N Ordre ……..Faculté/UMBB/202.

République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université M'hamed Bougara - Boumerdès

Faculté des Sciences

Thèse de Doctorat

Présenté par :

Amine Nouasri

Filière: Informatique

Spécialité: Informatique

Contribution à la qualité de service et la sécurité dans un réseau dynamique et distribué

Devant le jury :

Mr M. MEZGHICHE	Professeur	UMB	BOUMERDES	Président
Mr MA. RIAHLA	MCA	UMB	BOUMERDES	Rapporteur
Mr M. HAMADOUCHE	Professeur	UMB	BOUMERDES	Examinateur
Mr B. BOUDERAH	Professeur	UMB	M'SILA	Examinateur
Mr. K. HERAGUEMI	MCA	UMB	M'SILA	Examinateur
Mr. A. SNOUCI	MCA	ES DAT	ALGER	Examinateur

Année Universitaire 2021/2022

Remerciements

Je tiens tout d'abord à remercier Allah le tout puissant et miséricordieux, qui nous a donné la force et la patience d'accomplir ce modeste travail.

Je tiens à exprimer mes sincères remerciements à mon directeur de thèse le Dr. Riahla Mohamed Amine pour l'encadrement de qualité et les précieux conseils durant toute la période du travail.

Je remercie les membres du jury pour avoir accepté de juger ce travail et en particulier le professeur Mezghiche pour avoir accepté de présider ce jury.

Mes vifs remerciements vont aux enseignants de l'UMBB, aux membres du Laboratoire Limose à Boumerdes et à toute personne ayant contribué, de près ou de loin, à la réalisation de ce travail.

Je tiens aussi à remercier ma famille pour leur support inconditionnel. Je ne peux à travers cette petite page que dévouer mes sincères gratitudes pour leur soutien tout au long de ma thèse de doctorat.

Résumé

Les réseaux dynamiques présentent l'avantage de mettre en place un réseau de communication peu coûteux et rapide à déployer. Un des exemples typiques de ces réseaux, et qui prend de plus en plus d'importance ces dernières années sont les flottes de drones, à travers leurs domaines d'application variés.

Il très important d'assurer une Sécurité et une Qualité de service (ou QoS) dans l'exploitation de ces réseaux. Il convient d'assurer différents services de sécurité, comme l'authentification, l'intégrité, la confidentialité, et la disponibilité. En plus, ces échanges doivent être fait dans des délais acceptables et en minimisant les pertes de données. Ceci présente beaucoup de challenges dû aux propriétés Ad Hoc de ces réseaux.

Notre travail dans cette thèse a donné le fruit à un système de monitoring d'une flotte de drones. Notre solution porte sur une approche réactive qui résume les incidents possibles à travers le calcul de certains paramètres clés du réseau, et de réorganiser les nœuds de manière à contrer les incidents et assurer une continuité de service.

Mots clés: Réseau dynamique, flotte de drones, Sécurité, QoS, Monitoring.

Summary

Dynamic networks have the advantage of setting up a communication network that is inexpensive and quick to deploy. One of the typical examples of these networks, which has become increasingly important in recent years, are drone fleets, through their various applications. It is very important to ensure Security and Quality of Service (or QoS) in the operation of these networks. Various security services must be ensured, such as authentication, integrity, confidentiality, and availability. In addition, these exchanges must be done within acceptable deadlines and minimizing data loss. This presents many challenges due to the Ad Hoc properties of these networks.

Our work in this thesis has produced a monitoring system for a fleet of drones. Our solution uses a reactive approach that summarizes possible incidents through the calculation of certain key network parameters, and to reorganize the nodes in order to counter incidents and ensure service continuity.

Keywords: Dynamic network, drone fleet, Security, QoS, Monitoring.

ملخص

تتمتع الشبكات الديناميكية بميزة إنشاء شبكة اتصالات غير مكلفة وسريعة الانتشار. أحد الأمثلة النموذجية لهذه الشبكات ، التي أصبحت ذات أهمية متزايدة في السنوات الأخيرة ، هي أساطيل الطائرات بدون طيار ، من خلال مجالات تطبيقها المختلفة.

من المهم جدًا ضمان الأمن وجودة الخدمة في تشغيل هذه الشبكات. يجب ضمان خدمات أمنية مختلفة ، مثل المصادقة والسلامة والسرية والتوافر. بالإضافة إلى ذلك ، يجب أن تتم عمليات التبادل هذه ضمن المواعيد النهائية المقبولة وتقليل فقد البيانات. وهذا يمثل العديد من التحديات بسبب الخصائص المخصصة لهذه الشبكات.

أدى عملنا في هذه الأطروحة إلى اقتراح نظام مراقبة لأسطول من الطائرات بدون طيار. يركز الحل المقترح على نهج تفاعلي يلخص الحوادث المحتملة من خلال حساب قياسات متعلقة بسيرورة الشبكة، وإعادة تنظيم عناصر الشبكة من أجل مواجهة الحوادث وضمان استمرارية الخدمة.

الكلمات المفتاحية: الشبكة الديناميكية ، أسطول الطائرات بدون طيار ، الأمن ، جودة الخدمة ، المراقبة.

Table des Matières

Liste des Figures

Liste des Tableaux

Introduction Générale

Grâce aux succès du phénomène sans fil, nous disposons aujourd'hui d'une multitude de technologies de communication à notre disposition, en raison de leur coût peu élevé, de leur flexibilité et de la commodité qu'ils offrent par rapport aux réseaux locaux câblés classiques. Les réseaux dynamiques se basent sur une connectivité des nœuds sans fil et présentent l'avantage de mettre en place un réseau de communication peu coûteux et rapide à déployer. Mais il a été constaté que ces réseaux engendrent des difficultés lors de la conception de certains services tels que le routage, la qualité de service ou encore la sécurité du réseau. En effet, en l'absence d'une entité centrale, les nœuds doivent vérifier l'intégrité des messages échangés et leur délivrance en un temps acceptable eux-mêmes.

Plusieurs raisons justifient le besoin en matière de Sécurité et de Qualité de service (ou QoS) dans l'exploitation de ces réseaux. Nous pouvons citer des services critiques tel que le routage par exemple, ou il faut assurer l'échange périodique des messages de contrôle qui maintiennent l'état du réseau. Il est aussi à mentionner que ces réseaux sont vulnérables, avec une possibilité de lancer des attaques de l'extérieur du réseau ou à partir d'un nœud interne déjà compromit. Afin de déployer un réseau fiable, il est donc nécessaire de proposer une architecture de communication permettant aux nœuds, non seulement de coopérer, mais aussi de sécuriser les messages véhiculés avec une qualité de service acceptable rendu par le réseau aux applications.

Généralement, pour sécuriser un réseau, il convient d'assurer différents services de sécurité, comme l'authentification, l'intégrité, la confidentialité, et la disponibilité. Nous nous focalisons dans ce travail sur la disponibilité du service et l'intégrité des échanges entre nœuds du réseau. En plus, ces échanges doivent être fait dans des délais acceptables et en minimisant les pertes de données.

Plusieurs travaux de recherches ont été menés pour résoudre les problèmes de Sécurité et QoS liés aux réseaux dynamiques. A titre d'exemple, nous pouvons citer les solutions de cryptage des communications entre les nœuds, assurer la sécurité du protocole de routage, la réservation des ressources tout au long du chemin pour assurer une QoS aux nœuds communicants, etc.

Les motivations principales qui recommandent l'amélioration de la Sécurité et la QoS dans ces types du réseau se résument en deux points: le besoin des protocoles de s'adapter à la dynamique du réseau, et le besoin d'assurer aux applications un fonctionnement avec un niveau de Sécurité et une QoS minimale.

Nous avons organisé ce travail en deux parties. La première partie de ce travail représente un état de l'art des travaux de recherche sur la Sécurité et la QoS dans les réseaux dynamique. La deuxième partie étudie un cas de déploiement d'un réseau dynamique pratique qui est les flottes de drones. Étant donné les perspectives applicatives prometteuses d'un tel scénario, nous avons proposé notre contribution spécifique à ce scénario. L'efficacité de l'approche que nous proposons a été vérifiée et validée par des simulations à travers l'implémentation de divers scénarios affectant les services du réseau.

A cet effet, Nous avons réparti notre travail comme suit :

- Le chapitre 1 présentera une vue générale sur les réseaux dynamiques, leurs caractéristiques ainsi qu'une vue sur les protocoles d'accès et de routage sur les couches MAC et réseau. Nous avons ensuite présenté un type spécifique d'un réseau dynamique qui est les flottes de drones sur lequel notre contribution sera appliquée.
- Nous avons consacré le chapitre 2 à l'étude de la Sécurité dans les réseaux dynamique. Nous avons passé en revue les différentes menaces sur ces réseaux et les approches pour les solutionner. Ensuite, nous avons passé en revue les recherches récentes liées à la sécurité des flottes de drones.
- Le chapitre 3 suit le même chemin et se focalise sur l'aspect QoS. On étale dans cette partie les différents concepts liés à la qualité de service (QoS) des réseaux dynamiques en général et les flottes de drones en particulier. Ces derniers se présentent comme étant des réseaux sans infrastructures et à forte mobilité, d'où beaucoup de contraintes liées à la qualité de services doivent être considérées.
- Le chapitre 4 décrit principalement notre contribution et se base sur un scénario de déploiement de drones pour assurer la couverture d'une zone. Nous avons détaillé le fonctionnement de notre plateforme de simulation basée sur le simulateur NS3 ainsi que les paramètres retenus afin de vérifier l'efficacité de notre approche par rapport aux scenarios de déploiement. Ensuite, les résultats obtenus ont été analysés et discutés.
- A la fin, nous achèverons notre thèse par une conclusion ainsi que diverses perspectives de recherches à ce travail.

1. Etat de l’art sur les réseaux dynamiques

1.1 Introduction

Dans un réseau dynamique, les nœuds s’auto-organisent par nature, car ils ne disposent pas d'une infrastructure centralisée de routage ou des serveurs pour les administrer. Ce type de réseau est qualifié de dynamiques dans la mesure où des nœuds peuvent joindre et quitter le réseau de manière dynamique dans le temps.

L’objet de ce premier chapitre est de faire un état de l‘art sur ce type de réseau. Nous l’avons divisé en deux parties : la première partie examine les réseaux dynamiques en général, en décrivant leurs types et leurs propriétés. Ensuite, nous présentons les méthodes d’accès à ces réseaux et les techniques de routage associés. Dans la deuxième partie, nous détaillons un cas pratique d’un réseau dynamique qui est les flottes de drones. Ces réseaux ont créé récemment de nouvelles opportunités de recherche et divers cas pratiques d’application.

1.2 Les réseaux dynamiques

1.2.1 Définition et propriétés

Un réseau dynamique est un réseau constitué de nœuds communiquant entre eux par des liaisons sans fil sans aucun organe central. Ces nœuds peuvent être des appareils personnels, des ordinateurs portables, des téléphones cellulaires ou tout autres dispositifs communiquant entre eux sans infrastructure fixe ni gestion centrale. Ces réseaux sont caractérisés par des moyens de communication peu fiables où la topologie du réseau change dynamiquement. De plus, chaque nœud est limité en termes de bande passante, batterie et puissance de calcul.

En raison de la nature auto-configurante de ces réseaux et de l'absence d'infrastructure centrale, les nœuds dans un réseau dynamique jouent à la fois le rôle de routeur et d'hôte. Comme les nœuds communiquent directement entre eux et sont très dynamiques, ils ont les propriétés et les exigences suivantes :

Fonctionnement distribué: Le réseau est distribué et ne dépend pas d'une autorité centralisée. Ceci est bénéfique car les nœuds peuvent entrer et sortir du réseau facilement.

Réseau Sans boucle: Pour un fonctionnement efficace du réseau, il est nécessaire de garantir que les routes dans le réseau sont exemptes de boucles. Cela permet d'éviter le gaspillage de la bande passante et de la puissance de calcul. De plus, les retards sont réduits si les routes sont sans boucle.

Fonctionnement basé sur la demande: Pour éviter le gaspillage inutile des ressources dans ces réseaux, il est préférable de ne réagir que lorsque cela est nécessaire. En d'autres termes, le protocole de routage doit être de préférence réactif.

Sécurité: La sécurité est une question importante dans ce type de réseau. Les nœuds sont sensibles aux attaques vue qu'ils sont exposés à l'extérieur. Pour garantir un comportement adéquat, certaines mesures de sécurité sont nécessaires. La sécurité peut être intégrée en appliquant le cryptage et l'authentification aux protocoles utilisés.

Prise en charge de la Qualité de service: La Qualité de service est un paramètre important pour fournir un service acceptable aux applications. Les protocoles de routage doivent prendre en charge les exigences des applications en termes de QoS. Par exemple, le trafic en temps réel doit avoir un faible délai.

Routes multiples: Le protocole de routage doit avoir des routes redondantes, de sorte que lorsqu'un lien tombe en panne, une route alternative peut être utilisée sans initier de découverte de route (Figure 1). De plus, la mise en mémoire tampon des routes rend le protocole résistant aux changements fréquents de topologie.

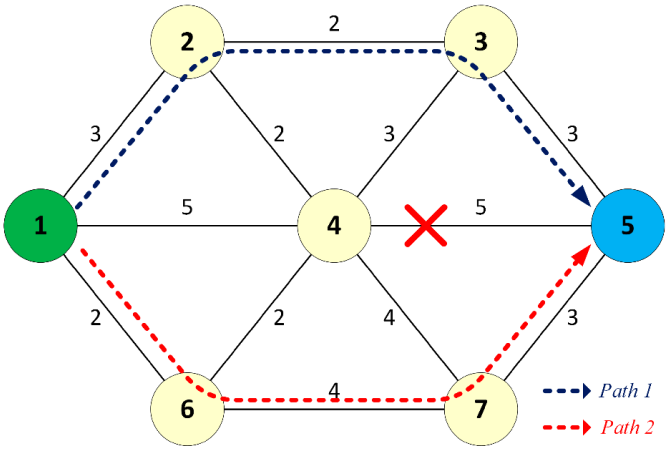

Figure 1: Exemple de routes multiples dans un réseau dynamique

Conservation de l'énergie: Les nœuds qui forment le réseau dynamique ont des ressources très limitées. L'une de ces ressources importantes est la batterie. Les nœuds doivent économiser l'énergie des batteries des appareils mobiles. Ils doivent passer en mode économie d'énergie ou en mode veille lorsqu'ils ne sont pas utilisés.

1.3 Types de réseaux dynamiques [NOU 19]

1.3.1 MANET

Un réseau mobile ad hoc (MANET) est un réseau sans fil et sans entité centrale (Figure 2). Il se base sur la capacité des nœuds à coopérer pour former un réseau entre eux. Chaque nœud relaye ainsi le message de l'émetteur jusqu'à la destination. Cette coordination permet aux nœuds de se déplacer librement, ce qui peut causer des changements fréquents de la topologie du réseau. Pour faire face à cette difficulté, le réseau doit utiliser des protocoles de communication fiables permettant de reconstruire une topologie communicante en tout temps [ELA 15].

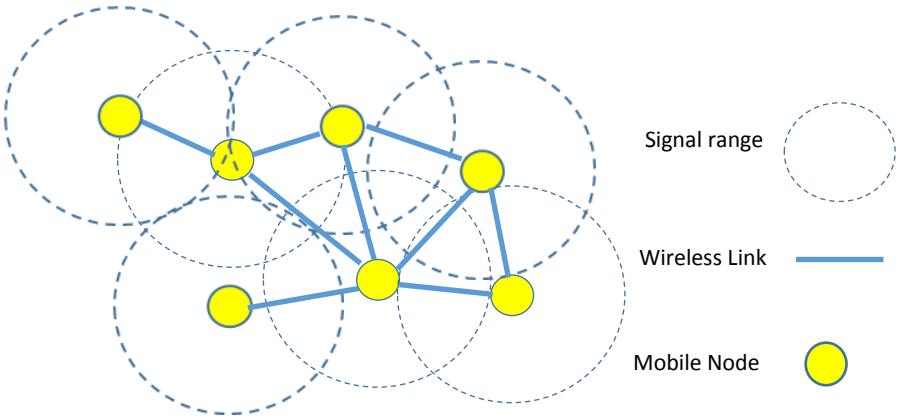

Figure 2: Exemple d'un réseau MANET

1.3.2 WSN

Un réseau de capteurs sans fil (Wireless Sensor Network ou WSN) est un réseau constitué de petits nœuds sans fil légers, déployés en grand nombre pour surveiller une zone (Figure 3). Le but est de prendre des mesures sur l'environnement à surveiller (par exemple la température, la pression ou l'humidité, etc). Les nœuds composant le réseau de capteurs collaborant entre eux pour former un réseau Ad Hoc capable de transmettre les données capturées à travers le réseau à un nœud particulier appelé **Sink,** qui est en charge de la collecte de données [ALZ 13].

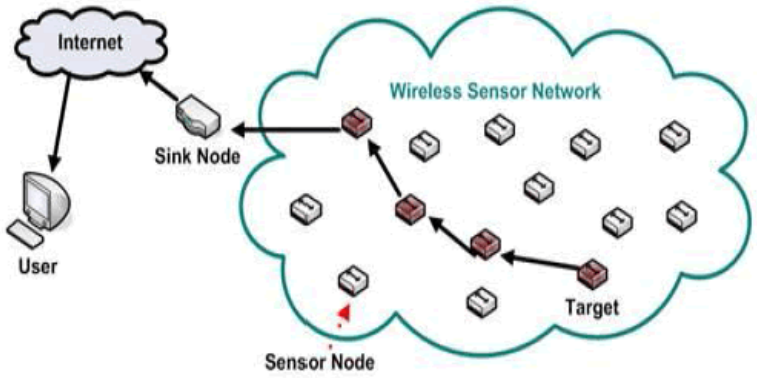

Figure 3: Exemple d'un réseau WSN [Puy 16]

L'objectif principal d'un réseau WSN est donc de collecter des données de l'environnement dans lequel ces capteurs ont été déployés et de les envoyer à un site de contrôle où elles peuvent être observées et analysées. Il faut noter que les nœuds du réseau WSN sont limités en ressources, avec une durée de vie énergétique faible, des calculs lents, une petite mémoire et des capacités de communication limitées.

1.3.3 VANET

Les VANET représentent des véhicules mobiles communiquant entre eux ou avec une infrastructure au bord de la route (figure 4). Par rapport à un réseau Ad Hoc classique, les réseaux VANET sont caractérisés par une forte mobilité des nœuds rendant la topologie du réseau fortement dynamique.

Les types de communication dans les VANET sont classés en trois catégories : la communication entre véhicules (V-V), la communication entre véhicules et infrastructure routière appelée unité d'infrastructure en bord de route (RSU), et la communication avec les autorités centrales responsables de la gestion de l'identité et de l'enregistrement des véhicules [YAD 11].

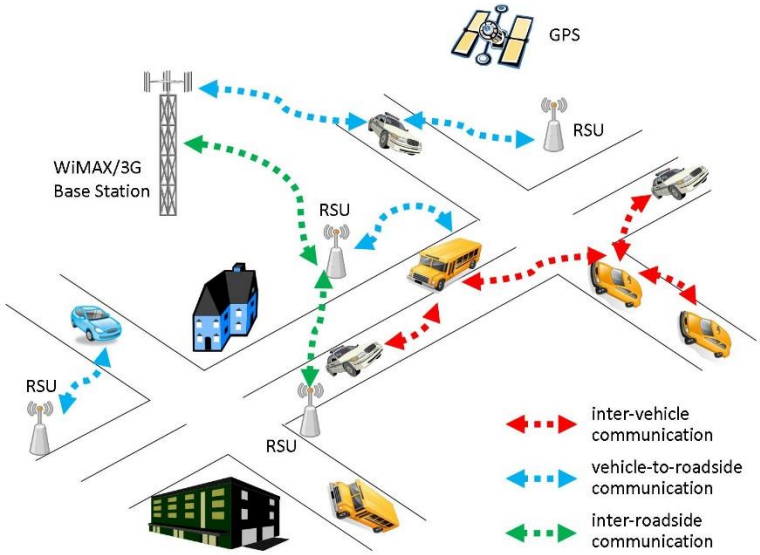

Figure 4: Exemple d'un réseau VANET [Ull 16]

Pour la mise en place d'un tel réseau, certains équipements doivent être installés (Figure 4) au sein des véhicules, tel: les dispositifs de perception de l'environnement (radars, caméras), un système de localisation GPS, et bien sûr une plateforme de traitement. Plusieurs technologies peuvent être mises en œuvre pour l'établissement des communications véhiculaires, tel : les réseaux sans-fil de type 802.11, WIMAX, Bluetooth, etc.

1.3.4 Mesh

Dans un réseau Mesh ou WMN (Wireless Mesh Network), les nœuds du réseau établissent automatiquement des liens sans fil et créer une connectivité mailée (Figure 5). Les nœuds dans un réseau WMN sont constitués de deux types de nœuds: les routeurs Mesh et les clients Mesh. Un routeur Mesh est équipé de plusieurs interfaces reposant sur des technologies d'accès sans fils. Les routeurs Meshs ont une mobilité minimale et constituent des passerelles pour les clients meshs et fournissent les fonctions de routage pour ces derniers. Bien que les clients Mesh puissent également fonctionner comme des routeurs, ils sont par contre légers, et les fonctions de routage ne sont pas implémentées pas sur ces derniers.

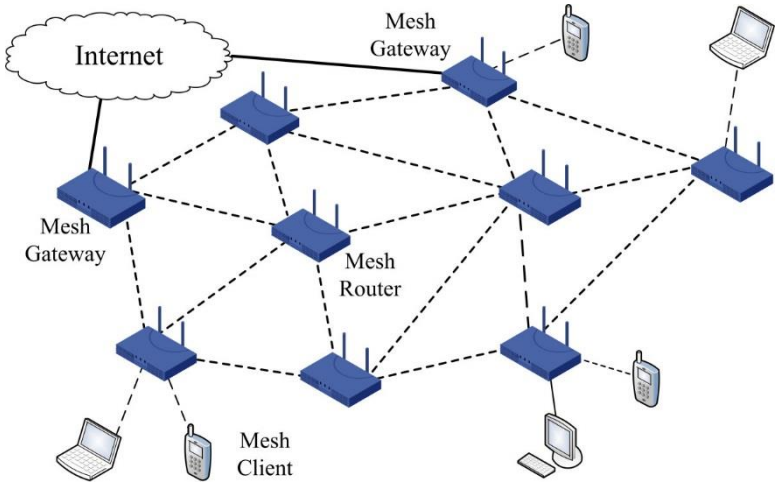

Figure 5: Exemple d'un réseau Mesh [LIU 12]

Le principal avantage d'un réseau WMN réside dans sa tolérance aux pannes et la simplicité de la mise en place d'un tel réseau, ainsi que et sa capacité de fournir un service à haut débit. Contrairement aux réseaux cellulaires, où la défaillance d'une seule station de base (BS) entraîne l'indisponibilité des services de communication sur une vaste zone géographique, un réseau Mesh est un réseau à large bande qui offre des services de communication sur une large zone géographique offrant une grande tolérance aux pannes même en cas de défaillance d'un certain nombre de nœuds [AKY 05].

1.3.5 Flotte de Drones

Les drones ont la possibilité de créer un réseau sans fil dans l'air (Figure 6). Lorsque les drones effectuent une tâche coopérative en volant en groupe par exemple, on peut considérer qu'ils volent dans une flotte. La flotte est capable de se reconfigurer en toute sécurité en fonction de l'évolution des missions, le nombre de drones et de l'environnement. En outre, la qualité des liaisons sans fil au sein d'un réseau de drones peut changer au fil du temps pour diverses raisons, comme les modifications de la distance de communication par exemple. Toutes ces exigences rendent le contrôle de la topologie plus important dans un environnement de réseau de drones [ZHA 12].

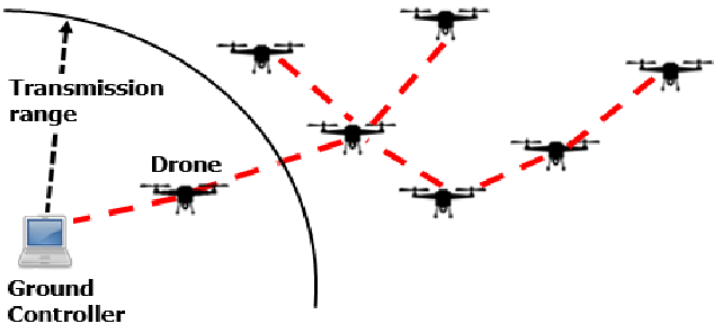

Figure 6: Exemple d'une flotte de drones [KIM 16]

L'intérêt dans l'utilisation d'une flotte de drones au lieu d'un seul drone réside dans le faite que pour une mission de plusieurs heures, et qui nécessite de parcourir une zone très large, l'utilisation d'un seul drone peut être limitée en matière d'autonomie de batterie et de portée (notamment en cas de présence d'obstacles). La collaboration de plusieurs drones est une solution plus intéressante. Egalement, avec une flotte de drones, l'opération peut se poursuivre en cas de panne d'un des drones ou en cas d'épuisement de la batterie en reconfigurant les ressources de la flotte.

1.4 Protocoles de contrôle d'accès au support (protocoles MAC)

Les protocoles de la couche liaison de données (ou protocoles MAC) assurent en premier lieu le contrôle d'accès au support. Ces protocoles tiennent compte des contraintes du canal, de l'atténuation et le bruit, tout en fournissant un accès efficace au support. Ces protocoles peuvent être classés en deux catégories : protocoles sans contention et avec contention. Le schéma sans contention définit au préalable les affectations pour permettre aux nœuds de transmettre sur le support. Nous retrouvons par exemple les méthodes d'accès au support TDMA, CDMA, FDMA et token-based. Les mécanismes sans contention sont généralement utilisés pour fournir un délai de bout en bout faible et une largeur de bande minimale, privilégiant ainsi les applications sensibles aux délais tels que les flux audio et vidéo. D'autre part, les schémas basés sur la contention sont plus appropriés pour le transfert de données sporadiques sur les réseaux mobiles en raison de la nature aléatoire et temporaire de la topologie.

Les réseaux personnels Bluetooth, par exemple, utilisent un mécanisme MAC maître-esclave sans contention. Les réseaux locaux Wi-Fi en mode Ad Hoc utilisent par contre le protocole MAC IEEE 802.11 qui basé sur un accès avec contention. Le protocole IEEE 802.11 est la technologie sans fil la plus répandue et comporte une la famille de protocoles de plusieurs variantes (Figure 7), par exemple, IEEE 802.11b, IEEE 802.11a, et IEEE 802.11g, qui diffèrent l'une de l'autre au niveau de la couche physique.

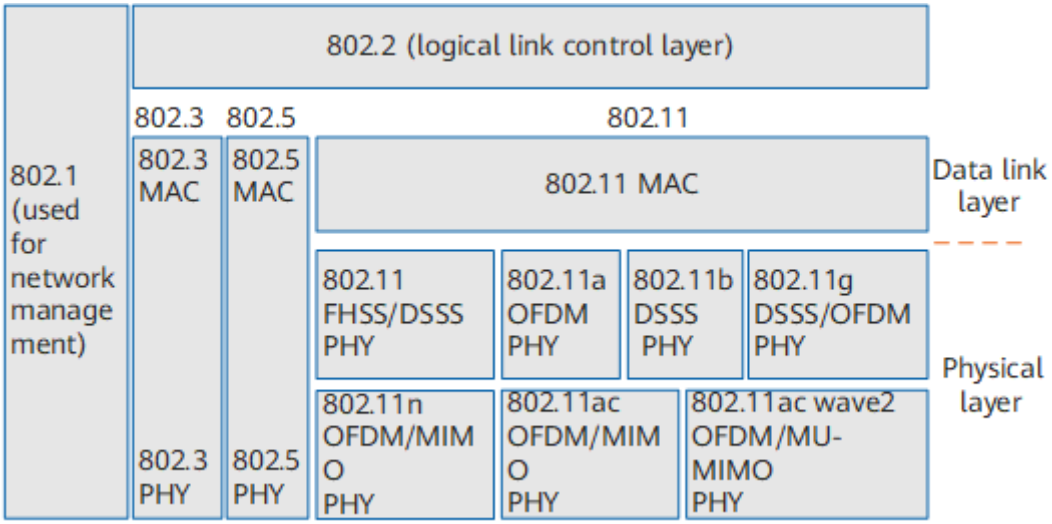

Figure 7: Couches du protocole IEEE 802.11 [HUA 22]

Le protocole MAC de l'IEEE 802.11 spécifie deux fonctions d'accès au support : la fonction de coordination distribuée (DCF) et la fonction de coordination ponctuelle (PCF). DCF est un mécanisme distribué dans lequel chaque nœud détecte l'utilisation du support et transmet si le support est libre. D'autre part, la PCF est un mécanisme centralisé dans lequel un point d'accès contrôle l'accès au support. Ce mécanisme est donc conçu pour les réseaux à infrastructure centralisée. La fonction DCF utilise l'accès multiple avec détection de porteuse et évitement des collisions (CSMA/CA) pour le contrôle du support. Une station qui souhaite émettre détecte d'abord le support. Tel que indiqué dans la Figure 8, si le support est disponible pendant au moins un temps appelé DIFS (Distributed Inter-Frame Space), la station transmet. Dans le cas contraire, si le support est occupé, la transmission est reportée à une période DIFS jusqu'à la fin de la fin de la transmission en cours. Ensuite, un processus de backoff est lancé en choisissant un nombre aléatoire entre zéro et une taille de la fenêtre de contestation (CW). Si le support reste inactif pendant le DIFS, la station reprend son délai de temporisation. Lorsque le temporisateur expire, la station envoie alors sa trame [RUB 06].

