

الجمهورية الجزائرية الديمقراطية الشعبية
RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE
وزارة التعليم العالي والبحث العلمي
Ministère de L'Enseignement Supérieur et de la Recherche Scientifique
جامعة أمّار ثليجي بالأغواط
UNIVERSITE AMMAR THLIDJI

كلية العلوم
Faculté des Sciences

قسم الإعلام الآلي
Département de Informatique



MÉMOIRE

Présentée pour l'obtention du **diplôme de Master**

En : informatique

Spécialité : réseaux, systèmes et applications répartis

Par :

YAGOUBI WAIL HADJ ALLAL DHIA EDDINE

BIDI MOHAMMED ABDELHAK

Sujet

**Dissémination des données dans les reseaux des drones tolérants
aux délais**

Soutenu publiquement le 25-06-2023 devant le jury composé de :

M.	Ali BOUKEHILA	Maître de Conférences A	à l'UATL	Président
Mme.	Zohra ABDELHAFIDI	Maître de Conférences A	à l'UATL	Examineur
M.	Mohamed el amine AMEUR	Maître de Assistant A	à l'UATL	Examineur
M.	Tahar ALLAOUI	Maître de Conférences B	à l'UATL	Encadreur

2022/2023

Je voudrais tout d'abord adresser toute ma gratitude a Monsieur Tahar Allaoui pour son aide et ses précieux conseils qu'il a sus me transmettre tout au long de ce projet.

Je tiens a le remercier tout particulierement pour son soutien durant toute cette année. Ma volonté de poursuivre dans ce domaine tient en particulier a son enseignement pour lequel, je souhaite lui témoigner toute ma reconnaissance. Je remercie tous les professeurs qui ont contribue au renforcement de mes connaissances et qui m'ont donn e les outils indispensables a la poursuite de mes études.

Un grand merci a l'ensemble de ma famille et mes amis pour leur amour, leur confiance, leurs conseils ainsi que toute personne qui a contribue de pres ou de loin .

YAGOUBI WAIL HADJ ALLAL.

Avec joie je veux dédier ce modeste travail

A mes chers parents , mon cher frères pour leurs soutiens
durant toutes ces années d'étude.

A toute la famille BIDI.

Je suis profondément reconnaissant à mon amie de
m'avoir accueilli une aide précieuse apportée. Il était
toujours présent dans les moments les plus difficiles, Merci
Aussi je dédie ce travaille à ma binôme ALLAL.

A tout mes Amis d'enfance et mes collègues et
enseignants de l'université Amar Telidji.

BIDI Mohammed abdelhak.

Remerciement

D'abord nous remercions Allah de nous avoir donnée santé, courage, volonté et foi pour mener ce travail. Au terme de la rédaction de ce mémoire, nous tenons à remercier notre encadreur Dr. TAHAR ALLAOUI pour suivi et Précieux conseils. et nous remercions le comité existant pour discuter de notre mémoire. On n'oublie pas de remercier nos professeurs, nos parents, nos frères et sœurs pour leur soutien moral et physique, pour les merveilleux moments qu'on a passés ensemble, et à tous amis sans exception.

ملخص

مع التطورات التكنولوجية الحديثة، أصبح إنتاج الطائرات بدون طيار ممكناً للدرون ، والتي يمكن استخدامها في العديد من التطبيقات العسكرية والتجارية والمدنية. ومع ذلك ، هناك حالات يكون فيها اتصال الشبكة متقطعاً ، وبالتالي فإن الشبكات المتسامحة للتأخير DTN هو نوع من الشبكات التي يمكن أن تعمل في بيئات قاسية حيث قد تفضل طرق الاتصال التقليدية. حيث لا يمكن ضمان الاتصال الدائم من طرف إلى طرف. وبالتالي ، فإن DTN تجعل من الممكن مواجهة مشاكل التنقل والتأخير التام والتأخير والكمون والطاقة المحدودة لمعدات الاتصال اللاسلكي. تتمثل مساهمتنا وهدفنا ، من خلال هذه الرسالة ، في تقييم أداء بروتوكولات التوجيه المطبقة على شبكات الطيران FANET اللاسلكية ، باستخدام محاكي OMNET++ لتحديد أفضل بروتوكول من حيث متوسط الإنتاجية ، والحزم المستلمة ، ومتوسط التأخير من طرف إلى طرف.

الكلمات المفتاحية: المحاكات ، OMNET++ ، DTN ، بروتوكول التوجيه ، FANET .

Abstract

With recent technological advances, the production of drones (unmanned aerial vehicles) has become possible, which can be used for several military, commercial and civilian applications. However, there are cases where network connectivity is intermittent, DTN is a type of network that can work in harsh environments where traditional communication methods may fail. where permanent end-to-end connectivity cannot be guaranteed. Thus, DTN makes it possible to face the problems of mobility and end-to-end delay and latency and limited energy of wireless communication equipment. our contribution and objective, through this thesis, is to evaluate the performance of routing protocols applied to FANET, using the omnet++ simulator to determine the best protocol in terms of average throughput, packet received, average delay end to end.

Keywords: FANET, DTN, Routing Protocol, Omnet++, Simulation.

Résumé

Avec les récents progrès technologiques, la production de drones (véhicules aériens sans pilote) est devenue possible, ce qui peut être utilisé pour plusieurs applications militaires, commerciales et civiles. Cependant, il existe des cas où la connectivité réseau est intermittente. DTN est un type de réseau qui peut fonctionner dans des environnements difficiles où les méthodes de communication traditionnelles peuvent échouer, où une connectivité permanente de bout en bout ne peut être garantie. Ainsi, DTN permet de faire face aux problèmes de mobilité, de retard et de latence de bout en bout et de l'énergie limitée de l'équipement de communication sans fil. Notre contribution et objectif, par le biais de cette thèse, est d'évaluer les performances des protocoles de routage appliqués aux réseaux sans fil FANET, en utilisant le simulateur Omnet++ pour déterminer le meilleur protocole en termes de débit moyen, de paquets reçus et de retard moyen de bout en bout.

Mots Clée : FANET, NTR, Protocole de Routage, Omnet++, Simulation.

Table des matières

Table des figures	i
Liste des tableaux	ii
Liste des Algorithmes	iii
Nomenclature	iv
Introduction Générale	1
1 État de l'art	3
1.1 Introduction	3
1.2 Définition	3
1.2.1 Un réseau filaire	3
1.2.2 Un réseau sans fil	4
1.2.3 Caractéristiques des réseaux Ad Hoc	8
1.2.4 Réseau mobile ad hoc (MANET)	9
1.2.5 réseau ad hoc véhiculaire (VANET)	10
1.2.6 Réseaux ad hoc volants (FANET)	11
1.2.7 Comparaison	12
1.3 FANET	14
1.3.1 Caractéristiques des réseaux FANET	14
1.3.2 Méthodes de communication dans FANET	14
1.3.3 Domaines d'application de FANET	15
1.3.4 Protocoles de routage FANet	16
1.3.5 Modèles de mobilité Fanet	18
1.4 Réseau tolérant aux retards (DTN)	19
1.4.1 Définition	19
1.4.2 Caractéristiques DTN	20
1.4.3 Routage dans un DTN	21

1.5	Conclusion	22
2	Étude comparative et proposition de nouvelle méthode	23
2.1	Introduction	23
2.1.1	Epidemic	23
2.1.2	Spray and wait	24
2.1.3	Prophet	25
2.1.4	Comparaison des protocoles	27
2.2	Notre contribution	29
2.2.1	Principe de fonctionnement	29
2.2.2	Pseudo code	30
2.3	Conclusion	31
3	La simulation et discussion de résultat	33
3.1	Introduction	33
3.2	La simulation	33
3.3	Outils de simulation	33
3.3.1	Omnet++	33
3.3.2	Inet Framework	34
3.3.3	OPS Framework	34
3.3.4	Fonctionnalités de Omnet++	34
3.4	Comparaison entre les autres outils de simulation	35
3.5	Paramètres de simulation	35
3.5.1	Modèle de mobilité	35
3.5.2	Scénarios de simulation	37
3.6	Résultats de simulation	37
3.6.1	l'influence du nombre de nœuds dans le données envoyé moyen . . .	38
3.6.2	l'influence du nombre de nœuds dans le taux de livraison moyen . .	38
3.6.3	l'influence du nombre de nœuds dans le retard moyen	39
3.6.4	l'influence du nombre de nœuds dans le duplication moyen	39
3.6.5	l'influence du nombre de nœuds dans le nombre de sauts moyen . .	40
3.6.6	l'influence du nombre de nœuds dans le cache moyen	40
3.6.7	l'influence du nombre de nœuds dans l'overhead moyen	41
3.6.8	l'influence du nombre de nœuds dans l'énergie moyen	41
3.7	Discussion de résultat	42
3.8	Conclusion	43

Conclusion Générale	44
Bibliographie	45

Table des figures

1.1	un réseau filaire	4
1.2	Un réseau sans fil	5
1.3	range de technologie sans fil	7
1.4	types de réseaux ad hoc	8
1.5	un réseau vanet	11
1.6	un réseau fanet	12
1.7	MANET, VANET, and FANET relationships.	13
1.8	le domaine de utilisation pour fanet	16
1.9	Protocoles de routage pour fanet.	16
1.10	modèles de mobilité pour fanet.	19
2.1	Epidemic for Hosts A and B within Communication Range	24
2.2	binary spray and wait exemple	25
2.3	prophet exemple	27
3.1	data envoyé moyen par rapport nombre de nœuds	38
3.2	taux de livraison moyen par rapport nombre de nœuds	38
3.3	retard moyen par rapport nombre de nœuds	39
3.4	duplication moyen par rapport nombre de nœuds	39
3.5	hop moyen par rapport nombre de nœuds	40
3.6	cache moyen par rapport nombre de nœuds	40
3.7	overhead moyen par rapport nombre de nœuds	41
3.8	energy moyen par rapport nombre de nœuds	41

Liste des tableaux

1.1	DESCRIPTION COMPARATIVE DES DIFFÉRENTS AD HOC RÉSEAUX [1]	13
1.2	Comparaison entre le DTN et les nœuds de réseau de communication tra- ditionnels [2]	20
2.1	Etude comparative des protocoles de routage DTN	29
3.1	Comparaison de haut niveau entre les simulateurs OppNets	35
3.2	Paramètres de simulation	37
3.3	Paramètres de spray and wait	37
3.4	Paramètres de prophet	37

Liste des Algorithmes

2.1 Our Contribution Routing Algorithm	31
--	----

Nomenclature

Acronymes / Abréviations

DTN	(Delay Tolerant Network)
FANET	(Flying Ad hoc Networks)
MANET	(Mobile Ad Hoc Network)
OMNeT++	(Objective Modular Network Testbed in C++)
UAV	(Unmanned Aerial Vehicle)
VANET	(Vehicular Ad hoc Network)
WEP	(Wired Equivalent Privacy)
Wi-Fi	(WIreless FIdelity)
WLAN	(Wireless Local Area Network)
WMAN	(Wireless Metropolitan Area Network)
WPA	(Wi-Fi Protected Access)
WPAN	(Wireless Personal Area Network)

Introduction Générale

Ces dernières années, le besoin de drones dans de nombreux domaines tels que la réponse aux catastrophes naturelles et la surveillance s'est généralisé. Ce besoin est confronté au défi que représentent les drones en raison de leur nature. En conséquence, de nouveaux concepts sont apparus, tels que les réseaux sans fil et les réseaux ad hoc. Les réseaux ad hoc sont des réseaux sans fil capables de s'organiser sans infrastructure. Par conséquent, la topologie du réseau peut changer rapidement et de manière imprévisible. Ce type de réseau a attiré l'attention des fabricants et des chercheurs lorsque des drones (UAV) ont été utilisés comme nœuds dans les flying ad hoc networks (FANET).

Toutefois, ce type de réseau se heurte à d'autres difficultés lorsque la connectivité est intermittente, d'où la nécessité de créer des réseaux tolérants aux retards (DTN). Les DTN sont une nouvelle classe de réseaux de communication qui visent à assurer la communication dans des scénarios où les réseaux traditionnels ne peuvent pas fonctionner correctement. Ces dernières années, le besoin de communication dans des environnements difficiles s'est accru, et les DTN sont apparus comme une solution potentielle à ce défi.

L'un des domaines d'application des DTN est celui des FANET. En raison de leur nature, les FANET connaissent des déconnexions fréquentes et une topologie de réseau imprévisible. Cela pose d'importants problèmes de communication, car les paquets doivent être livrés même en l'absence de connectivité de bout en bout.

Dans ces mémoire, nous souhaitons contribuer au développement et à la compréhension des DTN dans les FANET en explorant divers aspects de leur conception et de leur performance. Notre objectif sera de relever les défis posés et de répondre au besoin d'algorithmes de routage efficaces.

Dans ces mémoire, nous avons choisi des protocoles de routage pour les réseaux tolérants aux retards. Dans notre démarche, nous proposons le plan suivant :

Chapitre 1 : nous avons présenté les réseaux filaires et sans fil, les FANET en général, leurs caractéristiques ainsi que leurs applications, et nous les avons comparés aux MANET et VANET.

Chapitre 2 : nous avons fait une comparaison complète entre des algorithmes tolé-

rants au délai de routage théoriquement et pratiquement en utilisant OMNeT++. et nous avons optimisé et proposé un algorithme, l'avons simulé et évalué ses performances.

