

Etat de l'art du domaine

Chapitre 2

Contexte de nos travaux de recherche

2.1	MANet : une définition	25
2.2	MANet : quel intérêt ?	26
2.2.1	Absence d'infrastructure	26
2.2.2	Eviter d'utiliser l'infrastructure	26
2.2.3	Extension de l'infrastructure existante	27
2.3	Différents MANets, différentes contraintes	27
2.3.1	Contraintes	27
2.3.2	Exemple : réseau véhiculaire	30
2.3.3	Exemple : réseau de capteurs mobiles, application scientifique	30
2.3.4	Exemple : réseau à vitesse humaine, jeu collaboratif	31
2.3.5	Une solution unique est elle possible ?	31
2.4	Nos hypothèses de travail	31
2.4.1	Mobilité, volatilité	31
2.4.2	Autonomie	32
2.4.3	Applications visées, trafic	32
2.4.4	Sécurité	32
2.5	Conclusion	33

Dans ce chapitre nous présentons ce qu'est un MANet¹, et quelle en est l'utilité, avant de préciser le contexte dans lequel nous plaçons notre travail.

2.1 MANet : une définition

Un réseau mobile ad hoc, appelé aussi MANet, est un réseau autoconfiguré qui se constitue spontanément entre des terminaux sans fil mobiles (type PDA, Pocket PC, laptop) se déplaçant librement, sans utilisation d'une infrastructure préalablement établie [23].

Les réseaux ad hoc multisauts possèdent de nombreuses caractéristiques les différenciant des réseaux filaires classiques et des réseaux sans fil à un saut plus anciens :

Routage multisauts. Les MANets présentent la particularité de pouvoir router les messages en l'absence d'infrastructure : deux terminaux pourront donc communiquer sans être à portée l'un de l'autre s'il existe une chaîne de terminaux qui les connectent. La tâche de routage, effectuée dans les réseaux filaires par des terminaux dédiés, incombe ici à tous les terminaux.

1. Mobile Ad hoc NETWORK

Gestion du réseau distribuée. En l'absence d'un élément central dans le réseau, sa gestion (sécurité, contrôle de congestion) doit être effectuée de concert et de façon distribuée par les terminaux.

Topologie dynamique. Du fait de la mobilité et de la "volatilité" des terminaux, la topologie du réseau est susceptible d'évoluer en permanence.

Capacité des liens variables. La capacité des liens varie au cours du temps suivant de nombreux critères : puissance d'émission du signal, distance entre les noeuds, bruit, interférences, obstacles. De manière générale, la bande passante est moins "large" que celle d'un réseau filaire.

Terminaux légers. Les terminaux mobiles sont limités en ressources matérielles : ils possèdent une puissance de calcul et un espace mémoire moindre que les stations de travail et les serveurs, et travaillent sur batterie.

2.2 MANet : quel intérêt ?

La couverture 3G étant de plus en plus étendue, elle permet aux terminaux sans fil de se connecter à une infrastructure. Dans de telles circonstances, en quoi un MANet est-il utile ?

2.2.1 Absence d'infrastructure

Les travaux les plus anciens sur les MANets se sont fait sur deux scénarii.

Le premier est un scénario militaire. Lors d'un déploiement sur un territoire où il n'y a pas d'infrastructure de communication à disposition, ou dans le cas où ces infrastructures ne sont pas sécurisées, les communications passent par satellite. Cependant, les communications via satellite ont de grands délais de transmission, avec des équipements encombrants et spécialisés (généralement des téléphones). Les MANets sont donc utilisés pour communiquer au sein d'une équipe sur le terrain, avec souvent un seul terminal possédant un accès satellite au sein du groupe.

On trouve de nombreuses références à des travaux de recherche sur les MANets tactiques, notamment ceux menés ou financés par le NRL (Naval Research Laboratory) [66] [19]. Cependant, de par la nature des travaux, il y a peu de rapports d'expériences réelles.

Le second scénario est celui d'une catastrophe naturelle suite à laquelle les infrastructures de communications sont tombées. Les infrastructures de communications cellulaires sont rapidement rétablies, mais comme les chances de retrouver des survivants diminuent très rapidement, les secours doivent donc se faire le plus tôt possible. Dans un tel contexte, les réseaux spontanés sont utilisés pour coordonner des équipes de secours.

Aujourd'hui, les MANets sont étendus à des applications non critiques en l'absence d'infrastructure, comme par exemple le travail nomade.