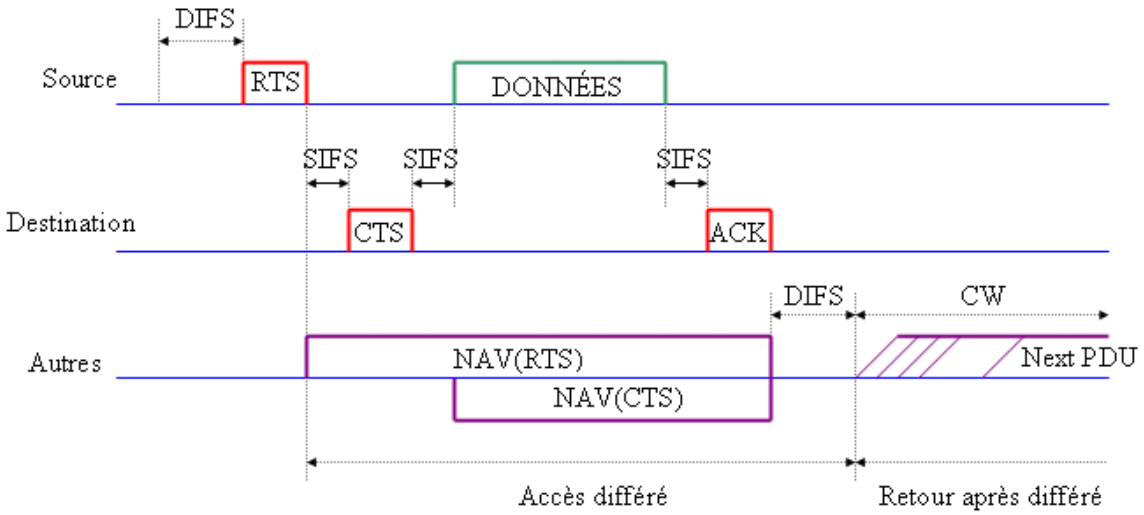

Figure 8: Principe d'accès au support avec la fonction DCF

1.5 Routage dans les réseaux dynamiques

L'objectif des protocoles de routage est de trouver le(s) meilleur(s) itinéraire(s) entre un nœud source et un nœud destination dans le réseau. Il est important que cela soit fait de manière efficace afin que les ressources ne soient pas gaspillées à transporter des informations inutiles d'une part, et de manière fiable afin que si un chemin existe, il soit découvert. Il est courant de supposer que la "meilleure" route est celle qui comporte le moins de sauts, car on peut s'attendre à ce que de telles routes aient une latence plus faible, offrent moins de possibilités de problèmes et atteignent la destination plus rapidement. Cependant, le meilleur itinéraire n'est pas toujours le plus court. Certaines liaisons peuvent être très encombrées ou soumises à des interférences entre des liaisons voisines à fort volume. De nombreux protocoles de routage permettent l'utilisation de métriques de routage pour évaluer la qualité d'une route et choisir la meilleure. Le nombre de sauts est probablement la métrique la plus utilisée.

Les protocoles de routage dans les réseaux dynamiques sont classés en trois types (Figure 9): proactifs, réactifs (ou à la demande) et hybrides. Les protocoles proactifs exigent aux nœuds d'un réseau de garder la trace des routes vers toutes les destinations possibles. Ceci est important car, chaque fois qu'un paquet demande à être acheminé, l'itinéraire est préalablement identifié et peut être utilisé immédiatement. Egalement, chaque fois qu'il y a une modification de la topologie, elle est diffusée dans tout le réseau.

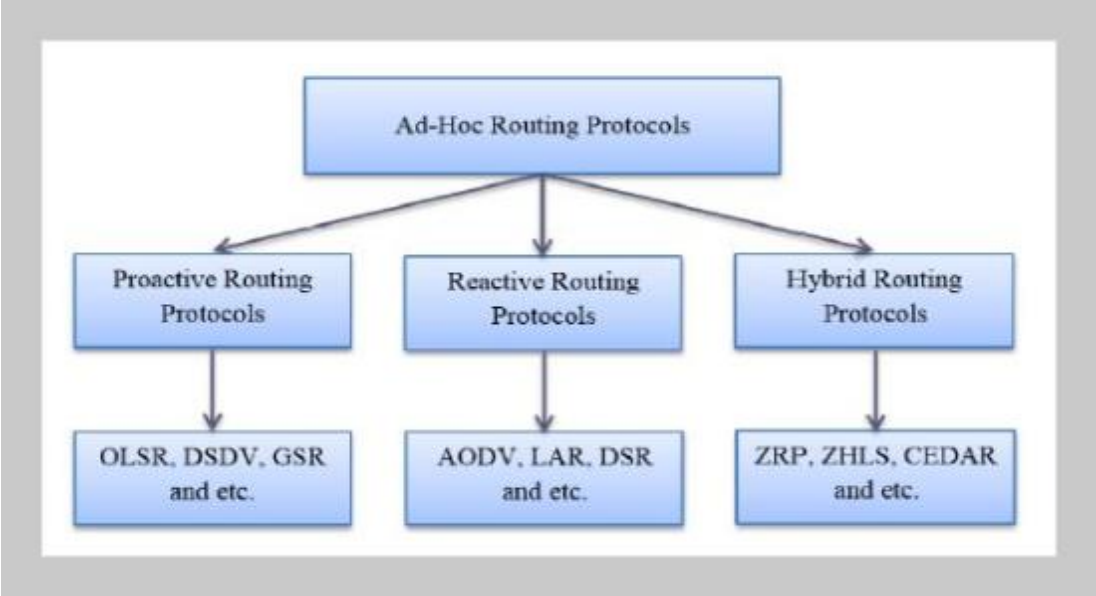

Figure 9: Classification des protocoles de routage [ALD 18]

Les protocoles à la demande (réactifs) construisent les routes lorsque le nœud source le demande. Lorsqu'un nœud a besoin d'envoyer des paquets mais n'a pas de route vers la destination, il commence un processus de découverte de route dans le réseau. Lorsqu'une route est trouvée, elle est sauvegardée et ensuite maintenue par une procédure de maintenance de route jusqu'à ce que la destination devienne inaccessible ou que la route ne soit plus souhaitée.

Les protocoles proactifs présentent l'avantage de minimiser le délai des communications avec les nouvelles destinations. Les nouvelles communications avec ces destinations subissent un retard minimal, mais présentent l'inconvénient d'une surcharge avec les messages de contrôle pour mettre à jour les informations de routage à tous les nœuds. Pour surmonter cette limitation, les protocoles réactifs adoptent la méthode inverse en recherchant la route vers une destination uniquement lorsque cela est nécessaire. Par conséquent, les protocoles réactifs utilisent régulièrement moins de bande passante que les protocoles proactifs.

Les protocoles de routage réactifs ont une surcharge plus faible que les protocoles proactifs car ils découvrent et maintiennent les routes uniquement lorsqu'elles sont réellement nécessaires. Cela réduit les surcharges de trafic pour le réseau qui n'a pas besoin de gérer des routes qui ne sont jamais utilisées. L'inconvénient est que les protocoles réactifs subissent un retard lors de l'établissement de la connexion pendant laquelle la route est découverte.

Les protocoles hybrides combinent les deux approches: celle des protocoles proactifs et celle des protocoles réactifs. Le principe est de divisé le réseau en zones et le principe est d'utiliser une approche proactive pour avoir des informations sur les voisins les plus proches, qui se trouvent au maximum à deux sauts du nœud mobile. Une approche réactive est utilisée au-delà de cette zone prédéfinie afin de chercher des routes vers les autres zones.

L'avantage de cette catégorie de protocoles est qu'elle s'adapte bien aux réseaux de grandes tailles. Cependant, cette approche a comme inconvénient de cumuler les points faibles des protocoles réactifs et ceux des protocoles proactifs, tels que les messages de contrôle périodiques et le coût associe à l'établissement d'une nouvelle route.

1.5.1 Protocole OLSR

Les protocoles proactifs, ou appelés aussi à état de liens, garantissent que chaque nœud du réseau dispose d'une route à jour vers tous les autres nœuds. Ces protocoles sont intéressants car ils trouvent des routes optimales sans délai. Le protocole OLSR (Open Link State Routing) [CLA 03] est un protocole proactif largement utilisé dans la recherche sur les réseaux sans fil. Ce protocole trouve la route optimale en se basant sur le plus petit nombre de sauts entre les nœuds du réseau.

Dans OLSR, tous les nœuds du réseau diffusent périodiquement des messages HELLO qui identifient le nœud du réseau et ses voisins immédiats. Les nœuds récepteurs utilisent ces informations pour découvrir leurs voisins immédiats, savoir si un lien bidirectionnel existe avec ce voisin et identifier les nœuds de réseau qui sont dans leur voisinage à deux sauts. En utilisant les informations des messages HELLO, chaque nœud du réseau calcule un ensemble de relais multipoints (MPR) (Figure 10) un sous-ensemble de ses voisins par lequel il peut atteindre tous ses voisins à deux sauts. Les mises à jour des routes sont diffusées sur le réseau sous la forme d'un message de contrôle (TC).

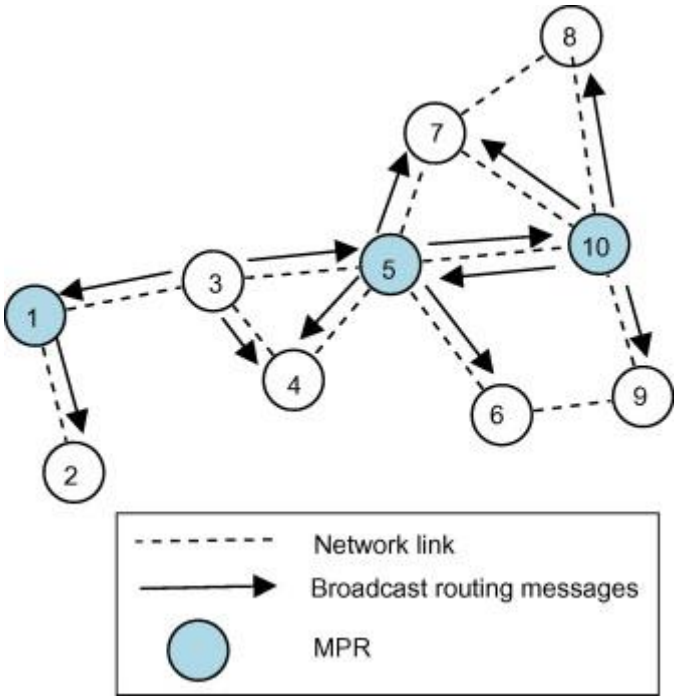

Figure 10: Utilisation des MPR dans le protocole de routage OLSR

Les MPR sont importants car ils sont utilisés pour diffuser et rediffuser les messages TC, minimisant ainsi la quantité de trafic diffusé pour les mises à jour de routage. Cela réduit considérablement le nombre de diffusions TC par rapport au mécanisme d'inondation classique. Cependant, ce mécanisme garantit que tous les nœuds du réseau vont recevoir la mise à jour. Un MPR peut également choisir de n'envoyer que des annonces partielles de l'état des liens en notifiant uniquement les liens vers les nœuds du réseau qui ont sélectionné le MPR. Ces informations partielles sont suffisantes pour que les récepteurs puissent calculer les routes optimales vers tous les nœuds du réseau.

1.5.2 Protocole DSDV

Un autre example d’un protocole de routage proactif est DSDV (Destination Sequenced Distance Vector). DSDV fait partie de la famille des protocoles de routage proactif à vecteur de distance, basé sur l’algorithme distribué de Bellmen-Ford. DSDV utilise les propriétés de la diffusion pour transmettre les informations de routage. Périodiquement, chaque station diffuse l’ensemble de sa table de routage suivie d’un numéro pour dater l’information. Ce numéro est appelé "numéro de séquence". A partir de deux numéros de séquence, il est possible de déterminer quelle information est la plus récente.

La table de routage d’un nœud contient les informations liées à chaque route. A la réception de ces informations, les voisins mettent à jour leur table de routage en suivant un schéma bien précis. Toute entrée de la table de routage est mise à jour, seulement, si l’information reçue est plus récente. A terme, le protocole DSDV fournit pour chaque destination, la route qui possède le plus faible nombre de nœuds.

1.5.3 Protocoles AODV

Les protocoles réactifs ou à la demande fonctionnent mieux pour les réseaux dynamiques dans lesquels il y a de nombreux nœuds mobiles et une topologie de réseau qui change fréquemment. Le protocole de routage On-demand Distance Vector (AODV) est un des exemples de protocoles de routage réactifs largement utilisés dans les réseaux sans fil à sauts multiples, et il est décrit en détail dans le RFC 3561 [PER 03].

Le processus de recherche d'un itinéraire d'un nœud source à une destination dans AODV se compose de deux parties, et commence lorsque le nœud source diffuse un paquet de demande d'itinéraire (RREQ) à tous ses voisins immédiats (Figure 11). Les récepteurs inspectent le numéro de séquence dans le RREQ pour déterminer s'ils ont déjà vu la demande auparavant. Si ce n'est pas le cas, ils mettent à jour leur table de routage avec une entrée vers la source et rediffusent la demande. Les demandes en double sont tout simplement ignorées ; cette méthode est connue sous le nom de *suppression des doublons.* Ceci permet d'éviter la présence de boucles de routage et le problème du comptage à l'infini, tout en réduisant le nombre de messages de rediffusion. Si la demande n'a pas été reçue auparavant, elle est rediffusée.

La deuxième partie du processus commence lorsque le RREQ est reçu par un nœud. La destination répond à la source en envoyant une réponse de route unicast (RREP) le long du chemin que la diffusion a emprunté jusqu'à la destination. Par souci d'optimisation, il est possible pour un nœud recevant un RREP de répondre au nom de la destination finale s'il possède déjà une entrée dans la table de routage. Dans ce cas, le nœud intermédiaire envoie le RREP à la source et un RREP unicast à la destination réelle. Ce dernier garantit que la destination dispose d'une entrée dans de table de routage en retour vers le nœud intermédiaire.

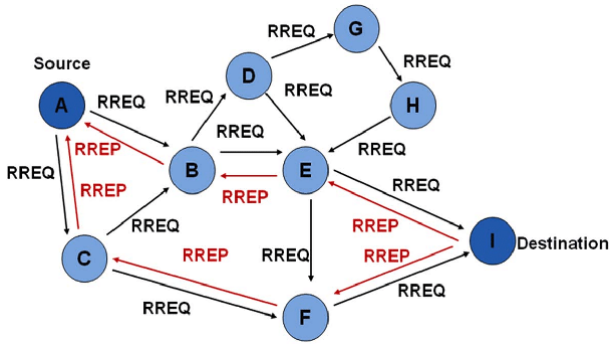

Figure 11: Messages RREQ/RREP dans AODV [NAG 10]

1.5.4 Protocole DSR

DSR (Dynamic Source Routing) est un protocole réactif. Il se différencie des autres protocoles dans l'utilisation du source routing. Dans ce cas, l'émetteur précise dans l'en-tête de chaque paquet la liste des nœuds qu'il devra traverser pour atteindre sa destination. Ce type de routage présente certains avantages particulièrement intéressants ; il autorise en particulier la source à conserver dans sa table de routage plusieurs chemins valides vers une même destination. Le choix du chemin emprunté pourra donc être fait indépendamment pour chaque paquet, et permet un meilleur équilibrage de la charge dans le réseau et une meilleure réactivité aux changements de topologie.

Dans la pratique, DSR est structuré en deux sous-parties complémentaires: la recherche de route et la maintenance de route. La recherche de route se fait par inondation: un paquet de recherche est diffusé de proche en proche jusqu'à la destination. Au fur et à mesure, les identifiants des noeuds traversés sont ajoutés dans le paquet de recherche de route. Quand elle reçoit ce paquet, la destination sait donc déjà quel chemin il a emprunté, et obtient ainsi (en l'inversant) la route pour retourner à la source. A la réception, les paquets de recherche ayant suivi des chemins différents, la destination répond sur les chemins inverses, et la source aura ainsi finalement plusieurs chemins valides pour l'atteindre.

1.5.5 Protocole ZRP

ZRP (Zone Routing Protocol) est un protocole hybride qui définit pour chaque noeud mobile une zone (en terme de nombre de sauts) dans laquelle les paquets seront routés en utilisant une approche proactive. Cependant, les routes en dehors de cette zone sont découvertes en utilisant une approche réactive. Une zone de routage est alors définie pour chaque noeud mobile. Cette zone inclut les voisins se trouvant à une distance minimale (inférieure ou égale au rayon de la zone) du noeud en terme de nombre de sauts. L'espace de travail de ZRP est défini localement par le protocole de routage intra-zone IARP (IntrAzone Routing Protocol) et pour le reste du réseau par le protocole de routage inter-zone IERP (IntErzone Routing Protocol) (Figure 12).

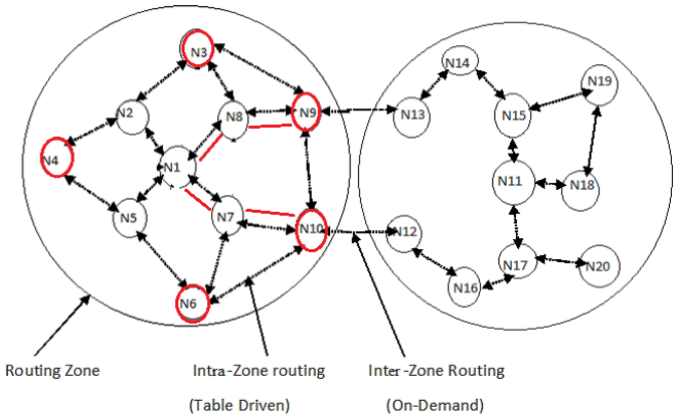

Figure 12: Utilisations des zones dans le protocole hybride ZRP [BHO 16]

1.6 Etude de cas d'un réseau dynamique : flotte de drones

Un type particulier des réseaux dynamiques sont les flottes de drones qui intéressent ces dernières années de plus en plus les scientifiques, à travers leurs domaines d'application variés, et le besoin de les faire coopérer pour une meilleure exécution de la mission. Cette coordination est réalisée par un échange régulier de messages dans un environnement mobile dynamique. Pour cela, il est judicieux de choisir le système de communication le mieux adapté aux caractéristiques des systèmes de drones coopératifs.

1.6.1 Domaines d'application

L'utilisation de véhicules aériens sans pilote (UAV) ou communément appelés drones dans différents domaines a augmenté ces dernières années. Leurs applications vont des situations d'urgence à la surveillance vidéo, en passant par la capture de données en direct à l'aide de capteurs embarqués, là où l'accès humain est difficile. Dans le domaine de la protection civile, une flotte de drones peut être une solution prometteuse car elle ne nécessite pas d'infrastructure coûteuse (câbles, tours, etc.). De plus, elle peut facilement être déployée pour aider aux opérations de sauvetage de personnes dans des situations d'urgence [LAS 20]. Un autre scénario d'utilisation des drones consiste à étendre la couverture 4G/5G. Mozaffari et al. [Moz 17] ont proposé des drones transportant des stations de base sans fil volantes comme complément pour un environnement 4G/5G afin de surmonter certains des défis des technologies existantes. Dans le domaine de l'agriculture, un drone peut utiliser ses capteurs pour recueillir des données pertinentes pour les agriculteurs. Par exemple, Rametta et Schembra [RAM 17] ont décrit une flotte de drones qui pourrait être utilisée comme un service de surveillance vidéo avec l'objectif de capturer des vidéos d'une large zone rurale, fournissant un service qui peut être utilisé par les agriculteurs afin de souscrire à un service de surveillance de leurs terres.

1.6.2 Description fonctionnelle d'un drone

Un drone désigne un appareil de vol, muni d'un autopilote embarqué et pouvant être télécommandé à distance depuis une station au sol. Il dispose de divers capteurs et module, et peut embarquer une charge utile Ces éléments participent à son autonomie et lui permettent d'exécuter sa mission (Figure 13) [MAX 17].

Dans la littérature, deux termes sont habituellement employés : UAV (Unmanned Arial Vehicule) ou drone. Les drones peuvent remplir diverses missions, historiquement dans le cadre d'applications militaires (surveillance d'une cible, renseignement, etc.), mais aussi, récemment, dans le cadre d'applications civiles (audiovisuel, industrie, agriculture). Par exemple, dans le domaine de l'audiovisuel, la réalisation d'un reportage a été pendant longtemps exécutée par des avions ou des hélicoptères pilotés. Non seulement ces missions peuvent être dangereuses et inadaptées aux pilotes, mais peuvent aussi engendrer des coûts conséquents. Les drones réalisent actuellement ces tâches en s'adaptant aux différents types et conditions de ces missions.

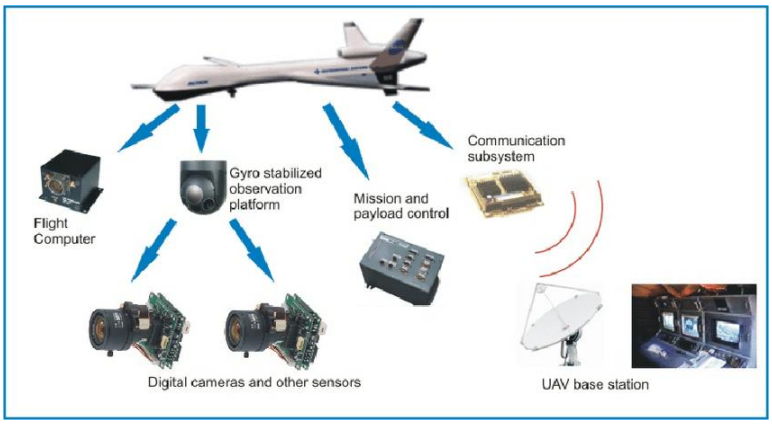

Figure 13: Eléments composant un drone [PAS 06]

Les drones peuvent être classés, en fonction de leur type de mouvement en deux types (Figure 14): les drones à voilures fixes et les drones multirotors. Une autre classification se base sur l'altitude à laquelle le drone opère [MOZ 19].

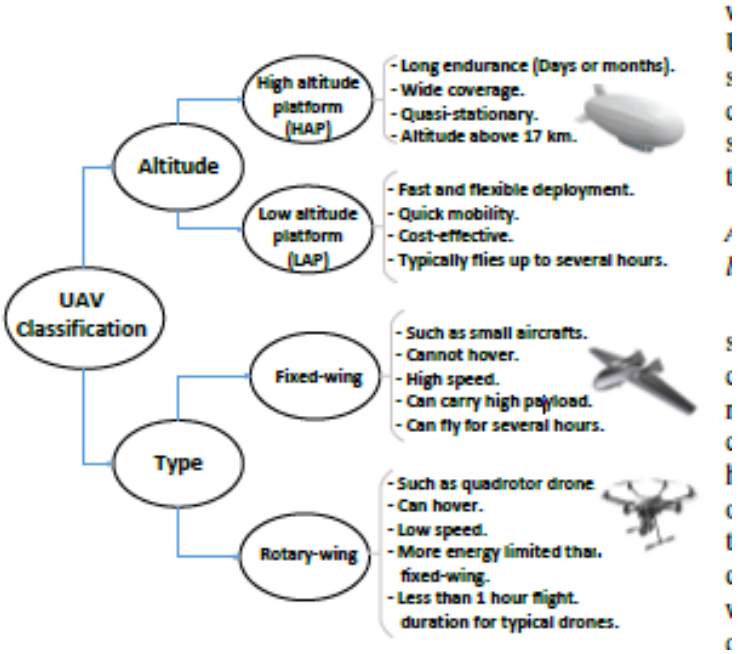

Figure 14 : Classification des drones [MOZ 19]

- Les drones multirotors (Figure 15): peuvent être des quadricoptères, hexacoptères, octocoptères ou décacoptères. Ce type de drones est souvent utilisé pour des vols stationnaires ou à très faible vitesse, ce qui les rend particulièrement adaptés à la prise de vue aérienne, photo ou vidéo [MAX 17].
- Les drones à voilure fixe: (Figure 16): ils permettent de couvrir de longues distances ou d'atteindre de hautes altitudes. Ils sont plutôt dédiés aux applications topographiques ou militaires sur de grandes surfaces [MAX 17].

Figure 15: Drone multirotors

Figure 16: Drone à voilure fixe

Charge utile

La charge utile d'un drone est l'ensemble des systèmes embarqués qui lui permettent de réaliser sa mission, par exemple, un appareil photo, une caméra vidéo, une caméra multi spectrale, une caméra thermique, des sondes ou tout autre type de capteurs (mesurant, entre autres, des paramètres dans l'air, tels que la température, la pression ou encore le niveau de pollution). Grâce à sa charge utile, un système de drones peut être utilisé pour inspecter une zone donnée ou relevés des données utiles de la zone à couvrir [MAX 17].

Station au sol

Les drones reçoivent les commandes de contrôle depuis une station au sol appelée GCS (Ground Control Station). Ils renvoient aussi vers cette station les informations concernant les conditions de vol (position, vitesse, etc.) et les données acquises par les capteurs. Ces données permettent à l'opérateur au sol de surveiller le vol et d'intervenir potentiellement sur le drone en lui envoyant des commandes [MAX 17].

1.6.3 Architectures de Communication

La Figure 17 montres les différents modèles de communication utilisée par une flotte de drone pour communiquer avec la station au sol. Ces modèles sont les suivants:

Architecture de communication centralisée

Une architecture de communication centralisée est caractérisée par un lien sans fil direct entre un nœud centralisé (par exemple, la station sol) et les drones aux alentours. Dans cette architecture, chaque drone est directement connecté à la station sol pour transmettre les données de la charge utile et pour recevoir le flux de commande et de contrôle. Les drones ne sont pas directement connectés entre eux, ce qui nécessite d'envoyer les informations entre drones voisins en passant par la station sol. Dans ce cas, la station sol agit comme un nœud relais [MAX 17].

Architecture de communication par satellite

Un autre type d'architecture de communication centralisée, envisageable pour établir une communication entre les différents drones, est le déploiement d'un satellite de communication. Dans cette configuration, le satellite fonctionne comme un relais de communication. Ses antennes de réception reçoivent les signaux émis depuis la station sol ; ces signaux sont par la suite transposés en fréquence et amplifiés avant d'être retransmis vers les drones. Il existe deux types de satellites utilisables : le satellite géostationnaire et le satellite orbital. Le satellite géostationnaire est situé dans le plan équatorial. Il tourne à la même vitesse et dans le même sens que la terre ; sa trajectoire est ainsi fixe au-dessus d'un point au sol. Le second est un satellite qui couvre des zones géographiques différentes. L'utilisation des satellites présente l'avantage d'assurer une couverture plus efficace [MAX 17].

Architecture de communication Ad hoc

Un réseau Ad Hoc de drones, connu sous la dénomination anglaise *UAV ad hoc NETwork* (UAANET) ou encore *Flying Ad hoc NETwork* (FANET), est une sous-catégorie des réseaux mobile MANET. Il s'agit du déploiement d'une flotte de drones à travers un réseau Ad Hoc sans fil. Les drones collaborent entre eux et avec la(les) station(s) sol pour échanger des données qui peuvent être des données propres au réseau FANET (des paquets de contrôle) ou des données propres à la mission pour laquelle ils ont été déployés.