Chapitre 3 : nous le simulons et évaluons les performances.

Enfin, ces mémoire se termine par une conclusion générale, concluant les travaux menés dans le cadre de notre projet de fin d'études.

Chapitre 1

État de l'art

1.1 Introduction

DTN est un domaine relativement nouveau et en évolution qui a suscité un intérêt considérable au cours des dernières années. L'objectif de Delay Tolerant FANET est de créer un réseau capable de fonctionner même en l'absence d'un chemin de bout en bout. Dans ce chapitre, nous visons à fournir un aperçu complet de l'état de l'art du FANET et DTN. L'objectif est de fournir une base solide aux chercheurs intéressés par ce domaine et d'inspirer de nouvelles innovations dans le développement de DTN.

1.2 Définition

1.2.1 Un réseau filaire

Le réseau filaire est un réseau où les périphériques réseau sont connectés avec des câbles physiques [3]. les appareils se connectent à un concentrateur central, un commutateur ou un routeur, qui agit comme l'épine dorsale du réseau et est responsable de la transmission des données entre les appareils, gestion du trafic réseau et fourniture d'un accès Internet [4]. chaque routeur se connecte ensuite à un ou plusieurs routeurs pour que les données puissent être transmises d'un réseau local à un autre [3].

Ces réseaux sont plus fiables et ont une sécurité élevée, ainsi que des vitesses de transfert rapides et de faibles erreurs lors de la transmission [4]. Le câblage physique utilisé dans les réseaux câblés fournit également une connexion directe et dédiée entre les appareils, ce qui se traduit par une latence plus faible et moins de congestion du réseau par rapport aux réseaux sans fil [3]. Les réseaux filaires sont également hautement évolutifs. [3,4]

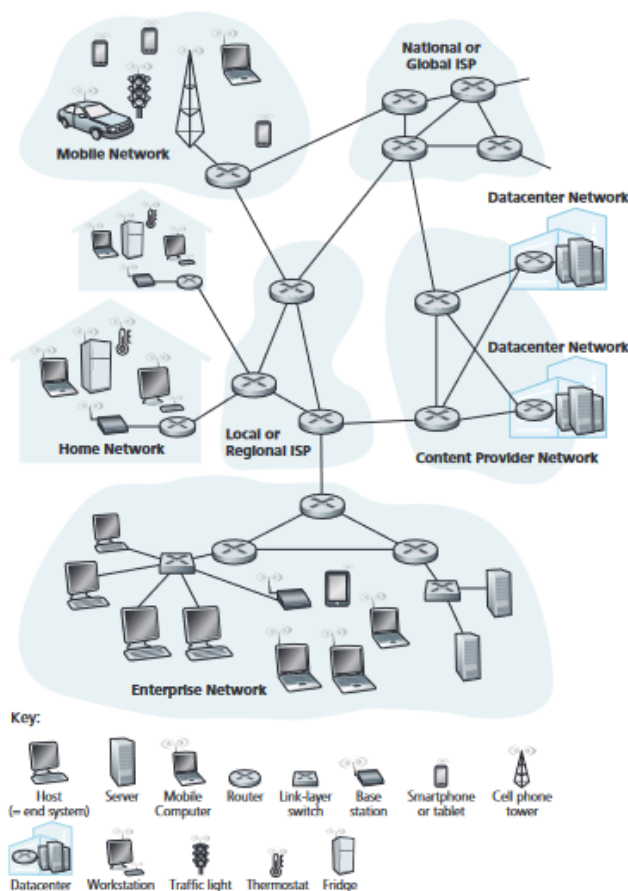


FIGURE 1.1 – un réseau filaire [4]

1.2.2 Un réseau sans fil

Le réseau sans fil est un réseau où les appareils communiquent sans utiliser de câbles [4]. mais avec l'utilisation d'ondes radio ou de signaux infrarouges pour transmettre des données entre appareils. Le plus utilisé est Wi-Fi, qui est utilisé pour connecter des appareils à Internet [4].

Les réseaux sans fil offrent également l'avantage de la mobilité, car les appareils peuvent se déplacer n'importe où dans la zone de couverture et être toujours connectés au réseau [3].

Le principal problème de ces réseaux est la sécurité, car les signaux sans fil peuvent être interceptés. Pour résoudre ce problème, les réseaux sans fil utilisent des protocoles de sécurité, tels que WPA2 et WEP. d'autres problèmes sont les interférences d'autres appareils, ce qui peut entraîner des performances réduites et des vitesses lentes.

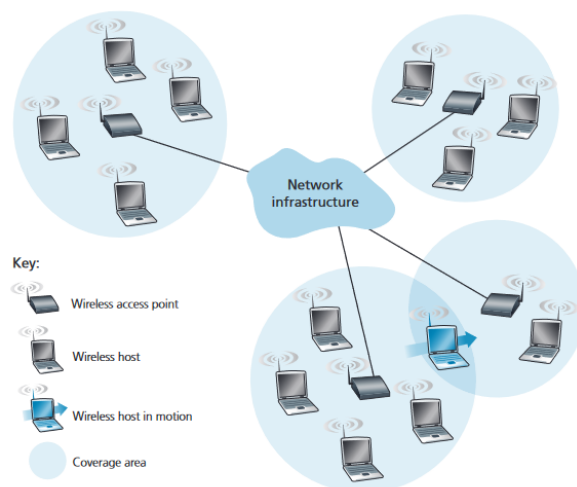


FIGURE 1.2 – Un réseau sans fil [4]

1.2.2.1 Les Catégories des réseaux sans fils

Les Catégories des réseaux sans fils On distingue habituellement plusieurs catégories de réseaux sans fils, selon le périmètre géographique offrant une connectivité (appelé zone de couverture) :

Réseaux personnels sans fils (WPAN) Le réseau personnel sans fils (appelé également réseau individuel sans fils ou réseau domotique sans fils et noté WPAN pour Wireless Personal Area Network) concerne les réseaux sans fils d'une faible portée : de l'ordre de quelques dizaines mètres. Ce type de réseau sert généralement à relier des périphériques (imprimante, téléphone portable, appareils domestiques, ...) ou un assistant personnel (PDA) à un ordinateur sans liaison filaire ou bien à permettre la liaison sans fils entre deux machines très peu distantes. [5] Il existe plusieurs technologies utilisées pour les WPAN :

-La principale technologie WPAN est la technologie Bluetooth, lancée par Ericsson en 1994, proposant un débit théorique de 1 Mbps pour une portée maximale d'une trentaine de mètres. Bluetooth, connue aussi sous le nom IEEE 802.15.1, possède l'avantage d'être très peu gourmand en énergie, ce qui le rend particulièrement adapté à une utilisation au sein de petits périphériques. La version 1.2 réduit notamment les interférences avec les réseaux Wi-Fi.

Réseaux locaux sans fils (WLAN) Le réseau local sans fils (WLAN pour Wireless Local Area Network) est un réseau permettant de couvrir l'équivalent d'un réseau local d'entreprise, soit une portée d'environ une centaine de mètres. Il permet de relier entre-

eux les terminaux présents dans la zone de couverture. [5] Il existe plusieurs technologies concurrentes :

-Le WiFi(ou IEEE 802.11), soutenu par l'alliance WECA (Wireless Ethernet Compatibility Alliance) offre des débits allant jusqu'à 54Mbps sur une distance de plusieurs centaines de mètres.

-hiperLAN2 (High Performance Radio LAN 2.0), norme européenne élaborée par l'ETSI (European Telecommunications Standards Institute), permet d'obtenir un débit théorique de 54 Mbps sur une zone d'une centaine de mètres dans la gamme de fréquence comprise entre 5 150 et 5 300 MHz.

-Réseaux métropolitains sans fils (WMAN) Le réseau métropolitain sans fils (WMAN pour Wireless Metropolitan Area Network) est connu sous le nom de Boucle Locale Radio (BLR). Les WMAN sont basés sur la norme IEEE 802.16. La boucle locale radio offre un débit utile de 1 à 10Mbit/s pour une portée de 4 à 10 kilomètres, ce qui destine principalement cette technologie aux opérateurs de télécommunication.

Réseaux étendus sans fils (WWAN) Le réseau étendu sans fils (WWAN pour Wireless Wide Area Network) est également connu sous le nom de réseau cellulaire mobile. Il s'agit des réseaux sans fils les plus répandus puisque tous les téléphones mobiles sont connecté à un réseau étendu sans fils. [5] Les principales technologies sont les suivantes :

-GSM (Global System for Mobile Communication ou Groupe Spécial Mobile)

-GPRS (General Packet Radio Service)

-UMTS (Universal Mobile Telecommunication System)

– Wimax (standard de réseau sans fils poussé par Intel avec Nokia, Fujitsu et Prowim). Basé sur une bande de fréquence de 2 à 11 GHz, offrant un débit maximum de 70 Mbits/s sur 50km de portée, certains le placent en concurrent de l'UMTS, même si ce dernier est davantage destiné aux utilisateurs itinérants.

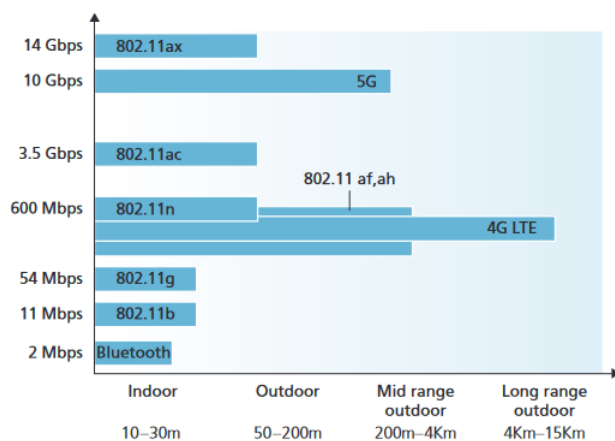


FIGURE 1.3 – range de technologie sans fil [4]

1.2.2.2 Fonctionnement d'un réseau sans fil

Le téléphone sans fil communique avec un correspondant par l'intermédiaire du socle qui fait office de point d'accès vers le réseau téléphonique. De même, chaque ordinateur du réseau sans fil muni d'une carte réseau adéquate peut émettre (et recevoir) des données vers (et depuis) un point d'accès réseau. Ce dernier peut être physiquement connecté au réseau câblé et fait alors office de point d'accès vers le réseau câblé. plus on s'éloigne du point d'accès, plus le débit diminue : pour un débit de 1Mbps, la portée est de 460 m dans un environnement sans obstacle et de 90 m dans un environnement de bureau classique. Le réseau sans fil offre deux modes de fonctionnement différents : le mode avec infrastructure et le mode sans infrastructure. [6, 7]

Les réseaux avec infrastructure (cellulaire) En mode avec infrastructure, également appelé le mode BSS (Basic Service Set) certains sites fixes, appelés station de base sont munis d'une interface sans fil pour la communication directe avec des sites mobiles ou unités mobiles, localisés dans une zone géographique limitée, appelée cellule. A chaque station de base correspond une cellule à partir de laquelle des unités mobiles peuvent émettre et recevoir des messages. Alors que les sites fixes sont interconnectés entre eux à travers un réseau de communication filaire, généralement fiable et d'un débit élevé. Les liaisons sans fil ont une bande passante limitée qui réduit sévèrement le volume des informations échangées. Dans ce modèle, une unité mobile doit être, à un instant donné, directement connectée à une seule station de base. [6, 7]

Les réseaux sans infrastructure (ad hoc) Le réseau sans infrastructure également appelé réseau Ad hoc ou IBSS (Independent Basic Service Set) ne comporte pas l'entité

site fixe, tous les sites du réseau sont mobiles et communique d'une manière directe en utilisant leurs interfaces de communication sans fil. L'absence de l'infrastructure ou du réseau filaire composé de station de base, oblige les unités mobiles à se comporter comme des routeurs qui participent à la découverte et à la maintenance des chemins pour les autres hôtes du réseau. La différence entre le mode Ad hoc et le mode avec infrastructure est que dans le premier mode, la communication entre deux machines se fait directement si elles se trouvent à la portée l'une de l'autre, alors que dans le second mode, toutes les communications passent par le point d'accès. [6, 7]

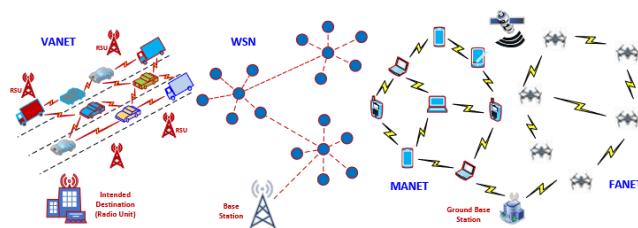


FIGURE 1.4 – types de réseaux ad hoc [8]

1.2.3 Caractéristiques des réseaux Ad Hoc

voici les caractéristiques du réseau ad hoc :

- **Liens asymétriques** : En théorie, les liaisons sont symétriques, car on a un affaiblissement du signal inversement proportionnel à la distance entre l'émetteur et le récepteur. Mais en pratique, ils sont asymétriques. On peut noter un déphasage dû aux multiples réflexions du signal sur différents obstacles. De plus, la route inverse n'est pas nécessairement la même que la route directe. [9]
- **Sécurité limitée** : Compte tenu des contraintes précédentes, les méthodes de sécurité (chiffrement, etc.) sont réduites, ce qui augmente les risques d'attaques ou de piratage. En effet, les réseaux mobiles Ad-Hoc sont considérés comme très fragiles face aux attaques de toutes sortes. Lorsqu'une station transmet des données, tout appareil équipé d'un dispositif d'écoute (ici des cartes Wifi) a la possibilité d'intercepter ces données. Les pirates peuvent donc intercepter les données d'un utilisateur directement des antennes pirates (car les données circulent dans les airs) ou forcer une station à consommer une bonne partie de ses ressources énergétiques en l'inondant de toutes sortes de requêtes inutiles. [9]
- **Contraintes de bande passante** : Les réseaux sans fil sont basés sur le partage de supports de communication, de sorte que la bande passante réservée à un hôte sera relativement modeste. Cela implique des liaisons sans fil à haute capacité, variable. Pour les réseaux ad hoc, les messages seront cryptés. Nous avons également des clés « de groupe ». On sait que seules les stations en possession de la clé peuvent décrypter les messages.