2.2.2 Eviter d'utiliser l'infrastructure

L'entité propriétaire d'une infrastructure en fait souvent payer l'accès.

Prenons par exemple le cas d'une équipe de chercheurs partie à l'étranger dans le cadre d'un projet. Tous les membres de l'équipe sont logés dans le même hôtel où chaque chambre est équipée d'une connexion Internet, disponible à l'heure moyennant rémunération. Au sein du groupe des fichiers sont édités par plusieurs membres de l'équipe. Dans l'absolu,

un accès à internet n'est pas nécessaire, mais passer par un réseau permet d'envoyer les fichiers à tous sans avoir à échanger une clé USB et en suivant les évolutions du fichier édité en temps réel.

En établissant un MANet, l'édition peut se faire en ligne, par exemple en utilisant un éditeur collaboratif, sans passer par l'infrastructure de l'hôtel.

2.2.3 Extension de l'infrastructure existante

En présence d'un accès limité à Internet, on peut utiliser un MANet en extension de l'infrastructure existante.

Lors d'une réunion, un seul ordinateur peut avoir accès à Internet, via un câble ethernet. Les participants se passent donc le câble régulièrement afin d'accéder à leur boîte mail. Une autre alternative serait que les terminaux se constituent en réseau ad hoc. Le terminal ayant accès à internet devient alors relai et permet à chacun de consulter son mail en même temps.

2.3 Différents MANets, différentes contraintes

Comme nous l'avons vu dans la section précédente, les MANets répondent à un besoin réel, malgré l'étendue de l'infrastructure de communication actuelle. Cependant, un réseau mobile ad hoc peut être constitué dans différentes conditions.

Les caractéristiques variables sont nombreuses. Nous les détaillons ci-dessous, avant de présenter 3 implémentations concrètes de MANets avec différentes contraintes, menées dans le cadre de projets de recherche.

2.3.1 Contraintes

2.3.1.1 Taille du réseau

Le problème de taille du réseau se pose à différents niveaux :

- Le nombre de terminaux impliqués est-il connu par avance ? Dans ce cas, les connaît-on tous ? Les terminaux peuvent-ils rentrer dynamiquement dans le réseau ?
- Quel est le nombre maximum souhaité de terminaux possibles ?

Si des terminaux peuvent entrer dynamiquement dans le réseau, on a alors un problème d'attribution d'identifiants uniques, comme une adresse IP.

La taille du réseau influe sur le choix des protocoles de routage et de communications. Pour les réseaux de grande taille, des algorithmes de routage hiérarchique ont été proposés afin de limiter la surcharge créée par la découverte des routes. Par ailleurs, dans un réseau de petite taille, on peut utiliser des techniques d'inondation qui sont trop coûteuses dans un grand réseau.

2.3.1.2 Mobilité

La mobilité des terminaux recoupe plusieurs problèmes :

- Vitesse : quelle est la vitesse de déplacement des terminaux ?
 - Schéma de déplacement : comment les terminaux se déplacent-ils les uns par rapport aux autres ?
 - Volatilité : quelle est la probabilité qu'un terminal disparaisse du réseau ?
-

La vitesse des terminaux peut varier de la vitesse d'un piéton à celle d'une voiture. Une vitesse élevée influence les communications au niveau de la couche physique. Par ailleurs, deux terminaux se croisant à grande vitesse ne peuvent échanger que peu d'information.

Le schéma de déplacement peut prendre différentes formes : groupe d'utilisateurs se déplaçant et travaillant ensemble ; utilisateurs se croisant par hasard et échangeant des informations parce qu'ils en ont l'opportunité ; ou encore voitures sur une autoroute où toutes se déplacent à vitesse égale dans la même direction, sans que leurs utilisateurs se soient concertés. Le type d'application dans ces 3 cas ne sera, bien entendu, pas le même.

La volatilité des terminaux reflète la stabilité du réseau. On peut avoir, par exemple, un réseau de capteurs qui s'endorment périodiquement afin de sauvegarder leurs batteries, mais dans lequel on peut cependant compter sur le fait qu'ils se réveilleront à nouveau plus tard, pour effectuer une communication. Sur une autoroute au contraire, une voiture avec laquelle une communication était établie et qui emprunte une bretelle de sortie ne sera probablement jamais recroisée.

2.3.1.3 Autonomie et stockage

Un terminal étant mobile, il travaille a priori sur batterie. L'autonomie d'un terminal définit le temps de travail, que nous appelons ici session, possible pour le terminal.