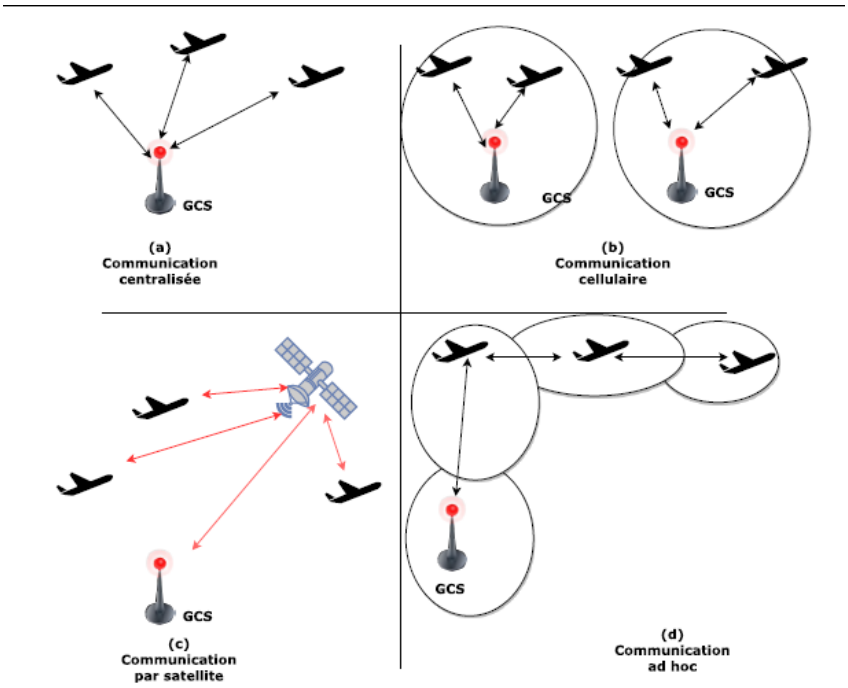

Figure 17: Architectures de communication des flottes de drones [Max 17]

1.6.4 Challenges dans les flottes UAV

Eviter les Obstacles

Les drones sont sujets à des collisions avec des obstacles mobiles ou stationnaires. C'est l'un des principaux risques liés au vol des drones autonomes. De nombreuses méthodes d'évitement des collisions ont été proposées. Plus précisément, les principales approches d'évitement des collisions, sont [AHM 21] : l'approche géométrique, l'approche de la planification de la trajectoire et l'approche basée sur la vision. L'approche géométrique est une méthode utilisée pour éviter les collisions entre deux UAV sur la base d'équations géométriques, ainsi que pour décider de la direction des UAV dans la zone à couvrir. La planification de la trajectoire est une approche basée sur une grille. On utilise des algorithmes de planification de trajectoire avec des méthodes de recherche de graphe. Cette approche utilise une carte de vol qui est divisée en une grille sans collision obtenue à l'aide d'un l'algorithme de recherche de graphe. La détection des obstacles par la vision se fait à l'aide de petites caméras sur les drones. Les images capturées permettent au drone de manœuvrer autour de l'obstacle sans collision. La principale faiblesse de cette méthode est la complexité et le temps de calcul associé.

Challenges Réseaux [LAS 21]

Au niveau de la couche physique du réseau, le modèle de propagation radio et le type d'antenne utilisé dans la communication entre nœuds ont été initialement conçues pour un environnement 2D. Donc, Il devrait y avoir une conception de la couche physique en 3D. La qualité du lien peut être modifiée en raison de la mobilité élevée des drones, c'est pourquoi dans la couche MAC, les antennes omnidirectionnelles ne répondent pas aux exigences des UAV. Par conséquent, des antennes directionnelles peuvent donc être utilisées pour surmonter ce problème.

Au niveau de la couche réseau, une question se pose par rapport à l'efficacité de l'algorithme de routage lors de la mobilité des drones et les changements fréquents dans le réseau. Il s'agit d'une question importante avant de choisir un protocole de routage. Ceci afin d'assurer un mécanisme de protocole de routage efficace pour assurer une mise à jour rapide dans la table de routage lorsque la topologie change fréquemment.

Gestion de la flotte

La partie gestion de la flotte se concentre sur la configuration optimale de la formation d'une flotte (positionnement, vitesse, hauteur) y compris la prise de décision en cas de collisions ou d'établissement des liaisons. Les techniques de gestion de flotte peuvent offrir différents niveaux d'automatisation allant de vols entièrement automatisés (sans intervention humaine) à des vols entièrement pilotés par l'homme. Les techniques de gestion de flotte peuvent être classées en schémas centralisés et décentralisés. Dans le schéma centralisé, un gestionnaire de formation peut être l'un des véhicules aériens de la flotte ou une station au sol. Une station au sol, agit comme un superviseur pour tous les véhicules aériens et gère leur topologie. Dans le schéma décentralisé, chaque véhicule aérien dispose d'une certaine liberté dans la prise de décision, tandis que l'ensemble de la formation doit être capable de se reconfigurer, de prendre des décisions et d'atteindre les objectifs de la mission. Ce schéma est économe en énergie et présente des temps de réaction réduits, bien qu'il puisse produire des décisions conflictuelles, mettant en danger la sécurité de la mission.

1.6.5 Modèles de fonctionnement d'une flotte de drones

Canaux de communication

Dans un système de flotte de drones, il peut y avoir différents canaux de communication (Figure 18). Un canal **Drone-Station de Contrôle** à travers lequel l'UAV peut envoyer ou obtenir des données relatives au vol et à la mission depuis la Station de Contrôle. Le deuxième canal de communication est un le canal **Drone-Drone**. Ce canal est utilisé lorsque certains UAV sont éloignés de la Station de Contrôle, ou bien que les informations doivent être transmises en chaîne, depuis la Station de Contrôle puis d'un drone à un autre jusqu'au drone cible. Le troisième canal possible est Drone-Infrastructure, qu'on peut trouver dans certaines applications telles que les réseaux cellulaires. Dans ce scenario, les drones sont connectes aux réseaux cellulaires pour servir de relais par exemple.

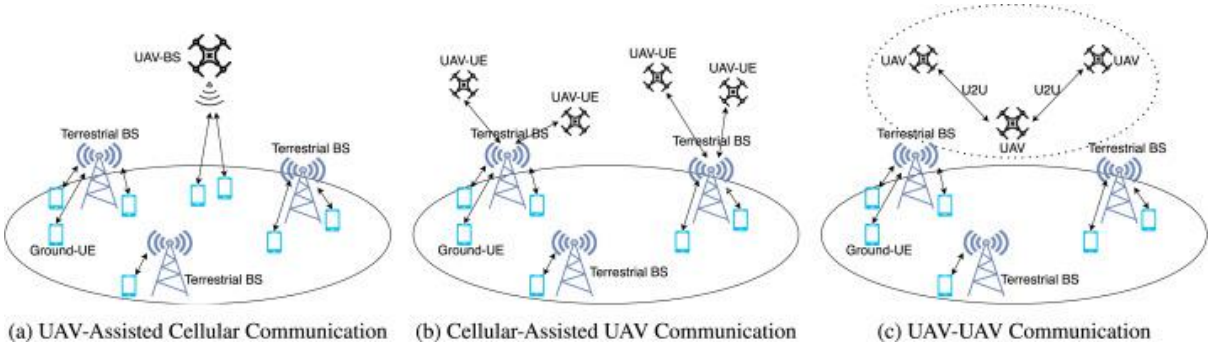

Figure 18: Canaux de communication des flottes de drones

Modèles de Mobilité

Le modèle de mobilités d'une flotte de drones est différent de celui des nœuds MANET. En effet, les nœuds MANET se déplacent souvent sur une zone se trouvant, dans la plupart des cas, au sol. Par exemple, pour les réseaux ad hoc véhiculaires VANET (Vehicular Ad hoc NETwork), les nœuds se déplacent sur la route ou l'autoroute. En revanche, les drones tout comme les avions, se déplacent dans le ciel. En outre, le réseau MANET utilise généralement un modèle de mobilité *random waypoint* dans lequel la direction et la vitesse des nœuds sont choisies au hasard. Pour le réseau VANET, le modèle de mobilité est hautement prévisible. En ce qui concerne le réseau UAV, le modèle de mobilité dépend généralement de divers paramètres. Il est le plus souvent prévisible, mais, dans la majorité des cas, il est dynamiquement modifié à cause de la vitesse des drones, des conditions climatiques et de nombreux autres paramètres géographiques et topographiques. En effet, la plupart des applications de flottes de drones fonctionnent avec un modèle de trajectoire bien prédéfini (Figure 19). Néanmoins, comme l'environnement est dynamique, le plan de vol est souvent amené à être recalculé par le système autopilotage.

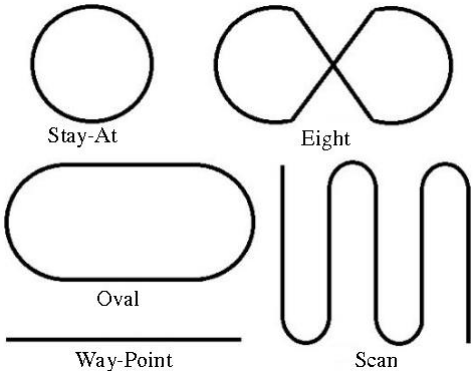

Figure 19: Modèles de mobilité des flottes de drones

Modèle de Coopération

Dans une architecture décentralisée, les drones doivent coopérer explicitement entre eux à différents niveaux pour atteindre les objectifs de la mission, partager des tâches ou prendre des décisions collectives : Les drones doivent donc :

- observer leur environnement,
- évaluer leurs propres observations ainsi que les informations reçues des autres drones,
- et en tirer des conclusions, et agir de la manière la plus efficace.

Les actions possibles sont déterminées par les capacités des drones et l'objectif du système en sa globalité. Habituellement, un bloc de coordination sur chaque drone est nécessaire pour utiliser les observations locales et les observations des autres drones. En bref, il est nécessaire de calculer les trajectoires des véhicules et prendre des décisions sur la façon de répartir les tâches pour atteindre un objectif commun. La coordination peut signifier la réalisation et le maintien de la formation, mais aussi la distribution des tâches entre les véhicules de manière auto-organisée

La coopération dans le contexte des drones consiste à réaliser collectivement une tâche ou à échanger des informations clés sur le réseau. Trois modèles ont été définis [YAN 17] [LAG 18] pour permettre aux drones de coopérer:

- Centralisé : Dans ce modèle de collaboration, il y a un puissant drone maître dans la flotte qui recueille toutes les informations provenant des drones individuels et aide la flotte au traitement et à se mettre d'accord sur les décisions.
- Décentralisé : Dans ce modèle de collaboration, il n'y a pas de drone maître unique, mais un petit sous-ensemble de drones puissants qui collectent les flux de leurs drones voisins, puis ces drones puissants effectuent l'apprentissage, l'évaluation et la décision en collaboration.
- Distribué : Dans ce modèle, chaque participant de la flotte a un rôle plus ou moins égal dans tous les processus d'apprentissage, d'évaluation et de prise de décision en collaboration. On peut noter que la charge d'activité est distribuée parmi la population en fonction de leurs capacités individuelles, de leurs performances actuelles et de leurs ressources énergétiques.

Les recherches basées sur des solutions coopératives ont différents objectifs ou problèmes à résoudre. Certaines se sont concentrées sur la collaboration des drones pour accomplir une tâche commune à la flotte. D'autres l'ont utilisé pour résoudre des problèmes tels que l'évitement des collisions. Et d'autres ont travaillé sur la manière d'accomplir l'agrégation des données vers la station de contrôle au sol.

1.7 Conclusion

Les réseaux dynamiques restent un sujet de recherche d’actualité vu les divers domaines d’application possibles. Nous avons analysé dans ce chapitre ces réseaux en dégageant leurs caractéristiques, intérêts et limitations. Nous avons ensuite présenté les protocoles d’accès au réseau et les protocoles de routage qui lui sont associés.

Les réseaux de flottes de drones prennent de plus en plus un intérêt vu les nouvelles opportunités d’application qui lui sont associées. La communication entre drones en mode Ad Hoc présente des défis plus importants en raison de la vitesse élevée des nœuds mobiles, et des changements fréquents de topologie qui peuvent avoir un impact sur l’efficacité du routage.

Pour la suite, nous nous focalisons sur les aspects Sécurité et QoS dans les réseaux dynamiques en général, et des flottes de drones en particulier, en décrivant l’état actuel des travaux de recherche.

2. Sécurité des réseaux dynamiques

2.1 Introduction

Dans un réseau dynamique, nous devons fournir un mécanisme de communication fiable et sécurisé aux nœuds du réseau. Il n'est pas possible de prédire le moment où ces nœuds quitteront le réseau ou le moment où ils seront associés au réseau de nouveau. Ainsi, la nature dynamique du réseau fait que d'une part, des nœuds compromis ou malveillant peuvent exister dans le réseau, et d'autre part, les paquets traversent un support vulnérable, vu la nature broadcast du réseau.

Ce deuxième chapitre est consacré à l'étude de la problématique de la sécurité dans les réseaux dynamiques. Dans un premier temps, nous allons examiner les menaces de sécurité existantes et leurs classifications dans la littérature. Nous décrivons ensuite les attaques spécifiques au routage et les solutions associées tel que l'authentification, le cryptage et les approches basées sur la réputation et le crédit. Nous terminons ce chapitre en examinant la sécurité dans le contexte d'une flotte de drones et les travaux de recherche associés.

2.2 Problématique de la sécurité dans les réseaux dynamiques

Les réseaux dynamiques sont vulnérables aux attaques de sécurité car la transmission se fait sur un support ouvert. Il n'y a pas de serveur centralisé, de station de surveillance ou d'administrateur dans le réseau, et les nœuds ne cessent de le joindre et de le quitter. Aussi, les réseaux dynamiques doivent crypter les communications de signalisation qui représente la partie critique de l'infrastructure du réseau. Les réseaux câblés sont généralement sécurisés à l'aide de pare-feu et de dispositifs de cryptage et de surveillance en utilisant par exemple un proxy, un système de détection d'intrusion, etc. Cependant, ces dispositifs ne sont pas disponibles dans le cadre des réseaux dynamiques. D'un autre cote, les techniques de détection d'intrusion utilisées dans les réseaux câblés ne sont pas efficaces car des nœuds inconnus peuvent rejoindre le réseau à un moment donné. Les algorithmes de la cryptographie asymétrique doivent être modifiés et personnalisés pour être utilisables au sein des réseaux dynamiques. L'infrastructure à clé publique (PKI) par exemple est difficile à mettre en œuvre dans un réseau dynamique car il n'y a pas de connexion en permanence aux réseaux externe pour l'authentification par une autorité centrale de certification. L'adhésion de nouveaux nœuds à un endroit éloigné rend également difficile la distribution des clés aux autres nœuds du réseau en utilisant un canal sécurisé.

Le service du routage de son coté, peut être une cible d'attaques en raison de son importance. Un nœud compromis ou un nœud malveillant peut dissimuler des changements dans le réseau ou générer des messages erronés et propage ainsi une erreur aux autres nœuds, créant une représentation inexacte du réseau et conduit à une attaque Déni de Service (DoS).

La densité des nœuds d'un réseau dynamique est un autre facteur important mais généralement ignorés dans la conception des mécanismes de sécurité. Il existe quelques facteurs critiques tels que la puissance de transmission, le nombre de canaux utilisés par chaque nœud, et la vitesse de déplacement du nœud qui sont aussi à prendre en compte lors de la conception des protocoles de sécurité.

2.2.1 Classifications des menaces

La Figure 20 résume les menaces sur les réseaux dynamiques qu'on retrouve dans la littérature. Nous distinguons deux classes d'attaques sur ces réseaux: les attaques actives et les attaques passives. Ces attaques sont ensuite classifiées selon la couche du modèle OSI auxquelles ils appartiennent. Une autre classification se base sur la source de l'attaque si elle provient d'une source externe ou une source interne au réseau déjà compromis.

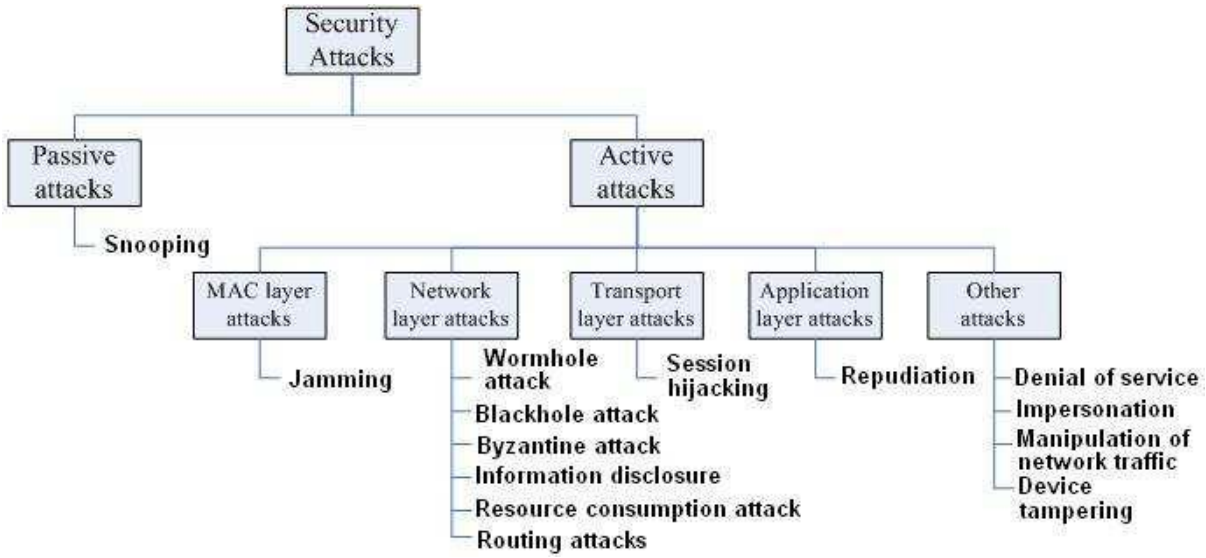

Figure 20: Classification des attaques sur les réseaux dynamiques

Attaques actives vs passives

Lors d'une attaque active, l'attaquant a accès au canal de transmission de manière à pouvoir modifier les données ou transmettre ses propres données de manière "cachée". Le déni de service (DoS), la modification, la rediffusion et l'injection sont les méthodes les plus courantes des attaques actives. Dans une attaque passive, l'attaquant ne peut qu'écouter le trafic du réseau ou accumuler des données à partir de celui-ci, mais les données ne sont pas modifiées. Ceci afin de préparer par la suite une attaque active sur la base des données collectées. L'écoute, l'analyse du trafic, et l'usurpation d'identité sont des formes générales d'attaques passives [SEV 11].

Attaques internes vs externes

Dans ce modèle, on considère deux types deux nœuds : les "**insiders**" a qui ont fait confiance et les "**outsiders**" à qui on ne fait pas confiance (Figure 21). En présence d'un protocole de sécurité efficace, les attaques des outsiders sont réduites, du fait que l'attaquant n'est pas autorisé à participer au réseau. Les techniques de cryptographie et d'authentification protègent l'accès au réseau de ce type d'attaque. Cependant, l'attaquant peut uniquement déclencher des attaques passives telles que l'écoute du canal par exemple.

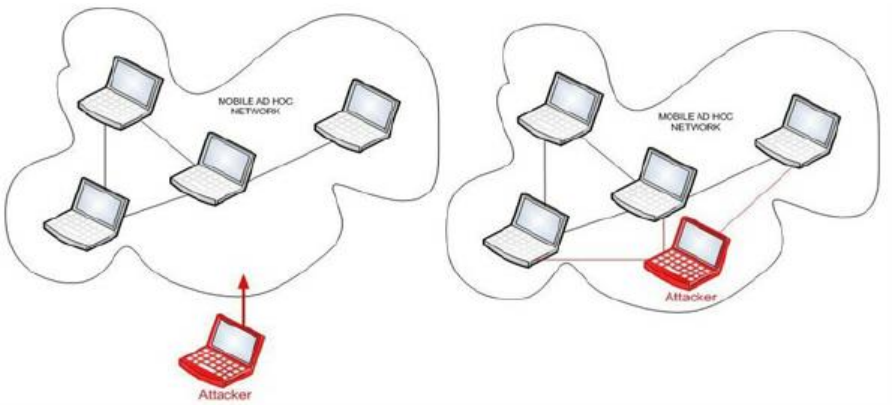

Figure 21: Attaque externe vs attaque interne [GOU 13]

Dans le cas d'une attaque qui se fait d'un **insider** (nœud déjà compromis), un sérieux problème de sécurité se pose. Les auteurs dans [GOK 11] décrivent quatre menaces clés découlant du manque de sécurité à cause d'un nœud compromis:

- Suppression des nœuds du réseau
- Inspection des nœuds pour récupérer les clés de cryptage, les tables de routage ou du trafic transitant par le nœud.
- Modification de l'état interne d'un nœud
- Clonage et déploiement de nœuds compromis

Ces menaces sont particulièrement graves, car elles exposent le réseau à une éventuelle attaque hostile de la part d'un nœud déjà compromis. Ces nœuds peuvent accéder aux clés de cryptage utilisées par le protocole de sécurité et permettent ainsi à l'adversaire hostile de participer au réseau. Cela ouvre la possibilité à des attaques plus avancées à un stade ultérieur, lorsque les nœuds sous le contrôle de l'adversaire s'associent pour porter atteinte à l'intégrité du réseau.

Une solution efficace aux problèmes posés par ces attaques reste un sujet de recherche ouvert. Il est donc nécessaire de s'appuyer sur des mécanismes efficaces pour, par exemple, supprimer en toute sécurité les clés cryptographiques en cas ou on suspecte un accès non autorisé à l'équipement. Le protocole de sécurité peut implémenter un mécanisme de révocation rapide des informations d'identification dans ce cas.

2.2.2 Synthèse des attaques et des solutions

Le Tableau 1 liste les attaques les plus populaires sur les réseaux dynamiques et les contre-mesures correspondantes [PIE 14] [NOU 19]:

Couche	Type de l'attaque	Détail de l'attaque	Contre-Mesures
Physique	Brouillage du signal	Perturbe la bonne réception des paquets	Saut de Fréquences
Liaison de données	Nœuds égoïstes	Supprimer/Ignorer le routage des paquets	Systèmes de réputation
	Comportement malicieux	Perturber les opérations de routage	Systèmes de réputation
	Analyse du trafic	Obtenir des informations sur la topologie	Cryptographie
Réseau	Trou noir	Faux messages de routage	Routage Authentifié
	Trou de ver	Tunnel entre les nœuds malicieux	Packets Leashes
	Attaque de bousculade (Rush)	Perturber le processus de découverte des routes	Routage Authentifié
Transport	Vol de session	Spoofer l'adresse IP de la victime	Authentification
	Inondation avec des messages SYN	Ouvrir multiples sessions TCP avec la victime	Cryptographie
Application	Code malicieux	Injecter des virus et vers	Protéger le système d'exploitation
	Attaque de Répudiation	Nier la participation à une partie de la communication	Hashage

Tableau 1: Synthèse des attaques dans la littérature et les contre-mesures

2.3 Attaques contre le routage et la sélection de chemin

Les objectifs des protocoles de sécurité sont d'assurer la confidentialité, l'intégrité et l'authenticité du trafic réseau, tout en préservant la disponibilité des communications. Les attaques visant à compromettre l'intégrité du routage constituent une menace importante et peuvent entraîner une perte de disponibilité à l'échelle du réseau. Un adversaire malveillant peut perturber le processus de découverte de route pour affecter les métriques de routage, introduire des détours gratuits, tenter de créer des boucles ou inonder les tables de routage. Les sections suivantes décrivent certaines menaces qui pèsent sur l'intégrité des routes d'un réseau dynamique.

2.3.1 Attaque de bousculade (Rush Attack)

Il s'agit d'une attaque contre les protocoles de routage réactifs. L'attaque influence le processus de découverte d'itinéraire et augmente la probabilité qu'un nœud hostile soit inclus dans un itinéraire donné. Cela permet à l'adversaire d'effectuer une analyse du trafic, de mener d'autres attaques et d'empêcher l'établissement de routes via d'autres nœuds. Cette attaque à partir du nœud compromis transmet rapidement les messages de demande d'itinéraire pour s'assurer que les messages RREQ(Route Request Packet) de ce nœud arrivent plus tôt que ceux des autres nœuds (Figure 22). Le mécanisme de suppression des doublons garantit que les demandes en double arrivant plus tard aux autres nœuds seront ignorées.

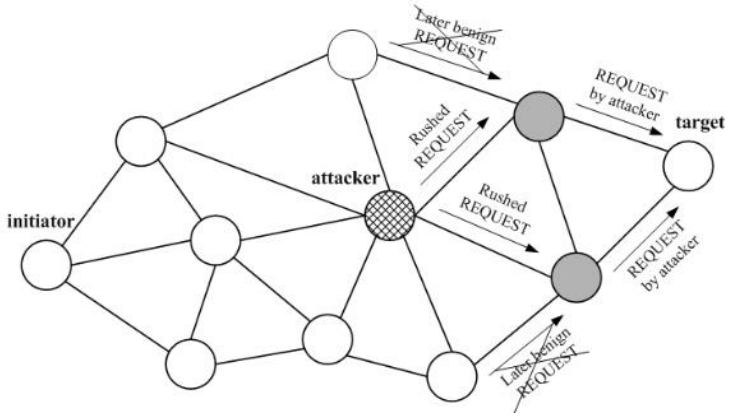

Figure 22: Messages RREQ ignorés dans l'attaque Rush

2.3.2 Trous Gris et Trous Noirs (Black Hole et Gray Hole)

Un trou noir est un nœud qui annonce sa volonté de prendre part à une route mais qui ne transmet aucun trafic (figure 23). Comme il s'agit d'une attaque contre la transmission de messages et non contre la découverte de routes, cette attaque s'applique aussi bien aux protocoles de routage ou de sélection de chemins proactifs et réactifs. Les trous noirs n'informent pas l'expéditeur de leur incapacité à transmettre des données, ce qui compromet la propriété normale d'auto-organisation d'un réseau dynamique. Le trou gris est une variante de l'attaque par trou noir dans laquelle le nœud compromis décide de manière conditionnelle du trafic qu'il transmettra et de celui qu'il ne transmettra pas. En conséquence, il peut être très difficile à découvrir.

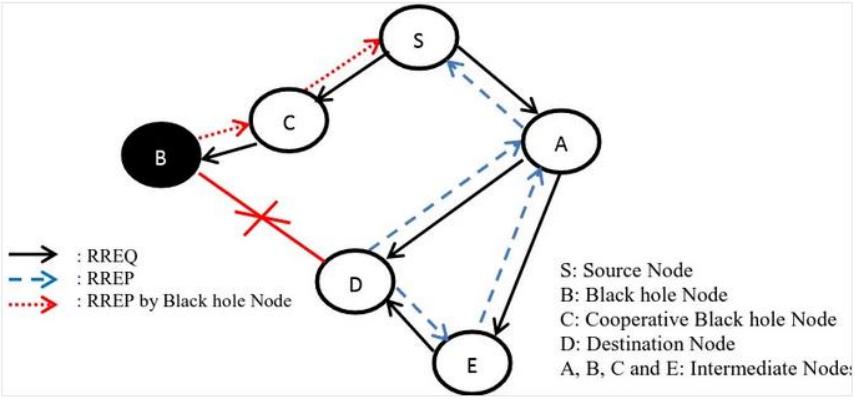

Figure 23: Message RREP non transmis par le trou noir

2.3.3 Trous de ver (Wormhole)

L'attaque par trou de ver constitue une menace pour l'intégrité du routage du réseau. Un trou de ver est une attaque Man In The Middle spécialisée dans laquelle l'adversaire connecte deux régions du réseau autrement distantes. À première vue, un trou de ver semble bénéfique car il optimise le flux de trafic à travers le maillage, mais il le fait en utilisant un lien qui est sous le contrôle total de l'adversaire hostile. La présence d'un trou de ver modifie la topologie du réseau et compromet ainsi les algorithmes de routage du réseau. Les routes passant par le trou de ver bénéficient d'un nombre de sauts et d'autres mesures de qualité de liens inférieurs à ceux des routes légitimes et augmentent ainsi la probabilité que le trafic soit acheminé via le trou de ver.

Dans la Figure 24, un nœud malveillant (1) situé dans une partie du réseau entend le paquet RREQ. Il l'encapsule et l'envoi vers un second nœud complice (8) situé à une un emplacement distant proche de la destination. Le nœud 8 rediffuse le paquet RREQ à son tour. Les voisins du nœud (8) reçoivent la RREQ et abandonnent toutes les autres demandes RREQ légitimes qui pourraient arriver plus tard des autres nœuds. Le résultat est donc un tunnel qui se créer entre les deux nœuds complices, et cela empêche de découvrir des chemins légitimes qui sont à plus de deux sauts.

