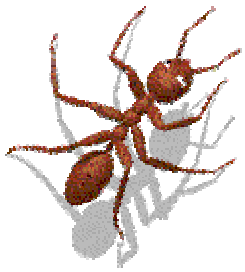
République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Mouloud Mammeri De Tizi-Ouzou

Faculté de Génie Electronique et Informatique

Department d'Informatique

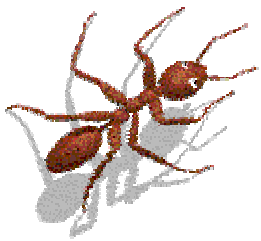


Mémoire de fin d'étude dans le cadre de l'obtention de diplôme de Master.

Option : Système Informatique.

THEME

Etude Des Vulnérabilités De Protocole De Routage AntTrust Et Proposition D'un Modèle Basé Sur La Confiance Pour Le Sécuriser.



Encadré par :

M^elle BOURKACHE Ghenima.

Présenté par :

M^elle DAMOUCHE Nasrine.

Promotion 2010/2011

Résumé

Suite à l'importance croissante des réseaux ad hoc depuis leurs naissances dans divers milieux d'applications, de nombreux enjeux relatifs à la sécurité des échanges entre les nœuds et aux performances de routage sont apparus. A titre du routage des paquets, les protocoles de routage se répartissent en stratégies proactives et réactives. Un problème majeur découlant de ces deux catégories réside en le nombre important de messages de contrôle générés, dégradant ainsi les performances de la bande passante du réseau et les capacités énergétiques des nœuds. De coté sécurité, une vague de sujets de recherches orientée à l'étude des comportements malveillants des nœuds a été mis en avant afin de faire face aux attaques visant le réseau ad hoc. Le traité synthétique pointant sur l'ensemble des protocoles existants a dévoilé une série de problèmes. Sur cette lumière est conçu le nouveau protocole de routage multi chemin « AntTrust» qui représente une grande flexibilité aux changements de l'environnement du réseau ad hoc. Et dans l'objectif de sécuriser notre protocole et de contrer les failles et les mauvais comportements des nœuds rencontrés dans ce genre de réseau, on a opté pour un modèle basé sur la confiance. Les résultats détenus à l'égard des autres protocoles, ont révélés et persistés la validité du nouveau protocole mis en évidence, ainsi son aptitude à contrecarrer une des attaques sévères : l'attaque par usurpation d'identité.

Mots clés : réseaux ad hoc, routage, protocoles de routage, sécurité, attaques, AntTrust, confiance.

Abstract

Following the growing importance of ad hoc networks since their births in various media applications, many issues related to the security of exchanges between nodes and to the routing performance have emerged. For the packet routing, routing protocols are divided into proactive and reactive strategies. A major problem arising from these two categories lies in the large number of control messages generated, thus degrading the performance of the network bandwidth and the energy capabilities of the nodes. Security aside, a wave of research topics geared to the study of malicious behavior of nodes has been put forward to address attacks against the ad hoc network. The treaty synthetic pointing to all the existing protocols unveiled a series of problems. In this light is designed the new multi path routing protocol ''AntTrust'' which represent an important flexibility to environmental changes of the ad hoc network. And in order to secure our protocol and to counter the faults and bad behavior of nodes encountered in this type of network, we opted for a model based on trust. The results held against other protocols, have persisted and proved the validity of the new protocol highlighted, and its ability to counteract a severe attack: Spoofing.

Keywords: ad hoc networks, routing, routing protocols, security, attacks, AntTrust, trust.

Si ce mémoire a pu voir le jour, c'est certainement grâce au bon Dieu ainsi le soutien et l'aide de plusieurs personnes qui m'ont permis d'accomplir ce travail dans des conditions idéales. Je profite de cet espace pour les remercier tous.

Je veux bien tout d'abord remercier Dieu, le tout puissant, qui m'a donné la force, la volonté et surtout le courage pour accomplir ce modeste travail ;

Ma gratitude et mes sincères remerciements vont également à mes très chers parents, je leurs suis infiniment reconnaissante pour leurs soutien illimité. Qu'ils trouvent dans ce mémoire le fruit de leurs sacrifices ;

Je suis profondément reconnaissante à Melle Ghenima BOUREKACHE, pour m'avoir donné l'opportunité de travailler sur ce sujet. J'aimerais bien lui adresser mes plus vifs remerciements pour sa disponibilité et son suivi, et ses conseils ;

Je remercie vivement les membres de jury de m'avoir fait l'honneur d'accepter de jurer ce modeste travail ;

A tous les enseignants du département Informatique de l'UMMTO, pour leurs participations à notre formation tout au long de notre cursus universitaire ;

A vous mes amis, merci encore pour votre amicales et efficaces collaborations, étudiants à l'UMMTO et particulièrement à toute la promotion Master 2 du département Informatique ;

Merci à tous ceux qui m'ont aidé sans ménager ni leurs temps, ni leurs encouragements, ni leurs savoirs.

Nesrine DAMOUCHE.

DEDICACES

C*'est avec un énorme plaisir qu'on a réservé cet espace pour dédier cet humble travail,*

A*ma précieuse maman, à qui je dois le meilleur de moi-même, en témoignage de ma reconnaissance infinie, qui a toujours été là pour moi, m'a toujours soutenu, compris et fait tout ce qu'il faut pour me faciliter la vie, un vif merci maman,*

A*mon adorable papa, sans qui je ne serai jamais arrivé là, cet homme qui a toujours su être présent pour moi, à tout moment et en toutes circonstances, faisant ainsi tout les sacrifices, soucieux toujours de me propulser vers le meilleur, un très grand merci papa,*

A*celles et ceux qui ensoleillent ma vie, qui m'ont toujours soutenu, supportant mes sauts d'humeur et mon stress, inconditionnellement présents auprès de moi, à vous mes sœurs et frères,*

A*toute ma famille avec qui j'apprends toujours de la vie, des acquis que je n'aurais jamais su avoir sans elle, merci à vous,*

A*tous mes ami(e)s et mes camarades.*

Encore merci du fond du cœur,

NESRINE 

Table Des Figures

CHAPITRE I

CHAPITRE II

CHAPITRE III

CHAPITRE IV

CHAPITRE V

Liste Des Tableaux

CHAPITRE II

CHAPITRE III

CHAPITRE IV

CHAPITRE IV

SOMMAIRE

SOMMAIRE

PARTIE II : Contributions

CHAPITRE IV Le protocole AntTrust, principes, fonctionnalités et failles

INTRODUCTION GENERALE

INTRODUCTION GENERALE

Le tandem réseaux et communication se profile comme un champ de challenge au sein de l'informatique émanant de l'expansion perpétuelle de la technologie dans les télécommunications qui ne cesse de révéler de nouvelles perspectives de plus en plus alléchantes. Des réseaux qui s'évertuent à répondre en termes d'indépendance de localisation géographique des périphériques informatiques et en termes d'absence de toute infrastructure préalablement définies.

Récemment, un autre type de réseau est apparu, se particularisant par une fluctuation des unités ainsi une auto-organisation, dépourvu de toutes infrastructures, tirant parti d'une interface non filaire et qui se forme d'une façon absolument arbitraire, qui n'est que le réseau ad hoc.

Ces réseaux découlent des réseaux sans fils où la notion d'une infrastructure préexistante est omise. De même, les équipements terminaux se fondent sur le déploiement des voies hertziennes pour effectuer des communications tout en ayant la capacité de se déplacer dans la zone de couverture sans interrompre la connectivité.

L'aspect dynamique et auto-organisé des réseaux ad hoc provoque un impact défavorable sur les performances des communications et augmente les vulnérabilités à diverses sortes d'attaques. Pour palier à ces écueils, il est indispensable de se servir de certains mécanismes de sécurité telle que la confidentialité, l'intégrité, l'authentification et la non-répudiation des informations.

C'est pourquoi, la conception des algorithmes de routages a du être adaptée en conséquence afin de déterminer des trajets de routage optimaux et efficaces pour une paire de nœuds (OLSR, DSV, AODV), mais sur le plan pratique, aucun de ces protocoles n'a pu interrompre ou empêcher un comportement illégitime de quelques nœuds dans le réseau.

Dans cette perspective, il est quasiment recommandé de proposer un modèle robuste apte à inciter les nœuds à coopérer entre eux pour diminuer la dégradation des performances de ces réseaux dans le routage des informations.

Notre travail de recherche entre dans le cadre de perfectionner la sécurité dans les réseaux ad hoc, cela est du en proposant un nouveau protocole de coopération entre les nœuds du réseau.

Cette perspective vise essentiellement à compléter la thèse de magister accomplisse par M^R RIAHLA Mohammed Amine assistée par M^R TAMINE Karim, et qui se résume par la conception et l'implémentation du protocole de routage AntTrust [ART.08]. Et ceci dans l'objectif d'intégrer un nouveau protocole de coopération entre les nœuds au protocole de routage ***AntTrust***.

L'objectif de notre travail est d'étudier les vulnérabilités de ce protocole et de proposer une approche de sécurité pour minimiser certaines de ces vulnérabilités. Cette approche se base sur la notion de confiance.

Et pour la mise en œuvre de notre travail de recherche, on a opté pour le plan suivant :

- Nous esquissons par une introduction générale consacrée à construire une idée globale et percutante reflétant le travail à développer.

- Une première partie consiste en un état de l'art englobant trois chapitres :

  - Le premier chapitre s'intéresse à invoquer les notions de base des réseaux ad hoc.
  - Le second chapitre est orienté à étudier le routage ainsi quelques protocoles de routage dans les réseaux ad hoc.
  - Le troisième chapitre est destiné à se positionner au niveau de la problématique de sécurité dans les réseaux ad hoc.

- La deuxième partie a recourt à tendre notre contributions, elle couvre deux chapitres :

  - Le quatrième chapitre est dédié à présenter un détail pointilleux sur le principe de fonctionnement du protocole de routage ***AntTrust***, ainsi que ses vulnérabilités.
  - Le cinquième chapitre est conçu pour proposer un nouveau modèle pour sécuriser le protocole de routage ***AntTrust***, et qui sera plié par un exemple d'utilisation de ce nouveau protocole pour détecter une attaque très sévère, l'attaque usurpation d'identité.

- La clôture de ce travail sera avec une conclusion générale cernant les résultats apportés et nos perspectives pour des travaux futurs.

PARTIE I

ETAT DE L'ART

CHAPITRE I

INTRODUCTION AUX

RESEAUX AD HOC

I.1) INTRODUCTION :

L'essor perpétuel de la technologie au sein de l'informatique et plus étroitement au cœur des réseaux de télécommunication a permis à différents concepts de voir le jour tout en mettant le point sur le passage quasi-obligatoire par la notion de facilité de déploiement et tout en adoptant au moins une de ces propriétés : la centralisation, la planification, l'administration, la mobilité et le support de transmission, à titre d'exemple on trouve les réseaux sans fil et les réseaux mobiles.

Dans notre présentation, on va se restreindre aux réseaux ad hoc qui sont un type de réseaux sans fil où chaque nœud est prêt à transmettre des données aux autres nœuds. Ces derniers jouent le rôle de stations mais la notion du nœud principal est omise. Le premier réseau ad hoc remonte aux années 1970, c'est un réseau radio du paquet (PRnet) parrainé par la DARPA.

Selon cette perspective, on va initier par un tour d'horizon sur quelques notions de base afin de mieux éclaircir et acheminer ce travail.

I.2) Concepts & définitions :

I.2.1) Réseau :

Un réseau est structuré par un environnement matériel regroupant les équipements terminaux et les câbles ou les ondes hertziennes, et par un environnement logiciel désigné par l'ensemble des protocoles. Ces environnements s'associent pour accomplir leur rôle qui consiste à atteindre de très haut débits afin de mieux véhiculer les données d'un équipement terminal vers un autre. **[GPU.03]**

L'architecture des réseaux forme un panorama de point de vue de leurs fondements, leurs caractéristiques, et leurs fonctionnalités, à titre d'exemple on cite les réseaux sans fil, les réseaux mobiles et les réseaux cellulaires.

I.2.2) technologies de communication sans fil dans les réseaux informatiques :

I.2.2.1) réseaux informatiques :

Bien entendu, pour pouvoir développer ce point, il est préférable de faire un bref tour sur la notion des réseaux informatique.

Donc, un réseau informatique est structuré par un groupe d'équipements ou d'ordinateurs reliés les uns aux autres avec un certain media de communication pour permettre le transfert d'informations. Et si ce dernier s'agit de signaux de voix, on parle alors de réseaux de télécommunication.

I.2.2.2) Les technologies de communication des réseaux sans fil :

A l'heure actuelle, nombreuses sont les technologies sans fils qui envisagent toutes à répondre au mieux aux exigences suivantes : échange accéléré de données, consommation réduite de l'énergie, utilisation optimale de la bande passante. On distingue deux primordiales classifications :

I.2.2.2.1) Selon la zone de couverture : [APV.01], [RAD.05]

Comme son nom l'indique, les technologies issues de cette perspective se différencient par l'espace géographique à couvrir. Quatre grandes classes découlent de ce contexte :

- ***WPAN*** : conçu pour les réseaux personnels avec une faible portée (une dizaine de mètres) servant de relier des périphériques (PDA, imprimante) à un ordinateur sans lien filaire. On trouve ici le Bluetooth, le Zigbee et l'infrarouge…etc.
- ***WLAN*** : ce réseau est destiné à couvrir une zone géographique correspondante à un réseau local d'entreprise. Il renferme l'ensemble des cellules composées de points d'accès. A titre d'exemple, on cite le wifi, le Hiper LAN 2… etc.
- ***WMAN*** : connu encore par BLR (Boucle Local Radio), s'articulant autour de la technologie WIMAX du standard IEEE 802.16, offrant de larges débits pouvant atteindre 70 Mbps.
- ***WWAN*** : ce sont des réseaux cellulaires mobiles considérés comme étant les plus connus du fait que tous les téléphones mobiles sont liés à un réseau étendu sans fil tel que GSM, GPRS, UMTS.

Un nombre très important de normes issues de ces classes, se concentrant toutes sur les réseaux sans fil sont mises en valeur et voici quelques unes:

A) WIFI (Wireless Fidelity) **:**

Cette technique de réseau informatique sans fil normalisée en 1999 par l'IEEE (Institute of Electricals and Electronics Engineers), se focalise sur le déploiement des standards IEEE 802.11 encore connu par le nom générique WIFI, dont le système se souci de proposer des services de communications quasiment indépendant des médias filaires de transmission. Et donc cette configuration repose sur d'autres moyens d'accès tel que l'infrarouge et les ondes hertziennes (radio). **[APV.01]**

A Les technologies du WIFI : [BAF.02], [RAD.05]

Le premier standard pour les réseaux locaux sans fil remonte en 1997, lancé par l'IEEE, apte à fonctionner avec des débits de l'ordre de 2 Mb/s. Ce standard international a donné lieu à plusieurs versions de la technologie WIFI nommées 802.11x qui se distinguent essentiellement par leurs portées, leurs débits et leurs méthodes de modulation de fréquence.

a) IEEE 802.11a :

Ce standard est dédié pour les réseaux locaux sans fil, reposant sur une bande de fréquence de 5 GHz, et un débit théorique de 54Mb/s et mettant en avant une modulation par multiporteuses (Orthogonal Frequency Division Multiplexing, OFDM). Cette dernière permet de scinder la bande de fréquence en 8 canaux de 20MHz eux-mêmes divisés en 52 sous-canaux, et lors d'une transmission, tous les sous-canaux s'utilisent en parallèle excepté 4 qui sont réservés à la correction des erreurs.

b) IEEE 802.11b :

Cette norme est caractérisée par un débit pouvant atteindre 11Mb/s, une porté de radio sept fois plus que le 'IEEE 802.11a', avec une bande de fréquence de 2.4 GHz et une technique de modélisation par étalement de spectre direct (DSSS, Direct Sequence Spread Spectrum) qui consiste à diviser la bande de fréquence en 14 canaux où les données ne sont envoyées que sur un seul canal parmi ces canaux, ce qui fait que cette méthode est très sensible à de nombreuses interférences.

c) IEEE 802.11 e :

Il s'agit d'un standard fondé sur le '802.11a' portant essentiellement sur l'intégration des qualités de services, des fonctionnalités de sécurités et d'authentification améliorée, orienté à transmettre la parole et les données.

d) IEEE 802.11g :

C'est une version améliorée (sophistiquée) du '802.11b'. Elle exploite la technique de modulation OFDM du standard '802.11a' et se focalise sur la norme '802.11b' qui s'appuie sur une bande de fréquence de 2.4Ghz.

B) Wimax: [TQT.09]

Cette technologie de télécommunication sans fil fondée sur le standard 'IEEE 802.16' encore nommé Broadband Wireless Access, fonctionne avec une large bande symétrique pouvant atteindre une vitesse allant jusqu'à 75 Mb/s. A nos jours, deux approches de Wimax sont mises en valeur : la '802.16 d' dédiée pour les utilisateurs fixes et la '802.16 e' destinée pour les utilisateurs mobiles.

C) Zigbee :

Dans le contexte d'effectuer des communications sans fils avec de moindre coûts et une basse consommation d'énergie est développé le standard '802.15.4' PAN (Personal Area Network), implémenté dans de multiples applications : home automation, monitoring, sécurité et bien d'autre, orienté pour répondre aux soucis de communications en terme de :

» Débit : 10 kbps-115kbps.
» Cout avantageux.
» Bande passant 2.4Ghz.
» Pas de restriction géographique.

D) Bluetooth : [RAD.05], [LAA.02]

Dans Cette norme reposant sur le standard '802.15.1' lancé par Ericsson en 1994, le but principal est de substituer l'interconnexion en câble pour former des PAN (Personal Area Network), autrement dit, les équipements peuvent se connecter avec une bande non autorisée 2.4 GHz à une distance s'étendant généralement sur une portée maximale d'une trentaine de mètres (portée très courte) grâce à un lien non filaire mais orienté. Le Bluetooth s'appuie sur une organisation automatique, dynamique, transparente, de type maître-esclave. Bien entendu, chaque dispositif peut accomplir le rôle d'un maître ou d'un esclave et établir des communications par paires. Cependant, les esclaves ne peuvent pas communiquer entre eux.

E) HomeRF:

Le HomeRF fondé en 1998 par le Home RF Working Group tel qu'Intel, HP, Motorola, Compaq et bien d'autres constructeurs, est adapté à un usage au sein de l'environnement domotique où elle doit s'occuper de mettre en place une nette communication en associant les équipements de la maison aux liaisons sans fils (internet). Cette norme opère avec un débit théorique de 10 Mbps sous une portée allant de 50 à 100 mètres sans amplificateurs.

I.2.2.2.2) Selon la composition : [GPU.03], [RAD.05]

Elle consiste en une collection de terminaux dotés d'une carte d'interface réseau '802.11', se coordonnant pour mettre en avant une communication directe, constituant ainsi une BSS (Basic Set Service) et la zone allouée pour les équipements d'une BSS est soit une BSA (Basic Set Area) soit une cellule.

Cette norme mis l'accent sur deux modes de fonctionnement, le mode avec infrastructure et le mode sans infrastructure ou encore nommé ad hoc.

A) Le mode avec infrastructure :

Ce mode est dédié à délivrer aux différentes stations des services spécifiques, sur une zone de couverture définie par la taille du réseau. Il est mis en évidence en employant des points d'accès (AP) qui représentent des stations de bases pour une BSS.

Quand on dispose d'un réseau constitué par un ensemble de BSS, chacun d'eux est associé à un système de distribution (DS) qui n'est qu'un réseau Ethernet, token-ring, FDDI (Fiber Distributed Data Interface) ou autre réseau 'IEEE 802.11' par le biais de leur AP. Ainsi une panoplie de BSS associée à un système de distribution résulte un ESS (Extended Set

Service) apte à fournir aux différentes stations mobiles une passerelle permettant de connecter le réseau ‘802.11’ à un autre réseau.

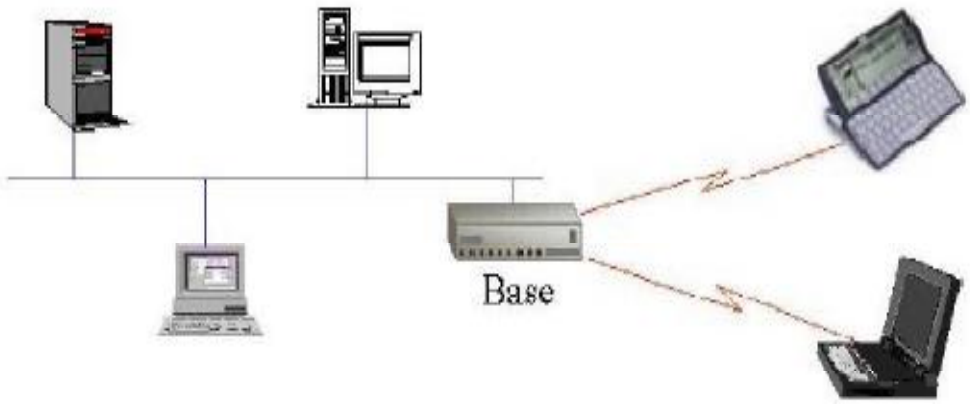


Figure 1.1 : Réseau en mode avec infrastructure.

B) Le mode sans infrastructure :

Cependant, le mode sans infrastructure aussi désigné par Ad Hoc est une collection d’équipements terminaux constituant un IBSS (Independent Basic Set Service) accomplissant la tâche, aux stations, de communiquer et de se déplacer tout en restant connectés, avec d’autres stations dans IBSS sans le passage obligatoire par aucune infrastructure que ce soit un AP ou une connexion au DS.

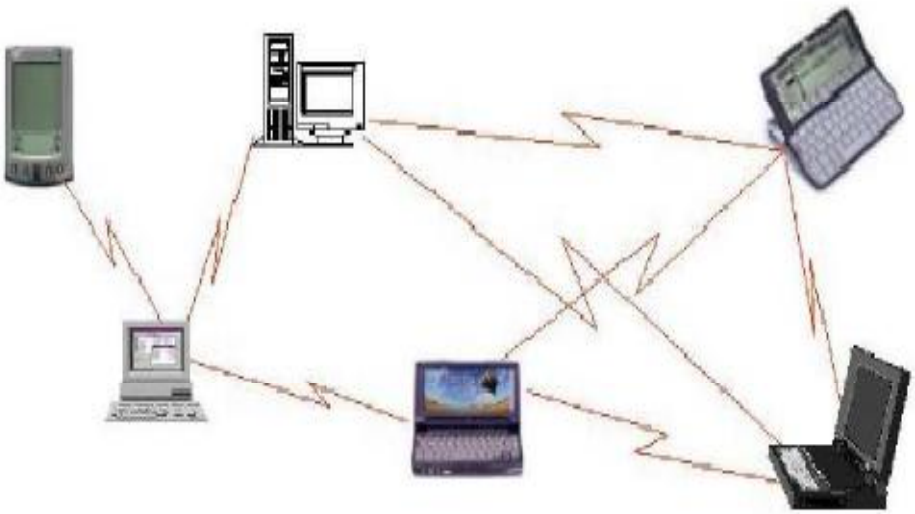


Figure 1.2 : Réseau en mode sans infrastructure.

I.2.3) Propriétés des réseaux sans fils :

Afin d'assurer une gestion adéquate de l'interface radio, certains paramètres doivent être étudiés à savoir :

1) Sécurité des réseaux mobile :

Du fait que les utilisateurs d'un réseau mobile partagent un même support de transmission, il est quasiment indispensable d'intégrer des mécanismes sécurisant l'émission des informations afin d'échapper à l'espionnage des informations et l'écoute des conversations. Ceci est du grâce à l'incorporation d'un ou de plusieurs algorithmes de cryptage de ces réseaux mobiles qui envisagent la protection du contenu des informations envoyées via l'interface radio.

2) Contrôle de puissance :

Le contrôle de puissance des signaux émis par les terminaux mobiles est réalisé essentiellement pour répondre à deux points percutants qui sont la conservation de l'énergie électrique pour une durée plus longue et la réduction du bruit d'interférences sur les autres équipements du réseau.

En revanche, le terminal se charge d'augmenter les signaux de la puissance quand il se localise le long du périmètre de la couverture et de le diminuer lorsqu'il s'approche relativement de sa station de base et donc affaiblir la consommation d'énergie.

Au moment où le terminal invoque la station de base, cette dernière détermine sa localisation et prend en charge la puissance de son signal en incorporant dans ses messages de contrôles un ou plusieurs bits orientés pour augmenter ou réduire sa puissance.

3) Paramètres de capacité :

Un tel réseau se soucie de répondre aux besoins des utilisateurs et ce en assurant une communication continue, ainsi une disponibilité de ressources qui garantit que tout utilisateur souhaitant effectuer un appel est lui associer un canal. Ce réseau est sensé de faire une distribution optimale de ressources et de mettre en valeur deux propriétés fondamentales à savoir :

a) Probabilité de blocage :

Pour pouvoir effectuer une communication entre un terminal et sa base de station, il est nécessaire de se disposer d'une ressource qui n'est que le canal radio. Cette dernière est gérée par le commutateur qui se charge de l'affecter selon certains critères, et pour une raison ou une autre, le commutateur peut se contrarier à l'attribution du canal radio et bloque la communication. Chaque communication est dotée d'une probabilité de blocage

déterminée par le nombre d'appel refusés, servant d'évaluer la congestion du système et d'éviter sa saturation.

b) Probabilité de coupure :

Une communication rompue est du essentiellement par les interférences causés par le nomadisme du signal d'un utilisateur ou par la faiblesse de la couverture radio.

I.2.4) L'apport des réseaux sans fil : [LAA.02], [RAD.05]

- **Mobilité :** garantir une liberté accrue a contribuée grandement à répondre efficacement aux besoins des utilisateurs.
- **Inter-connectivité avec les réseaux locaux filaires** : la compatibilité des réseaux locaux sans fil avec les réseaux locaux filaires (Ethernet) assure leur coexistence au sein d'un même environnement.
- **Evolutivité** : cette propriété est sensée de suivre l'extensibilité des besoins des utilisateurs en insérant ou retirant des points d'accès à titre d'exemple.
- **Accès sans fil plus ou moins rapide** : les communications sans fil sont aussi rapides, offrant ainsi des débits pouvant atteindre 50 Mbps.
- **Usage facile** : un réseau sans fil offre l'opportunité de relier aisément des espaces géographiques relativement difficile à atteindre par le biais de câbles.
- **Coût avantageux** : bien entendu que leur installation est généralement plus onéreuse que celle d'un réseau filaire, les réseaux sans fil se caractérisent par des coûts de maintenances assez réduits.

I.2.5) Les contraintes des réseaux sans fil : [LAA.02], [RAD.05]

Les technologies des réseaux sans fils illustrés précédemment présentent en contrepartie quelques soucis s'opposant à leurs performances, dont on cite :

- Le problème de renforcement de la robustesse du réseau.
- Le problème d'optimisation de la bande passante.
- Le problème d'économie d'énergie.
- Le problème des protocoles de routages.
- Le problème d'affaiblissement des signaux transmis.
- Le problème du piratage d'information.
- Le problème d'interférence du aux transmissions parallèles.

I.3) Réseau Ad Hoc :

I.3.1) Définitions :

Le réseau Ad Hoc est une dérivée des réseaux sans-fil sans infrastructure préexistante dont les équipements terminaux exploitent la voie hertzienne pour établir des communications

tout en ayant la capacité de se déplacer dans la zone de couverture sans interrompre la communication. **[GPU.02]**

Le réseau Ad Hoc est un regroupement de périphériques fondé sur la technique de transmission sans fil et procédant des protocoles élaborant la mise en réseau de ceux-ci. Un tel réseau répond en terme d'adaptabilité et d'auto-organisation, plus précisément les nœuds se forment et se déforment aléatoirement sans l'intervention d'une gestion administrée tout en mettant en avant la possibilité que chaque nœud puisse ouvrir une session de connexion, un partage d'information et de services avec autres nœuds du réseau**. [DEL.07]**

Figure 1.3 : Réseau mobile ad hoc.

Dans cette approche, la communication se déploie sans l'aide d'autre infrastructure que les stations elles-mêmes, ce qui revient à attribuer le rôle d'une passerelle ou routeur pour chacune de ces stations du fait qu'elles permettent le passage de l'information d'un mobile à un autre tout en assurant que ces derniers demeurent toujours connexes**.[GPU.03]**

I.3.2) Architecture :

Il existe deux principales catégories de topologies déterminant l'organisation des nœuds au sein des réseaux ad hoc :

a) Topologie plate :

Dans une topologie plate tous les nœuds accomplissent le même rôle. Les nœuds sont semblables en termes de ressources et donc ils ont tous part au routage des paquets.

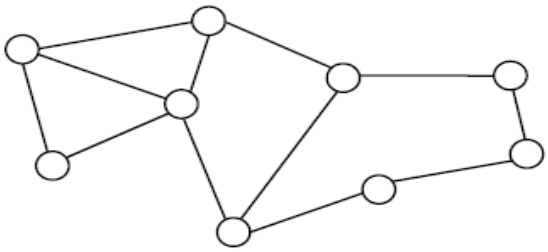


Figure 1.4 : Topologie plate.

b) Topologie hiérarchique :

Cette architecture hiérarchique cible essentiellement à améliorer la scalabilité du réseau par le biais de clustering, qui sert à partitionner les nœuds en groupes communément désignés par clusters où chacun d'eux est constitué d'un cluster-head (chef) responsable du routage des paquets et de membres.

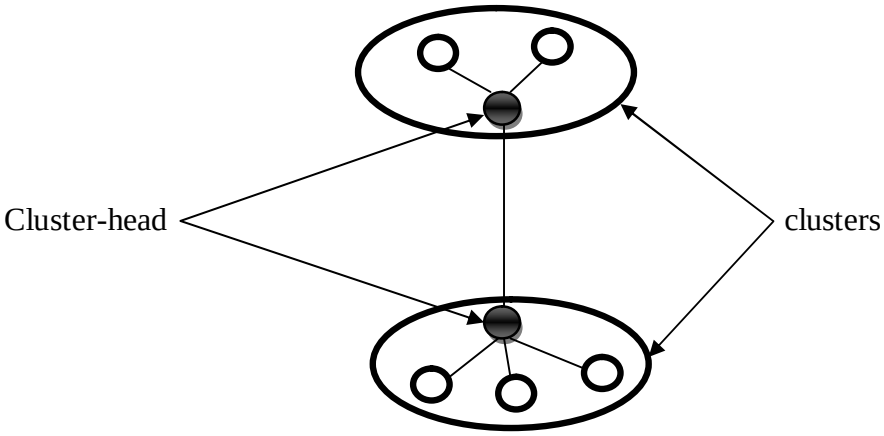


Figure 1.5 : Topologie hiérarchique.

I.3.3) Caractéristiques : [BAN.00], [RMA.08], [LAI.08]

Un réseau ad hoc est structuré par un ensemble de nœuds mobiles autonomes permettant d'effectuer des communications de façon hertzienne. Lorsque des nœuds se situant dans des zones de couverture (cellules) différentes veulent établir une communication, ils la réalisent en sollicitant des nœuds intermédiaires qui se chargent de router l'information de la source à la destination. A l'issue de cette définition, nous exposons les caractéristiques intrinsèques des réseaux Ad Hoc.

- ***Absence d'administration centralisée*** : elle consiste en une contrainte tés forte vue qu'elle provoque une importante difficulté au moment de contrôler et de

gérer la topologie dynamique et évolutive résultant de l'apparition et le déplacement des nœuds dans le réseau Ad Hoc.

q ***La taille du réseau*** : l'absence de limitation de la taille du réseau ou de nombre des nœuds dans un réseau Ad Hoc autorise d'intégrer autant de nœuds suivant les besoins.

q ***Mobilité*** : grâce à cette caractéristique, les nœuds peuvent joindre ou quitter le réseau d'une manière aléatoire et non prédictible ce qui illustre leur topologie dynamique.

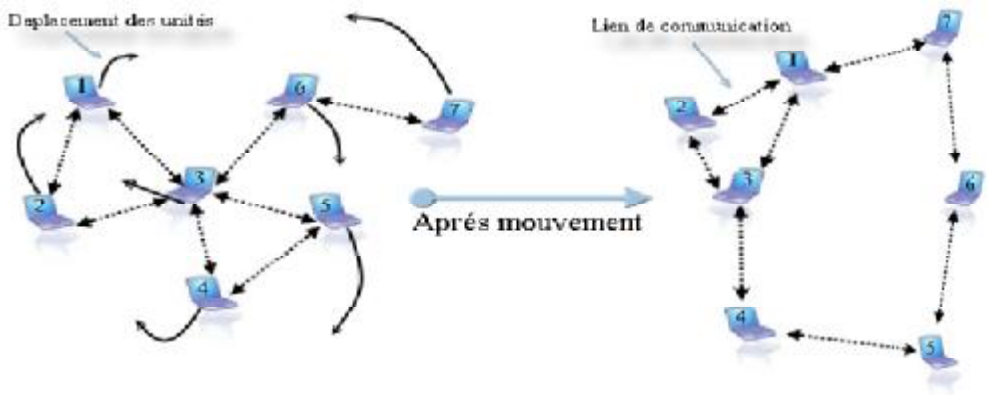


Figure 1.6 : Le changement de la topologie des réseaux ad hoc.

q ***Source d'énergie limitée*** : cette caractéristique fait que les nœuds mobiles sont alimentés par des ressources énergétiques autonomes (batteries) avec une courte durée de vie, ce qui nécessite de faire appel à des algorithmes convenables qui prennent en charge le mode de gestion d'énergie dans les réseaux Ad Hoc. A titre d'exemple, on cite les PDA (Personal Assistant Digital) qui sont limités en énergie, puissance de calcul et en capacité mémoire.

q ***Equivalence des nœuds du réseau*** : contrairement aux réseaux classiques qui distinguent les nœuds terminaux (stations) supportant les applications des nœuds routeurs assurant l'acheminement des données, les réseaux Ad Hoc écartent cette distinction de sorte que tous les nœuds peuvent accomplir la tâche de routage.

q ***Liaison sans fil*** : dans un réseau Ad Hoc, l'absence d'infrastructure oblige les nœuds mobiles qui sont connectés par des liens sans fil à se comporter comme des routeurs participant à la découverte et la maintenance des chemins pour les autres hôtes du réseau.

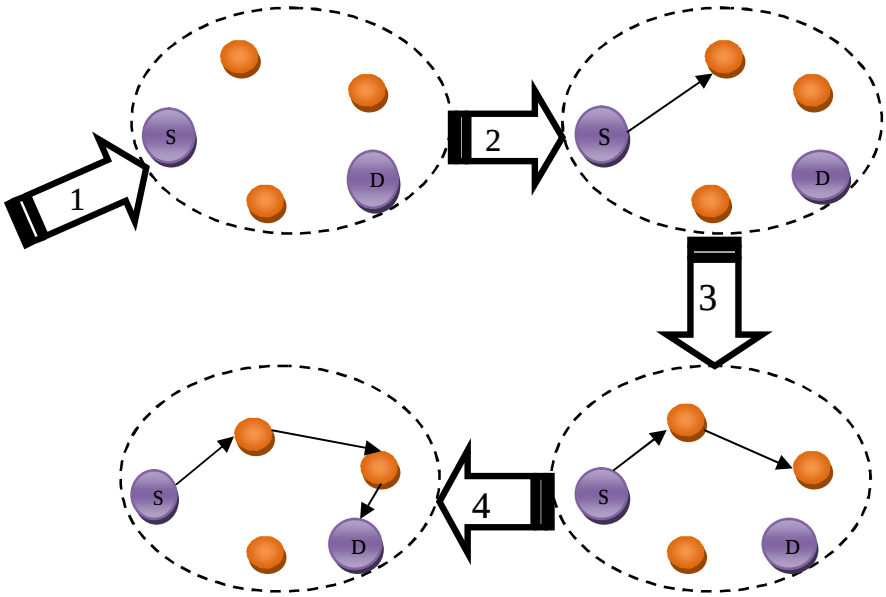


Figure 1.7: La communication entre les nœuds.

- ***Sécurité et vulnérabilité*** : la vulnérabilité dans les réseaux Ad Hoc ne touche pas uniquement le media de transmission mais aussi les nœuds mobiles par leurs autonomies. Et donc, s'introduire dans le réseau devient une tâche assez aisée et l'absence de la centralisation complique de plus en plus le pouvoir de détecter des intrusions ou des dénis de service.

- ***Bande passante limitée*** : une des propriétés primordiale spécifique aux réseaux communiquant au biais d'un lien non filaire consiste en l'usage en commun d'un medium de communication qui n'est que les ondes radio, ce qui explique la modestie de la bande passante attribuée à chaque équipement.

- ***Erreur de transmission*** : la communication radio est plus exposée aux erreurs de transmission que celle des réseaux filaires.

- ***Interférence*** : le fait que les réseaux ad hoc utilisent un medium de communication partagé explique l'interférence due à une transmission parallèle avec une même fréquence ou des fréquences proches.

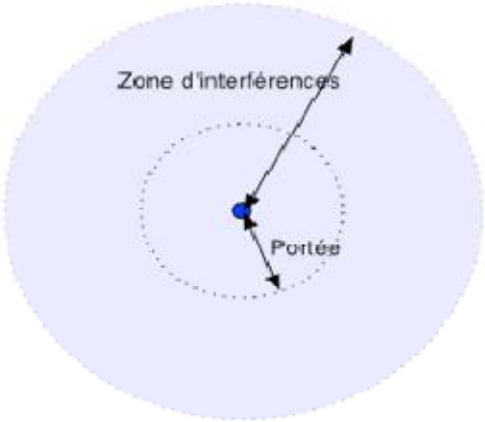


Figure 1.8 : Portée et interférence généré par un nœud.

q ***Liens asymétriques :*** les réseaux ad hoc se distinguent des autres réseaux par l'asymétrie des liens autrement dit, quand un chemin est établi d'une source à une destination, le chemin inverse ne renvoie pas conformément sa copie identique. Cette asymétrie est due essentiellement pour ces raisons à savoir :

- Les nœuds s'amènent à limiter leurs périmètres de communication dans le but d'économiser l'énergie de leurs liens et d'opérer avec des durées de vie plus longues.
- Du fait que les nœuds se dissipent, il arrive que ces dernières se caractérisent par des réceptions déphasées, plus précisément, une meilleure réception dans un sens et une mauvaise dans l'autre sens.

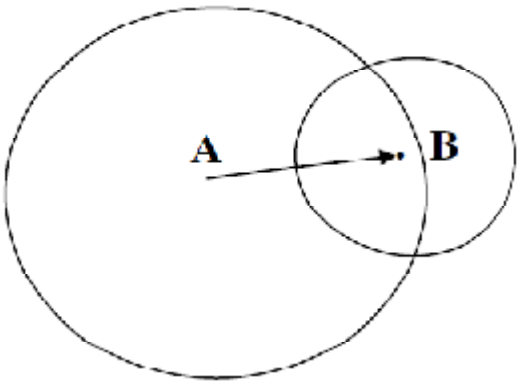


Figure 1.9 : Liens asymétriques.