Un terminal peut avoir une autonomie illimitée, comme par exemple pour une voiture, limitée mais avec possibilité de recharge (session limitée), comme, par exemple, pour un PDA ou ne plus fonctionner une fois que les batteries sont vidées (durée de vie limitée), dans le cas de certains capteurs.

Les sources principales de consommation de la batterie sur un terminal sont l'écran, les mémoires de masse nécessitant une partie mécanique (disque dur) et la carte réseau. De plus en plus des terminaux portables de nos jours utilisent de la mémoire SSD, qui, ne comportant pas de pièces mécaniques, consomment moins. La fréquence des accès disques et l'affichage sont gérés de manière optimisée par le système. Ce ne donc pas des points sur lesquels nous pouvons jouer.

D'après [57], les communications peuvent consommer jusqu'à 50% de la batterie. Ces chiffres datent de 10 ans, et les techniques de gestion de la carte réseau se sont améliorées depuis (passage en mode sleep plutôt que idle). Cependant, les utilisateurs de smartphone peuvent facilement constater le coût de l'utilisation du réseau. Apple annonce, par exemple, une autonomie de 40h de vidéo pour son iPhone 3GS, utilisant pourtant le processeur et l'écran, contre 10h si on surfe en wifi.

Par ailleurs, les capacités de stockage d'un terminal mobile sont souvent plus limitées que celles d'un ordinateur de bureau classique. Dans les réseaux de capteurs, des algorithmes d'agrégation des données sont parfois mis en oeuvre afin de sauvegarder de l'espace mémoire.

Enfin, les capacités de calcul d'un terminal mobile sont aussi plus limitées, ce qui peut poser problème par exemple quand on cherche à mettre en place des communications sécurisées, comme expliqué dans la section suivante.

A titre d'exemple, le tableau 2.1 liste les capacités de différents types de terminaux.

2.3.1.4 Sécurité

Le besoin de sécurité a deux aspects :

- la sécurisation des communications : empêcher un tiers de capter et comprendre un échange, voire d'empêcher les communications d'avoir lieu,
-

TABLE 2.1 – Quelques plateformes

Plate-forme	CPU	RAM	Stockage secondaire	Autonomie	Autres
Capteur Iris Mote	16MHz	8ko	512ko	2 batteries AA	GPS, différents capteurs
OLPC XO-1	433MHz	256 Mio	1Gi	5h, 10 à 12h selon sources	Recharge manuelle
Smartphone N900	600MHz	256Mo	32Go	5h en conversation	GPS
Subnotebook EEE pc 1001 HA	533MHz à 1,6GHz	1Go	160Go	8h30	
Portable macbook 13 pouces	2,4GHz	4G	250Go	10h	
Ordinateur de bureau imac	4*2,8Ghz	4 à 16Go	500Go à 1To		
Serveur Bell Poweredge M910	8 * 2,4GHz	1Go à 512Go	4To à 8To		

– l’authentification et l’identification des pairs : identifier un pair et prouver son identité. Un MANet étant un réseau spontané et sans fil, n’importe quel terminal peut potentiellement s’y joindre et s’en prétendre membre. Il est donc nécessaire d’avoir un moyen d’authentifier les pairs. Dans un réseau classique, cela se fait généralement en utilisant les services d’un tiers de confiance [56], service sur lequel on ne peut pas compter dans un MANet. Cela rend donc le réseau plus sensible aux attaques de type déni de service, un brouilleur créant des interférences électromagnétiques pouvant d’ailleurs empêcher toute communication.

Par ailleurs, même sans essayer de se faire passer pour un membre du MANet, les communications sans fil peuvent être écoutées. Afin de protéger les données, celles ci doivent donc être chiffrées avec un secret partagé. Le chiffrement des données est problématique pour des terminaux avec des processeurs peu puissants car le temps de chiffrement et déchiffrement est proportionnel à la garantie de sécurité offerte. Une meilleure sécurité ralentit donc le travail. Par ailleurs, le calcul est consommateur de batterie.

Ce besoin de sécurité varie selon le type d’application visé. Dans le cas d’un usage militaire, le chiffrement des communications et la détection des intrus sont cruciaux, alors que dans le cas d’un usage civil ces contraintes peuvent être relâchées.