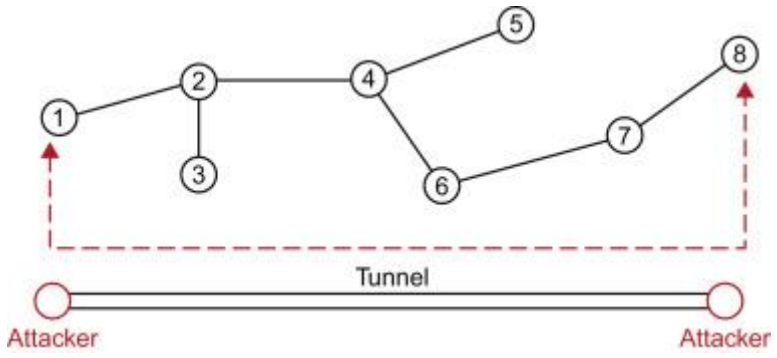

Figure 24: Création d'un tunnel lors de l'attaque par trou de ver

2.3.4 Solutions contre les attaques sur le routage et la sélection de chemin

Plusieurs mécanismes de base ont été proposés dans la littérature pour assurer une sécurité du routage dans les réseaux dynamiques. Il s'agit notamment de l'application des techniques tel que la cryptographie, la découverte et à la maintenance des itinéraires, l'utilisation de systèmes basés sur la réputation pour choisir les routes de confiance et de l'utilisation des informations sur la localisation et la distance. Ces techniques sont décrites ci-dessous.

Routage authentifié

Pour faire face aux menaces sur l'intégrité des routes, un certain nombre de protocoles de routage sécurisés ont été proposés. Ces protocoles utilisent des approches basées sur la cryptographie pour prévenir de nombreuses attaques. L'utilisation de la cryptographie permet d'établir l'authenticité et l'intégrité des messages de routage. La propriété de non-répudiation permet d'identifier sans ambiguïté les nœuds fautifs. Les techniques cryptographiques utilisent la cryptographie symétrique ou asymétrique pour signer les messages. Cette dernière est de plusieurs ordres de grandeur plus sure que la première, mais elle n'est pas souhaitable pour les gros volumes de trafic. Un exemple peut être tiré du protocole ARAN (Authenticated Routing for *Reseau dynamique* Networks) [SAN 05] dans lequel les nœuds du réseau à chaque saut doivent calculer et ajouter une signature numérique au message RREP/RREQ. Dans ce protocole, la taille du message RREP/RREQ augmente en proportion directe du nombre de sauts et la validation du message exige que le vérificateur obtienne des certificats pour tous les nœuds du réseau le long de la route. Certains schémas évitent cette surcharge et signent les messages uniquement à leur origine, mais dans ces cas, ils sont incapables de détecter les modifications apportées par les nœuds intermédiaires.

La cryptographie à clé publique, étant coûteuse en calculs, des approches moins gourmandes ont été proposé. L'une des plus courantes est l'utilisation de chaînes de hachage, introduite dans le protocole SEAD (Secure *Ad Hoc* On-Demand Distance Vector) [ALM 18]. Les chaînes de hachage sont efficaces et offrent des garanties d'authenticité et d'intégrité similaires à celles des signatures numériques, mais à un coût de calcul inférieur.

Modification du protocole de routage

L'idée de cette solution est de modifier la logique du fonctionnement du protocole de routage afin de contrer certaines attaques. Par exemple, l'utilisation d'un protocole sécurisé de découverte des voisins ou bien une modification de la logique de découverte de route. Voici des exemples de quelques techniques qui utilisent cette approche:

- **Détection sécurisée des voisins:** Cette technique permet à l'expéditeur et au destinataire d'une demande de route (Route Request) de vérifier que l'autre partie se trouve à l'intérieur de la zone de sécurité. Ceci empêche un attaquant d'introduire des nœuds (qui ne sont pas dans la portée de transmission maximale) comme voisins, et prétendre qu'il est voisin d'un autre nœud, sans pouvoir entendre des paquets de ce nœud.
- **Vérification des routes:** Chaque nœud vérifie que dans la demande, toutes les étapes de détection de voisins ont été effectuées entre toute paire de nœuds adjacents.
- **Randomize Message Forwarding:** la technique de sélection aléatoire minimise le risque que qu'un adversaire pressé puisse dominer toutes les routes. Chaque nœud doit recueillir le plus grand nombre possible de message avant de les transmettre. Cette approche fournit une défense contre l'attaque de bousculade (Rush Attack).

Exemple de solution : Solution contre l'attaque Trou de Ver

Pour contrer les attaques sur le routage, la plupart des solutions proposent de modifier le fonctionnement du protocole de routage. Prenons l'exemple de l'attaque Trou de Ver. Hu et al [HU 03] ont proposé l'utilisation de paquets leashes comme défense contre ces attaques. Les paquets leashes sont destinés à limiter le déplacement d'un paquet dans une zone géographique étroitement définie. Malgré le préfixe "paquet", il s'agit d'un mécanisme de la couche MAC car il s'applique sur chaque saut. Les paquets leashes sont de deux types :

- *Géographique :* L'expéditeur ajoute son emplacement au paquet sortant. Le récepteur peut utiliser cette position pour calculer un vecteur de distance entre l'expéditeur et sa propre position.
- *Temporel :* dans lequel l'expéditeur ajoute un timepstamp indiquant l'heure de transmission du paquet (alternativement, le temps maximum auquel le paquet sera valide). Le récepteur calcule la différence entre le timpestamp du paquet et l'heure réelle d'arrivée du paquet.

Compte tenu de cette différence de temps et d'une estimation de la vitesse de déplacement du signal, le récepteur peut calculer la distance qui le sépare de l'expéditeur. Il est important que les paquets leashes ne puissent pas être simplement modifiés par l'adversaire qui mène une attaque par trou de ver. Les informations doit être protégée par un protocole de sécurité pour garantir leurs authenticité. Pour les leashes géographiques et temporelles, si le vecteur de distance entre l'émetteur et le récepteur est trop grand, le récepteur suppose que c'est parce qu'un adversaire hostile mène une attaque par trou de ver. Dans ce cas, le nœud peut prendre des mesures correctives telles que l'invalidation des entrées de la table de routage qui traversent le trou de ver, la mise sur liste noire du nœud atteint par le trou de ver et la recherche d'itinéraires via des nœuds qui ne sont pas sur liste noire. La condition nécessaire pour une utilisation réussie des paquets leashes est donc de disposer de données géographiques fiables ou d'horloges synchronisées avec précision pour limiter le déplacement d'un paquet dans une zone géographique définie.

2.4 Solutions basée sur le cryptage et la gestion des échanges des clés

La gestion des clés est un mécanisme permettant d'assurer la sécurité des services réseau basés sur une solution de cryptographie. Dans le mécanisme de cryptographie symétrique, les deux côtés de la communication utilisent la même clé pour le cryptage et le décryptage. La cryptographie symétrique présente des avantages évidents en termes de vitesse de calcul et de consommation d'énergie Par contre, la distribution de la clé a toujours été un défi. La conception d'un schéma de distribution de clés hautement efficace et flexible est toujours un point clé de la recherche. Dans la pratique, choisir quel type d'algorithmes cryptographiques dépend de la capacité de calcul et de communication des nœuds, donc, en plus de l'amélioration de l'algorithme cryptographique, l'amélioration des performances du matériel est nécessaire aussi. En travaillant sur les deux axes, les chercheurs peuvent mieux assurer la sécurité des réseaux dynamique. Par contre, Un algorithme de cryptographie asymétrique, tel que RSA par exemple, est gourmand en termes de ressources et n'est donc pas adapté aux réseaux dynamiques.

Cependant, ces dernières années, les recherches ont montré que si on choisit l'algorithme et les paramètres appropriés, et on optimise ou réduise la consommation d'énergie, les algorithmes de cryptographie à clé publique peuvent également être utilisés [XIA 16]. Principalement, la littérature porte sur la recherche et l'amélioration des algorithmes RSA et l'utilisation des courbes elliptiques (ECC).

2.4.1 Infrastructure à clé publique (PKI ou Public Key Infrastructure)

L'objectif d'une infrastructure de gestion des clés ou PKI est de générer, distribuer, installer, mettre à jour, révoquer et stocker les clés associées. Une entité tierce de confiance doit exister, à laquelle les parties communicantes font confiance pour fournir le service de gestion des clés dans le réseau. Dans une Infrastructure à clé publique, si deux utilisateurs souhaitent communiquer, ils doivent échanger leurs clés publiques de manière authentique, ce qui nécessite la distribution initiale de clés publiques. Cependant, la clé privée n'est détenue que par son propriétaire. Chaque nœud génère sa clé privée à l'aide d'un algorithme particulier en utilisant la valeur reçue de l'entité de confiance. L'autorité de certification est responsable de la distribution des clés ainsi que de la révocation de la clé au cas où la clé a été compromit (Figure 25).

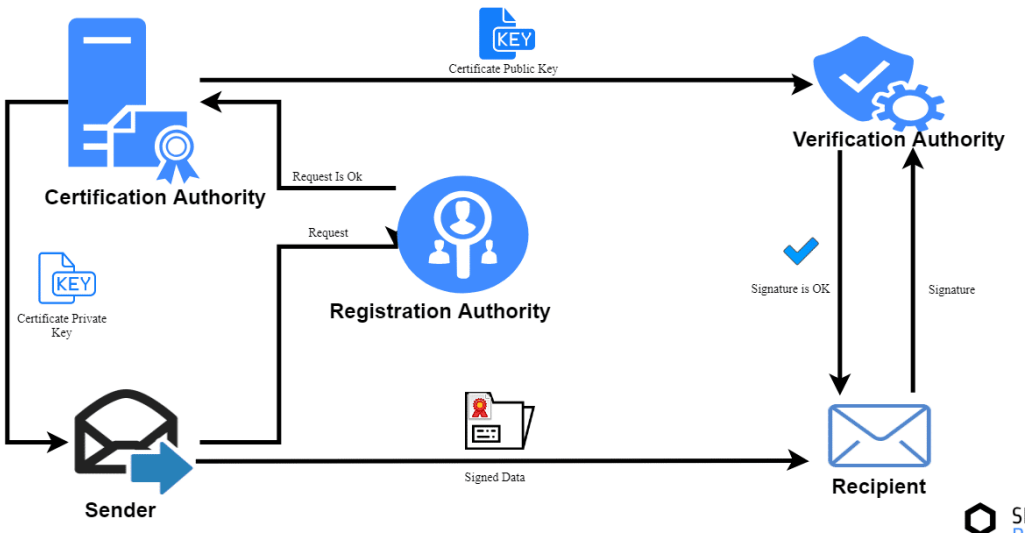

Figure 25: Architecture d'une infrastructure PKI [JET 22]

Une PKI a été mis en place pour une infrastructure Internet filaire. Avec l'avènement des réseaux sans fil, en général, et des réseaux dynamiques, plus spécifiquement, on a continué à les utiliser sans modifier l'infrastructure ou le protocole. De nombreux schémas ont été proposés dans une PKI pour réduire le délai d'obtention d'une réponse du serveur, distribuer les serveurs pour améliorer la fiabilité, équilibrer la charge et mettre en œuvre des serveurs tiers de confiance. La plupart d'entre eux, cependant, ne sont pas appropriés pour être utilisées dans les réseaux dynamiques, car ces solutions ne sont pas conçues pour eux.

La grande mobilité des nœuds dans les réseaux dynamiques est également un sujet de préoccupation en termes d'authentification et de connectivité, ce qui n'est pas si fréquent dans les réseaux câblés. Par exemple, pour obtenir une liste de révocation dans une PKI standard, chaque nœud, à la réception de chaque message signé, doit contacter individuellement le serveur central ou distribué de l'autorité de certification disponible sur le réseau pour récupérer la liste de révocation. Le serveur de l'autorité de certification peut également transmettre la liste de révocation et ses mises à jour à chaque révocation ou suspension de clé directement à tous les nœuds du réseau dynamique par l'intermédiaire d'autres stations, ce qui entraîne une inondation et une surcharge de communication. Les systèmes existants ne comportent pas de protocole optimisé pour être utilisé dans un réseau dynamique [MIS 11].

2.4.2 Gestion distribuée des clés publiques

Dans ce schéma, il n'y a pas de gestion centralisée de la distribution des clés et il n'est pas nécessaire d'avoir une autorité de confiance. L'utilisateur peut créer, distribuer, stocker et révoquer les clés sans l'aide d'une entité tierce de confiance. Une gestion des clés publiques indépendante de l'extérieur et complètement auto-organisée a été proposée par Capkun et al [CAP 03]. Chaque nœud est censé gérer les certificats par lui-même. Les nœuds conservent le référentiel de certificats en leur possession. Un nœud génère localement sa propre clé publique et la clé privée correspondante à cette clé publique générée localement.

L'émission du certificat est basée sur la relation de confiance entre deux nœuds. Une fois le certificat émis, les deux nœuds procèdent à l'échange de certificats. Les nœuds forment un graphe connecté basé sur les liens reliant les nœuds voisins. Ce graphe aide les nœuds à collecter les certificats de leurs voisins. Le référentiel de certificats est mis à jour à partir de ces certificats collectés. Le référentiel de certificats non mis à jour peut également être mis à jour en appliquant un algorithme de construction de référentiel. Le processus d'authentification essaye de trouver le graphe dirigé vers le nœud destinataire. Si le chemin existe, l'authentification réussit, sinon elle échoue. Les certificats dans ce schéma sont limités dans le temps, et le certificat contient l'heure d'émission et d'expiration.

Dans l'exemple de la Figure 26, lorsqu'un nœud u veut vérifier l'authenticité de la clé publique Kv d'un autre nœud v, u essaie de trouver un chemin dirigé de Ku à Kv dans (Gu U Gv). Les certificats sur ce chemin sont alors utilisés par u pour authentifier Kv. S'il n'y a pas de chemin de Ku à Kv dans (Gu U Gv), u ne parvient pas à authentifier Kv et par conséquent l'authentification échoue.

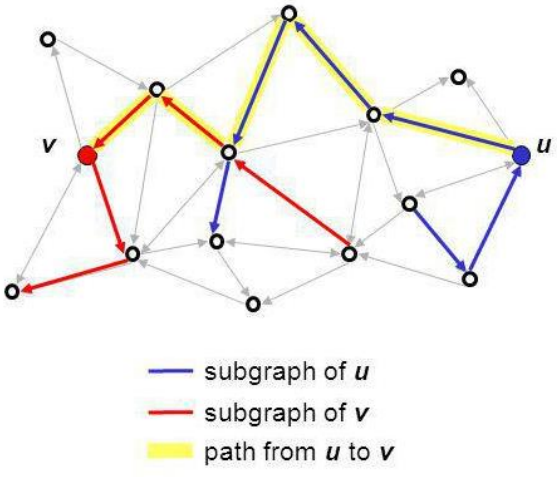

Figure 26: Authentification des nœuds en utilisant des clés distribuées

2.5 Systèmes basés sur la réputation et le crédit

L'objectif des systèmes basés sur la confiance dans les réseaux dynamiques est de fournir des informations permettant aux nœuds de distinguer les nœuds dignes de confiance des nœuds indignes de confiance dans le réseau. Ces systèmes sont généralement utilisés pour renforcer les solutions de sécurité existante telle que la cryptographie.

Dans ces systèmes, la valeur qui représente la réputation est initialisée de l'une des trois manières suivantes :

- Tous les nœuds du réseau sont initialement supposés être dignes de confiance. Chaque nœud fait confiance aux autres nœuds du réseau. La réputation des nœuds diminue à chaque mauvaise rencontre.
- Chaque nœud est considéré comme indigne de confiance lors de la phase d'amorçage du système, et les nœuds ne se font pas confiance entre eux au départ. Avec un tel système, la réputation des nœuds augmente à chaque bonne rencontre.
- Chaque nœud du réseau est considéré comme n'étant ni digne de confiance ni indigne de confiance. Tous les nœuds commencent avec une valeur de réputation neutre. A chaque bon ou mauvais comportement, la valeur de réputation est augmentée ou diminuée, respectivement.

Ces systèmes peuvent utiliser des informations de première main et s'appuient sur les observations directes ou les expériences rencontrées par les nœuds. Les nœuds des systèmes utilisant des informations de seconde main utilisent les informations fournies par les nœuds dans leur voisinage. La plupart des systèmes de réputation actuels utilisent à la fois des informations de première et de seconde main pour mettre à jour la réputation. Cela leurs permet d'utiliser davantage d'informations sur le réseau pour calculer les valeurs de réputation.

Il existe des systèmes qui n'utilisent que des informations de première main. Cela rend les systèmes complètement robustes contre la propagation des rumeurs. Observation-based Cooperation Enhancement in *Ad Hoc* Networks (OCEAN) [SOR 03] est un exemple de ces systèmes. Dans d'autres systèmes, certains nœuds n'utilisent que des informations de seconde main. Dans ce cas, un nœud ne dispose pas d'informations de première main pour évaluer la fiabilité des informateurs.

Dans un système distribué, chaque nœud peut maintenir la réputation des nœuds qui se trouvent à sa portée de communication, ou maintenir les informations de réputation de tous les nœuds du réseau. Par exemple, dans les applications de réseaux de capteurs (WSN), chaque nœud maintien des informations de réputation uniquement pour ses voisins. Cela réduit la surcharge de mémoire pour la maintenance des informations de réputation. Par contre, pour les réseaux à forte mobilité, la maintenance de la réputation d'autant de nœuds que possible est une option préférée.

2.5.1 WatchDog

Un exemple d'un système à base de réputation et de confiance est le **WatchDog**. Cette approche vise à détecter les nœuds qui se comportent mal (y compris les trous gris, les trous noirs et les trous de ver). Le **WatchDog** surveille les voisins pour voir si chacun d'entre eux se comporte honnêtement et ne présente pas de dysfonctionnement. Pour ce faire, on surveille le canal radio et on observe la transmission des messages. Pour intercepter les transmissions du prochain saut, la carte réseau sans fil est placée en mode *promiscuous* dans lequel toutes les trames reçues sont transmises au noyau. Dans l'exemple cité dans la Figure 27, le nœud A utilise son WatchDog pour vérifier que le B a bien retransmis le message envoyé de A vers B au nœud C.

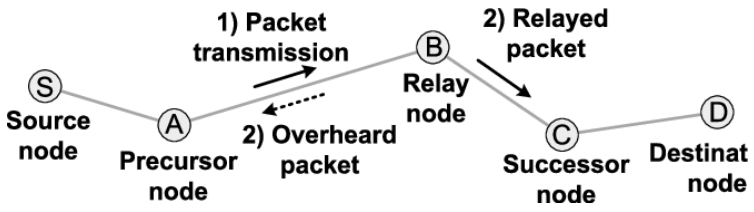

Figure 27: Exemple d'utilisation d'un Watchdog (nœud B)

Dans les premières générations des cartes sans fil, il s'agissait d'un mode de fonctionnement distinct qui interdisait le fonctionnement normal. Les cartes modernes sont capables de recevoir dans ce mode et de maintenir un fonctionnement normal en même temps en utilisant des dispositifs logiques distincts sur le même matériel physique. Le WatchDog peut enregistrer un échec de transmission qui peut être dû à diverses raisons, par exemple : un dysfonctionnement du nœud, une congestion du réseau ou une collision au niveau du récepteur du WatchDog. Ainsi, le WatchDog est donc sujet aux faux positifs et aux faux négatifs.

2.5.2 Watchdog collaboratif

Le WatchDog collaboratif réduit le temps de détection des nœuds égoïstes (ou non coopératifs) dans un réseau. Cette approche se base sur la détection des nœuds égoïstes et la diffusion des contacts. Si un nœud a déjà détecté un nœud égoïste en utilisant son WatchDog, il peut diffuser cette information aux autres nœuds lorsqu'un contact se produit. Nous disons qu'un nœud a un contact positif s'il connaît le nœud égoïste. La détection des contacts entre les nœuds est simple en utilisant le WatchDog du nœud. Il faut noter que le WatchDog écoute les paquets du voisinage ; ainsi, lorsqu'il commence à recevoir des paquets d'un nouveau nœud, on suppose qu'il s'agit d'un nouveau contact. Ensuite, le nœud transmet un message comprenant tous les contacts positifs connus qu'il connaît à ce nouveau nœud contacté. Le nombre de messages nécessaires pour cette tâche est l'overhead du WatchDog collaboratif [HER 12].

2.5.3 Systèmes basés sur le crédit

Dans un schéma basé sur le crédit, les nœuds qui coopèrent sont récompensés en termes de monnaie virtuelle. Le nœud source ou destination doit payer de la monnaie virtuelle aux nœuds intermédiaires participant au routage. Un autre exemple de systèmes basés sur le crédit est d'utiliser un compteur de crédit. Le compteur d'un nœud sera diminué en envoyant ses propres paquets alors qu'il augmentera en transmettant des paquets pour d'autres nœuds du réseau. Pour persister dans le réseau, un nœud doit équilibrer ses activités d'envoi et de transfert.

Ces systèmes n'ont pas été largement acceptés en raison des défauts tels que les performances limitées face aux nœuds égoïstes et malveillants. En particulier, les nœuds qui ne participent pas au processus d'établissement de la route (c'est-à-dire les nœuds qui abandonnent les messages de demande de route et de réponse à la route) utilisent les ressources du réseau à leur propre avantage.

2.6 Sécurité d'une flottes de drones

2.6.1 Problématique

Les drones représentent les nœuds d'un réseau dynamique, mais leurs caractéristiques sont différentes d'un réseau traditionnel ; ils ont un plus grand degré de liberté dans leur mouvement, et il est important de maintenir la connectivité entre les drones, et avec la station de contrôle au sol. Nous avons essayé de distinguer les problèmes de sécurité spécifiques à une flotte de drones, ceci en essayant de répondre aux questions suivantes : Quelles mesures de sécurité et de vérification pour assurer un environnement d'exploitation sûr et sécurisé pour une flotte de drones? Quelles sont les actions à effectuer au cas où une menace a été détectée dans le réseau? Comment rendre possible la coopération entre les drones d'une même flotte pour accomplir une mission particulière en toute sécurité? Pour répondre à certaines de ces questions, nous avons examiné quelques articles dans le contexte de la sécurité et de la collaboration des drones dans un environnement distribué.

Les drones sont vulnérables aux attaques, soit sur le canal de communication qu'ils utilisent, soit sur le nœud lui-même. Les messages peuvent être écoutés ou de faux messages peuvent être injectés ou rejoués dans le réseau. Les nœuds sont vulnérables aux accès non autorisés s'ils ne sont pas protégés par un système de clés de cryptage efficace. En outre, les principales exigences de sécurité sont toujours applicables à une flotte de drones. La disponibilité, l'intégrité, la confidentialité et la non-répudiation des échanges doivent être vérifiées. De plus, seuls les nœuds autorisés doivent pouvoir utiliser les services du réseau et ces nœuds doivent être authentifiés. Un autre défi est d'assurer la confidentialité des données utilisateur échangées entre les nœuds. Les solutions de cryptage classiques sont toujours applicables aux drones, mais leur efficacité doit être évaluée. Cela est dû au fait que les drones sont de petits appareils et ne disposent pas d'une grande capacité de calcul. Un autre facteur à prendre en compte est de savoir si la solution repose sur un point central (comme le GCS), par exemple pour générer des clés secrètes ou des certificats. Un schéma de chiffrement asymétrique distribué pourrait également constituer une bonne alternative. Dans le cas d'un nœud déjà compromis dans le réseau, d'autres mesures de sécurité doivent être mises en œuvre, comme des systèmes de détection des intrusions.

2.6.2 Travaux de recherche sur la sécurité des drones

La plupart des articles que nous avons examinés se focalisent sur la sécurité du drone et non la sécurité de l'ensemble de la flotte et adopte des solutions déjà utilisé pour les réseaux dynamiques. Nous citons ci-après quelques articles que nous avons examinés:

L'article de [ALT 16] a considéré les menaces sur les drones comme des nœuds uniques et non comme une flotte. Les auteurs ont présenté une enquête qui identifie divers aspects de sécurité, de sûreté et de confidentialité des opérations des drones civils. Ils ont classé les cyberattaques possibles en fonction des composants du drone qu'ils ciblent (capteurs, module de navigation, GPS, etc.).

L'article de [KRI 17] étudie la cybersécurité en se concentrant sur les attaques réelles. Ce travail a été motivé par l'utilisation croissante de petits drones pour l'inspection d'infrastructures critiques telles que les réseaux électriques, qui pourraient constituer une cible potentielle.

Les auteurs dans [MAX 16] ont considéré la sécurité sous l'aspect du routage du réseau. Ce travail a étudié l'impact des protocoles de routage existants sur les réseaux de drones afin d'évaluer leurs performances et de choisir un protocole de routage adéquat. Un protocole réactif de routage sécurisé appelé SUAP (Secure UAV Ad hoc routing protocol) a été proposé pour assurer l'authentification des messages et fournir une détection, notamment des attaques par trou de ver. Le protocole utilise la cryptographie à clé publique et les chaînes de hachage. Afin de détecter les attaques par trou de ver un algorithme basé sur les paquets leashes géographique est utilisé pour estimer la corrélation entre la distance parcourue par les paquets et la valeur du nombre de sauts.

L'article de [AKR 17] a défini quelques exigences de sécurité pour sécuriser une flotte de drones. Les auteurs ont proposé une solution théorique basée sur un module matériel embarqué appelé Secure Element (SE) afin de répondre aux exigences de sécurité qu'ils ont spécifiées. Le rôle du module Secure Element est de fournir un identifiant unique pour un drone, et l'utiliser pour la gestion des clés de cryptage pour la communication avec les autres membres de la flotte.

Les auteurs dans [LIN 18] ont décrit une architecture d'Internet des drones (IoD) à gérer à l'aide d'une infrastructure Cloud. L'article décrit plusieurs défis en matière de sécurité et de confidentialité, tels que la fuite des données privées et la nécessité d'un partage sécurisé et efficace des données. Ils ont ensuite décrit des solutions potentielles adaptées à la nature de l'architecture Internet des Drones. Les auteurs ont discuté des problèmes potentiels de sécurité et de confidentialité et ont conclu qu'un certain nombre d'autres services de sécurité doivent être mis en œuvre pour l'IoD, comme la détection des intrusions et l'agrégation sécurisée des données.

2.7 Conclusion

Dans ce chapitre, nous avons étudié la sécurité des réseaux dynamiques. Les attaques et les contre-mesures que nous avons présenté mettent en évidence le fait que seule la protection du protocole de routage ne peut apporter qu'une partie de de la solution. Cette protection est efficace contre les attaques au niveau de la couche réseau pour permettre le bon acheminement des paquets de données, mais elle doit être complétée pas d'autres solutions pour assurer la sécurité sur le reste des couches.

Dans le cas d'une flotte de drones, il est important de définir et concevoir des mécanismes de sécurité adaptés vu leurs contexte de déploiement et leurs spécificités en terme de mobilité.

3. Qualité de service dans les réseaux dynamiques

3.1 Introduction

Fournir une Qualité de service (QoS) aux applications est toujours une préoccupation majeure dans les réseaux dynamiques. Nombreuses applications consistent en un trafic temps réel qui nécessite un soutien de la QoS pour une communication efficace. L'objectif de tout modèle de QoS est d'offrir des services avec des garanties en termes de délai, de largeur de bande, de gigue et un taux de perte de paquets faible. Pour fournir de telles garanties, les couches du réseau doivent allouer de la bande passante nécessaire, et prendre en considération les ressources disponibles tout au long du chemin de transmission.

Dans ce chapitre, nous allons présenter le concept de la Qualité de service dans les réseaux dynamiques. Les différentes classes de solutions seront décrites ainsi les approches et les protocoles associés à ces classes. Ensuite, nous présenterons quelques travaux de recherche adoptant la QoS dans les flottes de drones.

3.2 Définition et Métriques d'évaluation.

Du point de vue utilisateur, la Qualité de service est le degré de satisfaction d'un utilisateur des services fournis par un système de communication. En terme de service, la Qualité de service représente la capacité d'un élément du réseau (exemple: routeur, nœud ou une application) de fournir un niveau de garantie dans l'acheminement des données [BEL 20].