I.3.4) Applications: [GUK.06], [IGL.XX], [BAN.00]

Bien entendu, les réseaux Ad Hoc sont mieux placés pour concevoir les applications n'ayant pas besoins de déployer une infrastructure réseau filaire pour une raisons ou une autre tel que la difficulté de leurs mise en place, on liste :

- ***Application militaires*** : coordination des efforts, guidage et recherche.
- ***Applications de tactiques*** : opérations de secours tel que les incendies et les tremblements de terre.
- ***Application à l'automobile*** : déplacement autonome de véhicules en ville.
- ***Application pour conférence/réunion*** : partage de données instantané, vote secret, diffusion des changements de dernières minutes.
- ***Application de recherche*** : accès internet publique.
- ***Application pour les grands sites*** : nécessitant le déploiement des réseaux à la demande (aéroport).
- ***Application pour les réseaux de capteurs*** : étude des migrations des animaux et des interactions entre animaux.

Figure 1.10 : Applications diverses de réseaux ad hoc.

I.3.5) Modes de communication : [MRN.06]

Il est très utile de rappeler les principaux modes de communications invoqués par les réseaux Ad Hoc bien avant de pénétrer le concept de routage proprement dit. Et sous cette lumière on trouve la communication unicast ou point à point dont elle se repose sur une source et une seule destination, la communication multipoints ou multicast pour laquelle un message est envoyé à plusieurs destinataires, et enfin la diffusion ou broadcast qui réside sur l'envoie d'un message à tous les nœuds du réseau.

La figure suivante schématise ces différents modes de communications :

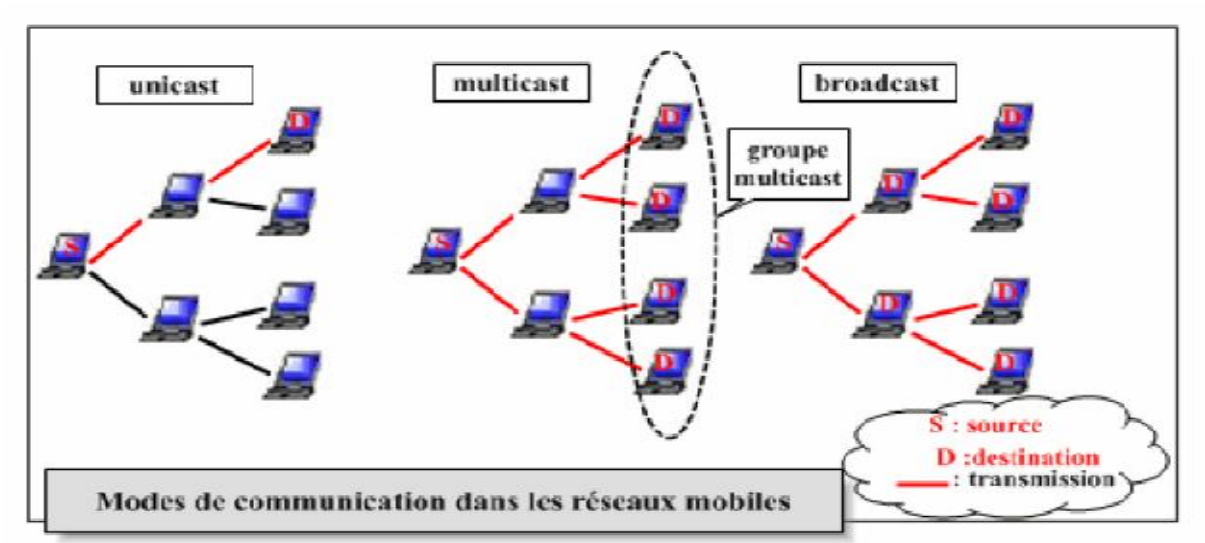


Figure 1.11 : Les modes de communications dans les réseaux ad hoc.

I.4) MANet: [MXP.09]

On désigne par un réseau mobile Ad Hoc un système autonome représenté par une vaste panoplie d'unités mobiles relayées par des liens non filaires visant à propager le concept de mobilité à toutes les unités de l'environnement sans avoir recours à une administration centralisée ni une infrastructure préalablement définie. Néanmoins, les nœuds se fluctuent d'une manière arbitraire accomplissant le rôle d'un routeur ou d'un hôte dans le réseau.

Cette définition donne un bref aperçu des réseaux ad hoc mobile qui se penchent sur les fondements suivants :

- ♣ Extensibilité du réseau.
- ♣ Autonomie du système.
- ♣ Absence d'infrastructure.
- ♣ Routage multi-sauts.
- ♣ Dynamité de la topologie du réseau.
- ♣ Variation des liaisons et des capacités des nœuds.
- ♣ Prise en charge de contraintes d'énergie.

I.5) Modélisation d'un réseau ad hoc : [BEA.06]

D'une manière plus générale, les réseaux ad hoc sont formalisés à l'aide des graphes dynamiques $G_t = (V_t, E_t)$; où :

V_t désigne les sommets du graphe qui sont les unités mobiles.

E_t illustre les arêtes du graphe autrement dit les connections existantes entre ces nœuds.

$e = (u,v) \in E_t$, signifie que les deux nœuds (u) et (v) sont directement connectés à l'instant **t**.

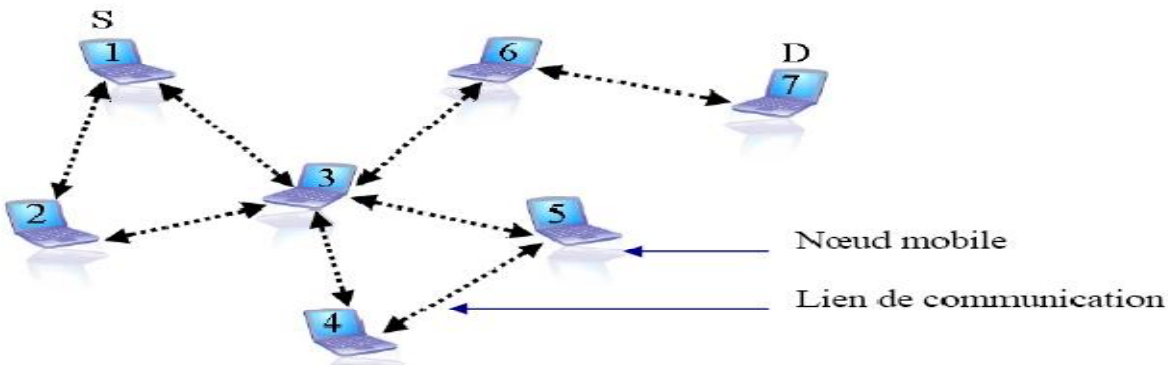


Figure 1.12 : Modélisation d'un réseau ad hoc.

Dans un réseau ad hoc où les connexions se résument par des transmissions radio, un signal n'est reçu que s'il est ***K*** fois supérieurs au bruit, typiquement ***K =10***. De plus, une autre propriété à respecter pour pouvoir modéliser ce réseau, l'atténuation des ondes radio avec la distance obtenue par la relation : $\mathbf{1/r^{\alpha}}$ où ***r*** représente la distance et $\boldsymbol{\alpha}$ est intimement lié à l'environnement tel que $\boldsymbol{\alpha=2}$ dans l'air mais susceptible à se fluctuer face à des perturbations ou des obstacles, et si on pose ***Pe*** la puissance d'émission du signal et ***B*** le bruit ambiant figé, ça implique qu'un émetteur radio du signal sera reçu jusqu'à une distance

$$\mathbf{R = (Pe/KB)^{1/\alpha}}$$

Remarque : Dans un espace homogène, α est stable.

La panoplie des emplacements permettant de recevoir le signal forme un disque centré sur l'émetteur, où cette panoplie se complique face aux obstacles (murs).

Le modèle classique est plus souple du fait qu'il révèle un graphe de disque unitaire (disk unit graph), plus précisément, une paire de nœuds du réseau ad hoc ne peut communiquer que si la distance séparant les deux nœuds soit inferieure à ***R***. De ce fait, les distances sont adaptées pour que ***R=2***, et donc un disque unitaire est centré sur chaque nœud, et deux nœuds peuvent communiquer si leurs disques s'intersectent.

Liens unidirectionnels :

On désigne par lien unidirectionnel, une liaison entre deux nœuds mais dans un seul sens uniquement.

Si le nœud A dispose d'un lien vers le nœud B, et pour que ce lien soit mis en valeur, A est recommandé d'être au courant de son existence. Ce qui résulte que B doit informer A qu'il le reçoit.

I.6) Avantages & inconvénients : [IGL.00], [SSM.03]

C Avantage :

- **A** ***Absence de câblage*** : en raison de l'absence de toutes connectivités dans un réseau Ad Hoc, il arrive que les fluctuations topologiques soient entièrement prises en charge par le réseau, ce qui résulte des données éphémères dépendantes de la nature de la mobilité.

- **A** ***Facilement déployable*** : un point opportun ornant le réseau ad hoc se révèle par l'absence d'infrastructure qui contribue grandement à une mise en œuvre souple et rapide d'un tel réseau en mettant en place plusieurs unités (nœud). Et pour de plus amples exemples on peut mettre le point sur les réseaux déployés pour couvrir les zones touchées par les catastrophes naturelles tel que les séismes.

- **A** ***Tolérance aux pannes*** : grâce à cette propriété, les unités participantes dans le réseau sont aptes à pallier aux problèmes de coupure des liaisons en réparant la panne par y emprunter d'autres chemins.

- **A** ***Coût avantageux*** : l'établissement et la maintenance d'un réseau ad hoc s'avère moins couteux que ceux d'un réseau filaire.

- **A** ***Indépendance à l'égard des points d'accès*** : la notion du point d'accès dans les réseaux ad hoc est omise puisque toutes les entités constituants ce réseau accomplissent le rôle de routeur.

- **A** ***Mobilité*** : l'absence d'une connectivité filaire confère aux entités participantes dans un réseau ad hoc l'aptitude d'une topologie hautement mouvante.

- **A** ***Extensibilité*** : si un nœud désire joindre un réseau ad hoc préétabli, il procède à une stratégie qui s'illustre par sa mise à la limitrophe d'au moins d'un nœud, néanmoins pour le quitter, il na qu'à se mettre à l'écart.

D Les inconvénients :

En contrepartie, le design des réseaux ad hoc présente des motifs inhérents ayant un impact défavorable sur les performances de ce réseau dont on trouve: la taille du réseau, la connectivité, la charge du trafic et les modèles de la mobilité.

A ce titre, les réseaux ad hoc parviennent à un nombre très important de conséquences fâcheuses comme : le routage, la gestion de la mobilité, la gestion de la puissance de calcul, la consommation de l'énergie, la qualité de service, l'interface radio et la sécurité.

A ***l'interface radio*** : les problèmes essentiels émergeant de ce point sont :

- **Ø** ***débit faible*** : ceci se révèle du fait qu'il faut attribuer une petite partition de la bande passante à la gestion du réseau alors qu'on réserve la plus grande portion aux communications.
- **Ø** ***Erreurs de transmissions*** : ces erreurs sont plus répondues à cause de la connectivité radio.
- **Ø** ***Interférence*** : elle se produit lors des transmissions parallèles des nœuds partageant un même support.
- **Ø** ***Liens*** : le triplet 'liens unidirectionnels, puissance limitée, portée limitée' contribue grandement à l'atténuation rapide des signaux.

A ***La consommation*** : les limitations des entités formant le réseau ad hoc en terme de stockage, de traitement et de capacités des batteries, les amènent à consommer d'une manière réduite l'énergie vis-à-vis son rôle délicat dans l'optimisation du fonctionnement global d'un réseau ad hoc. Parmi les facteurs provoquant une consommation excessive de l'énergie on cite le cas où autant de messages sont routés par chacun des nœuds, et dont leurs portées de communication sont très grandes.

A ***La sécurité*** : les réseaux ad hoc se manifestent par une grande vulnérabilité et une véritable difficulté de protection. Le problème montré ici est celui de la prise en charge du routage des paquets de données par les entités elles-mêmes dans de tel réseau.

I.7) Conclusion

Après avoir discuté succinctement les réseaux sans fil et les réseaux ad hoc de part quelques notions de bases, leurs technologies, leurs définitions, leurs architectures, caractéristiques, modélisation et bien d'autres points, et après avoir acquis le concept concernant leurs variabilités et leurs imprévisibilités en terme de topologie dû aux déconnexions fréquentes des nœuds, il nous parait très important d'éclaircir comment ces nœuds arrivent à relayer les paquets de données à destination, et à découvrir et maintenir les chemins de communications entre les différentes entités du réseau, ce qui souligne le cœur du sujet du notre prochain chapitre.

CHAPITRE II

LE ROUTAGE DANS LES RESEAUX AD HOC.

II.1) Introduction :

Revenant d'abord brièvement sur la définition d'un réseau ad hoc qui consiste en une population d'entités mobiles monopolisant une dissémination dynamique et arbitraire conduisant à une fréquente versatilité des interconnections entre les nœuds. A titre de cette définition, il convient que les nœuds d'un tel réseau sont capables de se détecter entre eux mais bien entendu ils sont chargés de découvrir et de maintenir des routes de communications entre ces nœuds.

Lorsque les nœuds se situent dans la même portée radio, la communication s'effectue directement de sorte que les paquets émis doivent traverser les hôtes mobiles du réseau avant d'aboutir à la bonne destination. Par contre, il arrive souvent que le nœud destinataire ne fait pas partie du territoire de communication du nœud source ce qui recommande vivement le passage par des stations intermédiaires servant de relais dans le but d'acheminer les données entre n'importe quels deux nœuds.

Gérer l'acheminement ou le routage des données dans un réseau ad hoc requiert de mettre en valeur une série de challenges spécifiques. Avant de se mettre sur le point d'étudier quelques protocoles de routage, nous allons dans un premier temps passer en revue la différence entre les deux concepts : routage et acheminement, ensuite on va détailler les principes de quelques stratégies de routage qui nous semble percutantes.

II.2) Le routage et l'acheminement :

Le routage est une stratégie servant de faire véhiculer des informations depuis une certaine source vers une destination cible à travers le réseau. Cette gestion de routage doit garantir à tout instant le meilleur acheminement des données entre n'importe quelle paire de nœuds appartenant au réseau, tout en mettant l'accent sur les différents métriques de coûts employés afin de prendre en charge la variation de la topologie et autres caractéristiques du réseau ad hoc (bande passante, nombre de liens, ressources du réseau).

De l'autre coté, l'acheminement des données s'agit de faire transiter les paquets depuis un routeur vers un autre sur la route détectée ou découverte. En d'autre terme, par exemple, l'acheminement aide fortement à la validation d'une route dans le réseau.

Dans un premier temps, ce routage peut être vu tel qu'un processus décentralisé de la sorte que chaque routeur englobe des informations sur son voisinage. Détaillons plus cette note, chaque routeur administre une liste des nœuds disponibles qui à leur tour sont conférés à un ou plusieurs nœuds voisins vers qui le message peut être transféré. Cette liste désignée par 'table de routage' peut distinguer trois sortes de routes à savoir :

- **A** Directe : le routeur achemine directement le paquet vers la destination finale et ce par le biais d'un protocole de la couche 2 (par exemple Ethernet).
- **A** Statique : elle est configurée sur le routeur par l'administrateur du réseau.
- **A** Dynamique : elle est émanée des protocoles de routage dynamiques qui s'occupe de diffuser les informations à l'égard des réseaux disponibles.

Sur ce point, une table de routage peut être optimisée de manière à maintenir la liste des nœuds directement connectés plus une route par défaut (statique ou dynamique) servant à communiquer les paquets n'appartenant pas à un réseau disponible sur la table de routage vers un routeur par défaut.

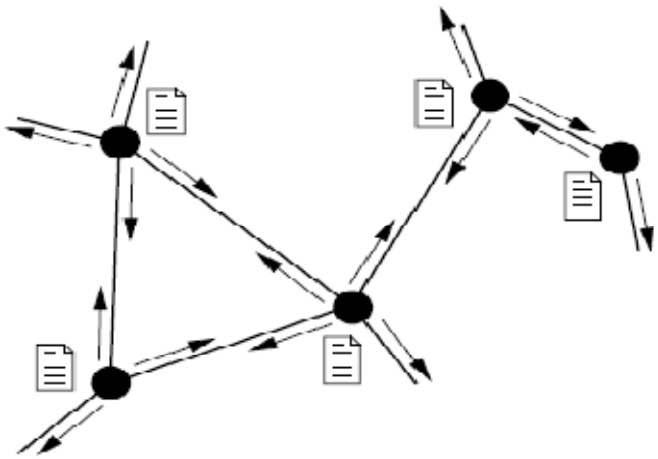


Figure 2.1: Maintien des tables de routage.

Dans un réseau ad hoc, il parait plus facile d'entamer une communication avec des équipements appartenant à un même champ de couverture. Cependant, si un dispositif désire communiquer avec un autre se situant hors de sa portée, chacun des nœuds du réseau actionne comme routeur pour son voisinage afin que les paquets parviennent à destination.

L'exemple ci-dessus donne une illustration de ce qui est dit précédemment. Lorsque le terminal A veut établir une connexion avec le terminal C n'appartenant pas à sa zone de réception, il arrive que le terminal A fasse appel à un autre terminal B qui partage obligatoirement la portée de réception des deux terminaux A et C afin que les données aboutissent à destination.

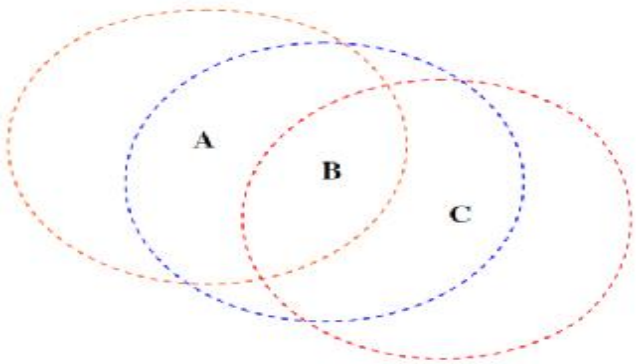


Figure 2.2 : La communication entre les nœuds.

II.3) Les méthodes de routage : [VUN.07], [JPB.00], [RAD.05]

On a mentionné plus haut que la portée des ondes radio des entités mobiles bénéficient d'une propagation limitée, et dans le but de répondre à une caractéristique intrinsèque qui dénonce qu'un réseau ad hoc doit demeurer connecté, il arrive que le terminal destination ne soit pas dans la portée de communication de nœud source, ce qui requiert de se référer à un mécanisme de routage multi-saut pour véhiculer les paquets de messages vers la bonne destination. Cette technique d'acheminement de paquets de messages, le routage, vise à employer des protocoles de routage apte à garder à tout moment les connectivités entre toute paire de nœuds du réseau.

Ces protocoles sont sensés de mettre en valeur les changements topologiques plus autres caractéristiques du réseau ad hoc tel que la bande passante, le nombre de liens, les ressources du réseau.

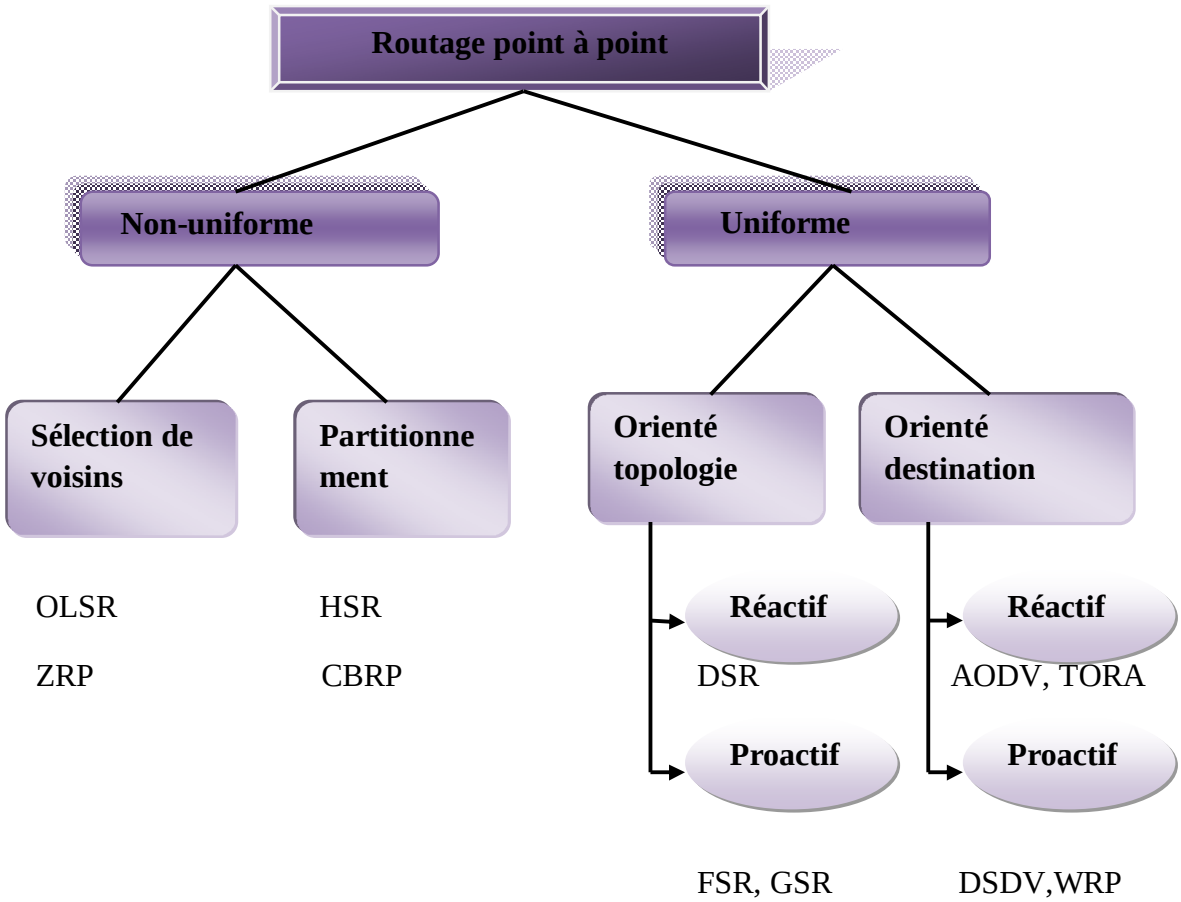


Figure 2.3: L'organisation des protocoles de routage pour les réseaux ad hoc.

Il est à noter que les études protocolaires sur les réseaux ad hoc ont fait paraitre plusieurs possibilités de classifications suivant divers critère. Et dans ses grandes lignes, les protocoles de routages peuvent être distingués selon leurs type de vision du réseau et les activités accomplies par ses nœuds (plat ou hiérarchique), ou bien selon la manière d'utiliser les données pour calculer les routes (vecteur de distance ou état de lien), ou encore par la méthode adoptée pour établir une route entre une paire de hôtes (réactive, proactive ou hybride).

II.3.1) Le routage non-uniforme : [VUN.07], [JPB.00]

Cette classification des protocoles de routage est scindée en deux parties à savoir est-ce-que les nœuds appartenant au réseau ont des rôles équitables ou pas.

II.3.1.1) Routage à sélection de voisins (plat) :

Un réseau ad hoc soulignant le mode de routage plat s'intéresse à définir une équité entre tout les nœuds du réseau de sorte que ces nœuds appartiennent à un même niveau hiérarchique et ayant les mêmes rôles et activités, par exemple le protocole OLSR.

En effet, la figure suivante donne une présentation de réseau ad hoc s'appuyant sur un routage plat et dont tous les nœuds remplissent la même tâche qui est d'acheminer l'information reçue vers le prochain nœud.

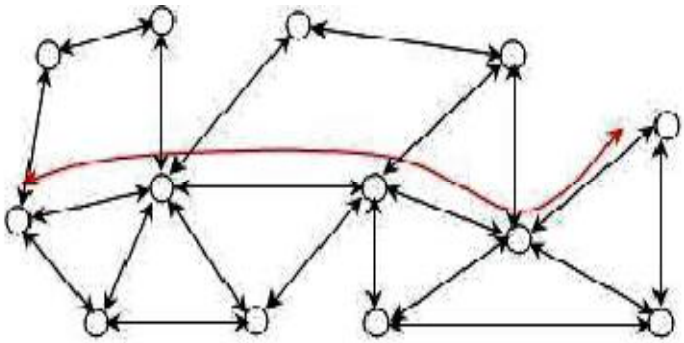


Figure 2.4: Le routage à plat.

II.3.1.2) Routage à partitionnement (Hiérarchique) :

Ici, contrairement à ce qui a été cité précédemment, les protocoles sont appelés à accorder de différentes fonctions aux hôtes du réseau, ainsi les nœuds d'une même hiérarchie remplissent les mêmes rôles et sont reliés aux nœuds du niveau plus haut. Ce type de protocole de routage s'avère intéressant dans la mesure où on a un réseau ad hoc dont quelques unes de ses hôtes n'exigeant pas de déplacements sont dotés d'une énergie assez grande, et donc ces hôtes sont considérés comme des passerelles et les autres nœuds du réseau seront liés à la passerelle la plus contigüe (par exemple CBRP).

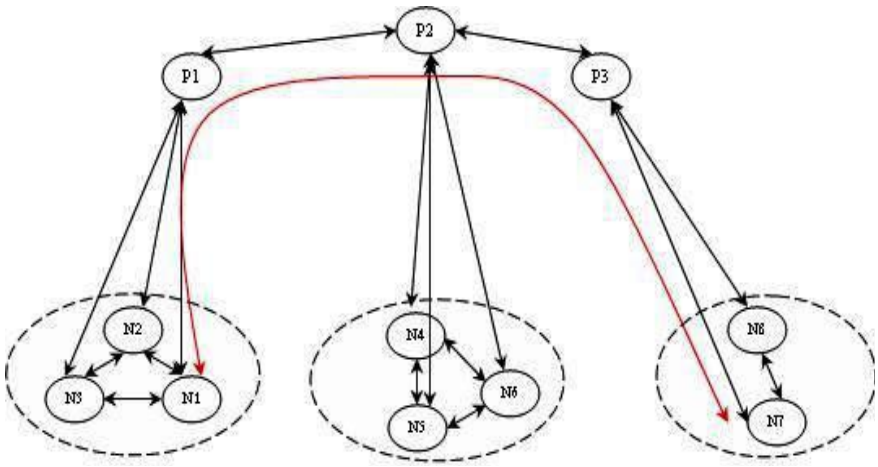


Figure 2.5 : Le routage hiérarchique.

II.3.2) Le routage uniforme : [VUN.07], [JPB.00], [GAI.08]

Le routage est l'élément de base dans le fonctionnement d'un réseau, pour cette raison et pour répondre aux attentes grandissantes de mécanismes fiables et éprouvés, il est quasiment primordial de trouver une route pour une destination et ce grâce à plusieurs méthodes de routage dont on cite :

II.3.2.1) Le routage par inondation :

Une des techniques les plus populaires de routage qui souligne une vaste trivialité, le routage par inondation, elle actionne comme suit : chaque dispositif du réseau en recevant un paquet de contrôle le retransmit à son tour à tous les autres dispositifs s'il ne s'agit pas de la destination envisagée. Et pour appréhender cette inondation, il suffit de mettre en avant une de ces techniques :

1) Le premier cas opère sur les paquets transmis en mettant en œuvre un champ de durée de vie 'time to live' qui sera décrémenté à chaque fois que le paquet est retransmit, ainsi, si le résultat est égal à zéro, cela signifie que le paquet n'est pas retransmis. Le problème qui se pose à ce stade est celui de la valeur initiale à mettre en place afin de parvenir au point destination sans avoir recours à surcharger le réseau. Certain protocoles attribuent à ce champ une valeur inferieur à 255.

2) le deuxième cas repose sur le concept d'assigner à chaque paquet un identificateur doté globalement de l'adresse de la source plus un numéro de séquence qui sera incrémenté à chaque fois que la source envoie un paquet, et ce dans le but de détecter si le paquet a déjà été reçu et empêcher sa retransmission une seconde fois sur le réseau en créant une duplication inutilement.

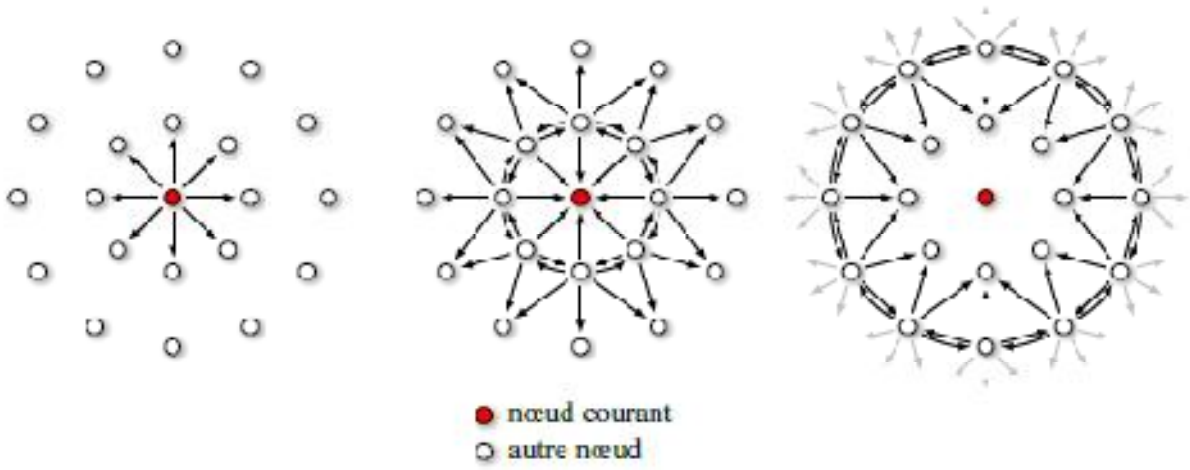


Figure 2.6 : L'émission par inondation sur le réseau.

L'émission par inondation confère un critère percutant du point qu'elle invoque parallèlement l'ensemble des chemins possible sur le réseau en intégrant ainsi le meilleur d'entre eux pour parvenir à la destination désirée. Tandis qu'il est très important de prendre en considération la surcharge du réseau due à l'énorme trafic généré qui peut toucher hautement à ses performances.

Un avantage extrêmement visible dans le routage par inondation tirant profit de la duplication accordée à l'inondation s'expose lors de la perte d'un paquet sur une route précise par la mesure d'adopter une autre route disjointe de la précédente pour que le paquet aboutisse à la destination.

II.3.2.2) Le routage par vecteur de distance : [VUN.07], [JPB.00], [GAI.08], [BEK.09]

Une deuxième technique baptisée ***'distance vector'*** reposant sur l'algorithme de Bellman-Ford Distribué, DBF, opère comme suit : toute entité du réseau est appelée à manipuler une table de routage munit de deux informations pour chaque destination : le dispositif à traverser pour aboutir à la destination ainsi le coût conjoint suivant une certaine métrique. Et par conséquent, il arrive que pour chaque dispositif du réseau, l'ensemble des adresses présentes dans la table de routage de chacun de ses attenants soit connu et atteignable par ce dispositif grâce à l'émission périodique des informations listées précédemment vers tout son voisinage.

Il est à signaler que l'information indiquant l'éruption d'un dispositif sur le réseau soit publiée très rapidement implémentant donc un algorithme de routage réactif face à l'arrivée de nouveaux dispositifs. Cet algorithme repose sur une métrique avantageuse opérant sur le nombre de sauts entre les dispositifs et offrant ainsi une importante fiabilité du fait qu'il pose la distance séparant deux dispositifs vaut '1' et en omettant tout calcul supplémentaire.

Pour de plus amples exemples, on a opté pour le réseau figuré juste après de la sorte de bien assimiler cette technique de routage en exposant l'avancement de la mise en œuvre des tables de routage comme suit :

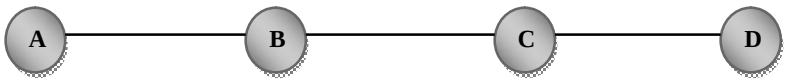


Figure 2.7 : La transmission par vecteur de distance.

Bien entendu, ici chaque hôte du réseau effectue des calculs de manière à tracer le chemin le plus optimal en nombre de sauts menant à une destination quelconque et ce en se référant aux informations cueillies par l'ensemble de son voisinage.

Hôte / N° d'échange	A	B	C	D
Initialement	Vers A : 0	Vers B : 0	Vers C : 0	Vers D : 0
1er échange	Vers A : 0 Vers B : 1	Vers A : 1 Vers B : 0 Vers C : 1	Vers B : 1 Vers C : 0 Vers D : 1	Vers C : 1 Vers D : 0
2eme échange	Vers A : 0 Vers B : 1 Vers C : 2	Vers A : 1 Vers B : 0 Vers C : 1 Vers D : 2	Vers A : 2 Vers B : 1 Vers C : 0 Vers D : 1	Vers B : 2 Vers C : 1 Vers D : 0
3eme échange	Vers A : 0 Vers B : 1 Vers C : 2 Vers D : 3	Vers A : 1 Vers B : 0 Vers C : 1 Vers D : 2	Vers A : 2 Vers B : 1 Vers C : 0 Vers D : 1	Vers A : 3 Vers B : 2 Vers C : 1 Vers D : 0

Tableau 2.1 : Progression des distances dans les tables de routage de A, B, C et D.

Une des limitations tracassant cette stratégie est la forte lenteur pour communiquer l'information concernant la rupture de liens. Et pour mieux comprendre ce problème, on procède à garder le même exemple précédent à la différence on suppose qu'une péripétie est survenue mettant en cause le dispositif A. il résulte donc que les routeurs B, C, D se bâclent de fausses informations du fait que chacun d'eux ignore que l'autre dispositif n'a pas un chemin vers A, en outre, à chaque échange le nombre de sauts augmente.

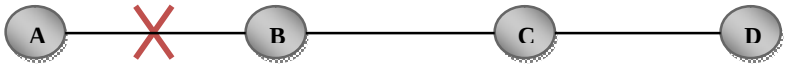


Figure 2.8 : Le problème de rupture de liens dans le routage par vecteur de distance.

Hôte / **N° d'échange**	B	C
Initialement	Vers A : 1 Vers B : 0 Vers C : 1	Vers A : 2 Vers B : 1 Vers C : 0
1er échange	Vers A : 3 Vers B : 0 Vers C : 1	Vers A : 2 Vers B : 1 Vers C : 0
2eme échange	Vers A : 3 Vers B : 0 Vers C : 1	Vers A : 4 Vers B : 1 Vers C : 0
3eme échange	Vers A : 5 Vers B : 0 Vers C : 1	Vers A : 4 Vers B : 1 Vers C : 0
4eme échange	Vers A : 5 Vers B : 0 Vers C : 1	Vers A : 6 Vers B : 1 Vers C : 0
Etc…	...	…

Tableau 2.2 : Progression des distances dans la table de routage de B et C en cas de rupture de lien entre A, B.

Et dans ce stade, une approche a été abordée pour mettre fin à cette incrémentation et de la traiter comme une coupure de lien. Cette approche s'incline à deux extrémités intrinsèques puisqu'elle emploie une valeur qui n'est que la distance entre les nœuds dans un réseau, et donc deux cas se profilent : le premier cas s'expose quand la distance dépasse le seuil de cette valeur, et comme résultat le chemin sera éliminé, paradoxalement, le deuxième cas se dévoile par l'usage d'une valeur trop petite causant ainsi la limitation de la portée maximale du réseau.

Cette stratégie découle de principe du protocole RIP qui a été déployé au départ d'internet, axant sur des réseaux avec une portée limitée. Un souci névralgique heurtant cet algorithme issu de la convergence des informations lors de la disparition d'un routeur, coupure de lien, a mis en cause le routage par vecteur de distance et suscitant ainsi une nouvelle méthode centrée sur le routage par état de lien.

II.3.2.3) Le routage par état de lien : [VUN.07], [JPB.00], [BEK.09], [GAI.08]

Le concept du protocole *'Link state'* essaie d'étendre la notion qui vise à ce que tout les nœuds doivent être en mesure de garder leurs propre connaissance concernant la topologie complète du réseau ainsi l'état de leurs liens. En outre, bien que cette connaissance soit fiable, elle a recours à un double processus local et global : un tout premier dont son rôle est de recueillir une vision locale de réseau tandis que le second se focalise sur la dissémination de l'ensemble des visions locales sur le réseau créant ainsi une vision globale qui n'est que la topologie du réseau.

Si un nœud désire connaître ses proches, il n'a qu'à répandre un message de type ***HELLO*** sur toutes ses interfaces, ensuite tout nœud réceptionnant ce type de message émis une réponse qui permet au nœud initial d'être au courant de nœuds ayant reçus le message, et arbitrairement ses voisins. Et d'une manière régulière, on procède à la répétition de ce processus pour prendre en charge la versatilité de l'état de liens suite à l'apparition ou à la disparition d'un nœud voisin dans le réseau.

Comme dans le routage par vecteur de distance, le routage par état de lien opte pour une métrique du coût de lien entre une paire de nœuds qui se résume soit par le nombre de sauts ou par une autre mesure tel que le débit des liens.

Arrivant à ce stade, l'ensemble des informations collectées par chaque nœud portant sur ses nœuds voisins ou sur les coûts des liens le menant à ceux-ci sont mises dans un paquet d'état de lien qui à son tour sera générer par inondation sur tout le réseau. Ce processus enclin une répétition périodique apte à sortir de l'ordinaire en ne respectant pas l'intervalle, à cause de la péripétie des nœuds voisins en joignant ou quittant le réseau.

Il semble donc important que tous les nœuds recevant les informations à propos de l'état des liens, doivent mettre à jour leurs visions topologiques du réseau et appliquant une stratégie garantissant à tout moment le meilleur chemin, le plus court, en destination vers tous les autres nœuds se trouvant dans le réseau.

Le critère de choix le plus souvent sollicité pour avoir le chemin le plus optimal est l'algorithme du Dijkstra qui se résume par la détermination du plus court chemin relayant une source à une destination donnée, et ce par le biais d'une image absolue de la topologie dans chaque nœud du réseau illustrée par les récentes mises à jour des liens de tout les nœuds contribuant au routage.

Parmi les protocoles monopolisant la philosophie 'état de liens' les plus adoptés est le protocole OSPF (Open Shortest Path First).

II.3.3) Le routage géographique :

Une autre catégorie des protocoles de routage nommée géographique, s'articulant autour des informations de localisation externe (obtenues par GPS ou autre) et/ou autour de la position des nœuds pour découvrir des routes. Ce protocole s'appuie sur une méthode triviale de mise en service, qui s'illustre par une simple transmission d'un message sur tout le réseau incluant l'identifiant du nœud destinataire et celui concernant sa localisation, ainsi, uniquement le ou les nœuds s'avérant le plus proche géographiquement de la destination donnée le réémettront.

II.3.4) Le routage réactifs & proactif [AMF.07], [BEK.09], [GAI.08]

On peut noter dans cette classification que les protocoles sont scindés en trois grandes familles en s'articulant autour de la périodicité de calcul des routes. Elle regroupe les protocoles proactifs calculant les routes à différents intervalles, les protocoles réactifs calculant les routes à la demande i.e. au moment où le message doit être propager par le dispositif, et les protocoles hybrides qui représentent une combinaison de ces deux protocoles.

