'un certain critère de performance. Le problème consiste à trouver l'investissement de moindre coût en capacités nominales et de réserves qui assure le routage du trafic nominal et garantit sa survabilité en cas de n'importe quelle panne d'arc ou de nœud,la classification des protocoles de routage est illustrée dans la figure suivante :

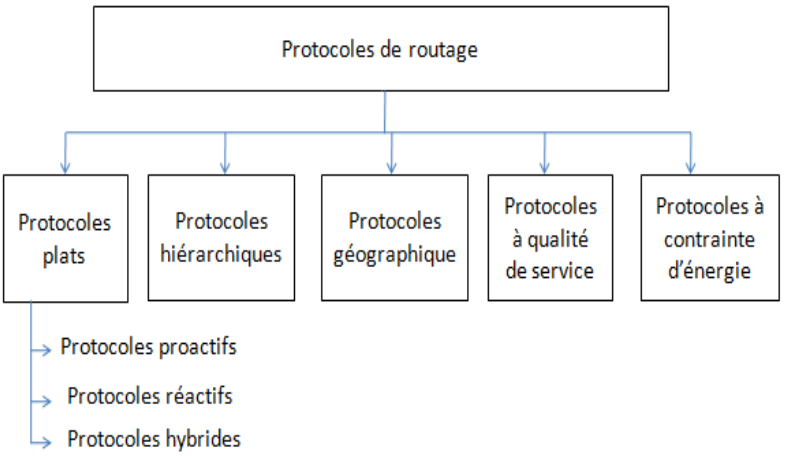

FIGURE 1.3 – Protocoles de routage.

1.3.1 Protocoles plats

De nombreux protocoles de routage ont été proposés. Dans l'approche proactive, chaque nœud connaît une route vers n'importe quel nœud du réseau. Si chaque nœud envoi un paquet de topologie dans tout le réseau de façon périodique, l'over Head induit est élevé et une tempête d'inondation risque d'apparaître. DSDV est donc basé sur l'algorithme de Bellman-Ford et n'échange pas des paquets de topologie qu'avec ses voisins radios. OLSR optimise la diffusion des paquets de topologie via un sous-ensemble de nœuds chargés de relayer seuls les inondations. Les protocoles proactifs optimisent les délais de livraison mais engendrent un overHead important. A l'opposé, le réactif crée des routes à la demande. Un nœud initie une découverte de route lorsqu'il doit envoyer un paquet et qu'il ne connaît aucune route vers la destination. DSR envoi un message Route Request inondé dans le réseau, accumulant dans le paquet les adresses des nœuds relais. Lorsque la destination reçoit le Route Request, elle renvoie un Route Reply sur la route inverse contenue dans le paquet. La source peut donc mettre en cache la nouvelle route et commencer à envoyer ses paquets de données. Lorsque cette route n'est plus valide, une nouvelle découverte est initiée. Une telle approche permet d'optimiser la taille mémoire allouée à la table de routage, et présente un Overhead réduit lorsqu'un nœud ne possède qu'un nombre réduit de correspondant, changeant peu au cours du temps. Par contre, les délais d'établissement de route peuvent être longs, ce qui peut être problématique pour des applications multimédia. AODV propose une approche similaire, mais en maintenant des tables de routage distribuées, supprimant le routage par la source[9].

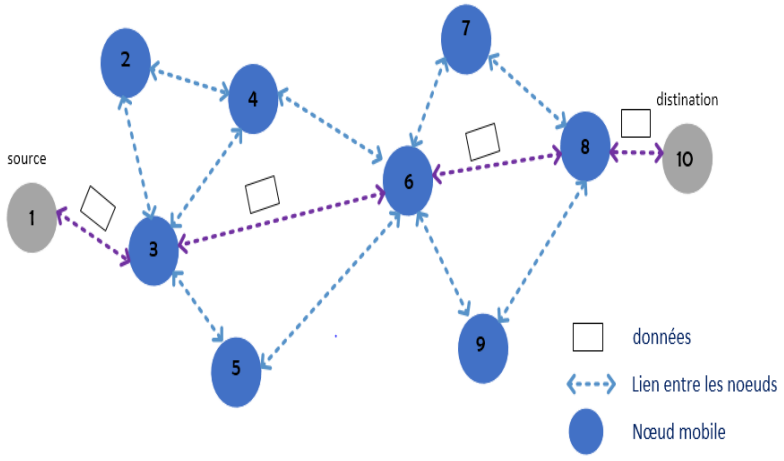

FIGURE 1.4 – Routage plats.

1.3.1.1 Protocoles proactifs

Le principe de base des protocoles proactifs est de maintenir a jour les tables de routage, de sorte que lorsqu'une application désire envoyer un paquet à un autre mobile, une route soit immédiatement connue. Dans le contexte des réseaux mobiles ad-hoc les nœuds peuvent apparaitre ou disparaitre de manière aléatoire et la topologie même du réseau peut changer ; cela signifie qu'il va falloir un échange continuel d'informations pour que chaque nœud ait une image à jour du réseau. Les tables sont donc maintenues grâce à des paquets de contrôle, et il est possible d'y trouver directement et à tout moment un chemin vers les destinations connues en fonctions de divers critères. On peut par exemple privilégier les routes comportant peu de sauts, celles qui offrent la meilleure bande passante, ou encore celles de délai est le plus faible. L'avantage premier de ce type de protocole est d'avoir les routes immédiatement disponibles quand les applications en ont besoin, mais cela se fait au coût d'échanges réguliers de messages (consommation de bande passante) qui ne sont certainement pas tous nécessaires (seules certaines routes seront utilisées par les applications en général)[9].

1.3.1.2 Protocoles réactifs

Le principe des protocoles réactifs est de ne rien faire tant qu'une application ne demande pas explicitement d'envoyer un paquet vers un nœud distant. Cela permet d'économiser de la bande passante et de l'énergie. Lorsqu'un paquet 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). L'avantage majeur de cette méthode est qu'elle ne génère pas du trafic de contrôle que lorsqu'il est nécessaire. Les principales contreparties sont que l'inondation est un mécanisme coûteux qui va faire intervenir tous les nœuds du réseau en très peu de temps et qu'il va y avoir un délai à l´établissement des routes[9].

1.3.1.3 Protocoles hybrides

Les protocoles hybrides combinent les approches réactives et proactives. Le principe est de connaitre notre voisinage de manière proactive jusqu'à une certaine distance (par exemple trois ou quatre sauts), et si jamais une application cherche à envoyer quelque chose à un nœud qui n'est pas dans cette zone, d'effectuer une recherche réactive à l'extérieur. Avec ce système, on dispose immédiatement des routes dans notre voisinage proche, et lorsque la recherche doit être étendue plus loin, elle en est optimisée (un nœud 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, et sinon il va propager de manière optimisée la demande hors de sa zone proactive). Selon le type de trafic et des routes demandées, ce type de protocole hybride peut cependant combiner les désavantages des deux méthodes : échange de paquets de contrôle réguliers et inondation de l'ensemble de réseau pour chercher une route vers un nœud éloigné[9].

1.3.2 Protocoles hiérarchiques

Fonctionnent en confiant aux mobiles des rôles différents qui varient les uns des autres. Certains nœuds sont élus et assument des fonctions particulières qui conduisent à une vision en plusieurs niveaux de la topologie du réseau. Par exemple, un mobile pourra servir de passerelle pour un certain nombre de nœuds qui lui seront attachés. Le routage sera simplifié, puisqu'il se fera de passerelle à passerelle, jusqu'à celle directement attachée au destinataire. Un exemple est donné sur la figure 1.5 où le nœud N3 passe par les passerelles F1, F2 et F3 pour atteindre N9. Dans ce type de protocoles, les passerelles supportent la majeure partie de la charge du routage (les mobiles qui s'y rattachent savent que si le destinataire n'est pas dans leur voisinage direct, il suffit d'envoyer le trafic à la passerelle qui se débrouillera)[9].

.

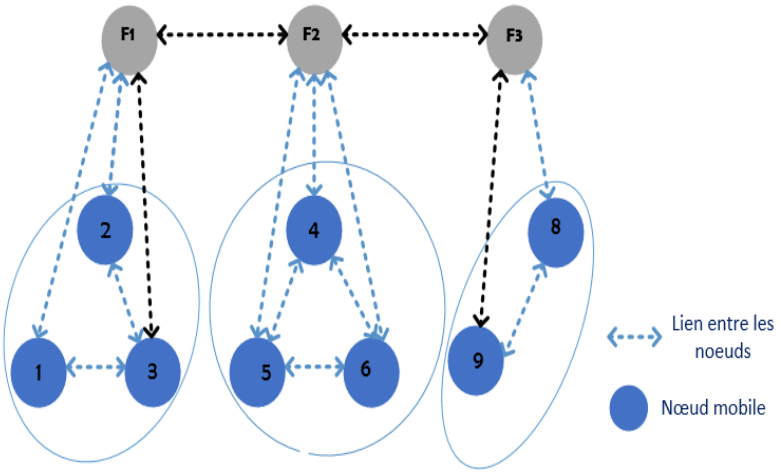

FIGURE 1.5 – Routage hiérarchique.

1.3.3 Protocoles géographiques

Le routage géographique sont entendus comme toute solution ou fonction qui permet de positionner, de localiser et de produire des informations géographiques liées aux nœuds dans un réseau mobile, afin d'augmenter l'efficacité de la procédure de découverte d'itinéraires. Les protocoles géographiques répondent à certaines limitations des protocoles basés sur la topologie en utilisant des informations supplémentaires qui concernent les positions géographiques des nœuds. Plus précisément, les changements fréquents de la topologie, conséquence de la mobilité des nœuds, implique de grands problèmes de passage à l'échelle des protocoles de routage traditionnels, basés sur l'utilisation de la topologie. Dans ces protocoles, chaque nœud a seulement besoin de connaître les coordonnées géographiques de ses voisins immédiats et du nœud destinataire pour prendre une décision d'acheminement des paquets. Chaque nœud peut déterminer sa propre position grâce à l'utilisation des données GPS ou d'un autre système de positionnement[10].

1.3.4 Protocoles à qualité de service

Dans le domaine des réseaux, la notion de qualités de services ou QoS (Quality of Service) est évoqué pour désigner la capacité du réseau à fournir un service : transfert de données par exemple. La performance d'un réseau est un élément fondamental et nécessaire pour l'utilisation d'applications, notamment les applications au temps réels. Les protocoles de l'internet subissent des fortes pressions pour offrir des garanties de qualité de service. Ces demandes proviennent des applications multimédias réparties. Ces applications exigent un transfert de données complexe telles que la téléphonie, la vidéo à la demande ou la conférence multimédia. La QoS au niveau d'un réseau se décline en

quatre paramètres : débit, latence, la gigue et la perte. Le routage au mieux consiste souvent à rechercher le plus court chemin en terme de distance entre une source et une destination afin de transférer des données. Dans le cas du routage avec qualité de service, le but n'est pas simplement de trouver le meilleur chemin selon un certain critère mais de trouver le meilleur chemin admissible. Pour cela, un certain nombre de contraintes sur les routes sont imposées afin de déterminer leur éligibilité. Par exemple, on peut vouloir rechercher une route disposant d'une certaine quantité de bande passante pour un trafic vidéo ou une route assurant que les paquets seront reçus par la destination moins d'un certain temps après leur émission par la source. Toute route satisfaisant un certain critère quantitatif peut être qualifiée de route assurant une certaine qualité de service[5].

1.3.5 Protocoles à contrainte d'énergie

Les Protocoles de routage à contrainte d'énergie reposent sur un calcul de métrique prenant en compte l'état de l'énergie disponible sur un nœud. Nous présentons trois exemples d'adaptation de ce type de routage :

- Le premier exemple, Minimum Battery Cost Routing (MBCR), calcule sa métrique à partir de l'information locale au nœud : sa puissance disponible. La route choisie est celle qui a un coût Ri minimal parmi toutes les routes possibles. Avec ce critère de sélection la route choisie peut passer par des équipements ayant beaucoup de batteries alors que certains équipements auront une batterie très faible qui sera épuisée.
- Le second exemple, Min-Max Battery Cost Routing (MMBCR), utilise a même information mais nécessite une vue globale pour faire son adaptation : le choix d'une route se fait en ayant la connaissance de l'énergie disponible sur tous les nœuds. Le coût d'une route est défini à partir de la capacité disponible minimale sur les nœuds qui la composent. L'objectif est alors d'éviter la route avec les nœuds ayant le moins de capacité parmi tous les nœuds dans toutes les routes possibles.
- Le troisième exemple, utilise une métrique dont le calcul repose sur deux informations : la puissance disponible également l'état du canal. C'est l'état du canal qui permet de calculer l'énergie nécessaire à la transmission[11].

1.4 Conclusion

Dans ce chapitre nous avons donné en premier lieu un aperçu général sur la communication sans fil et particulièrement sur les réseaux mobiles ad-hoc et ses applications ainsi ses caractéristiques et contraintes, puis nous avons cité les différentes technologies du réseau

mobile ad-hoc, et nous avons aussi détaillé les différents protocoles de routage.

CHAPITRE 2

MONITORAGE DES RÉSEAUX MOBILES AD HOC

2.1 Introduction

La taille des réseaux ne cessant de grandir de jour en jour et l'importance de ceux-ci dans le monde prenne une place prépondérante, le besoin de contrôler en temps réel leurs qualité et leurs état est rapidement devenu une priorité. C'est dans ce but qu'est apparu il y a maintenant une trentaine d'années ,le concept de supervision de réseaux.

Nous présenterons dans ce chapitre ce qu'est la supervision de réseaux et nous détaillerons le monitorage qui l'accomplit, cela en définissant son processus et en citant ses buts et ses techniques ensuite nous expliquerons les différentes approches de monitorage existantes avec une étude comparative en ce basant sur des critères bien définies.

2.2 Supervision des réseaux

La supervision réseau a pour but de surveiller le bon fonctionnement des réseaux. Ce concept est né au début des années 1980, lors de l'explosion de la mise en place de réseaux informatiques dans les entreprises. La taille grandissante de ceux-ci ainsi que leur hétérogénéité posaient un réel problème de gestion et d'administration, multipliant les besoins en main d'œuvre d'experts administrateurs. C'est donc à cette époque qu'ont été menées les premières réflexions sur un nouveau concept, celui de la supervision.

La supervision devait être capable de s'adapter à des milieux hétérogènes, d'automatiser le contrôle des réseaux et de générer un ensemble de statistiques donnant une meilleure vision du réseau, permettant par la-même d'anticiper les besoins de celui-ci. La supervision peut ainsi se définir comme étant l'utilisation de ressources réseaux adaptées (matérielles ou logicielles) afin d'obtenir des informations sur l'utilisation et sur l'état des réseaux et de leurs composants (logiciels, matériels). Ces informations peuvent alors servir d'outils pour gérer de manière optimale (automatique si possible) le traitement des pannes ainsi que la qualité des réseaux (problèmes de surcharge). Elles permettent également de prévoir toute futur évolution nécessaire[12].

2.3 Monitorage des réseaux

Le monitorage est une activité d'observation qui consiste à évaluer l'état opérationnel et le fonctionnement d'un réseau ,dans ce qui suit nous présenterons au premier lieu le processus de cette activité.

2.3.1 Processus de monitorage

La supervision consiste en : la collecte, l'analyse, le stockage des données, et le lancement d'alerte en cas d'anomalies finalement la correction des disfonctionnement trouvé. Les quatre premières étapes constituent le processus de monitorage :

Collecte de données : Cette étape consiste a récupérer les informations (l'adresse ip , le niveau d'énergie, la capacité de stockage, la bande passante) demandées par le gestionnaire.les informations collectées par les équipements individuels permettent d'obtenir une vue de plus haut niveau et de produire une connaissance sur l'environnement complet. cette connaissance est ensuite utilisée par les équipements eux même pour réagir de manière intelligente aux changements [13].

