Politiques de robustesse en réseaux ad hoc

Amadou Baba Bagayoko

Université de Toulouse

THÈSE

En vue de l'obtention du

DOCTORAT DE L'UNIVERSITÉ DE TOULOUSE

Délivré par :
Institut National Polytechnique de Toulouse (INP Toulouse)

Discipline ou spécialité :

Réseaux, Télécommunications, Systèmes et Architecture

Présentée et soutenue par :
Amadou Baba BAGAYOKO

le : mercredi 11 juillet 2012

Titre :

Politiques de Robustesse en réseaux ad hoc

Ecole doctorale :
Mathématiques Informatique Télécommunications (MITT)

Unité de recherche :
IRIT - UMR 5505

Directeur(s) de Thèse :

Mme Béatrice PAILLASSA, Professeur INPT/ENNSEEIHT

Rapporteurs :

M. Jean-Jacques PANSIOT, Professeur à l'Université de Strasbourg
M. David SIMPLOT RYL, Professeur à l'Université Lille 1

Membre(s) du jury :

Mme Claudia BETOUS ALMEIDA, Ingénieur Aéroconseil
M. Christophe CHASSOT, Professeur INSA Toulouse
Mme Francine KRIEF, Professeur ENSEIRB

A feu ma mère,
Mme BAGAYOKO Fanta TRAORE

`Vouloir` *nous brûle et* `Pouvoir` *nous détruit ; mais* `Savoir` *laisse notre faible organisation dans un perpétuel état de calme.*
Honoré De Balzac
'La Peau de chagrin'.

Remerciements

Je remercie tout d'abord tous les membres du jury : mes deux rapporteurs M. Jean Jacques PANSIOT et M. David SIMPLOT-RYL pour la qualité et la pertinence de leur rapport de soutenance, mes trois examinateurs Mme Claudia BETOUS, M. Christophe CHASSOT, Mme. Francine KRIEF pour leur disponibilité.

Mes remerciements sincères à ma directrice de thèse Mme Béatrice PAILLASSA pour avoir encadré ce travail de recherche. Un grand merci à M. André Luc BEYLOT pour m'avoir initié à la recherche et conseillé depuis mon stage de Master Recherche jusqu'à la fin de ma thèse.

Je remercie aussi tous les membres de l'équipe IRIT (les doctorants et les maitres de conférences) particulièrement Omer N'Guena Timo, Warodom Werapun, Hicham SLIMANI, Aziz Ahmed-Nacer pour toutes ces discussions. Je tiens aussi remercier nos secrétaires exceptionnelles, Les « Sylvie » pour leur disponibilité et leur bonne humeur.

Mes remerciements à Graziella RAKOTOMANANA pour toutes tes aides au cours de cette thèse et à sa sœur Sandra. Merci aux membres du grin de thé de Toulouse : Mahamadou Touré, Alain TCHANA, Aboubacar DIALLO, Cheick OMAR HAIDARA, Bafing CYPRIENS, Amadou Cheick O. TALL, Sékou SANGARE, Adama SIDIBE, Abdoulaye BERTHE, Oumar CAMARA, Mekossou BAKAYOKO. Je vous remercie pour toutes ces soirées de foot et de discussions. Mes remerciements vont aussi à Aida G KANTE et à Aissata N'Diaye pour avoir consacré leur temps précieux à préparer le pot de cette thèse. Merci aussi à Djeneba Coulibaly et à Niakalé *ma bouran mousso*.

Je remercie également tous les membres du grin DEFY'S : Adama BALLO, Boubacar DIALLO, Sallé DIALLO, Abidine DIAWARA, Aboubacar M. FOFANA, Modibo KANE, Bira KOITA, Sidiki KONE, Simbo SIDIBE, Souleymane TRAORE.

Je remercie infiniment toute ma famille pour leur soutien : mon père Sinsé, ma mère feue Fanta TRAORE et mes frères Nanko, Moussa, Ibrahima, Rokia et Souleymane. Un grand merci à mon cousin Issa Bakary SANGARE pour tout ce que tu as fait pour moi depuis que je suis en FRANCE, cette thèse est aussi la tienne. Enfin, je remercie ma chère Aissata Keita pour toute sa patience durant la rédaction de mon manuscrit de thèse.

Je remercie tous mes amis d'Algérie et du MALI que je ne pourrais citer ici nommément ici.

Résumé

Les réseaux sans fil sont sujets à des perturbations voire des pannes de liens et de nœuds en raison des caractéristiques intrinsèques de leur support de communication ; ces pannes sont aggravées par les particularités de relayage et de mobilité des nœuds dans les réseaux ad hoc. Ces réseaux requièrent donc la conception et la mise œuvre des protocoles robustes au niveau de toutes les couches protocolaires.

Dans cette thèse, nous choisissons une approche de robustesse pour améliorer les performances des communications dans un réseau mobile ad hoc. Nous proposons et étudions deux architectures de protection (protection par une analyse prédictive et protection par redondance de routes) qui sont couplées avec une restauration de niveau routage. Concernant la phase de détection, le protocole de routage utilise les notifications de niveau liaison pour détecter les pannes de liens.

La première solution repose sur un protocole de routage réactif *unipath* dont le critère de sélection de routes est modifié. L'idée est d'utiliser des métriques capables de prédire l'état futur des routes dans le but d'améliorer leur durée de vie. Pour cela, deux métriques prédictives reposant sur la mobilité des nœuds sont proposées : la fiabilité des routes et une combinaison fiabilité-minimum de sauts. Pour calculer ces métriques prédictives, nous proposons une méthode analytique de calcul de la fiabilité de liens entre nœuds. Cette méthode prend compte le modèle de mobilité des nœuds et les caractéristiques de la communication sans fil notamment les collisions inter-paquets et les atténuations du signal. Les modèles de mobilité étudiés sont les modèles *Random Walk* et *Random Way Point*. Nous montrons l'impact de ces métriques sur les performances en termes de taux de livraison de paquets, de surcoût normalisé et de ruptures de routes.

La seconde solution est une protection par redondance de routes qui s'appuie sur un protocole de routage *multipath*. Dans cette architecture, l'opération de recouvrement consiste soit à un basculement sur une route secondaire soit à une nouvelle découverte. Nous montrons que la redondance de routes améliore la robustesse de la communication en réduisant le temps de restauration. Ensuite, nous proposons une comparaison analytique entre les différentes politiques de recouvrement d'un protocole *multipath*. Nous en deduisons qu'un recouvrement segmenté donne les meilleurs résultats en termes de temps de restauration et de fiabilité.

Mots clés : réseaux ad hoc, robustesse, mobilité, redondance, multipath, fiabilité, métrique de routage

Abstract

Due to the unreliability characteristics of wireless communications, and nodes mobility, Mobile Ad hoc Networks (MANETs) suffer from frequent failures and reactivation of links. Consequently, the routes frequently change, causing significant number of routing packets to discover new routes, leading to increased network congestion and transmission latency. Therefore, MANETs demand robust protocol design at all layers of the communication protocol stack, particularly at the MAC, the routing and transport layers.

In this thesis, we adopt robustness approach to improve communication performance in MANET. We propose and study two protection architectures (protection by predictive analysis and protection by routes redundancy) which are coupled with a routing level restoration. The routing protocol is responsible of the failure detection phase, and uses the mechanism of link-level notifications to detect link failures.

Our first proposition is based on *unipath* reactive routing protocol with a modified route selection criterion. The idea is to use metrics that can predict the future state of the route in order to improve their lifetime. Two predictive metrics based on the mobility of nodes are proposed : the routes reliability and, combining hop-count and reliability metrics. In order to determine the two predictive metrics, we propose an analytical formulation that computes link reliability between adjacent nodes. This formulation takes into account nodes mobility model and the the wireless communication characteristics including the collisions between packets and signal attenuations. Nodes mobility models studied are *Random Walk* and *Random Way Point*. We show the impact of these predictive metrics on the networks performance in terms of packet delivery ratio, normalized routing overhead and number of route failures.

The second proposition is based on *multipath* routing protocol. It is a protection mechanism based on route redundancy. In this architecture, the recovery operation is either to switch the traffic to alternate route or to compute a new route. We show that the routes redundancy technique improves the communication robustness by reducing the failure recovery time. We propose an analytical comparison between different recovery policies of *multipath* routing protocol. We deduce that segment recovery is the best recovery policy in terms of recovery time and reliability.

Keywords : ad hoc networks, robustness, mobility, redundancy, multipath, reliability, routing protcol metrics

Table des matières

Table des figures

Liste des tableaux

Glossaire

AODV-BR	AODV with Backup Routes	96
AOMDV	Ad hoc On-demand Multipath Distance Vector	96
DCCP	Datagram Congestion Control Protocol	16
IP	Internet Protocol	32
MANET	Mobile Ad hoc NETwork	11
MDT	Mean Down Time	14
MDYMO	Multipath DYMO	96
MP-OLSR	Multipath OLSR	96
MP-TCP	Multipath Transport Control Protocol	31
MTBF	Mean Time Between Failures	14
MUT	Mean Up Time	14
PDR	Packet Delivery Ratio	96
SCTP	Stream Control Transport Protocol	16
SDF	Sûreté De Fonctionnement	9
SMR	Split Multipath Routing	96
TCP	Transport Control Protocol	16
UDP	User Datagram Protocol	16

Introduction Générale

A Motivations

Un réseau mobile ad hoc - MANET (Mobile Ad hoc NETwork) est une instance de réseau sans fil composée de nœuds mobiles auto-configurés qui communiquent entre eux sans avoir recours à une infrastructure centrale préexistante. Lorsque deux nœuds mobiles sont à portée radio l'un de l'autre, ils établissent un lien de communication et deviennent ainsi adjacents. Un MANET est donc constitué de composants élémentaires qui sont les nœuds mobiles et les liens établis entre les nœuds adjacents. Lorsque les nœuds d'extrémité sont adjacents, ils communiquent directement en utilisant le lien établi. Sinon, l'acheminement des données nécessite la mise en œuvre d'un routage multi-sauts.

La principale difficulté du routage dans un MANET est la gestion de la dynamicité de sa topologie due à la mobilité des nœuds, aux défaillances des nœuds et des liens. Les défaillances de nœuds dans un réseau mobile ad hoc sont plus fréquentes que dans un réseau filaire car en plus des pannes de cartes réseaux et des dysfonctionnements logiciels communs aux nœuds filaires, un nœud ad hoc peut tomber en panne suite à l'épuisement de la charge de sa batterie. En effet, ces nœuds disposent d'une énergie limitée par la capacité de leur batterie qui est difficilement rechargeable en cours de déploiement. Quant aux pannes de liens, elles sont principalement causées par la mobilité des nœuds. En effet, le déplacement de deux nœuds adjacents en dehors de la zone de couverture l'un de l'autre entraîne la rupture du lien établi. D'autre part, les dégradations du signal reçu (diminution du rapport signal-bruit, les interférences, la présence d'obstacle) entre deux nœuds à portée radio et les collisions inter-paquets sont également des raisons possibles de ruptures de liens.

Les défaillances de liens ou de nœuds entraînent des ruptures de routes entre les nœuds d'extrémité. Celles-ci conduisent à des pertes de messages donc une dégradation des performances du réseau. Pour éviter de telles dégradations, il faut assurer une robustesse aux communications ad hoc.

La robustesse peut être mise en œuvre au niveau architectural en fournissant aux protocoles, un ensemble de techniques efficaces pour assurer une résistance, une tolérance et permettre une élimination aux pannes de communication. Ces techniques

se classent en deux groupes : la restauration de service et la protection de service. Il s'agit dans ce document d'étudier les protocoles proposés et ensuite de proposer de nouvelles politiques gérant la restauration et la protection de service.

B Contributions scientifiques

B.1 Principales contributions

Dans cette thèse, nous proposons un cadre original pour gérer la robustesse dans un réseau mobile ad hoc. Nous étudions successivement les techniques de protection (prévention, anticipation et tolérance de pannes) et de restauration (détection, notification, localisation et élimination de pannes) dans un réseau ad hoc.

Nous proposons deux schémas de protection de service : protection par une analyse prédictive et protection par redondance. Notons que quel que soit le schéma de protection, une restauration de service est nécessaire pour rétablir le trafic. Ces deux schémas de protection proposés sont complétés par une restauration de niveau routage.

La protection par une analyse prédictive s'appuie sur des métriques capables de prédire l'état futur des routes. Nous utilisons l'approche de calcul de la fiabilité reposant sur le modèle de mobilité des nœuds. Un des atouts d'une approche analytique est la non-génération d'*overhead* durant le calcul de la fiabilité. Nous proposons une méthode analytique de calcul de la fiabilité de liens pour les modèles de mobilité *Random Walk* et *Random Way Point*. La fiabilité de liens dépend du modèle de mobilité des nœuds et des différents facteurs de communication sans fil notamment les atténuations du signal et les collisions-inter-paquets. Différents modèles d'atténuations du signal sont analysés en fonction de l'environnement de déploiement.

Dans ce document, nous présentons uniquement les travaux effectués sur les les modèles de mobilité *Random Walk* et *Random Way Point*. Durant cette thèse, le modèle *Semi-Markov Smooth* a été étudié et a fait l'objet de publications [BPD11, BDP12]. Dans VTC Fall 2011 [BPD11], nous améliorons le calcul de fiabilité de liens pour le modèle *Semi-Markov Smooth* en prenant en compte les caractéristiques de la communication sans fil. Quel que soit le modèle de mobilité que nous avons étudié, l'utilisation de la fiabilité de lien comme critère de sélection de route améliore la durée de vie de routes et le taux de livraison des paquets mais aussi le nombre de sauts moyen (donc l'énergie) et le délai de bout en bout des paquets. Nous proposons donc une nouvelle métrique qui assure un bon compromis entre les métriques *fiabilité de routes et minimum de sauts* (VTC Fall 2012) [BDP12]. Ensuite, nous étudions l'hypothèse d'indépendance entre liens adjacents en fonction du modèle de mobilité. L'étude montre que celle-ci est acceptable pour les modèles de mobilité *Random Walk* et *Random Way Point*. Dans le modèle *Semi-Markov Smooth*, les fiabilité des

liens sont fortement corrélés par le déplacement du nœud intermédiaire. Nous avons proposé une méthode d'approximation pour le calcul de la fiabilité de routes pour ce modèle de mobilité (VTC Fall 2012).

La protection par redondance a pour objectifs soit de tolérer les pannes soit de réduire les temps de restauration du trafic.

Après une étude synthétique des trois niveaux de redondances (redondances de liens, de routes et de chemins), nous analysons et comparons différentes architectures de protection par redondance en termes de fiabilité et de temps de restauration.

L'analyse des deux architectures de redondance possibles (redondance de routes et intégration *multihoming-multipath*) dans un réseau mono-domicilié montre que :

- L'intégration *multihoming-multipath* améliore la fiabilité et la disponibilité des communications entre les nœuds d'extrémité (ISPA 2009 et CRIMES 2009). Cependant, cette architecture nécessite la mise en œuvre de communications inter-couches entre les niveaux transport et de routage, ce qui augmente sa complexité.
- L'architecture de redondance de routes assure le meilleur compromis en termes de complexité, de fiabilité et de temps de restauration. Il est donc préférable de gérer la redondance uniquement au niveau routage.