L'ensemble des contraintes à garantir sur un lien afin de satisfaire les exigences d'une application sont connues comme étant les métriques QoS. Les applications ont des exigences différentes (Figure 28), et les services qu'elles requièrent ainsi que les paramètres QoS associés diffèrent d'une application à une autre. Nous citons ci-dessous les mesures couramment utilisées par les applications pour spécifier les exigences de QoS des applications ou des protocoles: [GAN 11]

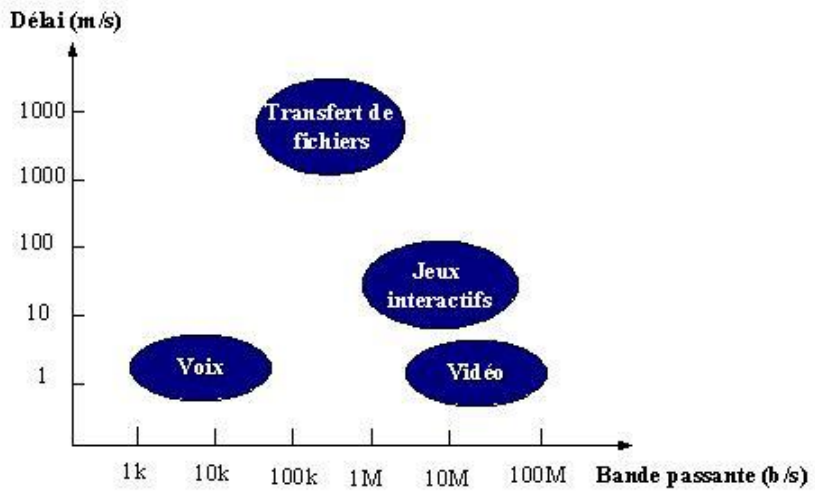

Figure 28: Exigences des applications en termes de Délai vs Bande Passante

- **Débit Minimum (bit/s):** la vitesse de transmission des données ou la bande passante minimale requise par l'application.
- **Délai Maximal (s):** le délai maximal des paquets sur un chemin de bout en bout qui est tolérable par l'application.
- **Gigue (ou variation de délai) (s):** la différence entre le délai maximal et le délai minimal durant la réception des paquets.
- **Taux de perte de paquets (%):** le taux total des paquets envoyés, qui ne sont pas reçus par la destination finale.

En plus, La valeur d'une métrique QoS peut être l'une des compositions suivantes:

- **Métrique additive** - Elle est représentée mathématiquement comme suit :

$$m(p) = \sum_{i=0}^{lk} m(lk_i)$$

Où m (p) est le total de la métrique m du chemin (p), lk_i est un lien dans le chemin (p), lk est le nombre de liens dans le chemin (p), avec i= 1,...lk
Le délai, la variation du délai (gigue), et le coût sont des exemples de ce type de composition.

- **Métrique concave** - Elle est représentée mathématiquement comme suit :

$$m(p) = \min(m(lk_i))$$

La bande passante est un exemple de ce type de composition. La bande passante qui nous intéresse est la bande passante résiduelle qui est disponible pour le nouveau trafic. Elle peut être définie comme le minimum de la bande passante résiduelle de tous les liens sur le chemin.

- **Métrique multiplicative:** Celle-ci peut être représentée mathématiquement comme suit :

$$m(p) = \prod_{i=0}^{lk} m(lk_i)$$

La probabilité de perte est un exemple de ce type de composition.

- **Métriques convexes:** Elle peut être représentée comme le maximum de toutes les métriques le long du chemin.

$$m(p) = \max(m(lk_i))$$

En plus, d'autres paramètres ont été considérés sur les couches inférieures, notamment la couche physique et la couche liaison de données. Par exemple:

- **Rapport signal/bruit (SNR)**: Cette mesure garantit la qualité de la liaison entre l'émetteur et le récepteur. La station réceptrice peut utiliser le SNR pour estimer la qualité du signal

en fonction de l'indicateur de force du signal reçu (RSSI) et le taux d'erreurs sur les bits (BER). Cette métrique de la couche physique assure le niveau de correction des erreurs et le nombre de retransmission que nécessite une liaison. Cela a un impact direct sur la fiabilité de la liaison et la consommation d'énergie.

- **Puissance de la batterie:** La charge résiduelle de la batterie peut être estimée en mesurant la tension de la batterie et en la comparant avec la fonction de décharge du modèle de batterie.
- **Délai MAC:** Sur la couche liaison de données, le temps nécessaire pour transmettre un paquet entre deux nœuds voisins basé sur un accès avec contention. Cela donne une bonne indication de la charge de trafic des nœuds voisins communicants.

3.3 Facteurs affectant la QoS

Lors de l'évaluation des performances des solutions QoS dans un réseau dynamique, un certain nombre de facteurs ont un impact majeur sur leurs performances. Nous listons ces paramètres dans ce qui suite suit :

- **Mobilité des nœuds:** Ce facteur détermine si le nœud se déplace à une vitesse uniforme à tout moment ou si sa vitesse varie constamment, ainsi que la manière dont le nœud accélère. Le temps de pause détermine le temps pendant lequel les nœuds restent immobiles entre chaque période de mouvement. Ce paramètre détermine donc la fréquence à laquelle la topologie du réseau change et la fréquence à laquelle les informations sur l'état du réseau doivent être mises à jour.
- **La taille du réseau:** étant donné que l'état de la QoS doit être recueilli périodiquement pour que des décisions de routage soit prises, plus le réseau est grand, plus cela prendra plus de temps. Il en va de même pour toutes les informations sur l'état du réseau en termes de surcharge de messages vu la taille du réseau.
- **Nombre, type et débit des sources de trafic:** intuitivement, un plus petit nombre de sources de trafic moins de routes sont nécessaires et vice versa. Les sources de trafic peuvent être à débit binaire constant (CBR) ou peuvent générer des paquets à un rythme qui varie dans le temps. Le débit maximal affecte le nombre de paquets dans le réseau et donc la charge du réseau.
- **Puissance de transmission du nœud:** certains nœuds peuvent avoir la capacité de varier leur puissance de transmission. Ceci est important, puisqu'avec une puissance plus élevée, les nœuds ont plus de voisins directs, ce qui augmente la connectivité, mais aussi les interférences entre les nœuds. Le contrôle de la puissance de transmission peut également entraîner des liens unidirectionnels entre les nœuds, ce qui peut affecter les performances des protocoles de routage.
- **Temps de calcul du nœud:** Du fait que la puissance de calcul des nœuds est limitée, surtout lorsqu'ils doivent non seulement exécuter les applications mais aussi les protocoles nécessaires à la prise en charge du réseau et des applications. Cependant, il s'agit probablement de la ressource la moins critique, car les protocoles de communication n'imposent généralement pas de charge sur le processeur.
- **Capacité énergétique du nœud:** si la batterie d'un nœud est épuisée, il ne peut pas fonctionner du tout. Les pannes de nœuds peuvent également provoquer le partitionnement du réseau, ce qui entraîne une défaillance complète du réseau et

l'impossibilité de fournir des services. Par conséquent, les protocoles MAC et de routage efficaces en énergie ont fait l'objet de nombreuses ont fait l'objet de nombreux sujets de recherches.

- **Espace tampon (mémoire):** les paquets de données doivent être mis en mémoire tampon en attendant d'être transmis. De plus, lorsque les tampons sont pleins, tous les paquets les paquets nouvellement arrivés doivent être abandonnés, ce qui contribue au taux de perte de paquets.
- **La capacité du canal:** Les nœuds doivent partager le support de transmission et une fraction de la capacité doit être accordée à l'utilisation de chaque nœud. La manière d'exprimer cela dépend de la technique de la couche MAC employée. Dans un accès basé sur la contention, on peut envisager des de transmission bien que l'accès au canal ne soit garanti à aucun nœud, il lui est simplement accordé avec une certaine probabilité.

3.4 Solutions QoS pour les réseaux dynamiques

Nous distinguons quatre classes de solutions pour l'implémentation de la QoS dans les réseaux dynamiques (Figure 29):

- L'implémentation de la QoS sur **la couche MAC**
- **Le contrôle d'admission** avant l'envoi du flux
- **L'ordonnancement** ou le **Scheduling** des paquets dans les files d'attente
- **Le routage** des paquets en prenant en considération **la qualité de service**

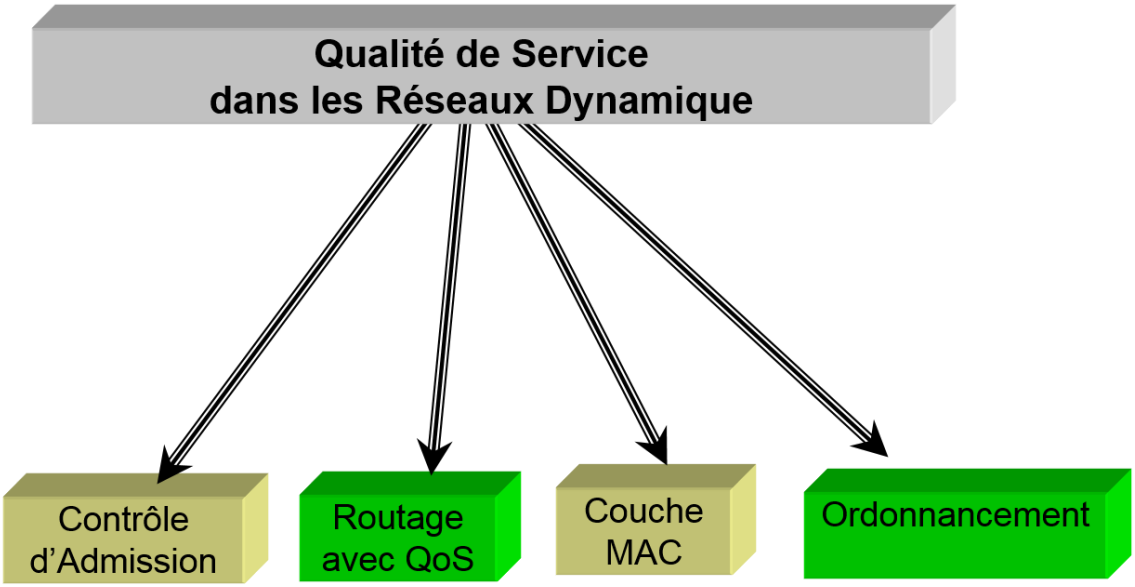

Figure 29: Solutions QoS dans les réseaux dynamiques

3.4.1 QoS sur la couche Mac

Le rôle des protocoles d'accès au support (protocoles MAC) sont multiples. Ils permettent d'éviter les collisions et d'assurer le partage de la bande passante. La QoS sur cette couche se base sur la priorité d'accès au support de communication: on distingue un accès sans contention et un accès avec contention. Dans l'accès sans contention, les ressources sont d'abord identifiées, puis elles sont réservées. On utilise essentiellement TDMA pour les allocations des times slots à réserver aux nœuds émetteurs. Dans ce cas on fournit une garantie de QoS physique (ou hard).

Dans les protocoles MAC avec contention, on estime les ressources disponibles de manière statistiques. L'idée est de doter le protocole IEEE 802.11 d'un mécanisme de priorités afin de concevoir des mécanismes de différenciation de services. Pour ce faire, on propose d'adapter certains paramètres de la fonction de coordination distribuée (DCF) du protocole selon la priorité des paquets. Rappelant que la fonction DCF repose sur la détection de porteuse par la méthode CSMA: si l'émetteur veut transmettre des données au récepteur, il commence par écouter le canal, si le canal est occupé, il attend que le canal devient libre. La station émettrice attend la période de temps DIFS (distributed Inter Frame Spacing) et invoque un temps d'attente backoff selon la formule :

Temps d'attente = rand(0, CW) x temps de slot

La nouvelle spécification IEEE 802.11e (Figure 30) propose d'intégrer la QoS dans les réseaux sans fil en utilisant une fonction de contrôle EDCA (Enhanced Distributed Channel Access), considérée comme la nouvelle version de la fonction DCF, ainsi qu'une autre fonction de coordination hybride appelée (HCF). EDCA introduit quatre catégories de trafics avec des priorités qui sont contrôlées par les stations en modifiant le schéma d'accès de base (DCF).

Lorsque la couche MAC reçoit des données qui contiennent la priorité du paquet et qui correspond à une catégorie de trafic, le système EDCF, définit les paramètres d'accès suivants : Cmin, Cmax, AIFS (Arbitration Inter Frame Spacing) et Transmission Opportunity Time (TXOP). TXOP est défini comme étant un intervalle de temps pendant lequel une station a le droit d'initier des transmissions. Pendant les périodes de contention, chaque AC d'une station essaye d'accéder au canal pour un TXOP et démarre indépendamment un compteur backoff après avoir détecté que le canal devenu libre.

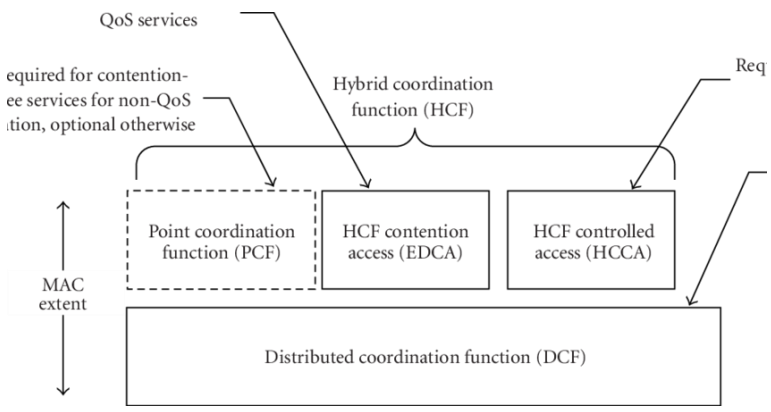

Figure 30: Champs QoS dans une trame 802.11e [MOR 10]

3.4.2 Contrôle d'admission

Le Contrôle d'Admission (CA) a pour but d'accepter ou de rejeter un nouveau flux selon si le réseau est capable de garantir ses contraintes ainsi que celles des flux préalablement admis. Les mécanismes de contrôle d'admission sont donc utilisés pour estimer l'état des ressources du réseau, et par conséquent, décider quelles sont les ressources, que les applications peuvent utiliser, sans violer les garanties précédemment accordées (Figure 31). L'objectif du contrôle d'admission est d'admettre uniquement les sessions dont les exigences de QOS peuvent être satisfaites. Ce qui est intéressant dans le protocole d'admission est que cette procédure peut être effectuée par un routage conscient de la qualité de service, tout en découvrant la route au moment où elle assure l'allocation des ressources [KHO 13].

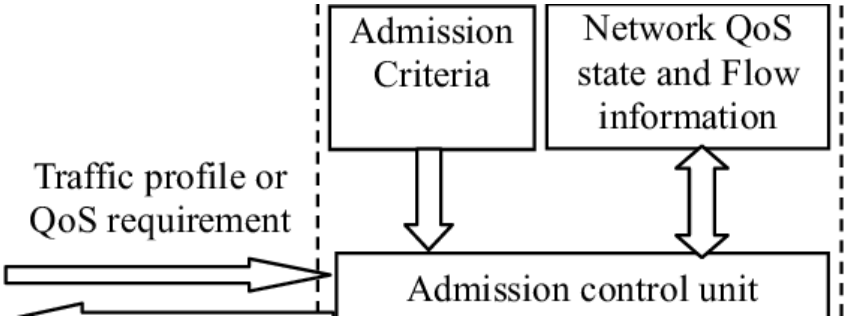

Figure 31: Mode de fonctionnement du module Contrôle d'Admission

Dans la littérature, plusieurs techniques passives et actives ont été proposées pour estimer la bande passante disponible et améliorer ainsi la Qualité de service [DRO 13]: l'estimation de la bande passante à l'aide d'une technique passive où la bande passante disponible est estimée à l'aide de l'utilisation mesurée du canal sans aucun impact sur les flux existants. Dans les approches dynamiques. On peut détecter l'état en temps réel de l'environnement du réseau, et ajuster la stratégie de contrôle d'admission en conséquent.

Il existe des solutions de contrôle d'admission qui sont découplées du routage, car ils supposent que la route ait été préalablement découverte. Le module Contrôle d'admission vérifie ensuite si cette route peut garantir les contraintes du flux. Ce découplage permet à ces solutions d'être implémentés sur n'importe quel protocole de routage et d'être ainsi modulables. Cependant, l'inconvénient est que le rejet d'une route entraine la perte de ressources consommées pour établir la route. Le module CA découplé du routage peut être soit avec état ou sans état. Un CA sans état ne stocke aucune information sur un flux au niveau des nœuds intermédiaires de sa route. Un CA avec état, contrairement à un CA sans état, peut continuer à garantir les contraintes des flux, même si certains ne respectent pas leurs contraintes en termes de réservation car il peut limiter le débit des flux à ceux qu'ils ont demandé.

Les CAs couplés avec un protocole de routage apportent une plus grande granularité, puisque, lors de la découverte d'une route, chaque nœud vérifie s'il peut garantir ou non les contraintes du flux, et si l'un d'entre eux ne peut pas les garantir, on évite alors ce nœud dans la construction de la route. Ainsi, si un nœud ne peut pas garantir les contraintes d'un flux, on rejette uniquement un nœud et non pas toute une route. La Figure 32 montre les caractéristiques des CAs couplés et découplés des protocoles de routage.

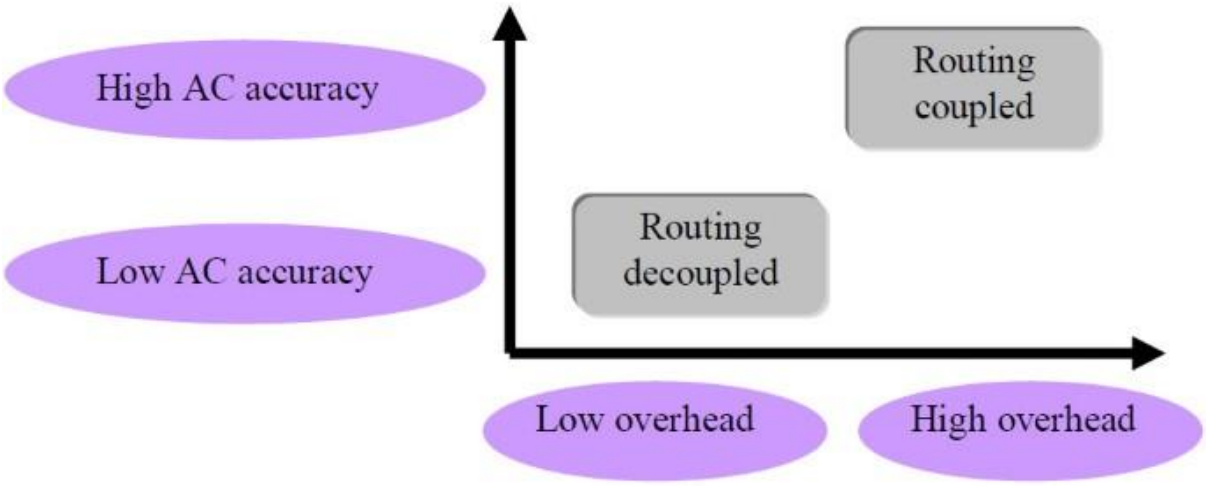

Figure 32: Caractéristiques des protocoles avec Contrôle d'Admission [KHO 13]

3.4.3 Ordonnancement (Scheduling)

La transmission de paquets nécessite un algorithme d'ordonnancement pour déterminer le paquet suivant à router (Figure 33). Les algorithmes d'ordonnancement sont un facteur clé pour améliorer la Qualité de service dans un réseau. Par exemple, un algorithme d'ordonnancement prioritaire applique pour les paquets de données la file d'attente FIFO standard, et les paquets de routage ou prioritaires sont ordonnancés avec un algorithme de priorité. Par conséquent, les paquets de contrôle et de données sont maintenus dans des files d'attente séparées. Une priorité élevée est attribuée aux paquets de contrôle, par exemple, les paquets de routage RREQ, RREP et RERR. Lorsqu'une priorité élevée est attribuée aux messages d'erreur de route (RERR), ceci permet d'éviter un grand nombre de paquets de données mal dirigés qui viendront plus tard. Egalement, une politique drop-tail peut être utilisée pour la gestion des files d'attente par les algorithmes d'ordonnancement. Si le buffer est plein, on supprime les paquets qui débordent.

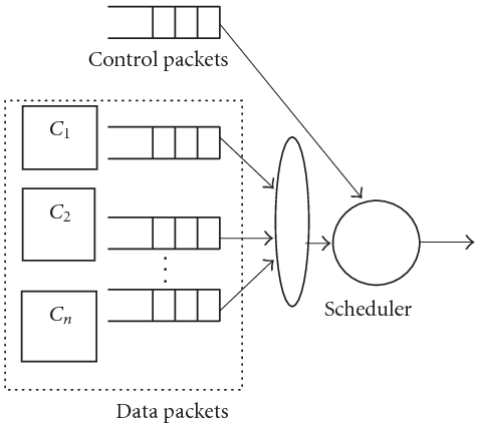

Figure 33: Traitements des paquets par l'ordonnanceur

3.4.4 Routage avec QoS

L'objectif principal des protocoles de routage tenant compte de la QoS est de déterminer un chemin d'une source à une destination qui satisfait les besoins des applications. Dans ce cas, le protocole de routage est qualifié de **QoS-Aware** (Figure 34).

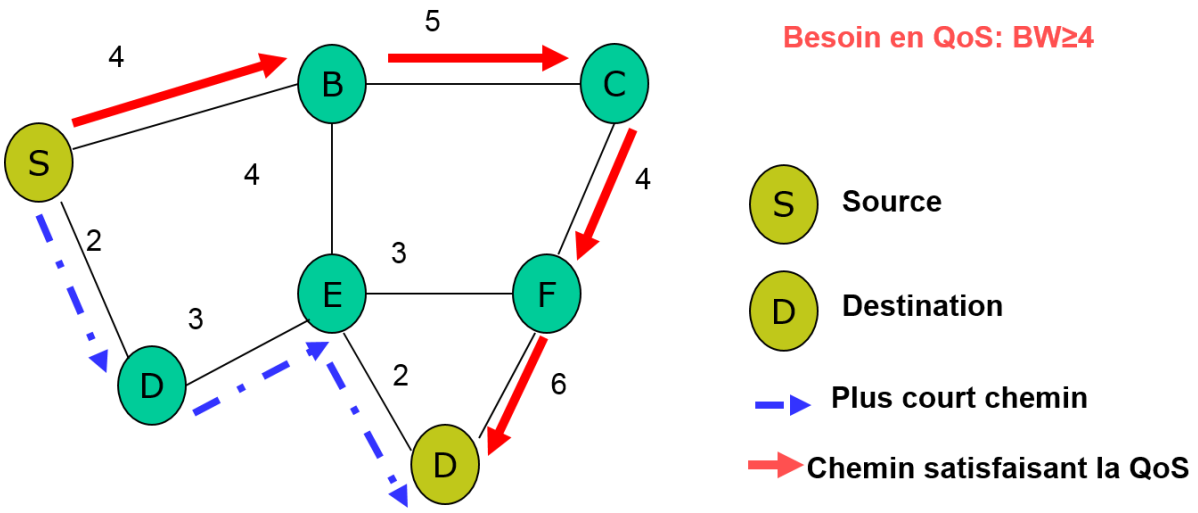

Figure 34: Routage avec prise en compte de la QoS

Dans la littérature, de nombreuses approches de routage avec QoS ont été proposées, quelques-unes sont décrites dans ce qui suit [GUL 12]:

Approche basée sur les trajets multiples

Le routage multi-chemins est une technique qui exploite les ressources physiques sous-jacentes du réseau en utilisant plusieurs chemins source-destination. Il est utilisé à de nombreuses fins, notamment pour l'agrégation de la bande passante, la réduction du délai de bout en bout, l'augmentation de la tolérance aux pannes, l'amélioration de la fiabilité, l'équilibrage de la charge, etc. Les chemins multiples entre la source et la destination peuvent être utilisés pour compenser les changements de topologie dynamiques et imprévisibles dans les réseaux Ad Hoc.

Approche basée sur les couches croisées (Cross Layer)

Assurer une QoS pour certains protocoles dépend beaucoup de l'état réel des couches inférieures. Par conséquent, il serait pratique de concevoir une solution inter-couches (Cross-layer). Cette approche se base sur un échange d'informations entre toutes les couches, éventuellement non adjacentes. Cette approche se réfère aux protocoles qui permettent l'échange d'informations entre couches dans le but d'obtenir un gain de performance. Les protocoles utilisent ces informations d'état pour adapter leur comportement adéquatement. Par exemple, en ayant l'état du canal et le niveau d'énergie, la couche physique peut adapter la vitesse et la puissance de transmission pour répondre aux besoins de l'application.

Approche basée sur la stabilité

Pour réduire les possibilités de rupture de route pendant la transmission des données, il est important de trouver des routes qui durent plus longtemps. La stabilité des liaisons peut être estimée à l'aide de nombreux paramètres tels que la force du signal, la vitesse des nœuds, la durée des liaisons et la puissance restante de la batterie des nœuds.

La stabilité ou la durée de vie d'une route est déterminée par le nombre de liens qui composent la route et la stabilité de chaque lien dans la route. On peut montrer que la probabilité de défaillance d'une route peut être réduite en diminuant soit le taux de défaillance des liens, soit le nombre de liens qui composent la route.

Approche basée sur l'équilibrage de la charge

L'équilibre de la charge des réseaux est nécessaire pour que le flux de données soit raisonnablement distribué à chaque nœud en raison de la limitation de la bande passante. L'idée de base du routage multi-chemins est de distribuer le flux de données sur plusieurs voies et d'équilibrer le réseau au moyen des informations de maintenance des nœuds. Les nœuds fortement chargés peuvent provoquer des congestions et des retards importants, voire épuiser leur énergie rapidement. La fonction d'équilibrage de la charge peut éviter la congestion en répartissant le trafic sur plusieurs chemins lorsque l'algorithme de routage juge que la bande passante atteint la limite maximale.

Approche basée sur l'efficacité énergétique

Dans les réseaux dynamiques, le processus allant de la sélection de la route à la maintenance de la route doit être économe en énergie et conscient de l'importance de l'énergie pour maximiser la durée de vie du réseau. La conservation de l'énergie est un problème crucial dans les réseaux dynamiques. Par conséquent, l'énergie doit également être traitée comme une mesure indirecte de la qualité de service, car la sélection de chemins sans efficacité énergétique peut entraîner l'épuisement prématuré d'un réseau ou d'un nœud. Les protocoles de routage économes en énergie visent à minimiser la consommation d'une ressource importante dans le réseau, à savoir la batterie. Pour y parvenir, les décisions de routage sont prises en fonction de la consommation d'énergie. En d'autres termes, lors de la conception des protocoles de routage, la route la moins coûteuse en énergie devrait avoir plus de chances d'être choisie.

3.4.5 Exemples de PROTOCOLES DE ROUTAGE TENANT COMPTE DE LA QOS

6.1. CEDAR (Core Extraction Distributed Ad Hoc Routing)

CEDAR [SIV 99] établit de façon dynamique un cœur du réseau, puis propage de manière incrémentielle l'état des liens stables aux autres nœuds. Le calcul des routes est à la demande, et est effectué par les nœuds centraux en utilisant uniquement l'état local. CEDAR définit trois composants clés :

- Etablissement du cœur de réseau (Figure 35): les nœuds formant le cœur du réseau doivent être performants et suffisamment dimensionnés pour l'établissement et le maintien des routes avec les autres nœuds.
- Propagation de l'état des liaisons : Le routage avec la qualité de service dans CEDAR est réalisé en propageant l'information sur la disponibilité de la bande passante des liens stables à tous les nœuds centraux.
- Calcul d'itinéraire : En se basant sur le plus court chemin et la bande passante requise. Les routes sont divisées en deux : routes principales répondant aux exigences performantes de QoS et des routes secondaires de QoS moindre, empruntées lors de la perte des routes principales. L'objectif principal étant de garantir des routes avec suffisamment de bande passante entre les nœuds du réseau.

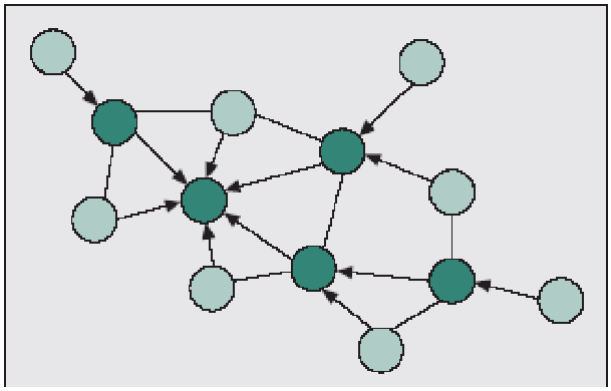

Figure 35: Nœuds cœur de réseau du protocole CEDAR [RAG 3]

Protocole de routage multivoie (MRP)

Chaque nœud sélectionne dans son voisinage un ensemble de nœuds appelés ses MPR ou relais multipoints. Les MPRs sont un sous-ensemble des voisins à un saut par lequel il faut passer pour atteindre tous ses voisins à deux sauts (Figure 36). On dit d'un nœud qu'il est un MPR s'il a été sélectionné de cette manière par au moins un de ses voisins à un saut [NGU 07]. Badis et al. [BAD 04] ont proposé QOLSR, une extension de routage QoS à OLSR. Il est basé sur l'utilisation d'une heuristique spéciale pour la sélection des MPR et une modification des messages TC pour diffuser les informations QoS dans le réseau. Pour la sélection des MPR, la stratégie consiste à trouver les MPR qui maximisent la largeur de bande disponible et minimisent le délai vers les voisins à deux sauts. De cette façon, le calcul de l'itinéraire est effectué sur un meilleur ensemble de liens qu'avec un réseau standard OLSR. Pour appliquer une telle heuristique, les nœuds ont besoin de certaines connaissances sur le voisinage à deux sauts. Les messages HELLO sont modifiés pour prendre en charge l'échange d'informations sur la qualité de service entre voisins à un saut. Chaque nœud annonce la bande passante disponible et le délai pour chacun de ses voisins à un saut. Il peut éventuellement annoncer d'autres métriques QoS, en utilisant un champ QoS extensible.