L'analyse de données et le lancement d'alertes en cas d'anomalies : Cette étape consiste à comparer les données collectées à des seuils spécifiques et a étudier le taux d'influence des valeurs de ces données sur le fonctionnement du réseau et ses performances, elle permet aussi de lancer des alertes en cas de présence d'un dépassement de seuil[14].

Le stockage de données : Dans cette étape les données analysées après l'étape de collecte et les rapports de surveillance seront stockées dans des bases de données [14].

2.3.2 Buts de monitorage

Le monitorage est utilisé pour avoir des connaissances qui seront utilisées dans :

Gestion des performances : Le monitorage permet le suivi et l'évolution des moyens de communication grâce aux informations collectées sur les services et les propriétés des nœuds et leurs comportements dans le réseaux par exemple la détection des nœuds égoïstes qui aura un impact direct sur les performances de réseau.

Gestion des fautes : Grace au détail collecté ; le monitorage permet de détecter les anomalies qui affectent le fonctionnement du réseau afin de les corriger dans un temps très bref pour assurer la continuité de service ou un fonctionnement en mode dégradé.

Configuration de réseau : La configuration de réseau permet l'initialisation et l'arrêt du réseau ainsi la maintenance et la mise a jour, elle consiste aussi à définir les liaisons entre les nœuds de réseau grâce aux connaissances fournies par le monitorage, nous pouvons arriver à configurer de manière optimale.

Assurer la sécurité : Grace aux informations collectées le contrôle d'accès aux ressources sera plus facile ainsi l'accès aux services offert cela en définissant les moyens de sécurisation comme le cryptage et décryptage, ses informations permettent aussi la détection des intrusions et des nœuds malveillant qui est très important pour la sécurité[15].

2.3.3 Difficultés du monitorage des réseaux ad hoc

Les réseaux mobiles Ad hoc sont confrontés à de nombreux problèmes liés à leurs caractéristiques qui rendent les solutions de sécurité développées pour les réseaux filaires ou sans fil avec infrastructure inapplicables dans le contexte des réseaux mobiles Ad hoc.
Parmi les vulnérabilités qui touchent les réseaux mobiles Ad hoc nous pouvons citer :

L'absence d'infrastructure : les réseaux mobiles Ad-hoc sont des réseaux sans infrastructure fixe. Ceci ne nous permet pas d'opter pour une architecture centralisée. En effet, l'absence d'une unité centralisée accentue le défi pour proposer une solution de sécurité comme c'est le cas dans les réseaux filaires ou sans fil avec infrastructure fixe. Cependant, une architecture centralisée est déconseillée dans les réseaux mobiles Ad hoc, car elle peut créer un point de vulnérabilité dans le réseau.

La topologie réseau dynamique : parmi les caractéristiques des réseaux mobiles Ad hoc, on trouve l'environnement dynamique, qui est dû à la mobilité des nœuds. Cette caractéristique nécessite le développement de protocoles de routage sophistiqués et

de solutions de sécurité adaptées à un tel environnement, ce qui constitue un vrai défi.

La vulnérabilité des nœuds : les nœuds ne sont pas physiquement protégés, ils peuvent être capturés par des attaquants (l'ennemi), ce qui pose problème au niveau des relations de confiance entre les nœuds. Ainsi, n'importe quel modèle de sécurité dédié au réseau mobile Ad hoc doit prendre en compte la compromission des nœuds, ainsi que la résistance à cette attaque.

La vulnérabilité du canal : le support de transmission est l'air. Ce dernier est très vulnérable aux écoutes clandestines. N'importe quelle machine qui dispose d'une carte sans fil adaptée à la technologie utilisée, est capable de capturer le trafic, de l'analyser et même d'injecter du nouveau trafic, soit dans le but de surcharger le réseau ,soit dans celui de faire circuler des fausses informations pour changer la topologie du réseau. De plus, le canal sans fil est fortement vulnérable au risque de brouillage "jamming", ce qui a des conséquences néfastes sur le réseau.

Les ressources limitées : les nœuds mobiles dans les réseaux mobiles Ad-hoc ont des ressources très limitées, comme la capacité de calcul, de stockage et surtout d'énergie. La batterie ne tient pas longtemps si le nœud travaille sans arrêt, ce qui complique davantage le problème de la sécurité. En effet, nous savons que la plupart des solutions de sécurité sont basées sur la cryptographie, mais malheureusement ce dernier est gourmand en termes de ressources : capacité de calcul, consommation d'énergie et mémoire de stockage. Par conséquent, de nombreux thèmes de recherches ont surgi au cours des dernières années pour remédier à ces vulnérabilités et assurer les services de sécurité dans les réseaux mobiles Ad hoc[3].

2.3.4 Techniques de monitorage

Les chercheurs ont proposé deux techniques de monitorage qui se différent selon le trafic à analyser qui sont :

Monitorage passif : Le monitorage passif consiste à observer le trafic de réseau et le capturer pour évaluer un certain nombre de paramètres sans injecter un trafic spécifique c'est a dire en analysant seulement le trafic du réseau capturer durant les communications et aucun autre type de message n'est ajouté.

Monitorage actif : Le monitorage actif consiste au contraire de monitorage passif à injecter un trafic de contrôle dans un réseau pour vérifier et évaluer certains paramètres liées au fonctionnement et au sécurité[16].

2.4 Approches de monitorage

ANMP (Ad hoc Network Management Protocol) : ANMP [17] est basée sur une architecture centralisée hiérarchiques pour le monitorage des réseaux mobiles ad hoc fondée sur l'utilisation de SNMP comme protocole de gestion dont lequel l'information collectée est représentée d'une façon structurée dans Management Information Base (MIB).

Dans cette approche chaque nœud dans le réseau maintient un MIB et participent dans la construction de clusters et dans le processus d'élection de gestionnaire central comme administrateur pour chaque cluster dans le réseau ; le monitorage est réalisé de la façon suivante :

Chaque agent rassemble un ensemble d'informations telles que la qualité de lien, la localisation et la quantité d'énergie restante. Ces données seront sauvegardées par ces agents dans des MIB (Management Information Base) avant de les envoyer au gestionnaire local. Ce dernier rassemble toutes les informations qui lui sont destinées et les envoie au gestionnaire central correspondant qui les analyse et les stocke dans sa base appelée AnmpMIB, mais L'accès a la base d'informations est sécurisé a travers l'implantation du modèle LACM (Level-based Access Control Model) avec lequel chaque nœud dispose d'une visibilité différente en fonction de son niveau d'accès, dans l'addition, ANMP utilise les multicasts bloqués et le modèle militaire de sécurité, avec l'emploi des alarmes qui sont déclenchées lors de détection des anomalies.

Cette approche génère un trafic additionnel important en empoilant beaucoup de messages dans les étapes de monitorage ce que diminuera la largeur de la bande disponible.

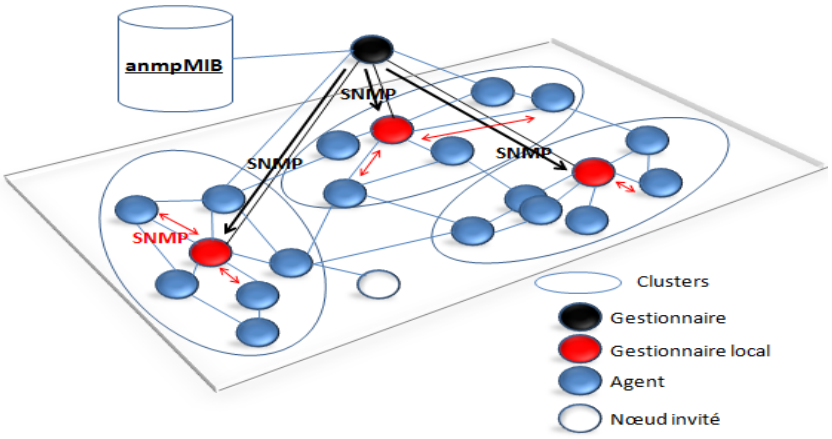

FIGURE 2.1 – Architecture ANMP.

CBA-IDS (Case-Based Agents for Packet-Level Intrusion Detection in Ad Hoc Networks) : Dans cette approche[18] un système modulaire réparti de détection d'intrusion qui utilise le moteur de raisonnement basé sur des cas (a general case-based reasoning system (CBR) est proposé mais La base de données pour le moteur de CBR est distribuée sur chaque nœud du réseau mobile ad-hoc sans fil.

Le composant le plus important du système CBR est l'archive des cas où les problèmes précédemment expérimentés sont stockés avec leurs solutions,chaque entrée dans ces archives s'appelle un "cas" qui contient les dispositifs décrivant le problème, et la mesure ou les actions qui ont été prises pour résoudre le problème. Quand un problème est détecté dans l'environnement, il est formulé puis le module de CBR qui assigne une valeur de similitude pour chaque cas comparé et les cas retournés sont rangés selon leurs degrés de similitude au problème donné ,à ce moment deux scénarios différents sont possibles : soit certains des cas choisis sont décidés comme solution au problème ou soit un nouveau cas est formulé pour résoudre le problème, ce système modulaire d'identification est basé sur les agents mobiles intelligents pour la surveillance de réseau, les nœuds de tête de cluster accueillant ces agents qui surveillent des paquets envoyés par chaque membre de son cluster ainsi le réseau entier est surveillé.

Quand des paquets sont capturés, ils sont insérés dans une file d'attente puis les paquets sont alors retirés de la file d'attente et traités par le moteur de raisonnement qui vérifie l'information de paquet (adresses de réseau, ports et contenu de charge utile) par rapport à l'ensemble des cas archivés et si une similitude est détectée ,une alerte sera expédiée à l'agent de prise de décision situé sur les mêmes nœuds que les agents surveillants et c'est a lui de décider avec une certaine confiance qu'un nœud est malveillant ,Quand un certain niveau de menace est atteint pour un nœud en

question, l'agent de décision expédie une commande qu'une action doit être prise par les agents locaux sur ce nœud.

Cette approche est lourde pour s'exécuté en temps réel a cause de nombreuse opérations pour la détection et génère des fausses alertes causées par sa sensibilité qui n'est pas adaptée pour le réseau mobile ad hoc qui est complètement sans fil.

GUERRILLA : C'est une approche[19] basée sur la gestion individuelle, L' architecture de GUERILLA fournit la continuité de gestion avec l'utilisation de deux rangés la première se compose de groupes de directeurs nomades ce qui possèdent l'intelligence de gestion, ils prennent leurs propres décisions et collaborent de façon autonome pour contrôler le réseau mobile ad-hoc entier sans aide de toute entité externe ;cela s'adapte au réseau dynamique, La rangée inférieure se compose de sondes actives (manuscrits programmables) qui peut être expédié aux nœuds à distance pour exécuter les opérations localisées de gestion et aussi pour rassembler l'information de gestion de ces nœuds.

Les directeurs nomades et les sondes actives facilitent des opérations de gestion et réduire la consommation de la largeur de bande sans fil.

Cette approche assure la consommation minimale de bande passante grâce à l'utilisation des sondes actives et les directeurs nomades, puisque un directeur nomade peut décider de publier une sonde active pour s'accorder le contrôlé entre les nœuds. Cette sonde exécute comme tâche la gestion par l'interaction avec l'agent local de SNMP donc une utilisation économique de la largeur de bande sans fil limitée en éliminant le besoin du vote mais elle n'offre aucun service de sécurité.

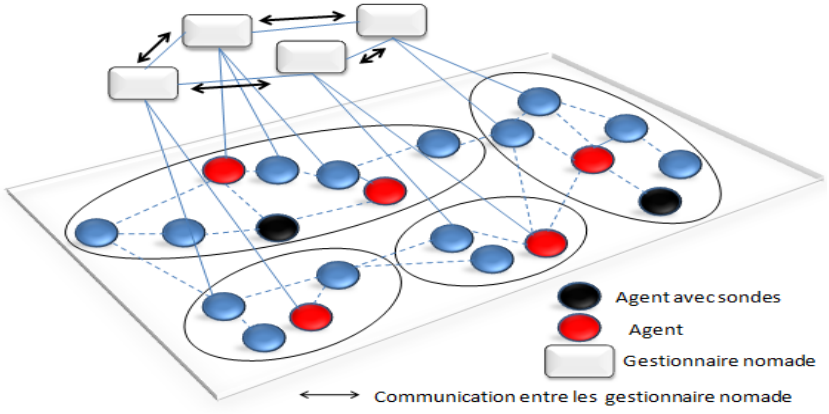

FIGURE 2.2 – La gestion individuelle avec la plate forme GUERILLA.

WANMON(A Resource Usage Monitoring Tool for Ad Hoc Wireless Networks) :
Cette approche [20] permet de collecter des informations sur l'utilisation des ressources, l'utilisation de la bande passante, la consommation d'énergie et sur l'occupation de la mémoire cela est assuré grâce a l'utilisation des agents, Chaque agent déployé sur un nœud sera responsable de déterminer statiquement le cout du routage en terme de trafic de consommation d'énergie l'occupation de la mémoire et la charge CPU, en particulier, il vise à distinguer les ressources consommées par le nœud lui-même et les ressources consommées par l'activité de routage au nom d'autre nœud ; cette consommation peut être évaluée à partir des traces réseaux obtenues à l'aide d'un analyseur de trafic.
Cette approche est centralisé et ne permet pas d'avoir des informations en temps réel et aussi ne permet pas d'avoir une vue global du réseau et elle n'offre aucun mécanisme de sécurité.

OLSRM (Optimized Link State Routing Protocol monitoring) : Cette approche[21] est basée sur le protocole de routage OLSR, le concept principal utilisé dans le protocole OLSRM est identique a celui de OLSR qui est l'utilisation d'un groupe de nœuds choisis par la diffusion des messages de contrôle de topologie nommés MPRs (MultiPoint Relays) cela permet de collecter un ensemble de données de la manière suivante :
des nouveaux champs sont inclus dans les messages HELLO(respectivement TC'Topologie Contole') tel que le délai entre deux nœuds, la consommation de la batterie et la qualité de trafic et aussi les données échangées via les messages HELLO (respectivement TC) seront stockés dans les tables des voisins et les tables de MPRs (respectivement dans les tables de topologie).
OLSRM fournit des améliorations significatives en terme de conservation de batterie et de la bande passante d'après la simulation dans [21] parce qu'il n'utilise aucun nouveau message mais elle ne fournit aucun service de sécurité.

DAMON(A Distributed Architecture for Monitoring Multi-hop Mobile Networks) :
DAMON [22] est un système de surveillance basé sur une architecture distribuée pour surveiller le réseau mobile,il emploie des agents dans le réseau pour surveiller et envoyer l'information à un ensemble distribué de centre de dépôts qui stockent l'information surveillée et il exige le protocole du cheminement de vecteur de distance (AODV),la fonctionnalité de dépôt peut être distribué parmi plusieurs nœud

qui sont de façon optimal non-mobile ou moins mobile comparé à d'autres nœuds.
Le monitorage est réalisé de la façon suivante :
Les agents surveillent et collectent des informations de monitorage pour les envoyer au centre de dépôts ou elles seront stocker dans le cas de disparition d'un centre dépôt (a cause de la mobilité) l'agent choisi un autre centre de dépôt et lui envoi les données collectées.il effectue la collecte de deux types de données les données dépendantes de Temps embraquées dans TDDs (time dependent digests) et donnée indépendantes de temps embraquée dans TIDs (time Independent Digests) les TDDs et TIDs qui sont livrées au centre de dépôt a l'aide de protocole de routage.
DAMON définit une solution robuste adaptée à la mobilité des équipements ad-hoc en permettant l'auto-d´ecouverte des centres de dépôts par les agents ainsi que la résistance aux pannes de ces centres .