Les mécanismes mis en place doivent permettre aux stations qui se sont déconnectées de pouvoir récupérer la ou les clés permettant le déchiffrement lors de leur reconnexion. [9]

- **Structure décentralisée** : Les réseaux Ad Hoc ne disposent pas d'une infrastructure centralisée, telle qu'un routeur ou une station de base, et permettent aux nœuds de communiquer directement entre eux.
- **Topologie dynamique** : Les réseaux Ad Hoc se caractérisent par une topologie de réseau en constante évolution à mesure que les nœuds se déplacent à l'intérieur et hors de portée les uns des autres. [7]
- **Communication multi-sauts** : les réseaux Ad Hoc reposent souvent sur une communication multi-sauts, où les données sont transmises d'un nœud à un autre avant d'atteindre leur destination finale.
- **Contraintes énergétiques** : Les réseaux ad hoc sont généralement composés de nœuds alimentés par batterie, de sorte que l'efficacité énergétique est une considération de conception essentielle. [7]

1.2.4 Réseau mobile ad hoc (MANET)

Le MANET se compose de plates-formes mobiles (par exemple, un routeur avec plusieurs hôtes et dispositifs de communication sans fil) – ici simplement appelés "nœuds" - qui sont libres de se déplacer arbitrairement. Les nœuds peuvent être situés dans ou sur des avions, des navires, des camions, des voitures, peut-être même sur des personnes ou de très petits appareils, et il peut y avoir plusieurs hôtes par routeur [10]. Un MANET est un système autonome de nœuds mobiles. Le système peut fonctionner de manière isolée ou peut avoir des passerelles et une interface avec un réseau fixe. Dans ce dernier mode de fonctionnement, il est généralement envisagé de fonctionner comme un réseau "stub" se connectant à un interréseau fixe [10]. Les réseaux de bout transportent le trafic provenant de et/ou à destination des nœuds internes, mais ne permettent pas au trafic exogène de « transiter » par le réseau de bout. Les nœuds MANET sont équipés d'émetteurs et de récepteurs sans fil utilisant des antennes qui peuvent être omnidirectionnelles (diffusion), hautement directionnelles (point à point), éventuellement orientables, ou une combinaison de celles-ci [10]. À un moment donné, en fonction des positions des nœuds et de leurs schémas de couverture d'émetteur et de récepteur, des niveaux de puissance de transmission et des niveaux d'interférence co-canal, une connectivité sans fil sous la forme d'un graphe aléatoire multisaut ou d'un réseau "ad hoc" existe entre les nœuds. Cette topologie ad hoc peut changer avec le temps lorsque les nœuds se déplacent ou ajustent leurs paramètres de transmission et de réception. [10]

Les MANET ont plusieurs caractéristiques saillantes :

1) **Topologies dynamiques** : Les nœuds sont libres de se déplacer arbitrairement ; ainsi, la topologie du réseau - qui est généralement multi-sauts - peut changer de manière aléatoire et rapide à des moments imprévisibles, et peut consister en des liaisons bidirectionnelles et unidirectionnelles [10].

2) **Liaisons à capacité variable et à bande passante restreinte** : Les liaisons sans fil continueront d'avoir une capacité nettement inférieure à celle de leurs homologues câblés. De plus, le débit réel des communications sans fil - après prise en compte des effets de l'accès multiple, des évanouissements, du bruit et des conditions d'interférence, etc. - est souvent bien inférieur au taux de transmission maximal d'une radio. L'un des effets des capacités de liaison relativement faibles à modérées est que la congestion est généralement la norme plutôt que l'exception, c'est-à-dire que la demande globale d'applications approchera ou dépassera probablement fréquemment la capacité du réseau. Comme le réseau mobile n'est souvent qu'une extension de l'infrastructure du réseau fixe, les utilisateurs mobiles ad hoc exigeront des services similaires. Ces demandes continueront d'augmenter à mesure que l'informatique multimédia et les applications de réseaux collaboratifs se développeront [10].

3) **Fonctionnement à énergie limitée** : Certains ou tous les nœuds d'un MANET peuvent dépendre de batteries ou d'autres moyens épuisables pour leur énergie. Pour ces nœuds, les critères de conception de système les plus importants pour l'optimisation peuvent être la conservation de l'énergie [10].

4) **Sécurité physique limitée** : Les réseaux sans fil mobiles sont généralement plus exposés aux menaces de sécurité physique que les réseaux câblés fixes. La possibilité accrue d'espionnage, d'usurpation d'identité et d'attaques par déni de service doit être soigneusement prise en compte. Les techniques de sécurité de liaison existantes sont souvent appliquées dans les réseaux sans fil pour réduire les menaces de sécurité. Comme avantage, la nature décentralisée du contrôle du réseau dans les MANET offre une robustesse supplémentaire contre les points de défaillance uniques des approches plus centralisées [10].

1.2.5 réseau ad hoc véhiculaire (VANET)

Le VANET est une sous-classe de Manet où les nœuds sont des véhicules. comme on peut le voir sur la figure 1.5 Les véhicules et les routes sont équipés de dispositifs de communication sans fil, d'unités embarquées (OBU) dans les véhicules, de nœuds fixes appelés unités routières (RSU) le long des routes.

La communication peut être dans trois scénarios : véhicule à véhicule (V2V) (entre OBU), véhicule à route (V2R) (entre OBU et RSU) et hybride (HVC) [11].

Les VANET sont appliqués dans l'industrie automobile, comme les systèmes de transport intelligents (ITS) pour assurer la sécurité routière, le confort de conduite et la diffusion d'informations. informations routières actualisées et véhicules autonomes.

Par exemple, en cas d'accident, les véhicules envoient des messages d'avertissement aux conducteurs pour qu'ils prennent les bonnes décisions avant d'entrer dans la zone de collision. et les conditions de circulation peuvent être communiquées pour faciliter la conduite en empruntant de nouveaux chemins en cas de congestion. [11]

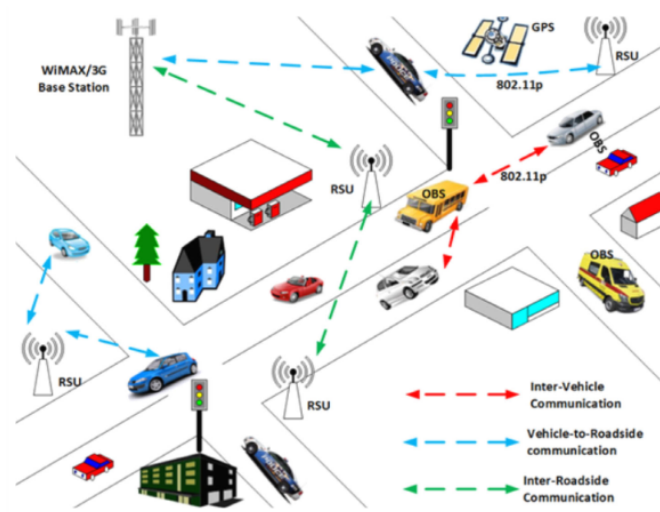


FIGURE 1.5 – un réseau vanet [11]

1.2.6 Réseaux ad hoc volants (FANET)

Le réseau volant ad hoc (FANET) est une branche de la mise en réseau qui assure la communication entre les nœuds volants, en particulier les véhicules aériens sans pilote (UAV), avec une station de base (BS). Les drones volants sont des nœuds autonomes capables de prendre des décisions (par exemple, changer de vitesse et de direction) dans les airs de manière distribuée plutôt que de recevoir des décisions prises depuis le sol de manière centralisée . FANET présente des caractéristiques distinctives par rapport aux réseaux ad hoc existants tels que les réseaux ad hoc mobiles (MANET) et les réseaux ad hoc véhiculaires (VANET). [12]

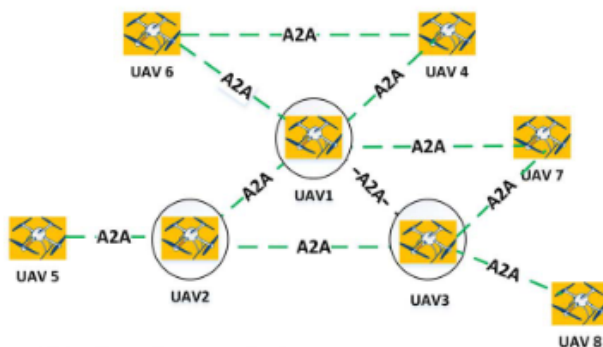


FIGURE 1.6 – un réseau fanet

1.2.7 Comparaison

nous pouvons voir la comparaison dans le tableau et l'image suivants :

network	manet	vanet	fanet
description	Les nœuds sans fil mobiles se connectent avec d'autres nœuds à portée de communication de manière ad hoc (aucune infrastructure centralisée requise)	Réseaux ad hoc dans lesquels les véhicules sont les nœuds mobiles. La communication se fait entre les véhicules et entre les véhicules et les unités en bord de route	Réseaux ad hoc ou basés sur une infrastructure de nœuds aéroportés. Communication entre drones et avec la station de contrôle
mobilité	Lent. Vitesses typiques 2 m/sec. Mouvement aléatoire. Densité variable, plus élevée dans certains endroits populaires.	Vitesse élevée, généralement 20 à 30 m/s sur les autoroutes, 6 à 10 m/s dans les zones urbaines. Prévisible, limité par le trafic routier et les règles de circulation	Vitesses de 0 à généralement aussi élevées que 100 m/s. Le mouvement peut être en 2 ou 3 dimensions, généralement contrôlé en fonction de la mission
topologie	Aléatoire, ad-hoc	étoile avec infrastructure en bord de route et ad-hoc parmi les véhicules	étoile avec centre de contrôle, ad-hoc/mesh parmi les UAV.

Changements de topologie	Dynamique - les nœuds se joignent et partent de manière imprévisible. Réseau sujet au partitionnement	Plus dynamique que les MANET. Mouvement linéaire. Cloisonnement commun	Stationnaire, lent ou rapide. Peut voler en essais contrôlés. Réseau sujet au partitionnement
Contrainte énergétique	La plupart des nœuds sont alimentés par batterie, l'énergie doit donc être conservée.	Les appareils peuvent être alimentés par batterie de voiture ou alimentés par leur propre batterie.	Les petits UAV sont limités en énergie. Les batteries affectent le poids et le temps de vol
Cas d'utilisation typique	-Diffusion d'informations (urgences, publicité, shopping, événements) Hotspots Internet	-informations sur le trafic et la météo, avertissements d'urgence, services basés sur la localisation - Infodivertissement -Systèmes de transport intelligents, -sécurité routière, -gestion du trafic, etc.	-Opérations de secours -Agriculture-récolte enquête -Recherche de la faune -Surveillance de plate-forme pétrolière

TABLEAU 1.1 – DESCRIPTION COMPARATIVE DES DIFFÉRENTS AD HOC RÉSEAUX [1]

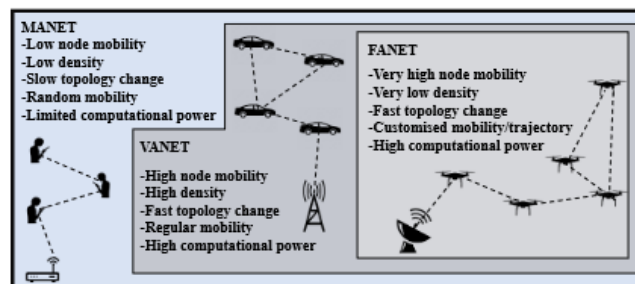


FIGURE 1.7 – MANET, VANET, and FANET relationships. [13]

1.3 FANET

1.3.1 Caractéristiques des réseaux FANET

voici les caractéristiques du fanet :