1) **Les protocoles réactifs** : le contrôle et les mises à jour se réalisent à la demande, autrement dit, le chemin est découvert à la demande (AODV, DSR, TORA).

2) **Les protocoles proactifs** : la procédure de création et de maintenance des routes durant les transmissions des données sont contrôlés périodiquement, autrement dit, les tables de routage sont construites avant que la demande en soit effectuée (OSLR, DSDV, WRP).

3) **Les protocoles hybrides** : c'est La combinaison des protocoles proactifs et réactifs (ZRP).

II.4) Le concept de nouveaux protocoles de routage :

Le besoin proliférant à l'égard de proposer de nouveaux protocoles pouvant endosser les handicaps de leurs précédents à savoir :

- **A** Une image globale de la topologie du réseau n'est pas obligatoirement requise ;
- **A** Une prise en charge de la mobilité accrue des nœuds (la forte convergence) ;
- **A** Une précision de nombre de messages de signalisation à propager ;
- **A** Une scalabilité des algorithmes est fortement recommandée ;

préconise vraiment le succinctement d'autres protocoles s'accentuant sur l'optimisation de colonie de fourmis largement inspirés des stratégies hybrides.

II.5) Protocole de routage basé sur le fonctionnement des colonies de fourmis : [ALI.09]

Une idée qui vient à l'esprit des chercheurs à propos de proposer une autre organisation des réseaux s'imprime par l'étude comparative du comportement collectif et intelligent des insectes qui se penche sur des interactions simples et microscopiques. Ainsi, l'excellent exemple à mettre en avant est celui des colonies de fourmis.

Vue que les fourmis vivent dans des communautés, chacune d'elle est sensée d'accomplir un comportement collectif et collaboratif. Ce comportement répond en termes de la distribution accrue du fait que chaque individu de la colonie soit indépendant et absolument non contrôlé, et en termes de l'hétérarchie, la contrepartie de l'hiérarchie, qui se dévoile par le fait que chaque individus demande du l'aide de sa colonie lors de sa progression et en retour il contribue à perfectionner le fonctionnement de celle-ci.

A l'issue de cette description, les chercheurs ont adoptés une nouvelle technique de routage au sein des réseaux ad hoc, l'algorithme de contrôle et d'optimisation, et ce par le biais d'une projection conférant le comportement autosupervisé des communautés de fourmis aux caractéristiques des réseaux ad hoc et précisément au moment du leurs calcul des routes.

II.5.1) Algorithme de fourmis de base : [RMA.08], [BON.08]

L'intégration d'algorithmes novateurs se focalisant sur une méthode de communication indirecte, ***stigmergie***, opérant comme intermédiaire au sein d'un environnement subissant des fluctuations locales a aidé hautement à combler les lacunes des réseaux ad hoc. En partant du nid vers la source de nourriture et vice-versa incidemment, les fourmis laissent une substance odorante sur leur trajet, appelée la phéromone, contribuant ainsi à la création d'une branche qui leurs permettent de s'y détectaient. Du fait que les phéromones jouent le rôle d'un repère, les fourmis ont recourt à opter pour la route ayant la plus haute concentration de phéromones qui leur permettent d'obtenir le trajet dirigeant à leur nid lors du retour. Ainsi, les autres fourmis utilisent leurs antennes pour capter les odeurs afin de trouver les sources de nourriture déjà découvertes.

Ce processus aide énormément les fourmis quand toute la communauté emploi les branches de phéromones à découvrir le meilleur chemin vers la source de nourriture. Plus précisément, si une fourmi constate l'existence d'autant de chemins menant à la destination, elle effectue son choix en adoptant la plus courte branche, ce qui résulte la naissance d'une nouvelle couche de phéromone sur la branche sélectionnée en devenant la plus alléchante.

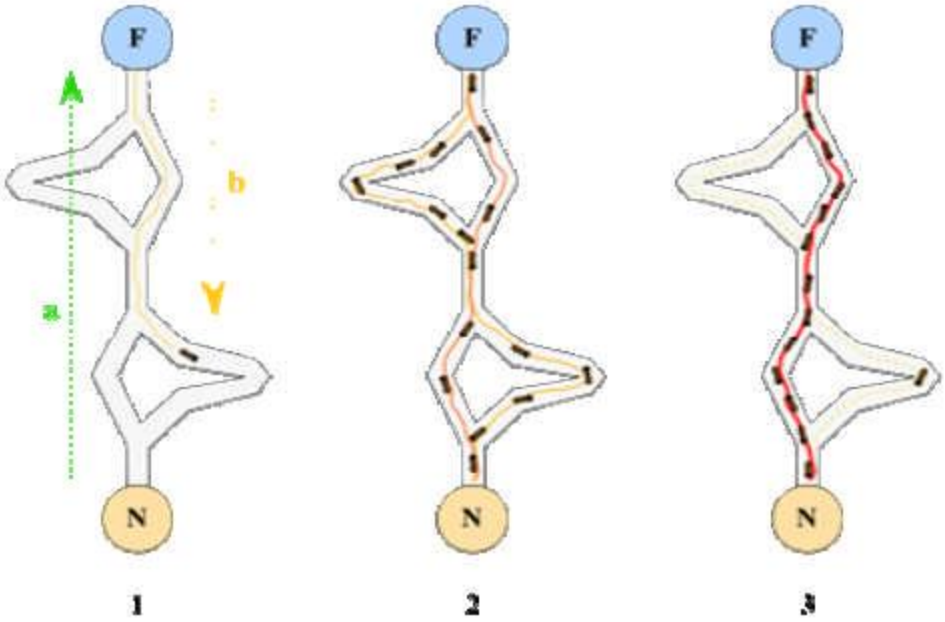


Figure 2.9 : La recherche de nourriture par les fourmis.

Cette figure met l'accent sur la procédure mise en avant par les fourmis afin de rechercher la source de nourriture dont elle s'illustre comme suit :

1) La première fourmi découvre la source de nourriture (F) en empruntant une route quelconque (a), ensuite retournant vers le nid (N) et laissant derrière elle une trace de phéromone (b).
2) Les fourmis optent pour arbitrairement les quatre routes possibles, or que le renforcement de la trace s'évertue à rendre plus attirant le plus court chemin.
3) Les fourmis en parcourant le chemin le plus optimal mettent en cause leurs traces de phéromones des parties longues des autres chemins.

Du fait que les fourmis fréquentent largement le plus court chemin, il en résulte que les dépôts de phéromones deviennent plus volumineux et intéressants par la majorité de leurs consœurs. Ce court chemin sera de plus en plus choisi jusqu'à ce qu'il sera emprunté par la totalité des fourmis, et se termine par être la route principale.

II.5.2) Les fourmis virtuelles vs réelles :

Une étude synthétique des fourmis virtuelles vs des fourmis réelles donne lieu à une série de conformités et de différences, dont on présente un concis aperçu sur.

II.5.2.1) Les ressemblances :

‼ ***Une coopération accrue*** : les fourmis virtuelles se comportent comme des fourmis réelles dont chaque groupe de fourmis doit participer à résoudre le problème confronté en proposant une meilleure solution ou même une mauvaise.

- ***Moyen de communication*** : les pistes de phéromones sont le seul médiateur de communication entre les fourmis.
- ***Mécanisme d'évaporation*** : il met en cause les décisions déjà prises dans le temps, modifié l'information phéromone, au profit d'une recherche vers de nouvelles directions.
- ***Plus court trajet*** : les deux catégories des fourmis essayent de trouver la plus courte distance séparant leurs nids de leurs sources de nourriture.
- ***Déplacements*** **:** une équité entre les deux colonies exige que les fourmis ne doivent pas séchées les étapes adjacentes du terrain.
- **Décision de transition** : les fourmis réelles et virtuelles quand elles sont sur un site, sont appelées à effectuer incidemment un choix sur quel site adjacent se transiter. En plus, cette décision probabiliste est strictement liée aux dépôts locaux des phéromones sur le terrain courant.

II.5.2.2) Les différences :

- ***La mémoire*** : les fourmis artificielles retiennent en mémoire toute les détails de leurs comportements ainsi d'autre informations concernant leurs performances, or que les vraies fourmis sont bornée en mémoire.
- ***Nature des phéromones*** : les vraies fourmis manipulent des informations physiques à déposer sur leur terrain parcouru, tandis que les fourmis artificielles changent les informations contenues dans leurs variables d'états qui seront décrémentés après chaque itération par l'évaporation des phéromones.
- ***Qualité de solution :*** la qualité de la solution que proposent les fourmis artificielles s'évertue à être proportionnelle à la quantité de phéromones déposées.
- ***Délai d'attente :*** les fourmis virtuelles patientent jusqu'à ce qu'elles finissent le choix de leurs solutions pour mettre à jour les pistes de dépôts de phéromones.
- ***Autres capacités*** : au sein des fourmis virtuelles, il s'avère possible qu'une fourmi puisse retourner sur un état déjà parcouru en cas de mauvaise décision comme elle peut anticiper les prochains états en plus de son état local afin d'effectuer son choix.

II.5.3) L'exposition du problème [ALI.09]:

L'algorithme méta-heuristique (ACO) fondé par Marco Dorigo, est une adaptation d'heuristique très récente destinée à concevoir des stratégies pour les problèmes d'optimisations combinatoires basées sur le fonctionnement des fourmis.

Le problème d'optimisation combinatoire peut être formulé par un graphe G= (V, E) dont sa résolution consiste en l'ensemble des chemins réalisables de G. l'objectif majeur de l'algorithme ACO réside dans la capacité de déterminer un chemin opportun, une séquence d'arcs avec un coût réduit, tout en mettant en avant les contraintes.

Solutionner ce problème revient à préconiser la coopération de tous les individus de la communauté de fourmis en procédant le codage des informations cueillies le long de leurs parcourt sur le graphe sous forme de phéromone artificielle. Ainsi, les informations heuristiques qui peuvent présenter sur les arcs du graphe plus les informations phéromones, sont employées pour déterminer les règles probabilistiques.

II.5.4) L'algorithme ACO:

Concevoir des algorithmes de fourmis pour le routage est une approche adaptée afin d'obtenir des informations de routage à partir des chemins empruntés en se référant aux petits paquets de contrôles appelés fourmis (Ant). D'une manière libre et parallèle ces derniers sont émis depuis des nœuds pour évaluer le trajet liant le nœud source S à la destination D. Ainsi, un paquet fourmi recueille les informations de qualité concernant le trajet parcouru afin de les employées lors de son retour depuis le nœud destinataire D vers le nœud source S, néanmoins, il met à jour les informations de routage du nœud source S et tous les nœuds médiateurs entre S et D.

Il est à noter que les individus, les fourmis, retirent à chaque fois des chemins entiers où leurs informations de routage sont mises à jour sans se souciés de l'information figée d'un nœud vers le prochain.

A chaque entrée dans la table de routage est associé un vecteur de valeurs réelles dont chaque valeur représente un nœud voisin précis. Ces entrées servent à mesurer la meilleure qualité du trajet parcouru jusqu'à la destination grâce à un nœud voisin bien connu. On désigne par variables de phéromones ces valeurs qui sont mises à jour continuellement en fonction de la qualité du trajet calculé par les fourmis. A l'égard de la concurrence et l'itération signées par les fourmis lors de l'extraction du chemin, il arrive que chaque nœud dispose d'un ensemble de chemins représentant un niveau de qualité estimée. En outre, les fourmis se penchent sur les tables de routage pour déterminer la route vers la destination, ainsi, au niveau de chaque nœud, ils optent pour le prochain saut en fonction des liens et des valeurs de la phéromone en se contentant le plus de choisir la probabilité la plus importante.

A l'issue de cette heuristique, nombreux sont les protocoles de routage conçus pour les réseaux MANETs, à titre d'exemple on cite : ***Ant AODV***, ***ARA*** (Ant-Colory Based Routing Algorithm For MANETs), ***PERA*** (Probabiliste Emergent Routing Algorithm), ***ANODR*** (ANonymous On Demand Routing), et ***AntHocNet*** (An Adaptative Nature Inspired Algorithm For Routing in Ad hoc Networks), et enfin ***AntTrust*** qui fera le sujet d'une étude détaillée le long de la deuxième partie de ce travail.

II.6) Le problème du routage dans les réseaux ad hoc :

Etant donné qu'un réseau ad hoc est une collection de dispositifs mobiles, dynamiquement et incidemment disséminés de façon que l'interconnexion entre les nœuds soit mouvante, il vient alors qu'un dispositif destination se trouvant en dehors du périmètre de la communication du dispositif source, nécessite l'intervention d'un routage interne via des nœuds intermédiaires servant de faire parvenir les paquets de message à la bonne destination.

La variation continuelle de la topologie des réseaux ad hoc due essentiellement au nomadisme des nœuds tracassant la problématique qui se résume par une question très délicate : quelle méthode de routage à la lumière d'un contexte se caractérisant par une grande capacité de calcul et de sauvegarde devrons-nous adapter ?

En effet, il est quasiment impossible qu'un nœud se trouvant dans un réseau aussi volumineux, puisse maintenir les informations de routage concernant tous les autres nœuds du réseau.

II.7) Les limitations de routage dans les réseaux ad hoc : [SSM.03], [BAN.00]

Un souci majeur intimement lié aux réseaux ad hoc de part leurs caractéristiques se montrant par une fréquente déconnexion des nœuds et une expansion dynamique de leurs environnements, s'illustre par la conception et la réalisation des algorithmes de routage plus fiables qui doivent confronter les problèmes donnés ci-dessus :

- ***La contrainte de la charge du réseau :*** minimiser les ressources d'un réseau ad hoc revient à se mettre devant deux sous problèmes à éviter : le premier est celui des boucles de routage, et le deuxième est la concentration du trafic autour de certains nœuds ou liens.
- ***La contrainte de la communication multipoint*** : garantir un routage efficace des paquets de données vers la bonne destination sans égard pour la fluctuation des chemins, ainsi en cas où un chemin est annulé pour une panne ou une mobilité, il est quasiment recommandé d'optimiser au maximum les temps de latence.
- ***La contrainte du routage*** : établir d'optimales routes et supporter divers métriques de coûts (bande passante, nombre de chemins, ressources du réseau) doit être la cible des algorithmes de routage. Du fait que la découverte de chemins fiables s'avère trop difficile résulte que la maintenance de ces chemins devienne de plus en plus délicate, et ainsi les stratégies de routage adoptées doivent répondre en terme d'une optimale maintenance et d'un faible coût.
- ***La contrainte du temps de latence :*** l'augmentation de la connectivité du réseau implique l'augmentation des temps de latence et des chemins.

II.8) Classification des protocoles de routage : [FSA.10],[SSM.03],[GLF.09]

Bien entendu, le routage est une méthode à travers laquelle les informations se transitent depuis un certain émetteur vers un destinataire bien déterminé. De ce fait, le routage présente un vrai défit qui retire l'attention de plusieurs sujets de recherches, au moment où le problème de routage ne se restreint pas essentiellement à élaborer un chemin entre deux unités mobiles du réseau, mais aussi à mettre au point le chemin le plus optimal et de qualité.

L'objectif principal envisagé par la stratégie de routage est de résoudre les problèmes d'acheminement des données, et ce par la mise en valeur d'une bonne gestion d'acheminement de données, robuste et efficace. A ce titre, les travaux sont scindés en trois grandes classes qui sont :

II.8.1) Les protocoles proactifs :

Les protocoles de routages proactifs des réseaux ad hoc sont largement inspirés des protocoles de routage des réseaux filaires classiques déclinant deux principales techniques qui sont : la méthode « état de lien » (Link state) et la technique « vecteur de distance » (distance vector) détaillées plus haut. Les protocoles de routage s'articulant autour de ces deux techniques qui sont sensées implicitement de mettre à jour les paquets de données de routage et les diffuser par la suite par les différents entités de routage participant dans le réseau, s'appuient sur une stratégie paritaire qui tente à sélectionner le plus court trajet. Dans la majorité des cas, où les liens de communications ont des coûts identiques, le plus court chemin séparant deux entités du réseau est obtenu par le nombre de nœuds ou de sauts formant les différents chemins existant entre les stations source et destination.

Ce concept a fait paraitre deux types de paquets de contrôles mettant en évidence la construction de la topologie du réseau d'une manière distribuée :

1) les paquets de contrôles sont relayés avec un seul saut pour découvrir leurs voisinages.
2) les paquets de contrôles sont diffusés par inondation dans tout le réseau pour passer les informations concernant leurs voisinages aux autres nœuds.

Un nœud, en recevant un paquet de contrôle, mis à jour ses tables de routages et en fonctions des informations contenues dans les trames de contrôles, il établit d'autres nouveaux chemins. On procède à répéter ce processus à chaque fois que la topologie du réseau change afin de rétablir de nouvelles routes.

II.8.1.1) Le protocole DSDV:[BAN.00]

Dans l'objectif d'endosser les changements topologiques au cœur des réseaux ad hoc, le groupe MANET lança un de ses premiers protocoles proactifs orienté destination dédié à échanger d'une manière régulière des paquets de contrôles pour maintenir les vecteurs de distance (tables de routage), DSDV, populaire sous le nom Distance Vector Protocol, bâti sur l'algorithme de Bellman-Ford. Et comme son nom l'indique, il opère en supposant que tous les entités du réseau propagent une image de leur table de routage, vecteur de distance, qui est attribué à une entité du réseau signalant les autre entités qui lui sont atteignables ainsi le nombre de sauts nécessaire pour accéder à ces entités du réseau.

S'étalons plus sur cette note, chaque entité DSDV, dissémine à des intervalles du temps réguliers une copie de son vecteur de distance vers les entités se situant dans sa portée de transmission. Lorsqu'un nœud reçoit ce vecteur, il procède à comparer le coût ou le nombre de sauts recommandé par le vecteur de distance réceptionné qui permet d'y parvenir à chaque entité avec celui précisé dans sa propre table de routage. A l'issue de cette comparaison, si le nœud mis en œuvre reçoit un vecteur de distance avec un coût plus optimal que celui existant dans sa table de routage locale, il procède à mettre à jour cette dernière. Et par conséquent, ce nœud devrait publier cette table de routage modifiée lors de la diffusion de son propre vecteur de distance.

Or que le protocole DSDV a fait paraitre un souci important qui se présente dans la lente convergence des tables de routage causé par une double raison, la première est dû au fait que les vecteurs de distance établissent des échanges asynchrones, et la deuxième réside dans le coût d'une route, i-e, un même nœud publiant deux routes, il arrive qu'une route dotée d'un coût avantageux sera remplacé par une route avec un coût plus onéreux.

Retraçant succinctement ce problème en mettant en place un réseau constitué de trois entités A, B, C de sorte qu'il y'a un lien de communication bidirectionnel entre A, B et entre B, C. Le nœud A en recevant le vecteur de distance de B met à jour sa table de routage, et donc il peut atteindre le nœud C en deux sauts. Si pour une raison la route liant B à C est rompue, le nœud B supprime cette route de sa table de routage. En revanche, le nœud B en recevant le vecteur de distance émis par A, il met à jour sa table de routage en indiquant que le nœud C est à trois sauts, ce qui est absolument erroné du fait que C est devenu inaccessible. Et quand A reçoit le vecteur de distance transmis par B, il modifie sa table de routage de façon que C sera atteignable avec quatre sauts. Sur le plan pratique, une boucle s'est créée entre les deux nœuds A et B émanant des problèmes de la lente convergence des tables de routage. Ce défaut de DSDV intimement issu du protocole RIP (Routing Information Protocol) employé pour le routage dans les réseaux filaires, sera résolu en proposant de nouveau protocoles tel que OLSR (Optimized Link State Routing), TBRPF (Topology dissemination Based on Reverse-Path Forwarding) qui se reposent sur le principe du OSPF (Open Shortest Path First).

II.8.1.2) Le protocole OLSR: [GAI.08],[ABR.09],[RAD.05],[TAB.07]

Le protocole abordé dans cette section consiste en une dérivée inspirée des protocoles du type LSR (Link State Routing) mené dans les réseaux classiques. Ce protocole proactif s'appuie sur le concept du MPR (Multi Point Relay, Relai Multi Point) qui procède à designer les entités s'occupant de diffuser le message, ainsi, les autres nœuds du réseau sont appelés à sélectionner ces MPR. En effet, ce protocole introduit deux types de messages : HELLO, TC. En outre, une paire de nœuds se focalise sur un état de lien susceptible de fluctuer à l'instant des échanges de messages entre les nœuds dont on marque : unidirectionnel, bidirectionnel et inexistant.

- **Message HELLO :** Ce type de message est bâtit sur des échanges à intervalles réguliers avec son voisinage, or que la notion de propagation est omise dans ce contexte. Un message HELLO renferme des informations concernant l'état des liens à propos de ses nœuds voisins organisées sous forme d'un triplet comportant une liste précisant les dispositifs à liens unidirectionnels, et une autre les dispositifs à liens bidirectionnels ainsi une toute dernière prend en charge les nœuds MPR issus du nœud initiant le message.
- **Message TC (Topologie Control) :** Ce type de message est diffusé sur tout le réseau par inondation dans le but de préciser l'état global du réseau.

Remarque : Certains protocoles sécurisés emploient les informations répétées introduites dans ces deux types de messages pour des fins de contrôle.

- **Sélection des nœuds MPR :**

Il est très utile de souligner qu'un nœud ***MPR*** est sensé de véhiculer les informations transmises par un des nœuds ***MPR*** sélecteurs l'ayant choisi comme ***MPR*** dans l'objectif de garantir la diffusion des messages dans le réseau. Perfectionner ce processus revient à opter pour une technique convenable portant sur la manière de choisir les nœuds ***MPR*** par un nœud, et qui se présente comme suit : en fonction des massages ***HELLO*** reçus, chaque nœud aura connaissance de tout les autres nœuds atteignables par uniquement deux sauts. Et ce en introduisant une stratégie d'optimisation qui dénonce que chaque nœud opte pour un nombre minimum de nœuds avec un saut permettant d'atteindre tout les nœuds pouvant être accéder par le biais de deux sauts, ensuite, on procède par récursivité pour que tout le réseau soit couvert.

L'algorithme adopté dans ce contexte ne répond pas en termes d'optimisation, surtout en cas des choix aléatoires, néanmoins, il doit garantir que chaque nœud du réseau soit couvert entièrement.

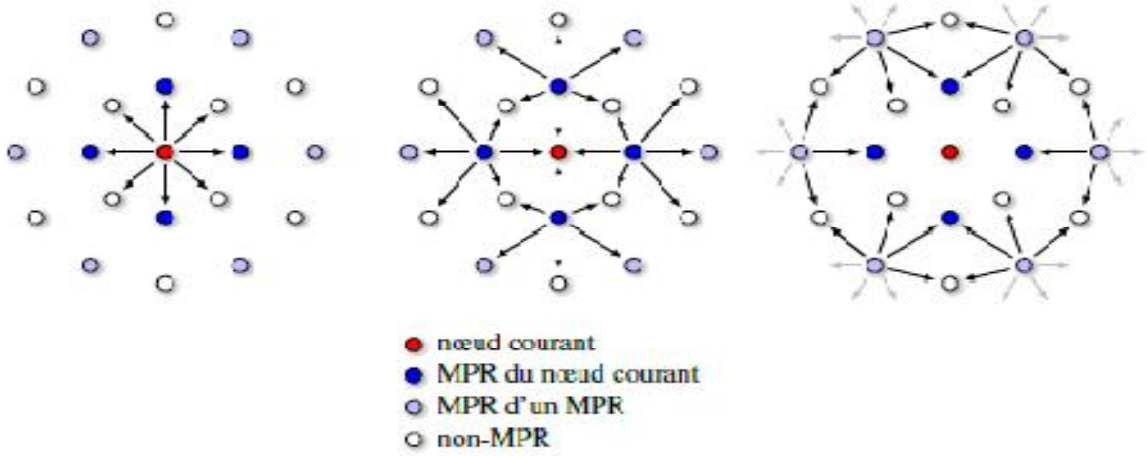


Figure 2.10 : Une diffusion optimisée sur le réseau.

II.8.2) Les protocoles réactifs :

Le groupe de travail MANET s'est intéressé actuellement au problème de routage dans les réseaux ad hoc, et le fruit de cette étude se souligne par la proposition de cet axe de protocoles de routage qui construisent les routes une fois le dispositif initial déclenche une demande de découverte de routes vers une destination cible.

Les protocoles de routage réactifs également nommés protocoles à la demande (on demand) se manifestent récemment dans l'objectif de garantir un service de routage dans les réseaux sans fil. A la différence des protocoles proactifs, cette classe de protocoles génère assez moins de messages de contrôles, de plus les informations incluses dans les tables de routage ne sont pas modifiées régulièrement et ne sont valide que pour une période bien précise, au moins une fois, connue par la durée de vie de la route. En outre, la découverte d'un trajet peut être scindée en deux phases essentielles, en la première phase, une requête de localisation est émise sur le réseau, et la seconde phase consiste à collecter les réponses reçues. Selon le contexte d'emploie, nombreux sont les protocoles de routage réactifs. On cite :

II.8.2.1) Le protocole DSR : [MRN.06]

DSR (Dynamic Source Routing) est un protocole de routage qui s'incline à un processus esquissant au moment où un nœud source désire router un paquet de données à un nœud destination alors que ce premier ignore le chemin menant à cette destination. À cet effet, il lance une recherche en diffusant une requête de type ***Route Request (RREQ)*** pour découvrir une route, ***Route Discovery***.

Plusieurs éléments définissent un message ***Route Request*** : l'adresse du nœud émetteur, l'adresse du nœud destinataire, un marqueur servant à identifier la découverte de routes ainsi une liste qui est vide au départ destinée à contenir les nœuds intermédiaires. A chaque fois qu'un nœud intermédiaire reçoit ce message, il vérifie s'il ne lui en est pas destiné et si sa table de routage ne mentionne pas le chemin désiré du nœud en question, si c'est le cas, lui aussi diffuse le message de type ***Route Request*** en lui insérant son adresse dans la liste des nœuds intermédiaires.

Si le nœud intermédiaire dispose d'un chemin vers le nœud cible dans sa table de routage, il retourne au nœud émetteur ce chemin encapsulé dans un message de type ***Route Reply (RREP)***. Sinon, il effectue les mêmes traitements que précédemment et ce jusqu'à ce que le nœud destinataire reçoit le paquet de requête. A cet instant, il fait l'objet d'un acquittement en générant un message de réponse ***Route Reply*** qui passera par tous les nœuds intermédiaires de la liste.

Au moment où le nœud initiant la découverte de route reçoit l'acquittement du message de réponse, il va mettre à jour sa table de routage avec la liste des nœuds intermédiaires accompagnée d'un coût. Ce dernier peut référencier le nombre de nœuds intermédiaires passé par le message de réponse, le débit, la fiabilité des liens ou la taille des messages. Ce qui revient à favoriser le choix d'un chemin parmi plusieurs aboutissants à une même destination.

A chaque fois que le nœud initiateur détecte l'existence d'un autre chemin menant à cette destination avec un coût plus avantageux, il met à jour sa table de routage en introduisant cette route. D'autre part, et lors de l'établissement d'une route, il est recommandé que les algorithmes de routage mettent en place des mécanismes de maintenance des routes afin de pallier aux événements survenus tel que la coupure d'une liaison entre deux nœuds à travers lequel passent les messages.

Il peut arriver qu'un nœud ne puisse pas transmettre un paquet de données vers une certaine destination, à ce moment, il génère un message d'erreur de type ***Route Error (RERR)*** pour le nœud source du paquet de données comme il détache cette route de la table de routage

Voici une image manifestant la procédure de découverte d'une route lorsqu'un dispositif initial S veut transmettre un paquet vers un dispositif destination D, or que le nœud S n'a pas connaissance du trajet vers le nœud D.

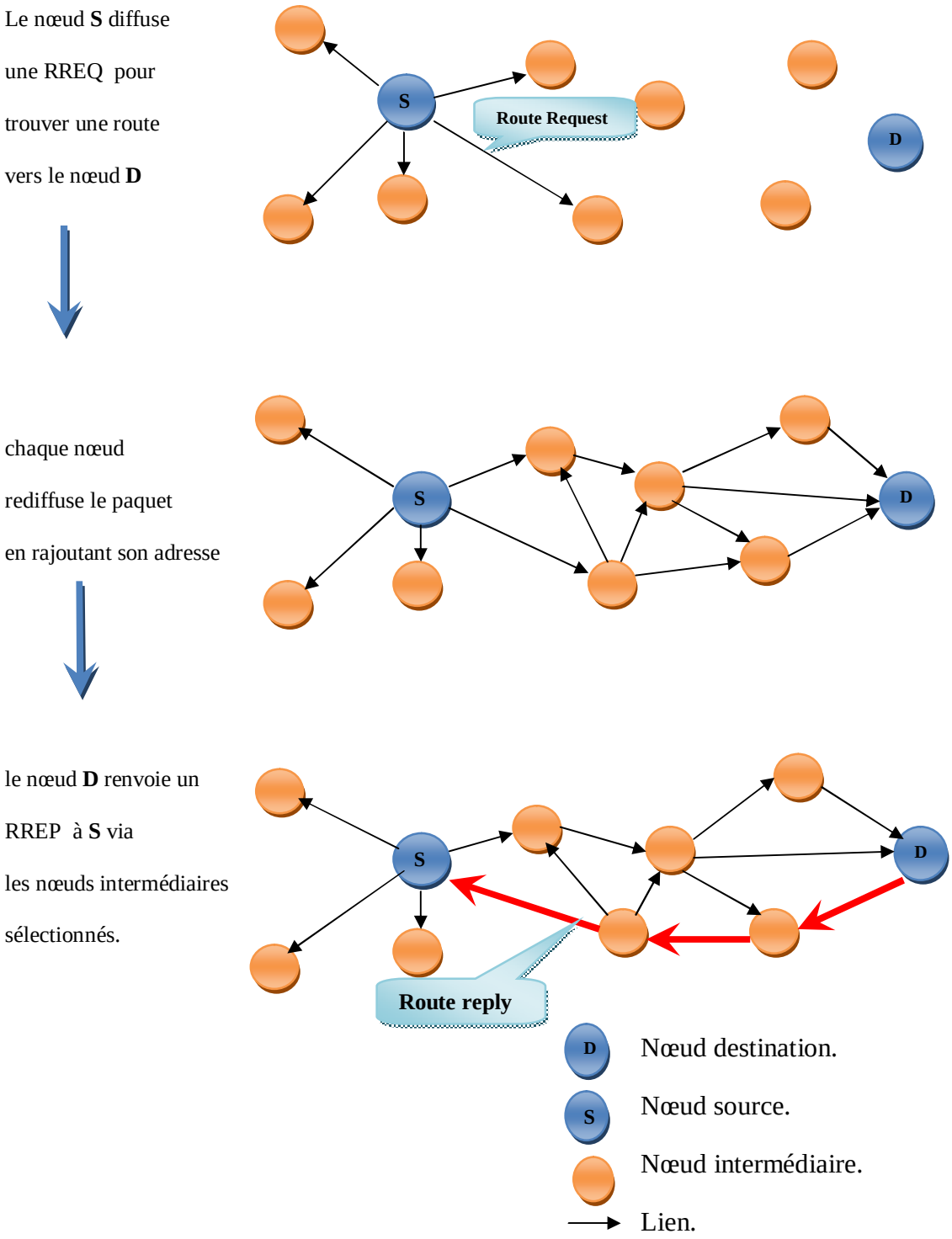


Figure 2.11 : La découverte de route dans les réseaux ad hoc.

II.8.2.2) Le protocole AODV : [LAA.02], [BAN.00]

L'AODV (Ad-hoc On Demand Distance Vector Routing) est une amélioration du protocole réactif DSR qui réagit bien avec une densité et une mobilité des nœuds non très importante. Notons aussi que AODV réduit le trafic du contrôle en ce qui concerne la taille des messages et le nombre de messages générés, ainsi, un nœud AODV ne stocke que

l'identifiant du nœud suivant, qui est dans sa portée de transmission, permettant d'acheminer le paquet vers la destination.

Le processus de localisation d'un nœud est effectué comme suit : un nœud AODV quand il ne stocke pas la route menant à une certaine destination, émis une requête de localisation sur le réseau munie de l'identifiant de la source et de la destination. Un nœud intermédiaire AODV conserve l'adresse du nœud source initiant le processus de localisation et l'adresse du nœud intermédiaire ayant émis le paquet, dans le but de réussir à faire transiter la réponse vers le nœud initiant ce processus. Arrivant sur ce point, un nœud AODV est face à deux situations se différenciant par la disponibilité ou non de l'information de routage. Quand le nœud ne dispose pas d'informations lui permettant d'accéder à la route demandée, il retransmit la requête (**RREQ**) de localisation sur le réseau sans lui introduire des modifications, mais lorsque le nœud intermédiaire possède l'information de routage, il achemine la réponse au nœud source. Il est à noter que le message de réponse (**RREP**) dispose de l'identifiant de la destination, puis chaque nœud intermédiaire, ayant reçus ce message de réponse de la source pour générer la requête de localisation, transmis le paquet vers le nœud intermédiaire suivant en supprimant l'adresse du prochain nœud intermédiaire de la table de routage.

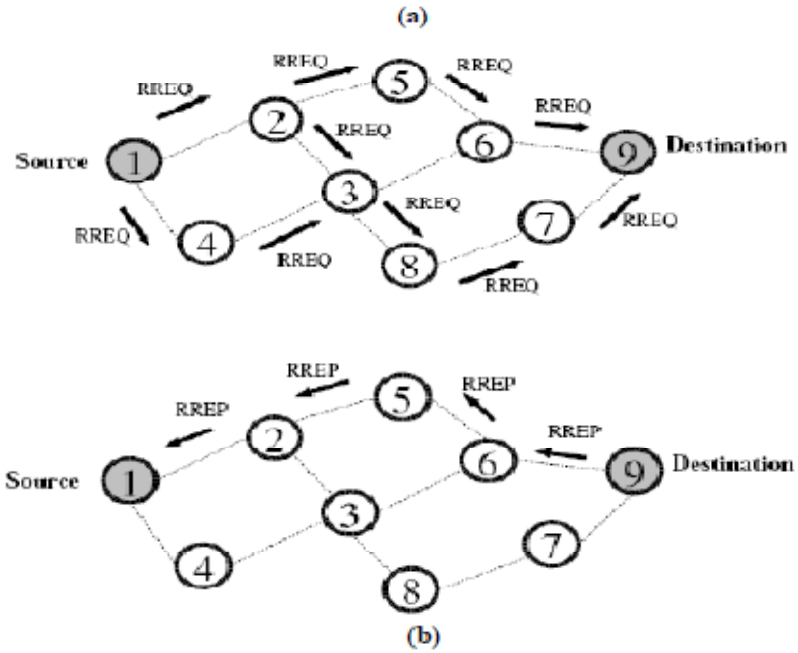


Figure 2.12 : (a) inondation de RREQ, (b) renvoie du RREP dans AODV.

II.8.3) Les protocoles hybrides :

Cette classe de protocoles fusionne les deux modèles vus précédemment, proactif et réactif, on cite ZRP (Zone Routing Protocol) et SHARP (Sharp Hybrid Adaptive Routing Protocol) qui mettent en valeur deux zones :

- Ø Une zone proactive (intra-zone) englobe l'ensemble des nœuds adoptant le modèle proactif.
- Ø Une zone réactive (inter-zone) contenant les nœuds restant du réseau qui se base sur un modèle réactif.

Cette approche s'avère très alléchante vu l'atout qu'elle présente de part la connaissance topologique locale du réseau du fait que les nœuds dont la distance les séparant est très importante communiquent moins souvent entre eux que leur voisinage.

II.8.3.1) Le protocole ZRP : [LAA.02]

Dans ses grandes lignes, le protocole ZRP, ayant défini son propre protocole IARP (IntrAzone Routing Protocol) destiné à maintenir les informations de routage dans une intra-zone, utilise deux méthodes appelées à diminuer le trafic résultant lors de la diffusion des requêtes de localisation :

La méthode de ***bordercasting*** qui recommande uniquement aux nœuds se trouvant à la périphérie de l'intra-zone, nœuds très distants, de réémettre les messages de requêtes.

La méthode d'***overlapping*** mis en service un nombre limité de nœuds périphériques dont ils appartiennent à des portées de transmissions différentes, ces nœuds sont appelés à retransmettre le message.

II.8.3.2) Le protocole SHARP :

Ce protocole définit à son tour le protocole SPR (SHARP Proactive Routing protocol) responsable de la maintenance proactive des informations liées aux nœuds appartenant au voisinage d'un nœud particulier, nommé nœud central. Ce protocole SPR se focalise sur les stratégies de routage des protocoles DSDV et TORA, ainsi le nœud central est appelé à maintenir les informations de routage par le biais d'un arbre acyclique dirigé ayant comme racine ce nœud central.

II.8.4) Le protocole AntHocNet : [ALI.09]

Le protocole AntHocNet (An Adaptative Nature-Inspired Algorithm For Routing in Mobile Ad hoc Networks) est une stratégie hybride multi-chemin, tirant partie de principes du routage ACO (Ant Colony Optimization). Si un nœud désire diriger un paquet de données au profit d'un nœud destination D, il consulte sa table de routage et sa table de phéromone, et voit si une mise à jour de l'information de routage liée à D est disponible. Si ce n'est pas le cas, le nœud source S transmit avec réactivité des petits paquets fourmis nommés *reactive Forward Ants* afin de découvrir des routes vers le nœud destination D, où ces paquets fourmis sont appelés à collecter des informations sur la qualité du trajet suivi par chacun d'entre eux.

Une fois arrivant à la destination D, ils changent d'aspect et deviennent *Backward Ants*, puis extraient les routes menant à destination et mettent à jour les tables de routage quand ils retournent au nœud source S.

Au départ, le nœud source S initialise les chemins et esquisse par émettre les paquets ***proactive Forward Ants*** vers la destination D. Ces fourmis supervisent la qualité des chemins empruntés, les maintiennent et les perfectionnent grâce aux valeurs de phéromones collectées. Si une coupure de liens s'est survenue, les nœuds procèdent à rétablir les routes locales ou à émettent un message ***Warning*** vers leurs proches afin que ces derniers puissent mettre à jour leurs tables de phéromones.

II.8.4.1) Table de routage :

Chaque entrée de la table de routage $\mathbf{T^i}$ correspond à un nœud ***i*** renfermant pour chaque destination **D** et pour chaque voisin **N** une valeur $\mathbf{T^i_{nd}} \in \mathbf{R}$ qui consiste en une valeur estimée du niveau de qualité du chemin menant à la destination **D** en transitant par les phéromones ici nommés N.

Les tables de phéromones soulignent pour chaque nœud les différents chemins existants de nœud source **S** vers la destination **D**, et alors les paquets de données peuvent circuler d'un nœud vers un autre tel qu'un datagramme via divers chemins en choisissant le prochain saut selon leurs valeurs de phéromones.