MMAN (Monitor for Mobile Ad hoc Networks) MMAN [23] est une approche distribuée de monitorage des réseaux mobile 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 nœud de gestion.
Chaque nœud de surveillance (MU) comporte trois composants indépendants :

Un composant de capture : il est déployé sur les MUs à traversé 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'informations (Info Files).

Un composant de la livraison da 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 (Graphique User Interface) : il permet d'analyse le contenu des dossiers d'information, les agrégées et produire des résultats finals,ces résultats sont utilisées pour la détection des nœuds égoïstes.

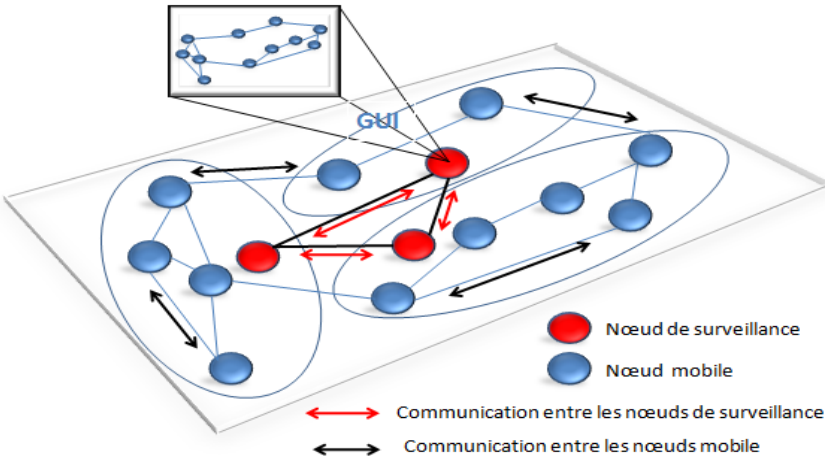

FIGURE 2.3 – Collaboration entre les MUs pour maintenir une vue de la topologie du réseau.

DIST-MONIT (Distributed Monitoring in Ad Hoc Networks) : Dans cette approche[24] une méthodologie formelle pour rassembler et analyser la trace de trafic de réseau est proposée dans la quelle chaque nœud de réseau rassemble sa trace locale de trafic, ces traces seront envoyées a un observateur global qui est responsable des tâches de corrélation et d'analyse de ces traces. La corrélation exécutée est basé sur un protocole précis de la synchronisation conçu pour réseaux mobiles ad hoc pour formé une trace global, l'analyse consiste à vérifier si la traces sont conforment à un ensemble de fonctionnel et aux propriétés de sécurité de protocole de routage. Une fois qu'une violation de propriété est détectée, Une identification de nœud irrégulier qui est derrière cette violation est effectuée.

JOUR -DYNAM (JOURNALISATION DYNAMIQUE DE TOPOLOGIE) :
Cette approche [25] permet le monitorage de topologie pour des réseaux mobiles ad-hoc d'une manière distribuée, basé sur des tables de hachage distribuées, le système stocke l'information topologique recueillie par les clients mobiles puisque chaque nœud a la responsabilité de rassembler l'information de voisinage à des intervalles de temps discrets (des slots de temps).

Les instantanés de la topologie sont pris pour chaque slot de temps et sont stockés de manière distribuée, les enregistrements topologiques obtenus par chaque nœud

et pour chaque slot sont stockés dans la DHT recouvrant l'ensemble des nœuds contrôlés.

Le système peut alors être interrogé à tout moment pour connaître la topologie dans n'importe quel slot de temps de l'historique par un ou plusieurs gestionnaires auprès de n'importe quel nœud du réseau.

HMA (Hierarchy Model for Ad hoc Network Monitoring Based on Clustering) :

HMA [26] est basée sur le principe de la division de réseau mobile ad hoc en plusieurs domaines, chacun d'eux se compose d'un nœud moniteur et des nœuds membre, le nœud de moniteur contrôle ses nœuds membre par l'intermédiaire de mécanisme adaptatif, HMA fournit un nouveau mécanisme pour choisir les nœuds appropriés à agir en tant que nœuds moniteur en considérant le degré d'un nœud mobile, le niveau d'énergie, la mobilité et la capacité de la transmission. Elle consiste en :

- Chaque nœud calcule sa métrique 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 nœud dans chaque cluster doit être compris entre une limite supérieure U et une borne inferieur L.

-lorsque le nombre de membres du cluster est inferieur à la limite inferieur L, ce cluster doit essayer de se fusionner avec un cluster voisin.

-lorsque le nombre de membres du cluster est plus que la limite supérieur U , cluster doit être scindé en deux clusters.

EDRAMA (Managing Network Security Policies in Tactical MANETs Using DRAMA) : Prolongation de DRAMA [27](Dynamic Re-Addressing and Management for the Army) qui est réalisée par les agents de politique qui sont organisés dans une hiérarchie ; au niveau le plus élevé se trouve l'agent global de politique ou GPA(Global Policy Agent) qui contrôle plusieurs agents de politique de domaine ou DPAs(Domain Policy Agent),ces derniers gèrent plusieurs agents locaux de politique LPAs(Local Policy Agent).

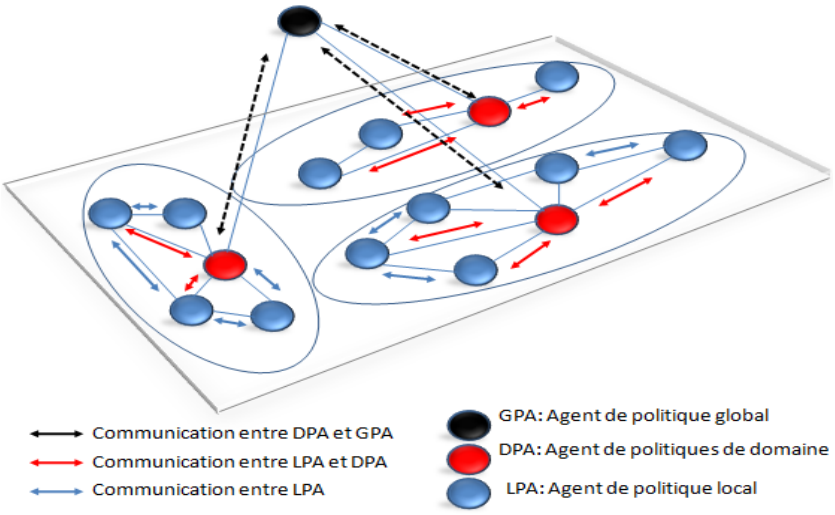

FIGURE 2.4 – L'architecture DRAMA.

EDRAMA[28] permet la définition des politiques de sécurité qui sont créés et distribués par l'agent global de politique et sont signés avec la clef privée du GPA et puis distribués à d'autres nœuds et tous les messages échangés sont signés et afin d'éviter des comportements malveillants EDRAMA emploi également des systèmes de détection d'intrusion (IDSs) et permet le contrôle d'accès en authentifiant les nœuds du réseau.

Cette approche offre plusieurs avantages concernant la sécurité en la comparant à DRAMA mais elle est centralisée.

ADMA(Autonomous Decentralized Management Architecture for MANETs) :

Cette approche [29] est basée sur une architecture de gestion distribuée qui permet aux nœuds du réseau mobile ad hoc de se configurer automatiquement et de s'adapter au changement dans un environnement en introduisant un degré d'autonomie au processus de gestion de réseau.

Un nœud d'ADMA se compose de quatre éléments de base qui sont :

– **LPDP (Point De Décision Local De Politique)** : Le LPDP est l'entité qui prend des décisions et régit à la gestion de ressource et la configuration de nœud. À la différence de l'utilisation traditionnelle du point de décision de politique (PDP) dans la commande d'admission, la décision de LPDP n'est pas prise en réponse aux demandes envoyées d'un utilisateur voulant accéder à une ressource, elle est plutôt basée sur des politiques appropriées prédéfinies d'ailleurs, le LPDP agit en

tant qu'autorité finale pour la décision qui doit être imposée et ne se rapporte pas à n'importe quelle entité haut-centrale de prise de décision.

- **Moniteur** : Le moniteur est le composant qui rassemble les informations de surveillance et les rapporte au LPDP, l'information rassemblée peut être locale (c.-à-d., relié à l'état de nœud) ou externe (c.-à-d., rassemblé des moniteurs et des sondes externes), ils seront stockés dans une base de données spécifique locale.
- **PEP (Point D'Application De Politique)** : Le PEP est l'élément qui impose des politiques et des décisions de LPDP. Il est également responsable de traduire des décisions et des buts de niveau élevé aux politiques de niveau bas.
- **Dépôt Local De Politique** : Le dépôt local de politique est une base de données locale où des politiques sont stockées d'une manière structurée.

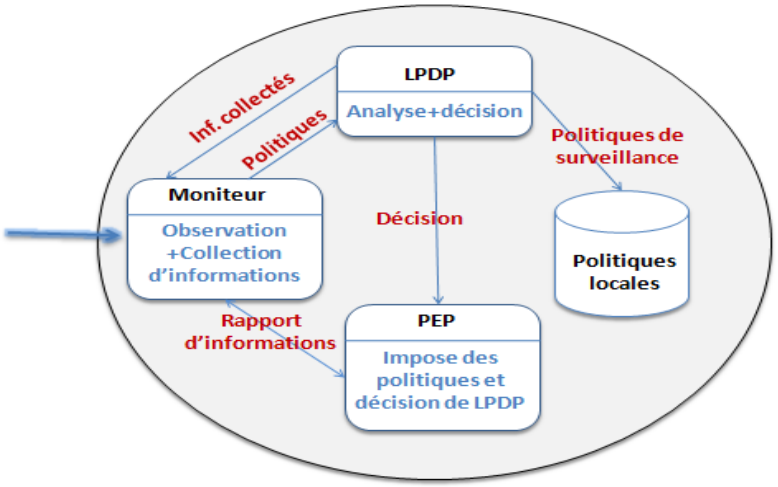

FIGURE 2.5 – Architecture d'un nœud ADMA.

NMCAM (Neighborhood Monitoring Based Collaborative Alert Mechanism to Thwart the Misbehaving Nodes in Mobile Ad Hoc Networks) : NMCAM [30] est une approche de monitorage basée sur le mécanisme de réputation pour la détection des nœuds qui se comportent mal dans le réseau, ce système est composé de trois composants principaux qui sont :

- **Le moniteur** : C'est un nœud responsable de l'écoute de 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 qui ne contiennent pas des nœuds conduisant mal,cela est considéré comme adjonction à la fonctionnalité dynamique existante du protocole de routage (DSR) grâce a l'aide d'un composant interne appelé le directeur de confiance basé sur

les événements rapportés par le moniteur, ce dernier enregistre un événement positif à la faveur d'un nœud si ce nœud réussi à acheminer un paquet vers la bonne destination et un événement négatif dans le cas contraire en fonction de ces événements le directeur de confiance attribut des valeurs de confiance aux nœuds de réseau.

Les cinq types des nœuds qui se conduisent mal dans les réseaux ads-hoc et qui sont détectés par NMCAM sont :

1. **Type 1** : Ces nœuds participent dans le routage mais aussi expédient des paquets de données au nom d'autres nœuds.
2. **Type 2** : Ces nœuds ne participent pas dans le routage. Ils emploient leurs énergies pour la transmission de leurs propres paquets seulement.
3. **Type 3** : Ces nœuds se comportent différemment à base de leurs énergies. Quand l'énergie se trouve entre l'énergie initiale E i et un seuil T 1, le nœud se comporte correctement. Mais si elle se trouve entre T 1 et un seuil inférieur différent T 2 alors elle se comporte comme un nœud de type 1 et pour une force inférieure à T 2, il se comporte comme un nœud du type 2.
4. **Type 4** : Ces nœuds modifient le paquet expédié au nom d'autres nœuds.
5. **Type 5** :Ce type de nœuds change son adresse (MAC/IP) afin d'accéder au ressources de réseau.

Le résultat de simulation [30] prouve que la perte de paquet a été réduite. Il montre efficacité du système proposé dans le choix de plus court et mieux chemin sans contenir des nœuds conduisant mal donc NMCAM permet la détection des nœud égoïstes et les nœuds malveillants mais aucun mécanisme d'authentification est discuté et même les donnée échangés sont pas chiffrées comme la table qui contient la liste des nœuds égoïstes et malveillants.

QOSMI (A Novel Quality of Service Monitoring for Mobile Ad hoc Network) :

QOSMI [31] est une approche distribuée hiérarchique pour le monitorage de qualité de service (QoS) dans les réseaux mobile ad hoc, elle se base sur les nœuds qui se caractérisent par leurs stabilité qui forme un ensemble nommé MIS (Maximal Independent Set) pour construire des nœuds VBB-QoS (Virtuel BackBone- QoS) en les reliant entre eux (se connecter) cela permet de former un domaine comportant des nœuds dominants (MIS) et des nœud dominés ainsi chaque dominateur forme un faisceau avec un ensemble des nœuds dominée. Une fois que des faisceaux sont établis, chaque nœud dominé est responsable de mesurer les paramètres de

QoS et les transmettre à son nœud dominant avec un message unicast, ces valeurs rassemblées sont évalués par le nœud dominant en utilisant un système de logique de flux qui produit finalement les résultats sous forme d'une variable linguistique (pauvre, moyen, bon) pour évalué la QoS.

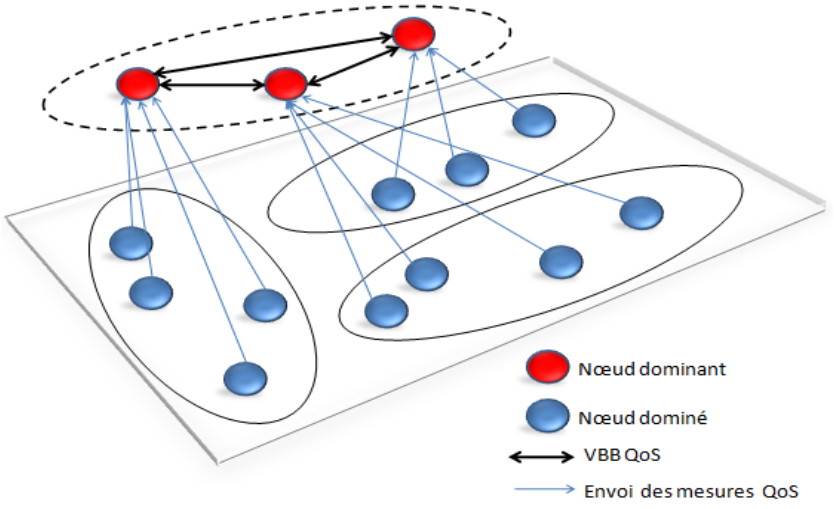

FIGURE 2.6 – Architecture de QoSMI.

QOSMA (ROUTING AND RESOURCE ALLOCATION USING QOS MONITORING AGENT IN MOBILE AD-HOC NETWORKS) : Dans cette approche [32] des agents surveillant la QoS vérifie la largeur de bande disponible et alloue la ressource temporairement pour les nœuds dans le réseau. Pendant la transmission les paquets de données si un lien tombe en panne ou une perte de donnée se produit l'agent surveillant la QoS assigne un chemin pour les nœuds dans le réseau en fournissant QoS. Cela permet d'après les résultats de simulation de réduire la rupture des liens et la perte de paquets de données.