1. **Mobilité et topologie des nœuds** [12] : Les nœuds d'un réseau FANET ont une grande mobilité et peuvent changer rapidement d'emplacement. Cette grande mobilité rend les FANET différents des autres réseaux ad hoc tels que les MANET et les VANET. et cette grande mobilité conduit à une topologie de réseau dynamique et imprévisible. Cela rend difficile le maintien de la communication entre les nœuds.
2. **Densité de nœuds** : nombre de nœuds dans une zone spécifique du réseau. Dans les réseaux FANET, la densité de nœuds peut varier considérablement en fonction de l'environnement, de la mission et du scénario. [12]
3. **Modèle de propagation radio** : Le modèle de propagation radio utilisé dans les réseaux FANET peut avoir un impact considérable sur les performances du réseau. Ce modèle prend en compte l'altitude, l'environnement et d'autres facteurs pouvant affecter la transmission des signaux radio. [12]
4. **Consommation d'énergie et durée de vie du réseau** : La consommation d'énergie et la durée de vie du réseau sont des considérations importantes dans les réseaux FANET, car les nœuds sont généralement alimentés par des batteries. [12]
5. **Emplacement** : L'emplacement des nœuds dans un réseau FANET change constamment, ce qui rend difficile la maintenance d'informations réseau précises et la gestion efficace du réseau. [12]
6. **Bande de fréquence** : Les réseaux FANET fonctionnent généralement dans la bande de fréquence ISM (Industriel, Scientifique et Médical). Cependant, différentes bandes de fréquences peuvent être utilisées en fonction du scénario et des exigences spécifiques du réseau. [12]

1.3.2 Méthodes de communication dans FANET

il y a deux types de communication dans fanet :

- **Communication UAV à UAV** : Cela implique une communication directe entre les UAV dans le FANET. Cela permet aux UAV d'échanger des informations sur leur emplacement, leurs trajectoires de vol et d'autres données nécessaires à une coordination efficace et à un fonctionnement sûr. [6, 12]
- **Communication UAV vers infrastructure** : Cela implique la communication entre les UAV et l'infrastructure fixe, comme les stations au sol ou les stations de base. Cette communication permet aux drones de recevoir des informations sur leur environnement,

telles que les conditions météorologiques, les instructions du contrôle du trafic aérien et d'autres données pertinentes. De plus, il permet aux drones de transmettre des données à l'infrastructure, telles que des flux vidéo en temps réel et des lectures de capteurs. [6, 12]

1.3.3 Domaines d'application de FANET

il y a deux domaines à appliquer fanet :

1. Applications militaires :

- Renseignement électronique [6] : Collecte de signaux électroniques et interception des communications de l'ennemi.
- Brouillage et destruction du système radar : perturber les systèmes radar ennemis pour obtenir un avantage.
- Relais de signaux radio [6] : Relais de signaux radio dans des zones où la communication directe n'est pas possible.
- Observation des flottes ennemies [6] : Surveillance des mouvements ennemis et collecte de renseignements.
- Désignation et suivi des cibles [6] : Désignation et suivi des cibles pour les armes guidées ou les frappes aériennes.
- Élimination des bombes qui n'ont pas explosé [6] : Détection et destruction des bombes non explosées.
- Leurre de missiles par émission de signatures artificielles [6] : émission de faux signaux pour leurrer les missiles ennemis.

2. Demandes civiles :

- Pulvérisation agricole et surveillance et gestion agricole [6] : surveillance et pulvérisation des cultures avec des engrais, des pesticides et des herbicides.
- Recherche de pétrole et de gaz [6] : Prospection et recherche de gisements de pétrole et de gaz.
- Livraison de colis [6] : Livraison de colis dans des zones éloignées ou inaccessibles.
- Recherche et sauvetage [6] : Les UAV équipés de caméras, de capteurs et d'appareils de communication peuvent être utilisés pour localiser des personnes, des animaux ou des objets disparus dans des zones éloignées ou inaccessibles. [14]
- Surveillance du trafic et des zones urbaines : Les FANET peuvent être utilisés pour surveiller le flux de trafic, et fournir des mises à jour en temps réel aux centres de gestion du trafic. [14]
- Détection environnementale : Les drones peuvent être utilisés pour surveiller des facteurs environnementaux tels que la qualité de l'air, la température et l'humidité du sol. [14]
- Réseaux de relais : Les FANET peuvent être utilisés pour relayer les communications

entre les nœuds terrestres et aériens dans les zones où la communication directe n'est pas possible en raison d'obstacles physiques ou de limites de portée. [14]

- Surveillance : Les drones équipés de caméras et de capteurs peuvent être utilisés pour surveiller les activités dans des zones éloignées ou inaccessibles (peuvent être utilisés pour surveiller les importations illégales). [14]

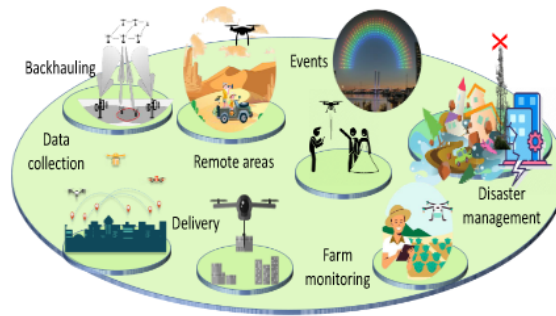


FIGURE 1.8 – le domaine de utilisation pour fanet [13]

1.3.4 Protocoles de routage FANet

Dans les réseaux FANET (Flying Ad Hoc Networks), divers protocoles sont utilisés à différentes couches de la pile réseau pour assurer la communication entre les UAV.

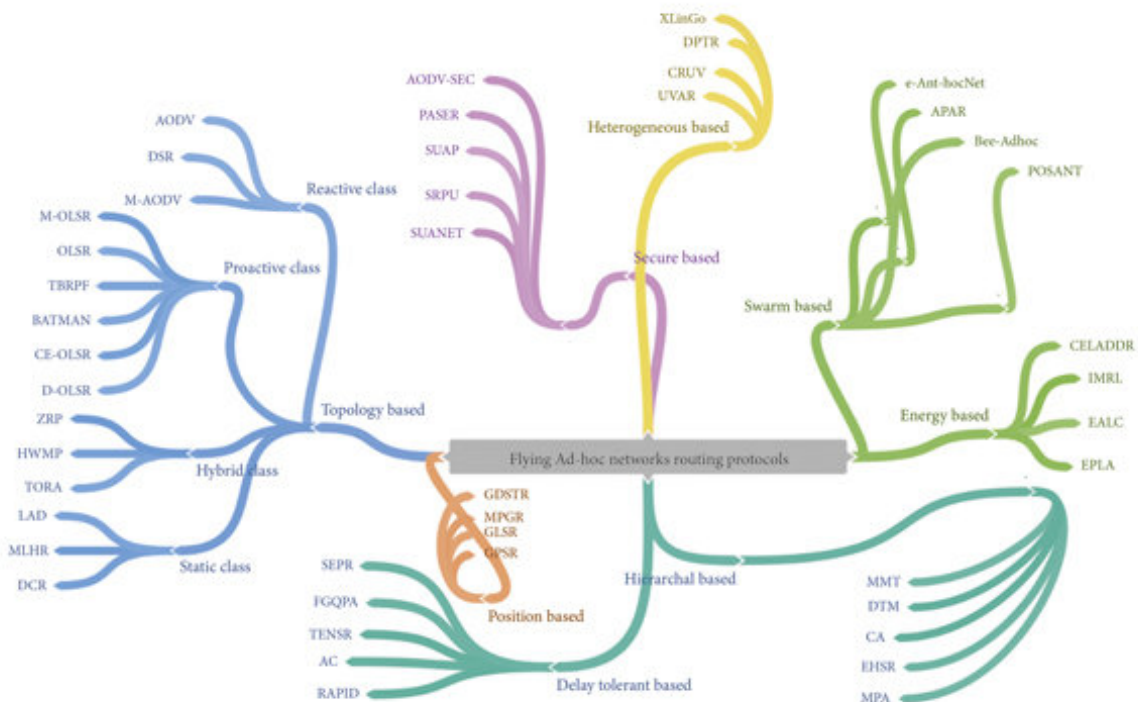


FIGURE 1.9 – Protocoles de routage pour fanet [15]

A. Protocoles de routage basés sur la topologie [12] :

- **Proactif [12] :** Stocke des informations sur tous les liens actuels entre les nœuds mobiles dans des tables de routage, permettant la sélection du chemin de routage le plus court. Cependant, ces protocoles génèrent une surcharge importante, consomment de la bande passante et réagissent lentement aux déconnexions.

- **Réactif [12] :** Lancer le processus de découverte d'itinéraire uniquement lorsqu'un UAV souhaite établir une communication, ce qui entraîne des retards et une surcharge élevés, en particulier dans les réseaux fragmentés.

- **Hybride [12] :** Combinez des protocoles proactifs et réactifs pour tirer parti de leurs avantages respectifs. La stratégie proactive est utilisée dans des zones spécifiques pour limiter les frais généraux, tandis que la stratégie réactive est utilisée entre les nœuds appartenant à différentes zones.

B. Protocoles de routage sécurisés [12] : Inclure des mécanismes de sécurité dans les protocoles de routage pour garantir la confidentialité, la confidentialité et la sécurité de la transmission des données, compte tenu des caractéristiques uniques des FANET.

C. Protocoles de routage bio-inspirés [12] : S'inspirer des comportements biologiques des insectes, tels que les abeilles, les fourmis ou les essaims de particules, pour résoudre divers problèmes de routage dans les FANET, en particulier pour établir des communications entre UAV.

D. Protocoles de routage basés sur la hiérarchie [12] : Utilisez des stratégies hiérarchiques en formant des clusters supervisés par des chefs de cluster (CH). Cette approche réduit le nombre de paquets transmis aux stations au sol et minimise la consommation d'énergie des drones. Cependant, la formation de clusters peut être complexe et les déconnexions fréquentes des liaisons ne sont pas bien prises en charge.

E. Protocoles de routage basés sur l'énergie [12] : Résoudre le problème de la consommation d'énergie déséquilibrée entre les UAV en tenant compte des niveaux d'énergie des UAV individuels lors de la sélection des chemins de routage. Les drones à faible énergie résiduelle sont épargnés de participer au routage de paquets, sauf cas exceptionnel.

F. Protocoles de routage hétérogènes [12] : Permettent un échange de données robuste entre les FANET et d'autres réseaux, tels que les MANET, les VANET ou les nœuds fixes. Cependant, seuls quelques protocoles de routage spécifiquement conçus pour les réseaux hétérogènes ont été proposés dans la littérature.

G. Protocoles de routage basés sur la position [12] :

- **Réactif [12] :** établissez des chemins de routage à la demande en fonction d'un processus de découverte lancé par les expéditeurs. Une récupération rapide et la recherche de chemins alternatifs sont cruciales en cas de déconnexion.

- **Greedy [12]** : Transfère les paquets de données aux UAV qui minimisent le nombre de sauts et la distance jusqu'à la destination, dans le but de réduire les délais de livraison. Cependant, la fiabilité du transfert gourmand diminue dans les FANET dynamiques.

- **Prédictif [12]** : Utiliser les mouvements prévisibles des UAV pour développer des protocoles de routage capables d'anticiper la durée des liaisons sans fil entre les UAV. La mise en œuvre de chemins de routage complets avec prédiction d'expiration de connectivité devient complexe, en particulier dans les FANET 3D.

H. **Réseaux tolérants aux retards [12]** : Dans les réseaux hautement fragmentés, les paquets sont transportés par des drones pour éviter toute perte jusqu'à ce que le réseau soit partiellement connecté. Diverses métriques et techniques sont employées pour déterminer la connectivité partielle.

1.3.5 Modèles de mobilité Fanet

On peut classer les modèles de mobilité en cinq classes :

- **Modèles de mobilité randomisés** : Les modèles de mobilité randomisés sont les modèles simples pour la recherche en réseau. Ils représentent plusieurs nœuds mobiles dont les actions sont complètement indépendants les uns des autres et des actions passées. où chaque nœud choisit au hasard une direction et une vitesse pour se déplacer pendant une certaine période. [14]

- **Modèles de mobilité dépendant du temps/de l'espace** : Cette catégorie de modèles de mobilité essaie d'éviter les changements brusques de vitesse et de direction. Le changement de mouvement en douceur peut être effectué à l'aide de différentes équations mathématiques. [14]

- **Modèles de mobilité planifiée** : Ces modèles de mobilité fournissent un schéma de trajet avec une forme prédéfinie. Les UAV suivent un schéma spécifique jusqu'à ce qu'ils arrivent au fin de celui-ci, et passer au hasard à un autre motif ou répéter le même. [14]

- **Modèles de mobilité de groupe** : Ces modèles incluent une contrainte spatiale entre tous les nœuds mobiles. [14]

- **Modèles de mobilité basés sur le contrôle de la topologie** : Lorsque certaines contraintes de réseau ou de mission doivent être satisfait en permanence, le modèle de mobilité a besoin d'un contrôle en temps réel de la topologie des nœuds mobiles. [14]

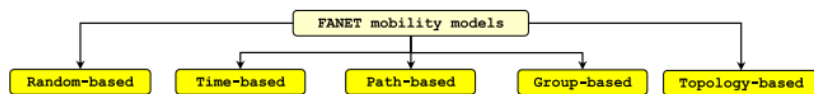


FIGURE 1.10 – modèles de mobilité pour fanet. [12]

1.4 Réseau tolérant aux retards (DTN)

1.4.1 Définition

Le DTN est un modèle conceptuel de réseau qui n'est pas spécifique à une couche de réseau particulière, mais qui s'applique à tous les réseaux qui nécessitent une tolérance au retard. La tolérance au retard fait référence à la capacité d'un protocole de réseau à maintenir la communication même dans des conditions extrêmes sans tomber en panne. Voici quelques-uns des scénarios extrêmes du DTN [2] :

- (1) La topologie globale du réseau est instable et une segmentation à long terme peut se produire [2] ;
- (2) Le canal de nœud entre les nœuds est instable et asymétrique [2] ;
- (3) Les capacités de traitement des nœuds sont différentes [2].