Nous avons également étudié un réseau ad hoc hétérogène (Wifi/Zigbee) avec trois niveaux de redondance combinés. Dans IWCMC 2011 et CFIP 2011, nous proposons une architecture de redondance multi-niveau qui s'appuie sur des protocoles normalisés IEEE et IETF. Elle prend en charge toutes les étapes du processus de recouvrement du chemin depuis la détection de la rupture d'un lien sur le chemin primaire jusqu'à la reprise du trafic sur le chemin secondaire. Une formulation analytique de la fiabilité de chacun des trois schémas de recouvrement de base (recouvrement lien par lien, de bout en bout et par segment) est proposée. L'étude de performance montre l'avantage en terme de fiabilité du recouvrement par segment par rapport aux deux autres politiques. Ces travaux ont été menés sur des topologies particulières et ne sont pas présentés dans ce document. Nous avons préféré présenter les travaux sur les topologies quelconques et les résultats obtenus sont similaires.

Pour l'approche de la protection par la redondance, nous obtenons les conclusions suivantes en termes de fiabilité et de temps de restauration, quel que soit le type de réseau utilisé (hétérogène ou homogène) :

- la redondance doit être mise en place uniquement au niveau routage,
- la gestion des pannes doit s'effectuer au niveau du routage par des protocoles *multipath* plutôt que par la couche transport,
- la recouvrement par segment de routes est préférable.

La restauration de service consiste à détecter, identifier, localiser et notifier les pannes puis à rétablir la communication entre les nœuds d'extrémité. Dans un réseau MANET, elle peut être mise en œuvre soit au niveau routage soit au niveau transport. Nous proposons une comparaison analytique des différents mécanismes de restauration en termes de coût, de temps de restauration et complexité. Nous en déduisons que la restauration au niveau trois par un protocole de routage réactif, où les pannes entre nœuds sont détectées par une notification de niveau liaison, donne les meilleurs résultats.

B.2 Publications

1. Amadou Baba Bagayoko, Riadh Dhaou, Béatrice Paillassa. **An efficient metric for reliable routing with link dependencies**, Dans : 76^{th} IEEE Vehicular Technology Conference (VTC Fall 2012), Quebec City - Canada, 03-06 Septembre 2012 (A Paraitre).

2. Amadou Baba Bagayoko, Béatrice Paillassa, Riadh Dhaou. **Practical Link Reliability for Ad hoc Routing Protocol**, Dans : 74^{th} IEEE Vehicular Technology Conference (VTC Fall 2011), San Francisco - USA, 05-09 Septembre 2011.

3. Amadou Baba Bagayoko, Béatrice Paillassa. **Analysis of Robustness in Heterogeneous Ad Hoc Networks**, Dans : Proceedings of the 7^{th} International Wireless Communications and Mobile Computing Conference, IEEE IWCMC 2011, Istanbul - Turkey, 5-8 Juillet 2011.

4. Amadou Baba Bagayoko, Béatrice Paillassa. **Comparaison des stratégies de redondance dans les réseaux ad hoc** (regular paper) . Dans : Colloque Francophone sur l'Ingénierie des Protocoles (CFIP 2011), Sainte-Maxime - France, 10-13 Mai 2011.

5. Amadou Baba Bagayoko, Béatrice Paillassa, Claudia Betous. **Transport and routing redundancy for MANETs robustness**. Dans : IEEE International Symposium on Parallel and Distributed Processing with Applications (ISPA 2009), chengdu and Jiuzhai valley - China, 10-12 Août 2009, pages. 348-353.

6. Amadou Baba Bagayoko, Béatrice Paillassa, Claudia Betous. **Etude analytique de la fiabilité dans les réseaux ad hoc multi-domiciliés** (regular paper). Dans : Convergence des Réseaux, de l'Informatique, et du Multimédia pour les E-services (CRIMES 2009), Université de la Réunion - France, 11-13 Novembre 2009.

7. Amadou Baba Bagayoko, Beatrice Paillassa **Robustesse de chemins dans les réseaux ad hoc : multipath et multihoming**, ResCom 2009, La Palmyre - France, 7-13 Juin 2009.

C Organisation du document

– **Le chapitre 1** commence par définir les termes génériques utilisés dans la sûreté de fonctionnement pour caractériser un réseau ou un composant réseau. Ensuite, il analyse les mécanismes et politiques (la protection et la restauration de service) qui permettent d'améliorer la robustesse dans un réseau mobile ad hoc.

– **Partie I : Robustesse par analyse prédictive**
Nous étudions l'amélioration de la robustesse à l'aide de mécanismes prédictifs au niveau routage.

• **Le chapitre 2** propose une méthode analytique de calcul de la fiabilité de liens entre nœuds. La fiabilité de liens déduite de ce modèle tient compte du modèle de mobilité des nœuds et des caractéristiques de la communication sans fil notamment les collisions inter-paquets et les atténuations du signal. Les modèles de mobilité étudiés sont les modèles *Random Walk* et *Random Way Point*.

• **Le chapitre 3** propose d'améliorer les performances (la robustesse) au niveau routage en utilisant des métriques prédictives. La métrique *fiabilité de route* améliore le taux de livraison mais aussi le nombre moyen de sauts. Ce qui entraîne une augmentation de l'énergie consommée par le routage. A partir cette observation, nous proposons une nouvelle métrique pour concilier de manière conjointe les métriques *fiabilité de route* et *minimum de sauts*. Les simulations montrent que celle-ci assure un bon compromis entre le taux de livraison de paquets et le nombre moyen de sauts.

– **Partie II : Robustesse par redondance**
Cette partie analyse la robustesse dans une architecture de redondance de niveau routage.

• **Le chapitre 4** étudie la redondance de routes dans le but d'améliorer les performances du réseau en réduisant le temps de restauration par rapport à un routage *unipath*. Nous analysons les protocoles de routage *multipath* proposés dans les réseaux MANETs en mettant l'accent sur le processus de recouvrement et le degré de similitude entre les routes. Ce chapitre propose aussi une comparaison analytique en termes de temps de restauration et de fiabilité entre les protocoles *unipath* et deux politiques de recouvrement (recouvrement de bout en bout et recouvrement par segment de routes) utilisés dans le routage *multipath*.

– Enfin, nous exposons une synthèse des propositions et résultats obtenus au cours de cette thèse. Des perspectives d'utilisation et d'extension de nos travaux sont ensuite proposées.

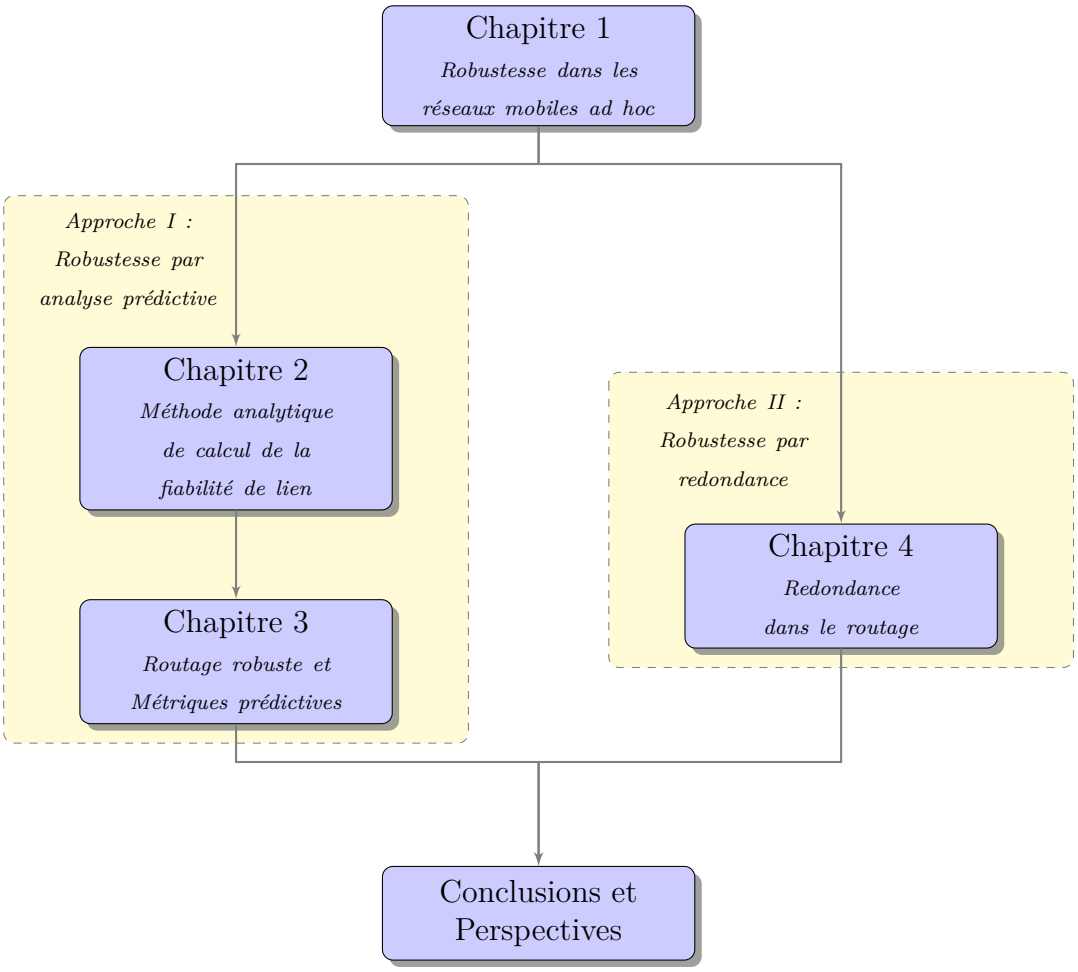


FIGURE 1 – Organisation de la thèse

Chapitre 1

Robustesse dans les réseaux mobiles ad hoc

Table des matières

L'objectif de ce chapitre est de présenter les différents mécanismes et politiques proposés dans la littérature pour améliorer la robustesse dans les réseaux ad hoc.

La première section définit les différents termes génériques utilisés dans la sûreté de fonctionnement *(SDF)* pour caractériser un réseau ou un composant réseau. Chaque définition est illustrée dans le contexte ad hoc.

La deuxième section est consacrée à l'étude de la protection et de la restauration de service. Ce sont deux techniques permettant de fournir un service robuste

et efficace aux communications ad hoc. La protection de service regroupe les mécanismes permettant l'évitement des pannes par anticipation et les reprises presque instantanées du trafic données. Elle s'effectue lors de la phase d'initialisation (ou de réinitialisation) du service. Quant à la restauration de service, elle englobe les politiques mises en œuvre pour assurer une reprise rapide et efficace du service après une panne de communication.

1.1 Définitions des termes de SDF dans un MANET

Dans cette première section, nous nous attachons à définir un ensemble de termes permettant d'appréhender la problématique et de mieux comprendre les différentes solutions mises en œuvre pour assurer une robustesse aux communications dans les réseaux ad hoc. Nous étudierons ainsi les différents concepts utilisés pour caractériser la sûreté de fonctionnement (SDF) des communications dans un réseau.

1.1.1 Robustesse

La robustesse est définie comme la capacité d'un système à fonctionner correctement malgré l'occurrence de la défaillance d'un ou plusieurs composants internes et dans des conditions hostiles [IEE90]. C'est un moyen pour fournir une qualité de service (*Quality of Service* QoS) aux applications. Un réseau ou une architecture robuste doit garantir une qualité de service (*Quality of Service* QoS) aux applications lors de l'acheminement d'un trafic de données entre une source et une destination en respectant leurs exigences exprimées [CNRS98].

Une application spécifie ses exigences à un réseau sous la forme de besoins traduits en un ensemble d'attributs mesurables : délai de bout en bout, variance de délai (gigue), débit (ou bande passante), taux de pertes de paquets. Les besoins exprimés dépendent des caractéristiques du trafic de l'application. La notion de QoS est donc subjective. Lorsque plusieurs routes vers une destination sont disponibles, le choix de la route dépend des attributs mesurables déduits des besoins exprimés. Par exemple, une route proposant un délai et un débit faibles sera choisie pour les applications interactives (voix, vidéo), tandis qu'une route acceptant un meilleur débit et un faible taux de perte au prix d'un délai plus long sera préférée pour les applications moins sensibles au délai (streaming, messagerie, transfert de fichiers et téléchargement, etc). Dans cette thèse, nous nous intéressons particulièrement à la métrique taux de pertes de paquets qui influence d'une façon directe et notable la QoS du réseau. En effet, les pertes de paquets compromettent l'intégrité des données ou interrompent totalement le service. Elles peuvent être influencées par la charge du réseau, le BER (Bit Error Rate), la défaillance de nœuds ou de liens.

La capacité d'un réseau à garantir une qualité du service (QoS) demandée est liée aux caractéristiques intrinsèques de ses composants. D'un point de vue de l'architecture protocolaire, la qualité du service fournie par le réseau n'est pas liée uniquement à la couche routage, elle nécessite des efforts coordonnés des couches MAC (Meduim Access Control), routage et transport.

1.1.2 Défaillance (Failure)

La défaillance d'un système ou d'un composant est définie comme son incapacité à accomplir ses fonctions dans les exigences de performances spécifiées [IEE90]. Un élément réseau est dit défaillant lorsqu'il cesse de délivrer la qualité de service requise [FB06]. La notion de défaillance est donc essentiellement conventionnelle car elle dépend des spécifications de la QoS demandée.

1.1.2.1 Défaillance de nœuds

Un nœud ad hoc est en état de panne quand il n'est plus capable d'accomplir une de ses fonctions (l'émission, la réception ou le relayage). Les défaillances de nœuds dans un réseau ad hoc sont plus fréquentes que dans un réseau filaire car en plus des pannes de cartes réseaux et des dysfonctionnements logiciels communs aux nœuds filaires, un nœud ad hoc peut tomber en panne suite à l'épuisement de la charge de sa batterie. En effet, les nœuds mobiles disposent d'une énergie limitée par la capacité de leur batterie qui est difficilement rechargeable en cours de déploiement.

1.1.2.2 Défaillance de liens

Si la QoS demandée pour un lien est la transmission des données entre deux nœuds sans aucune exigence de débit ni de délai, la défaillance d'un lien sans fil entre deux nœuds mobiles adjacents non défaillants est caractérisée par l'impossibilité de communication sur ce lien. Un lien établi entre deux nœuds n_i et n_j est dit rompu (en état de panne) lorsque le nœud récepteur (par exemple, le nœud n_j) ne reçoit aucun message émis par le nœud n_i. Les raisons d'une impossibilité de communication directe entre deux nœuds ad hoc sont diverses.

La mobilité des nœuds est la principale cause de défaillance de liens dans un MANET. Les atténuations du signal et les collisions inter-paquets sont d'autres raisons de défaillance de liens. Les dégradations du signal reçu (diminution du rapport signal-bruit, les interférences, la présence d'obstacle) dépendent du modèle de propagation et l'environnement de déploiement, elles sont susceptibles de réduire la portée de communication des nœuds. Les collisions inter-paquets sont des pannes intermittentes qui peuvent entraîner des ruptures de liens de communication en fonction de leurs durées.

1.1.3 Fiabilité (Reliability)

La fiabilité est définie comme étant l'aptitude d'une entité à accomplir une fonction, dans des conditions données, pendant une durée donnée [IEC74, IEE90]. La mesure de la fiabilité d'un équipement réseau est la probabilité que cet équipement accomplisse ses fonctions dans des conditions spécifiées durant un intervalle de temps donné [IEC74]. Elle correspond donc à une mesure de la délivrance continue d'un service correct, le temps jusqu'à la défaillance.