L'agent surveillant QoS envoi les paquets de sonde à partir du nœud de la source par le chemin avec la disponibilité minimum de coût et de largeur de bande. A chaque nœud intermédiaire dans le chemin l'agent surveillant met à jour sa liste avec l'information de nœud telle que son identification, drapeau, niveau de puissance, des informations sur le nœud voisin, il surveille également le niveau de QoS de chaque nœud intermédiaire le long du chemin grâce au faite chaque nœud est responsable d'estimer la largeur de bande disponible sur son lien. Si la contrainte de QoS est violée, alors l'agent de surveillance envoie un avis à la source de sorte que la source

puisse effectuer le contrôle de trafic ou choisir un autre chemin approprié satisfaisant la contrainte de QoS.
Dans cette approche pendant la transmission les paquets de données si un lien tombe en panne ou une perte de donnée se produit l'agent surveillant la QoS assigne un chemin pour les nœuds dans le réseau en fournissant QoS. Cela permet d'après les résultats de simulation [31] de réduire la rupture des liens et la perte de paquets de données. Cette approche permet également une authentification des nœuds voisin et garantit la distribution de la charge de la fonction de monitorage sur l'ensemble des nœuds de réseau et aussi mais les informations collectées ne concernent que la QoS et l'état des liens et aucune information sur la sécurité n'est collectée ou analysée et même les informations collectées sont pas chiffrées.

MA-IDS (A Mobile Agent Approach for IDS in Mobile Ad Hoc Network) : Dans cette approche [33] un nouveau système de détection d'intrusion est proposé, Il est basé sur l'agent mobile qui utilise des algorithmes de classification statistique, ces derniers sont largement automatisés donc ils sont précis.

L'architecture de système se compose de :

Agent Collecteur : L'agent collecteur est le premier agent qui opère dans ce système, il rassemble les données dans le réseau, stocke ces données dans un dossier, qui est donné comme entrée à l'agent de détection d'abus.

Agent de détection d'abus : L'agent de détection d'abus analyse les données capturées par l'agent collecteur. Il détecte les attaques connues dans le réseau par un algorithme, il rapporte une alerte à l'agent d'alerte s'il y a une similitude entre les paquets rassemblés et les signatures d'attaque dans la base de données, si il y'a pas, ces paquets seront comme entrée à l'agent de détection d'anomalie.

Agent De Détection D'Anomalie : L'agent de détection d'anomalie est employé pour détecter des nouvelles attaques inconnues en employant la classification techniques. Si les données entrantes sont détectées comme attaque, il rapport l'agent d'alerte au sujet de l'attaque, et mettre à jour l'attaque détectée dans la base de données.

Agent d'Alerte : L'agent alerte est utilisé pour alerter le système si l'intrusion se produit dans le réseau. Il est basé sur le rapport de l'agent de détection l'anomalie et l'agent de détection d'abus.

Les interactions entre ces déférents agents ainsi la base de donné des attaques est illustrées dans le schéma suivant :

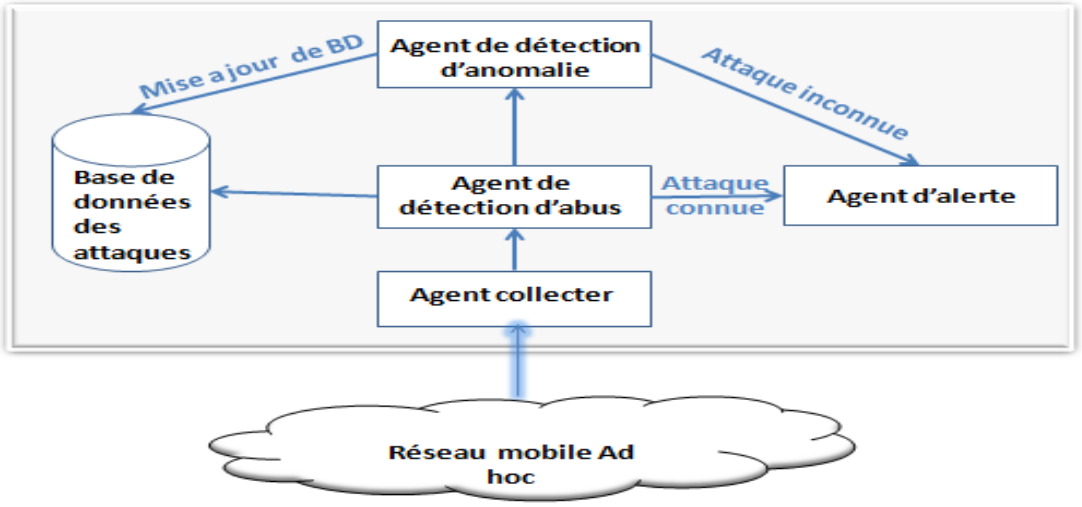

FIGURE 2.7 – Architecture du système MA-IDS.

Avant d'entamer la partie d'analyse nous allons spécifier pour chacune des approches présentées au dessous son objectif de gestion.

.

Approche	**Objectif de gestion**
ANMP[17]1999	Gestion des fautes, configuration Gestion de performance, gestion de sécurité
CBA – IDS[18]2001	Gestion de sécurité
GUERRILLLA[19]2002	Configuration
WANMON[20]2003	Les statistiques
OLSRM[21]2003	Gestion de performance
DAMON[22]2004	Gestion de performance
MMAN[23]2007	Statistique, Gestion de performance
DISTMONIT[24]2008	Gestion de sécurité, gestion des fautes
JOUR – DYNAM[25]2008	Gestion de faute ,Gestion de performance,Configuration
HMA[26]2009	Gestion de performance
EDRAMA[28]2010	Gestion de performance, Gestion de sécurité, configuration
ADMA[29]2010	Configuration, Gestion de performance
NMCAM[30]2011	Gestion de sécurité
QOSMI[31]2012	Gestion de performance
QOSMA[32]2013	Gestion de performance
MA – IDS[33]2014	Gestion de sécurité

TABLE 2.1 – Objectifs des approches de monitorage

2.5 Etude comparative

Dans cette section nous allons effectuer une analyse des approches présentées ici dessus, au premier lieu nous allons expliquer les critères sur lesquels cette analyse ce basera.

2.5.1 Les critères d'évaluation

1. **La non centralisation :** Une approche centralisée repose sur un unique gestionnaire chargé de collecter les données auprès des agents et de contrôler l'ensemble du réseau cette solution n'est adaptée au réseau mobile ad hoc parce que l'ensemble de l'infrastructure s'écoule si le gestionnaire n'est plus opérationnel. D'autre part, elle génère un trafic de gestion important de et vers le gestionnaire car toutes les opérations de monitorage sont opérées par cette unique entité donc une bonne approche de monitorage doit ne pas être centralisée.
2. **La distribution de la charge de traitement :** Une approche de monitorage doit permettre de distribuer la fonction de monitorage entre l'ensemble des nœuds de manière distribuée avec un équilibre équitable de charge sur chaque nœud dans le réseau en prenant en considération les capacités de chacun d'eux.
3. **La distribution de la charge de stockage :** Une bonne approche de monitorage doit garantit la disponibilité des données collectées lors de monitorage a tous les nœuds selon leurs besoins.
4. **La détection des nœuds égoïstes :** Un nœud égoïste est un noeud qui veut profiter du réseau et économise sa propre énergie et profite de routage par les autres donc il ne participe pas a l'élaboration des routes. Donc une bonne approche doit détecter les nœuds égoïstes puisque La présence des ces nœud a comme conséquence la dégradation de l'exécution et des marques de réseau. .
5. **Détection des fautes :** Dans le cadre de la supervision de réseaux, la gestion des fautes est l'ensemble des fonctions qui permettent de détecter, isoler et corriger les erreurs qui affectent le bon fonctionnement de réseau ,donc une bonne approche de monitorage doit permet de détecté ces fautes afin de les corrigé dans un temps très bref.
6. **La robuste aux attaques :** Les réseaux mobiles ad hoc représentent des caractéristiques contraignantes et sont très vulnérables aux attaques comparés aux réseaux filaires ou les réseaux sans fil basés sur une infrastructure Ainsi, une bonne approche de monitorage dédié au réseau mobile Ad hoc doit prendre en compte la compromission des nœuds, ainsi que la résistance aux attaque pour réduire la vulnérabilité d'un système contre les menaces .

Apres avoir expliquer les différent critères, nous allons présenter un tableau comparatif des différentes approches étudiées que nous avons résumées dans la section précédente.

	critère 1	**critère 2**	**critère 3**	**critère 4**	**critère 5**	**critère 6**
ANMP	non	oui	oui	non	oui	oui
CBA – IDS	oui	non	–	non	oui	oui
GUERRILLA	oui	oui	oui	non	non	non
WANMON	oui	non	oui	non	non	non
OLSRM	oui	non	oui	non	non	non
DAMON	oui	oui	oui	non	non	non
MMAN	oui	–	oui	oui	non	non
DIST – MONIT	oui	non	non	non	oui	oui
JOUR – DYNAM	oui	oui	oui	non	non	non
HMA	oui	oui	–	non	non	non
EDRAMA	non	oui	oui	non	non	oui
ADMA	oui	non	oui	oui	non	non
NMCAM	oui	non	–	oui	non	oui
QOSMI	oui	oui	–	non	non	non
QOSMA	oui	oui	–	non	oui	non
MA – IDS	non	–	–	non	non	oui

TABLE 2.2 – Tableau comparatif

2.5.2 Discussion

Nous avons remarqué à travers cette analyse qu'il existe des critères satisfaits par la majorité des ces approches, alors que d'autres sont pas satisfaits que par quelques une particulièrement le critère de la robuste aux attaques puisque la majorité de ces approches n'assure aucun service de sécurité, nous avons aussi remarqué que les critères satisfaits dépendent fortement de service de gestion pour lequel cette approche est conçue.

Parmi ces approche sauf ANMP , DIST-MONIT et JOUR-DYNAM et aussi EDRAM et NMCAM ,CBA-IDS et MOBILE AGENT IDS qui assurent un certain niveau de sécurité ,cela en utilisant des mécanismes déférents ,les service garantit par ces approches ainsi les mécanismes utilisé par ces approche seront détaillés dans le chapitre suivant.

2.6 Conclusion

Dans ce chapitre nous avons procédé à l'étude de la supérvision des réseaux et nous avons détaillé les concepts généraux de monitorage tel que son processus ses buts, et même ses difficultés.

Les avancées importantes dans les technologies sans fil ont notamment favorisé le développement de réseaux mobiles ad-hoc et ses domaines d'application d'où le besoin de monitorage pour une meilleures gestion des performances et des fautes et surtout pour la gestion de la sécurité, ce qui explique les nombreuses propositions et recherches sur le monitorage, nous avons présentés quelques approches en spécifiant pour chacune ses buts ,par la suite nous avons effectués une analyse détaillée de ces approches en basant sur des critères bien définis.

Nous avons remarqué à travers cette étude que les solutions proposés ne répondent pas aux nouvelles exigences de sécurité qui est sûrement un critère de performance capital, d'où la nécessité d'un monitorage sécurisé.

CHAPITRE 3

APPROCHE PROPOSÉE

3.1 Introduction

Une description des solutions proposées pour augmenter le niveau de sécurité de monitorage dans les réseaux mobiles ad hoc et la proposition d'une nouvelle approche fait l'objectif de ce chapitre, nous nous sommes focalisés sur l'étude et l'analyse de la sécurité dans le monitorage pour les solutions existantes ce que nous a permet de proposer une nouvelle approche basée sur la surveillance des moniteurs, les détailles ainsi la topologie seront présentés dans ce chapitre.

Dans la première partie de ce chapitre nous donnons quelques définitions nécessaires concernant la sécurité dans les réseaux mobiles ad hoc afin d'analyser l'aspect de sécurité pour les solutions existantes et la dernière partie sera consacrée à la description de l'approche proposée et deux autres topologies qui seront comparées avec notre topologie.

3.2 Services de sécurité

Nous définissons les paramètres de sécurité utilisées dans l'analyse des aspects de sécurité des réseaux mobiles Ad hoc :

3.2.1 Authentification

L'authentification permet de vérifier l'identité d'une entité ou d'un nœud dans le réseau. C'est une étape incontournable pour le contrôle de l'accès aux ressources réseau. Sans l'authentification, un nœud malicieux peut facilement usurper l'identité d'un autre

nœud dans le but de bénéficier des privilèges attribués à ce nœud ou d'effectuer des attaques sous l'identité de ce nœud et de nuire à la réputation du nœud.

3.2.2 La confidentialité

La confidentialité est un service essentiel pour assurer une communication privée entre les nœuds. C'est 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.
Elle est principalement basée sur la cryptographie, en particulier les algorithmes de chiffrement.

3.2.3 Intégrité

Ce service assure que le trafic de la source à la destination n'a pas été altéré ou modifié sans autorisation préalable pendant sa transmission. C'est la protection contre les menaces qui peuvent causer la modification non autorisée de la configuration du système ou des données. Les services d'intégrité visent à assurer le bon fonctionnement des ressources et la transmission. Ces services assurent une protection contre la modification délibérée ou accidentelle et non autorisée des fonctions du système (intégrité du système) et de l'information (intégrité des données).

3.2.4 La non-répudiation

La non-répudiation est la possibilité de vérifier que l'émetteur et le destinataire sont bien les parties qui disent avoir respectivement envoyé ou reçu le message. Autrement dit, la non-répudiation de l'origine prouve que les données ont été envoyées, et la non-répudiation de l'arrivée prouve qu'elles ont été reçues. En d'autres termes, la non-répudiation permet de garantir qu'une transaction (émission/réception/action) ne puisse pas être niée. Cela est très pratique pour détecter et isoler les nœuds compromis.

3.2.5 La disponibilité

La disponibilité consiste à assurer la continuité du service fourni par un nœud même en présence d'une attaque. En d'autres termes, les nœuds doivent assurer la continuité des services réseau quelle que soit l'attaque de déni de service.

3.3 Outils de sécurité

Il existe plusieurs outils pour assurer les services de sécurité dans un réseau, parmi eux nous pouvons citer :

3.3.1 La cryptographie

La cryptographie est une science qui étudie les outils servant à sécuriser les informations, de tout temps, l'art du chiffrement-déchiffrement a été employé. Le chiffrement et le déchiffrement des données sont effectués par des algorithmes cryptographiques. Ces algorithmes reposent généralement sur des problèmes mathématiques complexes, difficiles à résoudre, tels que la factorisation des nombres premiers, les logarithmes discrets, etc.Les algorithmes cryptographiques modernes nécessitent une clé pour le chiffrement et une clé pour le déchiffrement.

Il existe deux grands types d'algorithmes cryptographiques, ceux dits à clé secrète et ceux dits à clé publique :

Algorithmes cryptographiques à clé secrète, ou symétriques Les clés de chiffrement et de déchiffrement sont identiques. La sécurité repose sur la non-divulgation des clés et sur la résistance des algorithmes aux attaques de cryptanalyse. Les plus connus sont DES, IDEA, RC2, RC4 et AES (Advanced Encryption Standard).

Algorithmes cryptographiques à clé publique, ou asymétriques Les clés pour le chiffrement et le déchiffrement sont différentes. La sécurité repose sur le fait que le temps nécessaire pour déduire les clés secrètes associées aux clés publiques est théoriquement non raisonnable. Les plus connus sont RSA (Rivest Shamir Adleman), les courbes elliptiques, Pohlig-Hellman, Rabin et ElGamal.

Les algorithmes symétriques sont beaucoup plus rapides que les algorithmes asymétriques dans des conditions identiques de test. Il ne faut pas en conclure que les algorithmes symétriques soient plus ou moins sécurisés que les algorithmes asymétriques. Ils sont simplement destinés à des usages différents.