L'une des caractéristiques les plus importantes du DTN, en particulier dans les cas extrêmes, est l'instabilité de la topologie du réseau. La mise en œuvre du protocole TCP/IP suppose la présence d'un ou plusieurs liens de communication entre les nœuds source et destination pour une transmission réussie des paquets de données. Cependant, le DTN vise à relever le défi de la communication réseau lorsque ces liens de communication sont absents ou intermittents. Le DTN trouve de nombreuses applications dans les réseaux de communication d'urgence à la suite de catastrophes (par exemple, réseaux de transport, communication interplanétaire, réseaux de champ de bataille, tremblements de terre) et dans les zones éloignées à connectivité limitée (par exemple, communications régionales en réseau) [2].

Caractéristiques	DTN	Communication traditionnelle réseau
temps de survie	Nœuds avec un temps de survie court	Ne pas considérer le problème du temps de survie
Rapport d'espace	Réduire le ratio d'espace pour prolonger le temps de travail des nœuds	Le plus gros le meilleur
Capacité de stockage	Forte demande de fonction de stockage et mémoire supplémentaire requise pour les longues files d'attente	Mémoire et cache, faible besoin en mémoire

TABLEAU 1.2 – Comparaison entre le DTN et les nœuds de réseau de communication traditionnels [2]

1.4.2 Caractéristiques DTN

En raison des différents environnements applicables aux réseaux de communication traditionnels, DTN présente les caractéristiques suivantes :

(1) **L'incertitude du délai du réseau [2]** : La topologie du réseau de DTN est dynamique et le support de transmission est relativement spécial. Par conséquent, le délai du réseau est incertain.

Par exemple, dans les communications interstellaires et dans un réseau de modems acoustiques sous-marins, le délai de transmission est long.

(2) **Connexion instable [2]** : Dans le réseau DTN, la connexion des liens est fréquente. La mobilité des nœuds entraîne une déconnexion entre les nœuds.

(3) **Longue file d'attente [2]** : Les liaisons du réseau DTN sont fréquemment déconnectées. Pour avoir une communication normale, le nœud doit sauvegarder les données pendant une longue période afin d'éviter de les perdre. Le temps d'attente du nœud est donc fondamentalement imprévisible. Il peut parfois atteindre plusieurs heures, voire plusieurs jours.

(4) **Le taux élevé d'erreurs de transmission de données et d'erreurs [2]** : plus grande probabilité de perte de paquets et transmission de données plus instable que les réseaux de communication traditionnels dans le DTN en raison des changements dynamiques dans la topologie du réseau et des déplacements fréquents des nœuds.

(5) **Débit de transmission de liaison asymétrique [2]** : Dans le DTN, la liaison

de communication entre les nœuds peut être très différente, de même que les débits de transmission de données en liaison montante et descendante, même s'il existe une certaine liaison de communication entre les deux nœuds déterminés. Il existe également une liaison de communication de données à sens unique.

1.4.3 Routage dans un DTN

Problème de routage DTN [2] : Le DTN est soumis à des conditions extrêmes qui entraînent davantage de problèmes de routage que les réseaux de communication traditionnels. Ces problèmes sont les suivants :

1) Connexion des nœuds [2] : Le délai de communication de bout en bout comprend divers facteurs tels que les délais d'attente, de mise en file d'attente, de propagation et de transmission. Parmi ces facteurs, le délai d'attente est particulièrement critique, car il dure souvent plusieurs secondes, voire plusieurs jours, ce qui entraîne des retards dans les connexions entre les nœuds.

2) Performance des nœuds [2] : Les nœuds d'un réseau DTN utilisent un "stockage-transport-transfert" pour le transfert de données. Lorsqu'une liaison est coupée, le nœud stocke les données jusqu'à ce qu'une connexion soit établie. Toutefois, si le volume de données dépasse la capacité de stockage du nœud, il y a débordement des données, ce qui entraîne une perte d'informations.

La conception des algorithmes de routage DTN doit prendre en compte plusieurs facteurs, notamment le taux de changement dynamique de la topologie du réseau, la capacité des liens de communication, la capacité de la mémoire cache des nœuds et le volume moyen du trafic entre les nœuds [2].

algorithme de routage basé sur la répllication [2] : Les nœuds du réseau répliquent et relaient les messages en copiant les informations lorsqu'ils se rencontrent. Par conséquent, un grand nombre de répliques de messages circulent dans le réseau, ce qui consomme d'importantes ressources. Parmi les exemples de cet algorithme, on peut citer les méthodes epidemic et les méthodes de spray and wait.

Algorithme de routage basé sur la transmission [2] : L'algorithme de routage basé sur la politique de transmission est également appelé algorithme de routage basé sur la connaissance préalable. Les nœuds sélectionnent un chemin de transmission optimal basé sur des critères spécifiques en utilisant des informations sur les changements dynamiques dans la topologie du réseau. Un exemple de cet algorithme est la méthode du prophète.

1.5 Conclusion

En conclusion, le domaine de Delay Tolerant Fanet a fait des progrès significatifs ces dernières années, avec de nombreuses avancées dans la technologie, les protocoles et les algorithmes. Dans le chapitre état de l'art dans ce domaine, nous donnons un aperçu complet des avancées actuelles et soulignons le potentiel de cette technologie pour permettre la communication dans des environnements difficiles. Alors que la demande de solutions de communication robustes et fiables continue de croître, ce chapitre était destiné à fournir une base solide pour notre prochain chapitre où nous discuterons plus en profondeur des protocoles de routage DTN.

Chapitre 2

Étude comparative et proposition de nouvelle méthode

2.1 Introduction

Dans ce chapitre, nous examinons les protocoles de routage DTN, qui sont des protocoles conçus là où il n'y a pas de connexions directes et continues permanentes entre les nœuds. ces protocoles permettent ensuite la communication en utilisant une approche opportuniste de stockage et de retransmission.

Ce chapitre vise à comparer et à évaluer les performances de trois protocoles de routage populaires pour les FANET dans DTN : Epidemic, Spray and Wait et Prophet. L'objectif est d'évaluer les performances de ces protocoles de routage dans différents scénarios de réseau, tels que la densité du réseau. L'étude utilisera des expériences basées sur la simulation pour évaluer les protocoles.

et nous présentons notre contribution, le nouveau protocole qui est une hybridation de spray et wait and prophet, puisqu'ils sont tous les deux efficaces en termes de délai et de taux de livraison.

2.1.1 Epidemic

Le routage epidemic [16] est une technique couramment utilisée dans les réseaux tolérants aux délais (DTN) pour acheminer des messages vers des destinations arbitraires avec un minimum d'hypothèses sur la topologie et la connectivité du réseau sous-jacent. Le protocole repose sur la distribution transitive des messages à travers le réseau, les messages atteignant finalement leur destination. Le principe de fonctionnement de base de ce schéma de routage est d'initialiser un message et de le mettre en file d'attente dans une

mémoire tampon, d'attribuer un identifiant de message unique de 32 bits, puis d'échanger la liste des identifiants de message sous forme de vecteur récapitulatif lorsque deux nœuds entrent dans la portée de communication.

Chaque nœud maintient un tampon composé de messages qu'il a émis ainsi que de messages qu'il met en mémoire tampon pour le compte d'autres nœuds. Chaque nœud stocke un vecteur de bits, appelé vecteur récapitulatif, qui indique quelles entrées de leurs tables de hachage locales sont définies. Pendant l'anti-entropie, les deux nœuds échangent leurs vecteurs de résumé pour déterminer quels messages stockés à distance n'ont pas été vus par le nœud local. À son tour, chaque nœud demande alors des copies de messages qu'il n'a pas encore vus. comme présenté dans la figure 2.1 ci-dessous.

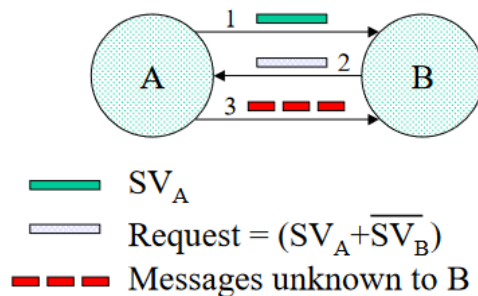


FIGURE 2.1 – Epidemic for Hosts A and B within Communication Range [16]

Le protocole associe également un nombre de sauts à chaque message, qui détermine le nombre maximal d'échanges épidémiques auxquels un message particulier est soumis. Alors que le nombre de sauts est similaire au champ TTL dans les paquets IP, les messages avec un nombre de sauts de un ne seront livrés qu'à leur destination finale. Des valeurs plus élevées pour le nombre de sauts distribueront un message plus rapidement sur le réseau, mais augmenteront également la consommation totale de ressources dans la livraison des messages. Chaque nœud maintient une taille de file d'attente maximale associée à sa mémoire tampon pour garantir une utilisation efficace des ressources.

L'un des avantages est qu'il tire parti de la localité physique des nœuds, ce qui signifie que les messages sont transmis de manière opportuniste en fonction de la proximité des nœuds lors des événements de contact. Cela permet des mouvements non aléatoires et aléatoires des nœuds, ce qui le rend adapté à une variété de scénarios où la connectivité réseau peut être intermittente ou imprévisible.

2.1.2 Spray and wait

Spray and Wait est un protocole conçu pour diffuser efficacement des messages dans des réseaux déconnectés, où les nœuds se déplacent de manière aléatoire et les liens de

communication ne sont pas fiables. Spray and Wait Routing est une stratégie de routage qui implique deux phases pour les nœuds L [17] :

1. Phase de pulvérisation : la première phase consiste à diffuser L copies d'un message provenant d'un nœud source vers L différents relais, la source et les autres nœuds retransmettant potentiellement les copies du message.

2. Phase d'attente : La deuxième phase, appelée phase d'attente, entre en jeu si la destination n'est pas localisée lors de la première phase. Dans cette phase, chacun des nœuds L qui possède une copie du message le transmet directement au destinataire prévu.

La propagation des L copies peut se faire en utilisant différentes techniques, telles que le Source Spray and Wait, où le nœud source transmet toutes les L copies aux L premiers nœuds distincts qu'il rencontre, ou le Binary Spray and Wait comme indiqué dans le figure ci-dessous 2.2, où les nœuds qui ont plusieurs copies les divisent en deux et en remettent la moitié à un autre nœud qui n'a pas de copies.

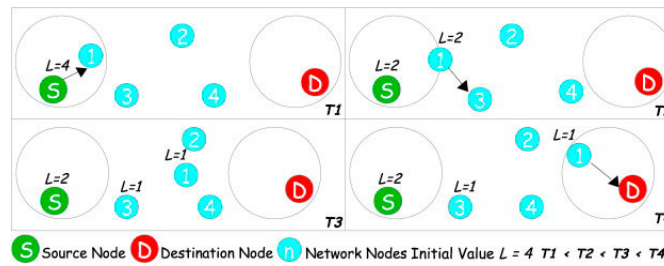


FIGURE 2.2 – binary spray and wait exemple [18]

2.1.3 Prophet

PROPHET [19] est un protocole de routage probabiliste qui vise à améliorer les performances de routage en tenant compte du caractère non aléatoire de la mobilité dans les réseaux ad hoc. Pour y parvenir, PROPHET établit une métrique probabiliste appelée prévisibilité de livraison, notée $P(a, b) \in [0, 1]$, à chaque nœud a pour chaque destination connue b. Cette métrique indique la probabilité qu'un nœud puisse livrer un message à une destination spécifique. et est calculé pour chaque nœud a par rapport à chaque nœud connu a. Plus la valeur de $P(a, b)$ pour une destination spécifique est élevée, meilleur est le candidat pour que le nœud a livre le paquet à cette destination b.

Lorsque deux nœuds se rencontrent, ils échangent des vecteurs récapitulatifs et un vecteur de prévisibilité de livraison contenant les informations de prévisibilité de livraison pour des destinations connues. Ces informations supplémentaires sont utilisées pour mettre à jour le vecteur de prévisibilité des livraisons internes à l'aide des équations suivantes :

1. Calcul de la prévisibilité de livraison :

$$P(a, b) = P(a, b)_{\text{old}} + (1 - P(a, b)_{\text{old}}) \cdot P_{\text{init}}$$

Cette équation met à jour la métrique de prévisibilité de livraison lorsqu'un nœud est rencontré. P_{init} est une constante d'initialisation et $P(a, b)_{\text{old}}$ est l'ancienne valeur de la métrique.

2. Équation de vieillissement :

$$P(a, b) = P(a, b)_{\text{old}} \cdot \gamma^k$$

Cette équation réduit la valeur de prévisibilité de la livraison pour une destination lorsque deux nœuds ne se rencontrent pas pendant un certain temps. γ est la constante de vieillissement et k est le nombre d'unités de temps qui se sont écoulées depuis le dernier vieillissement de la métrique.