On distingue plusieurs catégories de fiabilité selon les paramètres utilisés pour évaluer sa valeur. La fiabilité intrinsèque ou inhérente d'un composant est déduite directement de ses paramètres de conception. La fiabilité prévisionnelle est une fiabilité prédite et établie par l'analyse du système et à partir de la connaissance des fiabilités des différents composants du système. On appelle fiabilité opérationnelle ou observée d'un composant la valeur obtenue à partir de l'exploitation des fiabilités (après un retour d'expérience) d'entités identiques dans des conditions opérationnelles similaires. La fiabilité d'une entité obtenue par extrapolation de la fiabilité opérationnelle d'un composant identique dans des conditions ou des durées différentes est appelée fiabilité extrapolée.

Parmi les différentes catégories de fiabilités, nous nous intéressons durant cette thèse aux termes spécifiques : fiabilité prévisionnelle et fiabilité observée. La fiabilité prévisionnelle sera utilisée par les mécanismes de prévention de fautes de routes. Cette fiabilité prévisionnelle devra donc être comparée à la fiabilité effectivement observée pour évaluer l'efficacité du mécanisme prévisionnel (voir chapitre 2).

1.1.3.1 Fiabilité prévisionnelle d'un nœud

La fiabilité d'un nœud n_i durant l'intervalle [t, t+T] notée $R_{n_i}(t, t+T)$ est la probabilité qu'il soit continuellement actif jusqu'au moins à l'instant $(t+T)$ sachant qu'il fonctionnait à l'instant t.

$$R_{n_i}(t, t+T) = P\{n_i \text{ non défaillant sur } [t, t+T] \,|\, n_i \text{ fonctionne à } t\} \tag{1.1}$$

Cette fiabilité (Reliability) $R_i(t, t+T)$ dépend de la durée de l'intervalle, des probabilités de dysfonctionnements logiciels, d'apparition des pannes de son (ou ses) cartes réseaux et du taux d'épuisement de la batterie.

1.1.3.2 Fiabilité prévisionnelle d'un lien

La fiabilité d'un lien L_i entre deux nœuds n_i et n_{i+1} durant l'intervalle $[t, t+T]$ notée $R_{L_i}[t, t+T]$ est la probabilité que ces deux nœuds puissent communiquer

continuellement durant cet intervalle, sachant qu'ils pouvaient communiquer à l'instant t.

$$R_{L_i}(t, t+T) = P\{L_i \text{ non défaillant sur } [t, t+T] \,|L_i \text{ est actif à } t\} \quad (1.2)$$

La fiabilité d'un lien dépend de la durée de la communication, de la portée de la technologie, du modèle de mobilité, de l'environnement de déploiement du réseau (bruit, obstacles, interférences).

1.1.3.3 Fiabilité prévisionnelle d'une route

La fiabilité d'une route entre une source n_0 et une destination n_m composée de m liens et de $(m+1)$ nœuds est le produit entre la fiabilité de tous les équipements élémentaires composant cette route. Elle est égale à [CCGL06, DFH06, MZ99, SZG+07] :

$$\begin{aligned} R_{Ro_{(n_0 \leftrightarrow n_m)}}(t, t+T) &= R\left[L_0(t, t+T) \cap L_1(t, t+T) \cdots \cap L_{m-1}(t, t+T)\right] \\ &\quad \times \prod_{i=0}^{m} R_{n_i}(t, t+T) \end{aligned} \quad (1.3)$$

Dans le cas où les liens adjacents sont indépendants, la formule précédente (équation 1.3) peut se réécrire comme suit :

$$R_{Ro_{(n_0 \leftrightarrow n_m)}}(t, t+T) = R_{n_m}(t, t+T) \times \prod_{i=0}^{m-1} \left[R_{n_i}(t, t+T) \times R_{L_i}(t, t+T)\right] \quad (1.4)$$

La validité de l'hypothèse d'indépendance entre liens adjacents dépend du modèle de mobilité des nœuds. Dans le cas où elle n'est vérifiée, il est nécessaire de calculer le facteur de corrélation entre liens adjacents [BCF+99, Far04, ZD07, BDP12]. Par exemple, la fiabilité d'une route composée deux liens entre $(n_0 \leftrightarrow n_1 \leftrightarrow n_2)$ dépend de la mobilité du nœud intermédiaire n_1. La valeur de ce facteur de corrélation dépend des mouvements relatifs du nœud n_1 par rapport n_0 et n_2.

Dans la suite (chapitre 2), nous montrons que l'hypothèse d'indépendance est acceptable pour les modèles de mobilité *Random Walk* et *Random Way Point*.

1.1.4 Disponibilité (Availability)

La disponibilité d'un équipement réseau est la probabilité que cet équipement soit en état de fournir la qualité de service demandée dans des conditions données et à un instant donné [FB06]. A l'instar de la fiabilité, il existe plusieurs types de disponibilité. La disponibilité instantanée est définie comme étant la faculté d'un composant

d'être prêt à l'emploi à un instant donné. Alors que la disponibilité moyenne mesure la délivrance d'un service correct par rapport à l'alternance service correct - service incorrect [FB06]. Cette définition est assez générale et peut être précisée en fonction du contexte et de l'interprétation donnée au terme service correct.

La disponibilité moyenne du réseau est le rapport entre le temps où la connexion au réseau est disponible et le temps total d'ouverture théorique du service. Elle tient compte uniquement de la connexion au réseau sans aucune exigence de qualité de service. Lorsque le réseau (ou la route établie) doit respecter une certaine qualité de service négociée, on parle de disponibilité moyenne au service.

Notons que contrairement à la fiabilité qui est caractérisée par la notion de continuité et d'absence interruption du service, la disponibilité est une valeur instantanée (ou une moyenne de valeurs instantanées). Le système ou le composant peut avoir subi un ou plusieurs cycles de panne-réparation durant l'intervalle $[t, t+T]$. Lorsque le système ou le composant est non réparable, la fiabilité et la disponibilité sont équivalentes ; car il n'y a pas de réparation possible.

1.1.5 Réparation (Repair)

Un élément réseau est réparé lorsqu'il retrouve sa capacité à délivrer la qualité de service exigée. Il passe d'un état défaillant à un état de bon fonctionnement. Pour réparer une route ou un chemin, il faut procéder à son recouvrement. Le recouvrement d'un système permet de substituer un état exempt d'erreur à l'état erroné du système.

1.1.6 Temps entre deux pannes consécutives

Le temps entre deux pannes consécutives d'un système noté (MTBF *Mean Time Between Failures*) est composé du :

- Temps moyen séparant la survenance de la panne et la remise en état opérationnel du système noté *MDT Mean Down Time*. Par la suite, nous utiliserons le terme *temps de restauration de service* de route ou de chemin pour décrire cet indicateur.
- Temps de disponibilité (MUT *Mean Up Time*) qui représente le temps moyen qui sépare une remise en service opérationnelle du système de l'occurrence de la panne suivante. Dans les MANETs, cette métrique est aussi appelée durée de vie de la route (ou du chemin).

1.1.7 Redondance (Redundancy)

La redondance est une technique de la tolérance aux pannes ; elle consiste à la mise en place dans un système de composants secondaires qui sont capable d'accomplir des fonctions identiques ou similaires à celles du composant primaire dans le but de prévenir ou réparer les défaillances. On distingue plusieurs types de redondance :

- Redondance homogène : les composants primaire et secondaires sont identiques.
- Redondance hétérogène (ou avec dissemblance) : les composants primaire et secondaires réalisent les mêmes fonctions mais sont différents (par exemple, matériels ou technologies de communication différents).
- Redondance froide : un composant secondaire est activé uniquement après la défaillance de son composant primaire.
- Redondance chaude : les composants primaire et secondaire tournent en parallèle.

Notons que le type de redondance utilisé dépend de la politique de gestion et la disponibilité des composants dans le système.

1.2 Analyse de la gestion de pannes dans un MANET

Cette section dresse un panorama des mécanismes et politiques permettant de fournir une robustesse aux communications ad hoc. Ceux-ci se classent en deux groupes : la restauration de service et la protection de service.

Les deux groupes se différencient principalement par le moment de leur mise en place : avant ou après la panne. Tandis que la restauration de service s'effectue après la détection d'une panne de communication en vue de rétablir le service, la protection de service regroupe les moyens mis en œuvre avant la rupture de la communication (généralement lors de la phase d'initialisation de la communication) pour éviter, anticiper ou réduire les pannes. Notons que ces deux concepts (restauration et protection de service) ne sont pas antinomiques. Par exemple, lorsqu'un service protégé devient défaillant, une restauration est nécessaire pour rétablir la communication. Dans le domaine des réseaux, la restauration de service entre deux nœuds d'extrémité consiste à l'utilisation d'une nouvelle route (ou un nouveau chemin) ne comportant aucun élément défaillant (liens et nœuds) entre les deux nœuds d'extrémité.

Dans la première partie de cette section, nous étudierons respectivement la restauration de service effectuée par les protocoles transport puis celle des protocoles de routage MANETs. La seconde partie sera consacrée à la protection de service notamment l'analyse prédictive et préventive des pannes et les techniques de redondance de liens, de routes et de chemins.

1.2.1 Restauration de service (ou Elimination de fautes)

Un réseau MANET fournit les services à ses nœuds en établissant une route ou un chemin de communication entre deux nœuds d'extrémité (source et destination). La restauration de ce service consiste donc à détecter, identifier, localiser et notifier les pannes puis à rétablir la communication entre les nœuds d'extrémité. Elle peut être mise en œuvre aussi bien par les protocoles transport orientés connexion que par les protocoles de routage.

Quelle que soit la couche responsable, la restauration du service dans un réseau est composée de trois phases : la détection, l'opération de recouvrement de pannes et la reprise du trafic. La durée globale de la restauration du service T_R peut être calculée comme suit :

$$T_R = T_d + T_{or} + T_{rt} \tag{1.5}$$

Où

T_d – Temps de la détection des pannes par le nœud responsable du recouvrement
T_{or} – Temps de l'opération de recouvrement des pannes
T_{rt} – Temps de la reprise du trafic de données

Nous commençons par présenter la restauration de service d'un chemin de communication mise en œuvre par les protocoles transport orientés connexion. Puis, nous étudierons les différents mécanismes disponibles au niveau réseau pour permettre aux protocoles de routage MANET d'effectuer une restauration de service. Nous proposons aussi une formulation analytique de la durée de la restauration de service des protocoles transport et routage dans un réseau mobile ad hoc.

1.2.1.1 Restauration au niveau transport

La restauration de niveau transport est mise en œuvre lorsque celle de la couche routage échoue ou dure trop longtemps. Ce mécanisme est disponible uniquement dans les protocoles transport orientés connexion (les protocoles TCP [Pos81], SCTP [Ste07], DCCP [KHF06]). Les protocoles transport non orientés connexion comme UDP [Pos80] ne possédant pas de mécanismes d'acquittement, ne sont capables ni de détecter ni de procéder au recouvrement d'une panne ; ils continueront donc à utiliser le chemin défaillant jusqu'à ce que le protocole de routage effectue le recouvrement de routes.

Lorsque la couche transport est responsable de la restauration, toutes les phases s'effectuent au niveau du nœud source des données. Dans un protocole transport orienté connexion, la détection de pannes se fait par la surveillance du chemin transport. Elle s'effectue en deux étapes : émission de données par la source vers la destination et émission d'acquittement *ACK* par la destination vers la source. Après l'écoulement du temporisateur sans réception d'acquittement, la source suppose que le paquet de données émis n'est pas arrivé à destination. Comme les raisons d'une non réception d'acquittement peuvent être multiples (pertes de l'accusé de réception, temps d'aller-retour plus grand que la valeur du temporisateur, congestion temporaire), la source ne détecte pas immédiatement une panne de chemin mais entre en attente : *hold-off*. L'objectif de la période de *hold-off* est d'être sûr de l'état de panne du chemin. Pour celà, la source retransmet le paquet de données non acquitté et réarme le temporisateur (généralement sa valeur est doublée). Si un acquittement est reçu avant la fin de la période de *hold-off*, la source réinitialise toutes ses variables (temporisateur et nombre de retransmissions) et continue à envoyer ses autres paquets de données. Après un certain nombre de retransmissions consécutives infructueuses (*Nbre.Max.Retrans*) d'un paquet de données, le protocole transport de la source détecte l'état de panne du chemin. Il procède au recouvrement qui consiste à utiliser un autre chemin entre les nœuds d'extrémité.

Le temps de restauration d'une communication entre deux nœuds d'extrémité par le protocole transport après une panne de chemin est :

$$\begin{aligned} T_{R_{Trans}} &= T_d + T_{or} + T_{rt} \\ &= \left[\sum_{i=0}^{Nbre.Max.Retrans} \left(2^i \times RTO\right) \right] + T_{or} + T_{rt} \end{aligned} \tag{1.6}$$

Où

$T_{R_{Trans}}$ – Temps de restauration d'un protocole transport
RTO – Durée entre deux rétransmissions consécutives d'un paquet de données
$RTO.Initial$ – 3 secondes
$RTO.Min$– 1 seconde
$RTO.Max$ – 60 secondes
$Nbre.Max.Retrans$ – Nombre de maximum de rétransmissions (par défaut 5 dans SCTP et TCP)

Le temps de détection d'un chemin par un protocole transport peut être ainsi borné en fonction des valeurs des paramètres comme suit :

$$(63 \times RTO.Min) \leq T_d \leq (63 \times RTO.Max) \tag{1.7}$$

Ce temps de détection est très long comparé à celui de protocoles de routage MANETs que nous étudions dans la prochaine sous-section.

1.2.1.2 Restauration par le protocole de routage (ou Restauration de niveau routage)

Avant de décrire la restauration de service par les protocoles de routage, nous introduisons brièvement les trois grandes catégories de protocoles de routage MANETs. Ensuite, nous étudierons les différents mécanismes possibles pour chaque phase de la restauration de service.

1.2.1.2.1 Notion de routage dans les MANETs Dans le domaine des réseaux ad hoc, il existe trois grandes catégories de protocoles de routage : les protocoles réactifs, proactifs et hybrides. Ces catégories diffèrent selon la façon dont les nœuds obtiennent et maintiennent leurs routes. Les protocoles de routage proactifs maintiennent activement des routes permettant de joindre tous les nœuds du réseau, alors que les protocoles réactifs créent et maintiennent une route entre deux nœuds uniquement lorsqu'ils désirent communiquer. Les protocoles hybrides combinent les deux types de protocoles précédents ; ils adoptent généralement un fonctionnement proactif dans le voisinage de la source et une approche réactive pour les nœuds éloignés.

Dans un protocole proactif, un nœud obtient (ou met à jour) une route vers une destination grâce aux informations sur la topologie du réseau reçues. Ces informations sont diffusées périodiquement soit par l'ensemble des nœuds du réseau soit par un sous-ensemble de nœuds (dans le but de reduire l'overhead généré). Les protocoles OLSR [CJ03] et DSDV [PB94] sont des exemples de protocoles proactifs. Un nœud construit ses informations sur la topologie du réseau en éffectuant une corrélation entre les informations reçues et l'état de la communication avec ses voisins (mis à jour par les mécanismes de détection de pannes entre nœuds adjacents).

