III. Domaines d'application des réseaux mobiles ad hoc

La particularité d'un réseau Ad hoc est qu'il n'a besoin d'aucune installation fixe. Ceci lui permet d'être rapide et facile à déployer. Les applications ayant recours aux réseaux ad hoc couvrent un très large spectre :

- Les applications tactiques comme les opérations de secours (incendies, tremblements de terre, inondations...) ;
- Militaires, pour la mise en place de tactiques adaptées au mouvement des troupes ;
- Systèmes de surveillance, dans des milieux dangereux, comme les volcans, ou plus sensibles, pour des forêts par exemple ;
- Dans le monde des transports routiers pour assurer un meilleur confort de la conduite.

IV. Technologies utilisées dans les réseaux mobiles ad hoc

Différents types d'équipement existent pour la mise en place d'un réseau sans fil. Actuellement les standards IEEE 802.11, Bluetooth et HiperLAN sont principalement utilisés dans les réseaux ad hoc pour le support des communications sans fil.

V. Routage dans les réseaux mobiles ad hoc

1. Définition du routage

Le routage est une méthode d'acheminement des informations à la bonne destination à travers un réseau de connexion donné. Le problème consiste à trouver l'investissement de moindre coût en capacités nominales et de réserves qui assure le routage du trafic nominal et garantit sa fiabilité en cas de n'importe quelle panne d'arc ou de nœud.

Les protocoles de routage utilisent deux principales méthodes : **état de lien** qui cherche à maintenir dans chaque nœud une carte plus ou moins complète du réseau et à **vecteur de distance** qui ne conserve que la liste des nœuds du réseau et l'identité du voisin par lequel passer pour atteindre la destination par le chemin le plus court.

2. Les types de protocoles de routage dans les réseaux mobiles ad hoc

Dans les travaux menés à l'IETF, plusieurs familles de protocoles se sont rapidement dégagées et qui se basent sur l'utilisation des méthodes citées précédemment. Chaque protocole peut ainsi être classifié en tant que réactif, proactif, ou hybride [24, 25, 26].

- **Les protocoles réactifs :** le principe est de ne rien faire tant qu'une application ne demande pas explicitement d'envoyer un paquet vers un nœud distant. Cela permet d'économiser de la bande passante et de l'énergie. Lorsqu'un paquet doit être envoyé, le protocole de routage va rechercher un chemin jusqu'à la destination. L'avantage majeur de cette méthode est qu'elle ne génère du trafic de contrôle que lorsqu'il est nécessaire.

Les principales contreparties sont que l'inondation est un mécanisme coûteux qui va faire intervenir tous les nœuds du réseau en très peu de temps et qu'il va y avoir un délai à l'établissement des routes. **AODV** (**A**d hoc **O**n **D**emand **D**istance **V**ector) est un exemple d'algorithme de routage à la demande, et qui utilise le principe des numéros de séquence afin de maintenir la consistance des informations de routage. Le protocole "Routage à Source Dynamique" (DSR : Dynamic Source Routing), est basé sur l'utilisation de la technique "routage source". Dans cette technique, la source des données détermine la séquence complète des nœuds à travers lesquels, les paquets de données seront envoyés ;