3. Équation de transitivité :

$$P(a, c) = P(a, c)_{\text{old}} + (1 - P(a, c)_{\text{old}}) \cdot P(a, b) \cdot P(b, c) \cdot \beta$$

Cette équation utilise la propriété transitive de la métrique de prévisibilité de livraison. Si le nœud A rencontre fréquemment le nœud B et que le nœud B rencontre fréquemment le nœud C, alors le nœud C est probablement un bon nœud pour transmettre les messages destinés au nœud A. β est une constante de mise à l'échelle qui détermine l'impact de la transitivité sur la métrique de prévisibilité de livraison.

Le premier nœud ne supprime pas le message après l'avoir envoyé tant qu'il y a suffisamment d'espace tampon disponible. Si les tampons sont pleins lorsqu'un nouveau message est reçu, un message doit être supprimé selon le système de gestion de file d'attente utilisé (c'est-à-dire FIFO).

Le scénario de la figure 2.3 illustre la prévisibilité de livraison de PRoPHET et son fonctionnement, où le nœud A veut envoyer un message au nœud D. Les nœuds C et D se rencontrent fréquemment, ce qui rend leurs valeurs de prévisibilité de livraison élevées. Le nœud C rencontre également souvent le nœud B, ce qui augmente leurs valeurs de prévisibilité les unes pour les autres et pour D via la transitivité. Le nœud B rencontre ensuite A, reçoit le message et met à jour ses valeurs de prévisibilité de livraison. Enfin, A transmet le message à B, qui a des valeurs de prévisibilité plus élevées pour D et peut transmettre le message de manière plus fiable.

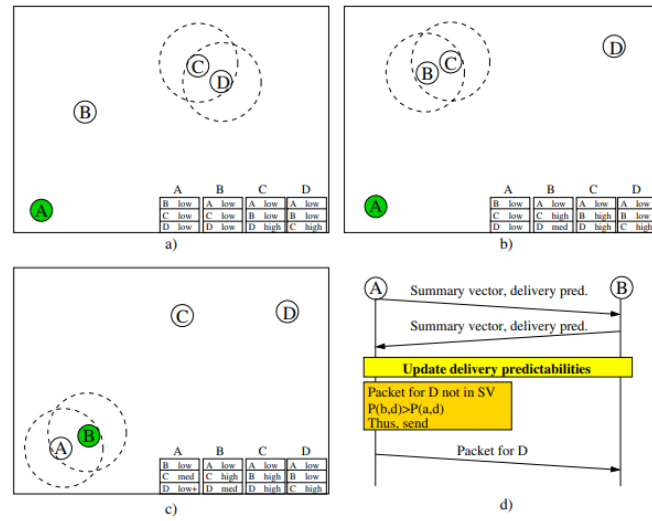


FIGURE 2.3 – prophet exemple [19]

2.1.4 Comparaison des protocoles

En ce qui concerne les protocoles de routage pour les réseaux FANET (Flying Ad-Hoc Networks), Epidemic, Spray and Wait et Prophet sont trois choix populaires. Chaque protocole a ses propres forces et faiblesses, ce qui les rend adaptés à différents scénarios dans les FANET. Dans cette comparaison, nous comparerons ces protocoles dans divers domaines en fonction de leurs performances dans les scénarios FANET.

Efficacité de la livraison des messages :

Epidemic : En raison de la réplification des messages vers tous les nœuds voisins, Epidemic peut assurer une livraison fiable des messages vers tous les nœuds du réseau. Cependant, il souffre d'une surcharge de réseau élevée et d'un retard de livraison.

Spray and Wait : Spray and Wait peut transmettre efficacement des messages dans des réseaux déconnectés avec une faible surcharge de communication. Cependant, dans les réseaux à haute densité, il peut souffrir d'un retard de livraison des messages élevé en raison du temps d'attente.

Prophet : L'approche basée sur l'apprentissage par renforcement de Prophet lui permet d'optimiser la diffusion des messages en fonction des expériences passées, ce qui le rend efficace et adaptable aux changements du réseau. Cependant, il peut souffrir d'une surcharge de calcul élevée et ne pas fonctionner correctement dans les réseaux hautement dynamiques.

Résilience à la dynamique du réseau :

Epidemic : Epidemic est résilient aux dynamiques de réseau telles que la mobilité élevée des nœuds et la connectivité intermittente, ce qui le rend adapté aux scénarios

FANET hautement dynamiques.

Spray and Wait : Spray and Wait peut gérer des réseaux déconnectés et une mobilité élevée des nœuds, ce qui le rend adapté aux scénarios avec une densité de nœuds faible à modérée.

Prophet : L'approche adaptative de Prophet lui permet de gérer les modifications du réseau et des modèles de trafic, ce qui le rend adapté aux scénarios FANET modérés à hautement dynamiques.

Frais généraux de communication :

Epidemic : En raison de la réplication des messages vers tous les nœuds voisins, Epidemic a une surcharge de communication élevée, qui peut ne pas convenir aux grands FANET.

Spray and Wait : Spray and Wait a un faible temps système de communication, car seul un sous-ensemble de nœuds est impliqué dans le processus de diffusion des messages. Cependant, dans les réseaux à haute densité, le protocole peut souffrir d'une surcharge de communication élevée en raison du grand nombre de messages retenus.

Prophet : Prophet peut nécessiter des ressources de calcul importantes pour maintenir les scores de qualité de chaque voisin, ce qui peut limiter son évolutivité dans les grands FANET.

Complexité :

Epidemic : Epidemic est un protocole simple et direct qui ne nécessite aucune connaissance préalable de la topologie du réseau ou de l'emplacement du nœud de destination.

spray and wait : Spray and wait est également un protocole simple, mais il nécessite le réglage de paramètres tels que le paramètre de pulvérisation et le temps d'attente.

Prophet : Prophet est un protocole plus complexe qui nécessite l'utilisation d'algorithmes d'apprentissage par renforcement pour optimiser la livraison des messages.

Chaque protocole a ses propres avantages et limites, et le choix du protocole dépend du scénario et des exigences FANET spécifiques. Epidemic convient aux scénarios hautement dynamiques avec une faible surcharge de communication, tandis que Spray and Wait convient aux scénarios avec une densité de nœuds faible à modérée et des réseaux déconnectés. Prophet convient aux scénarios modérés à hautement dynamiques qui nécessitent un routage adaptatif basé sur les expériences passées.

protocole	route	densité	complexité	avantage	inconvenient
Epidemic	Réplication sur tous les noeuds voisins	Haut	faible	Résilient à la dynamique du réseau, livraison fiable des messages à tous les nœuds	Surcoût de communication élevé, retard de livraison élevé
Spray and Wait	Pulvériser un message à un sous-ensemble de nœuds, attendre le nœud destinataire	Faible à modéré	Faible	Livraison efficace dans les réseaux déconnectés, faible surcharge de communication	Délai de livraison des messages élevé dans les réseaux à haute densité
Prophet	Prophète Sélectionne l'itinéraire le plus approprié en fonction des expériences passées en utilisant l'apprentissage par renforcement	Modéré à élevé	Haut	Adaptation aux évolutions du réseau, livraison efficace et optimisée des messages	Surcharge de calcul élevée, peut ne pas bien fonctionner dans les réseaux hautement dynamiques

TABLEAU 2.1 – Etude comparative des protocoles de routage DTN

2.2 Notre contribution

2.2.1 Principe de fonctionnement

Nous proposons l'hybridation des protocoles de routage Spray and Wait et Prophet afin de pouvoir mettre et combiner les points forts des deux protocoles pour obtenir les meilleures performances en termes de livraison et de délai des messages.

L'approche Spray and Wait est que les nœuds transmettent L copies de messages aux premiers nœuds qu'ils rencontrent, puis les nœuds avec les copies attendent une rencontre avec le nœud de destination afin qu'ils puissent lui transmettre le message.

L'approche de prophet est que les nœuds calculent les probabilités en fonction de leur taux de rencontre avec d'autres nœuds du réseau et lorsqu'ils envoient un message, ils l'envoient au nœud avec un taux de rencontre le plus élevé avec la destination, c'est pour maximiser le taux de livraison du message.

Pour hybrider ces deux protocoles, nous pouvons commencer par une approche de pulvérisation binaire où un nœud pulvérise le message aux premiers nœuds qu'il rencontre, que le nœud connaisse mieux la destination ou non.. le message commence par un nombre L que nous avons défini comme 10 et à chaque pulvérisation le L sera divisé par 2 jusqu'à ce qu'il soit inférieur à 2.

Une fois que le message a atteint un nombre L inférieur à 2, le nœud peut maintenant passer à l'utilisation de Prophet pour livrer le message à la destination. En effet, la probabilité de rencontrer des nœuds plus proches de la destination est plus élevée et Prophet peut utiliser ces informations pour améliorer le taux de réussite de la livraison.

2.2.2 Pseudo code

voici le pseudo code :

Algorithme 2.1 : Our Contribution Routing Algorithm

```

Function UpdateDeliveryPredictability( $a, b$ )
   $P [a,b] \leftarrow Pold [a,b] + (1 - Pold [a,b]) \times Pinit$ 

Function UpdateDeliveryPredictabilityTable( $a, b, c$ )
   $P [a,c] \leftarrow Pold [a,c] + (1 - Pold [a,c]) \times P [a,b] \times P [b,c] \times beta$ 

Function CheckCache( $a, b$ )
  for each message j in Cache do
     $c = Cache [j].destination;$ 
    if  $b = c$  then
       $\lfloor$  Transfer data Cache [j] to b and remove it ;
    else
      if  $P [b,c] > P [a,c]$  or  $Cache [j].L \geq 2$  then
         $\lfloor$  Transfer data Cache [j] of a to node b with L/2;

Pinit  $\leftarrow$  Initialization constant;
gamma  $\leftarrow$  Aging constant;
beta  $\leftarrow$  Scaling constant;
Initialize Cache as an empty cache;

foreach message from application layer do
   $\lfloor$  add message to Cache with duplication = L;

foreach meeting between nodes a and b do
  UpdateDeliveryPredictability ( $a, b$ );
  exchange Delivery Predictability Table;
  foreach node c do
     $\lfloor$  UpdateDeliveryPredictabilityTable ( $a, b, c$ )
  CheckCache ( $a, b$ ) ; // Check cache for data transfer

foreach time unit do
  foreach known node b do
     $\lfloor$   $P [a,b] \leftarrow P [a,b] \times gamma$ 

```

2.3 Conclusion

En conclusion, Dans ce chapitre, nous avons discuté de trois protocoles de routage - Epidemic, Spray and Wait et Prophet - pour les FANET. Nous avons comparé ces protocoles en termes d'efficacité de livraison des messages, de résilience à la dynamique

du réseau, de surcharge de communication et de complexité dans divers scénarios FANET.

De notre analyse, nous pouvons conclure que chaque protocole a ses propres forces et faiblesses, et le choix du protocole dépend du scénario et des exigences FANET spécifiques. Epidemic convient aux scénarios hautement dynamiques avec une faible surcharge de communication, tandis que Spray and Wait convient aux scénarios avec une densité de nœuds faible à modérée et des réseaux déconnectés. Prophet convient aux scénarios modérés à hautement dynamiques qui nécessitent un routage adaptatif basé sur les expériences passées.

Et nous avons présenté notre contribution qui est l'hybridation de Spray et Wait et Prophet dans le chapitre suivant, nous simulerons toute les protocoles et présenterons les résultats.

Chapitre 3

La simulation et discussion de résultat

3.1 Introduction

Dans ce chapitre, nous montrerons les outils utilisés pour la simulation ainsi que les paramètres de la simulation suivis des résultats et de leur discussion.

3.2 La simulation

La simulation informatique, est un processus dans lequel un ordinateur calcule le comportement d'un phénomène physique. Il crée un modèle virtuel du phénomène et utilise des équations mathématiques pour prédire ce qui se passerait dans le monde réel. La simulation peut produire des données, des images ou des vidéos qui montrent ce qui se passerait.

Les simulations numériques peuvent représenter des phénomènes physiques complexes qui sont décrits par des équations mathématiques, telles que la simulation de réseau sont utilisées pour évaluer les performances comme nous le faisons dans ce chapitre.

3.3 Outils de simulation

Pour simuler nous avons utilisé les outils suivants :

3.3.1 Omnet++

OMNeT++ est une bibliothèque et un framework de simulation C++ utilisés pour créer des simulateurs de réseau, y compris des réseaux de communication câblés et sans fil, des réseaux de file d'attente, etc. [20]. Il fournit des fonctionnalités spécifiques à un

domaine pour des éléments tels que les réseaux de capteurs, les protocoles Internet et les réseaux photoniques [21]. Il est open source et est livré avec un IDE basé sur Eclipse, un runtime graphique et d'autres outils [20]. La Plateforme de Simulation Omnet++ offre d'avantages. Il est facile à utiliser et fournit un ensemble complet d'outils pour créer et exécuter des simulations. Il est également open source et est disponible gratuitement.

3.3.2 Inet Framework

INET Framework est un outil gratuit qui fonctionne avec l'environnement de simulation OMNeT++ [21]. Il propose des protocoles, des agents et d'autres modèles prédéfinis pour aider les chercheurs et les étudiants à étudier les réseaux de communication [21]. Il est particulièrement utile pour tester de nouveaux protocoles et tester différents scénarios [21].