Contrairement aux protocoles proactifs, dans un protocole réactif, une source obtient une route vers une destination à la demande. Lorsqu'un nœud source S désire envoyer un paquet de données à un nœud destination D vers lequel il ne possède pas de route, il initie une découverte de routes. Un protocole réactif utilise deux mécanismes pour assurer le routage des données entre deux nœuds : la découverte de routes et la maintenance des routes. La découverte de routes s'effectue au moyen des cycles de requêtes (Route REQuest RREQ) /réponses (Route REPly RREP). La principale différence entre les protocoles réactifs réside dans la stratégie de routage adoptée (routage par la source et routage par destination).

- Routage par la source : On appelle stratégie de routage par la source, lorsque la source inclut dans l'en-tête des paquets de données un champ *'enregistrement de route'* qui contient toutes les décisions de routage. Le routage par la source est mis en œuvre dans le protocole DSR [JHM07] standardisé par l'IETF.
- Dans la stratégie de routage par destination, chaque nœud du réseau possède une table de routage locale dans laquelle à chaque destination est associée l'identifiant du prochain nœud sur la route. Les protocoles IETF AODV [PBRD03] et DYMO [CP10] utilisent cette stratégie pour assurer le routage entre deux nœuds d'extrémité.

L'objectif de la maintenance des routes est de détecter les défaillances de routes puis de notifier ces défaillances au nœud responsable du recouvrement (généralement la source des données). Le processus de détection de défaillance d'une route s'effectue en deux étapes : la défaillance de communication entre deux nœuds adjacents sur cette route et la notification de panne de route (RERR) envoyée par le nœud détecteur vers la source.

Intéressons nous à la restauration par les protocoles proactifs et réactifs. La différence entre la restauration de service des protocoles proactifs et réactifs réside dans la manière par laquelle la source détecte une panne de routes.

Dans un protocole réactif, la détection d'une panne de communication entre deux nœuds adjacents sur une route déclenche immédiatement une phase de notification de panne qui conduit à la détection de la panne de cette route par le nœud source. Le temps de détection de la panne d'une route $T_{d_{Route}}$ est donc composé du temps de détection de pannes de communication $T_{d_{(n_i,n_{i+1})}}$ entre deux nœuds adjacents (n_i et n_{i+1}) et du temps de notification T_n. La durée de la restauration de service d'un

protocole réactif est :

$$\begin{aligned} T_{R_{RoutReac}} &= T_{d_{Route}} + T_{or} + T_{rt} \\ &= T_{d_{(n_i,n_{i+1})}} + T_n + T_{or} + T_{rt} \end{aligned} \tag{1.8}$$

Dans un protocole proactif, les phases de détection et de recouvrement de panne de routes s'effectuent simultanément. Un nœud effectue les deux phases grâce aux informations sur la topologie du réseau reçues. Un nœud ayant détecté une défaillance de communication avec un voisin modifie en conséquence sa table de routage et attend sa prochaine période de diffusion pour communiquer ses informations sur la topologie du réseau à ses voisins. La table de routage d'un nœud est mise à jour par une corrélation entre ses routes et les informations sur la topologie du réseau reçues. Ces informations sont diffusées périodiquement de proche en proche jusqu'à la source qui met alors à jour sa table de routage (suppression, ajout de la nouvelle route, détection de défaillance d'une route). Dans le cas où les informations sur la topologie permettent à la source d'obtenir une nouvelle route, le temps de restauration de service est composé du temps de détection de pannes de communication $T_{d_{(n_i,n_{i+1})}}$ entre deux nœuds adjacents (n_i et n_{i+1}), le temps T_{P-rest} (somme des durées restantes des périodes de diffusions) et du temps de notification T_n (somme des temps de propagation des informations entre les nœuds diffuseurs) :

$$\begin{aligned} T_{R_{RoutProac}} &= T_{d_{Route}} + T_{or} + T_{rt} \\ &= T_{d_{(n_i,n_{i+1})}} + T_{P-rest} + T_n + T_{rt} \end{aligned} \tag{1.9}$$

En supposant qu'il existe M nœuds intermédiaires qui diffusent des informations sur la topologie entre le nœud détecteur n_i et le nœud source.

$$T_{P-rest} = \sum_{j=0}^{M} T_{P-rest_i} \tag{1.10}$$

$$T_n = \left[\sum_{j=0}^{M} T_{Propagation_{(j,j+1)}} \right] \tag{1.11}$$

La restauration de service par un protocole hybride dépend de la localisation des nœuds adjacents dont la défaillance de communication a été détectée. En cas de panne de communication entre nœuds adjacents dans le voisinage de la source, un protocole hybride se comportera comme un protocole proactif pour effectuer la restauration ; sinon il adoptera le comportement d'un protocole réactif lors de la restauration.

1.2.1.2.2 Détection de pannes de routes Nous présentons ici les différentes étapes permettant à une source (nœud responsable du recouvrement) de détecter la panne d'une route : détection de pannes de communication entre nœuds adjacents, corrélation et notification de pannes de routes.

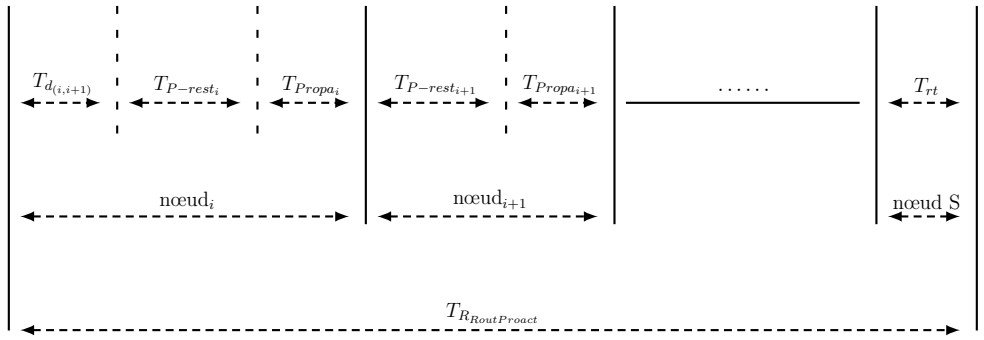


FIGURE 1.1 – Restauration de service d'un protocole proactif

1.2.1.2.2.1 Mécanismes de détection entre nœuds adjacents La défaillance d'une communication entre deux nœuds adjacents peut être détectée soit uniquement par le protocole de routage soit nécessiter une coopération entre les couches routage et liaison du modèle OSI. Les mécanismes considérés sont :

- Le protocole de découverte de voisins (*Hello Message*)
- La notification de niveau liaison (NNL)
- L'acquittement de niveau routage (ANR)

Pour chaque mécanisme, nous commencerons par la description de son mode de fonctionnement et son analyse par rapport aux autres. Pour effectuer une comparaison quantitative entre les mécanismes de détection de la panne de communication entre deux nœuds adjacents (n_i et n_{i+1}), nous utilisons deux critères : le temps de la détection $T_{d_{(n_i,n_{i+1})}}$ et le coût de la maintenance CM_d (en terme de nombre de messages de contrôle de niveau routage généré). Ensuite, nous comparons les coûts de maintenance des trois mécanismes étudiés sur la figure 1.2.

Notons que les mécanismes présentés permettent uniquement de détecter une panne de communication entre deux nœuds adjacents sans pour autant pouvoir faire une localisation exacte. C'est-à-dire qu'ils ne sont pas capables de différencier une rupture de communication due à la défaillance d'un lien de celle due à la défaillance du nœud récepteur.

- Protocole de découverte de voisins (Hello) : Dans ce mécanisme de détection, chaque nœud diffuse périodiquement à intervalle régulier *HELLO_INTERVAL(HI)*, un message *Hello* pour indiquer sa présence aux nœuds voisins. Les nœuds du réseau possèdent chacun une table contenant tous ses voisins à un saut, qui est mise à jour régulièrement (ajout et retrait de voisins). Un nœud supprime un voisin de sa table, lorsqu'il ne reçoit aucun message *Hello* ou de données de celui-ci durant $AHL \times HI$; *ALLOWED_HELLO_LOSS (AHL)* est défini comme le nombre d'intervalle de tolérance sans réception de *Hello* avant de déclarer une panne.
  La détection de pannes basée sur les messages *Hello* présente l'avantage d'être indépendante de la couche liaison. Elle est donc disponible quel que soit le type

de la sous-couche MAC (Meduim Access Control). D'autre part, elle permet de détecter les pannes aussi bien sur les routes actives (celles utilisées pour envoyer des données) qu'inactives (par lesquelles ne transitent pas actuellement des données). En plus, le mécanisme de détection avec *Hello Message* peut être utilisé aussi bien par les protocoles réactifs que proactifs.
Cependant, ce mécanisme possède deux inconvénients majeurs qui sont son temps de détection $T_{d_{(n_i,n_{i+1})}}$ et son coût de maintenance CM_d.
L'instant d'occurrence de la panne n'étant pas connu à priori, le temps nécessaire pour détecter une panne de communication entre nœuds adjacents survenue peut être modélisé comme une variable aléatoire uniformément distribuée entre HI et $AHL \times HI$. Dans [GMS+06], le temps moyen avant la détection de panne est formulé comme suit :

$$E\left\{T_{d_{(n_i,n_{i+1})}}\right\}_{(Hello)} = \frac{1+AHL}{2} \times HI \tag{1.12}$$

En utilisant les valeurs d'expérimentations fournies dans RFC 3561 [PBRD03] : $AHL = 2$ et $HI = 1000$ millisecondes, nous obtenons :

$$E\left\{T_{d_{(n_i,n_{i+1})}}\right\}_{(Hello)} = 1.5 \text{ sec} \tag{1.13}$$

Le coût de la maintenance CM_d d'une communication entre deux nœuds adjacents est fonction de la durée de vie de la communication DV_C et de la taille des paquets *Hello* T_{Hello} :

$$CM_{d(Hello)} = \frac{2 \times T_{Hello} \times DV_C}{HI} \tag{1.14}$$

La taille des paquets *Hello* T_{Hello} est égale à 13 bytes [PBRD03]. Du point de vue du nœud n_i, la durée de vie de la communication avec le nœud n_{i+1} est la différence entre le moment de détection de la défaillance et l'instant d'activation (réception du premier message *Hello* ou de données du nœud n_{i+1}).

- Notification de niveau liaison (NNL) : Pour détecter une rupture de communication entre deux nœuds adjacents, le protocole de routage peut utiliser les acquittements de la couche liaison (précisément la sous-couche MAC) lorsque ceux-ci sont disponibles. Dans le modèle 802.11, le protocole MAC émet une trame MAC CTS (Clear-To-Send) en réponse à une trame MAC RTS (Request-To-Send) et un acquittement Ack en réponse à une trame de données bien reçue. En cas de non réception de cet acquittement (respectivement de la trame MAC CTS) après un délai d'attente fixé, le protocole MAC de l'émetteur de la donnée (respectivement de la trame MAC RTS) entre en période de *hold-off* puis retransmet le paquet de données (respectivement la trame MAC RTS). L'objectif de cette période *hold-off* est d'être sûr de l'état de panne. Lorsqu'aucun acquittement n'est reçu après un nombre de retransmissions consécutives (retryLimit par défaut 7), le protocole MAC détecte une panne d'adresse MAC injoignable. Par un mécanisme de cross-layer entre la couche routage et la sous-couche MAC, cette panne remonte au niveau trois, ce qui permet au protocole

de routage de détecter une panne de communication entre les deux nœuds adjacents.
La notification de niveau liaison permet une détection rapide de la panne de communication entre nœuds adjacents sans générer aucun *overhead* supplémentaire au niveau routage ($CM_{d(NNL)} = 0$). Cependant, la notification de niveau liaison n'est pas adaptée pour les routes utilisées pour envoyer un trafic sporadique. En effet, la détection de rupture est liée uniquement à la transmission des données. Le temps de détection peut être long pour les routes à trafic sporadique. D'autre part, il ne permet pas de faire la différence entre les collisions et les ruptures effectives. Ce qui peut conduire à de fausses détections de pannes de communication [GMS+06].
Le temps de détection après une défaillance entre nœuds adjacents est composé du temps d'attente $T_{att-Paq}$ par le nœud n_i d'un paquet à émettre vers le nœud n_{i+1} et de la durée T_{Drop} des sept (07) émissions infructueuses du paquet.

$$E\left\{T_{d_{(n_i,n_{i+1})}}\right\}_{(NNL)} = T_{att-Paq} + T_{Drop} \tag{1.15}$$

Notons que la durée de chaque émission du paquet dépend de l'état de canal (libre ou non), la durée de la période de *backoff*, la taille du paquet de données et des valeurs des paramètres DIFS (Distributed Inter-Frame Space), SIFS (Short Inter-Frame Space). La durée moyenne avant la suppression d'un paquet dans le modèle DCF a été formulée dans [CBV03], elle est de l'ordre de la milliseconde (pour plus détails voir chapitre 2 section 2.3.3).
Concernant les catégories de protocoles de routage, la notification de la couche liaison est généralement utilisée par les protocoles de routage réactifs et très peu par les protocoles proactifs. Étant donné que dans un protocole proactif, les phases d'une restauration s'effectuent de façon périodique, ce mécanisme n'améliore pas généralement le temps global de la restauration. Par ailleurs, il peut entrainer des désynchronisations entre les tables de routage des nœuds [ATC+09]. Ces désynchronisations persisteront jusqu'à la prochaine diffusion des informations sur la topologie du réseau par le nœud détecteur.

- Acquittement de niveau routage (ANR) : Le protocole de routage Dynamic Source Routing DSR [JHM07] propose en absence d'autres mécanismes de détection d'utiliser les acquittements de la couche routage pour vérifier la disponibilité de la communication entre deux nœuds adjacents. Chaque nœud qui transmet un paquet vers un nœud adjacent sera responsable de la vérification de la bonne réception du paquet par son voisin. Dans le protocole DSR, chaque paquet possède une option appelée Acknowledge Request Option qui permet à un nœud émetteur de demander un acquittement explicite pour chaque paquet de données au nœud récepteur.
  Par exemple un nœud n_i souhaitant transmettre un paquet à un voisin (nœud n_{i+1}) positionne cette option pour indiquer qu'il souhaite recevoir un acquittement de niveau routage de la part du nœud n_{i+1}. Si le nœud n_i reçoit un acquittement provenant du nœud n_{i+1}, il peut choisir de ne plus lui demander d'acquittement durant une durée appelée *MaintHoldOffTime*. Sinon, le nœud n_i retransmet le paquet de données pour lequel il n'a pas reçu d'acquittement

MaxMaintRexmt fois. En cas de non réception d'acquittement après ces retransmissions, le nœud n_i détecte l'état de panne de communication avec le nœud voisin n_{i+1} et supprime le lien utilisé de son cache.
Cette méthode présente l'avantage d'être indépendante de la sous-couche MAC utilisée (à l'instar des protocoles de découvertes de voisins) et d'être assez rapide. Son temps de détection peut être formulé comme suit :

$$E\left\{T_{d_{(n_i,n_{i+1})}}\right\}_{(ANR)} = \frac{MaintHoldOffTime}{MaxMaintRexmt} \tag{1.16}$$

En utilisant les valeurs proposées RFC 4728 ($MaxMaintRexmt = 2$ et $MaintHoldOffTime = 250$ millisecondes) dans la formule précédente, nous obtenons le temps moyen avant la détection :

$$E\left\{T_{d_{(n_i,n_{i+1})}}\right\}_{(ANR)} = 0.125 \text{ sec} \tag{1.17}$$

Les principaux inconvénients de cette technique sont une augmentation de la taille des paquets de données (ajout de la demande d'acquittement de taille $T_{Ack-Request}$) et une génération d'*overhead* supplémentaire (les acquittements). D'autre part, le mécanisme n'est pas adapté pour les routes utilisées pour envoyer un trafic sporadique (trafic discontinu) car tout lien inutilisé durant *MaintHoldOffTime* est supprimé. Ce qui nécessitera une nouvelle découverte à chaque fois que les nœuds d'extrémité souhaiteront communiquer.
En supposant un lien symétrique établi entre les deux nœuds adjacents, le coût de maintenance dépend de la durée de vie du lien DV_C et de la taille des acquittements T_{Ack} et des demandes d'acquittement $T_{Ack-Request}$:

$$CM_{d(ANR)} = \frac{(T_{Ack} + T_{Ack-Req}) \times DV_C}{MaintHoldOffTime} \tag{1.18}$$

Les tailles des paquets de demande d'acquittement $T_{Ack-Req}$ et d'acquittement T_{Ack} sont respectivement 4 et 12 bytes [JHM07].