3.3.2 La réputation

Chaque entité réseau encourage la collaboration d'autres entités en utilisant une métrique de coopération appelée réputation. La métrique de réputation est calculée sur la base des données recueillies localement par chaque nœud et peut se baser optionnellement sur l'information fournie par d'autres nœuds du réseau impliqués dans des échanges de messages

avec les nœuds surveillés. Une note est attribuée à chaque entité, cette note sera augmentée chaque fois que l'entité participe au routage.

3.3.3 Les systèmes de détection d'intrusions

Un système de détection d'intrusions IDS est un processus de contrôle et d'analyse des évènements dans un réseau pour détecter et identifier toute tentative d'attaque. Il permet de détecter les violations de la sécurité dans un système donné et cherche à réduire et réagir contre les éventuelles intrusions. Un IDS comporte trois parties de base : la capture, le traitement, et la réponse[34].

3.3.4 Les politiques de sécurité

Une politique de sécurité peut être vue comme l'ensemble des modèles d'organisation, des procédures et des bonnes pratiques techniques permettant d'assurer la sécurité d'un système informatique.

Pour garantir la sécurité, une politique de sécurité est généralement organisée autour de 3 axes majeurs : la sécurité physique des installations, la sécurité logique du système d'information et la sensibilisation des utilisateurs aux contraintes de sécurité [35].

Après avoir énumérer les différents services et outils de sécurité ; nous détailleront dans le tableau suivant quelques approches citées auparavant dans le chapitre2 et qui assurent un certain niveau de sécurité, cela en citant pour chacune le service de sécurité garantit ainsi l'outil utilisé afin d'assurer pour chacun d'eux un but particulier.

.

Approche	**Service de sécurité**	**Outil utilisé**	**Le but**
ANMP	- Confidentialité - L'authentification - Control d'accès	- Cryptographie - Politique de sécurité	Assurer un routage sécurisé
NMCAM	- disponibilité	- Détection des nœuds égoïstes - Un système de réputation	Assurer un routage performant et sécurisé
EDRAMA	- Control d'accès - Authentification - Confidentialité - Intégrité -Non répudiation	- Politique de sécurité - Cryptographie - IDS	Assurer une configuration sécurisée
CBA – IDS	- Intégrité - Disponibilité	- IDS	Sécurisation de réseau ad hoc grâce à IDS basé sur les techniques d'intelligence artificielle
MA – IDS	- intégrité - Disponibilité	- IDS	Sécurisation de réseau ad hoc grâce une nouvelle architecture d'IDS
DIST – MONIT	- intégrité	- Algorithmes spécifiques	Assurer un routage sécurisé

TABLE 3.1 – Les approches de monitorage sécurisé

3.4 Motivation

Dans ce mémoire nous avons présenté plusieurs approches de monitorage qui tentent de répondre au défit de réseau mobile ad hoc en terme de sécurité, ces approches utilisent différentes mécanismes pour l'élection de moniteur ,dans l'approche [36] ils ont proposé une approche de monitorage performant basé sur un modèle de confiance dans le but de ne pas élire des nœuds malveillants ou égoïstes ,mais comme dans le réseau mobile ad hoc le comportement d'un nœud peut changé ,il est risqué qu'un nœud moniteur devient non légal après son élection soit par un comportement égoïste ou par un comportement malveillant ,dans ce cas les informations collectées par ce moniteur sur l'utilisation et sur l'état et les composants de réseau ne peuvent plus servir pour la gestion de réseau puisque ce nœud moniteur peut rejouer et modifier ces informations ,et même les décisions prises par ce moniteur à propos d'autres nœuds sont pas valables, les effets d'un tel comportement dans les domaines critiques sont catastrophiques vue que ce comportement ne perturbe pas seulement l'activité de monitorage mais le fonctionnement de tout le réseau par exemple dans le domaine militaire si un moniteur distribue une fausse politique pour les nœuds de son domaine et cette fausse politique consiste à attaquer les voisins à une distance donnée donc un partenaire sera cible de cette attaque s'il est voisin ,et même dans le cas d'utilisation de réseau mobile ad hoc pour le sauvetage dans les catastrophe naturel si le nœud moniteur soit égoïste et n'achemine pas un message au bout d'un instants précis c'est la vie des être humains qui sera en danger ,les risque sont particuliers dans les domaine sensible tel qu'une usine utilisante des produits explosifs ,un comportement malveillant ou égoïste de moniteur peut entrainer des explosion ou des incendies, Nous pouvons conclure que la surveillance de moniteurs est une activité indispensable.

L'intérêt principal de notre proposition est la détection de tous comportement malveillant ou égoïste des moniteurs après leurs élections et d'offrir une nouvelle topologie permet de les surveiller afin de renforcer la sécurité de monitorage, notre approche doit prendre en charge que les nœuds malveillants ou égoïstes ne peuvent pas être des moniteurs.

3.5 Quelques définitions

la confiance : Un nœud ne peut faire confiance à un autre nœud seulement si ce dernier se comporte d'une façon correcte. Dans les réseaux mobile ad hoc les nœuds ne sont pas physiquement protégés, ils peuvent être capturés par des attaquants, ce qui pose problème au niveau des relations de confiance entre les nœuds. La construction des

liens de confiance au début n'est pas une tâche difficile, mais maintenir ces liens de confiance et supporter les changements dynamiques des liens est un vrai défi.

La confiance est mise à jours en fonction de deux comportements qui diminuent son niveau pour un nœud.

Comportement égoïste : Si un nœud augmente les performances réseau (ex. bande passante) il aura plus de ressources ou de fonctionnalité avec un taux d'énergie minimum. Ce profil d'attaque est connu sous le nom de comportement égoïste. Alors la présence des ces nœuds égoïstes dans le réseau mobile ad-hoc a comme conséquence la dégradation de performances de réseau.

Comportement malveillant : En raison de la mobilité et l'absence d'une infrastructure dans les réseaux mobiles ad hoc, ils sont plus enclins pour souffrir des comportements malveillants que les réseaux de câble traditionnels. Un nœud malveillant peut exploiter ces vulnérabilités dans le but de perturber les mécanismes de surveillance et ou de routage dans ces réseaux.

3.6 Description de l'approche

3.6.1 Notre proposition

Notre nouvelle approche s'apporte sur le principe de détecter tous comportement malveillant ou égoïste de moniteur de ce fait, nous proposons que les moniteurs aussi seront surveillés pour palier ou réduire tous les effets pervers discutées dus au faite qu'un nœud moniteur devient non légal.

Principalement, nous proposons une nouvelle topologie dans laquelle chaque moniteur est surveillé par au moins deux nœuds légaux c'est-à-dire d'exiger que même après avoir élit un nœud comme moniteur sa valeur de confiance est mise à jour par ces surveillant et ils peuvent décider de le suspecte d'être moniteur et élire un nouveau moniteur.

Nous discuterons dans ce qui suit les paramètres que nous avons pris en considération dans l'élection de moniteur et nous spécifieront le choix des surveillants de moniteur parmi les nœuds légaux voisins.

3.6.2 Election des moniteurs

Le choix d'un moniteur dans notre approche se base sur le poids de nœud qui est calculé à partir de trois métriques qui sont l'énergie restante d'un nœud, sa mobilité et

surtout son niveau de confiance.

La valeur de confiance Le calcule de la valeur de confiance se base sur la technique utilisée dans [36] avec quelques améliorations, elle est faite en trois étapes qui sont :

Etape1 La valeur de confiance est initialisé à 0.5 puis chaque nœud estime une valeur de confiance de ses voisins cette solution peut être jumelée avec un mécanisme de surveillance entre voisins proches nommé mécanisme du chien de garde (watchdog) qui permet d'observer et de détecter les nœuds qui se comportent pas correctement, le composant watchdog maintient en cache les paquets qui ont été envoyés récemment pour un nœud et les comparés aux paquets émis par un nœud observé. Les paquet sont purgés du cache au fur et a mesure des transmissions faites par le nœud suivant, si un paquet est gardé dans le cache durant un temps supérieur à une valeur seuil, le watchdog considère que le nœud observé n'a pas été capable de relayer le paquet et envoi un message de notification au nœud source de paquet, le chien de garde incrémente un control d'échec pour les nœuds responsable de l'expédition d'un paquet. Si le contrôle dépasse un seuil le nœud est identifié comme un nœud se conduisant mal.

Etape2 Chaque nœud de réseau envoi une requête à ces voisins contient la liste de ses voisins dans le but que si un voisin a une valeur estimé de confiance sur un des voisins de nœud qui a envoyé la requête, il lui envoi cette valeur avec l'identité de nœud correspondant.

Etape3 Chaque nœud de réseau calcule les valeur de confiance grace au valeurs envoyées par ces voisins.

Un noeud est déclaré comme non légal si sa valeur de confiance est inferieure à un seuil.

Exemple : on prend l'exemple où c'est le nœud 4 qui calcule les valeur de confiance de ces voisins.

- **Etape1**

  Chaque noeud de reseau estime des valeurs de confiance de ses voisins.

- **Etape2**

  Le nœud 4 envoi à ses voisins une requête req(4 ;2,3,5).

  Le nœud 2 envoi au nœud 4 comme réponse à la requête le message ((4,0.5)(3,0.4)).
  Le nœud 3 envoi au nœud 4 comme réponse à la requête le message ((4,0.5)(2,0.7)).
  Le nœud 5 envoi au nœud 4 comme réponse à la requête le message (4,0.2).

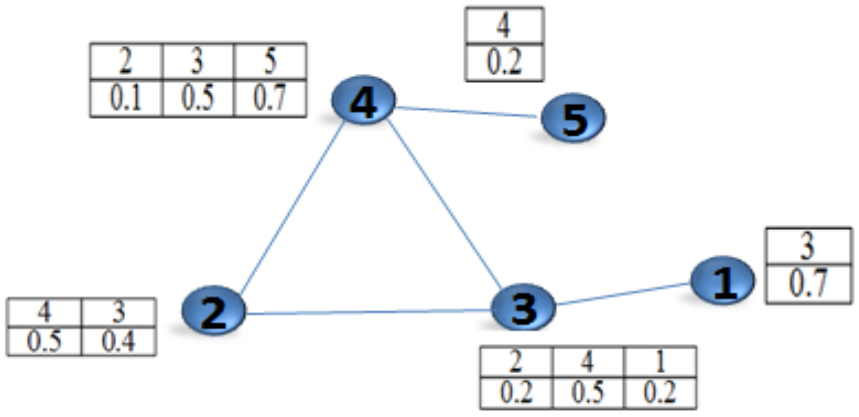

FIGURE 3.1 – Estimation des valeurs de confiance.

– **Etape3**

A la réception de ces réponses au niveau du nœud 4, il procède au calcule de la valeur de confiance.
Pour le nœud 5 n'a pas reçu d'estimation, alors il garde celle qu'il a estimée lui-même.
Pour le nœud 2 sa valeur de confiance est vc(2)=(0.1+0.7)/2=0.4
Pour le nœud 3 sa valeur de confiance est vc(3)=(0.5+0.4)/2=0.45
Pour le nœud 4, la valeur de confiance est vc(4)=(0.5+0.5+0.2)/3=0.4

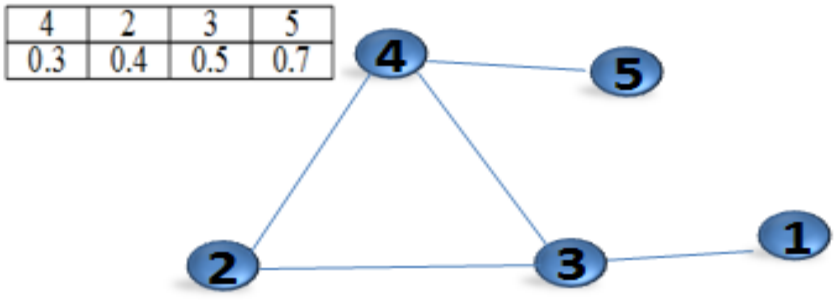

FIGURE 3.2 – Le calcule des valeurs de confiance.

Energie restante Un moniteur doit avoir une valeur d'énergie élevée pour assurer le

service de monitorage, dans notre approche nous considérons que ce paramètre est mise en 0 pour un nœud a une valeur de son énergie restante inferieure à un seuil, sinon il a la valeur 1.

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 [37].

La mobilité du nœud Un noeud moniteur doit être plus stable donc il ne doit pas se déplacer souvent, pour déterminé la mobilité, nous estimant la probabilité qu'un nœud se déplace pendant le cycle actuel de monitorage a base de sa mobilité dans les cycles précédents.

3.6.3 Maintenance des topologies

La topologie de monitorage est mise à jour dans plusieurs situations, nous concentrons sur les situations suivantes :

- L'arrivé d'un nouveau nœud voisin ce dernier reçoit les messages hello venant des nœuds à sa portée, il vérifie l'identité du moniteur qui se trouve dans les messages hello ; si il trouve que ce dernier est un voisin direct, ou a deux sauts, il lui envoi une demande d'ajout.
- Si un nœud moniteur se déplace ses voisins vont pas recevoire le message hello de sa part et ils vont conclure que ce moniteur a deplacer.
- Si un nœud moniteur se comporte plus d'une manière légale soit avec un comportement égoïste ou un comportement malveillant,cette situation sera detaillée pour chacune des topologies dans ce qui suit.

3.7 Influence de la topologie sur notre proposition

Dans cette partie nous présenterons des topologies pour l'élection des moniteurs ainsi que la maintenance de ces topologies dans le cas ou un noeud moniteur devient malveillant qui est le cas relié directement a notre proposition, le but est de comparer ces topologies à notre nouvelle topologie.

3.7.1 Les clusters

Divisant un réseau dans des zones s'appelle cluster, chacun d'eux a un cluster-head qui est choisi s'il a le poids le plus élevé dans le voisinage ou s'il a le ID le plus petit parmi ses voisin ou s'il a la plus haut connectivité.

Dans notre cas nous considérons que le moniteur est le nœud avec le poids le plus élevé dans le voisinage tel que le poids est calculé en fonction de la mobilité et l'énergie et surtout le niveau de confiance comme nous l'avons expliqué avant.

3.7.1.1 Construction des clusters

Pour construire la topologie des clusters nous avons suivi les étapes suivantes :

Etape1 Après avoir calculé le niveau de confiance comme illustré auparavant ,les noeuds non légaux (malveillants ou égoïstes)sont exlus de l'election de moniteur et ne peuvent pas etre des moniteurs, chaque nœud de réseau diffuse sa valeur d'énergie restante et la mobilité à ces voisins.

Etape2 Chaque nœud de réseau calcule le poids de ses voisins et de lui-même en prenant en consideration que le noeud doit étre légal en utilisant la formule suivante :

P(i) =w1*C(i)+w2*E(i)+w3*M(i)
telque :
P(i) : Le poids d'un nœud i.
C(i) : La valeur de confiance d'un nœud i.
E(i) : La valeur de l'énergie restante d'un nœud i.
M(i) : La valeur de mobilité d'un nœud i.
w1,w2 et w3 sont des coefficients qui sont spécifiés selon les besoins, dans notre approche le paramètre w1 est le plus grand vue que notre approche a comme but d'assurer un niveau du sécurité .

Etape3 – A partir des valeurs des poids calculées, Si un nœud a la valeur poids maximal parmi ses voisins il devient un moniteur et il envoi une requête à ces voisins pour qu'il soit un moniteur, Les voisins répondent avec des réponses favorables.
– Si un nœud reçoit plus d'une requête il répond avec une réponse favorable au moniteur qui a le poids max.
– Si un nœud moniteur ne reçoit pas aucune réponse favorable de ses voisins, il accepte la requête d'un moniteur en envoyant une réponse.