3.3.3 OPS Framework

OPS est un ensemble de modèles de simulation dans OMNeT++ pour la simulation de réseaux opportunistes pour MANet [22]. Il a une architecture modulaire où différents protocoles pertinents pour les réseaux opportunistes peuvent être développés et connectés et configurés pour évaluer leurs performances [22]. Les modèles d'OPS sont regroupés en couches de protocole d'une pile de protocoles [22].

3.3.4 Fonctionnalités de Omnet++

Avec Omnet++, vous pouvez créer des simulations à l'aide d'une interface utilisateur graphique dans laquelle vous pouvez ajouter et configurer des composants. Il fournit également une bibliothèque de composants et d'outils prédéfinis pour le débogage des simulations [23].

Vous pouvez également afficher les résultats de la simulation sous forme graphique et tabulaire, ainsi que consulter l'état de la simulation à tout moment. [23].

OMNeT++ a deux fichiers principaux :

Le fichier ned : Le fichier ned utilise le langage de description de réseau NED pour décrire les paramètres et les ports du module [24]. Il a deux modes : le mode graphique et le mode source. [24].

Le fichier ini : est lié au fichier ned et est utilisé pour initialiser les paramètres du module et la topologie du réseau [24].

3.4 Comparaison entre les autres outils de simulation

Dans le tableau suivant 3.1, nous voyons que OMNeT++ avec le cadre OPS est la meilleure option pour simuler les réseaux DTN.

TABLEAU 3.1 – Comparaison de haut niveau entre les simulateurs OppNets

Outil	Adyton	ONE	OMNeT++	ns-3
Plateformes	Linux	Java (JDK 6+)	Win, Linux, Mac	Linux, Mac, FreeBSD
Langage de programmation	C++	Java	C++, NED	C++, Python
Parallélisation	-	-	+	o
Documentation	+	+	++	+
Listes de diffusion et tutoriels	o	++	++	+
Interface utilisateur	-	+	++	-
Modèles de mobilité	o	+	++ (OPS)	o
Technologies de liaison	-	-	+ (OPS)	+
Propagation des données OppNets	++	++	+	o
Modèles de comportement des utilisateurs	-	-	+ (OPS)	-
Modèles de trafic	++	++	++ (OPS)	++
Évolutivité	+	-	+	o

- pas de soutien, o soutien partiel, + soutien adéquat, ++ très bon soutien

3.5 Paramètres de simulation

dans cette section nous avons présente les différent parametre de simulation :

3.5.1 Modèle de mobilité

Le modèle de mobilité de Gauss-Markov est un modèle mathématique permettant de simuler le mouvement des nœuds du réseau. Le modèle est un modèle basé sur la mémoire avec un seul paramètre de réglage alpha α , qui contrôle la quantité de mémoire

et la variabilité du mouvement des nœuds. Les trois principaux paramètres utilisés dans le modèle sont la vitesse, la direction et le temps de séjour. Le modèle suppose que les nœuds sont initialement placés au hasard dans l'espace virtuel et se déplacent indépendamment les uns des autres [25–27].

En deux dimensions, tous les nœuds se voient attribuer une vitesse et une direction initiales, une vitesse et une direction moyennes. À des intervalles de temps définis, pour chaque nœud, calculez une nouvelle vitesse et direction en fonction des valeurs précédentes, de la vitesse et de la direction moyennes et des variables aléatoires dans une distribution gaussienne. Le modèle peut être étendu pour fonctionner en trois dimensions en ajoutant une variable de pas pour suivre le mouvement vertical des nœuds. [27]

Pour simuler le mouvement des nœuds 3D à l'aide de l'algorithme de Gauss-Markov, nous ajoutons une troisième variable pour suivre le pas vertical aux variables de vitesse et de direction du modèle 2D. [27]

$$\begin{aligned} s_n &= \alpha s_{n-1} + (1 - \alpha)\bar{s} + \sqrt{(1 - \alpha^2)}s_{x_{n-1}} \\ p_n &= \alpha p_{n-1} + (1 - \alpha)\bar{p} + \sqrt{(1 - \alpha^2)}p_{x_{n-1}} \\ d_n &= \alpha d_{n-1} + (1 - \alpha)\bar{d} + \sqrt{(1 - \alpha^2)}d_{x_{n-1}} \end{aligned}$$

Car ces variables représentent avec précision le mouvement du nœud tout en gardant le modèle simple. Nous n'avons pas besoin de considérer les commandes de vol telles que les gouvernails, les volets, etc. Les variables de direction et de pas représentent les angles auxquels l'avion se déplace. [27]

Après calcul de ces variables, l'algorithme détermine un nouveau vecteur vitesse [27] :

$$\begin{aligned} v_x &= s_n \cos d_n \cos p_n \\ v_y &= s_n \sin d_n \cos p_n \\ v_z &= s_n \sin p_n \end{aligned}$$

Le modèle de Gauss-Markov est considéré comme l'un des modèles classiques et bien maîtrisés dans l'analyse des données statistiques. Il est utilisé dans de nombreux domaines de la recherche scientifique, ce qui garantit précision et fiabilité des analyses et prédictions.

3.5.2 Scénarios de simulation

Dans notre simulation nous avons changé le nombre de nœuds a chaque fois. voici les tableaux 3.2, 3.3 et 3.4 des paramètres de la simulation :

Paramètre	valeur
numéro de nœud	20-100
zone	1000*1000*1000
mobilité	gauss-markov
vitesse	10mps-20mps
temps de simulation	10min
données Taille	10000 bytes
données Intervalle de génération	1s
Taille maximale du cache	5 MB
Intervalle anti entropie	300s
Nombre maximal de sauts	25
Portée sans fil	30m
Largeur de bande	100 Kbps
Taille de l'en-tête sans fil	16byte

TABLEAU 3.2 – Paramètres de simulation

Paramètre	valeur
Type de spray	binary
nombre de doublons	4

TABLEAU 3.3 – Paramètres de spray and wait

Paramètre	valeur
Pinit	0.5
beta	0.9
gamma	0.998
Intervalle de temps standard	3600s

TABLEAU 3.4 – Paramètres de prophet

3.6 Résultats de simulation

nous avons obtenu des résultats pour le taux de livraison, le délai, l'utilisation du cache, le nombre de sauts, la duplication reçue, le total des données envoyées, la overhead et l'énergie pour tous les protocoles avec une variation du nombre de nœuds.

3.6.1 l'influence du nombre de nœuds dans le données envoyé moyen

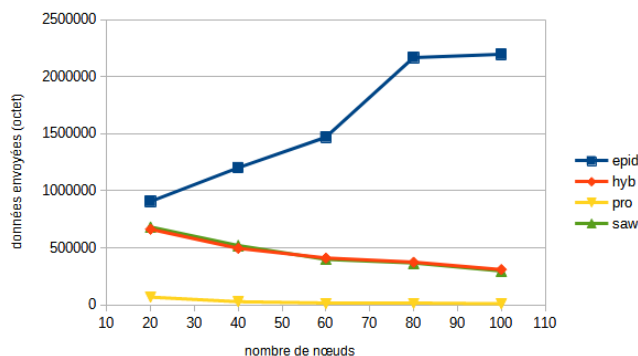


FIGURE 3.1 – data envoyé moyen par rapport nombre de nœuds

Dans le figure 3.1, nous remarquons que les données envoyées par chaque protocole, nous voyons que epidemic est élevé en raison de sa technique d'inondation et qu'il augmente avec la densité, car avec plus de densité, il y aura plus de rencontres entre les nœuds, ce qui signifie que plus de données sont envoyées. et nos protocoles viennent en deuxième position et comme spray and wait parce que le nombre de duplications est de 4. puis prophet en raison de sa technique de transmission.

3.6.2 l'influence du nombre de nœuds dans le taux de livraison moyen

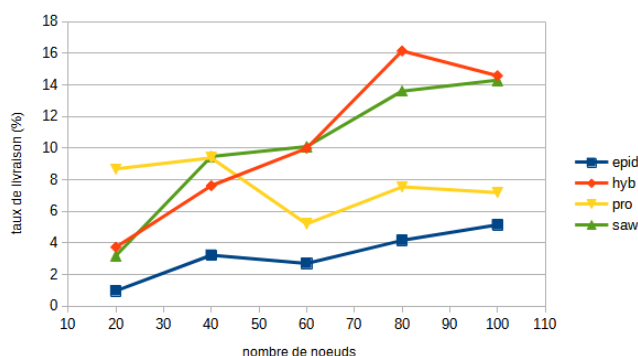


FIGURE 3.2 – taux de livraison moyen par rapport nombre de nœuds

Dans le figure 3.2, nous remarquons que le taux de livraison par chaque protocole, nous voyons que l'epidemic est faible. et spray and wait de plus taux de livraison en plus avec la densité en raison des copies limitées et plus de densité est plus de connectivité.

puis prophet qui préforme mieux avec des densités plus faibles. et notre protocole avec modéré en faible densité et le meilleur avec des densités élevées.

3.6.3 l'influence du nombre de nœuds dans le retard moyen

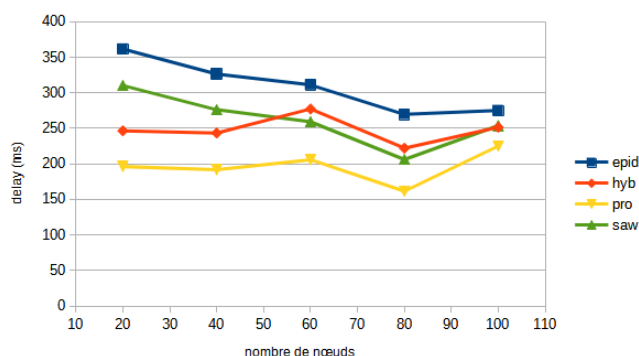


FIGURE 3.3 – retard moyen par rapport nombre de nœuds

Dans le figure 3.3, nous remarquons que le retard par chaque protocole, nous voyons que le prophet est faible car il transmet le message aux nœuds avec des rencontres de destination plus élevées. et spray and wait en seconde à cause de 4 copies de message. puis notre protocole avec les mêmes copies de message que spray and wait. et epidemic avec des copies de messages illimitées.

3.6.4 l'influence du nombre de nœuds dans le duplication moyen

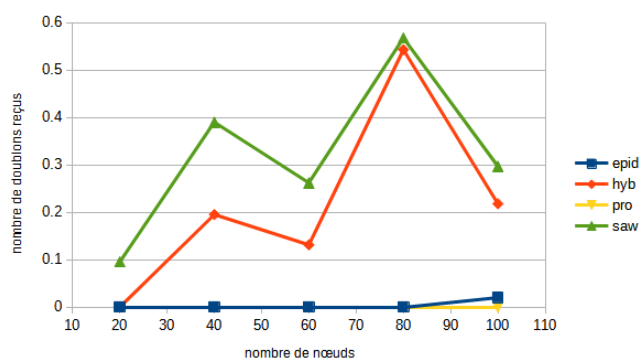


FIGURE 3.4 – duplication moyen par rapport nombre de nœuds

Dans le figure 3.4, nous remarquons que la duplication reçue par chaque protocole, nous voyons que le prophet est faible car il transmet le message aux nœuds avec des rencontres de destination plus élevées. et l'epidemic est faible car vecteur sommaire. puis

spray and wait à cause de 4 exemplaires. puis notre protocole avec le même nombre de copies.

3.6.5 l'influence du nombre de nœuds dans le nombre de sauts moyen

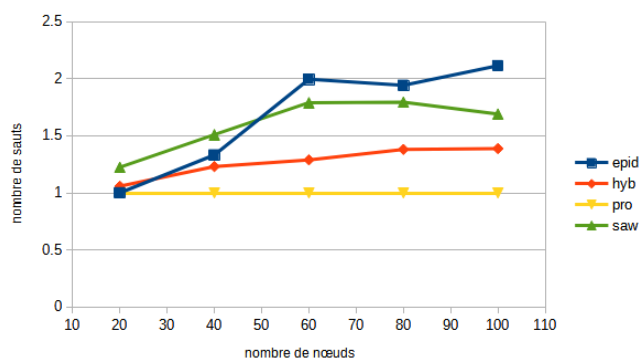


FIGURE 3.5 – hop moyen par rapport nombre de nœuds

Dans le figure 3.5, nous remarquons que des sauts par chaque protocole, nous voyons que le prophet est faible car il transmet le message aux nœuds avec des rencontres de destination plus élevées. et notre protocole qui combine spray and wait avec prophet. puis spray and wait et epidemic car inonder au hasard le message jusqu'à ce qu'il atteigne sa destination.

3.6.6 l'influence du nombre de nœuds dans le cache moyen

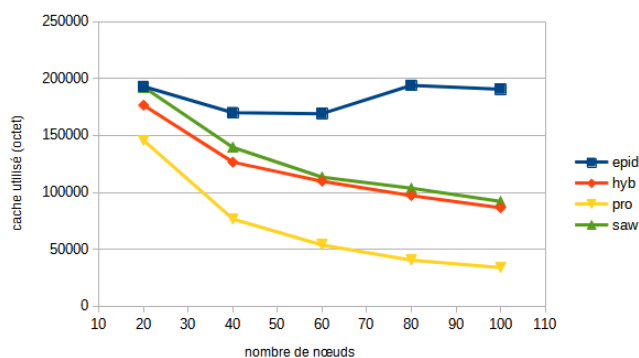


FIGURE 3.6 – cache moyen par rapport nombre de nœuds

Dans le figure 3.6, nous remarquons que le cache pour chaque protocole, nous voyons que epidemic est élevé à cause de sa technique d'inondation et qu'il augmente avec la

densité. et nos protocoles viennent en second parce que le nombre de duplications est de 4. puis spray and wait parce que le nombre de duplications est de 4. puis prophet parce qu'il transmet le message à la destination.