Comparaison des trois mécanismes de détection : La figure 1.2 représente le coût de la maintenance d'une communication entre deux nœuds adjacents par les messages *Hello* et acquittements de niveau routage (équations 1.14 et 1.18) et les notifications de couche liaison. Pour chaque mécanisme, l'overhead total généré pour maintenir une route active dépend du nombre de sauts N et du coût de la maintenance entre nœuds adjacents. A partir de la figure 1.2 et des équations 1.13, 1.15 et 1.17, nous déduisons que l'utilisation des notifications de la couche liaison offre le meilleur compromis entre de temps de restauration et de coût.

1.2.1.2.2.2 Corrélation de pannes Après avoir détecté la panne, à présent, il s'agit de permettre au nœud détecteur d'identifier toutes ses routes passant par le nœud pour lequel une panne de communication a été détectée.

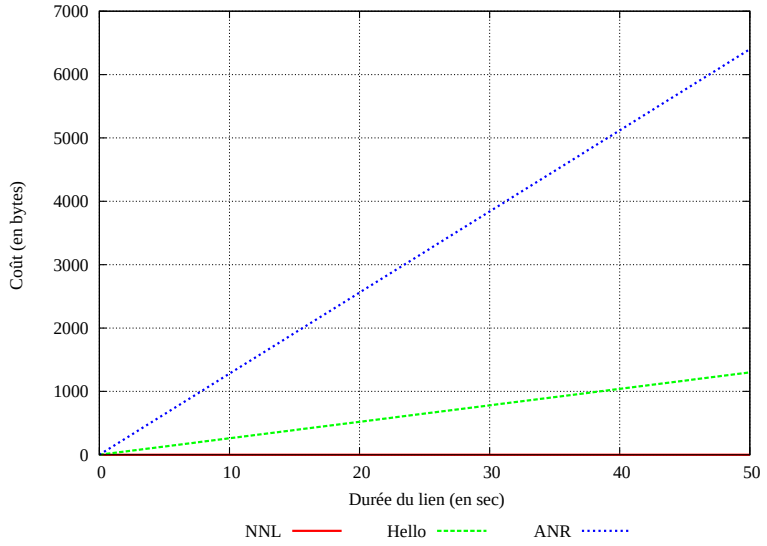


FIGURE 1.2 – Coût de la maintenance CM_d vs Durée de la communication DV_C

Lorsque le nœud détecteur possède une table de routage, il parcourt celle-ci à la recherche de telles routes. Contrairement aux nœuds d'un protocole proactif qui se contentent de supprimer simplement les routes dont le prochain nœud est injoignable, un nœud détecteur dans un protocole réactif crée un message d'erreur de route appelé *Route ERRor* (RERR) Message pour y enregistrer l'identifiant de toutes les destinations qui sont devenues injoignables. Outre, l'identifiant des destinations injoignables, le message RERR contient aussi l'identifiant du nœud détecteur.

Dans la stratégie de routage par la source, le nœud détecteur supprime de son cache toutes ses routes ayant comme prochain nœud, le nœud injoignable. Ensuite, il crée un message d'erreur qu'il va émettre vers le nœud source des données. Ce message contient l'adresse du nœud qui a détecté la défaillance et celle du nœud qui le suit sur la route rompue.

1.2.1.2.2.3 Notification de pannes de routes La notification de pannes dans un protocole réactif s'effectue grâce aux diffusions successives de message d'erreur alors que dans un protocole proactif, elle est mise en œuvre par diffusion des informations sur la topologie du réseau par les nœuds.

– *Protocoles réactifs :* Après avoir détecté la panne de communication et corrélé les pannes de routes, le nœud détecteur initie la phase de notification s'il n'est pas capable de procéder au recouvrement. Il diffuse donc le message d'erreur généré durant la phase de corrélation dans son voisinage à un saut. Le message *RERR* est ensuite diffusé de proche en proche par diffusions successives jusqu'à atteindre un nœud responsable du recouvrement.

La durée de l'opération de notification correspond au temps de parcours des messages d'erreur *RERR* entre le nœud détecteur et le nœud responsable du recouvrement.

– *Protocoles proactifs :* Dans un protocole proactif, la phase de notification de pannes de route s'effectue par les diffusions périodiques des informations sur la topologie du réseau. A l'instar du nœud détecteur, chaque nœud intermédiaire participant à cette étape attend la fin de sa période avant de diffuser ses informations de routage dans son voisinage. Les informations reçues par un nœud en provenance d'un nœud voisin, lui permettent de mettre à jour sa table de routage : suppression des routes vers les nœuds inatteignables, mise à jour des routes existantes, ajout de nouvelles routes.

1.2.1.2.3 Opération de recouvrement d'une route Quelle que soit la catégorie du protocole de routage, le recouvrement consistera à obtenir une nouvelle route.

– Dans le cas des protocoles réactifs *unipath*, le nœud responsable (généralement la source) initiera une nouvelle découverte de routes vers la destination. La durée du recouvrement de pannes correspond donc à la durée de la découverte de routes. Notons toutefois que des améliorations des protocoles AODV [PBRD03] et DSR [JHM07] proposent d'effectuer le recouvrement par les nœuds intermédiaires dans le but de réduire le temps de la restauration et le coût généré en termes de messages de contrôle. Cependant, les routes établies par un nœud intermédiaire ne sont pas en général d'aussi bonne qualité que celles établies par une source.
– Dans un protocole proactif *unipath*, la source obtiendra une nouvelle route vers la destination quand elle reçoit la nouvelle mise à jour de la topologie du réseau. L'opération de recouvrement dure le temps de propagation des informations sur la topologie du réseau entre le nœud détecteur et la source des données.
– Cette nouvelle route est déjà disponible au niveau du nœud responsable du recouvrement dans un protocole de routage *multipath*. Ces protocoles seront détaillés au chapitre 4.

1.2.1.2.4 Reprise du trafic de données Après la réception de la nouvelle route, le nœud responsable du recouvrement procèdera une reprise du trafic en le basculant sur cette dernière. La source et la destination pourront ainsi communiquer jusqu'à l'occurrence d'une nouvelle défaillance sur la nouvelle route.

1.2.1.2.5 Comparaison des durées de restauration La durée de la restauration de service T_R d'un protocole de routage dépend de celles des phases de détection, de notification et de recouvrement car les phases de corrélation et de reprise du trafic sont presque instantanées ($T_c \approx 0$ et $T_{rt} \approx 0$). Ces trois phases sont donc les plus

longues de la restauration de service. Afin de réduire le temps de rupture, il faut donc identifier et utiliser les meilleurs mécanismes possibles pour ces trois phases.

Quels que soient les mécanismes utilisés pour détecter une défaillance entre deux nœuds adjacents, la comparaison des temps de restauration entre les protocoles réactif et proactif consiste à une comparaison entre le temps de découverte d'une route T_{DR} et le temps T_{P-rest} (somme des durées restantes des périodes de diffusions). En utilisant les formules 1.9 et 1.8, nous obtenons :

$$\begin{aligned} T_{R_{RoutProac}} - T_{R_{RoutReac}} &= T_{P-rest} - T_{DR} \\ &= \left[\sum_{j=0}^{N} T_{P-rest_i}\right] - T_{DR} \end{aligned} \tag{1.19}$$

Les protocoles de routage réactifs comme AODV [PBRD03] et DYMO [CP10] définissent une borne maximale de la durée de la découverte à deux secondes ($T_{DR} \leq$ 2 sec). Alors que la valeur de T_{P-rest} n'est pas prévisible à priori et généralement supérieure au temps de découverte de routes des protocoles réactifs. Elle dépend du nombre de nœuds intermédiaires entre le nœuds détecteur et la source, et de leur état au moment de la réception de la notification de la défaillance. Pour effectuer une restauration rapide dans un protocole proactif, une première approche consiste à réduire la durée de la période de diffusion des informations de routage par les nœuds. Une seconde solution est de séquentialiser les phases de restauration de service. C'est-à-dire qu'après avoir détecté et corrélé la panne, le nœud détecteur commence immédiatement l'émission des informations de routage sans attendre la fin de la période prévue. L'inconvénient commun des deux approches est une augmentation importante du nombre des messages de contrôle.

Nous nous appuierons donc sur les protocoles de routage réactifs dans la mise en œuvre de notre architecture robuste pour une gestion efficace des communications.

1.2.1.3 Synthèse : Restauration de service

L'efficacité d'un service de restauration dépend de trois paramètres : le temps nécessaire à la restauration T_R, le coût de la restauration CG_{RS} et la qualité de service fournie par la nouvelle route ou le nouveau chemin. Pour assurer une continuité du service fourni et diminuer le nombre de paquets perdus, le temps de restauration doit être le plus court possible. D'un point de vue du fonctionnement strict, la qualité de service peut être considérée comme le temps de fonctionnement jusqu'à la nouvelle panne. L'objectif est donc d'assurer un certain compromis entre ces trois paramètres.

La durée de la restauration par les protocoles de transport orientés connexion est généralement très longue (supérieure à 63 secondes équation 1.7) comparée à celle des protocoles de routage (borne maximale (1.5+2) secondes). Les restaurations de

niveau transport seront donc très peu utilisées car avant leur mise en œuvre, la couche routage aura déjà recouvert la route rompue et basculé le trafic sur une nouvelle route.

1.2.2 Protection de service

Mis en œuvre lors de la phase d'initialisation (ou de réinitialisation), les mécanismes de protection de service permettent de prévoir, d'anticiper les pannes de communications et aussi d'assurer une tolérance aux défaillances de liens et de nœuds. Dans cette partie, nous commencerons par étudier les mécanismes de prévention et prévision des défaillances. Puis, nous verrons comment assurer une tolérance aux pannes en utilisant les mécanismes de redondances de différents niveaux de la couche protocolaire.

1.2.2.1 Analyse prédictive et préventive des pannes

Elle s'appuie sur un ensemble de mécanismes capable de déterminer l'état futur des composants élémentaires du réseau (les nœuds et les liens). Son but est d'éviter l'occurrence des ruptures de communication, de diminuer la probabilité de leur apparition. Les deux principales métriques utilisées sont la fiabilité et la durée de vie résiduelle (*ie* la durée jusqu'à la prochaine panne). La principale difficulté de cette technique est de pouvoir déterminer avec exactitude la valeur des métriques (fiabilité et durée de vie) des composants élémentaires.

La durée de vie résiduelle d'un nœud mobile dépend en général du niveau de charge restant de sa batterie et de la charge de trafic qui y transite (détermine l'énergie utilisée). La fiabilité et la durée de vie résiduelle d'un lien entre deux nœuds adjacents sont fonction de la distance initiale inter-nœuds, de la portée de la transmission et du modèle de mobilité des nœuds. Puisque la fiabilité est calculée sur un intervalle, la valeur dépend aussi de la durée de cet intervalle (*ie* la durée de la communication).

En fonction de la valeur de la métrique des différents éléments composant la route, l'analyse détermine sa valeur pour la route établie entre les deux nœuds d'extrémité. Ainsi, durant la phase d'initiation de la communication, le protocole de routage calcule la fiabilité ou la durée de vie résiduelle de chacune des routes possibles entre les nœuds d'extrémité (cf. Chapitre 2).

La fiabilité d'une route est le produit entre la fiabilité des équipements élémentaires qui la composent. Alors que la durée de vie résiduelle d'une route correspond à celle des composants élémentaires ayant la plus petite valeur. La route choisie pour transmettre le trafic est celle qui possède la plus grande valeur de fiabilité ou de durée de vie résiduelle. Lorsque la durée de vie résiduelle est déterminée avec

précision, le protocole de routage peut l'utiliser en procédant à une restauration pré-panne qui consiste à anticiper l'état de panne de la route. Cette prévision de défaillances peut permettre d'empêcher et/ou de réduire l'occurrence des ruptures de communications.

1.2.2.2 Redondance (ou Tolérance aux pannes) :

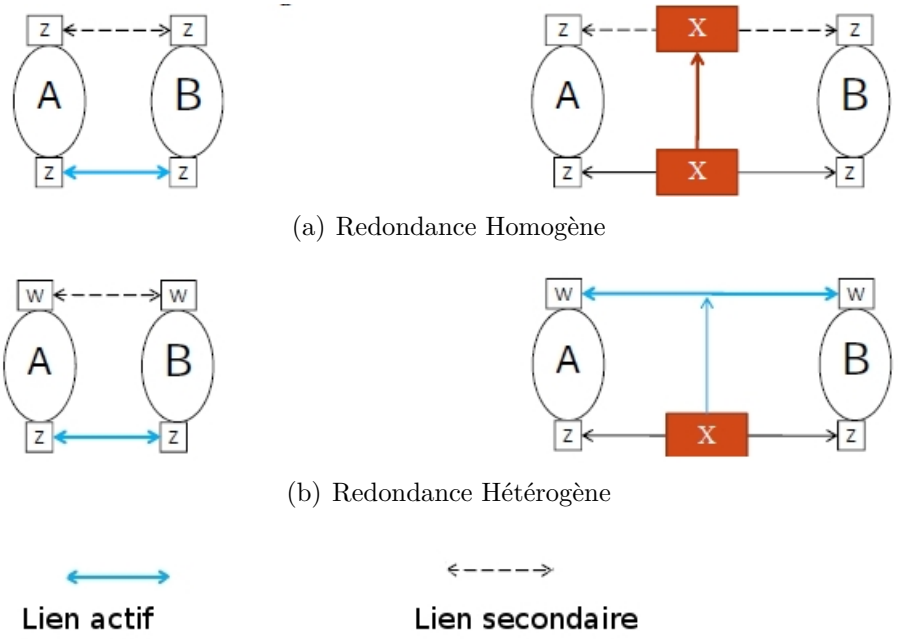
La redondance est un moyen pour améliorer la robustesse dans un réseau MANET qui permet de préserver le service en assurant une reprise presque instantanée du trafic malgré l'occurrence d'une panne. Il existe trois classes de redondance en fonction de l'élément réseau protégé.

Dans cette section, nous étudions ces classes qui sont la redondance de niveau liaison (redondance de liens), de niveau routage (redondance de routes), de niveau transport (redondance de chemins).

1.2.2.2.1 Redondance de liens La redondance de liens consiste à utiliser deux ou plusieurs liens entre nœuds adjacents. Le lien primaire est utilisé pour transmettre les paquets entre les deux nœuds jusqu'à ce qu'il tombe en panne. Après une panne du lien primaire, les communications entre les deux nœuds sont immédiatement basculées sur le lien secondaire. Il existe deux types de redondance de liens : homogène et hétérogène.