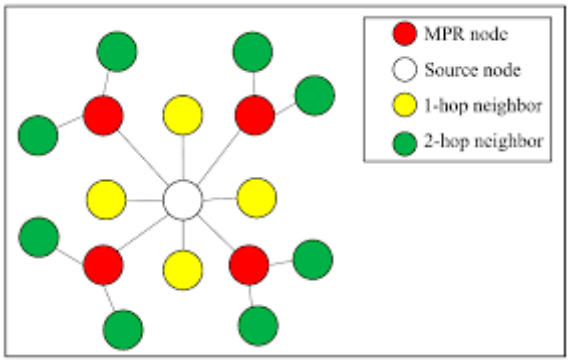

Figure 36: Nœuds MPR dans un réseau OLSR [JUB 19]

Routage à la demande avec QoS ad hoc (AQOR)

Ce protocole utilise une inondation limitée pour découvrir la meilleure route disponible en termes de bande passante et un délai de bout en bout le plus faible (Figure 37). Un paquet de demande d'itinéraire comprend des contraintes de bande passante et de délai. Soit Tmax la contrainte de délai. Si un nœud peut satisfaire les deux contraintes, il rediffuse la demande au saut suivant et passe en état d'exploration pendant une courte période de 2xTmax. Si plusieurs paquets de demande arrivent à la destination, elle renverra un paquet de réponse le long de chacune de ces routes. Les nœuds intermédiaires ne transmettront la réponse que s'ils sont toujours en état d'exploration. Cependant, la réservation de la bande passante pour chaque flux n'est activée que par l'arrivée du premier paquet de données du nœud source. Le délai est mesuré pendant la découverte de la route. La route qui présente le moins de retard est choisie par la source [XUO 03].

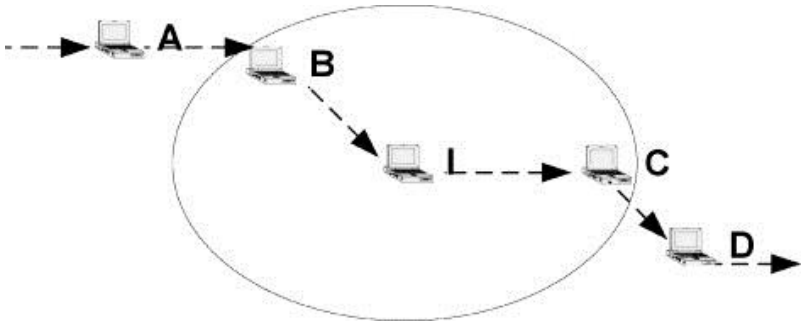

Figure 37: Exploration des chemins dans AQOR

3.5 Flotte de drones et support de la QoS

L'objectif principal d'un réseau dynamique avec un support QoS est de maintenir la connectivité de l'ensemble du réseau tout en garantissant la qualité de service demandée par les applications. Par exemple, un débit de données de bout en bout suffisant pour supporter le streaming audio/vidéo, une latence et gigue faible et un taux de perte de paquets minime. Nous listons dans ce qui suite quelques travaux de recherche adaptons une approche QoS dans ce contexte. Un scenario typique nécessitant un support de la QoS pour une flotte de drones est de rechercher des survivants à la suite d'une catastrophe naturelle ou humaine. L'objectif est de fournir une connectivité sans fil à l'équipe de secours afin de de coopérer pendant les opérations de sauvetage. Pendant ces opérations d'urgence, un réseau de communication sans fil temporaire est créé par la flotte de drones.

3.5.1 Optimisation du chemin des drones avec QoS

Ce problème décrit dans [SHI 20] consiste à trouver des trajectoires possibles pour qu'un ou plusieurs drones visitent des régions ou des points d'observation dans une zone d'intérêt. L'objectif est de trouver des chemins qui minimisent la consommation d'énergie des drones, de sorte que l'objectif de couverture soit atteint, et qui aura donc un impact direct sur la QoS (Figure 38).

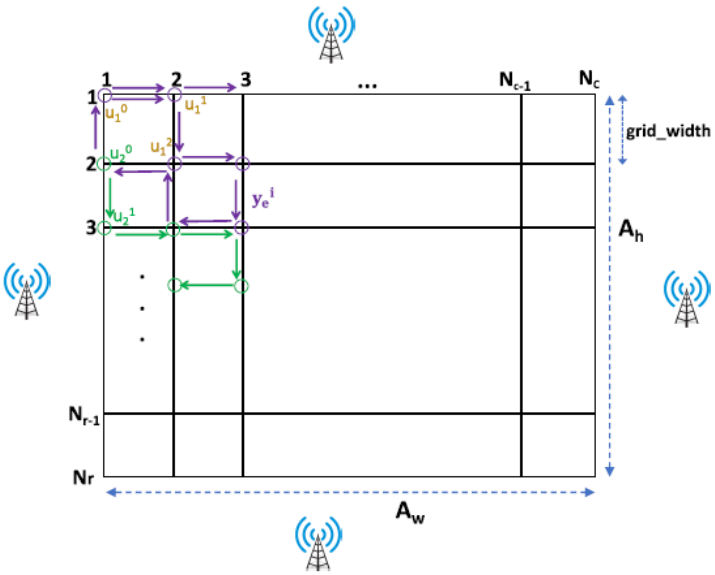

Figure 38 : Mouvement des drones et explorations des chemins [SHI 20]

Les auteurs [SHI 20] proposent une solution permettant de transformer ce problème mathématiquement en un problème de planification de chemin. Les paramètres qui sont pris en considération sont l'angle de la caméra, la hauteur de vol, la vitesse d'un drone, et qui aurons un impact direct sur la configuration des trajectoires des drones. La couverture d'une zone est modélisée sous forme de lignes d'une grille superposée sur la zone d'intérêt. Le mouvement des UAV doit répondre à des contraintes de débit de données, et qui sont représentées sous forme contraintes dans un modèle de programmation linéaire.

Le problème original est ainsi transformé en un problème d'optimisation combinatoire qui vise à minimiser le coût de la traversée du graphe. Le problème peut être réduit à un problème de vendeur itinérant, donc est NP-complet. En raison du nombre important de variables dans le modèle et de sa nature NP-complet, les auteurs ont choisi une solution heuristique basée sur l'optimisation. Les auteurs utilisent la méthode Ranked-Order (ROV) pour représenter un chemin à l'aide d'un vecteur de nombres réels et appliquent la recherche locale pour trouver le meilleur chemin.

3.5.2 Video streaming avec QoS

Dans ce scénario, les drones se déplacent dans une zone délimitée en suivant des trajectoires déterminées, capturent des vidéos et les diffusent a des téléspectateurs. Les téléspectateurs doivent pouvoir recevoir au moins une vue d'ensemble (basse définition) des vidéos provenant de plusieurs drones observant des zones différentes. Les téléspectateurs doivent ensuite être en mesure de sélectionner une vidéo d'un drone particulier et recevoir son flux de haute qualité en cas de besoin. Le choix d'un flux vidéo particulier par un premier intervenant doit être communiqué au drone à portée ou au nœud de téléspectateur voisin pour former un groupe de multidiffusion vidéo. Le respect de limites strictes de délai entre la transmission et la réception des paquets, et la prise en charge de la Qualité de service pour la diffusion vidéo en direct doit être respecter. Par exemple, des délais supérieurs à 250 ms ne sont pas acceptables pour la diffusion de vidéo en direct.

Tout d'abord, ont fait une recherche des itinéraires possibles de la source à la destination. Ensuite, le temps de connectivité de tous les nœuds relais intermédiaires est trié. La route choisie est celle qui fournit le temps de connectivité minimal de la source à la destination. Cependant, comme les nœuds sources sont mobiles, la route calculée peut se déconnecter et une nouvelle route doit donc être calculée avant que la source ne subisse une déconnexion. L'algorithme calcule donc une nouvelle route autant de fois qu'une déconnexion est attendue.

Dans une autre solution, les auteurs ont conçu un protocole inter-couche qui améliore les flux de transmission vidéo en utilisant un protocole de routage géographique combiné avec un estimateur de qualité de chemin. Cela permet au protocole de prévoir la détérioration de la qualité et de réagir en créant un nouveau chemin avant que le lien n'expire, évitant ainsi un arrêt de la vidéo pendant la diffusion.

3.5.3 Un Modèle de Mobilité avec QoS

Dans un protocole de communication adapté à la mobilité, on peut prévoir/réagir au mouvement des nœuds, et donc à un éventuel changement dans le réseau. Dans le premier cas, afin de faire face à la variabilité fréquente de la topologie du réseau, plusieurs solutions envisagent la possibilité de redéfinir les tables de routage en incluant directement dans les algorithmes de routage un type d'information tenant compte de la mobilité. Par exemple, les auteurs de [SHA 09] présentent P-OLSR, une version améliorée du routage OLSR, où l'état des liens tient également compte de la position et de la vitesse des nœuds. Une autre approche considère des indices de stabilité des liens en diffusant leurs indices de stabilité et la charge de leurs liens à travers le réseau. Dans le contexte des protocoles de routage réactif, l'idée est d'exploiter le message de demande de route (RREQ) afin d'éviter les routes considérées comme moins stables [ANG 18].

Le routage géographique peut être aussi considéré comme une autre alternative, puisqu'il peut définir des routes basées sur les positions des nœuds de destination. Dans ce cas, le réseau n'a pas besoin de maintenir toutes les informations sur les routes. Cela nécessite une bonne précision et une bonne fiabilité des informations sur les positions, dont l'estimation et la gestion ne peuvent être considérées comme un problème trivial.

3.6 Conclusion

Le déploiement de nouvelles applications dans les réseaux dynamiques a suscité récemment de nombreux intérêts. Par contre, les contraintes liées à l'infrastructure décentralisée ainsi que les caractéristiques des nœuds doivent être pris en considération dans l'implémentation d'une approche QoS pour ces réseaux.

Les drones permettent de créer un réseau Ad Hoc à la volée. Pour le support de la QoS dans un ce scenario, la plus part des travaux de recherche propose de découvrir des routes sur la base des exigences QoS des applications, ou bien relancer le processus de découverte de route en cas de dégradation des métriques QoS.

Dans le chapitre suivant, nous allons présenter notre contribution à la Sécurité et la QoS dans le contexte d'un réseau dynamique et plus précisément dans le cadre d'un scénario de déploiement d'une flotte de drone durant une mission de recherche.

4. Contribution

4.1 Introduction

Dans un réseau dynamique, on fait l'hypothèse que tous les nœuds du réseau coopèrent pour router les messages des autres, ce qui n'est pas toujours le cas car les ressources et les puissances de calcul des nœuds sont limitées. Egalement, Un nœud peut lancer une attaque sur d'autres nœuds ou refuser de router des messages de données ou de contrôle afin d'économiser son énergie. Une solution pour assurer le bon fonctionnement entre les nœuds est donc nécessaire afin de réduire la dégradation des performances et assurer une continuité de service. C'est sur cet aspect que porte notre contribution dans ce chapitre.

Ce chapitre est organisé comme suit. La prochaine section décrit les motivations de ce travail en tenant compte des faiblesses des solutions existantes du point de vue de la Sécurité et de la QoS. Nous présentons ensuite le cadre architectural que nous avons utilisé et les différents modules de la solution. La quatrième section détaille la partie implémentation avec un scénario réel de déploiement. La cinquième section présente l'environnement de simulation et les résultats obtenus comme preuve de concept. La dernière section conclut ce chapitre.

4.2 Motivations du travail

Dans les chapitres précédents, et à travers notre état de l'art sur la Sécurité et la Qualité de service associées aux réseaux dynamiques, nous avons pu dégager certaines faiblesses communes des solutions déjà proposées. Nous les avons résumées dans les points communs suivants:

- La plus part des travaux de recherche ciblent une attaque, une menace ou un comportement particulier dans le réseau. L'absence d'une solution globale qui offre un maximum de protection contre des menaces ou des mauvais comportements reste un sujet de recherche.
- Dans un réseau distribué tel que dans le cas des réseaux dynamiques, il n'est pas pratique d'implémenter une solution de sécurité ou de routage pour chaque type d'attaque ou d'incidents. Les nœuds du réseau disposent de peu de ressources, et les traitements associés à chaque solution vont influencer sur la performance du nœud et par conséquent la performance globale du réseau.
- Une solution proactive reste toujours l'option préférée par rapport à une solution réactive, mais dans le contexte des réseaux dynamiques, l'implémentation d'une telle solution dans un scenario réel peut être considérée non pratique en termes de faisabilité ou de performance.

La motivation à ce travail est donc de proposer une solution alternative [NOU 22] pour assurer une sécurité, et une qualité de service à travers la collaboration des nœuds, et qui aura une répercussion directe sur le service rendu par le réseau. Pour cela, et au lieu d'utiliser une approche standard, qui se base sur l'évaluation des solutions de sécurité et QoS existantes en termes d'efficacité ou de performance, nous avons opté pour une approche différente. Nous proposons une approche qui assure la continuité dans le réseau au lieu de prévenir des attaques ou des comportements indésirables. Si un incident est détecté par un nœud et confirmé par l'ensemble de ces voisins, les nœuds vont l'éliminer du réseau et étendre leur service pour couvrir la zone desservie par ce dernier.

Les nœuds surveillent donc le réseau pendant son fonctionnement de manière distribuée. La méthode que nous proposons permet aux membres du réseau de vérifier le comportement de leurs voisins immédiats à travers le monitoring de certaines métriques sur le service rendu par ces derniers. Le but est de pouvoir effectuer des actions correctives pendant le fonctionnement du réseau.

Nous avons choisi d'appliquer cette solution [NOU 22] sur une flotte de drone afin de permettre une implémentation qui prend un aspect pratique d'une part, et de bénéficier de la mobilité des nœuds pour remplacer le service des nœuds défaillants. Ces réseaux, tel qu'indiquer dans les chapitres précédents, prennent un intérêt de plus en plus important vu leurs aspects pratiques et leurs divers cas d'application.

4.3 Architecture de la solution

Un cadre architectural permet d'organiser la solution en modules et repartir les fonctionnalités sur ces modules. Nous divisons l'architecture de notre cette solution en trois modules (Figure 39):

- Module Classification
- Module Monitoring
- Module Adaptation et Isolation

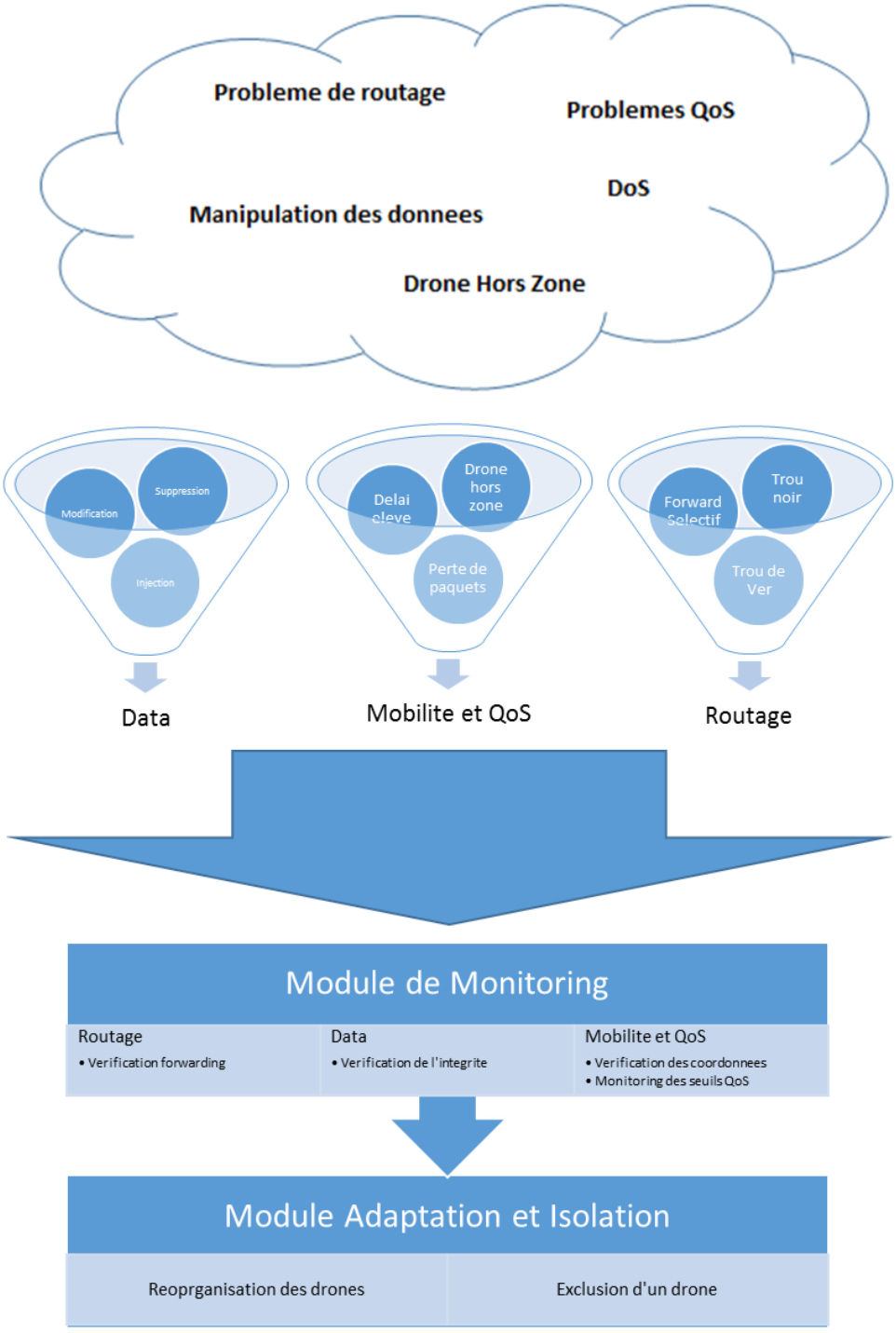

Figure 39 : Architecture du système de monitoring

Module Classification: ce module consiste à classifier un incident. Par exemple, un incident de sécurité, un mauvais comportement ou une dégradation de performation d'un nœud sera associé à une classe. Cela permet d'implémenter un monitoring adéquat des problèmes qui caractérisent cette classe. Nous proposons de diviser ces classes en trois catégories:

- **Classe Routage:** Nous incluons dans cette catégorie tous les problèmes que peut engendrer un mauvais routage des paquets, que ce soit le routage des paquets de données ou de control. Pour cela, chaque nœud va garder des statistiques de routage sur les paquets échangés par ses voisins immédiats.
- **Classe Data:** Cette catégorie regroupe les problèmes liés à la manipulation des données. Certes les paquets peuvent être routés correctement mais peuvent subir une manipulation qui va compromettre leurs intégrités. Dans cette classe, le nœud garde des statistiques sur le champ intégrité des paquets échangés par ses voisins immédiats.
- **Classe Mobilité et QoS:** Les aspects mobilité et Qualité de service sont très important dans un réseau dynamique. Dans notre modèle, nous supposons que les nœuds (ou les drones dans cette d'implémentation) se déplacent chaque un dans une zone à couvrir. Dans cette classe, le nœud garde des statistiques sur les coordonnées de mobilité des nœuds voisins et les métriques QoS de ces derniers.

Module Monitoring:

Le module de monitoring supervise les comportements des nœuds de chaque classe citée plus haut:

- **Monitoring du Routage:** Dans ce cas, nous supervisons le forwording des paquets vers le prochain saut. Ceci nous permet de détecter des attaques de type trou noir, d'inondation de paquets ou des attaques de Deni de Service, car la conséquence de ces attaques est une indisponibilité du service. Le module détectera que le nœud n'est pas en train de router les paquets correctement, du fait que le taux de forwarding est inférieur ou supérieur à un seuil prédéfinit.
- **Monitoring Data:** Dans cette classe, on supervise que le paquet n'a pas subi une modification par le nœud qu'il a routé précédemment. Pour cela, nous utiliserons le champ checksum déjà présent dans le paquet pour ne pas avoir à le recalculer pour chaque paquet.
- **Monitoring Mobilité et Qualité du lien:** Ce module vérifie les coordonnées mobiles des nœuds voisins. Le but est d'assurer qu'un nœud voisin n'accède pas à la zone d'un autre nœud dans son voisinage. Egalement, les métriques QoS (Bande passante, Délai, Perte de Paquets) seront monitorées, car ils ne doivent pas dépasser des seuils bien définie pour avoir un bon niveau QoS partout dans le réseau.

Module d'Adaptation:

Le but du module adaptation est de permettre au réseau d'être résilient et de s'adapter pour assurer une continuité du service en cas de détection d'un nœud défaillant ou ayant un mauvais comportement. L'idée est d'une part d'exclure le nœud en question du réseau, et d'autre part, d'étendre le service des nœuds voisins pour que l'impact de l'incident soit minimisé.

4.4 Solution proposée pour une flotte de drone

4.4.1 Scenario

Comme preuve de concept, nous considérons le scenario d'une flotte de drones à déployer dans une zone pour effectuer une opération de sauvetage (Figure 40). L'objectif est de trouver des survivants après une catastrophe naturelle là où l'accès humain est difficile. Les drones vont capturés des données/images/vidéos sur la zone à couvrir à l'aide de capteurs installés (Camera, Capteur de mouvement, de chaleur, etc.). Dans un tel scénario, la coopération entre les drones est nécessaire en raison de deux facteurs: la flotte de drones doit couvrir une zone généralement étendue, et aussi maintenir les informations de routage à travers un réseau Ad Hoc et en utilisant un protocole de routage. Ceci afin de retransmettre les données capturées à travers les liens sans fil établis entre les drones.

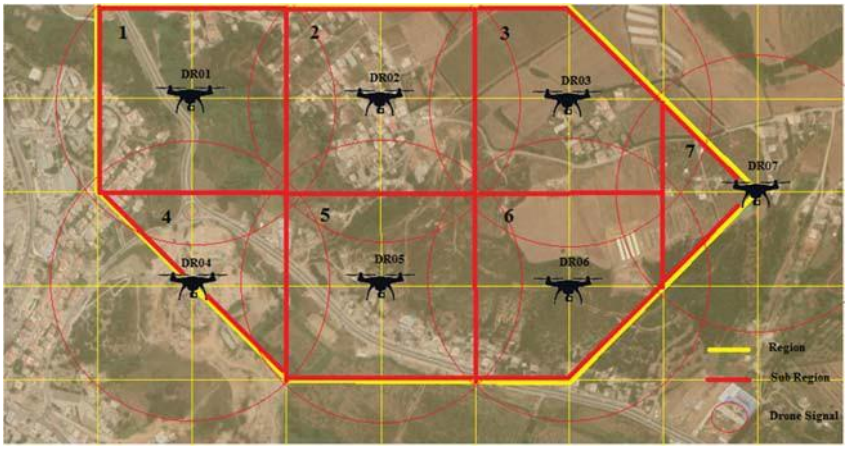

Figure 40: Exemple du scenario de déploiement

Nous avons défini certaines suppositions dans ce scenario afin d'atteindre les objectifs souhaités en termes de collaboration. Premièrement, le drone peut se déplacer librement dans sa région mais doit être capable de couvrir sa zone tout en maintenons des liens de connectivité avec ses voisins. Si la qualité de la liaison est faible en raison d'une mauvaise connectivité lorsque le drone se trouve à la limite de la zone par exemple, nous supposons que le drone peut faire un compromis entre la bande passante et la puissance de son émission, en réduisant par exemple la bande passante et en augmentant la puissance de son signal. Deuxièmement, le cadre proposé doit être indépendant du protocole de routage. Des actions telles que la réorganisation des drones ou l'exclusion d'un drone (en raison de son mauvais comportement ou à cause d'une dégradation de son service) déclenchera une mise à jour dans le la table de routage, pour éviter ainsi le passage par le nœud en question.

4.4.2 Phase de déploiement

Cette phase consiste à déployer une flotte de drones dans une région. Le nombre de drones à déployer dépend de différents paramètres : la surface de la région à couvrir au sol, la bande passante minimale souhaitée pour maintenir des relations de voisinage entre les drones, le gain de l'antenne installée sur les drones (paramètre qui indique l'efficacité de l'envoi et de la réception des signaux), etc.

Tout d'abord, nous devons diviser la région en sous-régions couvertes chacune par un drone. Une sous-région est représentée par un cercle avec les coordonnées *(x,y,z)* du centre et un rayon *(r)* qui indiquera la surface à couvrir. Nous utilisons deux fonctions *OptimalCoverage() (1)* et *DeployParams() (2)* pour calculer les paramètres nécessaires pour une mission donnée.

NBDrones=OptimalCoverage(RegionCoordTable[], MinBW, AntennaGain) (1)

Où *RegionCoordinatesTable* représente la surface de la région à couvrir en fonction des différentes valeurs de coordonnées, *MinBW* est la largeur de bande minimale requise entre deux drones voisins. Nous considérons le minimum car nous supposons que chaque drone se déplace librement dans sa sous-région à couvrir tout en assurant une largeur de bande minimale à assurer avec ses voisins. *AntennaGain* représente le gain de l'antenne omnidirectionnelle utilisée sur les drones, car ce paramètre affectera directement la qualité du signal émis et reçu. La fonction *OptimalCoverage()* calcule donc le parametre *NBDrones*, qui représente le nombre optimal de drones nécessaires pour une mission donnée.

DronesCoordTable[n] = DepolyParams(RegionCoordTable[], NBDrones) (2)

La deuxième fonction *DeployParams()* produit un tableau appelé *DronesCoordTable[]* qui représente les paramètres opérationnels de chaque drone pour démarrer la mission. Chaque entrée de la table comprend les coordonnées de mobilité initiales du drone, le rayon de la surface que le drone doit couvrir, et la puissance d'émission initiale à utiliser pour pouvoir établir des liaisons avec les drones voisins. Ces deux fonctions sont calculées avant le déploiement afin de donner à chaque drone tous les paramètres nécessaires pour opérer dans sa sous-région (Tableau 2).

ID du drone	Coordonnées de mobilité	Rayon de la sous-région	Puissance Tx
dr_i	$(x, y, z)_{dri}$	r_{dri}	pw_{dri}
dr_j	$(x, y1, z)_{drj}$	r_{drj}	pw_{drj}
dr_k	$(x, y, z)_{drk}$	r_{drk}	pw_{drk}
dr_l	$(x, y, z)_{drl}$	r_{drl}	pw_{drl}

Tableau 2: Exemple des paramètres de déploiement d'une flotte de drone

Comme décrit précédemment, une région est divisée en cellules où les drones peuvent se déplacer librement. Le modèle de mouvement est indépendant de la topologie du réseau puisque nous supposons qu'à tout point de la sous-région à couvrir par un drone, la connectivité avec les voisins est toujours maintenue. Le mouvement dépend principalement de la nature de la mission que les drones doivent accomplir. Le résultat de cette phase est un groupe de drones qui vont se déplacer vers leurs positions cibles et commencent leurs mouvements, chacun dans sa sous-région comme indiquée par les coordonnées de mobilités initiales.

4.4.3 Phase de Classification et de Monitoring

Pendant son mouvement, chaque drone va créer une table de statistiques *Stats* pour surveiller le comportement de ses voisins immédiats et échangera cette table avec eux (Figure 41). Ceci afin de construire un système de surveillance distribué. Les paramètres sélectionnés pour construire la table des statistiques sont choisis uniquement parmi les données qui peuvent être vérifiées par les voisins.