II.8.4.2) Découverte de routes réactive (Reactive Path Setup) :

Si un nœud source **S** veut communiquer un message vers un nœud destination **D**, il génère un paquet ***Forward Ant reactive*** $\mathbf{(f^s_d)}$ en mode *Broadcast* ou en *Unicast.* Si ce dernier est diffusé en Broadcast, rapidement il sera proliféré dans le réseau en empruntant ainsi une variété de routes vers la destination, néanmoins les paquets $\mathbf{f^s_d}$ ayant pris de mauvaises routes seront supprimés.

Le ***Reactive Forward Ant (L)*** s'occupe de découvrir une route liant la source **S** à la destination **D**, et d'enregistrer la liste des nœuds transités, **L** [1..N]. Une fois parvenu à la destination **D**, ***Reactive Forward Ant*** est transformé en ***Reactive Backward Ant*** qui explore la liste **L** jusqu'à atteindre la source **S**. Et continuellement, ce dernier traite la durée estimée $\mathbf{T_L}$ du trajet du paquet de données, qui sera employée pour la mise à jour des tables de routage, en transitant par les nœuds de la liste **L** vers la destination **D**.

Reactive Forward Ant attribue un parcourt virtuel vers la destination **D** pour chaque nœud médiateur $\mathbf{i} \in \mathbf{L}$, par la création ou la mise à jour des entrées de la table de routage $\mathbf{T^i_{nd}}$. Quand le paquet Fourmi atteint le nœud ***i*** depuis son voisin **N**, il suscite une entrée dans la table de routage $\mathbf{T^i}$ en mentionnant que **N** soit le prochain saut à suivre depuis le nœud présent afin d'arriver à la destination **D**. Cette entrée intègre la valeur de phéromone $\mathbf{T^i_{nd}}$ référant la qualité du parcourt qui permet de parvenir sur **D** à travers le prochain saut **N**.

Bien entendu, lorsque la quantité de phéromone n'est pas disponible, le paquet de Fourmi sera propagé sur le réseau. Mais dans le cas où cette information s'avère disponible, le paquet Fourmi opte pour une probabilité $\mathbf{P_{nd}}$ pour sélectionner le saut suivant (**N)** comme ceci :

$$P_{nd} = \frac{((T_{nd})_i)^{\beta}}{\left(\sum_{j \in (N_d)_i} ((T_{jd})_i)^{\beta'}\right)} \; et \; (\beta \geq 1)$$

Tel que :

$\mathbf{N^i_d}$: l'ensemble des nœuds voisins de (***i***) disposant d'une route vers un nœud destination (***d***) bien déterminé.

$\square$: généralement égal à 1, ce paramètre aide à superviser le comportement du parcourt des fourmis.

Il est à noter que chaque ***Forward Ant*** mémorise la liste **L** [1..N] contenant tous les nœuds intermédiaires dont il a passé par le long du son trajet, ainsi, quand il atteint la destination, il sera convertit en ***Backward Ant*** qui, adapte le même chemin indiqué par **L**, en retournant vers la source. De ce fait, le résultat sera communiqué d'une façon uniforme pour tous les chemins du réseau.

La fin de cette procédure de détermination de routes fait paraitre deux cas. S'i elle est achevée avec succès, un ensemble considérable de routes partant de la source vers la destination sera disponible. Mais en cas d'échec, i-e, aucun ***Backward Ant*** n'a fait l'objet de retour à la source après le découlement d'un certain temps, il sauvegarde temporairement les informations, ainsi, toute la procédure est à refaire, cependant, arrivant à un nombre précis de répétition, les informations seront supprimées.

II.8.4.3) Le routage stochastique des données (Stochastic Data Routing) : [ALI.09]

Dans les grandes lignes de protocole de routage ***AntHocNet***, les nœuds subissent une diffusion stochastique, autrement dit, lorsqu'un nœud se contente d'avoir, pour les informations, plusieurs sauts émanant tous sur la destination **D**, il choisit un seul parmi eux avec une probabilité $\mathbf{P_{nd}}$ du saut suivant. A titre de cette technique, le nombre de chemins sera choisi automatiquement selon leurs qualités, néanmoins, si un chemin s'avère mauvais par comparaison avec les autres, ce chemin est évité et sa congestion sera déchargée.

Il est quasiment essentiel de contrôler périodiquement la qualité de tous les chemins du fait que la portée du support radio dans les MANETs est très limitée, et ce grâce aux paquets **Proactive Ant** où les nœuds diffusent régulièrement les informations chargées sur le réseau**.**

II.8.4.4) Exploration et maintenance du chemin proactive : [ALI.09]

Les paquets ***Proactive Forward Ant*** sont propagés depuis un nœud source en adoptant un routage unicast, ils optent pour le prochain saut selon les valeurs de phéromones identiquement comme pour les paquets ***Reactive Forward Ant***, cependant, la probabilité

qu'ils soient routés en broadcast est très petite mais existe, ce qui fait l'objet d'apparition de deux résultats distincts :

A Cas n°1 :

Quand le paquet ***Proactive Forward Ant*** arrive à destination sans nécessiter un seul saut broadcast, il cueille les informations sur la qualité estimée du chemin parcouru, ensuite sera convertit en ***Proactive Backward Ant*** qui emprunte le chemin inverse, i-e, de la destination vers la source, en mettant à jour les valeurs de phéromones des nœuds médiateurs.

A Cas n°2 :

Ici, le paquet ***Proactive Forward Ant*** se concentre autour des pistes de phéromones et la recherche de nouveaux chemins, ainsi, lorsqu'il parvient à tous les voisins du nœud émetteur, il s'avère possible qu'il ne trouve pas les traces de phéromones menant à la destination, ce qui nécessite sa rediffusion. Cette rediffusion est limitée à un nombre de sauts **nb**, ainsi, le paquet Fourmi se prolifère et submerge rapidement le réseau, et s'il ne trouve pas l'information de routage au bout de **nb** sauts, il sera détruit.

Superviser les paquets ***Forward Ant*** revient à utiliser les messages ***Hello*** propagés par les nœuds toutes les t_{hello} secondes**,** entre outre, ces messages aident grandement les nœuds à bien connaitre leurs voisins directs ainsi les informations de phéromones correspondants. Un nœud en recevant un message ***Hello*** depuis un nouveau nœud **n**, il met à jour sa table de routage en insérant le nœud **n**. Puis, il se met en attente d'un message ***Hello*** pour t_{hello} secondes, s'il ne le reçoit pas en un certain nombre de fois depuis le nœud **n**, ce dernier sera retiré de la table de routage du nœud concerné. Quand un paquet parvient à un nœud proche de la destination **D**, il peut l'atteindre directement.

II.8.4.5) La rupture de lien (link failure) : [ALI.09]

Deux cas se présentent lorsqu'une coupure d'un lien survienne dans AntHocNet : le premier cas s'illustre par une perte non trop influente sur l'acheminement des paquets et alors le nœud met à jour sa table de routage et émet une notification de la mise à jour pour ses voisins, et ce, quand le nœud possède d'autres voisins menant à la même destination ou quand les données n'emploient pas régulièrement la destination mise en cause. Dans le deuxième cas, la perte est importante, dû à l'emploi régulier de la destination par les données ou puisque c'est le seul nœud conduisant à la destination, et donc ce nœud essaye de réparer la route. Cette réparation de route est effectuée seulement si le lien rompu ou brisé est signalé au moment d'une panne de transmission de paquet de données.

Une rupture de lien nécessite que le nœud génère un paquet ***Route Repair Ant*** explorant l'ensemble du réseau vers la destination et donc suivre l'information de routage disponible sinon opter pour la rediffusion. De plus, il est possible qu'un nœud possède plusieurs entrées menant à la destination touchée par la rupture de lien, or que le prochain saut

brisé présente le meilleur chemin vers la destination, à ce moment là, le nœud se limite par l'envoi d'une ***notification*** pour son voisinage. Cette ***notification*** est envoyée aussi lors de la réparation d'une coupure de route. Elle est dotée d'une liste de destinations ayant perdu leurs chemins ainsi le meilleur nombre de saut estimé optimal pour joindre la destination. L'ensemble de ces voisins reçoit cette notification et mettent à jour leurs tables de routage par les nouvelles estimations. Ensuite, si ces voisins perdent leurs meilleurs chemins ou les seuls chemins disponibles menant à la destination à cause d'une rupture de lien, la notification sera diffusée afin que tous les nœuds du réseau aient connaissance de cette notification.

Il est à noter que le nombre de diffusion ainsi la duplication des paquets sont limités. Un nœud se patiente pour une période précise, s'il ne reçoit pas un paquet ***Backward Repair Ant***, il se persuade que la destination est inatteignable et procède à la mise à jour de sa table de routage en omettant cette destination.

II.9) évaluation des protocoles de routage: [MXP.09], [BAN.00]

L'évaluation des protocoles de routage s'avère une étape très délicate du fait qu'elle s'accentue sur la mesure des performances et le test d'efficacité de la stratégie mise au point. A l'issu de cette évaluation sorte une comparaison très importante montrant les caractéristiques de chacune de catégories des protocoles de routage :

II.9.1) Protocoles proactifs :

- Structure de routage plate et hiérarchique.
- Routes toujours disponibles.
- Volume de trafic de contrôle plus important.
- Mise à jour périodiquement.
- Exigence de stockage très haute.
- Délais de détermination de la route réduit.
- Taille de réseau pouvant aller jusqu'aux 100 nœuds.

II.9.2) Protocoles réactifs :

- Structure de routage plate.
- Routes disponibles à la demande, au besoin.
- Volume de trafic de contrôle inferieur à celui des proactifs.
- Mise à jours périodique non requises, mais dans le protocole ABR c'est possible que les nœuds nécessitent des signaux périodiques.
- Capacité de stockage relativement moins que celle des proactifs.
- Délais de découverte de routes est plus haut par rapport au proactifs.
- Taille de réseaux peut touchée quelques centaines de nœuds selon le niveau de trafic et le nombre de sauts.

II.9.3) Protocoles hybrides :

- Structure de routage généralement hiérarchique.
- Routes strictement liées à la localisation des destinations.

- Volume de trafic plus optimal que celui des réactifs et proactifs.
- Mises à jour régulières le plus souvent appliquées dans toute zone ou entre les nœuds.
- Capacité de stockage dépend de la taille de chaque zone.
- Délai de détermination de routes plus important, l'interzone, que le réactif quand il s'agit de destination locales.

II.10) Avantage & inconvénients : [FSA.10], [SSM.03]

Une étude plus globale concernant les protocoles proactifs et les protocoles réactifs consiste à montrer les atouts et les défauts de chacun d'eux au sein d'une simple comparaison. Dans un premier lieu si on se base sur le concept de meilleures performances fournies, on constate que c'est les stratégies proactives qui sont en amant soit avec leur temps de réponse qui se présentent par l'acheminement des paquets en de très courts délais, ou avec leur rapidité de détermination du meilleur chemin. Or que l'autre face tracassant ces protocoles réside dans le fait qu'ils sont gourmands en terme de capacité de traitement et de mémoire essentiellement causées par la diffusion massive des paquets sur le réseau, sans oublier la bande passante qui est constamment mise en œuvre.

En contrepartie, les protocoles de routage réactifs offre un atout percutant se résumant par la mise en service d'une bande passante moins importante. Mais il est à noter qu'ils se confrontent à plusieurs inconvénients qui se manifestent par la surcharge du réseau lors du lancement d'une demande de découverte de route qui à son tour induit un temps de réponse ou d'attente accru, relativement très long.

II.11) Conclusion :

Dans les grandes lignes de ce chapitre on a dressé un bref aperçu sur la stratégie de routage, quelques protocoles de routages qui nous semblent primordiales à traiter, les handicaps et les avantages qu'ils mettent en place, ainsi une comparaison plus ou moins globale montrant les propriétés prises en charge par ceux-ci.

Actuellement, les réseaux ad hoc sont en amant d'une importante variété de stades d'application vu l'avantage indéniable qu'ils soulignent et qui réside dans leurs déploiements immédiat ainsi leurs faibles coûts sur le plan financier. Toutefois, et malgré ces point positifs, les réseaux ad hoc doivent faire face aux handicapes spécifiques dont ils soufrent afin d'augmenter grandement leur efficacités. Cela pousse alors plusieurs travaux de recherches à proliféré les efforts dans le contexte de perfectionner leur exploitations en proposant des solutions surmontant ces obstacles.

Le chapitre suivant illustre une étude plus détaillée sur les réseaux ad hoc de point des attaques, vulnérabilités ainsi la sécurité signée par ses différents protocoles de routage

CHAPITRE III

LES PROBLEMES DE SECURITE

DANS LES RESEAUX AD HOC.

III.1) Introduction :

Les réseaux ad hoc se définissent en tant que systèmes où l'infrastructure est absolument distraite, ainsi, les nœuds participants dans le réseau sont reliés par l'intermédiaire d'une voie hertzienne. Ces nœuds contribuent à une tâche très pratique consistant en faire transiter des informations sans l'aide d'un canal physique et gérer le routage de celles-ci, et entre autre, endosser les reconfigurations topologiques du réseau. En paradoxe, la médaille a un revers. En effet, les technologies sans fil émergent des désagréments qui ne sont pas des moindres à savoir la qualité de service, le routage et la sécurité.

III.2) Concepts de base sur la sécurité :

III.2.1) Définition : [GOD.05]

Selon Didier GODART, la sécurité est l'ensemble de mesures permettant d'assurer la protection des biens et/ou valeurs.

Et informatiquement parlant, ces biens sont planés en deux catégories à savoir :

1. Les informations (les données) : les commandes, les contrats, les offres, les données stratégiques, les données privées…
2. Les systèmes de traitement, acheminement, stockage d'information : les applications, les serveurs, les bases de données, les réseaux internes et externes…

III.2.2) Les menaces, vulnérabilités et risques :

III.2.2.1) Les menaces :

a) Définition :

Une menace [GOD.05] peut se résumer par l'action ou l'événement qui contribuent à tracasser la protection d'une ou de plusieurs propriétés des données ou des systèmes. Ces derniers essaient de remédier à ce genre de failles par traitement et maintenance, en faisant appel à la confidentialité, l'intégrité et la disponibilité. Néanmoins, pour qu'une menace puisse s'exécuter, elle stipule un contexte réactif baptisé vulnérabilité.

On va traiter au passage les deux familles d'événements et d'actions citées précédemment :

- ***Les actes malicieux*** : cette famille peut avoir l'air volontaire ou intentionné, de provenance interne ou externe à savoir : les intrusions, les accès non-autorisés, les usurpations d'identité, l'établissement ou l'intégration de codes cachés, les opérations de Denis de Service, les bombardements électroniques, les écoutes de trafic, la répudiation, l'extraction des données, la contrefaçon, le vol d'identité, le détournement de courriels…etc.

- ***Les événements involontaires*** : cette famille est conférée aux accidents tel que : les bugs, les divulgations accidentelles, les fautes de manipulations, les oublis de sauvegarde, les différents problèmes techniques, ainsi les événements environnementaux comme les coupures de courant, les incendies et les dommages des eaux. Ces événements peuvent résulter de fâcheux impacts implicitement liés aux contextes des organisations en question. On distingue :

  - Les divulgations des données.
  - Les préjudices de l'intégrité des données.
  - L'endommagement des données.
  - Les pertes de service.
  - L'usurpation d'identité.

A leur tour, ces impacts présentent de crucials résultats voir pénibles tel que : la mise en cause de la confiance, les dommages touchant la réputation, les dégâts financiers, les poursuites judicaires.

b) Types de menaces : [GND.03],[HGG.08]

Ce présent point est scindé en deux types à savoir :

Menace passive : dans cette menace, l'attaquant se restreint par écouter et analyser les trafics transmis. A l'issu de cette menace, la notion de la confidentialité des messages dans le réseau sera privée.

Menace active : ici, l'attaquant consacre sa tâche en opérant sur la gestion, l'exploitation et la configuration du réseau, et donc, il peut agir sur ce dernier par différentes manières tel que : l'intégration de son propre trafic, changement du comportement ou l'usurpation de l'identité d'un nœud, retransmettre les messages, changer les messages émis sur le réseau, résulter un Denis de Service…etc.

II.2.2.2) Les vulnérabilités : [GND.03]

Avant de tenter de présenter les attaques touchant la sécurité dans les réseaux ad hoc, il est primordial de spécifier quelques vulnérabilités qui sont essentiellement issues de la technologie sans fil :

Une toute première vulnérabilité se dévoile pleinement aux yeux consiste en la liaison sans fil qui contribue grandement à ce que les messages transmis seront écoutés ou perturbés par n'importe qu'elle entité disposant d'un récepteur adéquat.

Un deuxième point de vulnérabilité du réseau se traduit par les nœuds laissés sans surveillance, ce qui facilite la tâche à l'attaquant de compromettre une de ces entités.

Une troisième vulnérabilité se mesure par l'absence d'infrastructure où les entités du réseau mettent à l'égard toute gestion des accès aux ressources.

Une dernière vulnérabilité se montre par les techniques de routage, et ce du fait que toute entité dans les réseaux ad hoc est appelée à véhiculer les paquets à travers le réseau, mais aussi, il faut se rendre compte que ces messages suivent des chemins sur des supports radio.

II.2.2.3) Les risques : [GND.03]

Pour bien cerner les risques percutants le concept de la sécurité dans les réseaux ad hoc, il s'avère primordial de passer par ces différentes phases concourantes à mettre en avant les points crucials de la sécurité :

1) Préciser les données et les fonctions sensibles du réseau.
2) Investiguer les objectifs de la sécurité.
3) Etudier les vulnérabilités.
4) Etudier les menaces et mesurer leur probabilité d'occurrence ou de réalisation.
5) Evaluer les risques détenus par les vulnérabilités et les menaces mises en place.

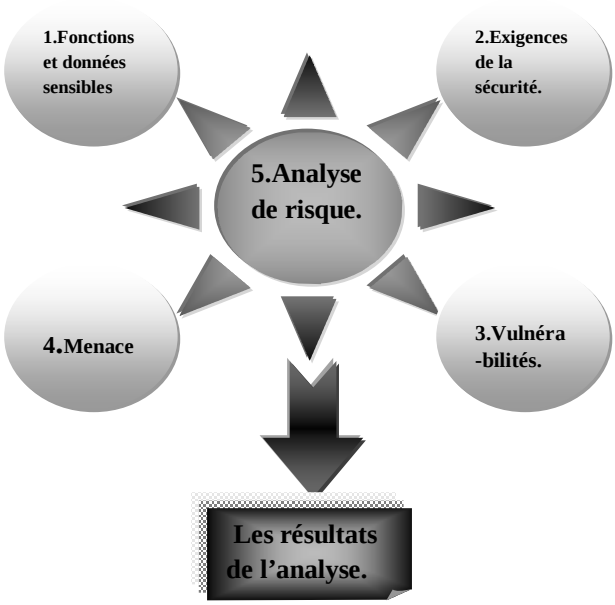


Figure 3.1 : Les phases d'analyse de risque.

A savoir les contraintes à respecter et les contextes d'utilisation, l'analyse de risque se soucie à fournir des solutions pertinentes et appropriés répondant intégralement aux besoins. Cette présente analyse peut être généralisée afin de cerner différentes études.

III.2.2.3.1) Fonctions et données sensibles: [GND.03]

Dans un réseau ad hoc, les fonctions sensibles sont soulignées au niveau des nœuds par la stratégie de routage, la configuration, la gestion de l'énergie, et aussi les mécanismes de sécurités.

De l'autre coté, la majorité des données sensibles s'imbriquent avec ces fonctions du fait qu'il consiste en données de configuration concernant la gestion de l'énergie, ou en données liées au routage ou au table de routage, ou en données liées à la sécurité comme les mots de passe et les clés cryptographiques. Néanmoins, les informations privées des utilisateurs sont sensées d'être vue tel que des données sensibles.

III.2.2.3.2) Les exigences de sécurité :

Les exigences de la sécurité esquissent par une étude détaillée des contraintes alourdissant le réseau, ensuite, s'orientent à mesurer les objectifs de la sécurité.

a) Les contraintes : [GND.03]

Nombreuses sont les contraintes à respecter dans un réseau ad hoc, on peut citer :

- ***Caractéristiques des nœuds*** : les nœuds se profilent par l'hétérogénéité et des capacités de calculs détériorés.
- ***Gestion de l'énergie*** : les nœuds doivent se ramener à consommer le moins d'énergie et à se mettre en veille dans le but de réserver le plus longtemps les charges.
- ***Caractéristiques du réseau*** : il est à noter qu'il est nécessaire de garantir une équité de charge distribuée entre les participants du réseau, comme il faut prendre en charge l'absence d'infrastructure et l'autonomie des nœuds.
- ***Medium sans fil*** : cette contrainte s'avère très délicate du fait qu'elle doit tenir en compte les perturbations résultant du support radio qui provoquent une détérioration du débit et de la bande passante.
- ***Mobilité*** : à cet égard, il est préconisé de se rendre compte des variations topologiques du réseau, ainsi, la forte mobilité des nœuds.
- ***Configuration*** : ici, l'auto configuration contribue à faciliter l'injection des nœuds dans le réseau, ce qui donne une nécessité fluctuante pour déployer des réseaux ad hoc à grande échelle.

b) *Les objectifs* : [GOD.05], [RTR.02], [PMJ.02]

Il est net que la sécurisation des communications dans les réseaux ad hoc nécessite la mise en œuvre de mécanismes concourant à réaliser certains objectifs de la sécurité. Et si ces objectifs sont bien munis, ils peuvent servir de contre-mesures percutantes à l'ensemble des attaques dans ces réseaux. **[THC.08]**

Et bien entendu, la confiance et l'assurance sont deux points crucials au cœur de la sécurité. Etablir un canevas de confiance préconise le développement et la mise en œuvre de mesures sujettes à assurer la validité et la disponibilité des informations, l'authenticité, la confidentialité, l'intégrité de données échangées et stockées.

- ***La confidentialité*** : elle a comme objectif de garantir la protection des données transmises en appréhendant toute divulgation accidentelle ou malveillante prohibées. Sa réalisation est sensée d'être systématique à chaque transmission des données sensibles, que ce soit des données de couches applicatives ou de données des couches inferieures. [ABR.09], **[PMJ.02]**

- ***L'intégrité :*** assurer la protection de communications entre les entités du réseau en appréhendant toute sorte de fluctuation ou disparition des entités accidentelle ou malveillante. [ABR.09], **[PMJ.02]**

- ***La disponibilité :*** assurer, au besoin, l'accès et l'usage des ressources, des données et des systèmes, avec une qualité de service adéquate par les entités autorisées. En plus, pour sécuriser la duplication des données, cette propriété rend intelligible les systèmes quand l'événement de Dénis de Service est survenu (DoS).

- ***L'authentification*** : cet objectif de sécurité permet aux unités du réseau de s'assurer de la meilleure identification des unités avec lesquelles elles échangent les données ainsi les opérations effectuées sur celles-ci. Une fois cet objectif réalisé, toute sorte d'attaque se déclinant sur les usurpations d'identité ou de rôle se finira par l'échec, et ce par le biais de mots de passes, PIN (Personal Identification Number), la cryptographie ou la biométrie. [THC.08], **[PMJ.02]**

- ***La non-répudiation :*** étant donné que cette propriété consiste à prouver l'origine des données, il arrive qu'elle permette d'identifier les entités malveillantes qui essaient de faire des actes malencontreux afin de ne pas les reconnaitre, surtout dans les communications sensibles. [THC.08]

III.2.2.3.3) Les résultats de l'analyse de risque: [GND.03]

Après avoir traité les contraintes et les objectifs de la sécurité des réseaux ad hoc, et après avoir étudié les menaces et les vulnérabilités relatives à ces réseaux, il est temps d'extraire l'ensemble des attaques ayant une importante probabilité ou faisabilité, et décrivant en cas de réalisation un véritable risque.

A Le Dénis de Service (Denial of Service, DoS) :

Cette attaque consiste en l'ensemble des actions malveillantes opérant au niveau applicatif ou au niveau des couches inferieures ayant comme cible d'empêcher de conférer régulièrement des services dans le réseau. Le Denis de Service s'averti l'une des attaques les plus cruciales à contrer en raison de ses multiples formes qu'il peut prendre, parmi les exemples les plus saillants de cette attaque, on peut trouver : le brouillage touchant le support radio afin d'obstruer les échanges, l'épuisement des ressources des terminaux ou du réseau dû essentiellement à l'envoie massif des paquets, aussi l'exploitation des vulnérabilités protocolaires. **[THC.08]**

- **Les attaques passives d'écoute et d'analyse du trafic** : elle exprime une menace touchant la confidentialité et l'anonymat.

- **L'usurpation de l'identité d'un nœud** : cette attaque interne consiste à illusionner les mécanismes de contrôle d'accès au réseau, et donc, la sécurité de stratégies de routage devient plus vulnérable aux attaques actives. Elle émerge les différents stratégies de routage et qui est soumise à de multiples caractéristiques dont on cite :
  - » Des informations falsifiées liées aux identités ;
  - » Des nœuds isolés ;
  - » Vision non équité de la topologie du réseau ;
  - » Calcul distribué et non uniforme;

- **L'attaque physique d'un élément valide** : dans un réseau ad hoc, cette attaque consiste à mettre en péril un nœud qui est considéré comme étant un point faible du réseau.

- **Les attaques liées aux stratégies de routages :** il s'agit des attaques les plus critiques dont les réseaux ad hoc souffrent.

III.2.3) Les mécanismes de sécurité : [MEA.05]

Garantissant la confidentialité, l'intégrité et la disponibilité des services, la sécurité se contente de définir des mécanismes servant d'accorder l'accès aux données uniquement aux personnes autorisés et de réaliser correctement les services. A titre de ces mécanismes, on trouve :

Cryptographie : il s'agit d'un mécanisme de sécurité qui se penche sur de multiples stratégies tel que le chiffrement, la signature numérique, l'authentification et les certificats électroniques.

Firewall : il s'agit d'un système ou un ensemble de systèmes opérant sur les contrôles d'accès entre deux réseaux et limitant le nombre d'attaques à distances. Et dans ce contexte, il existe deux mécanismes, l'un consiste à interdire le trafic, or que l'autre le permettre.

Système de détection d'intrusion (IDS) : ce mécanisme a recourt à déceler dans un système une vulnérabilité de la sécurité et opte pour limiter et appréhender les intrusions possibles.

III.3) Les attaques:

Le but principal d'une attaque est de provoquer un disfonctionnement en touchant l'intégrité et la confidentialité des informations qui circulent dans le réseau.

III.3.1) Classification des attaques: [MEA.05], [BUC.09]

Cette présente section se focalise sur la présentation des attaques les plus populaires touchant les réseaux ad hoc. Bien entendu, ces réseaux s'avèrent très sensibles aux différentes intrusions ayant comme but de tirer parti de ses multiples vulnérabilités afin de gérer au mieux les attaques ou les aspects malicieux. Ces attaques sont organisées selon divers critères comme les stratégies de routage vulnérables, l'intégration dans le réseau, les méthodes utilisées, la discrétion des attaques [APO.07], et donc on cite :

- ***Attaques interne ou externe :***
  - ***Attaque interne*** : ce type d'attaque révèle une difficulté non négligeable pour détecter l'attaquant du fait qu'il dispose d'un accès aisé au réseau en appelant le *nœud compromis* qu'il possède. Ainsi, cette attaque met en cause la confiance entre les entités du réseau ad hoc.
  - ***Attaque externe*** : dans ce contexte, l'attaquant se serve d'un autre réseau, tel que l'internet, pour pouvoir communiquer avec le réseau extérieur, voir victime, puisqu'il n'appartient pas à ce dernier. Il est clair que dans cette perspective, la détection de la source d'attaque est très difficile en raison de l'absence d'un point de concentration de trafic dans le réseau et de fait que l'attaquant puisse se valider dans le réseau depuis plusieurs points d'accès.

- ***Attaques passive ou active :***
  - ***Attaque active*** : elle consiste à recueillir des informations depuis des nœuds ou des paquets émis dans l'ensemble du réseau. Néanmoins, cette attaque s'évertue à devenir dangereuse dans le cas où les informations détenues sont sensibles.
  - ***Attaque passive*** : ce mode d'attaque se manifeste par un caractère malicieux, à titre d'exemple, il saisit les failles provenant sur les programmes ou sur les protocoles employés afin de munir un disfonctionnement dans le réseau.

- **Attaques sur les protocoles ou par consommation de ressources** :
  - ***Attaque sur protocoles*** : elle survient spécialement sur des protocoles ayant recourt à une collaboration entre les différents nœuds du réseau de la sorte à altérer le bon enchainement de la procédure du routage. Ce dernier est aussi exposé à ce genre d'attaque, et donc, toute entité du réseau peut jouer le rôle d'un relais et détecter ou détourner le trafic en transit.

- ***Attaque par consommation de ressources*** : cette attaque est relative au protocole d'accès au support radio qui résulte une importante vulnérabilité, par exemple en occupant pour longtemps la bande passante et faisant abstraction aux autre entités d'employer le canal radio pour communiquer.

Ø Attaques individuelles ou distribuée :

- ***Attaque individuelle*** : comme son nom l'indique, cette attaque met en œuvre une seule source et une route optimale sans avoir besoin à des relais.

- ***Attaque distribuée*** : contrairement à l'attaque individuelle, celle-ci fait intervenir un ensemble de sources et de nœuds intermédiaires. De ce fait, il devient plus pénible et compliqué de capturer ces attaques et d'identifier la source de l'attaque.

III.3.2) Taxonomie des attaques :

Alors que la sécurité des réseaux ad hoc pose un défi très important, ils ont fait l'objet avec leur développement exponentiel, d'innombrables attaques qui constituent encore actuellement une menace sérieuse. Egalement, une variété d'attaques s'appuyant sur les vulnérabilités du réseau ad hoc et ciblant le concept de routage dans ces réseaux, sans égard pour le protocole utilisé, sont présentes. On distingue :

III.3.2.1) Attaque par Wormhole: [MAG.06], [THJ.07], [AHA.08], [LBJ.06]

Wormhole ou encore nommé trou de vers est l'une des attaques les plus sévères dans les réseaux MANET du fait qu'elle met en jeu un ensemble de nœuds compromis. L'objectif souligné par cette attaque est la simulation d'un nœud dans le voisinage. Se focalisant sur l'encapsulation des messages, les deux attaquants se trouvant dans deux points différents du réseau esquissent par établir un lien entre eux, lien du tunnel de vers, par un câble Ethernet ou grâce à une émission non filaire à longue portée. Après avoir formé le lien, l'attaquant détecte les communications sans fil sur une limitrophe du réseau et procède à les retransmettre à travers le tunnel de vers et les envoyer à l'autre limitrophe du réseau. En effet, l'attaquant en formant un chemin virtuel très court en termes de nombre de sauts, illusionne les nœuds du réseau et ainsi, évertue la totalité des messages transitant par ces nœuds de passer par lui.

La figure suivante donne une illustration de cette attaque. Les deux attaquants A et B sont reliés par un lien de trou de vers, l'attaquant B capture les transmissions sans fil dans son voisinage, les retransmettent à travers le lien du tunnel de vers au profit de l'attaquant A, qui a son tour propage l'ensemble des paquets reçus sur tout le réseau, et vice versa.

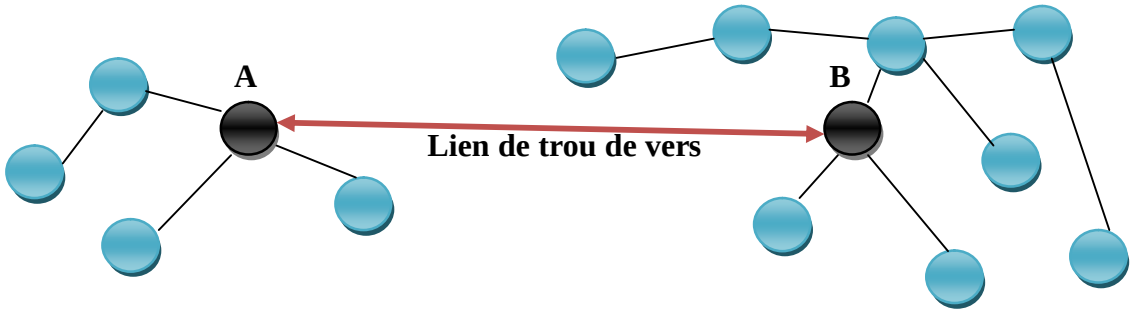
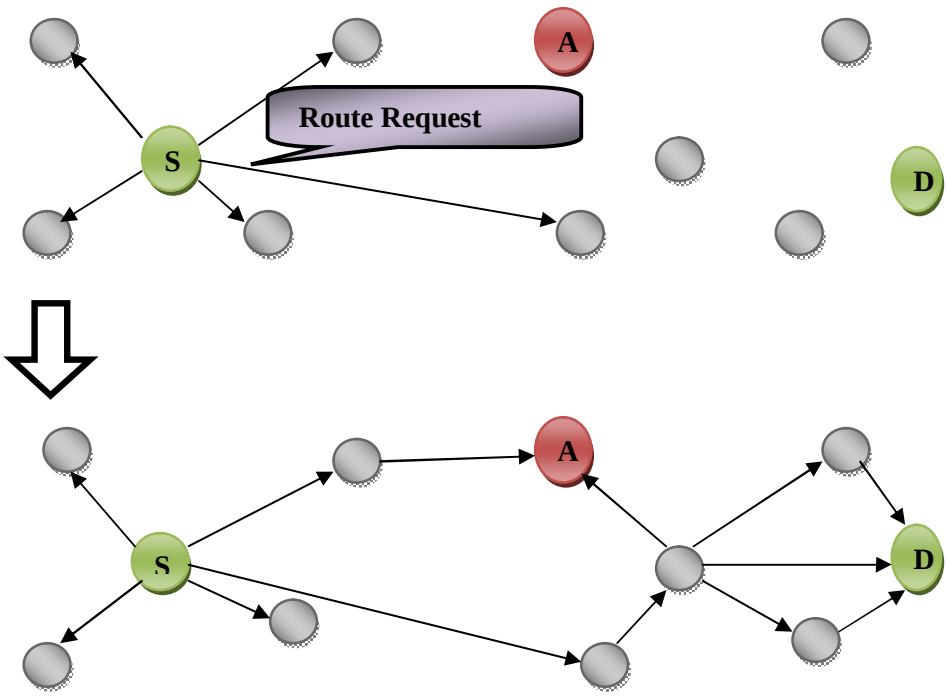


Figure 3.2 : L'attaque du trou de vers.

III.3.2.2) Attaque par Blackhole (le trou noir): [MAZ.07],[ABB.06],[AHA.07],[GLF.09]

Blackhole est une attaque interne concourant à remplir l'objectif qui stipule qu'au plus, une seule partie des paquets reçus sera transmise. Sur ce point, l'attaquant se charge de falsifier les informations concernant les routes, les liens et les vecteurs de distance de la sorte qu'il soit choisi dans une route valide, et donc, détourner et absorber le trafic. Il arrive qu'un nœud dans le réseau soit inapte de router les paquets et donc se restreindre à favoriser une partie du trafic. A cet effet, il devient difficile de déceler ce genre d'attaque.



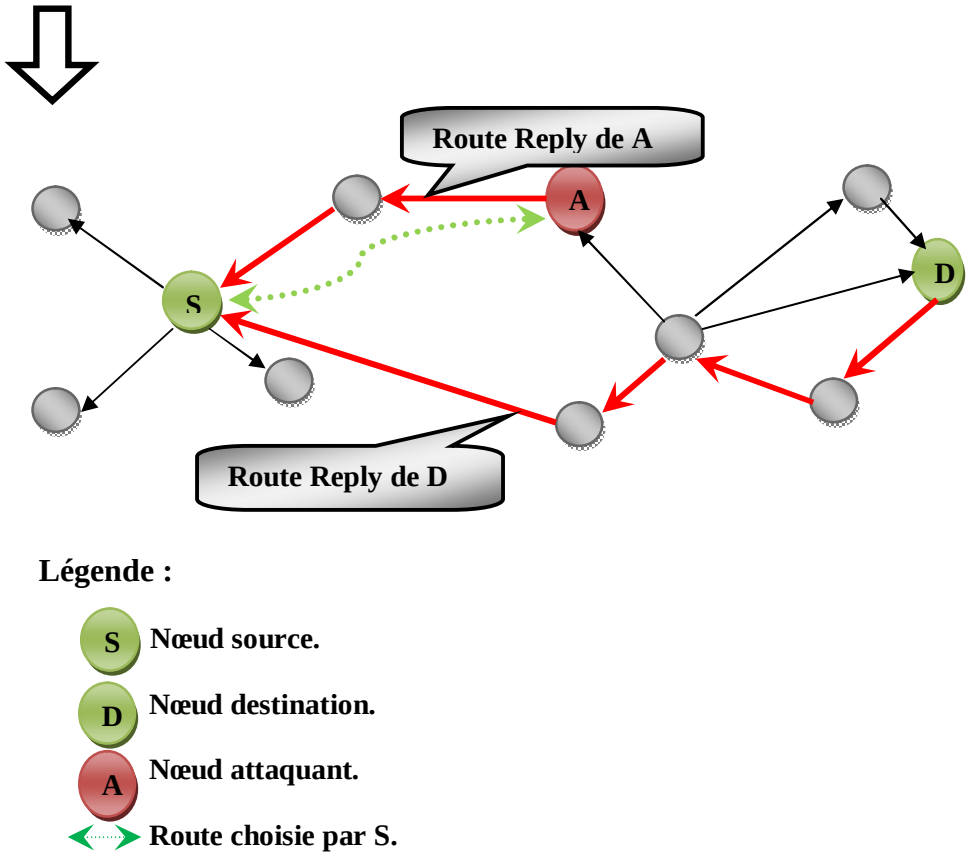


Figure 3.3 : L'attaque Blackhole**.**

Et pour mieux saisir cette attaque, on va prendre comme exemple un réseau où un nœud source (**S**) diffuse une requête ***Route Request (RREQ)*** sur le réseau afin de trouver un itinéraire vers un nœud destination (**D**). En recevant le paquet, chaque nœud le retransmit vers le reste du réseau y compris le nœud malicieux (**A**) en intégrant son adresse. Ce nœud malicieux (**A**) capte le trafic dédié au nœud **D** lors de la découverte de la route, ensuite, envoie une réponse ***Route Reply (RREP)*** au nœud initiateur en proposant un chemin avec un coût minimal vers la destination (**D**), ce qui explique que (**S)** le choisi, et donc, tout les paquets du nœud S vers la destination (**D)** vont passés par le nœud malicieux qui procède tout simplement à les absorber ou les ignorer.

III.3.2.3) Attaque par Spoofing : [AHA.07],[APO.07],[GLF.09],[THJ.07]

La technique de Spoofing ou l'attaque par imposture réside dans le fait qu'un nœud attaquant aura l'opportunité d'usurper les informations concernant l'identité d'un autre nœud du réseau en modifiant ses adresses MAC ou IP. Et alors, l'attaquant fournit une fausse vue de la topologie du réseau dû fait qu'il a isolé le nœud victime.