On parle de redondance homogène de liens, lorsque le primaire et le secondaire utilisent la même technologie (figure 1.3(a)). L'inconvénient de la redondance homogène est qu'elle ne résiste pas aux défaillances de mode commun. En effet, la rupture du lien primaire entre deux nœuds causée par leur déplacement hors de portée l'un de l'autre entraîne aussi la rupture du lien secondaire. Dans ce cas, aucun recouvrement n'est possible.

Afin de résister aux défaillances de mode commun, une solution consiste à utiliser une redondance hétérogène où les liens utilisés sont de technologies différentes donc des portées et des caractéristiques de puissance différentes (figure 1.3(b)). Par exemple, une application nécessitant un trafic régulier d'un nombre important de paquets de petites tailles entre deux nœuds mobiles très contraints en énergie, peut utiliser une redondance hétérogène (Zigbee/ WiFi)[YWL07]. Le lien établi avec technologie Zigbee est choisi comme lien primaire afin d'optimiser l'énergie utilisée et la taille des paquets (un en-tête Zigbee est plus petit qu'un entête WiFi). Lorsque le lien primaire en Zigbee est rompu suite aux déplacements des nœuds en dehors de la portée Zigbee l'un de l'autre ; le trafic est basculé sur la technologie WiFi, car la portée WiFi est supérieure à celle de la technologie Zigbee.



(a) Redondance Homogène

(b) Redondance Hétérogène

FIGURE 1.3 – Exemple de redondance de liens

1.2.2.2.2 Redondance des routes Les protocoles de routage *multipath* assurent une protection de niveau routage (protection de route) ; contrairement aux protocoles de routage classiques (*unipath*), ils établissent deux ou plusieurs routes entre une source et une destination en fonction de la topologie du réseau. Une première application des protocoles *multipath* est d'envoyer des copies multiples d'un même paquet sur les différentes routes dans le but d'améliorer la probabilité de livraison des paquets. Cependant, cette approche n'est pas très efficace en termes de bande passante et de consommation d'énergie en raison de la grande quantité de messages inutiles transmis. Une seconde approche consiste à utiliser le routage *multipath* uniquement pour assurer une reprise rapide du trafic après une rupture de route, l'objectif est donc de réduire le temps de recouvrement. Ainsi, contrairement aux protocoles *unipath* qui ne prennent en charge que la restauration de service, les protocoles *multipath* mettent en œuvre la protection et la restauration de service. Ce qui leur permet de fournir une robustesse aux communications établies. Le service de protection est assuré par redondance des routes. C'est-à-dire qu'à chaque demande de communication entre une source et une destination, un protocole *multipath* crée une route primaire et un ensemble de routes secondaires en fonction de la topologie du réseau. Donc, en cas de rupture de la route primaire, le trafic est immédiatement basculé sur une des routes secondaires. Cette technique peut permettre de réduire le temps de recouvrement et le trafic de contrôle du protocole qui n'a pas à initier une nouvelle découverte de route. Notons que la capacité de tolérance aux pannes dépend surtout du degré de similitude entre les routes primaires et secondaires (disjoints en lien, en nœud, en interférences), (figure 1.4).

Une route primaire et une route secondaire sont disjointes en interférences si aucun nœud sur la route primaire n'est à portée radio d'un nœud sur la route secon-

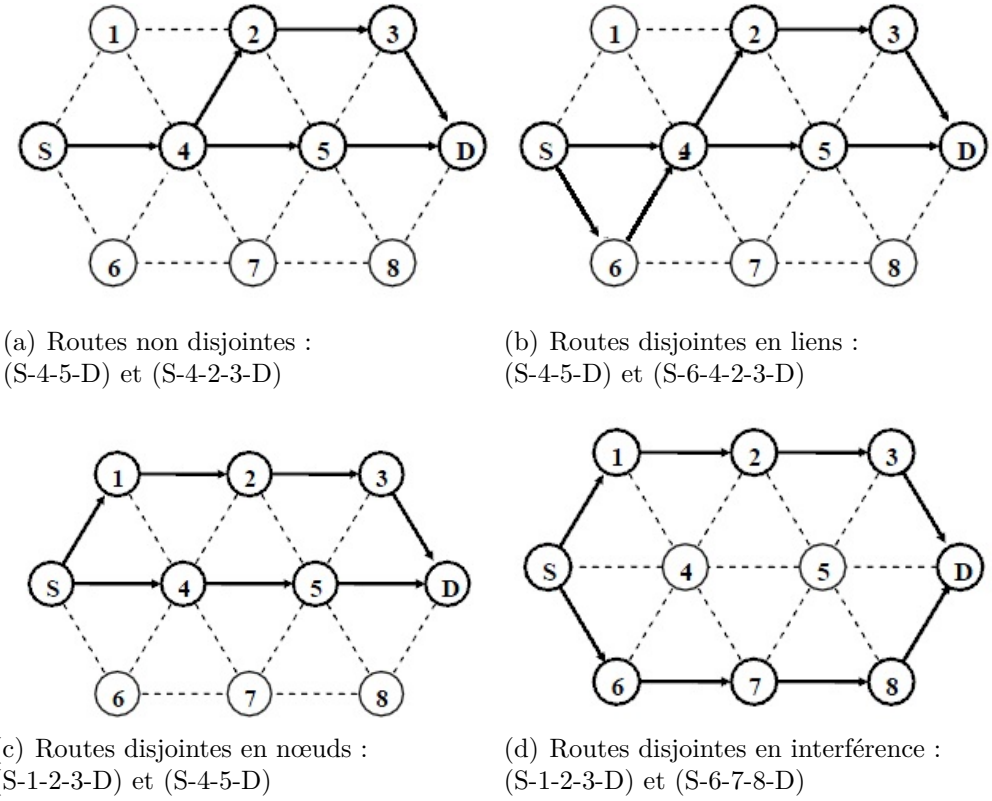
daire et inversement (figure 1.4(d)). Deux routes disjointes en nœud ne possèdent aucun nœud commun excepté la source et la destination (figure 1.4(c)). Alors que deux routes disjointes en lien n'ont aucun lien en commun mais peuvent cependant avoir des nœuds communs (figure 1.4(b)). Naturellement, deux routes disjointes en interférences ou en nœuds sont aussi disjointes en lien.

En fonction du degré de similitude entre les routes primaire et secondaire, deux schémas de recouvrement peuvent être utilisés : recouvrement de bout en bout et recouvrement par segments de routes.

1.2.2.2.2.1 Recouvrement de bout en bout Lorsque la route primaire et la route secondaire sont disjointes en nœuds ou en interférences, seul le recouvrement de bout en bout est possible. Dans ce type de recouvrement, le nœud responsable est la source qui procède soit à un basculement du trafic sur la route secondaire soit à l'initialisation d'une nouvelle découverte. La complexité du processus de recouvrement est simplifiée au niveau des nœuds intermédiaires qui se contentent d'émettre et de relayer la notification de panne. Le principal inconvénient de cette technique est la longueur du domaine de recouvrement qui est la route complète. Ceci peut entraîner une durée importante de restauration lorsque la panne détectée est éloignée de la source.

1.2.2.2.2.2 Recouvrement par segment de routes Quand le protocole de routage met en place des routes disjointes en liens, en plus de la source, le recouvrement peut être effectué par tout nœud intermédiaire qui possède une autre route alternative quand la route primaire est rompue. Ceci est appelé recouvrement par segment de routes. Dans cette stratégie de recouvrement, une route n'est plus considérée comme un ensemble homogène unique mais plutôt comme un ensemble de segments de routes. Ainsi chaque segment de la route primaire peut être protégé ou non par un segment de route secondaire en fonction de la topologie. Le recouvrement segmenté fournit une meilleure protection que le recouvrement de bout en bout. En effet, lorsque des pannes simultanées surviennent sur les routes primaire et secondaire en même temps (par exemple, ruptures simultanées des liens $L_{S,4}$ et $L_{2,3}$ figure 1.4(b)), le recouvrement par segment procède à une reprise du trafic en isolant le segment en panne sur la route primaire pour le remplacer par un segment secondaire. La nouvelle route utilisée sera $(S \leftrightarrow 6 \leftrightarrow 4 \leftrightarrow 5 \leftrightarrow D)$. Par ailleurs, le recouvrement segmenté est généralement plus rapide que le recouvrement de bout en bout car son domaine de recouvrement est plus court que la route entière.

1.2.2.2.3 Redondance de chemins (Redondance de niveau transport) Le *multihoming* est défini comme étant la capacité d'un nœud à pouvoir utiliser plusieurs interfaces (ou adresses IP) pour communiquer avec un autre nœud, il a été introduit dans les réseaux filaires pour permettre aux nœuds d'extrémité de disposer de plusieurs accès (fournisseurs) internet. Plusieurs chemins peuvent alors être



(a) Routes non disjointes : (S-4-5-D) et (S-4-2-3-D)

(b) Routes disjointes en liens : (S-4-5-D) et (S-6-4-2-3-D)

(c) Routes disjointes en nœuds : (S-1-2-3-D) et (S-4-5-D)

(d) Routes disjointes en interférence : (S-1-2-3-D) et (S-6-7-8-D)

FIGURE 1.4 – Degré de similitude entre routes dans un protocole de routage *multi-path*

associés aux interfaces de la source et de la destination. Ces multiples chemins sont utilisés soit pour assurer le partage de charge soit pour améliorer la robustesse du transfert de données.

Dans cette thèse, nous nous intéressons à l'utilisation de la multi-domiciliation comme technique de redondance dans le but d'augmenter la probabilité de survie d'une session en présence d'une défaillance dans le réseau. Le *multihoming* fournit donc un service complémentaire de tolérance aux pannes.

Lorsque la redondance est utilisée pour améliorer la robustesse du transfert de données, la transmission des données s'effectue sur le chemin primaire jusqu'à la détection d'une rupture de connexion (indisponibilité de la connectivité IP). Ensuite, la source se connectera de façon transparente à un des chemins secondaires puis y basculera son trafic. Le chemin alternatif choisi assurera la communication jusqu'à ce qu'il tombe en panne lui aussi ou que le chemin primaire soit restauré. Notons que les chemins établis peuvent de ne pas être disjoints de bout en bout. Le recouvrement est géré de bout en bout par le protocole de transport.

Les protocoles transport SCTP [SXM+00, Ste07] (Stream Control Transport Protocol) et MP-TCP [Bag11, FRH+11] (Multipath Transport Control Protocol) sont des exemples de protocoles capables de prendre en charge la multidomiciliation (*mul-*

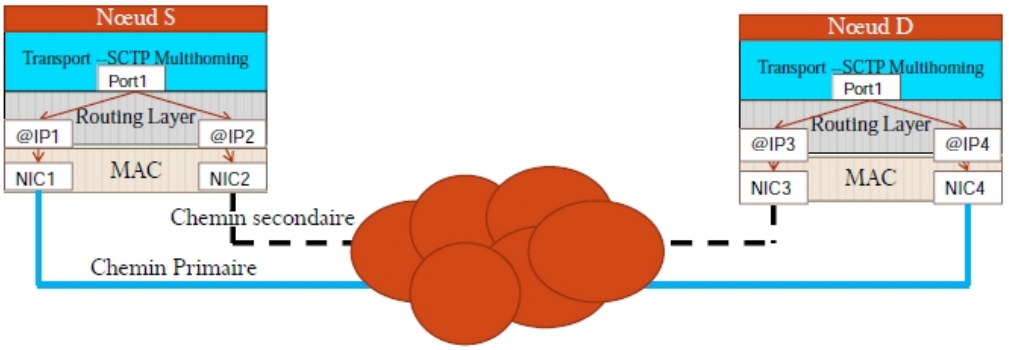


FIGURE 1.5 – Exemple de multidomiciliation SCTP

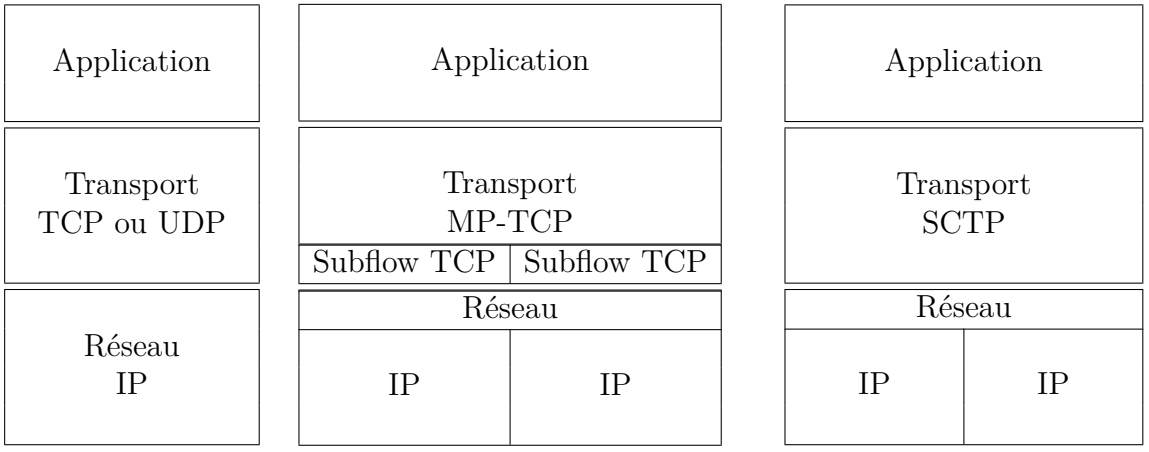


FIGURE 1.6 – Comparaison entre les architectures TCP/UDP, MP-TCP et SCTP

tihoming). Ces deux protocoles s'appuient sur l'expérience du protocole TCP pour améliorer certains aspects de la communication fiable et définissent une notion de "méta connexion" pour gérer un transfert d'information composé de plusieurs flux (*multistreaming*) et le *multihoming* des extrémités (figure 1.6). La gestion de la multi-domiciliation par les protocoles SCTP et MP-TCP est assez semblable.

La figure 1.5 répresente un exemple de communication SCTP à travers un réseau entre deux nœuds A et B multi-domiciliés possédant chacun deux adresses IP(Internet Protocol).

1.2.2.2.3.1 Protocole MP-TCP [Bag11, FRH+11] Un nœud source initie une "méta connexion" lorsqu'une application utilisatrice désire joindre son pair sur un nœud destination D. Une *méta connexion* MP-TCP est composée d'une ou de plusieurs connexions TCP (*sous-flux TCP*) en fonction du nombre d'interface(s) disponible(s) sur les deux nœuds d'extrémité. Un sous-flux TCP est identifié par un quintuplet : adresse IP source, port source, adresse IP destination, port destination,

protocole. Dans MP-TCP par défaut, l'ensemble des sous-flux TCP sur les nœuds d'extrémité utilisent le port 80.

Le protocole MP-TCP commence par établir un premier sous-flux TCP en ajoutant aux messages d'ouverture de connexion du protocole TCP (SYN, SYN/ACK et ACK) son option MP_CAPABLE. L'option MP_CAPABLE est utilisée uniquement lors de l'établissement de la connexion du premier sous-flux TCP entre les deux nœuds dans le but d'identifier la "méta connexion" MP-TCP ouverte. L'ajout à la "méta connexion" d'un nouveau sous-flux TCP se fait par l'échange des trois messages (SYN, SYN/ACK et ACK) avec l'option MP_JOIN.