2.3.1.5 Application

Selon le type d’application visé, les terminaux vont générer des profils de trafic différents. Les réseaux de capteurs envoyant périodiquement un relevé de mesure ne posent pas les mêmes contraintes qu’un réseau d’utilisateurs humains partageant des documents en édition. Par ailleurs, certaines applications ne font que des communications locales (1 ou 2 sauts), alors que d’autres ont besoin de joindre un terminal précis appartenant au réseau. Le premier cas ne nécessite pas forcément un algorithme de routage, alors que le second nécessite une découverte du réseau.

Nous allons présenter trois projets de recherche utilisant les MANets pour différents usages, et voir à quel point ces différentes caractéristiques peuvent varier selon le domaine d'application.

2.3.2 Exemple : réseau véhiculaire

Les VANets, ou Vehicular Ad Hoc Networks, sont des réseaux constitués de véhicules. Le projet StreetSmart [26] propose de constituer les voitures sur une autoroute en VANet, afin de véhiculer des informations sur l'état du trafic. Une forte densité de véhicules avançant à faible vitesse permet de détecter une congestion. Cette information remonte ensuite le flot de véhicules et peut être utilisée par les systèmes de guidage GPS pour optimiser les trajets.

Le nombre de terminaux impliqués dans ces communications est élevé, puisque le réseau couvre l'ensemble du segment d'autoroute. Cependant, l'information ne circule que dans un sens, à l'inverse du flot de voitures, et les communications ne se font pas entre entités spécifiques. Il n'y a donc pas réellement de routage, et on doit simplement connaître les positions relatives des terminaux à un saut afin de décider comment les messages doivent être diffusés. Enfin, aucune information n'a à être stockée après avoir été transmise. Il n'y a pas de problème d'autonomie ou de stockage. La sécurité n'est pas abordée.

2.3.3 Exemple : réseau de capteurs mobiles, application scientifique

Dans le projet ZebraNet [50], une équipe de chercheurs veut étudier le comportement d'un troupeau de zèbres. Chaque zèbre est équipé d'un collier capteur GPS faisant régulièrement un enregistrement de position. Périodiquement, un des chercheurs passe à proximité du troupeau afin de récupérer les informations. C'est le seul moment dans l'absolu où les terminaux ont à communiquer, ce qui utilise leur batterie, mais des communications sont tout de même maintenues en dehors des périodes où l'information est recueillie.

La création de nouvelles données est périodique. Si on connaît la fréquence de passage du chercheur, on peut donc prédire les capacités de stockage nécessaires. Cependant, la capacité de stockage d'un capteur étant faible, les données recueillies sont agrégées afin de ne pas occuper tout l'espace-mémoire. La durée de vie d'un capteur est par ailleurs limitée par ses batteries. Quand les batteries d'un collier sont vides, il faut capturer à nouveau l'animal portant ce collier pour les remplacer ou changer le capteur. Les données sont donc répliquées sur différents capteurs, afin qu'aucune ne soit perdue.



FIGURE 2.1 – Un zèbre équipé du collier GPS

Le nombre de terminaux ici est de l'ordre de la centaine. Les terminaux se déplacent en groupe, et les communications sont faites de manière opportuniste pour sauvegarder les informations. L'autonomie des terminaux étant faible, ce système cherche donc à la maximiser.

2.3.4 Exemple : réseau à vitesse humaine, jeu collaboratif

Dans le projet Transhumance [30], un jeu de piste est organisé sur la Butte-aux-Cailles. Les utilisateurs sont organisés en groupes, chaque membre ayant un PDA. Au début d'une session de jeu, un questionnaire est distribué sur les terminaux des joueurs. La première équipe à trouver tous les éléments et revenir à l'arbitre a gagné. A défaut, l'équipe ayant trouvé le plus d'éléments à la fin du temps imparti gagne.

La durée d'une session de jeu pour un groupe est limitée par la batterie de ses terminaux. Différents utilitaires sont proposés aux joueurs, comme un chat, un vote, ou un partage de fichier. Ici, les joueurs sont organisés en groupes collaborant. Même s'ils peuvent se séparer, par exemple pour que chacun aille chercher un indice individuellement, ils se retrouvent par la suite et leurs feuilles de réponses doivent être synchronisées.



FIGURE 2.2 – Une session de jeu sur la Butte-aux-Cailles

Les communications peuvent être chiffrées, pour que les membres des équipes adverses ne puissent pas connaître les réponses, cependant sécuriser les données n'est pas ici critique.