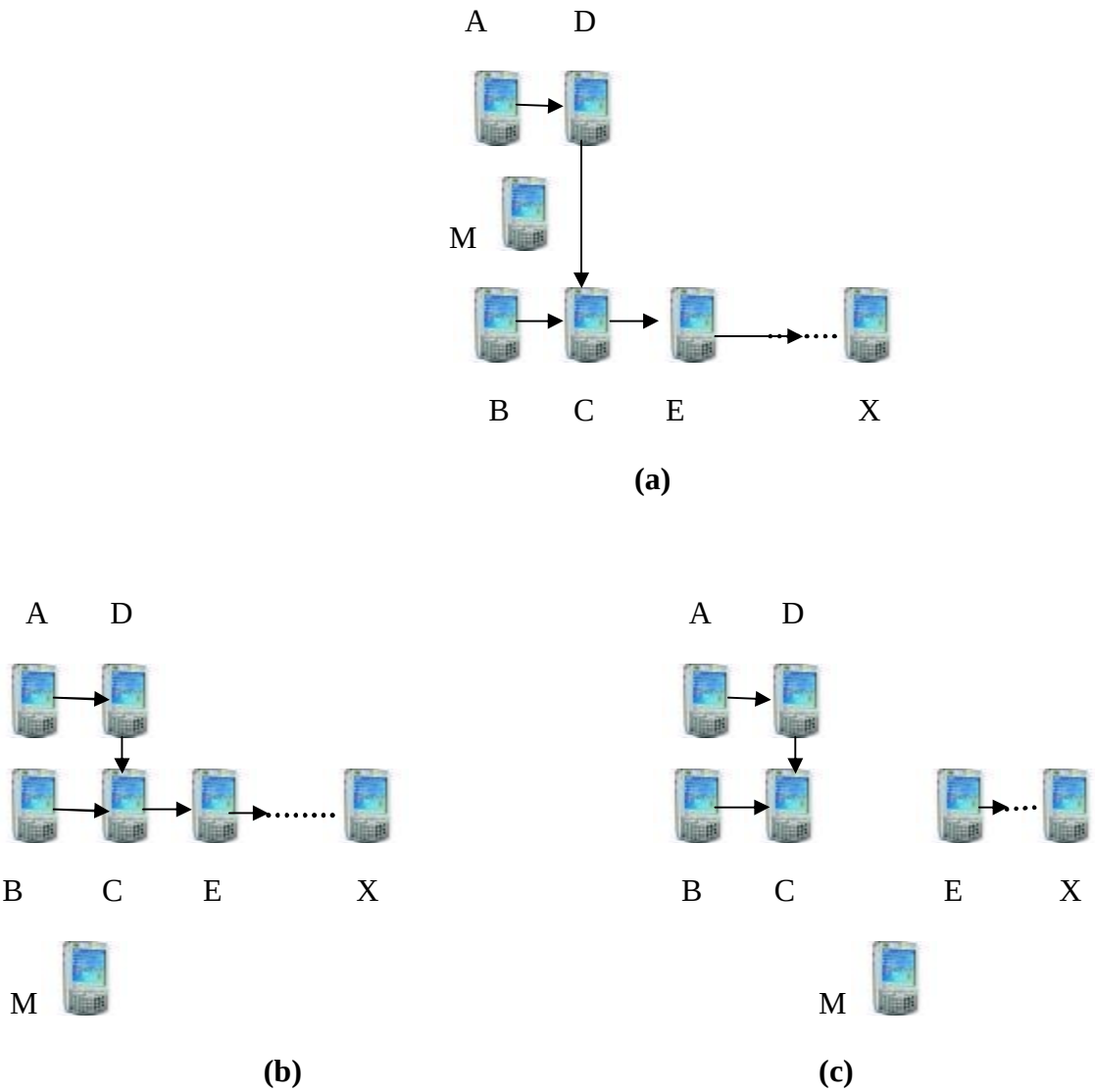


Figure 3.4 : (a), (b), (c), Les étapes du Spoofing.

Pour éclaircir un peu cette stratégie d'attaque, prenons un exemple de réseau qui met en valeur une route reliant les cinq nœuds avec le nœud destination X (voir la figure (**a**)). Ainsi, chaque nœud du réseau se trouve dans une portée bien précise comme dicte le tableau qui suit :

Le nœud	***a la portée de***
A	B.D
B	A.C
C	B.D
D	A.C
E	C
M	A.B.C.D

Tableau 3.1 : Les portées des nœuds du réseau.

Lors de l'établissement de la route, un nœud malicieux (M) est apte à avoir connaissance de la structure du réseau en capturant les transmissions des paquets ***RREQs/RREPs***. Ensuite l'attaquant peut créer une boucle qui empêche l'ensemble de nœuds se trouvant dans sa portée d'aboutir à la destination. Tout d'abord, l'attaquant esquisse son activité par modifier son adresse de telle sorte qu'elle soit équivalente à l'adresse de nœud (A), comme illustre la figure (**b**), ensuite, il communique un message ***RREP*** vers le nœud (B) qui dispose d'un chemin plus court vers le nœud (X) par rapport à celui fourni par le nœud (C). A cet effet, le nœud (B) modifie l'itinéraire des paquets vers le nœud (X) au profit de nœud (A), voir figure (**b**). L'attaquant (M) modifie encore son adresse en se servant cette fois de celle de nœud (B), il se met prés de nœud (C) et hors de la portée de nœud (B), il transmit ensuite un message ***RREP*** vers le nœud (C) muni d'un chemin plus optimal vers le nœud (X) en terme de nombre de sauts que celui envoyé par le nœud (E), et donc, le nœud (C) véhicule les paquets vers la destination (X) en passant par le nœud (B). Ce processus conduit finalement à la création d'une boucle et donc, la destination (X) sera inatteignable depuis les quatre nœuds comme illustré dans la figure(**c**). **[RMA.08]**

III.3.2.4) Attaque par harcèlement ou DoS : [AHA.07], [BUC.09], [APO.07]

Une autre attaque plus ou moins subtile de type Denis de Service (DoS) touchant les réseaux ad hoc, c'est l'attaque par harcèlement. Dans cette technique, l'attaquant procède par l'inondation périodique et sans signification des paquets de la sorte à surcharger le réseau et épuiser les ressources énergétiques des nœuds. A titre d'exemple, l'attaquant peut envoyer incessamment des requêtes de découvertes de routes (***RREQ***) ou des messages préconisant la modification de la topologie du réseau...etc.

III.3.2.5) Attaques spécifique à l'AODV :

Parmi les attaques submergeant les protocoles de routage réactifs on trouve :

III.3.2.5.1) Attaque par modification: [KAG.06],[HHG.05]

Cette attaque distingue d'autres attaques à savoir :

a) Redirection par modification du nombre de séquence de la route :

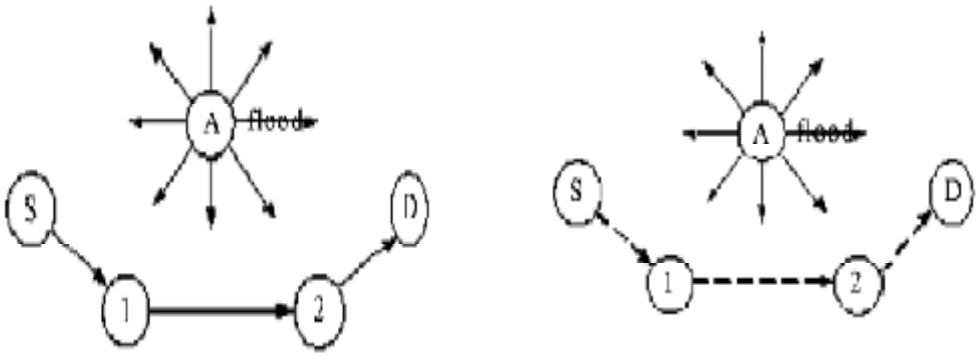
Le protocole AODV procède à attribuer des valeurs aux routes menant à une destination précise afin de définir la priorité de chaque route. En effet, la route disposant de la plus grande valeur sera choisie. Il est alors possible qu'un nœud opte pour modifier son numéro de séquence en publiant une route avec une valeur super grande.

b) Redirection par modification de nombre de sauts :

Ici, les nœuds malicieux dans les protocoles AODV procèdent soit par la mise à zéro de la valeur du champ de nombre de sauts (Hop Count) afin qu'ils puissent s'introduire dans une route, ou bien de tendre cette valeur vers l'infini pour s'exclure de la route.

III.3.2.5.2) Attaque par falsification des paquets RREQ : [HZC.07],[MAZ.09]

L'attaque RREQ flood opère par l'envoie de messages broadcast inutilement dans le but de ralentir le fonctionnement du réseau, ainsi les nœuds illégitimes émettent massivement et continuellement les paquets ***Route Request*** (***RREQ***) de la sorte à pousser les nœuds voisins à se servir de ces paquets et donc consomme les ressources énergétiques ainsi la bande passante du réseau.



(a) Flood attack par un nœud malicieux. (**b**) Après RREQ flood attack.

Figure 3.5: L'attaque par falsification des parquets RREQ.

Comme illustré dans cette figure **[HZC.07]**, le nœud adversaire envoie un ensemble de faux message ***RREQ*** pour falsifier le réseau. Les autres nœuds traitent et répondent à la fausse ***RREQ,*** ainsi, cette falsification provoque une dégradation dans la capacité de stockage et la communication des ressources des nœuds.

III.3.2.5.3) Attaque par falsification des paquets *RREP* (RREP Route Loop Attack) : [HZC.07],[YWS.06],[MAZ.09]

Le ***Routing Loop*** est un chemin dont les mêmes nœuds le traversent plusieurs fois. De ce fait, il en résulte qu'un paquet sera émis par le même nœud récursivement jusqu'à ce que le champ duré de vie se trouvant dans le paquet soit égale à zéro. Cette boucle de routage peut être exploitée pour mette en œuvre une autre attaque, le Denis de Service, au moment où elle est gourmande en termes de ressources énergétique des nœuds. Comme il est très important de souligner que le nœud destination sera exclue du réseau puisque peu de paquets aboutissent à leur destination.

(a) Avant Loop Attack. (b) après Loop Attack.

Figure 3.6: L'attaque par *RREP* Route Loop.

La figure ci-dessous **[HZC.07]** concrétise un exemple de falsification des paquets ***RREP*** comme suit : le réseau en question dispose de deux relais (1) et (2) formant une route de nœud (S) vers le nœud (D). L'attaquant est apte à créer une boucle entre les deux nœuds intermédiaires, et ce en prétendant d'être le nœud (1) et envoyer le message ***RREP*** en incrémentant le numéro de séquence de ***RREP***. Une fois ce paquet est reçu par le nœud (2), ce dernier change son prochain saut depuis le nœud (D) vers le nœud (1). Après avoir met à jour le numéro de séquence de la destination dans la table de routage, ces paquets seront d'abord envoyés pour le nœud (1), et par la suite vers le nœud (2) et puis revenir au nœud (1), et donc, une boucle de route s'est créée entre les deux relais.

III.3.2.5.4) Attaque par la non-diffusion des paquets *Route Error* : [KAG.06]

Après avoir mis en place une route reliant la source (S) à la destination (D), il vient que cette route sera maintenue autant que le nœud source désire. Vue la mobilité des nœuds, il se peut que la source change de localisation, et donc, un processus de découverte de route est exigé. Et en cas où le nœud destination ou un nœud intermédiaire change d'emplacement, un message ***Route Error*** (***RERR***) doit être transmis à l'ensemble des nœuds valides sur la route pour les informés de cette fluctuation. Or que, un nœud attaquant peut ne pas envoyer ce type de message aux autres nœuds du réseau pour perturber le fonctionnement du réseau.

III.3.2.6) Attaques spécifiques à l'OSLR : [ABR.09], [JPB.03]

Le protocole OLSR présente deux grands axes d'attaques qui donnent lieu à des vulnérabilités inhérentes aux réseaux ad hoc.

III.3.2.6.1) Attaque par DoS à N sauts:

Pour chaque message ***HELLO*** envoyé par un nœud voisin, l'attaquant se contente d'émettre un nouveau message ***HELLO*** qui suppose que tout les liens inclus dans le message ***HELLO*** initiateur, sont asymétriques. Ce type d'attaque consiste à attribuer des modifications au niveau de l'état de lien de façon à troubler le déroulement normal de la fonction du routage, et aussi de mettre en cause le nœud initiant le message ***HELLO***.

III.3.2.6.2) Attaque par détournement de MPR:

Dans cette classe d'attaques, le nœud adversaire se fait sélectionner comme MPR depuis ses nœuds voisins après avoir diffusé de faux messages ***TC*** indiquant son aptitude de parvenir à des nœuds n'ayant pas d'existence. Et de ce fait, les nœuds se trouvant dans son voisinage lui remettre les différents messages spécifiques à des nœuds distants dans le réseau.

III.4) Sécurisation du routage :

Après avoir détaillé les différentes attaques provenant sur les protocoles de routage dans les réseaux ad hoc, ce présent titre va être sacrifié à étudier les techniques mises en place pour protéger les protocoles de routage.

Réussir la sécurisation du routage stipule la prise en charge de ces critères [XIX.06] :

- La disponibilité : en cas d'existence, la route sera détectée.
- L'exactitude : une route opérationnelle doit au moins exister.
- La sureté : une route opérationnelle ne dispose ni de nœuds malicieux ni d'attaquants tolérables.
- L'efficacité des ressources : une large souplesse dans les techniques de sécurisation du routage.
- La stabilité : la stabilité se résume par l'existence des attaques non contrées.

III.4.1) Solution pour l'authentification : [RMA.08], [GND.03]

Prémunir des stratégies d'authentification le long du processus de routage est une solution de sécurité qui vise à exclure les nœuds malicieux et les nœuds non autorisés de contribuer à l'acheminement des données dans le réseau. La majorité des solutions émergeant de cette technique procèdent à modifier les protocoles utilisés au profit d'autres protocoles centrés autour de l'authentification.

Le fait que ces solutions opèrent sur les signatures numériques, explique leur raison de se focaliser sur le concept d'autorité de certification (CA) où le certificat a recourt à assurer qu'une clé publique appartient à son propriétaire et non plus à un nœud usurpateur. La vérification du certificat sert à superviser la signature du serveur central qui l'a signé, à garantir la validité et la non révocation de cette certificat. L'atout le plus important souligné par cette solution qui dénonce une centralisation et une flexibilité réduite, est la mise en cause des différentes attaques vues antérieurement quand elles proviennent d'un nœud externe n'ayant pas le droit de router les informations.

L'authentification dans les réseaux ad hoc permet de définir trois vecteurs qui sont :

a) Clé Secrète Commune (Key Agreement) : les nœuds du réseau se mettent d'accord sur une clé secrète.
b) The Duckling Policy Model : bâtit sur le modèle maître-esclave, les entités du réseau s'échangent une clé secrète via un support radio valide.

c) Public Key Infrastructure (PKI) : s'appuyant sur des infrastructures à clé publique, chaque entité du réseau définit des certificats pour les entités en qui elle a confiance.

III.4.2) Solution pour la confiance : [RMA.08]

Cette solution, métrique de confiance, rentre dans le cadre de gérer le comportement du protocole de routage, autrement dit, elle est sensée d'être intégrer dans les paquets de contrôle de la sorte à exprimer la valeur minimale de confiance préconisée par le nœud émetteur. Et par conséquent, un nœud en recevant un paquet s'avère incapable de le traiter ou de l'envoyer en cas où il dispose d'une mesure de confiance ne conformant pas à celle requière dans le paquet reçu.

III.4.3) Solution pour les messages : [RMA.08]

Dans l'objectif de faire face aux attaques par précipitation où l'attaquant se contente de s'intégrer dans toutes les routes de réseau, est née la technique de randomiser l'envoi des messages. Cette solution opère comme suit : après avoir envoyé une requête ***RREQ***, un nœud en recevant le premier ***RREQ***, le retransmet directement et ne tiennent pas compte de ***RREQs*** arrivant après. Sur ce point, il arrive qu'un nœud procède à regrouper un ensemble de ***RREQs*** avant qu'il sélectionne incidemment un ***RREQ*** pour l'envoyer. Arrivant à ce stade, cette technique met en valeur deux critères qui sont le nombre de paquets ***RREQs*** à réunir et la stratégie adoptée pour choisir les intervalles de temps (timeouts).

En revanche, cette solution présente un handicape du fait qu'elle exige que chaque nœud doit attendre un délai de temps ou recevoir un certains nombres de paquets ***RREQs*** avant d'émettre la requête. Ainsi, le choix arbitraire des routes contrarie la notion d'optimalité qui obéisse à certaines mesures telles que le nombre de sauts.

III.4.4) Solution pour l'anonymat des routes : [RMA.08],[GND.03]

Le chiffrement en oignon est une solution proposée dans le but de chiffrer asymétriquement une route sous forme d'un oignon lors de l'établissement du parcourt et de communiquer les paquets grâce à cette route (oignon chiffré). Et donc, crypter le message à l'aide d'une clé publique du destinataire et le décrypter avec sa clé privée. [MOB.06]

Cette solution vise à ce que chaque élément du réseau puisse identifier son successeur au moment où la suite du chemin lui reste cachée et anonyme.

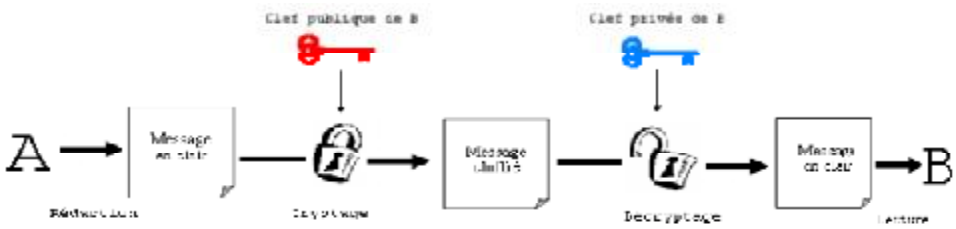


Figure 3.7 : Chiffrement asymétrique.

Chaque nœud du réseau suit le processus suivant afin de pouvoir lire uniquement le prochain saut lors de l'émission des paquets :

La réponse de route : chaque nœud du réseau intègre son adresse dans la prochaine partie de la route établie, et chiffre le résultat par la clé publique du nœud précédent.

La diffusion de la demande : chaque nœud du réseau intègre son adresse à la partie précédente de la route établie, et chiffre le résultat par sa propre clé publique.

Et pour mieux comprendre cette solution, on va la concrétiser par cet exemple :

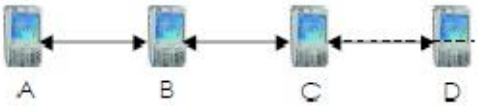


Figure 3.8 : Chiffrement en oignon.

Pour réussir à véhiculer un paquet de données depuis le nœud (A) jusqu'à le nœud (D), on suppose qu'un chemin est établi relayant le nœud (A) au nœud (D). La solution 'oignon chiffré' est schématisée par [B, [C, [D] P_C] P_B] P_A, où $\mathbf{P_N}$ représente la clé publique du nœud (N). S'étalons plus sur cette écriture en la déchiffrant comme suit : le nœud (A) recherche l'adresse du nœud (B) vers qui il émet le paquet, et comme les autres adresses sont asymétriquement chiffrées, cachées, il arrive que le nœud (A) ne peut pas les déduire, on parle de (C) et (D). En appliquant la même procédure, les nœuds (B) et (C) obtiennent l'adresse du nœud suivant, en optant pour l'usage de leurs propres clé privées, afin d'acheminer le paquet.

III.4.5) Solution pour la confidentialité: [GND.03]

Frequency Hoping est une solution se basant sur un envoie de données grâce à une séquence de fréquences, destinée à assurer la confidentialité dans les réseaux ad hoc. Le nœud adversaire devrait savoir cette séquence pour qu'il puisse se synchroniser en réception. Après avoir authentifié les nœuds du réseau, il reste à appliquer les mécanismes d'une cryptographie symétrique qui consiste à utiliser la même clé pour crypter et décrypter le message [MOB.06], pour obtenir des transmissions confidentielles.

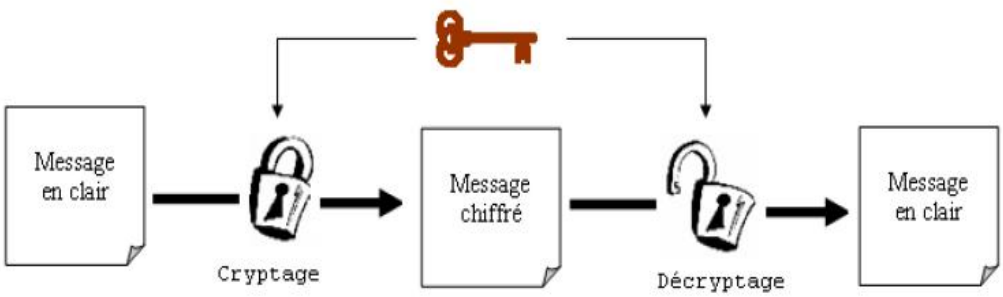


Figure 3.9 : Chiffrement symétrique.

III.4.6) Solution pour Blackhole: [GND.03]

Contrer les attaques d'un nœud malicieux de type Blackhole sur les protocoles de routage, revient à mettre aux point deux solutions : en premier lieu, le ***watchdog*** qui est une technique se chargeant d'identifier les nœuds adversaires, et en deuxième lieu, on a la technique de ***pathrater*** qui permet au protocole de routage d'échapper aux nœuds malicieux appartenant à la liste noire, ***blacklist***.

Ces deux solutions présentent un manque que le système de détection d'intrusion peut être une solution complémentaire. L'***IDS*** est destiné à recueillir et analyser les informations relatives au trafic pour capturer les éléments non autorisés dans le réseau et ceux se comportant de manière bizarre.

III.5) Le modèle de coopération :

Un environnement de fonctionnement dépourvu des attaques subtiles portant sur la disponibilité des services et l'intégrité d'informations, plus une consommation énergétique optimale résultant de la solidarité des nœuds dans le réseau, sont deux hypothèses mises en œuvre par les protocoles de routage ad hoc dans des études récentes. Prémunir le routage dans les réseaux ad hoc qui ne possèdent pas une administration centralisée, se ramène à contrer l'ensemble des vulnérabilités comme l'altération des tables de routage, la modification des paquets en transit, l'abstention au routage afin de préserver de l'énergie. Et sur ce dernier point, plusieurs protocoles forment leur hypothèse qui relate que les nœuds du réseau coopèrent pour acheminer les paquets des autres nœuds. Or que sur le plan pratique, cette hypothèse n'est pas toujours satisfaite du fait que certains nœuds s'attendent à une récompense ou un profit à l'issu de leur coopération.

Les modèles de renforcement de coopération concourant à encourager et collaborer les nœuds du réseau entre eux, ont suscités un double classement :

1) Modèle basé sur la réputation, reputation-based.
2) Modèle basé sur les crédits, credit-based.

Et pour pallier à l'égoïsme des nœuds et le manque de collaboration entre eux pour réduire la consommation d'énergie, de nombreux protocoles découlent de la proposition de renforcement de coopération tel que : CORE, CONFIDANT,…etc.

III.5.1) CORE : [MIP.06]

Fondé sur une technique de surveillance distribuée (watchdog), CORE consiste en un mécanisme servant à imposer la coopération entre les nœuds. Le principe signé par ce mécanisme est de punir les nœuds refusant la coopération ou se comportant illégitimement en ne leur consentant pas les services de communication. Bien entendu, ce mécanisme est valable pour les autres fonctions du réseau, l'envoie de paquet, l'établissement des routes, la gestion de réseau et de localisation des nœuds.

CORE se réfère à une mesure de coopération qui est la réputation, qui se charge de confier chaque nœud à inciter la collaboration d'autres nœuds du réseau. Cette mesure est obtenue depuis les données collectées au niveau de chaque nœud et les données provenant d'autres nœuds du réseau qui participent à la transmission des messages avec les nœuds surveillés.

En effet, un réseau ad hoc mettant en valeur le mécanisme CORE, se contente d'une consommation réduite de l'énergie qui s'explique par le fait que les nœuds collaborant au sein du réseau ne servent pas les nœuds illégitimes s'avérant égoïstes.

III.5.2) CONFIDANT : [REO.05], [ALI.09]

Largement inspiré du protocole de routage réactif DSR, CONFIDANT (Cooperation Of Nodes Fairness In Dynamic Ad hoc Network) est une technique élaborée par Buchegger et Bordec pour gérer au mieux le processus de découverte de route tout en abstenant les entités illégitimes.

Le principe de fonctionnement de CONFIDANT consiste à attribuer à chaque nœud un processus de quatre phases comme suit :

La phase Monitor ou gestionnaire est conçue pour surveiller et capter une conduite égoïste d'un nœud, et puis appeler le système de réputation qui examine le routage et le comportement des communications selon le protocole du réseau, et par la suite, si le nœud reçoit une observation malicieuse d'autres nœuds, il délivre des messages d'alarmes depuis le gestionnaire de confiance (Trust Manager) annonçant la présence d'un nœud illégitime dans le réseau. Il est à noter que les messages émanant des nœuds étrangers subissent d'abord une évaluation de véracité et d'origine avant de réagir. Le problème dont il souffre ce mécanisme, consiste en la nécessité de relations de confiance préétablies qui visent à évaluer la coopération des nœuds dans le réseau.

Dans le cas où plusieurs messages d'alarmes de malveillance concernant un nœud sont reçus, l'information est transmise au système de réputation qui maintient une table avec des entrées représentant les nœuds et leur estimation. Une fois qu'il a eu lieu de plusieurs messages indiquant un comportement malveillant ou si une mauvaise conduite est reçue un certain nombre de fois, cette estimation sera mise à jour. En outre, chaque nœud est lui assigné un ***rang*** susceptible d'être changer par une fonction ***Taux*** qui fournit le poids le plus important de sa propre expérience. Au moment où ce taux dépasse un seuil précis, la phase de gestionnaire de route, Path Manager, sera déclenchée, et alors, elle élimine les routes ayant des nœuds malveillants et les regroupe dans un cache afin de générer une alarme concernant ce nœud.

La première version de CONFIDANT est celle de PGP qui est vulnérable pour la propagation des phéromones, une deuxième version venant appréhender le problème posé par la première version, se base sur un modèle Bayesian qui organise et élimine les nœuds menteurs.

III.5.3) NUGLETS : [REO.05]

L'objectif de ce protocole est de pousser les nœuds du réseau à participer au processus d'acheminement des paquets (packet forwarding) et d'abstenir la surcharge du réseau.

Une ***nuglet*** ou encore appelée ***devise virtuelle*** circulant entre les nœuds du réseau qui concourent au protocole de routage des paquets, est gérée à l'aide d'un module de sécurité matériel, ***tamperproof hardware***. De cet échange, découle deux modèles.

1) ***Le modèle Packet Purse*** : les nuglets sont incorporées dans chaque paquet en transitant par les relais qui conservent une portion du nuglet, jusqu'à la destination. En effet, ce modèle résulte que les nœuds sont dissuadés de surcharger le réseau.
2) ***Le modèle Packet Trade*** : dans ce modèle, les nœuds appartenant à l'itinéraire reliant la source à la destination du trafic ont recourt à acheter les paquets et par la suite les vendre. De ce fait, il en résulte que c'est la destination du trafic qui doit endosser le payement de la réception des paquets.

Le point positif signé par cette stratégie est que le nœud source ignore à l'avance le nombre de nuglets à inclure dans un paquet, et ce à la charge du concept de découragement relatif à la surcharge du réseau qui n'est plus maintenu.

III.6) Conclusion :

Ce chapitre montre un point très subtil agaçant les réseaux ad hoc de part leur nature, la sécurité. Après avoir donné un bref aperçu sur la sécurité, on a illustré par quelques attaques qui nous semblent percutantes, et à la fin, on a présenté quelques solutions concourant à appréhender les attaques pour prémunir ce type de réseau.

La sécurité dans les réseaux ad hoc fait l'objet d'une vaste panoplie de sujets de recherche vue leurs amplifications fulgurantes et leurs caractéristiques, mais il reste à mentionner que sur le plan pratique, il n'existe qu'une minorité de techniques qui ont pu satisfaire les différentes contraintes inhérentes à leurs infrastructures. Parmi les thèmes de recherches traitant la sécurité dans les réseaux ad hoc, un axe s'accentuant spécialement sur les algorithmes de routage qui réclament une sensibilité accrue que doivent la résoudre convenablement pour garantir un déploiement subtil et protégé de ces réseaux.

PARTIE II

CONTRIBUTION :

ETUDE DES VULNERABILITES DE PROTOCOLE AntTrust ET PROPOSITION D'UN MODELE POUR LE SECURISER.

CHAPITRE IV

LE PROTOCOLE *AntTrust*,

PRINCIPES, FONCTIONNALITES ET FAILLES.

IV.1) Introduction :

Plusieurs efforts de recherche ont été entrepris ces dernières années dans le cadre de proposer de nouveaux protocoles de routage répondant aux problèmes subtils signés par l'absence d'infrastructure et la mobilité des nœuds dans un réseau ad hoc.

A travers ce chapitre, on va expliquer d'une façon détaillée le fonctionnement du protocole de routage AntTrust, ainsi les vulnérabilités et les attaques relatives à ce protocole.

IV.2) L'idée de base du protocole AntTrust:[ART.08], [RMA.08]

Dans le souci de proposer un protocole de routage comblant les lacunes qui découlent des protocoles déjà vus, AntTrust part de l'idée de base s'accentuant sur le principe de colonies de fourmis et qui consiste à établir un système multi-agents en procédant deux manières à la découverte de routes : active et proactive. [BON.08][MOJ.06][ZAM.10]

Au sein du routage, le concept des agents mobiles recense deux sortes d'agents : l'agent mobile Ant et l'agent mobile rectificateur. Le premier agent mobile est sensé d'opter pour deux manière différentes de découvrir les routes, en outre, le deuxième agent mobile est sujet à être déclencher par un élément du réseau à chaque fois qu'il détecte une fluctuation topologique du réseau ou un problème de coupure de liens.

L'apport décelé par la mise en place d'un protocole s'inspirant d'un système multi-agent peut être perçu par l'autonomie des agents. Ce protocole répond aussi en termes de la grande dynamité et l'auto-organisation du réseau.

Et pour compléter l'image de ce protocole, on s'est servi de la figure suivante qu'on a tirée de [RMA.08] et qui détaille plus le principe de fonctionnement de notre protocole AntTrust.

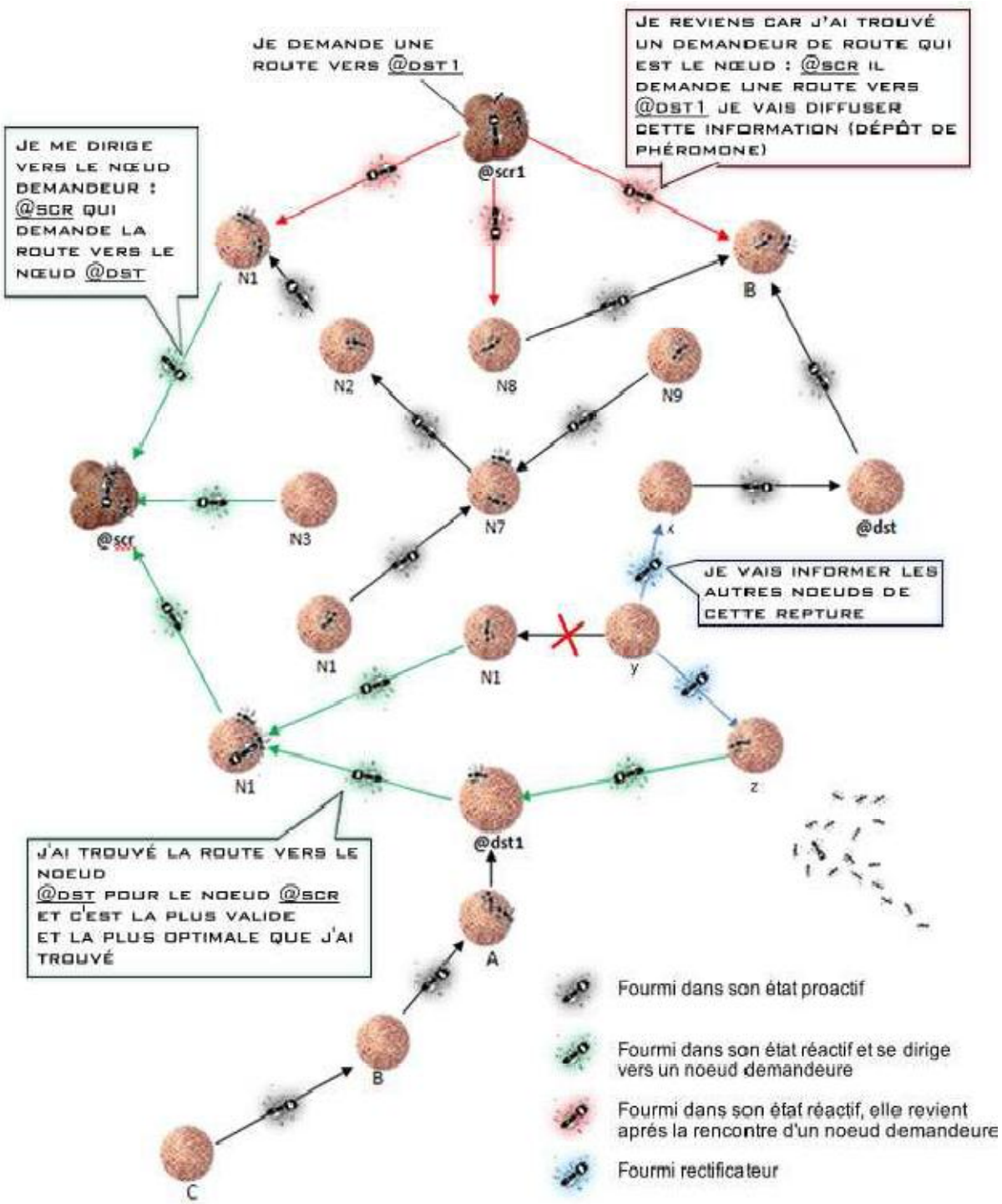


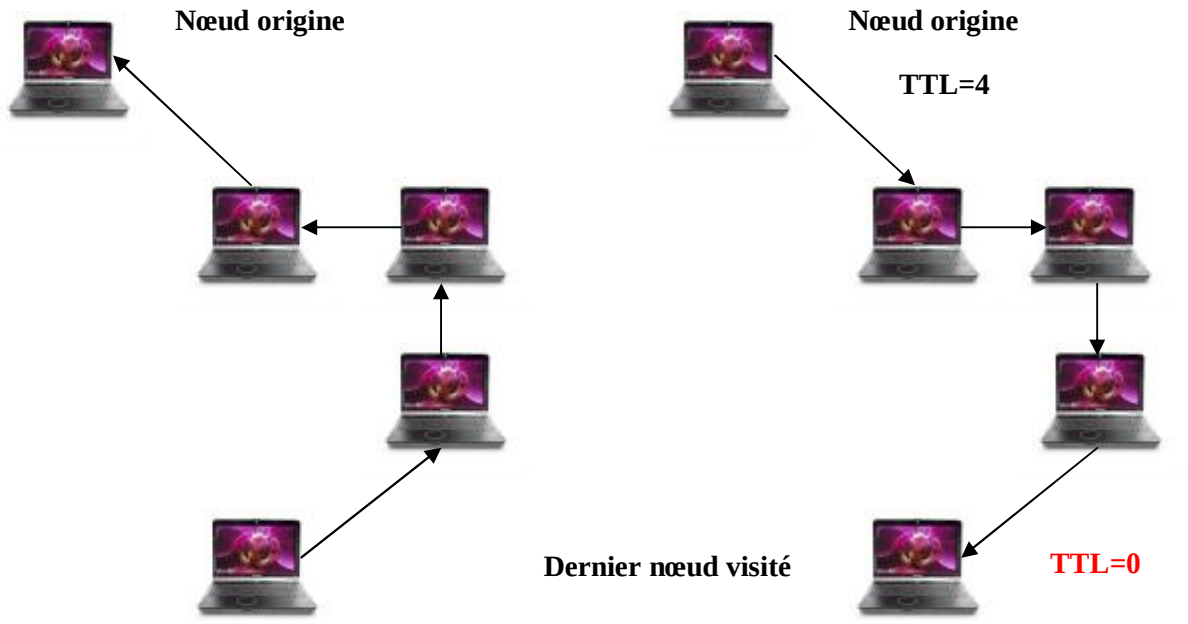
Figure 4.1: Le principe de fonctionnement du protocole AntTrust.

IV.2.1) La méthode proactive du protocole AntTrust: [ART.08], [RMA.08], [ALI.09]

Dans le cadre du protocole AntTrust, cette méthode dicte que chaque nœud ait recourt à émettre d'une façon régulière un agent Ant mobile appelé à accomplir la découverte de chemins optimaux et robustes. Ce concept permet de réduire au maximum les messages de contrôles qui s'avèrent gourmands en bande passante.

Ce protocole, pour le calcul et la maintenance des routes entre les nœuds, opère sur les agents mobiles Ant qui sont répandus par chacun des nœuds du réseau régulièrement. Bien entendu, un agent Ant n'est lié qu'à un seul nœud origine. En transitant entre les nœuds dans un réseau et arrivant sur un nœud, l'agent mobile procède à construire un lien entre ce nœud et son origine comme illustre la figure suivante. Et pour s'abstenir aux boucles de routage, chaque agent Ant est lui assigné un identificateur <***Node ID, Ant ID***> où ***Node ID*** réfère le nœud origine, tandis que ***Ant ID*** est incrémenté à chaque fois que le nœud origine génère un nouvel agent. Dans le cas où un même agent Ant est reçu plusieurs fois par un nœud, ce dernier accepte les informations délivrées par le premier agent Ant mobile et met en cause le reste des agents mobiles.

Et pour investiguer les tâches des agents Ant, il arrive que chaque nœud attribue une valeur de durée de vie proportionnelle à la taille du réseau, TTL, représentant le nombre de nœuds à visiter. En se déplaçant dans le réseau, deux phases sortent aux yeux, les agents Ant mobiles en phase Aller découvrent des routes vers leurs nœuds d'origine et vers le dernier nœud visité en phase Retour, TTL=0.



(a) : phase Aller. **(b)** : phase Retour.

Figure 4.2 : L'étape proactive du protocole AntTrust.

IV.2.2) La méthode réactive du protocole AntTrust: [ART.08],[RMA.08],[ALI.09]

Lorsqu'un nœud souhaite véhiculer un paquet de données à une destination alors que cette dernière n'apparait pas dans sa table de routage, il génère une demande locale d'établissement de route vers cette destination. Et dans l'objectif de satisfaire cette demande, les agents optent pour une conduite hybride, autrement dit, l'approche réactive fait appel aux agents se trouvant sur le réseau durant l'état proactif.