Un exemple d'ouverture de "méta connexion" MP-TCP entre deux nœuds d'extrémité S et D est illustré à la figure 1.7. Le nœud S établit les deux premiers sous-flux TCP ($S_1 \leftrightarrow D_1$ et $S_2 \leftrightarrow D_1$). Ensuite, le nœud D ajoute sa seconde interface à la "méta connexion" : ($S_1 \leftrightarrow D_2$ et $S_2 \leftrightarrow D_2$). Notons qu'à tout instant durant la "méta connexion", un nœud peut informer son pair de la disponibilité ou non de certaines de ses interfaces, changer la priorité d'un sous-flux TCP.

Chaque segment transmis par le protocole MP-TCP possède deux numéros de séquence : un numéro de séquence de niveau "méta connexion" MP-TCP et un numéro de séquence pour chaque sous-flux TCP. La numérotation de niveau "méta connexion" permet au nœud récepteur de réordonner les segments de données reçus sur différents sous-flux TCP avant de les transmettre à sa couche applicative. Alors que les numéros de séquence niveau sous-flux TCP permettent de détecter et retransmettre les segments perdus sur un même *subflow TCP*.

Le protocole MP-TCP est proposé pour faire un partage de charge sur les différents chemins établis. Dans ce cas, la validité des multiples chemins est vérifiée comme dans TCP. En conséquence, contrairement au protocole SCTP (voir la sous-section suivante), il n'existe aucun mécanisme pour vérifier la validité d'un chemin de secours non utilisé pour transmettre le trafic.

1.2.2.2.3.2 Protocole SCTP [SXM+00, Ste07] Dans le protocole SCTP, une "méta connexion" appelée association SCTP s'établit par l'échange de quatre messages (INIT INIT-ACK, COOKIE-ECHO COOKIE-ACK) entre les nœuds d'extrémité pour offrir une meilleure protection contre le dénis de service. Nous illustrons l'établissement d'une association entre deux nœuds S et D multi-domiciliés (figure 1.8).

Les messages INIT et INIT-ACK émis respectivement par la source (pour initier l'association) et la destination (en réponse à un message INIT) contiennent l'ensemble des adresses IP du nœud émetteur. Un nœud effectue une corrélation entre ses adresses IP et les adresses IP de l'autre nœud d'extrémité apprises à la réception d'un message INIT ou INIT-ACK. Notons que les quatre paquets d'établissement

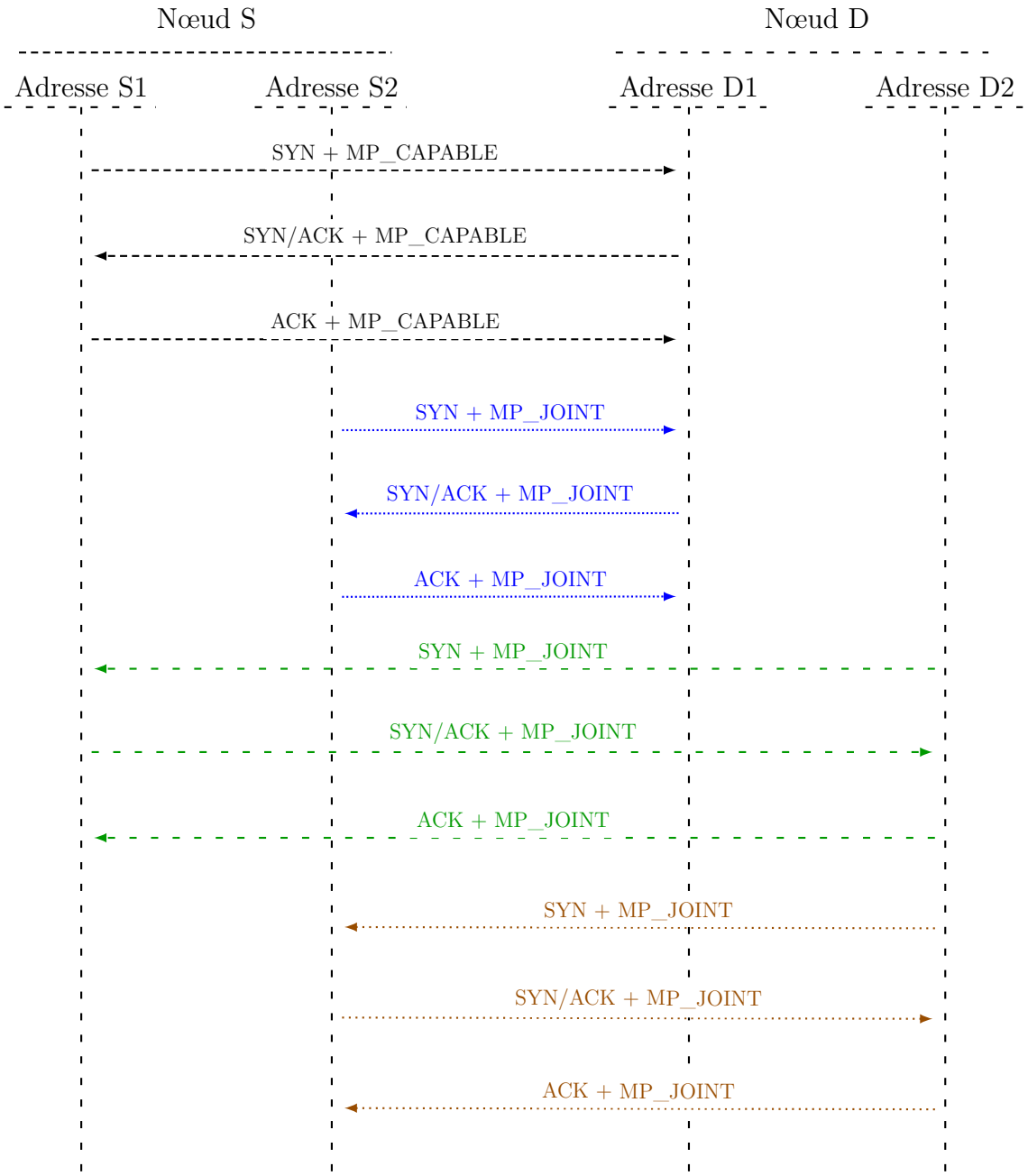


FIGURE 1.7 – Etablissement d'une "meta-connexion" MP-TCP

de l'association sont échangés entre les adresses transport primaires des nœuds S et D.

Après l'établissement de cette association $\{[S_1 , S_2 : Port_S] : [D_1 , D_2 : Port_D]\}$, le protocole SCTP suppose qu'il existe quatre chemins de communications entre les nœuds S et D : $(S_1 \leftrightarrow D_1)$, $(S_1 \leftrightarrow D_2)$, $(S_2 \leftrightarrow D_1)$ et $(S_2 \leftrightarrow D_2)$. Cette hypothèse est juste, lorsque les nœuds communiquent à travers internet comme sur la figure 1.5. Cependant, dans le cas où chaque nœud est connecté à deux réseaux totalement disjoints (par exemple S_1 et D_1 utilisant Ethernet ; et S_2 et D_2 satellite ou sans fil),

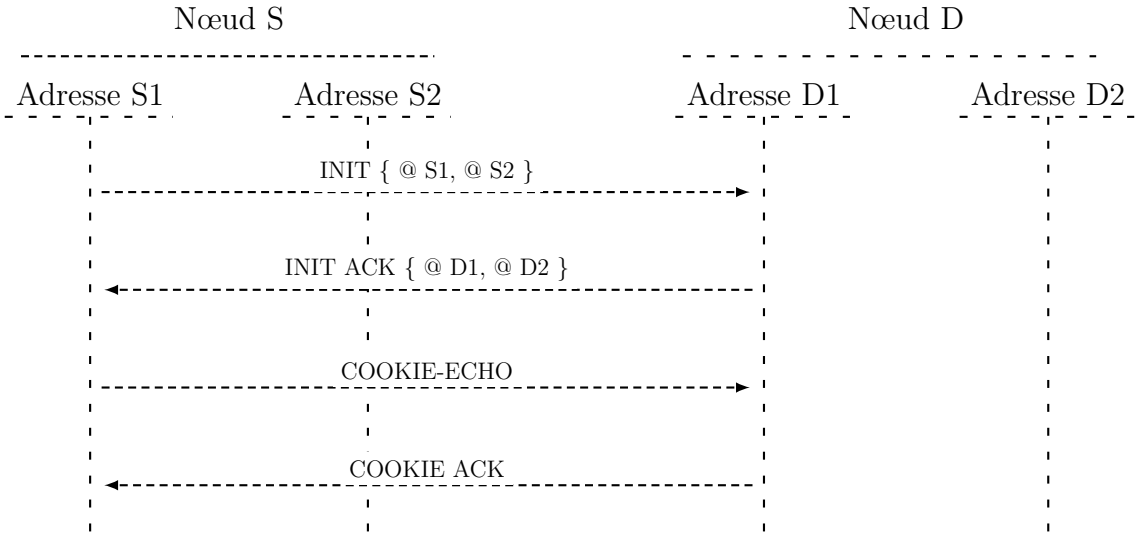


FIGURE 1.8 – Etablissement d'une association SCTP

uniquement deux chemins sont possibles : $S_1 \leftrightarrow D_1$ et $S_2 \leftrightarrow D_2$. La vérification de l'existence ou non d'un chemin de communication sera effectuée par la source S.

D'une manière générale, tout au long de l'association, un nœud SCTP vérifie la validité de chaque chemin de communication dont l'adresse transport destination est déclarée inoccupée par émission périodique de message HEARTBEAT. Une adresse transport est déclarée inoccupée si elle n'a pas été utilisée durant une période prédéfinie (normalement supérieure ou égale à HB.interval) pour transmettre des données ou des acquittements. Un message HEARTBEAT est associé à une adresse transport source et à une adresse transport destination. A chaque HB.interval (30 secondes par défaut), un nœud SCTP envoie un HEARTBEAT à chaque adresse transport inoccupée du nœud destination négociée lors de la phase d'établissement de l'association. La destination transport acquitte chaque requête HEARTBEAT par une réponse HEARTBEAT-ACK qui empruntera le chemin inverse de la requête.

Un nœud d'extrémité incrémente le paramètre *error counter* associé à une adresse transport destination lorsqu'il ne reçoit pas d'acquittement de cette adresse avant une durée RTO (*retransmission timeout*) Le paramètre *error counter* d'une adresse transport destination est réinitialisé chaque fois que le nœud émetteur reçoit un acquittement provenant de cette adresse destination. Ce mécanisme permet de vérifier la validité des chemins secondaires utilisés.

Cette surveillance SCTP permet de détecter deux pannes possibles soit une rupture d'un chemin de communication soit un nœud destination injoignable.

– Une rupture d'un chemin de communication associé à une adresse transport est détectée quand la valeur de son compteur d'erreur dépasse le seuil *Path .Max.Retrans* (par défaut 5 essais). L'émetteur marque alors cette adresse destination transport comme inactive arrête de transmettre ses paquets de

données sur le chemin associé. Quand le chemin primaire est marqué inactif, l'émetteur bascule automatiquement son trafic de données vers le nœud destination sur un chemin alternatif actif entre les deux nœuds s'il existe. Notons que si l'association n'est pas fermée (le trafic a été basculé sur le chemin secondaire), le nœud source continuera à envoyer périodiquement des *chunck* HEARTBEAT sur le chemin primaire pour vérifier son état. Quand le chemin primaire redevient actif (réception d'un *chunck* HEARTBEAT-ACK par la source), le protocole SCTP basculera le trafic dessus.
Ce mécanisme permet surveiller en même temps le chemin primaire et les chemins alternatifs au prix d'un nombre important de message de contrôle.

– La source considère qu'un nœud destination n'est plus joignable lorsque son paramètre *error counter* (la somme des paramètres *error counter* associées aux différentes adresses du nœud destination) devient supérieur à la valeur du *Association.Max.Retrans* (par défaut 10 essais), elle entre alors en phase de fermeture de l'association. Le paramètre *Association.Max.Retrans* associé à un nœud terminal distant doit être inférieur égale à la somme des paramètres *Path.Max.Retrans* de ses toutes adresses transport. Sinon, toutes les adresses de destination peuvent devenir inactives tandis que le nœud d'extrémité source considère toujours le nœud pair destination atteignable.

1.2.3 Architectures couplées de protection et restauration de service

Les figures 1.9 et 1.10 détaillent les processus de restauration des deux architectures de protection. Dans la première architecture, la protection et restauration s'effectuent au niveau routage alors que dans la seconde architecture, elles sont mises en œuvre au niveau transport.

Dans la section 1.2.1, nous avons montré analytiquement qu'une restauration par le routage est plus rapide qu'une restauration par le protocole transport. Notons qu'en terme de protection, le recouvrement de bout en bout du niveau routage fournit un service similaire que la redondance de chemins. En conclusion, si nous utilisons une protection par la redondance, l'architecture de protection et restauration de niveau de routage est préférable.