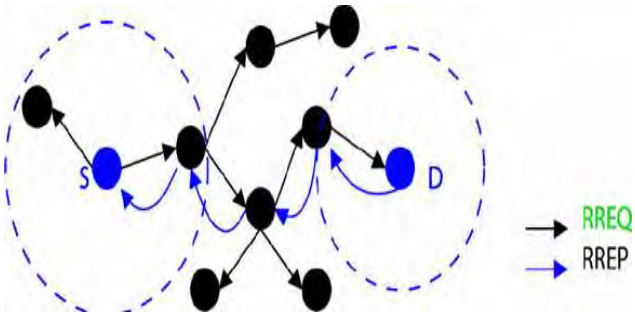

Figure 2. 2 : principe du routage par la source

- **Les protocoles proactifs :** le principe de base est de maintenir à jour les tables de routage, de sorte que lorsqu'un nœud désire envoyer un paquet à un autre nœud, une route soit immédiatement connue. Dans le contexte des réseaux ad hoc les nœuds peuvent apparaître ou disparaître de manière aléatoire et la topologie même du réseau peut changer. Cela signifie qu'il va falloir un échange continuel d'informations pour que chaque nœud ait une image à jour du réseau. L'avantage premier de ce type de protocole est d'avoir les routes immédiatement disponibles quand les applications en ont besoin, mais cela se fait au coût d'échanges réguliers de messages (consommation de bande passante) qui ne sont certainement pas tous nécessaires (seules certaines routes seront utilisées par les applications en général). **OLSR** (**O**ptimized **L**ink **S**tate **P**rotocol) est un exemple de protocole pour le routage proactif. Principalement deux types de messages sont introduits : "Hello" et "TC"(Topology Control) ;

- **Les protocoles hybrides :** combinent les approches réactive et proactive. Le principe est de connaître notre voisinage de manière proactive jusqu'à une certaine distance (par exemple trois ou quatre sauts), et si jamais un nœud cherche à envoyer quelque chose à un nœud qui n'est pas dans cette zone, d'effectuer une recherche réactive à l'extérieur. Selon le type de trafic et les routes demandées, ce type de protocole hybride peut cependant combiner les désavantages des deux méthodes : échange de paquets de contrôle réguliers et inondation de l'ensemble du réseau pour chercher une route vers un nœud éloigné.

En guise d'exemple pour ce type de protocole nous pouvons citer le protocole ZRP. Le protocole **ZRP** (ou **Z**one **R**outing **P**rotocol) tente de réunir les avantages de chacune des approches. Pour cela, il utilise un découpage du réseau. La zone proche (ou IARP) se base sur l'approche proactive et la zone éloignée (ou IERP) utilise plutôt un protocole réactif. IARP (ou IntrAzone Routing Protocol) reposant sur un protocole à état de lien permet la construction au niveau de chaque nœud interne à la zone des routes optimales vers les voisins proches. IERP (ou IntErzone Routing Protocol) se charge de rechercher les routes, à la demande, situées dans la zone externe. Comme dans tout protocole réactif cette recherche se fait par inondation.

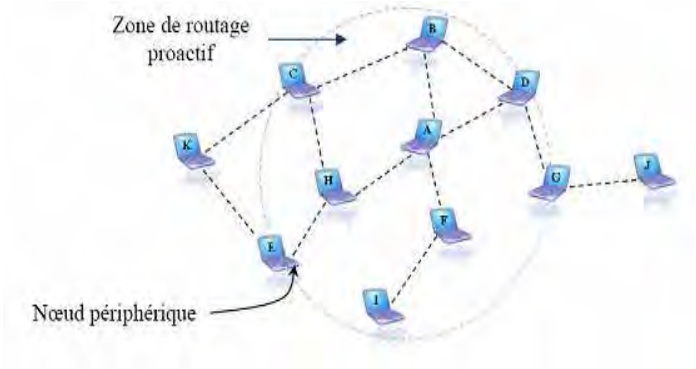

Figure 2. 3 : la zone de routage A à deux sauts

Introduction

La sécurité est un domaine qui concerne la protection des biens mais aussi de l'information. La sécurité réseau repose sur l'utilisation des moyens pour protéger les données lors de leur transmission [24, 31]. Cependant les MANETs sont des réseaux sans fil, mobiles, sans infrastructure préexistante, et chaque nœud est autonome et participe activement au routage. De par leurs caractéristiques, les réseaux ad hoc sont soumis à de nombreux problèmes de sécurité et sont souvent victimes d'attaques. C'est pourquoi nous devons disposer de services et de mécanismes pour assurer la sécurité de ce type de réseau.

1. Les attaques

Une attaque est une action qui vise à compromettre la sécurité du réseau. Elles peuvent être actives ou passives.