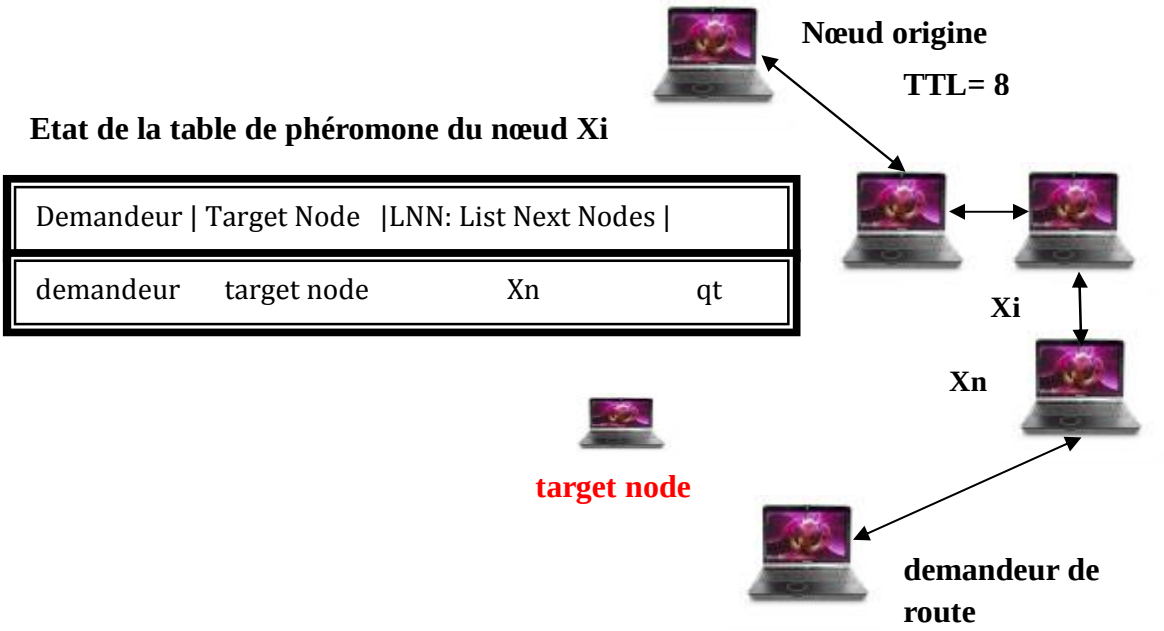


Figure 4.3 : L'étape réactive du protocole AntTrust.

En se référant à la figure ci-dessus, lorsqu'un nœud désire transmettre un paquet de données vers un autre nœud or qu'il ne dispose pas d'un chemin menant à ce dernier, il génère alors une demande locale de découverte d'itinéraire vers cette destination. Il faut signaler que l'unique cas qui pousse un agent Ant à déclencher sa phase Retour bien avant que son TTL ne s'annule c'est au moment où il visite un nœud demandeur de route. Durant son retour, l'agent dépose une quantité de phéromone au niveau de chaque nœud transité depuis le nœud demandeur vers le nœud origine dans le but de mettre les autres agents au courant de cette demande. A cet effet, il en résulte que les agents Ants s'intéressent plus au nœud demandeur.

Durant la phase proactive, un agent mobile en arrivant à un nœud sélectionne le prochain nœud à transiter, et ce en proportion à la quantité de phéromones. La probabilité de sélection du prochain nœud $\mathbf{n_i}$ parmi les autre nœuds $\mathbf{n_k}$ est donné par la formule suivante :

$$p\ (n_i) = Q_i \,/\, \sum_{nj\ \epsilon\ N} Q_j$$

Tel que :

N : tous les nœuds du réseau.

nj : représente les voisins du nœud courant.

$\boldsymbol{Q_i}$: représente la quantité de phéromones du nœud ***i***.

IV.2.3) La robustesse de la route : [ART.08],[RMA.08],[ALI.09]

L'idée centrale abordée dans ce protocole est de pouvoir fournir la route la plus courte et la plus robuste. A chaque fois qu'il arrive à un nœud, l'agent mobile procède à la mise à jour des informations concernant le routage locale et se serve des informations contenues dans la table de routage relatives au nœud visité pour rafraichir ses propres informations de routage. Et dans cette compréhension, prenons l'exemple où cet agent qui est en phase réactive se mène vers un nœud demandeur, il arrive qu'il va opter pour un chemin optimale et valide conduisant à la destination désirée par le nœud demandeur.

IV.2.4) La maintenance des routes : [ART.08],[RMA.08],[ALI.09]

On se situe au niveau de la volatilité et la mobilité des nœuds qui s'expriment en terme de la dynamité topologique du réseau, ce protocole se serve d'un agent ***Ant Rectifier*** qui est suscité par un nœud une fois qu'il constate une coupure de lien vers un nœud voisin appartenant à la table de routage du nœud courant du point qu'il consiste en le prochain saut à une destination bien définie. Après avoir généré les agents ***Ant Rectifier***, ils sont propagés dans leur voisinage susceptible de cette destination inatteignable pour renseigner les nœuds voisins à propos de la fluctuation de la topologie, et ainsi prendre en considération cette nouvelle information. Ce mécanisme est itéré par chacun des voisins en question, ce qui s'oppose avec le protocole AODV qui transmit un message d'erreur vers tous les nœuds y compris ceux non intéressés par cette rupture de lien.

IV.3) Description détaillée de fonctionnement du protocole :[ART.08], [RMA.08]

Cette section s'attache à la description du protocole AntTrust qui traite en passage quelques définitions qui nous semblent majeures, les différentes tables de routage élaborées par l'ensemble des nœuds du réseau, et sera pliée par les principes de fonctionnalité de chaque type d'agent.

IV.3.1) Définition :

Le travail collaboratif et commutatif des fourmis en colonies a occasionné par émergence leur aptitude de remédier aux problèmes d'optimisation telle que la découverte de plus courte route reliant leur nid à la source de nourriture. **[BAM.09]**

Revenant au domaine informatique, toute route établie par cette colonie de fourmis, relie deux entités x, y du réseau. Cette route est formulée par une suite de nœuds tel que (x) désigne le nœud source (initial) et (y) représente le nœud destination (terminal).

Route (x, y) = (x, i1, i2,……, y) où :

- Init (Route(x, y)) = x ;
- Terminal (Route (x, y)) = y ;
- Suiv (i_k) =i_{k+1} , est le nœud successeur de i_k dans la Route (x, y).

IV.3.2) Les tables gérées par les nœuds : [ART.08],[RMA.08],[ALI.09]

En raison de leurs besoins, les nœuds mettent en relief trois tables distinctes permettant de garder quelques informations, nécessaires, à solliciter lors des déplacements des agents, des calculs des routes ainsi l'acheminement de paquets de données.

IV.3.2.1) La table de routage :

Se situant au niveau de la table de routage, ***TABROUT***, qui est sensée de router les paquets de données, est structurée comme suit :

Destination *Dest*	**Nœud suivant** *N-suiv*	**Distance** *D*	**Liste-voisins** *Listv*	**Numéro de séquence** *Seqn*	**Date expiration** *E*	**Etat** *Stat*

Tableau 4.1 : Table de routage.

Cette figure permet de distinguer les entrées de la table de routage du nœud qui sont :

- ***Dest*** : représente l'adresse de nœud destination ;
- ***N-suiv*** : représente l'adresse de prochain nœud permettant de parvenir à cette destination ;
- ***D*** : représente la distance séparant le nœud de la destination, exprimée par le nombre de sauts restant.
- ***Listv*** : représente la liste des nœuds voisins concernés par cette route ;
- ***Seqn*** : représente le numéro de séquence qui sera incrémenté à chaque fois que le nœud se déplace ;
- ***E*** : représente la date d'expiration de l'entrée, i.e, la durée nécessaire calculée par l'agent lors du son transit pour atteindre la destination ;
- ***Stat*** : représente l'état de l'entrée, up, down, in-reparation ;

Il est à noter qu'une table de routage, s'accompagne d'une clé sous la forme ***<Destination, Nœud-suivant>,*** est rafraichie en sauvegardant les routes menant à la destination grâce au transit des agents.

D'une manière cohérente et consistante, et en respectant le concept des multi-chemins de ce protocole, chaque nœud est appelé à sélectionner la route la plus courte et la plus optimale. Cette route doit affranchir et satisfaire l'un des points suivants :

Ä ***Point n° 1*** : prenons l'exemple de deux routes ***Route i (x, y)*** et ***Route j (x, y)*** ;

L'optimalité de la route doit quasiment respecter la relation suivante :

Route i (x, y) != Route j (x, y) => suiv(init(Route i (x, y))) != suiv(init(Route j (x, y))).

Ä ***Point n° 2*** : bien entendu, lorsqu'un nœud (S) désire véhiculer un paquet de données vers un nœud destination (D), il opte pour la route la plus courte, en se penchant sur la distance ou sur le temps, en procédant comme suit :

Mettons : ***Routes(S, D)*** ∈ ***TABROUTs :*** l'ensemble des routes disponibles pour la destination (D).

RouteOptimale (S, D) = Route I (S, D) € Routes (S, D) tel que:

TABROUTs[D, suiv(init(Route i (S, D)))].D <= TABROUTs[D, suiv(init(Route j (x, y)))].D

pour toute route ***Route j (x, y) € Routes(S, D) - {Route i (x, y)}***

De plus, à l'égard de l'aptitude des agents Ant à estimer le temps écoulé pour se déplacer d'un nœud à un autre, une autre technique de calcul de la route optimale peut être donnée par :

RouteOptimale(S, D) = Route i (S, D) ϵ Routes (S, D) tel que:

TABROUTs [D, suiv(init(Route i(S, D)))].t <= TABROUTs[D, suiv(init(Route j (x, y)))].t

Pour toute route ***Route j (x, y) ϵ Routes (S, D) - {Route i (x, y)}.***

IV.3.2.2) La table de voisinage : [ART.08],[RMA.08],[ALI.09]

Comme son nom l'indique, cette table (***TABV***) renferme la liste des nœuds voisins ainsi le type de lien existant entre eux. Construire cette table revient à propager périodiquement des messages ***Hello*** à tous les nœuds voisins à un seul saut, ***TTL***=1. Chaque message s'est muni d'un ensemble d'adresses des nœuds pour lesquels il a reçu le message ***Hello***. En recevant un nouveau message ***Hello***, le nœud se charge de vérifier l'existence de son adresse dans la liste des voisins incluse dans le message, si c'est le cas, l'état du lien avec le nœud émetteur du message devient bidirectionnel.

Liste des voisins	**Type de lien**
V1, v2, v3, …etc.	**Unidirectionnel / bidirectionnel**

Tableau 4.2 : Table de voisinage.

Il est clair que le choix de la valeur du ***TTL*** est tributaire à la taille du réseau. Cette valeur souligne diverses cibles qui sont :

- ≈ Une meilleure supervision de mobilités des agents ;
- ≈ Une meilleure exploration des différentes portées des nœuds et ainsi garder figé le nombre d'agents manifestant sur le réseau.

IV.3.2.3) Table de phéromones : [ART.08],[RMA.08],[ALI.09]

Le rôle majeur qui s'attache à la table de phéromone, ***TABPH***, est de concourir au transit des agents Ant, et ce du fait qu'ils établissent leurs choix sur le prochain nœud vers lequel se déplacer d'une façon stochastique et proportionnelle à la quantité de phéromones. Durant leurs retours, chacun d'eux agit sur la table de phéromone du nœud visité en la rafraichissant.

En effet, l'existence de chaque entrée de la table de phéromone est intimement liée au mécanisme d'évaporation des quantités de phéromone qui est décrémentées d'une manière régulière, et lorsque cette quantité s'annule, l'entrée en question est supprimée.

Demandeur	Destination de demande	Liste voisins	Quantité de phéromone
X1	Xn	V1, V2, …etc	Qté

Tableau 4.3 : Table de phéromone.

IV.4) Fonctionnement : [ART.08],[RMA.08],[ALI.09]

Les deux types d'agents mobiles recensés dans le protocole AntTrust sont : l'agent Ant, chargé de l'établissement des routes, l'agent Ant Rectifier qui repose essentiellement sur la rectification des erreurs de routage provoquées par la variation continuelle de la topologie du réseau.

Cette organisation stipule que chacun des nœuds du réseau est lui conféré un seul agent de chaque type, et ce pour une durée d'attente initialisée par chaque nœud localement pendant laquelle ce dernier attend le retour de l'agent Ant généré antérieurement.

Il faut bien noter que tout agent Ant subisse un double comportement distinct s'illustrant lors la phase Aller et la phase Retour. Ainsi, chaque nœud du réseau donne lieu à un nouveau agent Ant, et ce au moment de son intégration dans le réseau ou lors de l'expiration de temps d'attente ou bien pendant la phase du retour du l'agent dont sa durée de vie n'a pas encore écoulée.

IV.4.1) agent Ant: [ART.08],[RMA.08],[ALI.09]

Un agent Ant est une entité réelle ou virtuelle dont le comportement est autonome. Cette définition aborde un certain nombre d'informations :

- L'adresse du nœud créateur de l'agent nommé ***NœudOrigine***.
- Le sens de direction de l'agent, ***Aller*** ou ***Retour***.
- Un numéro de séquence, ***SeqNumber***, incrémenté toute fois que le nœud créateur se déplace.
- L'adresse du dernier nœud transité qui est initialisée à l'adresse du nœud origine.

- Un champ ***TTL*** qui sera décrémenté après chaque transition, saut.
- La liste des nœuds pré-transités.
- Un ***NœudCible*** destiné à mémoriser l'adresse d'un nœud élaborant l'établissement d'une route à une destination dont l'agent la stocke dans une variable ***DestDemand***.
- Un ***NœudEtabRout*** renfermant l'adresse du nœud vers lequel l'agent est entrain de créer une route. Elle est initialisée à ***NœudOrigine***.
- Une valeur booléenne portant sur la validité de la route du ***NœudPreced*** vers ***NœudEtabRout***, initialement est à vrai.
- Le nombre de sauts, ***NS*** initialement nul, permettant d'accéder à ***NœudEtabRout***.
- ***NœudSuiv*** représente le nœud suivant que l'agent va visiter.
- Le temps consommé pour se déplacer de ***NœudEtabRout*** vers le nœud courant désigné par '***t***'.
- Un identificateur de l'agent, ***ID***, qui est incrémenté à chaque envoie d'un nouvel agent.
- Des champs réservés '***reserved***' spécifiques à des utilisations ultérieures.

Le couple « ***identifiant***, ***adresse*** »propre à l'agent, joue un rôle primordial dans la détection des boucles qui peuvent avoir lieu. Entre outre, si un nœud reçoit successivement un même agent, il procède sans égard pour l'information transportée par l'agent lors de la mise à jour de la table de routage. Cela peut être réalisé par un test permettant de savoir si le prochain nœud est inclus dans la liste des nœuds déjà visités.

IV.4.1.1) Cycle de vie d'un agent Ant :

Le cycle de vie d'un agent Ant conjugue deux phases à invoquer dans ce qui suit :

IV.4.1.1.1) La phase Aller :

Un agent, le long de cette phase, est consacré à accomplir de multiples activités. Ainsi, un exemple d'agent partant d'un nœud (**i-1)** à un nœud (**i)** semble nécessaire pour illustrer les opérations présentées dans cette phase.

1) Mise à jour de la table de routage au niveau du nœud courant :

Ici l'agent essaye d'explorer une route valide et optimale depuis le dernier nœud visité vers un nœud indiqué par la variable ***NœudEtabRout*** qui peut être le nœud origine ou bien une destination sollicitée par un nœud.

Au court de son transit, un agent est appelé à véhiculer la route la plus optimale, en termes de nombre de sauts, disponible vers le ***NœudEtabRout***. En cas où

la route qu'il manifeste s'avère meilleure que celle se trouvant dans la table de routage, il procède alors à rafraichir l'entrée en question avec la nouvelle route et à mettre au courant les nœuds voisins intéressés par cette route en propageant des agents rectificateurs. En revanche, si la route transmise n'apparait pas dans la table de routage, l'agent suscite une nouvelle entrée pour cette nouvelle route. Ce qui caractérise une table de routage est qu'elle ne contient que les routes valides, et donc une opération de mise à jour n'est effectuée que si l'agent fait l'objet d'une meilleure route.

2) Mise à jour de ses propres informations :

Une telle étape s'applique par l'agent en mettant à jour ses informations locales, et ce en décrémentant son champs ***TTL*** par exemple et en intégrant le nœud (***i***) dans la liste des nœuds déjà visités.

3) Choisir le prochain nœud à visiter :

Puisque le choix du nœud successeur à traverser se fait stochastiquement, cela conduit à conférer la priorité aux nœuds voisins disposant d'une quantité de phéromone importante. Néanmoins, en cas où le prochain nœud à visiter par l'agent est celui demandeur de la route, les nœuds présents dans la liste des voisins de l'entrée de la table de phéromone correspondant au demandeur sont choisis à tour de rôle.

Bien entendu, choisir la meilleure route à destination de ***NœudEtabRout*** à propager, revient à sélectionner l'ensemble des routes menant vers ***NœudEtabRout*** ayant la plus grande valeur du ***SeqNumber***. Mais aussi, il arrive que ces ***NœudEtabRout*** possède tous le même nombre de séquence, et donc, mettre en œuvre celle soulignant la distance ou le temps le plus court.

IV.4.1.1.2) La phase Retour :

Cette phase consiste en la deuxième partie de cycle de vie d'un agent Ant. Ce dernier passe à cette phase soit parce que son ***TTL*** est expiré, ou bien du fait qu'il a croisé une demande d'établissement de route, ou en confrontant un nœud demandeur d'une route dont il est porteur.

Au sein de cette phase, l'agent opère pour découvrir une route en empruntant le parcourt inverse, autrement dit, il esquisse son trajet depuis le dernier nœud transité lors de la phase ***Aller*** en se dirigeant vers son nœud d'origine ou créateur. Ainsi, comme mentionné plus haut, un agent en passant par un nœud demandeur de route pendant sa phase ***Aller***, il procède à quitter cette phase au profit de la phase ***Retour*** et ainsi il dépose une quantité de phéromone à l'entrée appropriée au nœud générant la demande dans la table de phéromones correspondante à chaque nœud visité durant son retour afin d'indiquer aux autres nœuds la présence d'une demande de découverte de route.

Pour une efficacité maximale de route, un agent en passant par chaque nœud, il se sert à actualiser les informations de routage locales et à rafraichir les informations de routage

appropriées à lui en s'accentuant sur les informations de routage locales. L'efficacité ou l'optimalité de la route doit satisfaire les deux points suivants : elle doit être la plus récente route dotée du plus grand numéro de séquence et elle doit offrir une distance succincte.

IV.4.2) Agent rectificateur ou *Rectifier*: [ART.08],[RMA.08],[ALI.09]

La solution proposée dans le contexte de pallier aux problèmes issus de la mobilité des nœuds est l'agent ***Rectificateur*** dont il est généré par un nœud à chaque fois qu'un de ces cas se présente :

- **Cas n° 1 :** détecter une coupure de lien avec un voisin revient à suivre l'une de ces approches :

  1) Cette approche se centre sur la mise en œuvre des messages ***Hello*** déjà traités pour la construction de la table de voisinage, et donc, pour une durée d'attente bien précise, si un voisin n'a pas reçu un message ***Hello***, le lien avec ce voisin est déclaré rompu et donc mettre en cause l'entrée approprié dans la table de voisinage.

  2) La deuxième approche se profile au moment de la transmission d'un message de données dont son acquittement n'est pas reçu. A cet égard, il faut se disposer d'une couche de liaison de données faisant l'objet d'acquittement.

  Après avoir détecté la rupture, une mise en cause des entrées de la table de routage optant pour ce lien rompu est établie. Il est primordial de noter que bien avant ca, un agent ***Rectificateur*** est transmis pour tous les nœuds présents dans la liste des voisins. Cet agent une fois initialisé, se comporte tel qu'un agent Ant en accomplissant les mêmes activités concernant la mise à jour de la table de routage.

- **Cas n ° 2 :** la modification de la valeur d'une entrée de la table de routage ramène les agents ***Rectificateurs*** à corriger la route acheminant vers toutes les destinations penchant sur ce lien en signalant à l'ensemble des nœuds appartenant à la liste des voisins qui sont intéressés par cette route.

Après avoir reçu un agent ***Rectificateur***, le nœud actualise sa table de routage suivant les informations véhiculées par l'agent et ainsi crée un nouvel agent ***Rectifier*** destiné à propager l'information concernant cette nouvelle route.

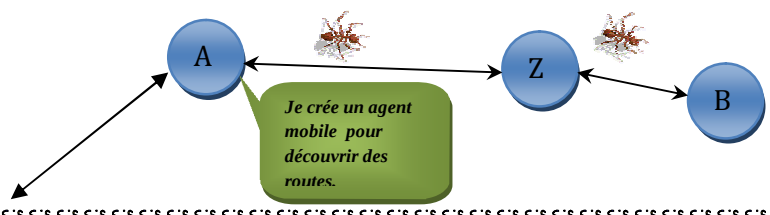
IV.5) Les failles du protocole :

Les sections précédentes de ce quatrième chapitre qui s'attachent à étudier le protocole de routage ***AntTrust*** s'appuyant sur le système multi-agents et se focalisant autour de l'approche de communauté de fourmis, nous ont aidés à faire une synthèse s'intéressant aux faiblesses issus de ce protocole, et ainsi, de déceler quelques restrictions invoquées par la non sécurisation du ***AntTrust*** et découlant de la propriété hybride du protocole qui supporte le caractère réactif et proactif des protocoles de routage au centre des réseaux ad hoc. Parmi celles qui nous paraissaient les plus importantes, on trouve :

IV.5.1) L'attaque par usurpation d'identité :

Vue déjà dans le chapitre précédant, cette attaque peut aussi toucher la sécurité et la performance du protocole en cours d'étude. Elle consiste à se faire passer pour quelqu'un d'autre en utilisant son identité après l'avoir mettre hors service, de manière plus clair, le nœud attaquant se présente en utilisant l'identité d'un nœud légitime en optant pour une comportement par déni de service, et donc, il peut communiquer avec les autres nœuds du réseau sans être rejeté.

Lors de la phase de découverte de routes, les agents Ant mobiles en transitant par les nœuds, collectent les informations permettant d'établir l'ensemble des chemins possibles dans le réseau pour des usages ultérieurs (voire figure (1)). En se plaçant dans la portée d'un nœud quelconque, le nœud attaquant peut usurper les informations relatives à l'identité d'un autre nœud du réseau en procédant d'abord à mettre hors service le nœud victime, ensuite, il propage un message de type ***Hello*** vers ses nouveaux voisins, ce qui fait que les agents mobiles quand le visitent, ils fournissent aux autres nœuds une fausse image de la topologie du réseau puisqu'ils transportent des informations erronées. Dans notre cas, le nœud illégitime (M) se met dans le champ de couverture des nœuds (X) et (Y), il met hors service le nœud qu'il souhaite usurper son identité qui est le nœud (Z), ensuite il change son adresse pour celle du nœud (Z) et déclare ainsi que les deux nœuds (X) et (Y) sont dans son voisinage (voire figure (2)). Une fois que le nœud source (@src1) dépose une demande locale pour établir un itinéraire vers une destination précise (@dest1), un agent mobile dans sa phase Aller en passant par ce nœud demandeur, dépose une quantité de phéromones et déclenche sa phase Retour en procédant ainsi à informer l'ensemble des nœuds visités lors de l'étape précédente de cette demande. Et de ce fait, les nœuds communiquent via le nœud (Z) sans se rendre compte de sa malveillance.



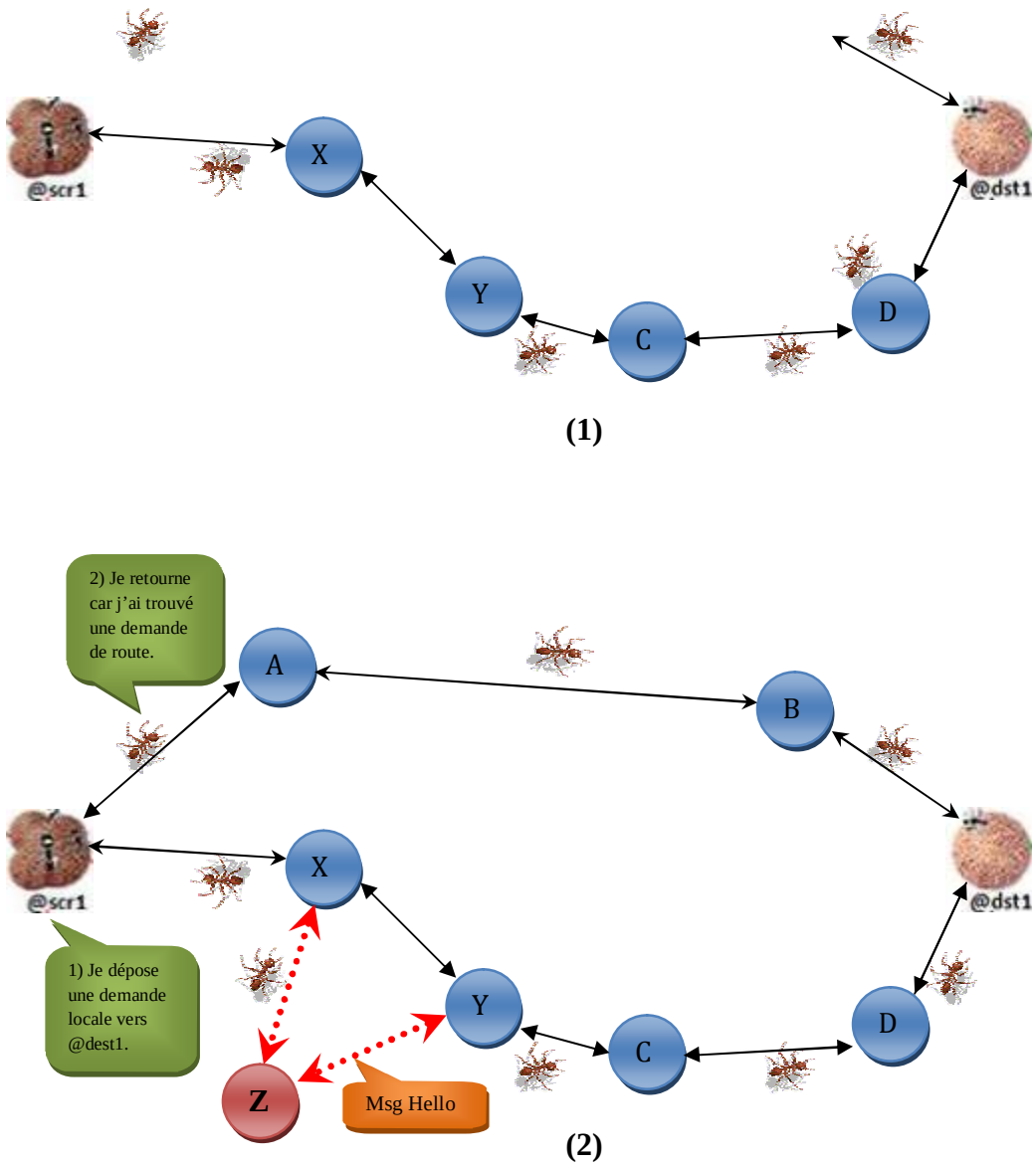


Figure 4.4 : les étapes de l'attaque par usurpation d'identité.

IV.5.2) L'attaque Sybil :

Dans de plusieurs situations et en raison de la versatilité de réseau ad hoc, il se peut que le protocole de routage ***AntTrust*** sera affronté par une autre vulnérabilité très inhérente intitulée ***Sybil***, touchant ainsi sa sécurité et ses performances. Dans cette attaque, un nœud malicieux se contente d'usurper son identité en fabriquant illégitimement de multiples identités, autrement dit, il ne se prend pas juste pour un autre nœud mais voire pour un très grand nombre de nœuds.

A l'ambre de cette attaque, trois démentions orthogonales possibles ont fait l'objet d'apparition et qui sont:

a) Communication directe vs communication indirecte :

Une première manière de faire, consiste à réaliser directement l'attaque ***Sybil*** entre un nœud légitime et un nœud ***Sybil***. Lorsqu'un message est transmis depuis un nœud légitime vers un nœud ***Sybil***, un nœud parmi les nœuds malveillants écoute le message.

Une deuxième façon faisant l'objet de cette attaque s'effectue indirectement du fait que les nœuds légitimes ne peuvent pas établir des communications directes avec les nœuds Sybil. Plus clair, à chaque fois qu'un nœud ***Sybil*** reçoit un message, il l'achemine via un de ces nœuds malicieux qui prétend à les envoyer vers la destination finale.

b) Identités fabriquées vs identités volée :

A la lumière de ce titre, un nœud ***Sybil*** est apte à avoir une identité soit en la créant en optant pour un identificateur aléatoirement, soit en se servant d'une déjà existante reflétant ainsi un nœud légitime du réseau.

L'absence d'une restriction à respecter pour la création d'une identité, ou l'absence d'une méthode adéquate pour la vérification de la légitimité d'une certaine identité, ont aidés énormément les nœuds ***Sybil*** à la fabrication des identités, de telle sorte qu'un nœud malicieux peut s'intégrer dans le réseau en fabriquant tout simplement une identité arbitraire.

En revanche, si l'attaquant ne peut pas adopter la fabrication des identités pour pénétrer le réseau, il se serve d'identités légitimes des nœuds du réseau et donc il utilise des identités volées. Le déroulement de cette opération de vol peut être mystérieux, l'attaquant met hors service les nœuds victimes.

c) Simultané vs non simultané :

Dans le cas simultané, l'attaquant se contente d'essayer de mobiliser tous ces identités simultanément, de les faire tous participer dans le réseau.

Dans l'autre cas, la participation des identités au réseau ne s'effectue pas simultanément. Pour une période de temps, l'attaquant peut présenter un nombre d'identité important, or que, pour une autre période de temps, il ne présente qu'un nombre très restreint d'identités. Il est à noter qu'une identité particulière peut joindre et déjoindre le réseau plusieurs fois.

IV.5.3) L'attaque par déni de service :

Le principe de cette attaque réside dans la création de routes vers des destinations inexistantes par le biais de dépôt locale de demandes d'établissement de routes vers des nœuds destinations n'appartenant pas au réseau. Lorsque les agents Ant mobiles visitent un tel nœud demandeur de route, ils lancent leur phase ***Retour*** en essayant de satisfaire cette demande en informant l'ensemble des nœuds visités lors de la phase ***Aller*** de cette demande, et donc, ils explorent plusieurs chemins en transitant par différents nœuds. A cet effet, il en résulte que les nœuds consomment leurs ressources énergétiques et leurs durées de vie inutilement dans la recherche de cette destination qui ne se présente pas réellement dans le réseau.

Se référant du schéma suivant mettant en place un simple réseau, le nœud (@src1) se comportant malicieusement peut dérouler cette attaque en déposant localement une demande d'établissement de route vers une certaine destination n'appartenant pas à l'ensemble du réseau, le nœud (X). Un agent Ant mobile en transitant par ce nœud initiateur de demande, il passe à la phase Retour afin de signaler aux autres nœuds cette demande, et ainsi de suite, chaque nœud faisant l'objet de réception de cette information essaye de trouver le chemin désiré. De cette manière, les agents Ant mobiles participants à la découverte de cette route exploitent négativement leurs durées de vie en se baladant dans le réseau à la recherche des nœuds inexistants, comme ils font perdre pour rien la capacité énergétique aux autres nœuds du réseau.

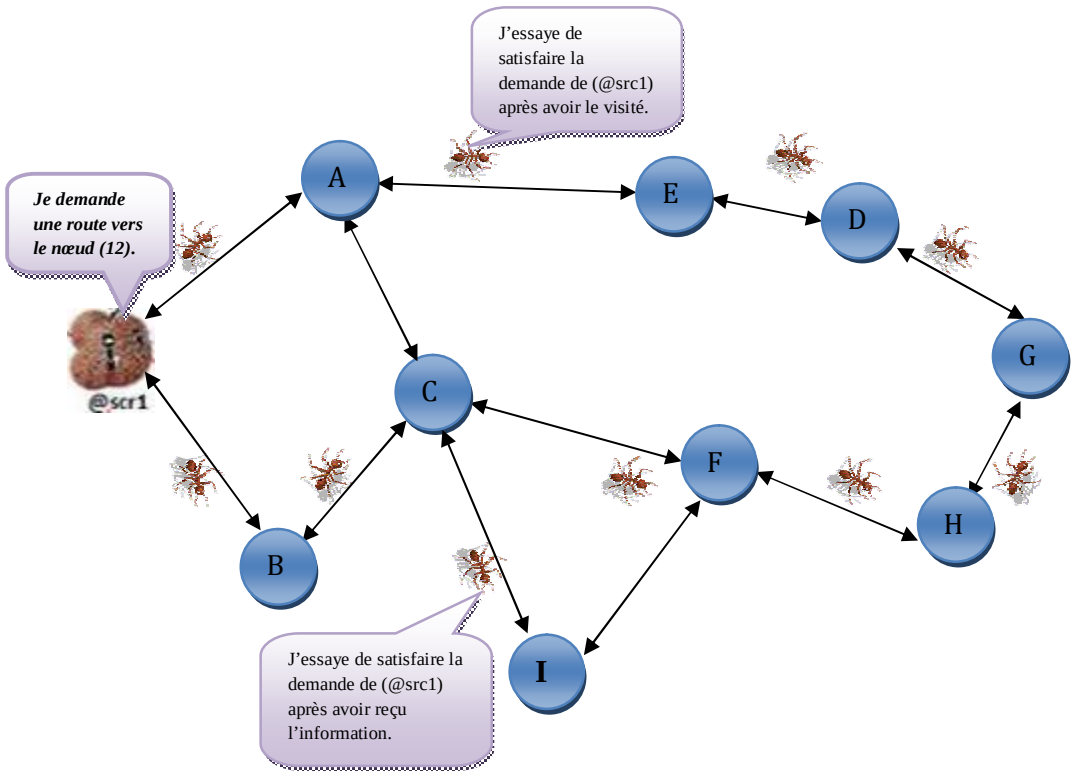


Figure 4.5 : L'attaque par déni de service.

IV.5.4) La non-retransmission des messages de données :

Le protocole ***AntTrust*** inspiré de la méthode de la colonie de fourmis et s'appuyant sur le paradigme d'agent mobile, met en conjonction ces deux critères en vue de la réalisation de l'hypothèse dictant que les nœuds doivent coopérer entre eux pour transporter les paquets de données à travers un réseau ad hoc. Mais sur le plan concret, cette hypothèse présente une limitation importante signée par l'égoïsme de certains nœuds mobiles du réseau, ayant peu de ressources, qui refusent cette participation si elle ne leur rend pas d'intérêts ou de profits.

Par conséquent, ce déni de service issu de mauvais comportement de quelques membres du réseau, peut engendrer le rejet total ou partial des données reçues par les agents Ant mobiles, et ce dans l'objectif de ne pas consommer ses ressources énergétiques. En d'autres termes, un nœud peut exploiter les services de routage offerts par les autres nœuds pour accomplir sa session de communication avec un nœud destinataire, entre outre, il ne le force pas à contribuer à l'acheminement des données transmises par les autres nœuds en optant pour les mêmes qualités de services. Une conduite pareille de nœuds de réseau entraine des limitations au niveau de routage des messages de données et une dégradation tangible de performance de services des éléments du réseau ad hoc.

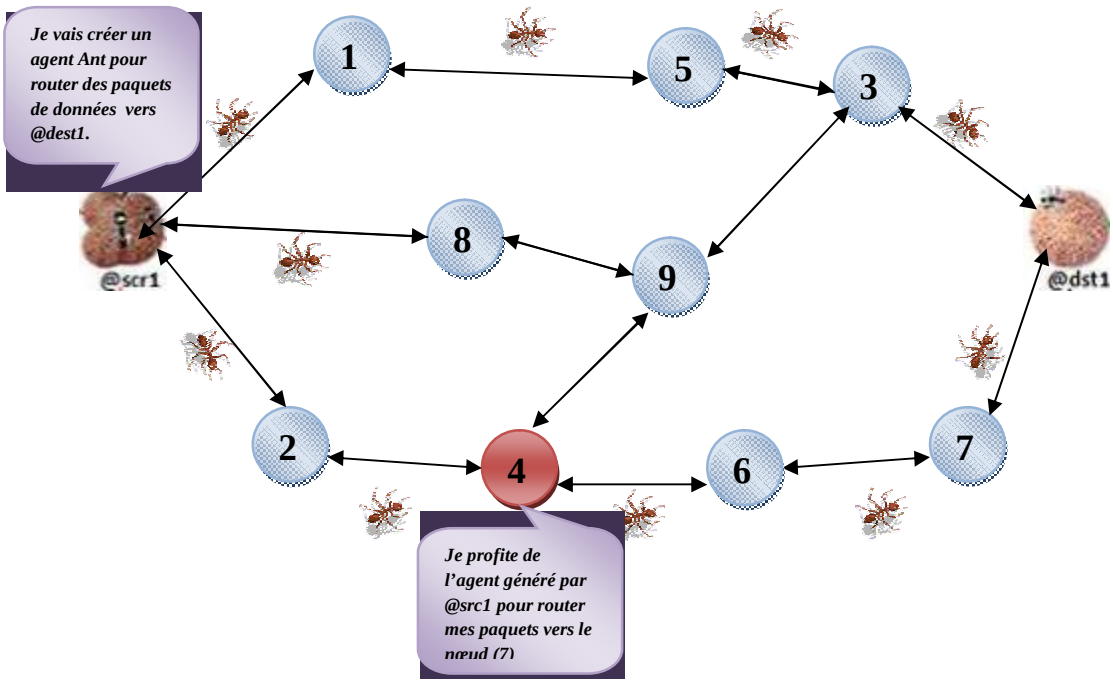


Figure 4.6 : La non-coopération des nœuds.

Se servant du schéma ci-dessus, mettant en place un réseau ad hoc où les éléments composants acheminent les informations entre eux grâce au protocole de routage ***AntTrust***, on va expliquer le contexte de cette attaque. Nous suggérons que le nœud (@src1) souhaite envoyer des paquets de données au nœud destination (@dest1) via le chemin se composant des nœuds (2), (4), (6) et (7). Ainsi, le nœud émetteur (@src1) envoie les paquets jusqu'à destination en transitant par les nœuds intermédiaires. Au sein du notre réseau et au moment du transit, il arrive qu'un nœud se comporte illégitimement en refusant de coopérer au routage des données, le nœud (4), il supprime une partie ou tous les paquets reçus par le nœud prédécesseur (le nœud (2)), et donc, il ne contribue pas au service de routage afin d'économiser la consommation de ses ressources énergétiques et se servir de cette communication établie par les autres nœuds du réseau pour accomplir sa propre tâche de routage et acheminer ses paquets de données à la destination envisagée, le nœud (7). Un tel comportement égoïste peut être adopté par plusieurs nœuds du réseau et influençant ainsi négativement les performances du réseau en engendrant une limitation plus ou moins importante concernant le concept de routage.