2.3.5 Une solution unique est elle possible ?

Comme on peut le voir dans ces différents exemples, un MANet est un réseau de terminaux mobiles, qui peut prendre de nombreuses formes. Plutôt que d'essayer d'offrir une solution globale non satisfaisante, nous préférons travailler à une solution adaptée à un contexte. Dans la section suivante nous présentons donc le cadre de nos travaux.

2.4 Nos hypothèses de travail

Dans cette thèse nous voulons proposer une solution facilitant le partage de données pour applications collaboratives. Nous détaillons donc, dans cette section, nos hypothèses de travail.

2.4.1 Mobilité, volatilité

Notre système est destiné à un réseau de piétons, avec des utilisateurs se déplaçant en groupes.

Le nombre de terminaux n'est pas connu par avance, mais ne dépasse pas la centaine. Des terminaux peuvent se joindre spontanément à une session de travail, mais afin de pouvoir

participer à la session de travail collaboratif, ils devront avoir les bonnes applications installées.

Les utilisateurs essayant de travailler en groupes, nous attendons des phases de stabilité au niveau de la présence. Cependant, des utilisateurs peuvent entrer et sortir du groupe, et différents groupes peuvent se croiser, voir fusionner, auquel cas des informations seront échangées.

Par ailleurs, des utilisateurs peuvent disparaître, par exemple à cause des problèmes de batteries susmentionnés.

2.4.2 Autonomie

Nous visons des terminaux de type portable ou PDA, travaillant en mode nomade. Il n'y a donc pas de problème critique de stockage, contrairement par exemple à un réseaux de capteur. Par contre, la batterie limite le temps d'une session de travail. Cependant, les batteries peuvent être rechargées et le terminal peut revenir dans le réseau. La durée d'une session de travail est donc limitée, mais la disparition d'un terminal n'est pas nécessairement définitive (faute transitoire).

2.4.3 Applications visées, trafic

Nous voulons permettre le travail nomade.

Dans leurs bureaux, les utilisateurs utilisent habituellement une application centralisée classique, comme un système de partage de fichiers, pour collaborer. Quand ils passent en mode nomade, une version distribuée de l'application est déployée sur les terminaux utilisateurs. Cette application distribuée reproduit les services offerts par sa version centralisée, avec éventuellement des restrictions (par exemple, les données de taille trop grandes, comme des vidéos, ne sont pas disponibles durant la phase de mobilité). Durant une période de nomadisme, qui peut durer plusieurs sessions de travail, les utilisateurs peuvent donc toujours travailler collaborativement. Quand les utilisateurs rejoignent leurs bureaux à l'issue de leur voyage, les modifications effectuées durant la période nomade sont fusionnées aux données de l'application centralisée.

Comme les données sont éditées par des utilisateurs humains, nous avons les contraintes suivantes :

- Les données sont modifiées.
- Les mises à jour des données sont sporadiques.
- Les mises à jour peuvent être effectuées depuis tous les terminaux.
- L'accès aux données est aperiodique.

Il est important de préciser ces contraintes, car des solutions ont déjà été proposées pour des systèmes de capteurs actualisant et utilisant périodiquement des données [34], ou les systèmes avec un serveur de fichier, seul habilité à modifier la donnée [62].

On ne peut donc pas prévoir à l'avance des schémas de trafic précis.

Enfin, nous ne souhaitons pas mettre en œuvre des applications de type flux multimédia qui imposent des contraintes temps réel au niveau des communications.

2.4.4 Sécurité

Ces applications n'étant pas destinées à l'échange de données critiques, nous ne proposons pas ici de système de sécurisation des données et des échanges par authentification et

chiffrement. Cependant, un système de sécurité peut être ajouté à notre proposition par la suite, sans que nous ayons à la modifier.

2.5 Conclusion

Nous avons vu dans cette section dans quelles circonstances un MANet peut s'avérer utile : les premières applications étaient liées aux situations d'urgence, par exemple suite à une catastrophe, ou dans une situation de militaire, mais on peut aussi les utiliser pour un usage civil quand les infrastructures sont inexistantes, ou compliquées d'accès.

Nous avons présenté les différentes contraintes liés aux MANets : taille du réseau, mobilité et capacité des terminaux (autonomie et stockage).

Nous avons ensuite vu trois projets de recherche utilisant les MANets dans des contextes très distincts avant de présenter le contexte de nos travaux : des MANets d'une centaine de terminaux mobiles opérés par des utilisateurs humains, qui utilisent des applications collaboratives.