- **Les attaques passives :** elles ne visent pas à compromettre les données elles-mêmes ou un service mais à dévoiler son contenu par exemple écouter le trafic, intercepter une donnée ;

- **Les attaques actives :** elles entraînent une modification ou une création de données dans le flux. Les MANETs puisent un grand nombre de leurs avantages dans la confiance qu'ils accordent à leurs nœuds mobiles. En effet, ces derniers sont à la fois les clients et routeurs du réseau. Il en découle une faille potentielle dans la confidentialité comme dans l'authenticité des données transmises, puisqu'un nœud malicieux peut tout à fait tenter une **mascarade** (usurpation d'adresse), une **modification** de messages, un **rejeu** (retransmission des données capturées), qui pourront engendrer un **déni de service** (empêcher un ou plusieurs services de fonctionner normalement). Pour diminuer ou empêcher ces attaques des mécanismes et des services devront être assurés.

2. Services et mécanismes

Les services de sécurité sont des moyens pour prévenir ou détecter les attaques et ainsi de renforcer la sécurité. Ces services sont assurés par des mécanismes. Les services de sécurité sont :

- **L'authentification :** c'est l'assurance que l'entité communicante est bien celle qu'elle prétend être. S'il existe de nombreuses solutions d'authentification par serveur pour les réseaux à topologie statique (LDAP...), l'absence de structure prédéfinie d'un réseau Ad Hoc, empêche son application. En effet, la disponibilité d'un serveur dans un réseau Ad Hoc ne peut en aucun cas être garanti et pourrait entraîner une inaccessibilité aux services. Afin de permettre l'authentification des communications entre clients, il est nécessaire de passer par des systèmes de clefs pour le cryptage en utilisant le principe de confiance ;

- **La confidentialité :** c'est la protection d'un dévoilement d'un contenu non autorisé. La confidentialité des données dans les réseaux mobiles est soumise aux mêmes problématiques que sur un réseau filaire. La conséquence est que les solutions sont logiquement identiques : l'utilisation d'algorithmes permettant le **chiffrement** par clefs symétriques ou asymétriques. Les clés WEP (Wire Equivalent Privacy) sont très répandues pour assurer la confidentialité des échanges. Il s'agit d'une clé privée partagée par tous les utilisateurs du réseau, d'une taille de 64 ou 128 bits ;

- **L'intégrité :** c'est l'assurance que les données reçues ne sont pas corrompues (modifiées, pas d'erreur). L'intégrité des données peut être vérifiée dans un réseau Ad Hoc comme dans un réseau filaire classique grâce aux fonctions de hachage. En effet, ce type de fonction permet d'obtenir une empreinte (**signature**) de taille fixe à partir d'un message de taille variable ;

- **La non répudiation :** elle assure qu'un participant ne peut pas nier d'avoir pris part à la communication. Dans les MANETs, l'absence de structure prédéfinie empêche l'utilisation de serveurs dédiés, donc il faut penser à la signature numérique et à la confiance. Chaque nœud possède une liste de nœuds de « confiance », pour lesquels il établit des certificats. Lorsque deux nœuds s'estimant dignes de confiance s'autorisent à communiquer, ils se transmettent l'ensemble de leurs contacts. Ainsi une chaîne de confiance est mise en place. Pour sécuriser le routage dans un réseau traditionnel, il est suffisant de protéger et d'authentifier les routeurs dédiés, mais pour assurer la sécurité du routage dans un MANET, chacun des nœuds doit non seulement prendre la

responsabilité de ses propres comportements mais aussi vérifier les comportements des autres nœuds ;

- **La disponibilité :** elle assure que les services réseau sont disponibles quand plusieurs entités (utilisateurs, applications) en auront besoin. Elle est assurée par des mécanismes non orientés cryptage comme l'utilisation des firewalls pour le filtrage des paquets, et des systèmes de détection d'intrusion.

Conclusion

Cette partie nous a permis de connaître les spécificités des réseaux mobiles ad hoc, les différents types de protocoles de routage qu'ils utilisent et aussi les notions de sécurité comme les attaques, les services et les mécanismes.

Cependant il se pose un problème de sécurité au niveau du routage dans les réseaux mobiles, où il est difficile de localiser la destination à un instant donné. La difficulté augmente dans le cas où tous les sites peuvent se déplacer de façon aléatoire, ce qui est le cas pour les réseaux mobiles ad hoc.

Partie III :
ATTAQUES DE TYPE DoS DANS LES RESEAUX MOBILES AD HOC