IV.5.5) L'attaque par suppression du trafic de routage :

Au cœur du protocole ***AntTrust***, l'attaque par suppression du trafic de routage ou la non-coopération des nœuds se veut bien dangereuse du fait qu'une partie de réseau devienne inaccessible ou isolée. Le contexte de cette attaque dicte que le nœud attaquant se penche sur la non-participation au processus de routage en rejetant ainsi les agents Ant mobiles qui ne le concernent pas, ou qui ne l'intéressent pas, ou qui ne l'appartiennent pas.

Eclaircissant un peu le contexte de cette attaque, lorsqu'un ensemble de nœuds est en communication en échangeant des agents Ant mobiles, soit pour découvrir des chemins ou pour acheminer des données à une certaine destination, un nœud malicieux en recevant des agents mobiles issus d'autres nœuds du réseau dont il ne les aurait pas besoin, il procède simplement à les supprimer et ignorer leur transmission vers ses voisins, ce qui résulte ainsi une isolation de ces nœuds interconnecté au réseau et donc, ils deviennent injoignables. Un tel comportement égoïste de nœud se profile essentiellement suite à la limitation de la charge et de la capacité de calcul des nœuds où à la malveillance des nœuds, et ce dans l'objectif d'altérer ou de compromettre le bon fonctionnement du réseau.

IV.5.6) L'attaque par falsification des erreurs de routes :

Sachant bien que le protocole de routage ***AntTrust*** pour remédier à une limitation tracassant les réseaux ad hoc et qui se résume par la forte mobilité des nœuds, il se serve d'un agent Ant ***Rectifier*** qui sera crée par chaque nœud après avoir constaté qu'un lien avec son voisin est rompu dans le but de mettre en connaissance l'ensemble des nœuds concernés par ce chemin.

Une attaque par falsification des erreurs de routes se réalise à l'aide d'un agent Ant ***Rectifier*** généré par un nœud illégitime, signalant ainsi une fausse information de coupure de lien à ses voisins intéressés par cet itinéraire pour les en informer. A leur tour, chaque nœud de ces derniers crée un nouvel agent ***Rectifier*** orienté à informer ses voisins de cette rupture, et ainsi de suite jusqu'à atteindre tous les nœuds du réseau qui utilisent ce lien. A cet égard, tous les nœuds concernés par ce lien rompu actualisent leurs tables de routage de façon conforme aux fausses informations transportées par les agents ***Rectifier***, et par conséquent, ils provoquent un déni de service du fait que certains éléments du réseau seront privés de communiquer entre eux.

Et pour mieux visualiser l'attaque par falsification des erreurs de routes, on va donner un concis exemple sur le principe de son fonctionnement en optant pour le réseau suivant :

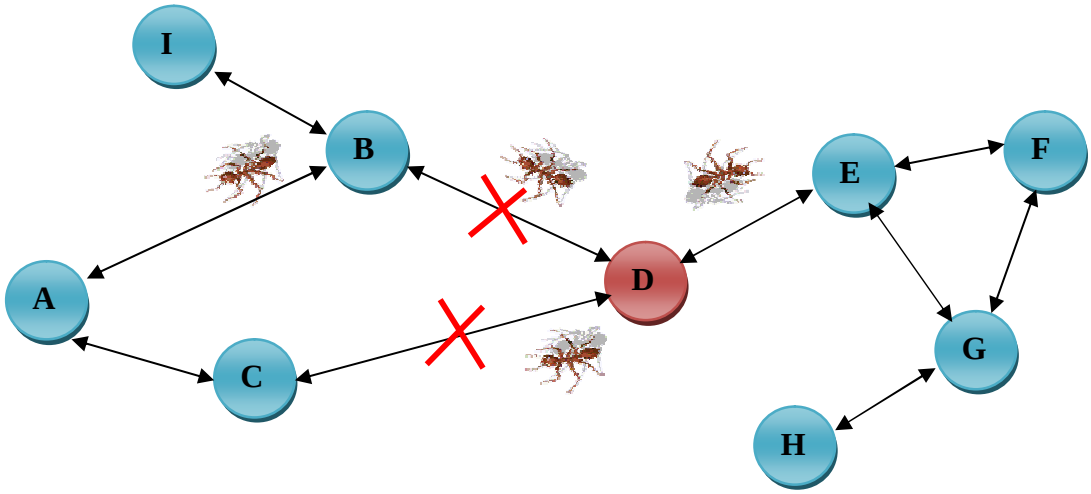


Figure 4.7 : Attaque par falsification des erreurs de routes.

Supposons que le nœud (D) opère avec malveillance dans le réseau, et pour réaliser cette attaque, il esquisse par l'envoie d'un agent ***Rectifier*** vers les nœuds du réseau en signalant qu'une coupure de lien avec le nœud voisin (B) est survenue (voire figure (1)). La réception d'une telle information implique que les nœuds concernés par ce chemin actualiseront leurs tables de routage et de voisinage. Ce nœud malicieux ne se suffise pas par une seule attaque, il génère donc un autre agent ***Rectifier*** indiquant cette fois ci que le chemin le reliant au nœud (C) est rompu. A cet égard, une autre mise à jour touchant les tables de routage et de voisinage s'avère nécessaire (voire figure (2)).

Le nœud	Listes des voisins
A	B, C
B	A, I
C	A, D
D	C, E
E	D, F, G
F	E, G
G	E, F, H
H	G

(1)

Le nœud	Listes des voisins
A	B, C
B	A, I
C	A
D	C, E
E	D, F, G
F	E, G
G	E, F, H
H	G

(2)

Tableau 4.4 : Tables de routage après la falsification des erreurs de route.

Ce processus sera répété par cet attaquant plusieurs fois jusqu'à ce qu'il atteindra son but, autrement dit, jusqu'à ce qu'il constate qu'une partie de réseau ne peut pas communiquer avec le reste des nœuds (voire figure 4.8). Il en résulte alors que les nœuds (A), (B), (C) et (I) seront isolés du réseau et ne peuvent communiquer avec les nœuds (D), (E), (F), (G), (H).

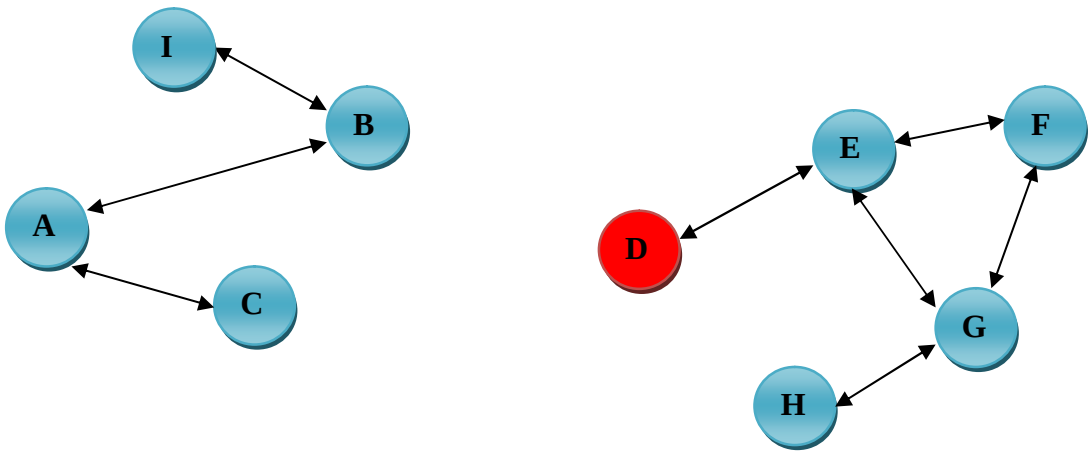


Figure 4.8 : Le réseau après la falsification des erreurs de routes.

IV.5.7) L'attaque par usurpation de liens :

Et dans l'objectif de rediriger le trafic ou de construire de plus longues routes, l'attaque par usurpation de liens représente un autre axe de failles pouvant porter sur le protocole de routage ***AntTrust***. Cette attaque consiste à provoquer des altérations de l'état de liens, soit lors de la génération des agents mobiles soit lors de leur retransmission. Ces altérations peuvent être réparties en deux catégories à savoir l'ajout de liens non-existants ou bien la suppression de liens existants.

Par l'ajout de liens qui n'existent pas, le nœud adversaire génère des agents Ant mobiles transportant un ensemble d'informations incorrectes à propos de l'état de liens avec ces voisins, autrement dit, il essaye de répandre des relations de voisinage non-existant sur le réseau via l'envoi de messages ***Hello*** à ces nouveaux voisins. Et comme résultat, cette première altération va réduire la distance séparant le nœud malicieux et les nœuds victimes à un saut. Et par l'élimination de liens existants, le nœud attaquant se contente de créer des agents Ant ***Rectifier*** appelés à propager de fausses informations concernant la rupture de liens existant sur le réseau. Due à cette altération, des pertes de connectivités avec le reste du réseau peuvent être soulignées par les nœuds voisins ignorés, aussi, il en résulte que les nœuds cibles voisins deviennent indirectement atteignables par le nœud adversaire et le contraire est vrai.

Pour une plus fine visualisation, nous avons optés pour le schéma suivant faisant l'objet d'un réseau ad hoc où les nœuds composants se communiquent à l'aide du protocole de routage ***AntTrust***, afin de mieux souligner l'attaque par usurpation de liens.

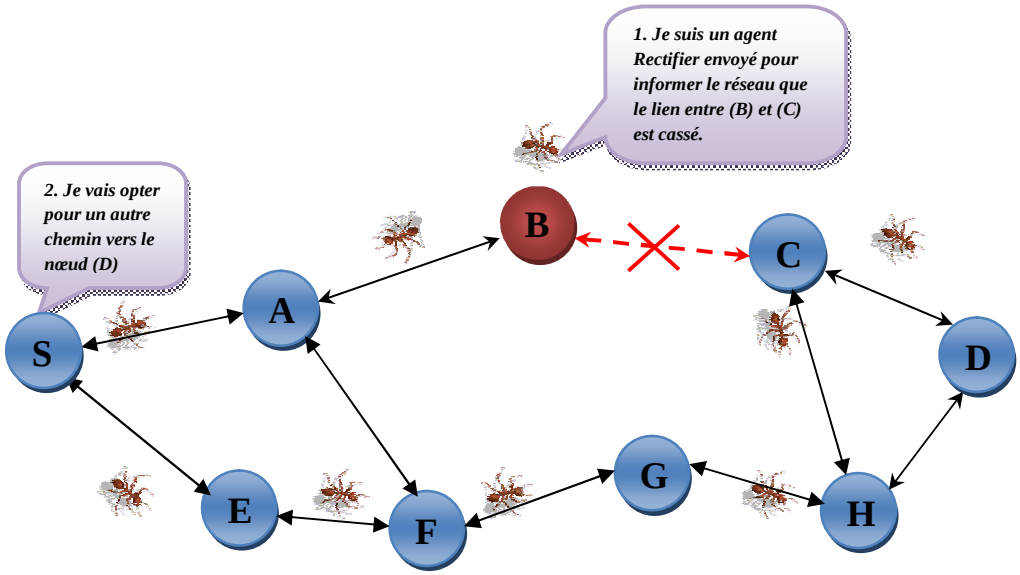


Figure 4.9 : L'attaque par usurpation de liens.

Cette attaque est réalisée comme suit : suggérons que le nœud (S) souhaite communiquer avec le nœud (D), et après avoir sollicité le processus de découverte de route ou après avoir consulté sa table de routage, ce nœud source opte pour le meilleur chemin en termes de nombre de sauts que les agents Ant mobiles ont trouvés conduisant vers sa cible. A cet égard, la route la plus optimale détectée est celle empruntant les nœuds relais (A), (B) et (C). Considérons maintenant, à un certain moment donné, que le nœud (B) se comporte avec malveillance en refusant par exemple d'accomplir son activité, autrement dit, il va ignorer l'existence d'un lien avec son nœud voisin (C).

Cette usurpation de lien va causer une altération puisque la communication ne peut pas atteindre le nœud (C) qui est chargé de l'acheminer vers destination, et donc ce chemin sera supprimé de la table de routage du fait qu'il est devenu invalide. A cet effet, des mises à jour au niveau de cette dernière et au niveau de celle de voisinage doivent être effectuées (voir tableau 4.5). Il semble donc nécessaire de chercher un autre itinéraire permettant au nœud source de parvenir à destination.

Le nœud	Ses voisins
S	A, E
A	S, B, F
B	***A, C***
C	***B, H, D***
D	C, H
E	S, F
F	E, A, G
G	F, H
H	G, C, D

(a)

Le nœud	Ses voisins
S	A, E
A	S, B, F
B	***A***
C	***H, D***
D	C, H
E	S, F
F	E, A, G
G	F, H
H	G, C, D

(b)

Tableau 4.5 : tables de voisinages avant et après l'attaque par usurpation de liens.

IV.6) Conclusion :

Ce chapitre nous a permis de comprendre le protocole de routage ***AntTrust*** pour les réseaux ad hoc, en présentant une description détaillée sur son principe de fonctionnement, les différentes tables qu'il gère, les différents agents motivés. Par la suite, nous avons invoqués les vulnérabilités qui peuvent survenir au protocole, en soulignant les attaques les plus sévères.

Le chapitre suivant décrit la proposition d'un nouveau modèle pour sécuriser le protocole de routage ***AntTrust***.

CHAPITRE V

PROPOSITION D'UN NOUVEAU PROTOCOLE DE COOPERATION ENTRE LES NŒUDS.

V.1) Introduction :

L'absence de nœuds spécialement envisagés aux tâches de routage dans les réseaux ad hoc, explique le fait que ces nœuds font office de routeurs en faisant appel à des communications multi-sauts. Mais cette coopération peut donner lieu à de nombreux problèmes au moment où des nœuds suspects peuvent refuser la coopération, altérer ou modifier le trafic qui les transitent. A l'ombre de cet objectif, une diversité de solutions ont été adoptées afin de sécuriser ces réseau. Des solutions basées sur les mécanismes de la cryptographie ou de chiffrement par clés et bien d'autre, ont cédés leurs places à de nouvelles solutions portant sur des modèles de renforcement de la coopération.

Pour sécuriser le protocole ***AntTrust***, nous envisageons un modèle qui devra être apte à délivrer un niveau de sécurité adapté à l'enjeu de la communication et dont le niveau pourra évoluer au fil du temps selon le contexte. Il est admis qu'une solution entièrement opérationnelle remédiant aux exigences spécifiques d'un réseau ad hoc n'a pas encore vue le jour. En revanche, il sorte aux yeux que la notion de confiance se présente comme un levier incontournable à la manifestation d'une solution globale pour l'enjeu de la sécurité dans les réseaux ad hoc et implicitement pour notre protocole du moment où la confiance est une partie intégrante dans la définition du concept de sécurité. Bien entendu, établir une relation de confiance entre un couple de nœuds autonomes, sans se servir d'un tiers, est une difficulté accrue.

V.2) La confiance :

V.2.1) Définitions :

Pour mieux apprécier le concept de la confiance, on a préféré présenter un panorama de définitions issues de divers domaines :

La confiance **[VLU.04]** est un mécanisme de coordination des échanges en situation d'ignorance ou d'incertitude : c'est elle qui permet de prendre une décision malgré l'existence d'un risque. Et sur la lumière de cette définition, il est quasiment évident que le concept de la confiance est invoqué en parlant d'une personne, morale, mais une fois le contexte est orienté vers les techniques ou les technologies, on parle très souvent de la sécurité, la fiabilité et la sûreté. En effet, sur le plan pratique, ces notions se chevauchent et en témoigne d'exemple : attribuer de la confiance à une entreprise est quasiment influencé par sa mise en œuvre de technologies sûres et fiables.

La confiance selon **[RAC.07]** est reconnue comme un aspect important pour la prise de décision dans les applications distribuées auto-organisées. Malgré cela, la littérature ne fournit aucun consensus sur la définition même de la notion de confiance et sur ce que constitue la gestion de la confiance.

La confiance **[RRD.94]** est d'accepter de s'exposer au risque d'opportunisme.

La confiance **[OWI.93]** est l'ensemble des attentes, suppositions et croyances concernant la probabilité que les actions futures d'un autre seront favorables ou au moins non préjudiciables à ses propres intérêts.

La confiance **[SAR.09]** est un élément important pour tisser des relations et établir de collaborations et des échanges entre les différents acteurs de l'environnement. Ce mécanisme permet de construire et d'élargir, à partir d'un ensemble de connaissances, le cercle d'activité de chacun.

La confiance selon **[OCB.07]** stipule qu'une entité ne fait confiance à une autre entité si et seulement si cette dernière se comporte exactement comme la première le prévoit.

V.2.2) Les fondements de la confiance :

Le concept de la confiance en étant une espérance développée à partir de modèles sociaux, fondée sur la connaissance à priori de l'identité du correspondant, raisonne ces trois composants tangibles sur lesquels elle est bâtie :

- L'historique des relations : '' cela s'est bien passé avant, donc cela se passera bien la prochaine fois''.
- Les recommandations des tiers : '' cela s'est bien passé avec d'autres, donc cela se passera bien avec moi''.
- La capacité à exercer des représailles : '' cela va bien se passer car il n'a plus à perdre plus que moi, si cela se passe mal''.

V.2.3) Les relations de confiance : [OCB.07]

D'après les définitions données plus haut, il est clair que ceci inclut la notion du rapport ou relation entre les entités. A cet égard, on peut lister quelques cas de relations de confiance :

- **A** L'entité A fait confiance à l'entité B, mais l'entité B n'a pas besoin de faire confiance à l'entité A.
- **A** L'entité A fait confiance à l'entité B, et l'entité B fait confiance à l'entité A.
- **A** L'entité A fait confiance à l'entité C, et l'entité B fait confiance à l'entité C, donc les entités A et B peuvent faire confiance à C.

V.3) La gestion de confiance :

Etudier la gestion de la confiance au cœur des réseaux ad hoc revient à étudier les modèles de confiance mis en œuvre. Mais bien avant d'entamer les modèles de confiances cernés par les MANETs, il semble primordial d'esquisser par éclaircir le concept de modèle de confiance.

1) Le modèle de confiance :

Une analyse fine ciblant à dessiner les vulnérabilités inhérentes aux réseaux ad hoc, a dévoilé qu'ils résident essentiellement dans leurs mécanismes de routage, leurs mécanismes d'auto-configuration et leurs déploiements de liens non-câblés. A cette image, il est clair que ces fonctionnalités de base s'accentuent sur une confiance totale entre l'ensemble des nœuds appartenant au réseau. Prenons l'exemple du routage, le transport des paquets au sein du réseau repose sur la véracité des informations délivrées par les autres nœuds. De plus, délivrer un paquet vers une destination dans les MANETs revient à effectuer un routage multi-sauts, et si un nœud refuse de coopérer, cela provoque le blocage, la modification ou le ralentissement du trafic qui passe par lui.

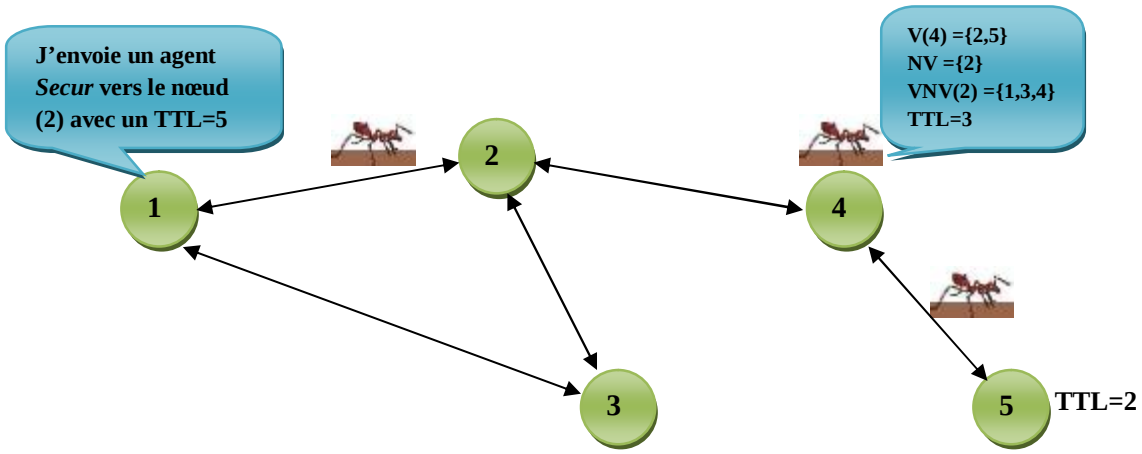
Pour cette raison, il est très utile de déterminer comment les différentes entités du réseau puissent faire confiance les unes aux autres. L'environnement et le stade d'application peuvent avoir un impact majeur sur le modèle de confiance. Par conséquent, les relations de confiance entre les éléments du réseau affectent la manière selon laquelle le modèle de confiance à base de coopération ou à base de certification devrait être conçu. **[HAK.07], [COB.11]**

V.4) Le modèle pour sécuriser AntTrust:

Les solutions de sécurités suggérées pour les réseaux ad hoc s'avèrent particulièrement difficiles à fournir dues à la conjonction de plusieurs facteurs. Le manque d'une relation de confiance appropriée entre les nœuds du réseau explique le fait que les modèles classiques de sécurité élaborés autour du l'établissement approprié de la confiance sont inadaptés et ne peuvent donc être directement appliqués aux réseaux ad hoc. De plus, les solutions de sécurité qui supposent l'existence d'un point central comme une tierce partie de confiance ou un serveur de clés, ne sont pas compatible avec la définition de base d'un réseau ad hoc où une infrastructure prédéfinie n'est pas disponible. [HAK.07]

V.5) Le protocole de calcul de confiance entre les nœuds :

Suite à la non-sécurisation du protocole de routage ***AntTrust*** détaillée précédemment, une nécessité incessante portant sur la conception d'un nouveau protocole plus sûre apte à s'opposer aux différentes failles du protocole : Sybil, usurpation d'identité, usurpation de liens, attaque par non retransmission des messages de données, par falsification des routes, par suppression du trafic de routage et bien d'autres. Dans ce contexte, un nouveau protocole se focalisant sur la notion de confiance pour remédier à ces malveillances, a été mis au point. Le schéma suivant permet d'éclaircir le principe du protocole dont on parle.



V(i) : les voisins du nœud courant.

NV : les nœuds déjà visités par l'agent.

VNV(i) : les voisins de nœud (i) visité.

TTL : la durée de vie de l'agent *Secur*.

Figure 5.1 : Le fonctionnement de l'agent ***Secur***.

Ce nouveau protocole opère comme suit : chaque nœud génère régulièrement un agent Ant mobile nommé ***Secur*** et le transmet vers un nœud destination se situant dans son voisinage en fonction d'un nombre arbitraire de sauts illustré par sa durée de vie (TTL). Lors du transit par un nœud, l'agent ***Secur*** cueille la liste des nœuds voisins du nœud courant et fournit à ce dernier l'ensemble des nœuds visités accompagnés de leurs voisins. Après avoir collecté toutes ces informations relatives au voisinage, il est temps au nœud du réseau d'élaborer le calcul de confiance envers ses voisins. Mais il faut bien voir que les nœuds voisins collectées par les agents ***Secur*** doivent être bidirectionnelement liés afin d'échapper aux erreurs qui se glissent au moment du calcul de la note de confiance de voisinage.

Pour cela, deux sortes de notes sont adaptées dans la métrique de confiance : une première note de confiance s'accentue sur la véracité du voisinage du nœud, i-e, le nœud ment-il ou pas sur son voisinage, et une deuxième note de confiance externe tirée depuis les différentes notes de confiances que les autres nœuds disposent sur le nœud en question.

La formule qui permet de déceler la note de confiance qu'un nœud (i) accorde à un nœud (j), est obtenue par :

$$NC(i, j) = (\alpha NCV(i, j) + \beta\, NCext(i, j)) / (\alpha + \beta)$$

où: ***NC(i, j)*** représente la note de confiance que le nœud (i) assigne au nœud (j) en tenant compte qu'il ne ment pas à propos des informations fournies sur son voisinage.

α, β représente les facteurs attribués aux deux confiances en fonction de l'importance qu'on veut accorder à chacune d'elles.

Remarque 1 : ∀ i, j deux nœuds, 0<= NC(i,j) <= 1.

Remarque 2 : Dés que la note de confiance d'un nœud devient inferieur à 0,5, le nœud est isolé définitivement et devient ainsi non digne de confiance.

V.5.1) Calcul de la note de confiance de voisinage :

La Note de Confiance de Voisinage abrégée à ***NCV*** sert à établir des vérifications liées aux informations de routage, que ce soit celles présentes dans la table de routage ou celles de voisinage, fournies par chaque nœud au profit des agents mobiles ***Secur***. Cela est dû essentiellement pour détecter si un nœud ***ment*** sur ces informations de voisinage, et donc faire l'objet d'une attaque par usurpation d'identité, de falsification de liens, attaque par suppression de trafic de routage ou bien d'autres types.

Et sur la lumière de comparer les informations délivrées par un nœud vis-à-vis à celles fournies par les autres nœuds du réseau, la ***NCV*** permet de vérifier les dires de chacun des nœuds sur leur voisinage, et ce en la recalculant pour l'ensemble des nœuds se trouvant dans la table de confiance à chaque fois qu'un agent ***Secur*** est reçu. Ainsi, la table de confiance, ***TABCONF***, d'un nœud (i) permettant d'enregistrer et de calculer les confiances des autres nœuds, est schématisée comme suit :

Nœud	Liste voisins	NCext	NCV	NC	B(i,j)	Tpenal
J	(V1(j),NC(j,v1)…	NCext(i,j)	NCV(i,j)	NC(i,j)	0/1	Tpenal(i,j)

Tableau 5.1 : Table de confiance (***TABCONF***).

Où :

j : représente l'un des nœuds reçus par le nœud (i) lors du transit d'un agent ***Secur***.

Vk(j) : représente le $k^{ème}$ voisin du nœud (j) à un seul saut.

NC(j,vk) : représente la note de confiance du nœud vk estimée par le nœud (j).

B(i,j) : représente une valeur booléenne sur la décision de la pénalisation.

Tpenal : représente la période de pénalisation du nœud (j).

Remarque :

Dans l'objectif de pallier à la mobilité fréquente de la topologie du réseau, il s'avère nécessaire d'affecter une durée de vie à chaque entrée de la table de confiance. La durée de vie d'un nœud est réinitialisée à chaque nouvelle réception de ce nœud.

Après avoir donné un aperçu concis sur la note de confiance de voisinage ainsi la table de confiance, il est temps maintenant d'exposer le mécanisme opté pour le calcul d'une ***NCV*** d'un nœud (j) pour un nœud (i) à l'instant (t). Ce mécanisme est réparti en deux algorithmes : le premier consiste à construire l'ensemble **(ξ)** des nœuds qui mentent sur le voisinage de nœud (i), et le second algorithme est appelé à former l'ensemble **(δ)** des nœuds disant la vérité sur le voisinage du nœud (i).

Algorithme 1 :

Cet algorithme résume les étapes de la procédure suivies pour extraire l'ensemble des nœuds qui fournissent des informations incorrectes concernant leur voisinage.

Algorithme 1 *: Procédure de formation de l'ensemble* ***(ξ)***

Pour tout noeud ***x*** *∈ TABCONF* ***i*** *[j].listeVoisins Faire {*
si j ∉ TABCONF ***i*** *[x].listeVoisins*
ξ := ξ + ***x*** *;*
}
Pour tout noeud ***x*** *∉ TABCONF* ***i*** *[j].listeVoisins Faire {*
si j ∈ TABCONF ***i*** *[x].listeVoisins*
ξ := ξ + ***x*** *;*
}
si i ∈ TABCONF ***i*** *[j].listeVoisins et j ∉ TABVi*
ξ := ξ + i ;

Algorithme 2 :

Cet algorithme détaille le processus adopté pour former l'ensemble des nœuds qui délivrent de vraies informations à propos de leur voisinage, i-e, les nœuds qui disent la vérité.

Algorithme 2 *: Procédure de formation de l'ensemble* **δ**

Pour tout noeud ***x*** *∈ TABCONF* ***i*** *[j].listeVoisins Faire {*
si j ∈ TABCONF ***i*** *[x].listeVoisins*
δ := δ + ***x*** *;*
}
Pour tout noeud ***x*** *∉ TABCONF* ***i*** *[j].listeVoisins Faire {*
si j ∉ TABCONF ***i*** *[x].listeVoisins*
δ := δ + ***x*** *;*
}
si i ∈ TABCONF ***i*** *[j].listeVoisins et j ∈ TABVi*
δ := δ + i ;

Après avoir crée les deux ensembles **(ξ)** et **(δ),** on passe maintenant à calculer la moyenne de confiance ***NCV*** estimée par le nœud (i). Il est admis qu'initialement la ***NCV*** de tous les nœuds est égale à 1 (***NCV***=1), autrement dit, au départ, les différents nœuds du réseau fassent confiance totale entre eux, et donc, il n'existe pas de nœuds non digne de confiance dans le réseau.

On pose (**λ**) le nombre de nœuds dans l'ensemble (**ξ**) tel que (**λ**) = ***card*** (**ξ**), et (**λ1**) le nombre de nœuds dans l'ensemble **(δ)** tel que (**λ1**) = **card** (**δ**).

En prenant en considération la précédente valeur de confiance de voisinage, la nouvelle ***NCV*** est obtenue par l'expression suivante :

$$\mathbf{NCVt(i, j) = (NCVt - 1 + (1-(\lambda/ (\lambda + \lambda 1)))) / 2}$$

Il est à noter que l'expression **(1-((λ / (λ+ λ1)))** s'agit de la note de confiance de nœud (j) estimée par le noeud (i), pour cela on établit une moyenne des notes de confiance.

V.5.2) Calcul de la note de confiance externe :

La note de confiance externe ou encore ***NCext*** permettant à un nœud (i) de calculer la note de confiance d'un nœud (j), est décelée à partir des informations ou des avis transportés par les agents Ant ***Secur*** des autres nœuds relativement à ce nœud, ce qui permette au nœud (i) d'avoir les évaluations des nœuds sur une plage de ***n-1*** sauts. Pour se faire, le nœud (i) est appelé à voir l'ensemble des nœuds ayant comme nœud voisin (j) depuis la table de confiance et puis récupérer la note de confiance soulignée par ces derniers envers le nœud (j), ensuite établir une moyenne récapitulant l'ensemble de ces notes de confiances détectées.
L'estimation de cette note de confiance est due à l'aide de la formule suivante :

$$\mathit{NCext\ (i, j) = 1/ \delta(\Sigma k \in v(j)\ TABCONF(k).listVoisins[j].NC).}$$

Ainsi le mécanisme adopté pour pouvoir effectuer le calcul de la ***NCext*** se résume par l'algorithme suivant qui porte essentiellement sur la formation de l'ensemble des voisins de nœud (j).

Algorithme 3 :

Cet algorithme permet de collecter les différents nœuds du réseau qui disposent d'une relation de voisinage avec le nœud en question.

Algorithme 3 *: Procédure de formation de l'ensemble* ***v****(j)*
Pour tous ***x*** *∈ TABCONF* ***i***   *si j ∈ TABCONF* ***i*** *(x).listVoisins*   *v(j) :=v(j)+****x*** *;*   *δ := δ + 1;*

V.5.3) Fonctionnement de l'agent Secur :

Passons maintenant à présenter le fonctionnement de l'agent ***Secur*** qui se résume comme suit : chaque nœud du réseau est sensé de créer un agent de type ***Secur***, ensuite, il l'envoie vers une destination, parmi son voisinage à un saut, choisie de manière aléatoire. Après avoir reçu l'agent, le nœud récepteur se charge d'effectuer les calculs nécessaires sur la confiance du voisinage et la décision de pénalisation des nœuds, et à son tour, il va retransmettre l'agent ***Secur*** à un autre voisin destination aléatoirement. Ce processus est illustré par les algorithmes (**4**) et (**5**) qui détaillent les étapes d'initialisation, d'envoie, de réception et de retransmission de l'agent ***Secur***.

Algorithme (4) :

Cet algorithme d'initialisation et d'envoie de l'agent ***Secur*** opère comme suit : au départ, le nœud créateur de l'agent ***Secur*** effectue un choix arbitraire en ce qui concerne le nœud voisin destination vers qui il veut transmettre l'agent, puis, il lui attribue une valeur de durée de vie correspondante à la dimension du réseau, il récupère ainsi les voisins du nœud courant depuis sa table de routage accompagnés des notes de confiances correspondantes à partir de la table de confiance, et à la fin il clôture ce processus par envoyer cet agent vers la destination sélectionnée précédemment.

Algorithme 4 : initialisation et envoie de l'agent Secur
Secur.adresse-destination = choisir un voisin de façon aléatoire (dans la table de voisinage ***TABV***). ***Secur***.TTL = ***n*** (n étant la dimension du réseau). ***Secur***.TABM = récupérer les voisins du nœud courant de la table ***TABV*** **&** les notes de confiance correspondante de la table de confiance. Envoyer l'agent ***Secur.***

Algorithme (5) :

Cet algorithme de réception et de retransmission de l'agent ***Secur*** décrit les points à suivre par un nœud faisant l'objet de réception de ce type d'agent. Une fois qu'un nœud (i) reçoit un agent ***Secur*** transmis depuis un nœud (j), il esquisse par décrémenter le nombre de sauts du l'agent, i-e, sa durée de vie, ensuite, il actualise sa table de confiance et recalcule la note de confiance pour décider s'il va pénaliser ou pas le nœud émetteur (j), et par la fin, il procède à réémettre l'agent ***Secur*** vers un autre nœud se situant dans son voisinage directe.

Algorithme 5 : réception et retransmission

Secur.TTL - - (décrémenter le nombre de sauts)
Mise à jour de la table de confiance
Table de confiance.listevoisin[j]= ***Secur***.TABM (mise à jour de la liste des voisins)
Calculer la note de confiance (NC) pour j
Calculer NCV(i,j)
Calculer NCext(i,j)
Calculer NC(i,j)
Décision de pénalisation
Si NC(i,j) < 0.5 alors le nœud j sera pénalisé
Initialiser Tpénal = $\propto$ P(i,j)
Préparer la réémission
Secur.adresse-déstination = choisir un voisin de façon aléatoire (dans la table de voisinage TABV)
Envoyer l'agent ***Secur.***

V.5.4) Structure de données transportée par l'agent Secur :

Bien entendu, un agent **Secur** en transitant par chaque nœud du réseau est appelé à transporter les voisins du nœud créateur plus ses propres informations (l'adresse source, numéro de séquence et TTL). Il est à noter que les agents doivent transportés des nœuds qui sont bidirectionnelement liés afin de surpasser les erreurs de calcul de la note de confiance de voisinage (***NCV***) puisqu'elle s'appuie sur les déclarations des uns et des autres concernant leur voisinage.

Posons : $\mathbf{n_1, n_2, \dots, n_n}$ les **n** derniers nœuds visités par un agent ***Secur*** ;

$\mathbf{V_j^{n1}}$: le $\mathbf{j^{eme}}$ voisin d'un nœud $\mathbf{n_1}$;

Alors, un agent ***Secur*** transporte une structure de données qui peut être schématisée comme suit :

$\mathbf{n_1}$	$\mathbf{v_1^{n1}}$	$\mathbf{NC(n_1,v_1^{n1})}$	……..	……..	$\mathbf{v_i^{n1}}$	$\mathbf{NC(n_1,v_1^{n1})}$

Tableau V.2: La structure de données transportée par l'agent Secur.

V.5.5) Pénalisation d'un nœud :

Une fois que les notes de confiances sont établis, il vient que chaque nœud (i) suit un processus lui permettant de calculer la note de confiance (***NC***) afin de voir s'il va pénaliser ou pas le nœud voisin (j).

Posons : ***C = NC(i,j)*** la note de confiance de nœud (j) estimée par le nœud (i).

Et alors :

Si ***(C >= 0.5)*** ***Alors*** ***ne pas pénaliser le nœud (j) ;***

Sinon ***pénaliser le nœud (j).***

- ***Comment pénaliser un nœud ?***

La réponse à cette question est très simple. Lorsqu'un nœud (i) désire pénaliser un nœud (j) après avoir calculé sa note de confiance, il n'a qu'a intercepté l'émission des agents vers ce dernier, et ce pendant le processus de calcul des routes que ce soit en phase proactive ou réactive du protocole de routage. Cette stratégie résulte qu'un nœud (x) du réseau sera isolé d'une manière définitive en devenant ainsi non digne de confiance, et alors, cette route sera mise en cause. Néanmoins, il est à noter qu'il est très important d'actualiser la table de routage du nœud courant en raison qu'elle est en rapport avec la confiance que les nœuds voisins de (x) confèreront envers lui. Ce nœud (x) sera pénaliser pour une durée pouvant être estimée et calculée en proportion à la valeur de P(i,j).

V.6) Le comportement du nouveau protocole pour détecter l'attaque par usurpation d'identité :

Une nouvelle approche fondée sur la notion de confiance, a été proposée pour dépister les attaques de type usurpation d'identité dans les réseaux ad hoc implémentant le protocole de routage ***AntTrust***. Ce terme de confiance est employé pour évaluer la participation et quantifier le niveau de coopération de chacun des nœuds dans le protocole afin de ressortir les nœuds malveillants des nœuds bénins. Cette estimation de la confiance est principalement basée sur le comportement des nœuds, autrement dit, chacun des nœuds est appelé à observer et surveiller ses voisins, et à collaborer avec ses voisins en termes de confiance qu'ils ont en lui.

Une meilleure façon de cerner le processus de détection d'une telle attaque à l'aide d'un mécanisme de confiance, est détaillée par l'exemple suivant :

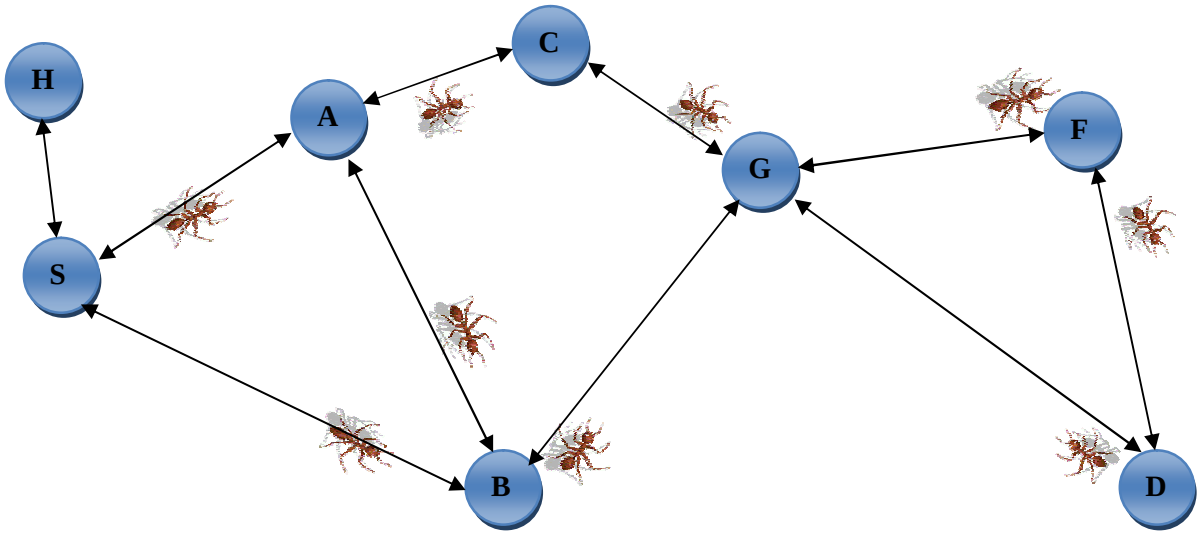


Figure 5.2 : La topologie du réseau avant l'attaque par usurpation de liens.