3.6.7 l'influence du nombre de nœuds dans l'overhead moyen

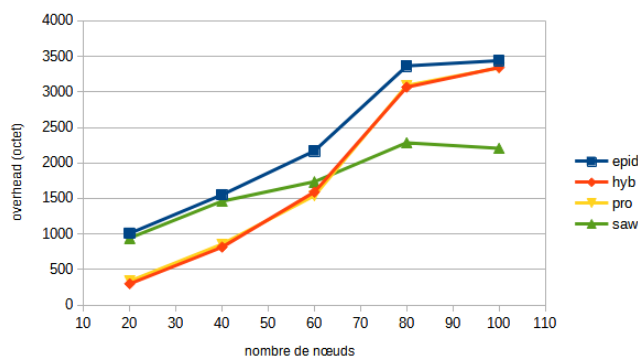


FIGURE 3.7 – overhead moyen par rapport nombre de nœuds

Dans le figure 3.7, nous remarquons que la overhead pour chaque protocole, nous voyons que l'epidemic est élevée en raison de l'échange de vecteurs sommaires. et nos protocoles et notre prophet viennent en deuxième position en raison de l'échange de table de probabilité de livraison. puis spray and wait. tous augmentent avec la densité car il y a plus de nœuds et des rencontres plus fréquentes.

3.6.8 l'influence du nombre de nœuds dans l'énergie moyen

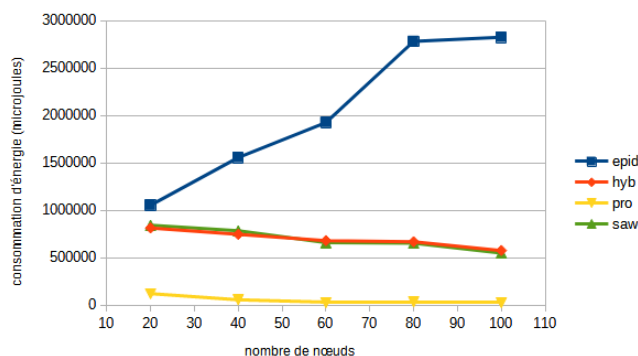


FIGURE 3.8 – energy moyen par rapport nombre de nœuds

Dans le figure 3.8, nous remarquons que l'énergie pour chaque protocole, nous voyons que epidemic est élevé à cause de sa technique d'inondation. et nos protocoles et spray

et wait viennent tous les deux en deuxième position à cause des duplications = 4. puis prophet parce qu'il n'inonde pas le message.

3.7 Discussion de résultat

Sur la base des résultats de simulation des protocoles, plusieurs observations peuvent être faites :

Protocole Epidemic : Le Protocole Epidemic, qui repose sur l'inondation, a tendance à entraîner des frais généraux et une consommation d'énergie élevés en raison de la duplication inutile des messages et des taux de transmission de données élevés. Cependant, il atteint de faibles taux de livraison et des retards et une utilisation du cache élevés.

Protocole Spray and wait : Le Protocole spray and wait, qui combine la pulvérisation opportuniste de messages sur des nœuds aléatoires et l'attente de rencontres avec d'autres nœuds pour le transfert de messages, a entraîné des rations de livraison élevées et une réduction des frais généraux et de la consommation d'énergie par rapport à l'Epidemic, et une utilisation modérée du cache. Cependant, il souffre de retards plus longs et de taux de livraison plus faibles dans les réseaux à faible densité..

Protocole Prophet : Le protocole Prophet, qui utilise une combinaison de décisions de routage basées sur l'historique et sur la rencontre, peut atteindre des taux de livraison modérés et des retards inférieurs par rapport à l'utilisation du cache pour les protocoles Epidemic et de Spray and wait. Il peut également réduire les frais généraux et la consommation d'énergie. en prenant des décisions de transfert plus éclairées. Cependant, il souffre d'un surcoût élevé dans les grands réseaux par rapport à la Spray and wait.

Notre contribution : Les observations suivantes peuvent être faites sur la base des les figures obtenus.

Dans le figure des données totales envoyées 3.1, nous remarquons que notre protocole a la même quantité que la pulvérisation et attend à cause du même nombre de duplications.

Alors qu'en retard dans le figure 3.3, nous remarquons que notre protocole est meilleur que l'épidémie et pulvérise et attends lorsque les nœuds sont inférieurs à 50, et lorsque les nœuds sont supérieurs à 50, notre protocole ressemble à pulvériser et attendre en raison d'un meilleur transfert plutôt que simplement diffusant au hasard.

En énergie dans le figure 3.8, nous remarquons que notre protocole est comme une pulvérisation et attend à nouveau à cause du même nombre de duplications.

Alors qu'en duplication reçue dans le figure 3.4, spray and wait et notre protocole sont à nouveau les mêmes car il n'y a pas de vecteur récapitulatif.

En nombre de saut dans le figure 3.5 nous remarquons que notre protocole est entre prophète et spray and wait.

Dans l'utilisation du cache dans le figure 3.6, nous remarquons que notre protocole est le même que spray and wait, en raison d'une duplication limitée à 4.

Dans le taux de livraison dans le figure 3.2, lorsque les nœuds sont inférieurs à 45, les mêmes performances que la pulvérisation et l'attente, mais lorsque les nœuds sont supérieurs à 45, le protocole est le meilleur de tous.

En termes de surcharge dans le figure 3.7, nous remarquons que notre protocole a le même montant que le prophète en raison de l'échange de table de probabilité de livraison.

3.8 Conclusion

Dans ce chapitre, nous avons simulé 3 protocoles (épidémique, pulvérisation et attente et prophète) et nos protocoles proposés dans OMNET ++, après avoir obtenu les résultats, nous remarquons que nos protocoles se préforment en tant que spray and wait dans la plupart des cas, sauf dans les overhead, notre préforme de protocole en tant que prophète, et dans le taux de livraison, notre protocole obtient les meilleures performances dans chacun d'eux en cas de densité élevée.

Conclusion Générale

Ces memoire s'est concentrée sur la comparaison et l'optimisation des protocoles de routage pour les réseaux tolérants au délai dans FANET. Nous avons examiné les protocoles d'épidémie, pulvérisation et attente, prophète et notre protocole proposé et évalué leurs performances à l'aide du simulateur OMNET++ 6.

A travers notre étude, nous avons observé que chaque protocole a ses forces et ses faiblesses. Le protocole epidemic peut souffrir d'une surcharge et d'une consommation d'énergie élevées en raison de sa technique d'inondation. Le protocole de spray and wait peut réduire les frais généraux et la consommation d'énergie par rapport aux protocoles épidémiques. Le protocole prophet combine des décisions de routage basées sur l'historique et sur la rencontre, et peut améliorer les taux de livraison et réduire les frais généraux. et notre protocole qui est une hybridation de pulvérisation et d'attente et de prophète peut atteindre une meilleure ration de dilevery qu'eux tous lorsque la densité du réseau devient élevée avec un retard modéré.

Nous avons simulé tous les protocoles et nous avons remarqué que nos protocoles ont un retard modéré et un meilleur taux de livraison en haute densité.

Nous indiquons également que des efforts de recherche et d'optimisation supplémentaires peuvent être nécessaires pour obtenir des performances optimales dans d'autres scénarios FANET spécifiques. Pour nos développements futurs, nous envisagerons de créer des mécanismes géographiques (prévisibilité du mouvement et de la position des nœuds) et d'ajouter des mécanismes de sécurité (cryptage), d'intégrer RED (Random Early Detection) pour une meilleure gestion de le mémoire cache et d'ajouter une méthode de parité pour minimiser la perte de paquets.

Bibliographie

- [1] Alexey V. Leonov. Application of bee colony algorithm for FANET routing. In *2016 17th International Conference of Young Specialists on Micro/Nanotechnologies and Electron Devices (EDM)*. IEEE, June 2016.
- [2] Jie Zhang, Gang Wang, Chen Liu, Fangzheng Zhao, and Xin Zhang. Delay tolerant network and the algorithms of DTN routing. *Journal of Physics : Conference Series*, 1169 :012058, February 2019.
- [3] David Wetherall Andrew Tanenbaum. *Computer Networks*. Pearson, 6 (global edition) edition, 2021.
- [4] Keith W. Ross James W. Kurose. *Computer Networking : A Top-Down Approach*. Pearson, 8 edition, 2021.
- [5] Les catégories de réseaux sans fils (la technologie wifi). <https://www.clicours.com/les-categories-de-reseaux-sans-fils-la-technologie-wifi/>. (accessed : 01.02.2023).
- [6] Rayane SEDRATI Raounak BABELHADJ. Routage dans les réseaux fanet, etude comparative, 2022.
- [7] KAMA Bellahcene DJEDIAI Mounir. Evaluation des performances des différents protocoles de routage des réseaux ad hoc pour les réseaux multi-uav (fanet), 2022.
- [8] Qamar Usman, Omer Chughtai, Nadia Nawaz, Zeeshan Kaleem, Kishwer Abdul Khalik, and Long D. Nguyen. A reliable link-adaptive position-based routing protocol for flying ad hoc network, 2020.
- [9] Djenidi Nabil. Analyse de la sélection dynamique des chefs de cluster pour fanet, 2022.
- [10] Mobile ad hoc networking (manet). <https://www.rfc-editor.org/rfc/rfc2501>. (accessed : 01.02.2023).
- [11] Barakat Pravin Maratha, Tarek R. Sheltami, and Khaled Salah. Performance study of MANET routing protocols in VANET. *Arabian Journal for Science and Engineering*, 42(8) :3115–3126, December 2016.

- [12] Omar Sami Oubbati, Mohammed Atiquzzaman, Pascal Lorenz, Md. Hasan Tareque, and Md. Shohrab Hossain. Routing in flying ad hoc networks : Survey, constraints, and future challenge perspectives. *IEEE Access*, 7 :81057–81105, 2019.
- [13] Mahyar Nemati, Bassel Al Homssi, Sivaram Krishnan, Jihong Park, Seng W. Loke, and Jinho Choi. Non-terrestrial networks with UAVs : A projection on flying ad-hoc networks. *Drones*, 6(11) :334, October 2022.
- [14] Armir Bujari, Claudio E. Palazzi, and Daniele Ronzani. FANET application scenarios and mobility models. In *Proceedings of the 3rd Workshop on Micro Aerial Vehicle Networks, Systems, and Applications*. ACM, June 2017.
- [15] Inam Ullah Khan, Muhammad Abul Hassan, Mohammad Dahman Alshehri, Mohammed Abdulaziz Ikram, Hasan J. Alyamani, Ryan Alturki, and Vinh Truong Hoang. Monitoring system-based flying IoT in public health and sports using ant-enabled energy-aware routing. *Journal of Healthcare Engineering*, 2021 :1–11, July 2021.
- [16] Amin Vahdat and David Becker. Epidemic routing for partially-connected ad hoc networks. *Technical Report*, 06 2000.
- [17] T. Spyropoulos, K. Psounis, and C.S. Raghavendra. Efficient routing in intermittently connected mobile networks : The multiple-copy case. *IEEE/ACM Transactions on Networking*, 16(1) :77–90, February 2008.
- [18] A.S.S. Vieira, J.G. Filho, Joaquim Jr, and Ahmed Patel. Vdtn-tod : Routing protocol vanet/dtn based on trend of delivery. *Advanced International Conference on Telecommunications, AICT*, 2013 :135–141, 01 2013.
- [19] Anders Lindgren, Avri Doria, and Olov Schelén. Probabilistic routing in intermittently connected networks. *ACM SIGMOBILE Mobile Computing and Communications Review*, 7(3) :19–20, July 2003.
- [20] Omnet++ simulation manual. <https://doc.omnetpp.org/omnetpp/SimulationManual.pdf>. Accessed : 5-2-2023.
- [21] Inet 4.4.0 documentation. <https://inet.omnetpp.org/docs/users-guide/>. Accessed : 5-2-2023.
- [22] Antonio Virdis and Michael Kirsche, editors. *Recent Advances in Network Simulation*. Springer International Publishing, 2019.
- [23] Thomas Chamberlain. *Learning OMNeT++*. Packt Publishing, 2013.
- [24] Omnet++ user guide. <https://doc.omnetpp.org/omnetpp/UserGuide.pdf>. Accessed : 5-2-2023.
- [25] Radhika Ranjan Roy. *Handbook of Mobile Ad Hoc Networks for Mobility Models*. Springer US, 2011.

- [26] Tsehay Admassu Assegie and Pramod Sekharan Nair. The performance of gauss markov's mobility model in emulated software defined wireless mesh network. *Indonesian Journal of Electrical Engineering and Computer Science*, 18(1) :428, April 2020.
- [27] Dan Broyles, Abdul Jabbar, and James Sterbenz. Design and analysis of a 3-d gauss-markov mobility model for highly-dynamic airborne networks. 01 2010.