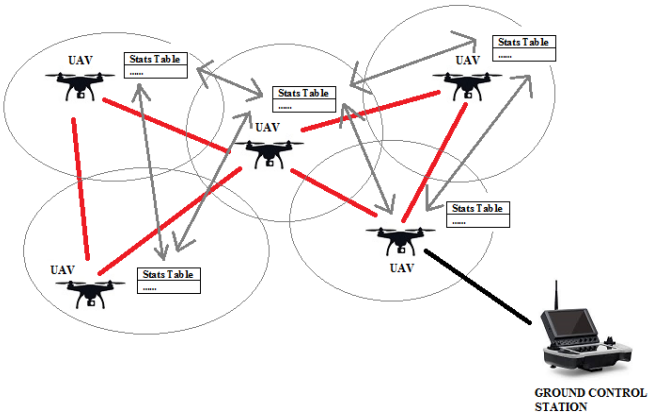

Figure 41 : Echange de la table *Stats* selon la solution proposée

Pour chaque classe, nous avons sélectionné certains paramètres à surveiller. A titre d'exemple:

- pour la classe Routage : le taux de forwarding des paquets d'un nœud vu par ses voisins.
- Pour la classe Data : le taux checksum des paquets d'un nœud vu par ses voisins.
- pour la classe Mobilité et QoS : les coordonnes du nœud ou sa distance du voisin ainsi que ses métriques QoS.

Un exemple de la table des statistiques diffusée par le drone dr_i à un instant t est présenté ci-dessous (Tableau 3) :

Neighbor	Taux FWD	Taux Checksum	QoS Metrics	Distance	Timestamps
dr_j	$fwd(dr_i, dr_x, dr_j)$	$chk(dr_i, dr_x, dr_i)$	$qm(dr_i, dr_i)$	d_{ij}	t
dr_k	$fwd(dr_i, dr_y, dr_k)$	$chk(dr_i, dr_y, dr_k)$	$qm(dr_i, dr_k)$	d_{ik}	t
dr_l	$fwd(dr_i, dr_z, dr_l)$	$chk(dr_i, dr_z, dr_l)$	$qm(dr_i, dr_l)$	d_{il}	t

Tableau 3: Exemple d'une table *Stats* du drone dr1

Taux Forwarding

Le Taux de forwarding $fwd(dr_i, dr_x, dr_j)_t$ (4) est calculé sur la base du nombre de paquets que le drone dr_i a envoyés à une destination finale, par exemple le drone dr_x, en utilisant comme prochain saut le drone dr_j. Le drone dr_i vérifiera que chaque paquet envoyé au drone dr_x via le drone dr_j a été effectivement transmit. Cela permettra au drone dr_i de confirmer que chaque paquet a été routé. Tout nœud dont le taux transfert des paquets est inférieur à un certain seuil et durant une période prédéfinie est détecté comme un nœud potentiellement malveillant et le drone dr_i met à jour sa table de statistiques par conséquent. Nous combinons les informations extraites de la couche liaison de données et de la couche réseau pour suivre les paquets envoyés selon la formule ci-dessous :

> ***$fwd(dr_i, dr_x, dr_j)_t$ = Number of packets sent (Src Mac@dr_i, Dst IP@dr_x, NextHop Mac@dr_j)/Number of packets received (Src Mac@dr_j, Dst IP@dr_x, NextHop Mac@dr_j) with TimeStampPacketSent - TimeStampPacketReceived < 50ms (4)***

Taux CheckSum

A chaque fois que le drone dr_i envoie un paquet au drone dr_x en utilisant comme prochain saut le drone dr_j, le champ checksum $chk(dr_i, dr_x, dr_j)_t$ (5) est enregistré afin de vérifier si le paquet retransmis par le drone dr_j a la même valeur. De cette façon, nous pouvons nous assurer qu'un paquet n'a pas été altéré avant d'être retransmis. Le champ checksum de la couche transport est utilisé afin d'éviter de recalculer un nouveau checksum pour chaque paquet. La formule pour suivre le checksum est la suivante :

> ***$chk(dr_i, dr_x, dr_j)_t$ = TransportLayerChecksum PacketSent(Src Mac@dr_i, Dst IP@dr_x, NextHop Mac@dr_j) XOR TransportLayerChecksum PacketReceived(Src Mac@dr_j, Dst IP@dr_x, NextHop Mac@dr_j) where TimeStampPacketSent - TimeStampPacketReceived < 50ms (5)***

Métriques QoS

La qualité de la liaison entre un drone dr_i et un drone dr_j appelée $mq(dr_i, dr_j)$ (métrique QoS) est la perception par le drone dr_i du lien avec son voisin dr_j. Cette mesure vise à surveiller la qualité des liaisons dans le réseau. Nous avons choisi pour la qualité du lien une métrique composite à calculer pour chaque voisin. Cette métrique se compose de trois paramètres :

Bande passante consommée: Elle représente à un instant t, la bande passante utilisée par dr_j (total des paquets envoyés et reçus) selon la perception de dr_i.

> ***$Bw(dr_i, dr_j)_t = \sum$ (packets sent and received by dr_j as seen by dr_i* packet size * 8)$_t$*** **(6)**

Délai de retransmission: Cette métrique mesure le temps entre l'émission du paquet au voisin et sa retransmission par le voisin vers le prochain saut.

> ***$Delay(dr_i, dr_j)_t$ = TimeStamp Packet sent (dr_i, dr_j)$_t$ – TimeStamp Packet Sent(dr_i, Next Hop dr_j)$_t$ (7)***

Taux de Paquets Non Retransmis (TPNR): On mesure avec cette métrique le taux de paquets envoyés par dr_i et non retransmis par dr_j.

$$TPNR(dr_i, dr_j)_t = 100 - (Number\ of\ packets\ checked(dr_i, dr_j)/Number\ of\ packets\ received(dr_i, Next\ Hop\ dr_j))_t \quad (8)$$

Contrôle des coordonnées de mobilité

Le contrôle de la mobilité est utilisée pour s'assurer que chaque drone opère dans la zone qui lui a été attribuée et qu'il n'interfère pas dans d'autres régions. Le drone peut vérifier la position d'un voisin en se basant sur la puissance du signal qu'il reçoit et sur les coordonnées publiées par les autres drones dans la table *Stats*. Tout d'abord, le drone vérifie que le drone voisin n'opère pas dans d'autres zones. Pour cela, le drone estime la position et la distance entre le drone dr_i et le drone dr_j et la compare avec la zone qu'il doit couvrir, en utilisant la formule d'affaiblissement du signal dans un espace libre [UIT 19]. Ensuite, il vérifie si les coordonnées reçues dans le tableau des *Stats* correspondent aux valeurs estimées en utilisant la méthode de localisation par triangulation [Kar 17]. L'algorithme de contrôle des coordonnées de mobilité est le suivant:

Calculate d_{ij} (distance between dr_i and dr_j) from Signal Strength RSSI(dr_i, dr_j)

Calculate $(x_j, y_j, z_j)'$ from dr_i, dr_k et dr_l Coordinates and d_{ij}, d_{kj}, d_{kl} Distances

If $(x_j, y_j, z_j)' \neq (x_j, y_j, z_j)$

Then node is Out Of Zone

Il s'agit en effet d'une double vérification. En premier lieu le drone dr_j n'opère pas dans la zone de dr_i. Et en deuxième lieu, que les coordonnées *x, y, z* des voisins publiées dans leurs tables sont actuellement correcte en utilisant la localisation par triangulation.

4.4.4 Adaptation de la topologie

L'adaptation de la topologie est utilisée pour permettre au réseau d'être résilient et de s'adapter et assurer une continuité de service. L'objectif de l'échange des paramètres précédents est de permettre aux nœuds de prendre des mesures correctives en fonction des valeurs reçues et vérifiées.

Chaque drone met à jour sa table de statistiques périodiquement et partage cette information avec les drones voisins. Si le drone reçoit la même information d'autres drones à propos du meme voisin, il va marquer le drone comme ayant des problèmes et pourra potentiellement terminer sa relation de voisinage. Les seuils des métriques sont fixés dans la phase de déploiement et représente le niveau minimal requit dans le réseau pour un service acceptable.

Une évaluation périodique de ces paramètres est effectuée et un événement d'adaptation de la topologie est déclenché dans les situations suivantes :

- Les métriques QoS d'un drone donné est en dehors des seuils prédéfinis et durant une période continue dans le temps, et a également été vérifié par les drones voisins.
- Les taux d'acheminement (forwarding) ou de contrôle (checksum) sont inférieurs à un seuil prédéfini et durant une période continue dans le temps, et ceci a également été vérifié par les drones voisins.
- Un drone n'opère plus dans sa zone autorisée, soit sa présence a été détectée dans une zone non autorisée ou bien il envoie des données de mobilité non valides pendant une période continue dans le temps. De plus, cela a été vérifié par les autres voisins.

Nous utilisons l'algorithme suivant pour vérifier si les seuils des métriques calculées sont atteints ou pas :

At t_i, for each Metric

Calculate Average (Local Metrics + Received Metrics)

From (t_i – Δt) to t_i

If Average values < $Threshold_{min}$ || Average values > $Threshold_{max}$

Then Trigger Adaptation

A travers ce système de surveillance distribué, chaque drone vérifie les métriques calculées en locale et ceux reçus par ces voisins. A la détection d'un drone en infraction pendant une période bien définie, on peut mettre fin à la relation de voisinage. Chaque drone va ensuite étendre sa zone de couverture pour inclure une partie de la zone du drone exclu et par conséquent augmenter sa puissance d'émission pour former éventuellement de nouvelles relations avec d'autres drones avec lesquels le drone en infraction était voisin.

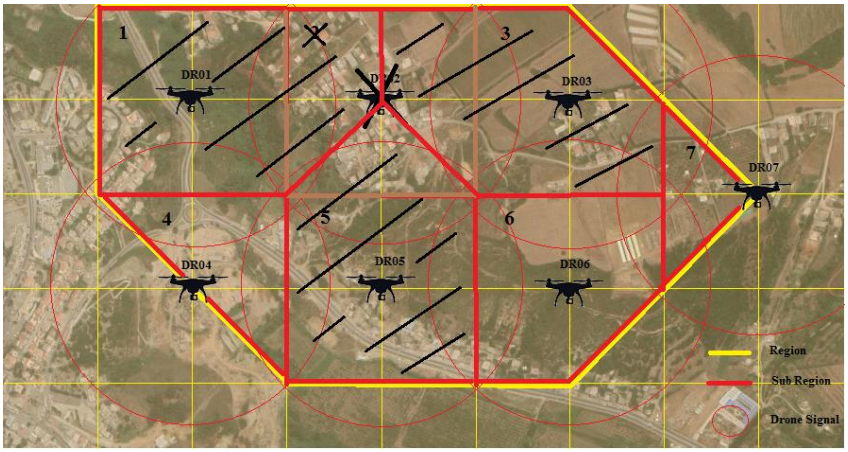

Figure 42 : Adaptation de la topologie par élimination du drone

4.5 Simulation et résultats

Nous avons utilisé NS3 pour implémenter la simulation et valider l'approche proposée. NS3 est un simulateur à événements discrets très largement utilisé dans la recherche académique. En raison de son modèle libre et évolutif, Il permet l'ajout de modèles correspondant à des technologies émergentes.

NS3 est capable de simuler des réseaux complexes de manière détaillée et réaliste, en combinant plusieurs objets définis en C ++ avec un modèle représentant un concept réseau. Les classes qui modélisent ce concept sont regroupées en modules. Le fait que NS3 fonctionne selon le principe à événements discrets signifie qu'une simulation consiste en une série d'événements, chacun étant lié à un certain temps. La tâche du simulateur consiste à exécuter ces événements (c'est-à-dire à effectuer l'appel de fonction approprié lié à cet événement), ce qui entraîne un changement de l'état de la simulation et éventuellement de l'arrangement d'autres événements.

Pour les besoins de notre simulation, nous avons considéré une zone de 750x750m divisée en zones qui seront couverte par 25 drones. Les drones sont organisés en grille 5x5 avec un diamètre de 150m pour chaque zone à couvrir selon le modèle NS3 **GridPositionAllocator**. Les drones peuvent se déplacer aléatoirement dans leur zone respective en utilisant le modèle **Randow2DWalk**. Les données seront envoyées et reçues par les drones situés à la périphérie du réseau afin d'impliquer les autres drones dans le routage des paquets. Le protocole de routage que nous avons utilisé est OLSR.

Nombre de nœuds	Distance entre les nœuds	Disposition des nœuds	Modèle de Mobilité	Protocole de Routage
25	150m	Grille 5x5	Random2DWalk	OLSR

Tableau 4: Paramètres de simulation dans NS3

4.5.1 Monitoring des paramètres Sécurité

Nous avons d'abord exécuté la simulation sans aucun nœud malveillant afin d'obtenir des mesures de base et de pouvoir exclure les valeurs faux positives plus tard dans la simulation. Ensuite, nous avons introduit un nœud malveillant en modifiant son comportement normal. Nous avons choisi deux types de comportement malveillant pour cette partie de la simulation: le nœud peut ne pas router des paquets de manière aléatoire dans le temps, ou bien le nœud peut altérer certains paquets avant de les router vers le prochain saut.

La figure 42 montre les mesures de base lorsque le réseau fonctionne sans aucun comportement malveillant. Nous avons inclus pour chaque nœud le nombre de fois où le nœud a participé au routage, et également le nombre d'occurrences où le nœud a une qualité de signal faible. Nous avons également inclut les valeurs de détection faux positives pour chaque nœud lorsque le taux de Forwarding est inférieur au seuil de 90%. Nous avons remarqué que les valeurs faux positives sont maximales lorsque le nœud est le plus utilisé (en terme de routage) ou il a des occurrences élevées d'un signal faible.

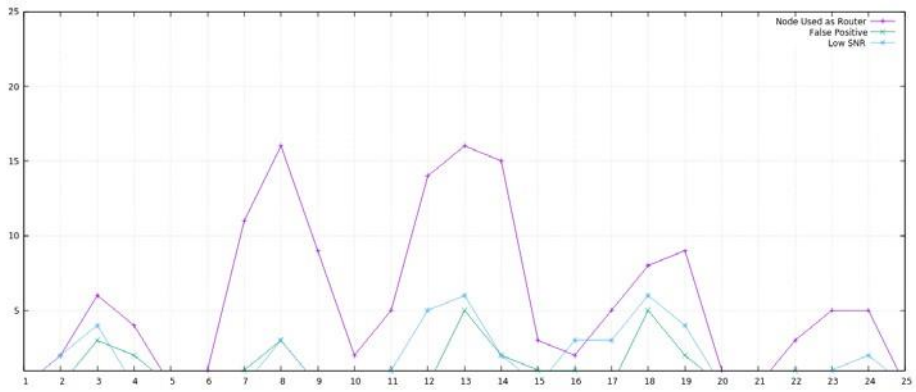

Figure 43 : Métriques sans nœud malveillant dans le réseau

Ensuite, nous avons exécuté le réseau en simulant chaque nœud comme étant malveillant séparément. Nous avons ensuite collectés les statistiques concernant le nombre de fois où les valeurs étaient inférieures au seuil de 90%. Lorsque le nœud malveillant ne route pas les paquets de manière aléatoire (Figure 43), nous avons remarqué que la détection devient efficace lorsque le nœud ait été utilisé plus souvent (le seuil de détection de l'abandon des paquets dans ce scénario est > 5). La méthode de détection est efficace dans ce cas car les valeurs obtenues sont toujours supérieures aux mesures faux-positives obtenues précédemment. De plus, un signal faible pourrait générer plus de valeurs faux-positives, et ceci pourra le faire détecter comme un nœud malveillant par ces voisins.

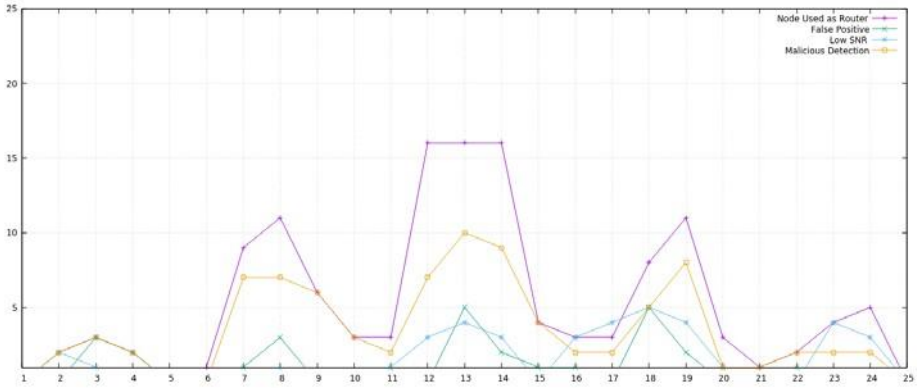

Figure 44 : Métriques avec un nœud malveillant qui abandonnant des paquets.

La figure 44 montre le même scénario lorsque le nœud modifie les paquets avant de les réacheminés vers un voisin. La détection est plus efficace car les valeurs faux positives sont toujours proches de zéro. De plus, la détection est efficace même si le nœud n'a pas été beaucoup utilisé ou son SNR est faible. Cela est dû au fait que la plupart des erreurs de transmission ne sont pas interprétées comme un problème d'intégrité des paquets, car les paquets sont déjà rejetés par la couche liaison de données.

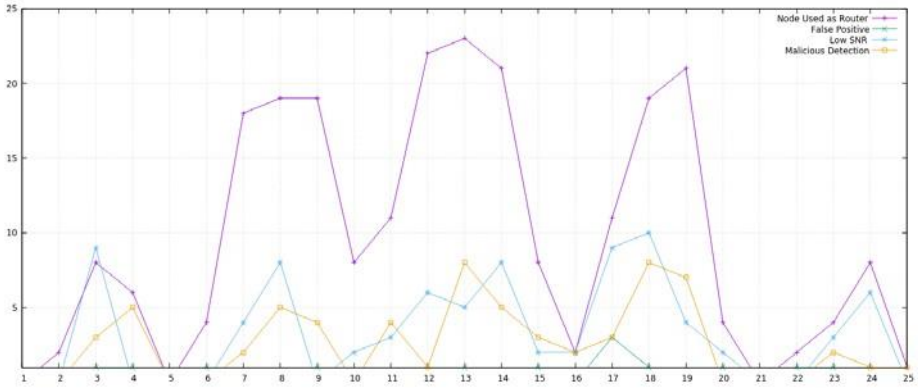

Figure 45 : Métriques avec un nœud malveillant modifiant des paquets

A travers l'analyse des résultats, l'efficacité de la détection est directement liée au taux de participation du nœud au routage des paquets. Par conséquent, les nœuds situés au centre du réseau avec plus de relations de voisinage seront détectés plus efficacement et leurs statistiques seront moins susceptibles d'être interprétés comme des valeurs faux-positives. De plus, l'efficacité de la détection est vérifiée sur la base de la différence entre les valeurs de faux positifs initialement calculées sans comportement malveillant dans le réseau et les valeurs calculées lors d'une attaque sur le routage et l'intégrité des échanges de paquets. Nous pouvons dans ce cas confirmer la validité de la méthode de détection en prenant en considération le niveau du SNR reçu et le taux de participation du nœud au niveau du routage des paquets.

4.5.2 Monitoring des paramètres QoS

Afin de valider l'efficacité du monitoring des métriques QoS, nous avons exécuté la simulation avec un maximum de trafic dans le réseau. Pour cela, chaque nœud va transmettre un maximum de paquets jusqu'à saturer son lien. Les paramètres utilisés sur chaque nœud sont les suivants:

Protocole	Taille des paquets	Fréquence d'envoie	Bande Passante	Nombre Max de Paquets
UDP	65500 octets	0.01s	1 Mbps	10 000

Tableau 5 : Paramètres de simulation QoS dans NS3

Nous avons mesuré les paramètres QoS cités plus haut (Bandwidth, Delai, TPNR) afin de pouvoir détecter des nœuds dont les métriques QoS ont atteint des valeurs critiques et qui peuvent par conséquent influencer sur les performances du réseau. Nous avons obtenues les graphes suivants:

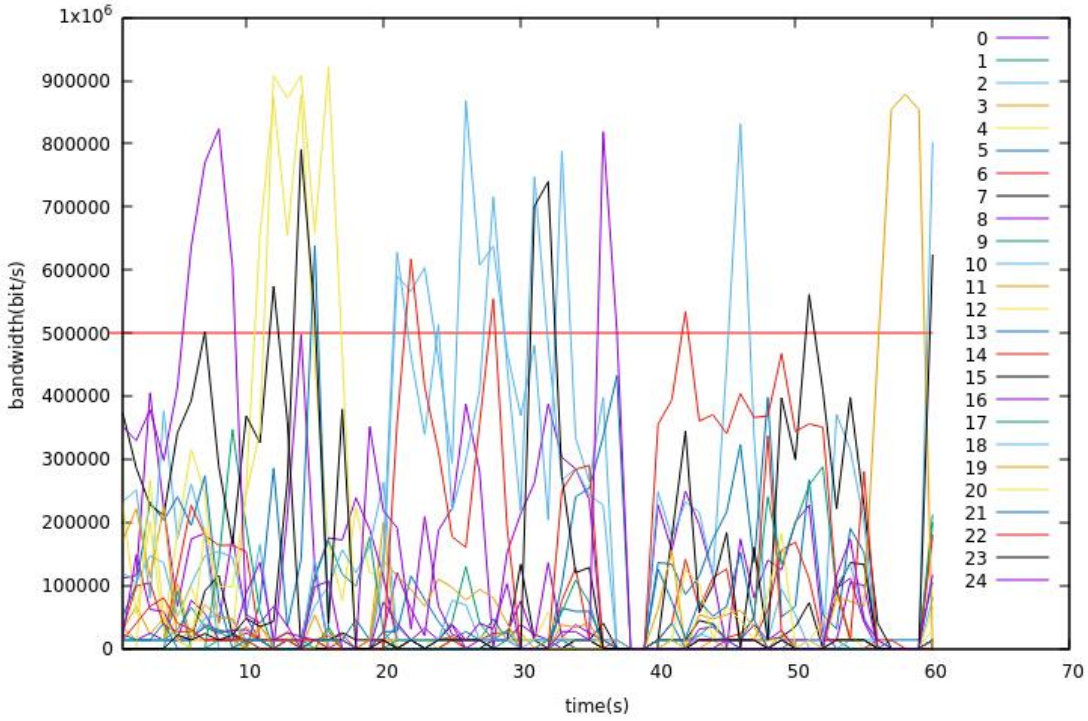

Figure 46 : Bande Passante par nœud durant la simulation QoS

La figure 45 montre l'utilisation de la bande passante par drone obtenue de l'estimation effectuée par ses voisins immédiats dans le temps. Nous avons défini le seuil critique de 500kps pour un lien à 1Mbps (50% de la capacité du lien). Nous remarquons que même si certain nœud dépassent la valeur du seuil, ceci n'est que momentané et ne dure pas dans le temps.

L'évaluation du paramètre Bandwidth permet donc au nœud d'estimer la charge du trafic sur le voisin en termes de bande passante. Un nœud saturé en permanence ne pourra pas traiter a temps le flux des paquets qui arrivent, et par conséquent va causer une dégradation des services si le nœud continu de recevoir des paquets a la même cadence.

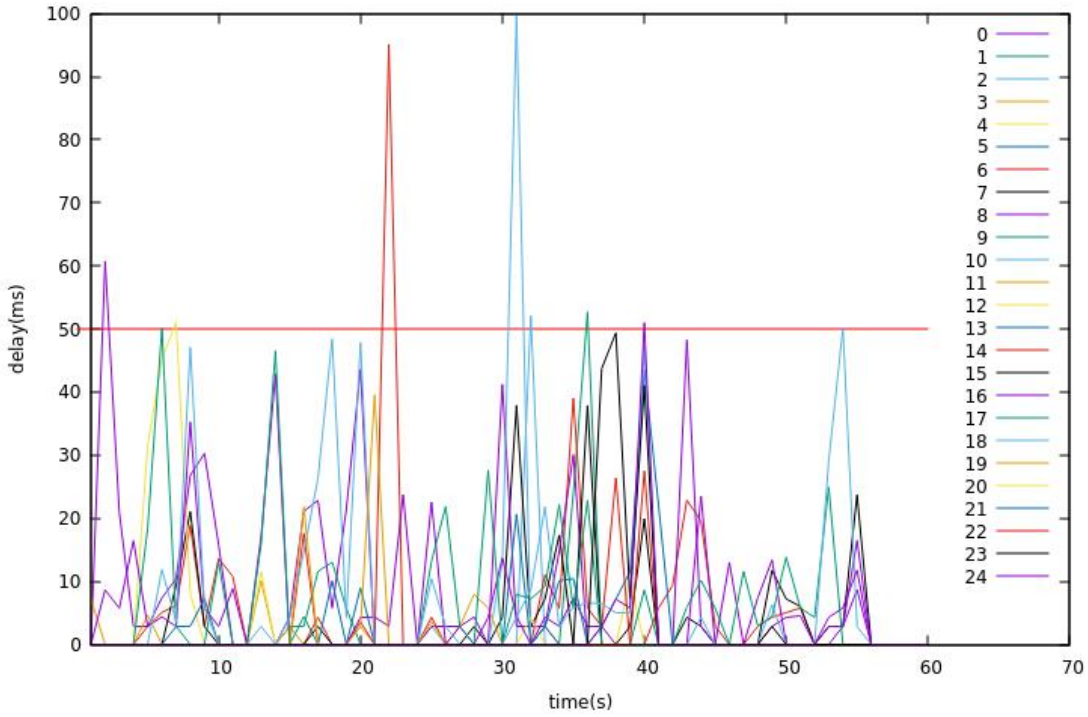

Figure 47: Délai de retransmission des paquets durant la simulation QoS

La figure 46 illustre la métrique délai qui représente le temps entre l'envoi d'un paquet et sa retransmission par le nœud voisin. Le seuil critique dans ce cas est 50ms. De même, les nœuds presque tous restent en dessous du seuil sauf pour certain nœuds ou nous remarquons des piques momentanés.

Un délai élevé peut être interprété comme une congestion sur le nœud lui-même, par exemple, une charge CPU/Mémoire ne permettant pas à ce nœud de traiter les paquets a temps, ou bien une saturation de la bande passante sur son lien, ce qui augmente le délai de traitement des paquets dans les files d'attente avant leurs retransmissions.

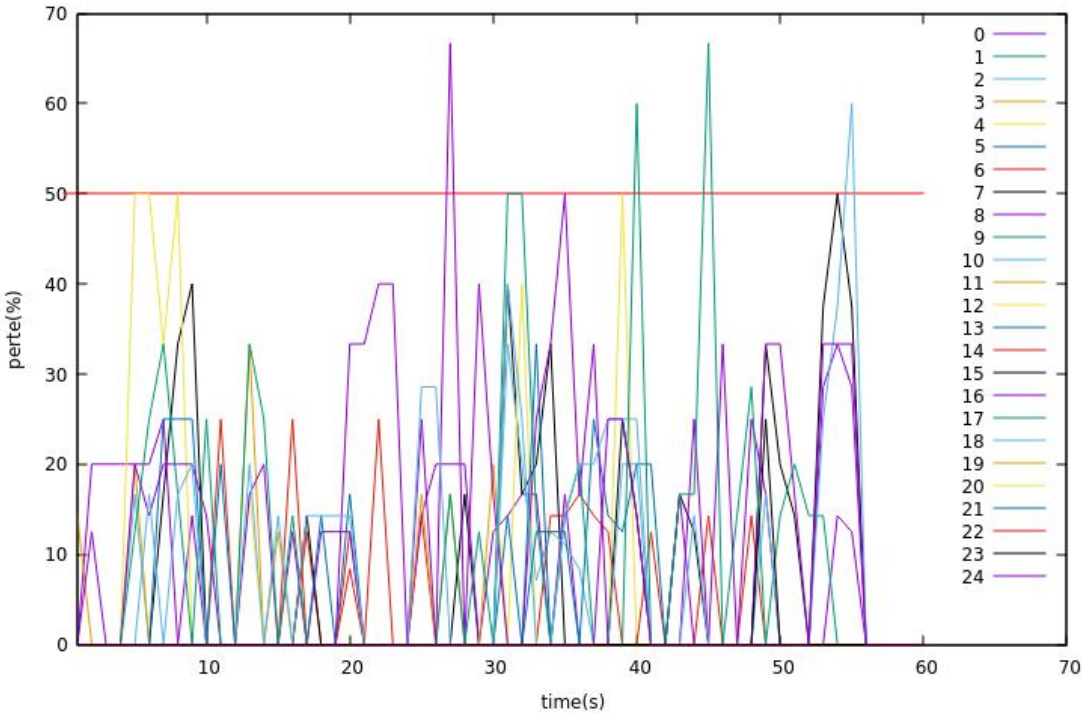

Figure 48: Taux TPNR par nœud durant la simulation QoS

La figure 47 montre le taux des paquets non retransmis par les nœuds voisins. Ces paquets sont observés sur la couche liaison de données et va causer donc la retransmission de ces paquets. Les valeurs de ce taux reflète la nature du réseau mobile ou les distances entre les nœuds varient dans le temps et se répercute les relations de voisinage. Par conséquent, des paquets seront perdus et donc retransmis à travers une route alternative dans la table de routage ou bien dès la découverte d'une nouvelle route.