3.7.1.2 Maintenance des clusters

Dans cette partie nous intéressant au dernier cas de maintenance cité auparavant dans lequel un nœud moniteur devient non légal, dans cette topologie les moniteurs sont pas surveillés donc leur comportement n'est pas évaluer et si le nœud moniteur devient non légal le résultat de processus de monitorage effectué par ce moniteur n'est plus valide et

si devient égoïste il n'exécute pas tout le processus de monitorage d'où des informations sur ces nœuds surveillés sont pas complètes est seront pas analysées.

3.7.2 CDS (connected dominating set)

CDS est défini par un ensemble de nœuds dont lequel un nœud peut être dominant ou dominée par d'autres , tandis qu'un nœud dominé est un voisin d'au moins un nœud dominant et les dominants sont reliés entre eux ,Par la définition, les CD est l'ensemble V' de G(V, e) sommets tels que :
(1) $\forall$ u $\in$ V,$\exists$ v $\in$ V'/ v $\in$ N(u)
(2) $\forall$ (u,v) $\in$ V',$\exists$ c = route (u,v) / $\exists$ w $\in$ c, w $\in$ V'
avec les notations suivantes :

- G(V, e) : graphe de réseau ad-hoc, avec tous les sommets V et tous les nœuds E.
- N k (u) : k est voisinage du sommet u.
- route u1,uk : tous les sommets (u 1. . .,u k) aussi bien que les arête (u i,u i+1) i $\in$ [1..k-1] existent. k est la longueur de chemin[38].

(1) :represente la surveillance entre le moniteur et ses voisins.
(2) :represente la surveillance bidirectionnel entre deux moniteur pour etablir le niveau de confiance.

3.7.2.1 La construction de CDS

Pour l'étape 1 et l'étape 2 sont les mêmes que les clusters.

Etape3 La construction de CDS est lancée par le nœud légal dans le réseau et tanque il exists des nœuds non surveillé dans le réseau les moniteurs vont choisir un nœud voisin qui a la valeur du poids maximal parmi ses voisins et qui n'est pas moniteur pour qu'il devient un nouveau moniteur sur ses noeuds voisins non surveillés ,nous expliquerons cette étape sous forme d'un algorithme qui est excuté sur chaque noeud :

Algorithme

Variables :
$\mathtt{n}$: Nombres des nœuds dans le réseau.
$\mathtt{E}$: Ensemble des nœuds légaux.
$\mathtt{Vi}$: Des ensembles des voisins pour chaque nœud i dans le réseau
$\mathtt{MV}$: Ensmble des moniteus et les voisins des moniteus.
$\mathtt{M}$: Ensembledes moniteurs.
Début

```
        M(1) = E(1);
        MV(1) = V1;
        MV(length(MV) + 1) = E(1);
        fin = length(MV);
    Tant que(fin < n) faire
          j=un élément dans l'ensemble MV ;
      si(appartien(j, E) et non(appartien(j, M))alors
            trouv=faux ;
        pour(k allant de 1 à length(Vj))faire
          si(non(appartien(Vj(k), MV))alors
                MV(length(MV)+1)=Vj(K) ;
                fin=fin+1 ;
                trouv=vrai ;
          Finsi ;
        Finpour ;
      Finsi ;
      si(trouv == vrai)alors
            M(length(m)+1)=j ;
      Finsi ;
    Tant que ;
  Fin ;
```

3.7.2.2 Maintenace de CDS

Dans cette partie nous intéressant au dernier cas de maintenance cité au auparavant dans lequel un nœud moniteur devient non légal, dans cette topologie le nœud moniteur est surveillé par un seul moniteur voisin, le problème qui se pose dans cette situation c'est que les décisions prises sur ce moniteur sont basées sur l'avis d'un seul moniteur qui peut être lui-même devenu non légal et le déclare comme malveillant alors qu'il est toujours légal, donc il y a un risque d'exclure un moniteur légal.

3.7.3 Une nouvelle topologie

Vue les inconvénients de deux topologies nous avons proposé une nouvelle topologie.

3.7.3.1 La construction de la topologie

Pour la construction de la topologie nous suivrons les étapes suivante : L'étape 1 et l'étape 2 sont les mêmes que le cluster et le CDS

Etape 3 Cette étape permet de définir l'ensemble des candidats au monitorage de la façon suivante : Les nœuds qui ont un seul voisin légal envoi un message à ces voisins légaux pour les informer qu'il ne peut pas les surveiller donc ces voisins le supprime de la liste des voisins qui peuvent les contrôler, cette étape et répété jusqu'à ce qu'il ne reste que des nœuds avec au moins deux voisins légaux qui peuvent surveillé ce nœud , tout cela est dans le but que c'est parmi cet ensemble que les moniteurs seront élis et si un nœud devient moniteur ces voisins légaux vont le surveillé et dans le cas où ce moniteur devient un nœud non légal c'est ses voisins qui sont chargés de prendre sa fonctionnalité de monitorage dans le réseaux,nous allons expliquer cette étape sous forme d'un algorithme qui est executé sur chaque noeud.

Algorithme

Variables :

$\mathtt{n}$: Nombres des nœuds dans le réseau.

$\mathtt{nbrv}$: Tableau de nombres de voisins des nœuds.

$\mathtt{dist}$: Un matrise de distance entre les nœuds de réseau.

$\mathtt{E}$: Ensemble des nœuds légaux.

$\mathtt{CM}$: Ensemble des nœuds condidat au moniteur.

$\mathtt{porte}$: C'est la porte des nœuds dans le réseau.

$\mathtt{appartien}(\mathtt{i}, \mathtt{E})$: Une fonction renvoi vrai si l'element i est dans l'ensemble E.

```
Début
      fin = faux;
  Tant que(fin == faux) faire
    pour(i allant de 1 à n)faire
      si(appartien(i, E)et(nbrv(i) == 1))alors
                        nbrv(i)=0 ;
        pour(j allant de 1 à n)faire
          si(dist(i, j) < porte)alors
                              nbr(j)=nbr(j) ;
          Finsi ;
        Finpour ;
      Finsi ;
    Finpour ;
          fin=vrai ;
    pour(i allant de 1 à n)faire
      si(appartien(i, E)et(nbrv(i) == 1))alors
                fin=faux ;
      Finsi ;
    Finpour ;
  Tant que ;
     k=1 ;
  pour(i allant de 1 à n)faire
    si(appartien(i, E)etnbrv(i) > 1)alors
                CM(k)=i ;   k=k+1 ;
    Finsi ;
  Finpour ;

Fin ;
```

Etape 4 C'est la même étape que l'étape 3 de la construction des clusters mais nous ajoutons une condition qu'un nœud ne peut pas être un moniteur seulement s'il est dans l'ensemble des candidats au monitorage.

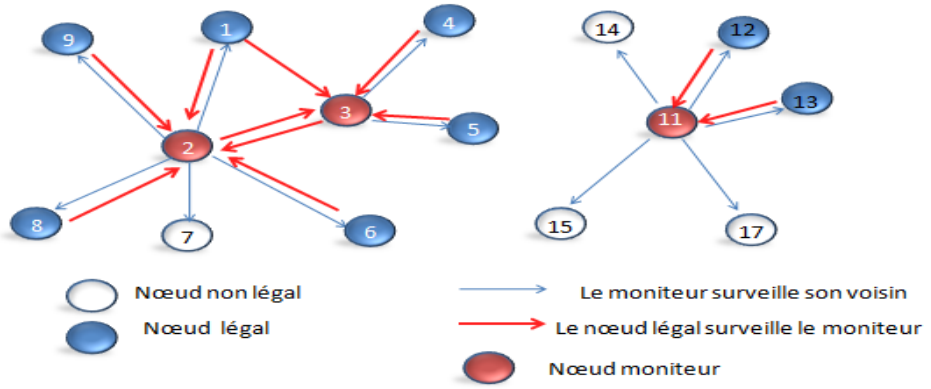

FIGURE 3.3 – Exemple sur notre topologie.

3.7.3.2 maintenance de la nouvelle topologie

Dans la partie maintenance nous intéressons à la situation où un nœud moniteur devient non légal, dans cette topologie chaque nœud est surveillé par au moins deux nœuds légaux, donc un moniteur ne sera pas exclu seulement si la moitié ou plus de ses voisins légaux le déclarent comme un nœud non légal, ce moniteur est exclu de la fonctionnalité de monitorage et une nouvelle élection est faite pour élire un autre moniteur parmi les voisins légaux de l'ancien moniteur.

3.7.3.3 Monitorage

Après avoir construit notre topologie, les nœuds de réseau peuvent entamer le processus de monitorage.

La collecte de données Pour la collecte de données, nous référons au travail réalisé dans [36] 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 par effectuer cette collecte.

l'analyse des informations Chaque moniteur analyse les informations venant des nœuds de ses voisins qu'il surveille et en cas d'anomalie il lance des alertes, à la fin de cette analyse un moniteur construit un rapport sur l'état de ces voisins surveillés.

Stockage des informations Au niveau de chaque nœud, il existe une base de données pour le stockage des données collectées et les rapports d'analyse.

Politiques proposées Nous proposons d'ajouter quelques politiques de sécurité dans le but de renforcer la sécurité :

- Si un nœud achemine des données critiques vers une destination donnée en passant par un nœud égoïste, il exige un accusé de réception.

- Si un nœud achemine des données critiques vers une destination donnée en passant par un nœud malveillant, il exige le chiffrement des ces données.
- Si un nœud moniteur est surchargé par plusieurs messages de ses voisins, il traite un nombre limité à un seuil de ces messages et ignore le reste afin de résister à l'attaque de déni de service.

3.8 Conclusion

Dans ce chapitre, nous avons détaillé notre solution qui a comme but la sécurité de monitorage, notre solution s'apuit sur le principe de la surveillance des moniteurs avec l'emploi d'une nouvelle topologie dans laquelle chaque noeud moniteur est surveillé par au moins deux noeuds legaux cette topologie sera comparée avec les cds et les clusters que nous avons aussi présentés dans le présent chapitre.

Dans le chapitre suivant nous allons valider notre proposition par une simulation ainsi les étapes et les résultats de simulation seront discutés.

CHAPITRE 4

SIMULATION

4.1 Introduction

Dans le chapitre précédent, nous avons présenté notre nouvelle approche de monitorage sécurisée basée sur la surveillance des nœuds moniteurs grâce à une nouvelle topologie, le but de cette section est d'évaluer notre topologie en décrivant notre environnement de simulation et rapportant les résultats de simulation.

Nous commençons par une brève description de l'environnement de simulation, nous donnons en suite une présentation des différentes métriques que nous allons prendre en considération lors de l'évaluation et nous terminerons par l'analyse des résultats obtenus.

4.2 Environnement de simulation

La simulation est une technique de modélisation largement utilisée dans l'évaluation de performances des systèmes informatiques et réseaux de communication. Il s'agit d'implanter un modèle simplifé du système à l'aide d'un programme de simulation adéquat,dans ce mémoire nous avons fait recours à la simulation pour évaluer les perfermances de notre approche discutée précédemment.

4.2.1 Le choix de matlab

Matlab est un logiciel de calcul numérique. Il est destiné à traiter des applications à partir des outils de l'analyse numérique matricielle.

Matlab possède aussi tout un ensemble de fonctionnalités graphiques permettant de visualiser les résultats numériques. Il possède des boîtes à outils, c'est à dire des fonctionnalités supplémentaires, dédiées à des domaines particuliers du calcul scientifique, comme la résolution d'équations aux dérivées partielles, l'optimisation, l'analyse de données, etc. Matlab est aussi un langage de programmation avec des possibilités d'interfaces vers des programmes écrits en C ou en Fortran.

En Matlab les calculs sont effectués avec une arithmétique à précision finie. Ceci le différencie des logiciels de calcul symbolique tel que Maple.

Matlab a initialement été développé en Fortran par Cleve Moler. Aujourd'hui Matlab est écrit en C et utilise les bibliothèques LINPACK et ARPACK. Il est distribué par la société The MathWorks[39].

4.3 Les paramétres de simulation

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

paramétre	**la valeur**	**unité de mesure**
Nombre de nœuds	100	Entier positif
Portée d'un nœud	20	métre
Temps de simulation	5000	secondes
Taille de réseau	100*100	m*m

TABLE 4.1 – Les paramétres de simulation

.

4.4 Les étapes de simulation

Début

inititialisation des variables de simulation ;
déploiment des nœuds dans le réseau ;
election des nœud légaux ;
construction de la topologie ;
monitorage ;
affichage des résultats de simulation ;

Fin ;

Ces étapes de simulation seront appliquées pour notre nouvelle topologie et ainsi deux autres qui sont les clusters et les CDS présentées dans le chapitre présédent dans le but de faire une comparaison entre eux.

4.4.1 Initialisation des variables de simulation

Cette étape est la première dans tout programme de simulation puisque elle inclut la déclaration des variables globales et leurs initialisation et ainsi la création des nœuds.

4.4.2 Déploiement de réseau

Les nœuds constituants notre réseau sont déployés d'une manière aléatoire sur une surface de 100*100(m*m).

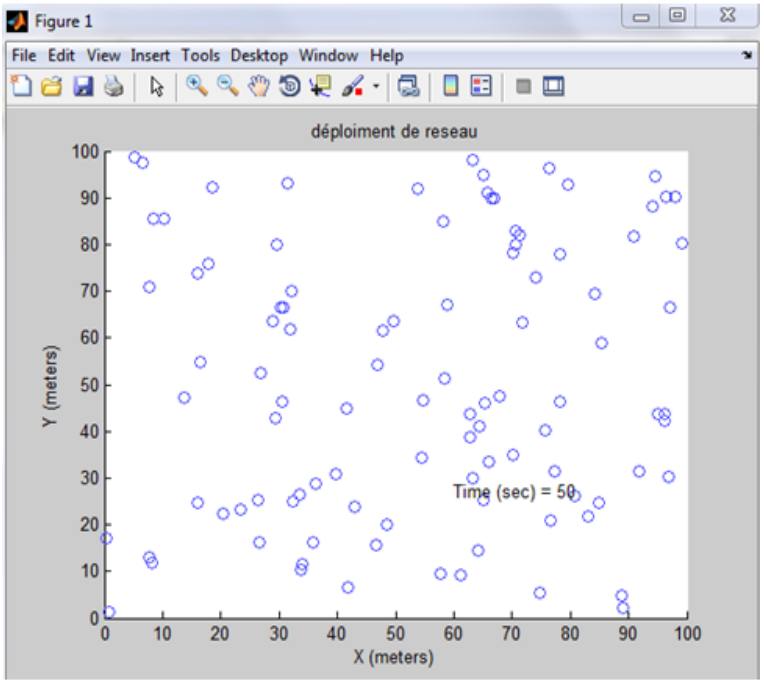

FIGURE 4.1 – déploiement de réseau .