À la lumière de l'exemple donné ci-dessus, nous avons mis en œuvre le protocole de routage ***AntTrust*** pour un réseau ad hoc avec une topologie couvrant un ensemble de nœuds dont on suggère par la suite qu'un nœud suspect va faire l'objet d'un nœud malveillant. Fondé sur le concept de colonies de fourmis et le paradigme de multi-chemins, ce protocole offre l'opportunité à chacun des nœuds du réseau d'explorer un ou plusieurs itinéraires vers d'autres nœuds à l'aide des agents Ant mobiles, et ce d'une façon proactive ou réactive.

Le nouveau protocole sollicité ne s'intéresse pas uniquement à calculer les routes les plus courtes, mais aussi, à calculer la route la plus sûre. Cette sureté en termes de relation de confiance entre les nœuds du réseau précédemment vue, est bâtie autour des connaissances propres de chaque nœud et les connaissances de ses nœuds voisins. Il faut bien noter que ce mécanisme de confiance intégré, permet à chaque nœud d'évaluer à tout instant une note de confiance portant sur son voisinage, ce qui met chacun des nœuds entre le choix de transmettre ou non des messages de données vers ou à travers un nœud voisin.

Bien entendu et à l'ombre du l'exemple schématisé ci-dessus, il arrive qu'un nœud du réseau désire initier une transmission de messages vers une destination spécifique, dans notre cas supposons que c'est le nœud (S) qui veut transmettre des informations au nœud (D), mais le problème c'est que le nœud (S) ne dispose pas dans sa table de routage d'une route permettant d'atteindre cette destination. Ainsi, ce nœud procède à déposer localement une demande d'établissement d'une route plus fiable et plus sûre vers la destination espérée. Cette demande sera routée ensuite à l'aide des agents Ant mobiles générés périodiquement par les nœuds du réseau avec une durée de vie précise. Lors de la rencontre d'une telle demande, l'agent Ant mobile lance sa phase ***Retour***, puis, il procède à déposer une quantité de la substance au niveau de chaque nœud du son trajet inverse afin d'informer les autres nœuds du réseau de cette demande de découverte de route et de les attirés vers cette route.

Nœud	Liste voisins	NCext(S,B)	NCV(S,B)	NC(S,B)	B	Tpénal
A	(B,1), (C,1), (S,1)	1	1	1	0	-1
B	(A,1), (G,1),(S,1)	1	1	1	0	-1
C	(A,1), (G,1)	1	1	1	0	-1
D	(F,1), (G,1)	1	1	1	0	-1
F	(D,1), (G,1)	1	1	1	0	-1
G	(B,1), (C,1), (D,1),(F,1)	1	1	1	0	-1
H	(S,1)	1	1	1	0	-1

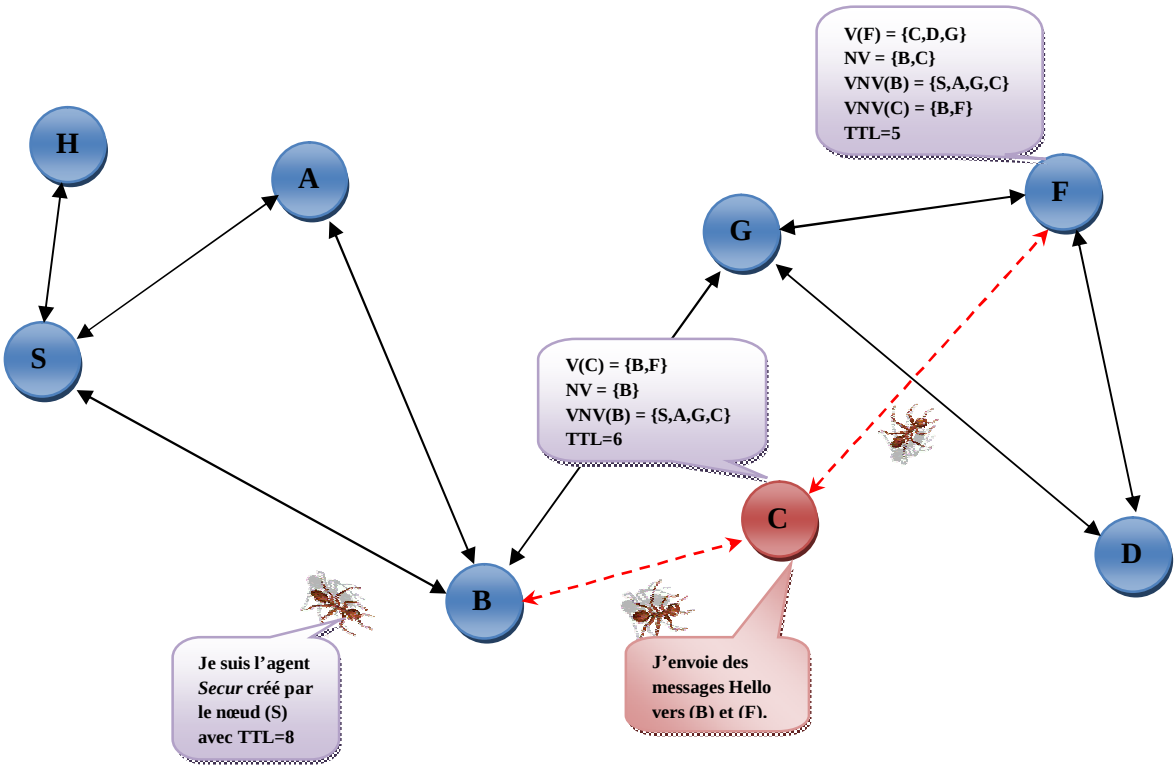
Tableau 6.1 : Table de confiance du nœud (S) à l'état initial t0.

Remarque :

Initialement, on suppose que tous les nœuds disent la vérité à propos de leurs voisinages, ce qui explique que NC(i,j) =1.

Un nœud malicieux peut s'insérer aisément dans le réseau grâce à la propriété intrinsèques des réseaux ad hoc, la mobilité, il se met ainsi dans la porté des nœuds (B) et (F), et il se contente de réaliser son attaque par usurpation d'identité, donc il se fait passer pour un autre nœud du réseau, et comme exemple, considérant que l'imposture sera pour le nœud (C). Donc, une nouvelle vue concernant la topologie du réseau va être crée (voir figure 5.3), et ce en mettant d'abord hors service le nœud victime (C), ensuite le nœud malicieux envoie des messages ***Hello*** vers ces nouveaux voisins (B) et (F) pour les informer qu'il est dans leurs voisinage.

En parcourant le réseau, les agents mobiles essayent de répondre au mieux au nœud initiateur de la demande en véhiculant les itinéraires les plus optimaux qu'ils ont trouvés vers le nœud destination. Le nœud demandeur de route en recevant ces informations apportées par les agents mobiles, émet un agent mobile de type ***Secur*** vers un nœud destination sélectionné arbitrairement parmi son voisinage directe et doté d'un ***TTL*** généralement égal à la dimension du réseau, chargé de collecter les informations nécessaires entrant dans le calcul des notes de confiance de chaque nœud au sujet d'un autre. Supposons que le nœud (S) génère un agent ***Secur*** en choisissant le nœud (B) comme destination.



V(i) : les voisins du nœud courant.

NV : les nœuds déjà visités par l'agent.

VNV(i) : les voisins de nœud (i) visité.

Figure 5.3 : La détection de l'attaque usurpation d'identité à l'aide d'agent Secur.

Chaque nœud du réseau faisant l'objet de réception de l'agent ***Secur*** depuis un autre nœud, tout d'abord il décrémente le nombre de sauts (***TTL***), il actualise sa table de confiance, recalcule la note de confiance pour qu'il puisse décider s'il va pénaliser ou pas le nœud émetteur, puis, il renvoie l'agent vers un autre nœud de son voisinage.

Le calcul de la note de confiance qu'un nœud peut avoir en un autre, permet d'exclure tout nœud s'observant avec un comportement suspect se résumant par un ensemble d'actions malveillantes au fil de son cycle de vie dans le réseau. L'ensemble des agents Ant délivrés par les nœuds du réseau répondent sur la demande mise en place en optant pour le plus sûre chemin menant vers le nœud (D) en passant par eux, tel que :

Le nœud (A) = {S,A,C,G,F,D} ; i-e, le nœud (C) est voisin avec les nœuds (A) et (G).

Le nœud (B) = {S,B,G,F,D} ; i-e, le nœud (F) est voisin avec les nœuds (G) et (D).

Le nœud (G) = {S,B,G,D} ; i-e, le nœud (B) est le voisin des nœuds (S) et (G).

L'agent ***Secur***, créé par le nœud (S), esquisse par recueillir l'ensemble des nœuds voisins du nœud (B) qu'il transite et par la suite, fournir à ce dernier l'ensemble des nœuds visités ainsi leurs voisins. Une fois que ces ensembles sont formés, il convient maintenant que le nœud (B) établisse une estimation de la confiance au profit de nœud émetteur (S). Cette estimation est obtenue grâce à la dualité: note de confiance de voisinage (***NCV***) et note de confiance externe (***NCext***).

Il est admis que la ***NCV*** est destinée essentiellement à évaluer la véracité de chaque nœud sur son voisinage, et pour ce faire, deux algorithmes sont adoptés en faisant appel à la table de confiance d'un nœud précis.

Après avoir effectué les vérifications nécessaires en ce qui concerne les informations se situant dans la table de voisinage du nœud (S) par rapport à celles présentes dans la table de confiance collectées par l'agent ***Secur*** et après avoir évalué les deux algorithmes (1) et (2), on a constaté que la note de confiance reste stable, c.à.d, au niveau du nœud (B), l'agent Secur n'a déduit aucun comportement suspect pour le nœud (S). A son tour, le nœud (B) choisi comme prochain saut le nœud (C) pour lui envoyé l'agent ***Secur***. En procédant les mêmes étapes précédentes, l'agent ***Secur*** ne détecte aucune malveillance concernant le nœud (B). Et de la même manière, le nœud (C) opte pour le nœud suivant à visiter le nœud (F). Arrivant sur le nœud (F), l'agent ***Secur*** effectue ses traitements en élaborant les deux listes suivantes qui mettent en œuvre la véracité ou non des dires des nœuds déjà visités sur leurs voisinages.

L'ensemble ξ = {C}. On a constaté après avoir évalué l'algorithme (1) que l'ensemble (ξ) présente un seul nœud menteur qui est le nœud (C), il donne des informations ambigües ou des faux dires à propos de son voisinage. Contradictoirement avec ce qu'il a déclaré dans sa table de voisinage en comparaison avec sa table de confiance, on a pu voir qu'il présente deux déclarations différentes sur son voisinage.

L'ensemble δ = {S,A,B,D,F,G,H}. L'algorithme (2) nous a permis de construire cet ensemble en se basant sur les nœuds qui disent la vérité sur leur voisinage. Par exemple, le nœud (D) est inclut dans la liste des voisins du nœud (G) dans la table de confiance du nœud (F), de l'autre coté, le nœud (G) appartient à la liste des voisins de nœud (D) dans la table de confiance du nœud (F).

Passons maintenant à recalculer la note de confiance que le nœud (F) attribue au nœud (C). Et pour avoir cette NC(F,C), on commence d'abord par poser :

$\lambda = 1$ ***(card(*** ξ ***)) ;***

$\lambda 1 = 7$ ***(card(*** δ ***)) ;***

$\alpha = 65$ représente le facteur associé à la ***NCV(i,j) ;***

$\beta = 35$ représente le facteur associé à la ***NCext(i,j).***

Ainsi, la note de confiance estimée par le nœud (F) est illustrée par la table de confiance suivante :

Nœud	Liste voisins	NCext(F,Noeud)	NCV(F,Noeud)	NC(F,Noeud)	B	Tpenal
S	(H,1),(F,1), (B,1)	1	1	1	0	-1
B	(S,1),(A,1), (G,1),(C,1)	1	1	1	0	-1
C	**(B,1),(F,1)**	**1**	**0.43**	**0.87**	**0**	**-1**

Tableau 6.2 : Table de confiance de nœud (F) à l'instant t_1.

Remarquons bien que la NC(F,C) = 0,87>0,50 et donc la probabilité que le nœud (C) sera pénalisé est P(F,C) =1- NC(F,C) = 0,13. Ce qui résulte une probabilité de pénalisation du nœud (C) très faible (13%).

A son tour le nœud (F) va retransmettre l'agent ***Secur*** vers son nœud voisin (G) qui va recalculer la note de confiance. Et après avoir effectué les traitements nécessaires, on a pu avoir les résultats suivants :

Nœud	Liste voisins	NCext(G,Noeud)	NCV(G,Noeud)	NC(G,Noeud)	B	Tpenal
S	(H,1),(F,1), (B,1)	1	1	1	0	-1
B	(S,1),(A,1), (G,1),(C,1)	1	1	1	0	-1
C	(B,1),(F,1)	1	0.43	0.87	0	-1
F	**(G,1), (C,1), (D,1)**	**1**	**0.44**	**0.15**	**1**	**t**

Tableau 6.3 : Table de confiance de nœud (G) à l'instant t_2.

Ces résultats montrent une régression remarquable au niveau de la note de confiance que le nœud (G) estime au sujet de nœud (F) en passant du 0.87 vers 0.15. Une NC(G,F)= 0.15 qui est trop petite et trop faible, nous a permis de détecter un comportement malveillant sur cette route, et alors, les nœuds composant cette route deviennent non digne de confiance. Ainsi, la probabilité de pénalisation de nœud (F) devient très importante puisqu'elle souligne un pourcentage très élevé égal à 85% (P(G,F) =1- NC(G,F) = 0,85).

Le nœud (G) en procédant le même processus avec l'agent ***Secur***, il choisi comme successeur le nœud (B). Le nœud (G) lui aussi sera non digne de confiance du fait que la NC(B,G) va régresser de plus en plus.

Cette méthode élaborée autour du concept de la confiance nous a permis largement de repérer que c'est le nœud (C) qui se comporte malicieusement dans le réseau du fait que la note de confiance a commencé à régresser après que l'agent ***Secur*** l'a visité. Le nœud attaquant s'est situé au voisinage du nœud (B) et (F) en usurpant l'identité d'un nœud légitime appartenant au réseau, et fournissant ainsi de fausses informations sur son voisinage. A cet égard, il nous parait légitime de pénaliser ce nœud attaquant non digne de confiance en l'excluant du réseau définitivement, plus précisément, on va arrêter et empêcher toute transmission des agents Ant mobiles vers ou à travers lui.

Et pour sécuriser au parfait le fonctionnement du protocole de routage ***AntTrust*** et protéger les communications à établir au sein du réseau, il nous semble très important d'actualiser la table de routage du nœud (S) en supprimant entièrement cette route, et essayer ainsi d'emprunter un autre itinéraire par l'envoie d'un nouveau agent ***Secur*** depuis le nœud (S) vers d'autres nœuds voisins excepté le nœud (B) en répétant ainsi le même processus.

V.7) Conclusion :

Le présent chapitre a porté essentiellement sur l'intégration d'une stratégie de calcul de confiance mutuelle entre les nœuds au cœur du protocole de routage ***AntTrust***. Ce nouveau protocole répondant le plus en termes de sécurité, se serve d'un agent ***Secur*** lui permettant de bien router les messages dans le réseau en optant pour le chemin le plus sûre et le plus fiable, suscitant ainsi, la détection des nœuds malveillants des nœuds légitimes en fonction des notes de confiance calculées. La décision de pénalisation d'un nœud malicieux et la note de confiance concernant ce nœud sont liés d'une manière ambivalente.

Ainsi, ce chapitre a été plié par un exemple applicatif permettant de tester l'aptitude du notre nouveau protocole à détecter une des attaques subtiles, l'attaque par usurpation d'identité.

CONCLUSION GENERALE

CONCLUSION GENERALE

Les réseaux ad hoc essayent d'étendre la notion de la mobilité à toute composante de l'environnement en éliminant le besoin d'infrastructure fixe pour communiquer, toutes les unités du réseau se déplacent librement et aucune administration centralisée n'est disponible. Vu leur grande mobilité et leur simple déploiement, les réseaux MANETs prennent de plus en plus de l'ampleur en offrant des solutions répondant bien aux applications qui préconisent une mobilité fréquente au sein d'un environnement nomade, en témoigne d'exemple, des soldats sur les champs de bataille ou des pompiers organisant les secours suite à une catastrophe naturelle.

Il est admis que chaque nœud du réseau ad hoc accomplisse la tâche d'un hôte ou d'un routeur pour des fins communicatifs. Dans ce contexte, nombreuses sont les stratégies de routage proposées pour satisfaire l'établissement des routes en optant pour la coopération des nœuds afin d'acheminer les paquets des autres. Cependant, une étude très fine au cœur de l'état de l'art portée sur les protocoles de routage existants, nous a ramené à cerner un ensemble de problèmes liés à la sécurité du routage suscitant ainsi une paralysie de fonctionnement et une dégradation des performances du réseau.

Dans ce mémoire, nous avons mis l'accent sur les résultats issus de nos études au sujet de la sécurité des réseaux ad hoc. Plus particulièrement, nous nous somme placés à étudier la stratégie de la colonie de fourmis permettant de déceler les meilleures routes comme solutions aux problèmes de routage, et au concept de la confiance optant pour les plus sûres routes comme solution de sécurité. En se basant sur ces deux points, nous nous somme intéressés à concevoir un nouveau protocole de renforcement de coopération entre les nœuds pour le protocole de routage ***AntTrust*** en termes de robustesse et de fiabilité.

Dans notre contribution, la mise en avant du nouveau protocole réside dans l'adjonction du l'agent Ant ***Secur***. Cet agent est suscité par chaque nœud du réseau vers une destination précise. En transitant par un nœud, l'agent ***Secur*** collecte tous les voisins du nœud visité et fournit à ce dernier la liste des nœuds qu'il a déjà transités accompagnée de l'ensemble de leurs voisins. Grace à toutes ces informations ramassées, chaque nœud du réseau se donne à calculer la note de confiance au sujet de ses voisins, puis la propage à l'ensemble du réseau. Arrivant à ce point, une décision probabiliste en rapport avec la véracité des connaissances fournies par chaque nœud, consiste à pénaliser ou pas le nœud en question. Ce mécanisme de pénalisation contribue énormément à découvrir les meilleures routes en termes de sécurité, de sûreté et de fiabilité.

Grosso modo, nous avons pu démontrer qu'un raisonnement opérant sur la note de confiance permet de vérifier les comportements des nœuds du réseau ad hoc et donc de détecter tout type de malveillance. Un tel résultat permet de garantir une opération de routage très efficace et plus fine, et par conséquent, sécuriser et perfectionner le protocole de routage ***AntTrust***.

PERSPECTIVES

En perspectives, nous envisageons implémenter le nouveau protocole de routage pour visualiser les résultats concrétisant l'apport de notre nouveau protocole proposé.

TABLE DES ACRONYMS

— ~ Table Des Acronyms ™ –

‘’A’’

ACO **Ant Colony Optimization.**

ANODR **ANonymous On Demand Routing.**

AntHocNet **An Adaptative Nature Inspired Algorithm For Routing in Ad hoc Networks.**

AODV **Ad hoc On Demand Vector.**

AP **Access Point.**

ARA **Ant-Colony Based Routing Algorithm For MANETs.**

‘’B’’

BSA **Basic Set Area.**

BSS **Basic Set Service.**

‘’C’’

CA **Certificate Authority.**

CBRP **Constant Bit Rate Protocol.**

CONFIDANT Cooperation Of Nodes Fairness In Dynamic Ad hoc Network.

CORE **Collaboration Reputation.**

‘’D’’

DARPA **The Defense Advanced Research Projects Agency.**

DBF **Distributed Bellman Ford.**

DOS **Denial Of Service.**

DSDV **Dynamic Destination Sequenced Distance Vector Routing Protocol.**

DSR **Distribution System Routing.**

DSSS **Direct Sequence Spread Spectrum.**

‘’E’’

ESS	**Extended Set Service.**

‘’F’’

FSR	**Force Seneing Resistor**

‘’G’’

GPRS	**General Packet Radio Service.**
GSM	**Global System Mobile.**
GSR	**Gigabit Switched Router.**

‘’H’’

HomeRF	**Home Radio Frequency.**
HSR	**Hot Standby Routing.**

‘’I’’

IARP	**IntrAzone Routing Protocol.**
IBSS	**Independent Basic Set Service.**
IDS	**Intrusion Detection System.**
IEEE	**Institute of Electrical and Electronics Enginneers.**

‘’M’’

MANET	**Mobile Ad hoc NETwork.**
Mbps	**Mega bit per second.**
MPR	**Multi Point Relay.**

‘’O’’

OFDM	**Orthogonal Frequency Division Multiplexing.**
OLSR	**Optimized Link State Routing.**
OSPF	**Open Shortest Path First.**

‘’P’’

PDA	**Personnal Digital Assistant.**
PERA	**Probabiliste Emergent Routing Algorithm.**
PKI	**Public Key Infrastructure.**
PRnet	**Paquet Radio network.**

‘’R’’

RERR	**Route ERRor.**
RIP	**Routing Information Protocol.**
RREP	**Route REPly.**
RREQ	**Route REQuest.**

‘’S’’

SHARP	**Sharp Hybrid Adaptive Routing Protocol.**
SMA	**System Multi Agent.**
SPR	**SHARP Proactive Routing protocol.**

‘’T’’

TC	**Topology Control.**
TORA	**Temporary Ordering Routing Algorithm.**
TTL	**Time To Live.**

‘’U’’

UMTS	**Universal Mobile Telecommunication System.**

‘’W’’

WIFI	**Wireless Fidelity.**
Wimax	**Worldwide Interoperability for Microwave Access.**
WLAN	**Wireless Local Area Network.**

WMAN **Wireless Metropolitain Area Network.**

WPAN **Wireless Personnal Area Network.**

WRP **Wireless Routing Protocol.**

WWAN **Wireless Wide Area Network.**

''Z''

ZRP **Zone Routing Protocol.**

BIBLIOGRAPHIE

BIBLIOGRAPHIE

1) [ABB.06]. Protocole de routage ad hoc sécurisé dans une architecture clustérisée. ADJIDO Idjiwa, BENAMARA Redhouane, BENZIMRA Rebecca, GIRAUD Laurent. Thèse de fin d'étude dans le cadre de l'obtention du diplôme Master 2 en informatique. Université Pierre et Marie Curie. France. 2006.
2) [ABR.09]. SU-OLSR une nouvelle solution pour la sécurité du protocole OLSR. ABDELLAOUI Rachid. Thèse de fin d'étude dans le cadre de l'obtention de la maitrise en génie concentration réseaux de télécommunications. école des technologies supérieures, Montréal. Canada. 2009.
3) [ADA.07]. Conception d'un protocole de routage réactif sécurisé à l'aide de processeurs sécurisé embarqué pour les réseaux ad hoc. ADOLF Abdallah. Thèse de fin d'étude dans le cadre de l'obtention du diplôme Master 2 en informatique. Université de Limogés. France. 2007.
4) [AHA.08]. La confiance dans le routage Ad hoc : étude du protocole OLSR. ADNANE Hassiba-Asmaa. Thèse de fin d'étude dans le cadre de l'obtention du grade de docteur en informatique. Université de Rennes 1. France. 2008.
5) [ALI.09]. Les modèles de coopération dans les réseaux ad hoc. ALLAM Ikram. Mémoire de fin d'étude dans le cadre de l'obtention du grade de magister en informatique. Université M'hamed Bougara. Boumerdes. 2009.
6) [AMF.07]. Les technologies sans fil : le routage dans les réseaux ad hoc (OLSR, AODV). AMEZA Fatima. Mémoire de fin d'étude dans le cadre de l'obtention du diplôme de Licence en informatique. Université ABD-ERRAHMANE MIRA. Bejaia. 2007.
7) [APO.07]. Les Attaques Sur Le Routage Dans Les Réseau Ad Hoc. POCQUET Alexandre. Article publié par l'Institut de Recherche en Informatique et Système Aléatoire, IRISA. France. 2007.
8) [APV.01]. Réseaux de mobiles & réseaux sans fil. Al AGHA Khaldoun, GUY Pujolle, GUILLAUME Vivier. Edition EYROLLES. France. 2001.
9) [ART.08]. A new multi-paths routing protocol for wireless ad hoc network based on multi-agent system. B.AIT SALEM, M.A.RIAHLA, K.TAMINE. La conférence MCSEAI, Oran. Algérie. 2008.
10) [BAF.02]. Travaux d'Etude et de Recherche: Les réseaux sans fil. BARRERE François. Université de Science Sociales de Paul Sabatier, Toulouse. France. 2002.
11) [BAM.09]. Approche dirigée par les fourmis pour la fragmentation horizontale des entrepôts de données relationnels. BARR Mohamed. Thèse de fin d'étude dans le cadre de l'obtention du diplôme du Magister en système d'information et de connaissances. ESI, Ecole nationale Supérieure d'Informatique, ex INI. Algérie. 2009.

12) [BAN.00]. le routage dans les réseaux mobiles ad hoc. BADACHE Nadjib. Rapport de recherche. Université des sciences et de la technologie Houari Boumediene, Alger. Algérie. 2000.
13) [BBO.04].Securing data transmission and retransmission management in ad hoc networks. BOUAM Souheila, BEN-OTHMAN Jalel. Conférence internationale sur les réseaux sans fil. France. 2004.
14) [BEA.06]. Algorithme des réseaux et télécoms. BENOIT Anne. 2006.
15) [BEK.09]. Conception d'un protocole de routage hiérarchique pour les réseaux de capteurs. BEYDOUN Kamal. Thèse de fin d'étude dans le cadre de l'obtention du grade de Docteur en informatique. Université de FRANCHE-COMTE. France. 2009.
16) [BON.08]. Routage dans les réseaux mobiles ad hoc par une approche à base d'agents. BOUKHECHEM Nadir. Thèse dans le cadre de l'obtention du diplôme du Magister en informatique. Université Mentouri. Constantine .2008.
17) [BUC.09]. Contribution à la sécurisation du routage dans les réseaux ad hoc. BURGOD Céline. Thèse de fin d'étude dans le cadre de l'obtention du grade de Docteur en informatique. Université de LIMOGES. France. 2009.
18) [COB.11]. Architecture de certification distribuée à base de multi-signature. CHALLAL Yacine, OMAR Mawloud, BOUABDALLAH Abdelmadjid. Article SAR-SSI 2011. France. 2001.
19) [DEL.07]. Protocole de routage pour l'interconnexion des réseaux Ad Hoc et UMTS. ELORRIETA David. Mémoire de fin d'étude dans le cadre de l'obtention du diplôme de Licence en informatique. Université Paris VI. France. 2007.
20) [DUT.07]. TER Ad Hoc. DUTREIGE Jonathan, TIMMERMANS Thomas. Thèse de fin d'étude dans le cadre de l'obtention du diplôma de Master en informatique. Université de Renne. France.2007.
21) [FSA.10]. Localisation des ressources dans un réseau ad hoc. SAILHAN Françoise. Thèse de fin d'étude dans le cadre de l'obtention du grade de docteur en informatique. Ecole doctorale : informatique, télécommunication et électronique du Paris IV. France. 2010.
22) [GAI.08]. Algorithmes distribués pour la sécurité et la qualité de service dans les réseaux ad hoc mobiles. GAWEDZKI Ignacy. Thèse de fin d'étude dans le cadre de l'obtention du grade de Docteur en informatique. Université de Paris-Sud 11. France. 2008.
23) [GLD.09]. Preventing layer-3 Wormhole Attacks in ad hoc networks with multi path DSR. GARCIA Luis Fernando. Thèse de fin d'étude dans le cadre de l'obtention du diplôme de Master en informatique. Ecole de technologie supérieure, université du Québec. Canada. 2009.
24) [GND.03]. La sécurité dans les réseaux sans fil ad hoc. GAYRAUD Valérie, NUAYMI Loutfi, DUPONT Francis, GOMBAULT Sylvain, THARON Bruno. Article SSTIC03. Bretagne. 2003.
25) [GOD.05]. Sécurité informatique Risques, Stratégies et Solutions. GODART Didier. Edition DES CCI de Wallonie. Deuxième Edition. France. 2005.
26) [GPU.02]. Les réseaux. GUY Pujolle. Edition EYROLLES n°3. France. 2002.
27) [GPU.03]. Les réseaux. GUY Pujolle. Edition EYROLLES n°4. France. 2003.

28) [GUK.06]. Securing AODV Routing Algorithm In Mobile Ad Hoc Networks. KAUR Gurpreet. Thèse de fin d'étude dans le cadre de l'obtention du diplôme de MASTER en informatique des technologies. Université PATIALA. Inde. 2006.
29) [HAK.07]. Sécurité dans les réseaux ad hoc. HAMOUID Khaled. Mémoire de fin d'étude dans le cadre de l'obtention du diplôme de Magister en informatique. Université d'Abderrahmane MIRA. Bejaia. 2007.
30) [HGG.08]. Anonymat dans les communautés de confiance. HEEN Olivier, GUETTE Gilles, GENET Thomas. Article SAR-SSI 2008, Rennes. France. 2008.
31) [HHG.05]. Security in Ad Hoc Network. BINGWEN Hu, HAGGLUND Joakim, QING Gu. Article IDT658. Université des sciences et technologies de Pékin. Chine. 2005.
32) http://www.ieee.org.
33) [HZC.07] .Using Network Processor to Establish Security Agent for AODV Routing Protocol. HONGSONG Chen, ZHONGCHUAN Fu, CHENGYAO Wang, ZHENZHOU Ji, MINGZENG Hu. Article CIT 15. Université des sciences et technologie de Pékin & institut de technologie Harbin. Chine. 2007.
34) [IGL.XX]. Réseaux ad hoc. LASSUS Isabelle Guérin.
35) [IGL.00]. Réseaux ad hoc. LASSUS Isabelle Guérin.2000. http://perso.ens-lyon.fr/isabelle.guerin-lassous.
36) [JPB.03]. Détection d'intrusions dans les réseaux ad hoc. PERCHER Jean-Marc, JOUGA Bernard. Article SSTIC03. Ecole supérieure d'électronique de l'Ouest & Supelec. France. 2003.
37) [KAG.06]. Securing AODV Routing Algorithm In Mobile Ad Hoc Networks. KAUR Gurpreet. Thèse de fin d'étude dans le cadre de l'obtention du diplôme de Master en informatique. Université de PUNJABI à PATIALA. Inde. 2006.
38) [LAA.02]. Unicast et Multicast dans les réseaux ad hoc sans fil. LAOUITI Anis. Thèse de fin d'étude dans le cadre de l'obtention du grade de Docteur en informatique. Université de Versailles Saint-Quentin-En-Yvelines. France. 2002.
39) [LAI.08]. Une approche pour l'assurance des qualités de services des systèmes publier/souscrire déployés sur un réseau mobile ad-hoc. LAHYANI ABDENNADHER Imene. Thèse de fin d'étude dans le cadre de l'obtention du diplôme du Master 2 en informatique. Ecole national d'ingénieurs de Sfax. Tunisie. 2008.
40) [LJB.06]. Les réseaux ad hoc et leurs problématique de sécurité. LEBEGUE Jerome, BIDAN Christophe, JOUGA Bernard. Rapport de recherche réalisé au sein de Supélec, Rennes. France. 2006.
41) [MAG.06]. Review of Existing Wormhole Attack Diskovery Techniques. GORLATOVA Maria Alexandrovna. Rapport réalisé en collaboration avec la Défence R&D Canada. université Ottawa. Canada. 2006.
42) [MAZ.07]. La sécurité dans les réseaux ad hoc. M.MEHDI, A.ANOU, S.ZAIR, M.BENSEBTI, M.DJEBARI. Rapport de recherche. Université de Blida. Algérie. 2007.

43) [MAZ.09]. Performance Comparisons of AODV, Secure AODV and Adaptative Secure AODV Routing Protocols in Free Attack Simulation Environnement. MOHD Anuar Jaafar, ZURIATI Ahmed Zukarnain. Le Journal européen des recherches scientifiques. ISSN 1450-216X vol.32 N°3. Université de Putra. Malaisie. 2009.
44) [MEA.05]. Système de détection d'intrusions dans les réseaux ad hoc. MELLASSINE Aymen. Thèse de fin d'étude dans le cadre de l'obtention du diplôme Ingénieur en informatique. Ecole Supérieure des Communications de Tunis. Tunisie. 2005.
45) [MIP.06]. Coopération dans les réseaux ad hoc : Application de la théorie des jeux et de l'évolution dans le cadre d'observabilité imparfaite. MICHIARDI Pietro. Article SSTIC06. institut Eurecom. France. 2006.
46) [MOB.06]. Http://www.gnupg.org/gph/fr/manual.html.
47) [MOJ.06]. Une approche multi-agents pour la gestion de la communication dans les réseaux de capteurs sans fil. JAMONT Jean-Paul, OCELLO Michel. Article RSM-TSI, volume 25, n°5. Laboratoire de Conception et d'Intégration des Systèmes (LCIS), Institut National Polytechnique de Grenoble (INPG). Université Pierre-Mendès. France. 2006.
48) [MRN.06]. Routage avec différenciation de terminaux dans les réseaux mobiles ad hoc. MERAIHI Rabah, NAIMI Amina. Article RIST, volume °16. France. 2006.
49) [MXP.09]. Simulation, Evaluation et Optimisation d'un algorithme de maintien de connectivité dans les systèmes multi-robot. MAI Xuan Phu. Rapport de recherche. Institut de la Francophonie pour l'Informatique. Chine. 2009.
50) [OCB.07]. ICARM : Infrastructure de Confiance pour les Architectures de Réseaux Mixtes. Mawloud OMAR, CHALLAL Yacine, BOUABDALLAH Abdelmadjid. Article publié dans 'sécurité, architectures réseaux et sécurité des systèmes d'information'. France. 2007.
51) [OWI.93]. "Calculativeness, trust, and economic organization''. O.WILLIAMSON. Journal of Law and Economics, Vol. 36, No. 1, pages. 453–486. Université de Chicago. USA. 1993.
52) [PMJ.02]. Network Security with OpenSSL. CHANDRA Pravir, MESSIER Matt, VIEGA John. Edition O'Reilly & Assocates. USA. 2002.
53) [RAC.07]. Analyse de la confiance implicite requise dans le routage ad hoc OLSR. TIMOTEO Rafael, ADNANE Asmaa, BIDAN Christophe, LUDOVIC Me. Rapport de stage, Supelec. France. 2007.
54) [RAD.05]. Security schemes for the OLSR protocole for ad hoc network. RAFFO Daniele. Thèse de fin d'études dans le cadre de l'obtention du grade de Docteur en informatique. Université de Paris VI. France. 2005.
55) [REO.05]. Sécurité des protocoles de routage des réseaux ad hoc. REZINE Othmane. Thèse de fin d'étude dans le cadre de l'obtention du diplôme D'Ingénieur en télécommunication. Ecole Supérieure des Communication de Tunis. Tunisie. 2005.
56) [RMA.08]. Conception et mise en œuvre d'un nouveau protocole de routage Multi chemins pour réseaux ad hoc base sur la réputation des nœuds. RIAHLA Med Amine. Université M'Hamed BOUGARA, Boumerdes. Algerie. 2008.
57) [RRD.94]. "Violating the psychological contract: not the exception but the norm". S. Robinson and D. Rousseau. Journal of Organizational Behavior, Vol. 15, pages.145–159. USA. 1994.

58) [RTR.02]. CISCO Security Specialist's Guide to PIX Firewall. TROUPE Ralph. Edition CALLISMA. USA. 2002.
59) [SAR.09]. The Chameleon : Un Système de Sécurité pour Utilisateurs Nomades en
60) Environnements Pervasifs et Collaboratifs. SAADI Rachid. Thèse de fin d'étude dans le cadre de l'obtention du grade de docteur en informatique. LIRIS (Laboratoire d'IinfoRmatique en Image e Système d'information) de Lyon. France. 2009.
61) [SSM.03]. application de techniques d'apprentissage dans les réseaux mobiles. SENOUCI Sidi-Mohammed. Thèse de fin d'étude dans le cadre de l'obtention du grade de Docteur en informatique, option : systèmes informatiques. Université de Pierre et Marie Curie, Paris VI. France. 2003.
62) [TAB.07]. Analyse de la confiance implicite requise dans le routage ad hoc OLSR. TIMOTEO Rafael, ADNANE Asmaa, BIDAN Christophe, ME Ludovic. Article SAL-07. France. 2007.
63) [THC.08]. Authentification dans les réseaux véhiculaires opérés. TCHEPNDA Christian. Thèse de fin d'étude dans le cadre de l'obtention du grade de Docteur en informatique. Ecole Nationale Supérieure des Télécommunications. PARIS. 2008.
64) [THJ.07]. Détection de la malveillance et réactions dans les réseaux ad hoc – bibliographie. JULIEN Thomas. Rapport de recherche, Ecole Nationale Supérieure des Télécommunications. France. 2007.
65) [VLU.04]. "Vers un modèle de confiance pour les objets communicants : une approche sociale". V. LEGRAND et S.UBEDA. Article réalisé au Centre d'Innovations en Télécommunications & Intégration de services CITI INRIA ARES, INSA de Lyon. France. 2004.
66) [TQT.09]. Protocoles de Routage dans les Réseaux Multi-radios Mobiles. TRAN Quoc Tuan. Rapport de recherche. Institut de la Francophonie pour l'Informatique de Pékin. Chine. 2009.
67) [VUN.07]. Les réseaux sans fil spontanés pour l'Internet Ambiant. UNTZ Vincent. Thèse de fin d'étude dans le cadre de l'obtention du grade de docteur en informatique, option : systèmes et logiciels. Institut Nationale Polytechnique De Grenoble. France. 2007.
68) [XIX.06]. Mécanismes de sécurité pour des protocoles de routage des réseaux ad hoc. XIAOYUN Xue. Thèse de fin d'étude dans le cadre de l'obtention du grade de docteur en informatique. Ecole Nationale Supérieure des Télécommunications. France. 2006.
69) [YWS.06]. Experimental Comparisons between SAODV and AODV Routing Protocols. YUXIA Lin, A.HAMED, MOHSENIAN Rad, W.S.WONG, SONG Joo-Han. Article LRWSc05. Université de British Columbia du CANADA & Samsung Electronics de KOREA.USA. 2006.
70) [ZAM.10]. Une architecture décisionnelle de contrôle pour un groupe de robots mobiles coopératifs dans un environnement dynamique et non structuré. ZAGANE Mohamed. Thèse de fin d'étude dans le cadre de l'obtention du diplôme du Magister en informatique. Ecole doctorale en science et techniques de l'information et de la communication. Algérie. 2010.