4.5.3 Monitoring des paramètres de mobilité

Dans ce cas, chaque nœud va estimer la distance avec ces voisins immédiats et vérifie ces valeurs sur la base du signal reçu du voisin et sa propre position actuelle. Afin de vérifier l'efficacité de la méthode vérification, nous avons comparé les distances calculées avec les distances réelles obtenues de la simulation, et observer ainsi si l'écart est toujours réduit. Egalement, nous avons considéré une valeur minimale du signal reçu (RSSI) de -90dbm pour prendre en considération l'estimation de la distance avec un drone.

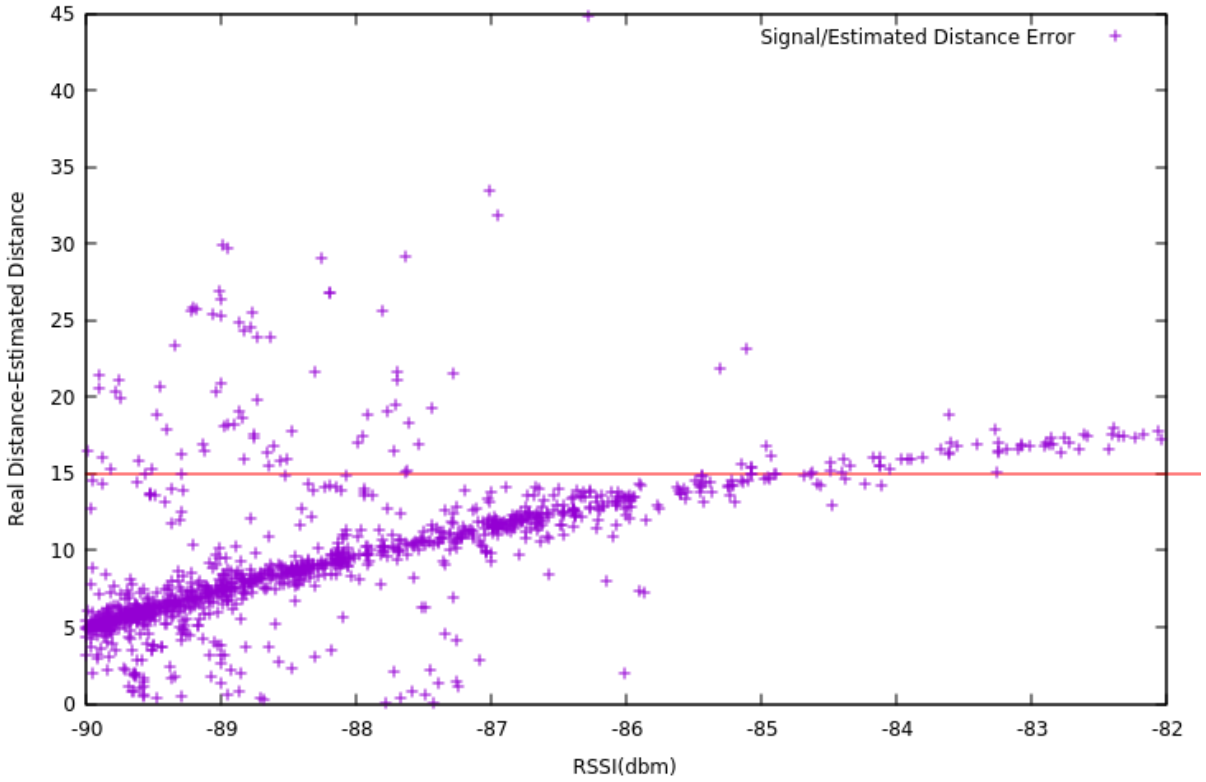

Figure 49: Différence entre la distance estimée et la distance réelle par rapport au signal reçu

Comme les drones se déplacent chacun dans une zone 150x150m, nous avons défini une marge d'erreur de 15m au niveau de l'estimation de la distance (10% de la largeur de la zone). La Figure 48 montre que la plupart des estimations sont en dessous de la marge d'erreur, et avec l'amélioration du signal RSSI reçu, nous avons moins de valeurs au-dessus du seuil d'erreur établi.

Il faut noter que le paramètre distance est important dans le contrôle des paramètres de mobilité du fait que la vérification se fait sur la base de l'estimation de la distance puis ensuite cette estimation est utilisée pour déterminer la position du voisin.

4.6 Discussion des résultats

Tout d'abord, les paramètres de la simulation ont été définis afin de se rapprocher d'un scenario de déploiement réel. Rappelons que nous avons utilisé 25 drones sur une surface de 750mx750m (0,5 Km^2 de surface à couvrir) et avec un mouvement aléatoire en termes de modèle de mobilité. Le changement de ces paramètres affectera la durée de la mission et les ressources nécessaires pour l'accomplir. Par exemple, augmenter la surface à couvrir nécessite forcément plus de drones pour couvrir la zone et prendra aussi plus de temps, et aussi dans le cas ou en procède à l'adaptation pour replacer le service de un ou plusieurs drones. Un autre paramètre à considérer dans ce cas et l'autonomie de la batterie vu que la mission prendra plus de temps.

Le choix d'une solution de monitoring réactive est justifié par le cout de calcul faible. Les paquets diffusés par les voisins sont reçus que ce soit si le nœud est destinataire du paquet ou pas. Au lieu que le nœud ignore le paquet d'un nœud voisin s'il n'est pas le destinataire, il en extrait les champs significatifs et calcule les métriques associées au module de monitoring. Un autre paramètre qui peut affecter les performances est la fréquence à laquelle on fera l'échange de la table S*tats*. Un échange fréquent peut entrainer une surcharge sur le réseau de ces paquets de contrôle, ou bien le traitement récurrent de ces tables par le nœud.

Le monitoring du forwarding des paquets permet de détecter un groupe de menaces dont le but est le déni de service sur le nœud. Ceci est économique en termes de cout de détection vu que nous supervisons que les conséquences de ce groupe de menaces. Le monitoring de la manipulation des paquets permet d'assurer l'intégrité des paquets retransmis. Certes, les méthodes de cryptages permettent d'assurer l'intégrité des paquets mais ils sont inefficaces si un nœud dispose déjà des clés de cryptage. L'avantage de notre méthode de contrôle d'intégrité est de réutiliser les champs checksum du paquet au niveau de la couche transport et donc pas de calcul additionnel est nécessaire en termes de contrôle d'intégrité.

Les métriques QoS sont également calculées de la même manière que les métriques de sécurité, à travers l'extraction des informations utiles à partir des entêtes des paquets. Les métriques Bandwidth, delay et TPNR sont interprétées indépendamment, et chaque métrique est supervisée dans le temps par rapport à un seuil prédéfini. Une autre alternative serait de combiner ces métriques en une seule. Les protocoles de routage utilisent cette technique en ajoutant des poids à chaque métrique afin que ces valeurs aient un même ordre de grandeur.

La vérification de la mobilité se fait par chaque drone de manière distribuée ou chaque drone vérifie que le signal reçu d'un voisin ne correspond pas à un drone opérant dans sa propre zone. En utilisant cette approche, il n'est pas nécessaire de connaitre les paramètres de zones des autres drones, ce qui simplifie la méthode de vérification.

4.7 Conclusion

Nous avons présenté dans ce chapitre une architecture qui permet à une flotte de drones de surveiller certains paramètres clés du réseau de manière distribuée. Chaque drone de la flotte surveille l'activité de ses voisins immédiats et enregistre les données recueillies dans un tableau de statistiques. Une décision n'est prise que si un groupe de drones se mettent d'accord sur la même conclusion. Cette décision est basée sur des paramètres que chaque drone peut vérifier sur ces voisons comme la qualité du lien, le taux forwarding, le taux checksum et la vérification des coordonnées de mobilité.

Nous nous sommes concentrés sur l'évaluation de l'efficacité de la détection en faisant fonctionner le réseau et en observant les statistiques collectées. Nous avons effectué une simulation afin de déterminer les valeurs opérationnelles de cette solution. Certains de ces paramètres clés que nous avons déterminées représentent les valeurs des seuils pour déclencher l'adaptation de la topologie dans le réseau en cas d'incidents ou une dégradation de la qualité dans le réseau.

Conclusion Générale

Les réseaux dynamiques présentent de nombreux challenges que ce soit en termes de sécurité des échanges ou bien en termes de la qualité des communications. Il faut non seulement éviter de nombreuses attaques causées par des entités externes ou par des nœuds compromis, mais aussi assurer que la dégradation des performances du réseau causées par un incident soit raisonnable afin d'offrir une continuité de service à tout moment.

En terme de Sécurité, des solutions différentes de sécurité sont proposées ; soit sous forme d'un protocole de routage sécurisé ; soit sous forme d'une solution globale assurant un ou plusieurs prérequis de la sécurité (Confidentialité, Disponibilité, Intégrité, etc.).

En terme de de Qualité de service, la plupart des approches visant à offrir une QoS dans les réseaux dynamiques se basent sur la modification d'un protocole de routage donné ou bien offrir des mécanismes permettant de garantir les ressources QoS sur une couche particulière du réseau. L'approche de communication inter-couches (cross-layer) permet également d'optimiser les performances pour un meilleur service rendu par les différents couches du réseau.

La partie contribution de cette thèse consiste à proposer une architecture de communication pour un système de monitoring d'une flotte de drones. Pour atteindre cet objectif, notre étude s'est d'abord focalisée sur l'étude des solutions actuelles de façon générale et les travaux de recherche récents sur les drones. Ensuite, nous nous sommes focalisés sur la proposition d'un modèle de monitoring qui puisse contrer un maximum d'incidents sans pour autant dégrader les performances du réseau.

Notre approche c'est portée sur une solution réactive qui résume les incidents possibles à travers le calcul de certains paramètres clés du réseau, et de réorganiser les nœuds de manière à contrer l'incidents en éliminant le nœud en question, et ainsi assurer une continuité de service. Notre approche est originale du fait qu'on ne retrouve pas dans la littérature une approche qui solutionne un problème de Sécurité ou de QoS par le remplacement et la réorganisation des nœuds.

Bien que cette thèse apporte des contributions dans le cadre des communications sécurisées pour les flottes de drones, plusieurs pistes de travaux futurs peuvent être considérées comme compléments de recherche à nos travaux. Nous pouvons lister par exemple:

- Intégrer et détecter plus d'attaques en incluant plus de paramètres à surveiller.
- Evaluer les valeurs des seuils pour la détection des incidents afin d'éviter des valeurs faux-positives.
- Evaluer la performance du système d'adaptation afin de trouver jusqu'à quel point nous pouvons éliminer des nœuds et garder toujours un service acceptable.

Malgré les résultats obtenus à travers la simulation, Il reste tout de même un certain nombre de choses à analyser avant de passer à une implémentation effective. Il faudrait effectuer de nouveaux essais dans différentes conditions de déploiement, et en changeant plus de paramètres de simulation avant une mise en œuvre pratique.

Publications et Conferences

A distributed monitoring scheme for a fleet of UAV flying drones

International Journal of Mobile Network Design and Innovation, 2022 Vol.10 No.3, pp.113 - 120

Received: 27 Jan 2021
Accepted: 30 Jul 2021
Published online: 26 Oct 2022

DOI: 10.1504/IJMNDI.2022.10051465

Security Threats to Wireless Dynamic Networks: a Survey

International Conference on Networking Telecommunications, Biomedical Engineering and Applications, Boumerdes (ICNTBA'19)

Boumerdes 4 – 5 Nov 2019

Références Bibliographiques

[AHM 21] Ahmad H. Sawalmeh, Noor Shamsiah Othman, An Overview of Collision Avoidance Approaches and Network Architecture of Unmanned Aerial Vehicles (UAVs), 2021, https://doi.org/10.48550/arXiv.2103.14497

[AKR 17] R. N. Akram et al., "Security, privacy and safety evaluation of dynamic and static fleets of drones," 2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC), 2017, pp. 1-12, doi: 10.1109/DASC.2017.8101984.

[AKY 05] Akyildiz, Ian & Wang, Xudong. (2005). Survey on wireless mesh networks. Communications Magazine, IEEE. 43. S23 - S30. 10.1109/MCOM.2005.1509968.

[ALD 18] Al-Dhief, Fahad Taha, Naseer Sabri, M. S. Salim, Sarah Fouad and Syed Alwee Aljunid. “MANET Routing Protocols Evaluation: AODV, DSR and DSDV Perspective.” (2018).

[ALM 18] AlMansour, Norah & Alahmadi, Saad. (2018). Secure Ad Hoc On-Demand Distance Vector Routing Protocol in WSN. 1-4. 10.1109/CAIS.2018.8441991.

[ALT 16] Altawy, Riham & Youssef, Amr. (2016). Security, Privacy, and Safety Aspects of Civilian Drones: A Survey. ACM Transactions on Cyber-Physical Systems. 1. 1-25. 10.1145/3001836

[ALZ 13] Alzaid, H., Alfaraj, M., Ries, S., Jøsang, A., Albabtain, M., Abuhaimed, A. (2013). Reputation-Based Trust Systems for Wireless Sensor Networks: A Comprehensive Review. In: Fernández-Gago, C., Martinelli, F., Pearson, S., Agudo, I. (eds) Trust Management VII. IFIPTM 2013. IFIP Advances in Information and Communication Technology, vol 401. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-38323-6_5

[ANG 18] Angelo Trotta, Luca Sciullo. QoS-Based Mobility System for Autonomous Unmanned Aerial Vehicles Wireless Networks. International Conference on Wired/Wireless Internet Communication (WWIC), Jun 2018, Boston, MA, United States. pp.233-245, 10.1007/978-3-030-02931-9_19. hal-02269724

[BAD 04] H. Badis and K. Al Agha, "QOLSR multi-path routing for mobile ad hoc networks based on multiple metrics: bandwidth and delay," 2004 IEEE 59th Vehicular Technology Conference. VTC 2004-Spring (IEEE Cat. No.04CH37514), 2004, pp. 2181-2184 Vol.4, doi: 10.1109/VETECS.2004.1390660.

[BEL 20] Sid Ahmed Hichame Belkhira. Optimisation de la QoS dans les réseaux adhoc mobiles. Réseaux et télécommunications [cs.NI]. Université de Haute Alsace - Mulhouse; Université Djillali Liabès (Sidi Bel-Abbès, Algérie), 2020.

[CAP 03] Capkun, Srdjan & Buttyan, Levente & Hubaux, Jean-Pierre. (2003). Self-Organized Public-Key Management for Mobile Ad Hoc Networks. Mobile Computing, IEEE Transactions on. 2. 52-64. 10.1109/TMC.2003.1195151.

[BHO 16] Bhoopathy, Vignesh Mandalapa, Mohamed Ben Haj Frej, Steve Richard Ebenezer Amalorpavaraj and Aishwarya Mandalapa Bhoopathy. “Zone Routing Protocol (ZRP) - A Novel Routing Protocol for Vehicular Ad-hoc Networks.” (2016).

[CLA 03] Clausen, T., Ed., and P. Jacquet, Ed., "Optimized Link State Routing Protocol (OLSR)", RFC 3626, DOI 10.17487/RFC3626, October 2003, <https://www.rfc-editor.org/info/rfc3626>.

[DRO 13] Juliette Dromard. Vers une solution de contrôle d’admission sécurisée dans les réseaux mesh sans fil. Réseaux et télécommunications [cs.NI]. Université de Technologie de Troyes, 2013. Français. ⟨NNT : 2013TROY0028⟩. ⟨tel-02969095⟩

[ELA 15] A Study of Black Hole Attack Solutions On AODV Routing Protocol in MANET, Elahe Fazeldehkordi, I.S. Amiri, Oluwatobi Ayodeji Akanbi, 1st Edition - November 3, 2015, eBook ISBN: 9780128053799

[GAN 11] Gangwar, Sanjeev & Kumar, Krishan. (2011). Mobile Ad Hoc Networks: A detailed Survey of QoS Routing Protocols. International Journal of Distributed and Parallel systems. 2. 10.5121/ijdps.2011.2626.

[GOK 11] Vikrant Gokhale, S.K. Ghosh, and Arobinda Gupta, Classification of Attacks on Wireless Mobile Ad Hoc Networks and Vehicular Ad Hoc Networks A Survey, CRC Press, 2011

[GOU 13] Gour, Mahesh & Suman, Amrit. (2013). Detection and Prevention of Wormhole Attack in ALARM Protocol (MANETs).

[GUL 12] Mandeep Kaur Gulati; Krishan Kumar, QoS routing protocols for mobile ad hoc networks: a survey, International Journal of Wireless and Mobile Computing, 2012 Vol.5 No.2, pp.107 - 118, DOI: 10.1504/IJWMC.2012.046783

[HER 12] E. Hernandez-Orallo, M. D. Serrat, J. Cano, C. T. Calafate and P. Manzoni, "Improving Selfish Node Detection in MANETs Using a Collaborative Watchdog," in IEEE Communications Letters, vol. 16, no. 5, pp. 642-645, May 2012, doi: 10.1109/LCOMM.2012.030912.112482.

[HU 03] Y. Hu, A. Perrig, and D. Johnson. Packet leashes: A defense against wormhole attacks in wireless ad hoc networks. In Proceedings of INFOCOM, 2003

[HUA 22] HUAWEI Configuration Guide - WLAN-AC S7700 and S9700 V200R011C10 https://support.huawei.com/enterprise/en/doc/EDOC1000178322/963d7c7d/80211-standards#fig_dc_fd_wlan_basic_000501 (2022).

[JUB 19] Jubair, M.A.; Mostafa, S.A.; Muniyandi, R.C.; Mahdin, H.; Mustapha, A.; Hassan, M.H.; Mahmoud, M.A.; Al-Jawhar, Y.A.; Al-Khaleefa, A.S.; Mahmood, A.J. Bat Optimized Link State Routing Protocol for Energy-Aware Mobile Ad-Hoc Networks. Symmetry 2019, 11, 1409. https://doi.org/10.3390/sym11111409

[KAN 19] Kanellopoulos, Dimitris. (2019). Recent Progress on QoS Scheduling for Mobile Ad Hoc Networks. Journal of Organizational and End User Computing. 31. 37-66. 10.4018/JOEUC.2019070103.

[Kar 17] T. Karlsson et M. Persson, 'Outdoor localization in long range WSN using trilateration', Dissertation, 2017.

[KHO 13] Khoukhi, Lyes & Badis, Hakim & Merghem-Boulahia, Leïla & Esseghir, Moez. (2013). Admission Control in Wireless Ad hoc Networks: A Survey. EURASIP Journal on Wireless Communications and Networking. 2013. 10.1186/1687-1499-2013-109.

[KIM 16] Kim, Geon-Hwan, Jae-Choong Nam, Imtiaz Mahmud and You-Ze Cho. “Multi-drone control and network self-recovery for flying Ad Hoc Networks.” 2016 Eighth International Conference on Ubiquitous and Future Networks (ICUFN) (2016): 148-150.

[KRI 17] C. G. L. Krishna and R. R. Murphy, "A review on cybersecurity vulnerabilities for unmanned aerial vehicles," 2017 IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR), 2017, pp. 194-199, doi: 10.1109/SSRR.2017.8088163.

[JET 22] Hitesh Jethva, Planning A Cloud PKI Infrastructure – Best Practices, In Certificate Services, PKI, 2022

[LAG 18] Lagkas, Thomas & Bibi, Stamatia & Argyriou, Vasileios & Sarigiannidis, Panagiotis. (2018). UAV IoT Framework Views and Challenges: Towards Protecting Drones as “Things”. Sensors. 18. 10.3390/s18114015.

[LAS 20] Lashari, Haque Nawaz & Ali, Husnain Mansoor & Laghari, Asif. (2020). UAV Communication Networks Issues: A Review (7.35 - IMPACT FACTOR). Archives of Computational Methods in Engineering. 10.1007/s11831-020-09418-0.

[LIN 18] C. Lin, D. He, N. Kumar, K. R. Choo, A. Vinel and X. Huang, "Security and Privacy for the Internet of Drones: Challenges and Solutions," in IEEE Communications Magazine, vol. 56, no. 1, pp. 64-69, Jan. 2018, doi: 10.1109/MCOM.2017.1700390.

[LIU 12] Liu, Fang & Bai, Yong. (2012). An Overview of Topology Control Mechanisms in Multi-Radio Multi-Channel Wireless Mesh Networks. EURASIP Journal on Wireless Communications and Networking. 2012. 10.1186/1687-1499-2012-324.

[MAX 16] J. Maxa, M. S. Ben Mahmoud and N. Larrieu, "Extended verification of secure UAANET routing protocol," 2016 IEEE/AIAA 35th Digital Avionics Systems Conference (DASC), 2016, pp. 1-16, doi: 10.1109/DASC.2016.7777970.

[MAX 17] Jean-Aimé Maxa. Architecture de communication sécurisée d’une flotte de drones. Réseaux et télécommunications [cs.NI]. Université Toulouse 3 Paul Sabatier (UT3 Paul Sabatier), 2017.

[MIS 11] Sudip Misra and Sumit Goswami, Key Management in Mobile Ad Hoc Networks, CRC Press, 2011. Security of Self-Organizing Networks: MANET, WSN, WMN, VANET (1st ed.). Auerbach Publications, DOI: 10.1201/EBK1439819197.

[MOR 10] Moraes, Ricardo & Portugal, Paulo & Vasques, Francisco & Custódio, Ricardo. (2010). Assessment of the IEEE 802.11e EDCA Protocol Limitations when Dealing with Real-Time Communication. EURASIP J. Wireless Comm. and Networking. 2010. 10.1155/2010/351480.

[MOZ 19] M. Mozaffari, W. Saad, M. Bennis, Y. -H. Nam and M. Debbah, "A Tutorial on UAVs for Wireless Networks: Applications, Challenges, and Open Problems," in IEEE Communications

Surveys & Tutorials, vol. 21, no. 3, pp. 2334-2360, thirdquarter 2019, doi: 10.1109/COMST.2019.2902862.

[NAG 10] Nagayama, Tomonori & Moinzadeh, Parya & Mechitov, Kirill & Ushita, Mitsushi & Makihata, Noritoshi & Ieiri, Masataka & Agha, Gul & Spencer, Billie & Fujino, Yozo & Seo, Ju-Won. (2010). Reliable multi-hop communication for structural health monitoring. Smart Structures and Systems. 6. 10.12989/sss.2010.6.5_6.481.

[NOU 19] Nouasri, Amine, Riahla Mohamed Amine, Security Threats to Wireless Dynamic Networks: a Survey, 1st International Conference on Networking Telecommunications, Biomedical Engineering and Applications (ICNTBA'19), Boumerdes 4 – 5 Nov 2019.

[NOU 22] Nouasri, Amine, Riahla Mohamed Amine, A distributed monitoring scheme for a fleet of UAV flying drones, International Journal of Mobile Network Design and Innovation (IJMNDI), Vol. 10, No. 3, 2022, doi: 10.1504/IJMNDI.2022.10051465.

[NGU 07] D. Nguyen and P. Minet, "Analysis of MPR Selection in the OLSR Protocol," 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07), 2007, pp. 887-892, doi: 10.1109/AINAW.2007.94.

[PAS 06] Pastor, Enric & López Rubio, Juan & Royo, Pablo. (2006). A Hardware/Software Architecture for UAV Payload and Mission Control. IEEE Aerospace and Electronic Systems Magazine - IEEE AEROSP ELECT SYST MAG. 22. 1 - 8. 10.1109/DASC.2006.313738.

[PER 03] Perkins, C., Belding-Royer, E., and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing", RFC 3561, DOI 10.17487/RFC3561, July 2003, <https://www.rfc-editor.org/info/rfc3561>.

[PIE 14] Security in wireless ad-hoc networks – A survey, Di Pietro, R. AU Guarino, S, Verde, N.V., Domingo-Ferrer, J. JO Computer Communications, https://doi.org/10.1016/j.com

[Puy 16] Puyalnithi, Thendral & V., Dr.Madhu Viswanatham. (2016). Visualization and Statistical Analysis of Multi Dimensional Data of Wireless Sensor Networks Using Self Organising Maps. International Journal of Engineering and Technology. 8. 391-395.

[RAG 13] Raghavendran, Ch. V., G. Naga Satish, Penumathsa Suresh Varma and K. Saravana Kumar. "Challenges and Advances in QoS Routing Protocols for Mobile Ad Hoc Networks." (2013).

[RAM 17] Rametta, Corrado & Schembra, Giovanni. (2017). Designing a Softwarized Network Deployed on a Fleet of Drones for Rural Zone Monitoring. Future Internet. 9. 8. 10.3390/fi9010008.

[RUB 06] A Survey on Wireless Ad Hoc Networks, Rubinstein, Marcelo Gonçalves, Igor Monteiro Moraes, Miguel Elias M. Campista, Luís Henrique Maciel Kosmalski Costa and Otto Carlos Muniz Bandeira Duarte, *MWCN* (2006)

[SAN 05] Sanzgiri, K. & Laflamme, Daniel & Dahill, B. & Levine, Brian & Shields, Clay & Belding, Elizabeth. (2005). An Authenticated Routing Protocol for Secure Ad hoc Networks. IEEE Journal on Selected Areas in Communications - JSAC.

[SEV 11] Sevil S¸en, John A. Clark, and Juan E. Tapiador, Security Threats in Mobile Ad Hoc Networks, CRC Press, 2011. Security of Self-Organizing Networks: MANET, WSN, WMN, VANET (1st ed.). Auerbach Publications. https://doi.org/10.1201/EBK1439819197

[SHA 09] S. Sharma, "P-OLSR: Position-based optimized link state routing for mobile ad hoc networks," *2009 IEEE 34th Conference on Local Computer Networks*, 2009, pp. 237-240, doi: 10.1109/LCN.2009.5355100.

[SHI 20] L. Shi and S. Xu, "UAV Path Planning With QoS Constraint in Device-to-Device 5G Networks Using Particle Swarm Optimization," in IEEE Access, vol. 8, pp. 137884-137896, 2020, doi: 10.1109/ACCESS.2020.3010281.

[SIV 99] R. Sivakumar, P. Sinha and V. Bharghavan, "CEDAR: a core-extraction distributed ad hoc routing algorithm," in IEEE Journal on Selected Areas in Communications, vol. 17, no. 8, pp. 1454-1465, Aug. 1999, doi: 10.1109/49.779926.

[SOR 03] Sorav Bansal, Mary Baker, Observation-based Cooperation Enforcement in Ad Hoc Networks, 2003, DOI:10.48550/ARXIV.CS/0307012

[UIT 19] UIT-R, Calcul de l'affaiblissement en espace libre, Recommandation UIT-R P.525-4 (08/2019), https://www.itu.int/dms_pubrec/itu-r/rec/p/R-REC-P.525-4-201908- I!!PDF-F.pdf

[Ull 16] Ullah, Dr. Saleem & KHAN, Dost & Rehman, Aqeel & Siddique, M. & Khan, Abbas. (2016). AN EFFECTIVE MODELING TO MINIMIZE THE TRANSMISSION TIME IN VANET BY REDUCING ROUTING OVERHEAD. Science International Lahore. 28. 3041-3047.

[XIA 16] Yang Xiaomei and Ma Ke, "Evolution of wireless sensor network security," 2016 World Automation Congress (WAC), 2016, pp. 1-5, doi: 10.1109/WAC.2016.7583032.

[XUE 03] Qi Xue, Aura Ganz, Ad hoc QoS on-demand routing (AQOR) in mobile ad hoc networks, Journal of Parallel and Distributed Computing, Volume 63, Issue 2, 2003, Pages 154-165, ISSN 0743-7315, https://doi.org/10.1016/S0743-7315(02)00061-8.

[YAD 11] Vikas Singh Yadav, Sudip Misra, and Mozaffar Afaque, Security in Vehicular Ad Hoc Networks, 2011. Security of Self-Organizing Networks: MANET, WSN, WMN, VANET (1st ed.). Auerbach Publications. https://doi.org/10.1201/EBK1439819197

[YAN 17] Yanmaz, Evsen & Quaritsch, Markus & Yahyanejad, Saeed & Rinner, Bernhard & Hellwagner, Hermann & Bettstetter, Christian. (2017). Communication and Coordination for Drone Networks. 10.1007/978-3-319-51204-4_7

[ZHA 12] Zhao, Zhongliang & Braun, Torsten. (2012). Topology Control and Mobility Strategy for UAV Ad-hoc Networks: A Survey.