4.4.3 Application de l'algorithme d'élection

Un nœud est non légal si sa valeur de confiance est inferieure à un seuil, Nous avons désigné dans cette étape l'ensemble de ces nœuds qui sont représentés avec une couleur rouge dans la figure suivante :

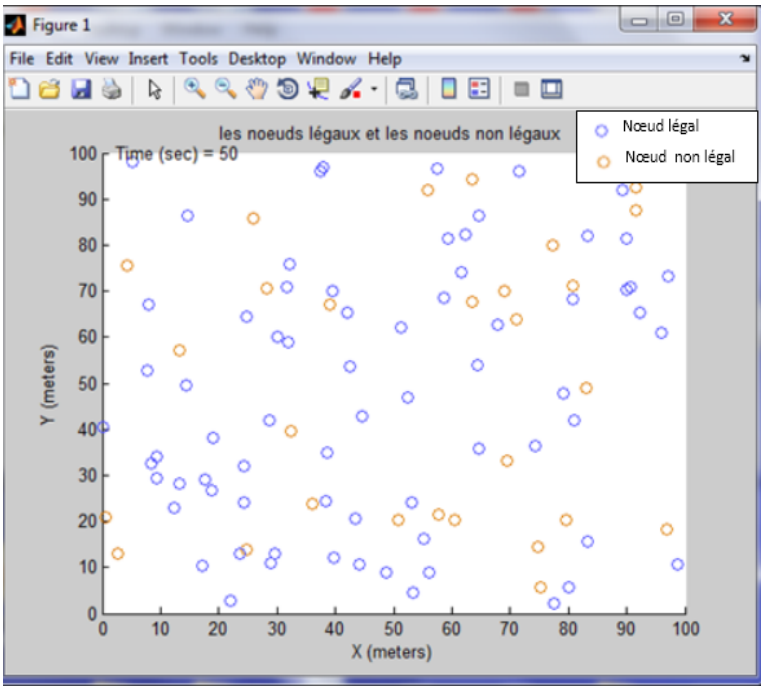

FIGURE 4.2 – Les nœuds légaux et les nœuds non légaux.

4.4.4 Création des topologies

Dans le but d'évaluer notre topologie nous allons la comparer avec deux autres topologies.

4.4.4.1 Les clusters

Dans cette première topologie le réseau est partagé en cluster dont chacun d'eux un cluster-head qui surveille les nœuds de son cluster, pour construire cette topologie nous avons suivi les étapes décrites dans le chapitre précédent.

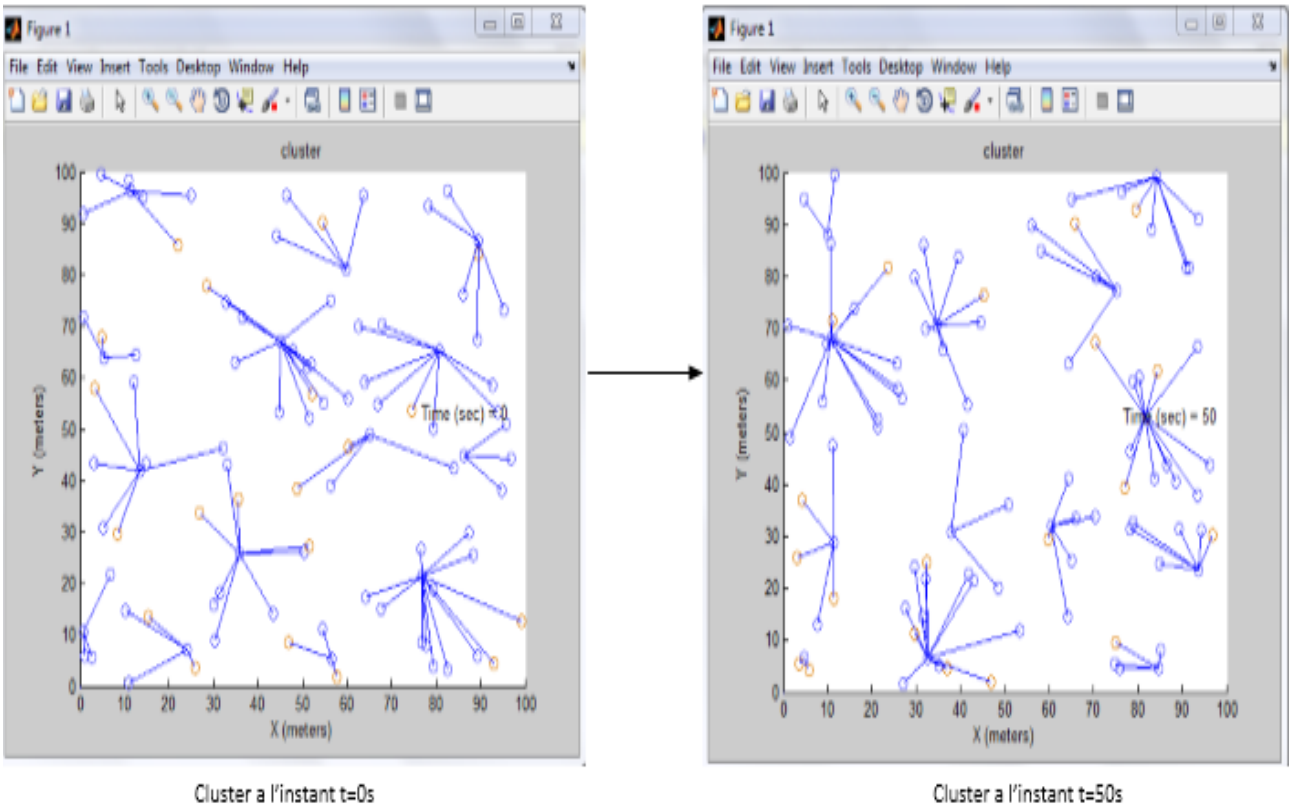

FIGURE 4.3 – Les clusters.

4.4.4.2 CDS

Nous avons implémenté aussi des CDS (connected dominating set) selon les étapes décrites dans le chapitre précédent.

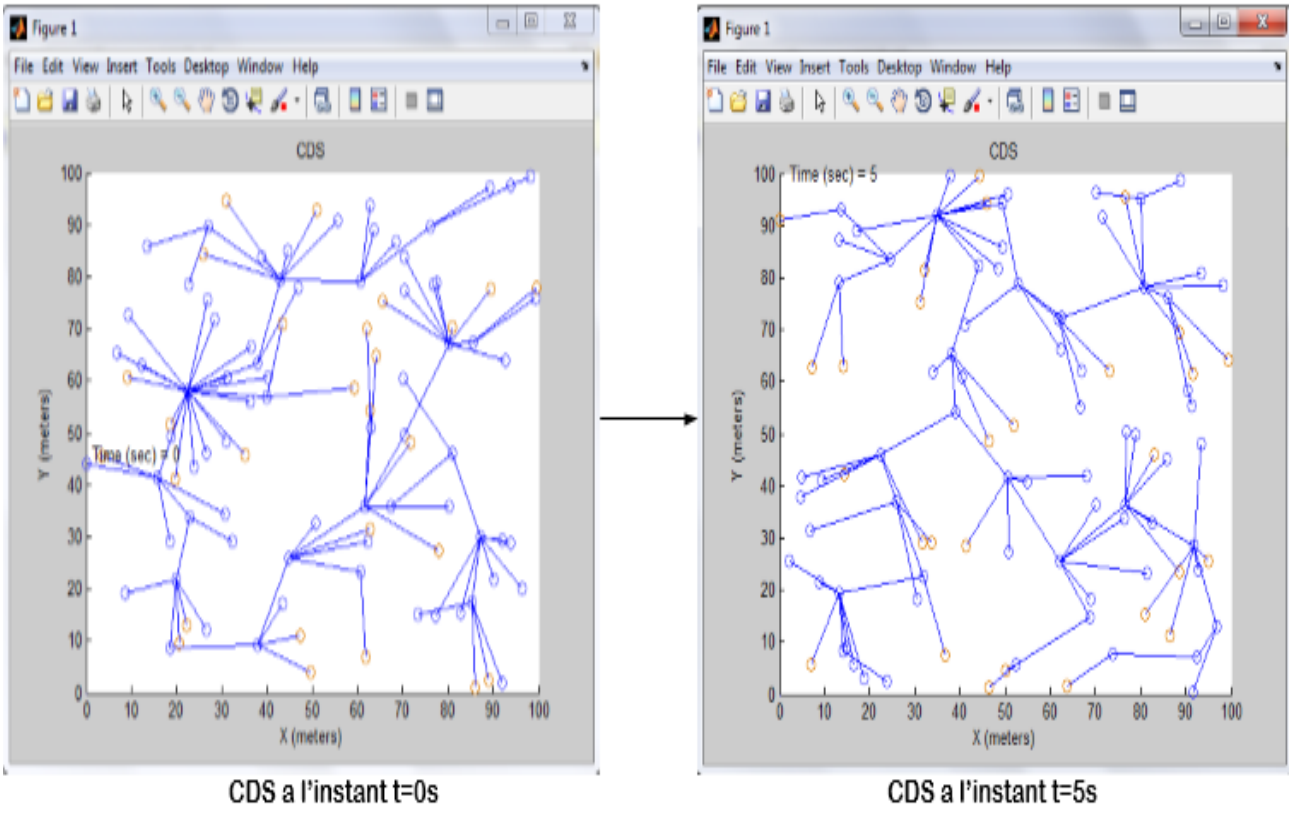

FIGURE 4.4 – Le CDS.

4.4.4.3 Notre topologie

Dans le chapitre précédent nous avons proposé une nouvelle topologie et nous avons aussi présenté ses détailles et les étapes que nous avons suivi pour sa construction.

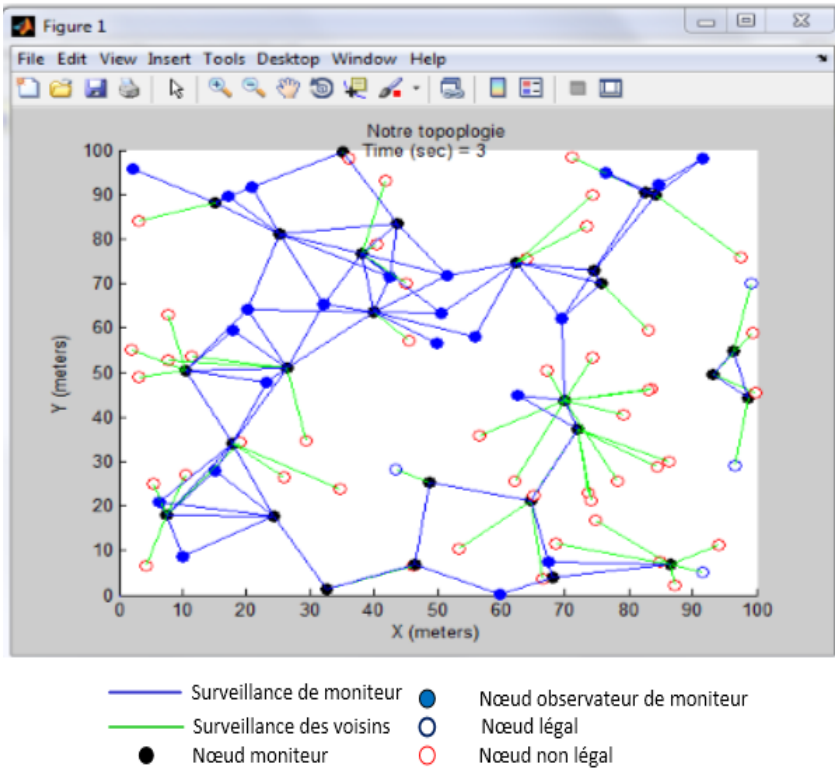

FIGURE 4.5 – Notre topologie.

4.5 Résultats et interprétations

Afin d'évaluer notre topologie nous allons la comparer avec les deux topologies implémentés précédemment (cluster et CDS) en évaluant le nombre des nœuds moniteurs égoïstes et malveillants détectés et ainsi le nombre des moniteur légaux exlus de reseau, la comparaison se basera aussi sur d'autres paramètres qui sont :le nombre de messages échangés pour la construction de chaque topologie ,le temps nécessaire pour la maintenance de la topologie en cas de détection de nœuds moniteurs non légaux.

4.5.1 Le nombre de messages échangés pour la construction de chaque topologie

.

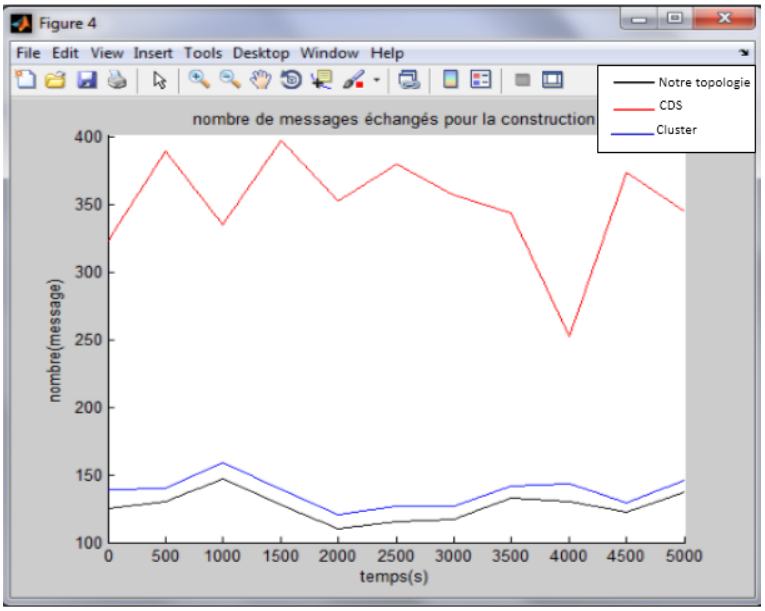

FIGURE 4.6 – Le nombre de messages échangés pour la construction .

Cette figure représente le nombre de messages échangés pour la construction de chaque topologie, les résultats obtenus montrent que notre topologie utilise moins de messages pour la construction de la topologie par rapport aux clusters et CDS. Ceci est du au fait que seulement des nœuds légaux avec au moins de voisins légaux et qui ont un poids maximum entre ses voisins qui peuvent être candidat au monitorage.

4.5.2 La détection des nœuds moniteurs non légaux

Notre topologie est capable de détecter plusieurs attaques reliées au comportement malveillant ou égoïste d'un nœud moniteur grâce aux mécanismes discutés dans le chapitre précèdent, nous citerons ici a titre d'exemple deux attaques :

Attaque de trou noir " Backhole Attack" Le but de cette attaque [40] est de falsifier les informations de routage ou de détourner le trafic, le nœud moniteur déclare un ensemble des nœuds qui sont pas ses voisin au tant que voisins, il peut lors du mécanisme de découverte de route de répondre au nœud initiateur avec un message en annonçant un chemin avec un cout minimal, vers le nœud demandé. Le nœud mettra alors sa table de routage à jour avec cette fausse route.les paquets de données du nœud émetteur vers le nœud destinataire transiteront par le nœud moniteur non légal qui peut tout simplement les ignorer.

Attaque Misrouting Dans cette attaque [41], un nœud moniteur non légal redirige le message de routage et l'envoie de données à la mauvaise destination. Ce type d'attaque est réalisé en modifiant l'adresse de destination finale du paquet de données ou en le relayant au faux prochain saut dans le chemin menant à la destination.

Nous avons spécifié précédemment que la détection d'un nœud moniteur non légal est basée sur sa valeur de confiance qui est mise à jour selon son comportement, nous avons utilisé le même principe dans la simulation.

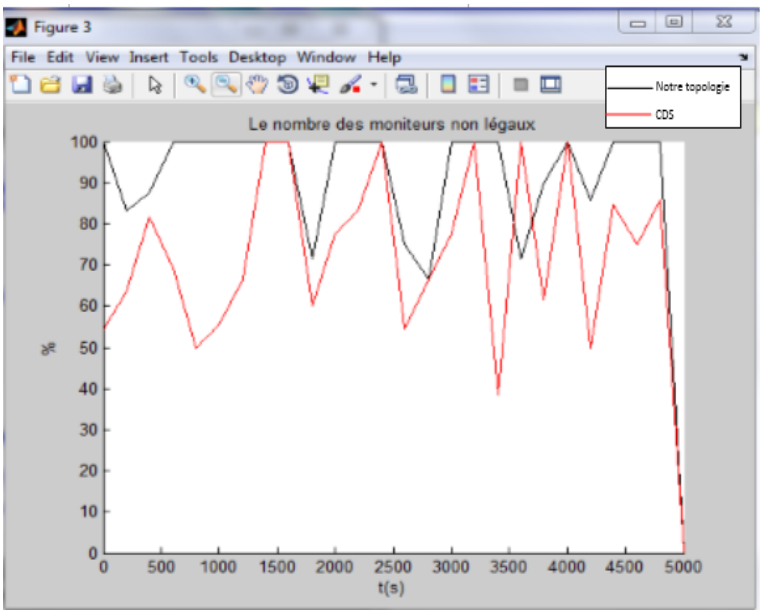

FIGURE 4.7 – Le nombre des nœuds moniteurs non légaux détectés.

Nous pouvons remarquer dans cette figure que notre topologie détecte plus de nœuds moniteurs non légaux par rapport au CDS, ceci est interprété par le fait que dans CDS, il y a un risque d'isoler des moniteurs légaux qui surveillent d'autres moniteurs non égaux et ils ne peuvent pas détecter un comportement malveillant ou égoïste de ces derniers.

4.5.3 Le nombre des nœuds moniteurs légaux exclus de la fonction de monitorage

Dans cette partie nous étudierons le nombre de nœuds moniteurs légaux détectés comme des nœuds non légaux et ils seront exlus de la fonction de monitorage.

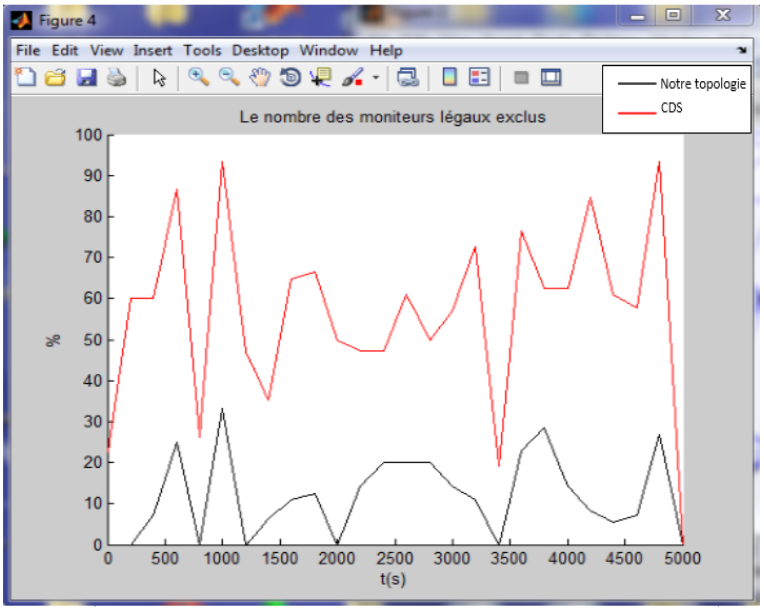

FIGURE 4.8 – Le nombre des moniteurs légaux exclus.

Nous constatons d'après cette figure que le nombre des nœuds moniteurs légaux exclus de la fonction de monitorage dans la topologie CDS est plus important que dans notre topologie .Ceci est interprété par le fait que la décision d'exclure un nœud moniteur est prise par un seul moniteur et ce moniteur peut être lui-même non légal alors que dans notre topologie un nœud moniteur est exclu seulement si plus de la moitié de ses surveillants le déclare comme non légal.

4.5.4 Délai de maintenance en cas de détection de moniteur non légal

.

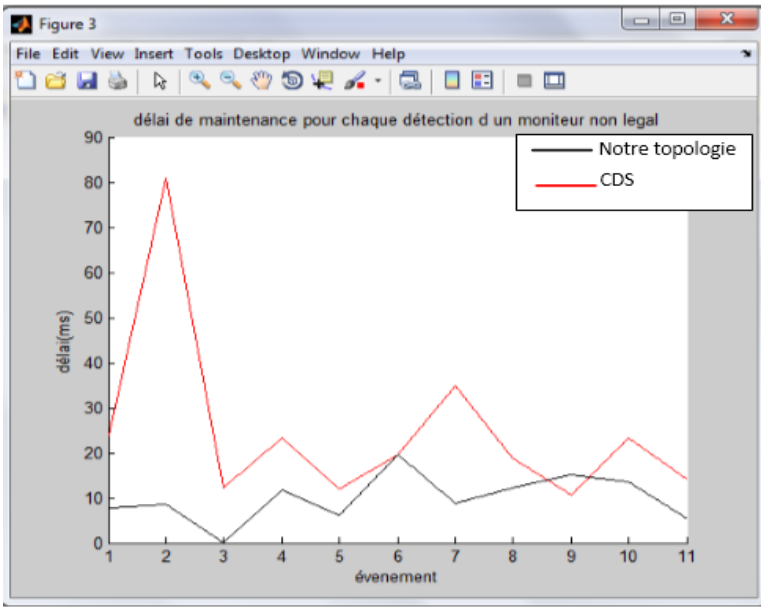

FIGURE 4.9 – Delai de maintenace.

Le délai de maintenance est le temps nécessaire pour la reconstruction de topologie en cas de détection de moniteurs non légaux. Nous remarquons à travers la figure que le délai de maintenance dans CDS est élevé par rapport à notre topologie ceci s'explique par le faite que dans notre topologie ,après détection d'un nœud moniteur non légal c'est un de ses surveillants qui deviendra moniteur c'est dans ce but que nous avons exigé qu'un nœud surveillant de moniteur doit avoir au moins deux voisins légaux .

Les résultats de simulation prouvent que notre approche présente un taux élevé de détection des moniteurs non légaux et une rapidité de reconstruction de topologie de monitorage dans ce cas, et même le nombre de nœuds moniteurs légaux exclus est minimum ,ces résultats nous ont permis de conclure que le monitorage dans notre solution est plus sécurisé.

4.6 Conclusion

Au cours de ce chapitre, nous avons présenté le choix de simulateur et les étapes de simulation. Nous avons implémenté notre topologie, et une topologie en clusters ainsi CDS, puis nous avons effectué des comparaisons entre ces trois topologies en termes de nombre de message nécessaire pour la construction de chaque topologie de détection des nœuds légaux, le taux de construction de topologie en cas de détection de moniteur non légal .

Dans ce chapitre, nous avons présenté les résultats obtenus par la simulation. Nous avons pu montrer à travers ces résultats que notre topologie détecte plus de nœud moniteurs non légaux et diminue le nombre de nœuds non légaux exlu de la fonction de monitorage, nous pouvons conclure que notre solution offre un monitorage plus sécurisé.

CONCLUSION GÉNÉRALE ET PERSPECTIVES

Le travail présenté dans ce mémoire contribue à l'étude de la sécurité de monitorage dans les réseaux mobiles ad hoc, il a comme objectif de proposer une nouvelle approche de monitorage sécurisé.

Dans ce mémoire, nous avons présenté un état de l'art sur les réseaux mobiles ad hoc et ses applications cela nous a permet de découvrir leurs principales caractéristiques qui se situent, notamment dans l'absence d'infrastructure de communication, la topologie dynamique, la sécurité et la fiabilité limitées, la gestion autonome de l'énergie, la capacité de stockage et mémoire limitées.

Nous avons aussi définit le monitorage dans un réseau mobile ad hoc et ses difficultés ainsi ses buts, pour cela nous avons dans un premier temps étudié quelques approches existantes avec une analyse détaillée de chacune à base de quelques critères bien définis, par la suite nous avons concentré sur les approches offrants un niveau de sécurité en spécifiant les mécanismes et les outils de sécurité pour chacune et nous avons achevé cette partie par une synthèse.

Comme nous l'avons constaté d'après cette analyse que ses approches ne prennent pas en considération la détection de comportement malveillant ou égoïste d'un moniteur lui-même après son élection, alors qu'un tel comportement de moniteur peut entrainer des résultats catastrophiques pas seulement sur l'activité de monitorage mais meme sur le fonctionnement de réseau surtout dans les domaines critiques tels que le domaine militaire.

C'est dans le but d'éliminer ces effets pervers que nous avons proposé une nouvelle approche de monitorage sécurisé permet de détecter le comportement malveillant ou égoïste d'un nœud moniteur avec une nouvelle topologie, les résultats de simulation prouve l'efficacité de notre topologie selon la comparaison avec d'autres topologies.

Notre approche est incapable de distinguer entre un comportement malveillant sur la disponibilité des informations et un comportement égoïste, en perspective nous envisageons d'assurer cette fonctionnalité, et aussi d'evaluer l'energie consommée par notre approche qui est un paramétre important et de prendre en compte la scalabilité .

BIBLIOGRAPHIE

[1] A. Bouzaher. *Pour l'adaptation des réseaux mobiles ad hoc. Mémoire de Magister Université Mohamed Khider Biskra.* 2009.

[2] D. Elorrieta. *Protocoles de routage pour l'interconnexion des réseaux Ad-Hoc et UMTS.Thèse de doctorat. Université d'avignon et des pays vaucluse.* 2006.

[3] A.Rachedi. *Contributions à la sécurité dans les réseaux mobiles ad Hoc. Thèse de doctorat. Université d'avignon et des pays vaucluse.* 2008.

[4] W. Mekki. *Définition et validation d'une approche de monitoring et d'analyse proactive des systèmes.* Thèse d' Ecole Nationale d'Ingénieurs de Sfax Tunisie, 2011.

[5] M. Dawoud. *Analyse du protocole AODV.These de doctorat.Université Paul Sabatier.* 2006.

[6] F. Di Gallo. *WiFi.* Extraits de source diverses récoltées, 2003.

[7] P.McDermott-Wells. *What is Bluetooth .IEEE Potentials, Vol. 23. pp. 33-35.* 2005.

[8] J.Francomme. *Propositions pour un protocole déterministe de contrôle d'accès et de routage avec économie d'énergie dans les réseaux ZigBee.* Thèse de doctorat . Universite de Toulouse, 2005.

[9] F. Theoleyre . F.Valois. *Routage Hybride sur Structure Virtuelle dans les Réseaux Mobiles Ad-Hoc.* projet Inria Aresina Lyon, 2008.

[10] A Nait-Sidi-Moh M.Bakhouya. *Localisation et routage géographique dans les réseaux MANETs.* 2009.

[11] C. Yawut. *Adaptation à la mobilité dans les réseaux ad hoc.These de doctorat.* 2005.

[12] M. Voland T. Briche. *Les outils d'administration et de supervision réseau.* 2004.

[13] R.Badonnel. *Supervision des Réseau et Service ad hoc .thèse de doctorat . Université Henri Poincaré Nancy1.* 2006.

[14] Z.Boughani . k.Bournane. *Le monitorage des réseaux ad hoc . Mémoire de Master . Université A Mira Bejaia.* 2010.

[15] E. Reuter. *Agents Mobiles : itinéraires pour l'administration système et réseau . These de doctorat . Université de Nice Sophia Antipolis.* 2004.

[16] M. Aida. N. Miyoshi. et K. Ishibashi. *A Scalable and Lightweight QoS Monitoring Technique Combining Passive and Active Approaches.* IEEE International Conference on Computer Communications .San Francisco. CA. USA, 2003.

[17] W. Chen . N. Jain. *ANMP : Ad Hoc Network Management Protocol.* IEEE journal on selected areas in communication. vol 19, 1999.

[18] D.G. Schwartz. S. Stoecklin. et E. Yilmaz R. Guha et O. Kachirski. *Case-Based Agents for Packet-Level Intrusion Detection in Ad Hoc Networks.* 2001.

[19] C.Shen . C.Jaikaeo . C.Srisathapornphat . Z.Huang. *The Guerrilla Management Architecture for Ad hoc Networks.* IEEE journal on selected areas in communication. vol 17, 2006.

[20] D. Ngo. N. Hussain. M. Hassan. J.Wu. *WANMon : A Resource Usage Monitoring Tool for Ad Hoc Wireless Networks.* 2003.

[21] F.Kamoun . S.Ghannay . S.Mettali Gammar . D Males. *The Monitoring of Ad Hoc Networks Based on Routing.* 2003.

[22] N.Krishna Ramachandran .M. Elizabeth Belding-Royer . C.Kevin Almeroth. *DAMON : A Distributed Architecture for Monitoring Multi-hop Mobile Networks.* 2004.

[23] A. DaSilva H. Kazemi, G. Hadjichristofi Luiz. *MMAN :A Monitor for Mobile Ad hoc Networks :Design, Implementation, and Experimental Evaluation.* the National Science Foundation under Grant No. CNS-0519825, 2007.

[24] W. Mallouli . B. Wehbi et A. Cavalli. *Distributed Monitoring in Ad Hoc Networks : Conformance and Security Checking.* 2008.

[25] C.Popi . O.Festor. *Monitorage et journalisation dynamiques des topologies dans les réseaux ad-hoc.* Colloque Francophone sur l'Ingénierie des Protocoles, 2008.

[26] C. Yidong . Q. Xirong Z. Yanping . J. Yuehui. *the research of hierarchy model for ad hoc network monitoring based on clustering.* IC-BNMT, 2009.

[27] G.Levin . S.Li . A.Poylisher R.Chadha . Y.Cheng . J.Chiang. *Policy-based Mobile Ad hoc Network Management for DRAMA.* 2004.

[28] M.Wolberg . C. Jason Chiang . G. Hadynski Y. Cheng . A.Ghosh et R.Chadha . M. Levin. *Managing Network Security Policies in Tactical MANETs Using DRAMA.* The 2010 Military Communications Conference - Unclassified Program - Cyber Security and Network Management, 2010.

[29] M. Ayari . Z. Movahedi . F. Kamoun. *ADMA : Autonomous Decentralized Management Architecture for MANETs - A Simple Self-Configuring Case Study.* 2010.

[30] K. Gopalakrishnan . V. Rhymend Uthariaraj. *Neighborhood Monitoring Based Collaborative Alert Mechanism to Thwart the Misbehaving Nodes in Mobile Ad Hoc Networks.* European Journal of Scientific Research ISSN 1450-216X . Vol 57 .No 3 . pp 411-425, 2011.

[31] Y. Al-sbou. *A Novel Quality of Service Monitoring for mobile ad hoc networks.* Journal of scientific Research 11(7) :934-942, 2012.

[32] P. Senthilnathan . C. Kalaiarasan. *A Joint Design Of Routing and Ressource Allocation Using QOS Monitoring Agent In Mobile AD-HOC NETWORKS.* Journal of Theoretical and Applied Information Technology .Vol. 55 No.2, 2013.

[33] Y.El Mourabit . A.Toumanari . H.Zougagh. *Mobile Agent Approach for IDS in Mobile Ad Hoc Network.* JCSI International Journal of Computer Science Issues . Vol 11, 2014.

[34] K. Ayad. *Sécurité du routage dans les réseaux ad hoc mobile.* memoire de Magister . Ecole nationale Supérieure en Informatique (ESI)Oued-Smar Alger, 2012.

[35] http ://cyberzoide.developpez.com/securite/methodes-analyse risques/.

[36] R.Salhi . H.sahali. *Monperf : Monitorage Performant des réseaux mobiles ad hoc.* Mémoire de Master . Université Abderhmane MIRA .Bejaia, 2013.

[37] A.Heinzelman Chandrakasan . H. Balakrishnan. *An application-specific protocol architecture for wireless microsensor networks,.* IEEE Tran.on Wireless Comm. Vol. 1 . No. 4. 660– 670, 2002.

[38] H. Labiod. *Wireless Ad Hoc and Sensor Networks.* 2008.

[39] P. Armand. *Une brève introduction à Matlab.* 2004.

[40] F.Stajona . R.J. Anderson. *Security issues for ad hoc wireless net-works.* security protocols workshop . volume 1796.

[41] K.Sanzgir . B.Dahill. *A secoure routing protocol for ad hoc networks.* European Wireless . Nicosia . Cyprus.