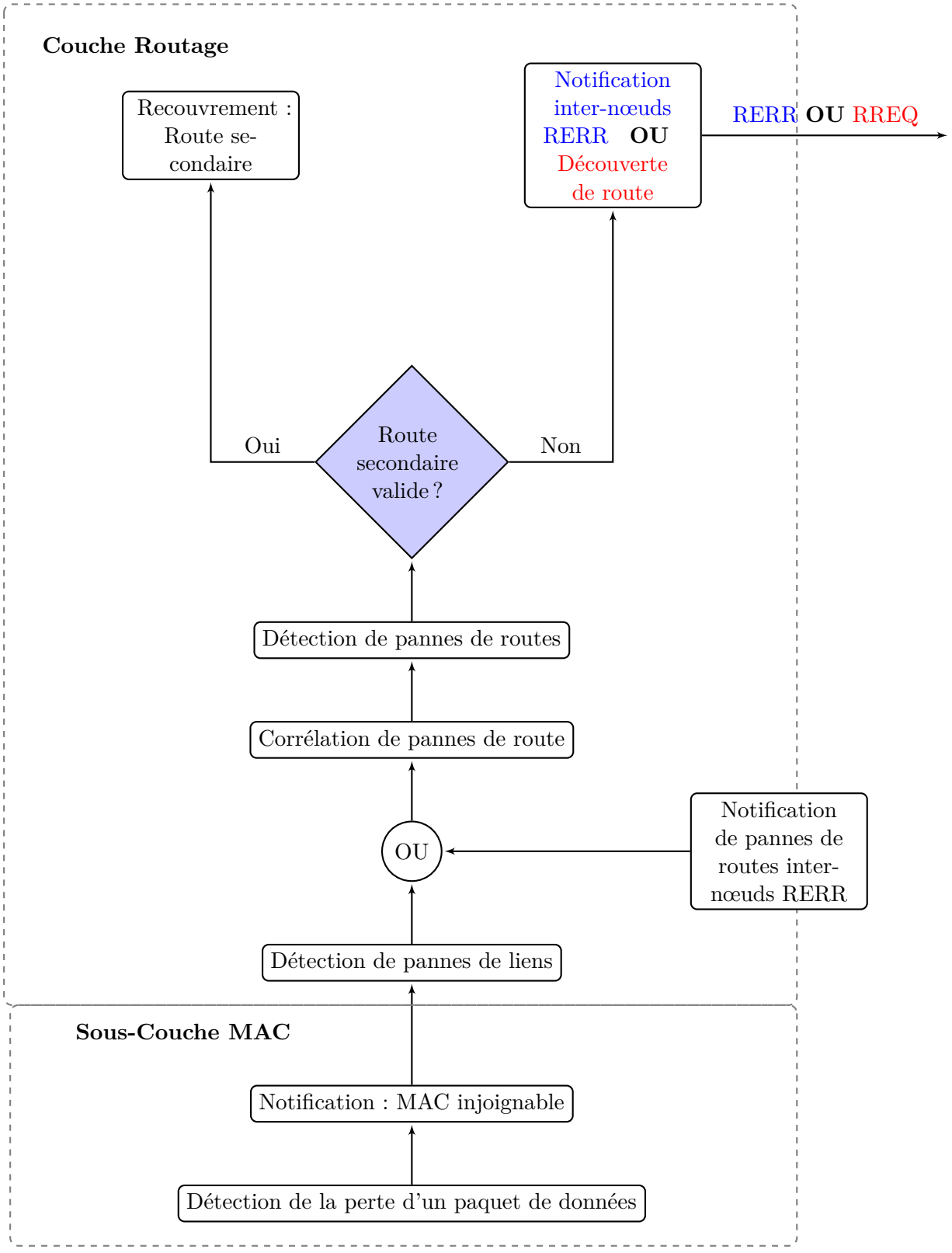


FIGURE 1.9 – Protection / Restauration de service par le routage

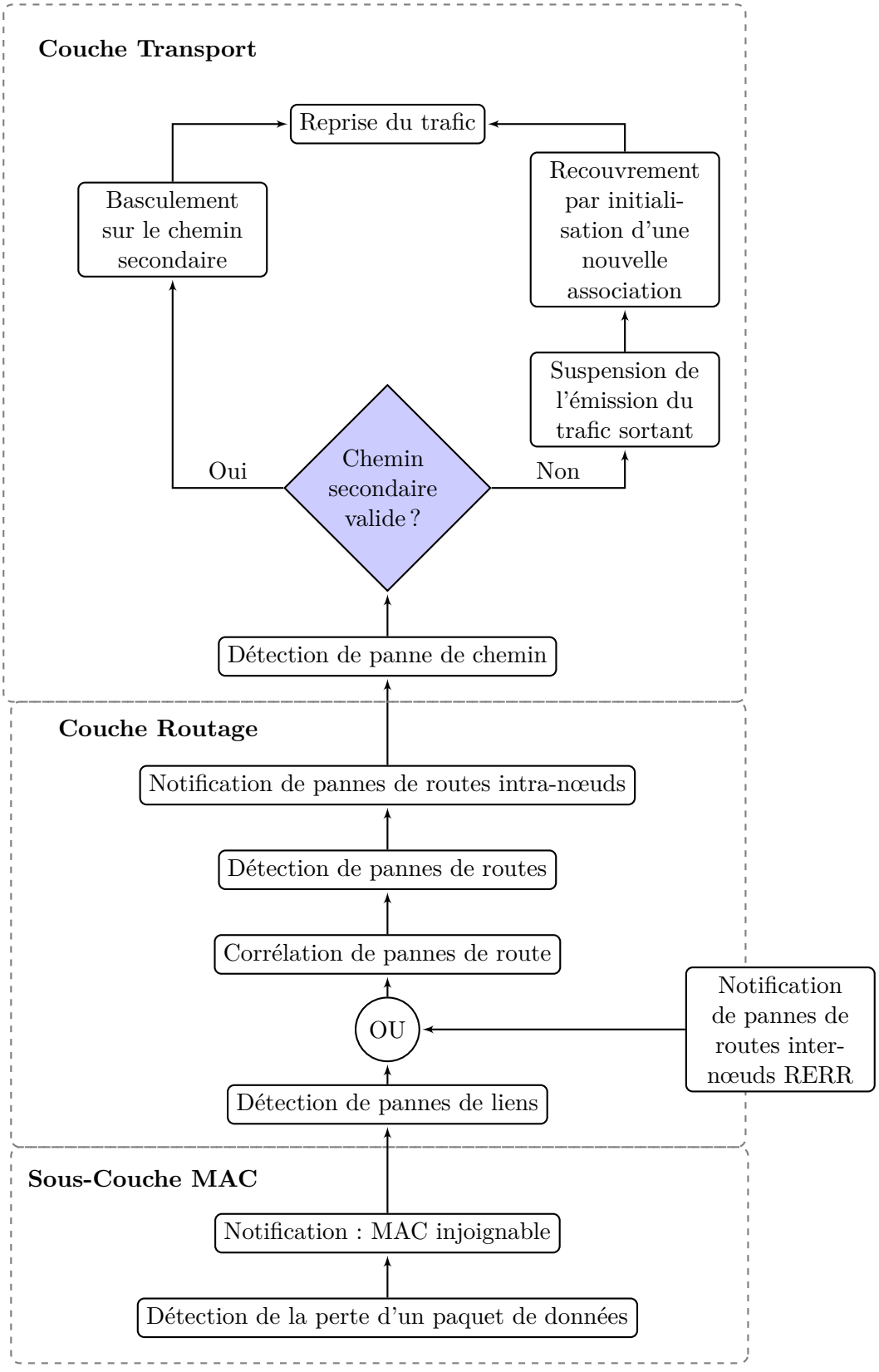


FIGURE 1.10 – Protection / Restauration de service par le protocole transport

1.3 Conclusion

Dans ce chapitre, nous avons fait un état de l'art des différents mécanismes permettant d'assurer une robustesse aux communications entre deux nœuds d'extrémité dans un réseau ad hoc.

Après une présentation des concepts de la sûreté de fonctionnement dans le domaine des communications ad hoc, nous avons étudié les techniques d'analyse et de gestion des pannes. Les deux techniques présentées sont la restauration et la protection de service. Dans un premier temps, nous avons étudié l'élimination des pannes à travers la restauration de service des protocoles de routage et transport. Cette étude nous a permis d'identifier et de comparer les mécanismes utilisés pour chaque phase de la restauration. Les principaux critères d'évaluation d'un service de restauration sont sa durée, son coût et le temps jusqu'à la prochaine défaillance. Nous en avons déduit que les protocoles de routage réactifs assurent un meilleur compromis des paramètres d'évaluation que les protocoles de routage proactifs et transport.

Ensuite, nous avons abordé les techniques de protection de service : protection par analyse prédictive et préventive et protection par redondance. La première solution assure la prévention et la prévision des ruptures de communications ad hoc. Elle s'appuie sur les méthodes qui permettent de prédire l'état futur des équipements du réseau. Ces méthodes peuvent être introduites dans un protocole de routage afin d'améliorer ses performances en termes de taux de livraison et de délai de bout en bout des paquets. La seconde solution fournit un service de la tolérance aux pannes en effectuant des reprises presque instantanées. Nous avons étudié les trois niveaux de redondances possibles à savoir les redondances de liens, de routes et de chemins. La prise en charge la multi-domiciliation a été aussi étudié à travers les protocoles de transport (MP-TCP et SCTP).

Dans la suite du document, nous proposons d'améliorer la robustesse selon deux approches : l'approche par une analyse prédictive (Partie I : chapitres 2 et 3) puis l'approche par la redondance (Partie II : chapitre 4).

Première partie

Approche de robustesse par analyse prédictive

Dans cette partie, nous étudions l'amélioration de la robustesse à l'aide des mécanismes prédictifs au niveau routage.

Le chapitre 2 propose une méthode analytique de calcul de la fiabilité d'un lien dans un réseau MANET. La fiabilité prédite par la méthode proposée tient compte des différents facteurs de la communication sans fil notamment le modèle de mobilité, les collisions inter-paquets et les atténuations du signal. Les modèles de mobilité étudiés sont *Random Walk* et *Random Way Point*. L'avantage de cette approche est la non-génération d'*overhead* supplémentaire pour le calcul de la métrique.

Le chapitre 3 est consacré à l'utilisation des métriques prédictives dans un protocole de routage réactif. Nous commençons par introduire le modèle analytique proposé dans le protocole DYMO [CP10]. Nous montrons ensuite que le choix de la fiabilité comme métrique améliore la durée de vie des routes (par rapport à métrique du *minimum de sauts*) donc une augmentation du taux de livraison. Cependant, son utilisation risque d'augmenter le nombre de sauts des routes. Nous proposons alors une nouvelle métrique qui assure un bon compromis entre la fiabilité et le minimum de sauts. Enfin, nous comparons les différentes métriques en termes de taux de livraison, de délai de bout en bout et de nombre de sauts.

Chapitre 2

Méthode analytique de calcul de la fiabilité de lien

Table des matières

Dans ce chapitre, nous proposons une méthode analytique pour calculer la fiabilité d'un lien dans un réseau MANET.

En introduction à ce chapitre, nous montrons l'avantage de l'utilisation la fiabilité de routes comme métrique dans le routage en termes de taux de pannes routes et taux de livraison des paquets. Ensuite, dans la section 2, nous étudions les deux approches proposées dans la littérature pour déterminer la fiabilité (ou stabilité) d'un lien dans un réseau mobile ad hoc : calcul fondé sur force du signal ou sur la mobilité des nœuds.

Dans la section 3, nous proposons une méthode analytique de calcul de la fiabilité d'un lien dans un MANET où les nœuds se déplacent selon les modèles de mobilité *Random Walk* et *Random Way Point*. La méthode de base modélise la probabilité d'évolution de la distance inter-nœuds. Celle-ci est ensuite affinée pour prendre en compte les propriétés de communication sans fil notamment la probabilité de collision inter-paquets et les atténuations du signal (liées au modèle de propagation caractéristique de l'environnement de déploiement du réseau). Le modèle analytique proposé est validé par simulation en comparant les fiabilités prédites et observées.

2.1 Introduction

L'objectif de tout réseau est d'assurer une transmission efficace des données en optimisant le compromis entre le taux de livraison des paquets de données et les messages de contrôle. Lorsque la source et la destination ne sont pas dans la même zone de couverture, l'acheminement des données nécessite alors la mise en œuvre d'un routage multi-sauts. La principale difficulté du routage dans un réseau MANET est la gestion de la dynamicité de la topologie due à la mobilité des nœuds, aux défaillances des nœuds et des liens de communication. Cette dynamicité de la topologie entraine des ruptures de routes entre des nœuds source et destination.

A chaque rupture de routes, le protocole de routage réactif doit procéder à une opération de maintenance corrective (restauration de service) en effectuant soit un basculement du trafic sur une route secondaire (protocoles *multipath*) soit une nouvelle découverte de routes (protocoles *unipath*). Cette restauration entraine la génération d'un nombre important de messages de contrôle. De plus, les ruptures de routes entrainent une dégradation des performances du réseau en termes de taux de livraison des paquets de données car toutes les données émises par la source entre l'occurence de la défaillance de routes et la réception de la notification de pannes sont perdues. Par ailleurs, les paquets de données non encore émis par la source avant la réception de la notification sont susceptibles de subir une augmentation du délai de bout en bout en raison du temps de recouvrement.

Pour améliorer les performances du protocole de routage, un des objectifs est donc de réduire le nombre de ruptures de routes. Pour cela, les protocoles de routage en charge de l'établissement, de la maintenance et du recouvrement des routes doivent choisir la meilleure route lors de la phase d'établissement en fonction d'un ou plusieurs critères. Par défaut, les protocoles classiques comme AODV [PBRD03], DSR [JHM07], DYMO [CP10], OLSR [CJ03] choisissent comme critère de sélection des routes : le minimum de sauts. Ils établissent entre la source et la destination, la route ayant le minimum de nœuds intermédiaires. Cependant, ce critère n'est pas très adapté dans un réseau mobile ad hoc car contrairement aux liens filaires, les liens ad hoc n'ont pas les mêmes probabilités de panne. En effet, lorsque le nombre de nœuds est minimisé, les nœuds sont plus éloignés ce qui peut conduire à une diminution de la qualité des liens en termes de débit (bande passante) et une augmentation du taux de pannes des routes.

Pour réduire le taux d'échec des routes, nous proposons d'utiliser comme critère de sélection : la fiabilité de la route. La route ainsi construite est celle qui possède la plus forte fiabilité. L'optimisation de la fiabilité de la route permet d'améliorer la qualité des liens utilisés et une meilleure utilisation des ressources du réseau (réduction du coût du routage) [XBJ07]. La connaissance de la fiabilité ou/et de la disponibilité d'une route dans un protocole de routage améliore la durée de vie et le débit de routes, le délai de bout en bout et le taux de livraison des paquets de données [SZG+06, SZG+07, SDJ01].

Nous étudions dans la prochaine section, comment déterminer la fiabilité d'un lien dans un MANET.

2.2 Méthodes de calcul de la fiabilité d'un lien

Les méthodes proposées dans la littérature pour déterminer la fiabilité ou la stabilité d'un lien ad hoc peuvent être divisées en deux catégories : les méthodes reposant sur la force du signal et les méthodes reposant sur la mobilité des nœuds.

2.2.1 Fiabilité reposant sur la force du signal

Dans cette première approche, un nœud déduit l'état du canal avec un voisin en fonction de la force du signal reçu. La stabilité du lien est calculée soit à partir de mesures réelles de la force du signal (comme les protocoles ABR[Toh96], SSA[DRWT97], ASBM [Lim02] et RABR[RAB00]) soit en s'appuyant sur un modèle analytique prédisant les futures positions du voisin dans le temps [PNBS99].

Le protocole ABR [Toh96] est un protocole réactif qui s'appuie sur la métrique stabilité des liens pour construire ses routes lors de la découverte de routes. Chaque nœud diffuse périodiquement un signal pilote (dans un message *Hello*) pour signaler son existence à ses voisins. Pour calculer la stabilité de ses liens adjacents, un nœud maintient une table d'association dans laquelle à chaque entrée est associée un compteur et une minuterie. Lorsqu'un nœud a reçoit un signal pilote d'un voisin b avant l'expiration de la minuterie associée, il incrémente le compteur $Cpt(L_{a,b})$ du nombre de signaux pilotes reçus consécutivement et réinitialise la minuterie. A chaque expiration du temporisateur, le nœud déclare le lien adjacent comme instable et réinitialise le compteur de signaux pilotes associé. Un nœud considère un lien $L_{a,b}$ comme stable si son compteur dépasse le seuil fixé $A_{threshold}$ (par défaut 5). Notons qu'un lien établi entre deux nœuds adjacents fixes ou ayant des mouvements corrélés est considéré stable.

Le protocole SSA [DRWT97] utilise une approche similaire au protocole ABR. C'est une extension du protocole DSR qui s'appuie sur la force du signal et la stabilité des positions des nœuds pour construire ses routes lors de la découverte. Le critère de sélection de la route est un compromis entre ces deux métriques. L'objectif principal est d'établir des routes composées exclusivement de liens courts, c'est-à-dire des routes où il existe une forte connectivité entre chaque pair de nœuds adjacents. Contrairement au protocole ABR, le calcul de la stabilité ne s'effectue plus uniquement sur les signaux pilotes mais à chaque réception de paquet. Un nœud a calcule la stabilité $SS_{cumulative_b}$ du lien $L_{a,b}$ avec le nœud b comme suit :

$$SS_{cumulative_b} = \alpha \times SS_{cumulative_b} + (1 - \alpha) \times SS_b \tag{2.1}$$

où SS_b est la force du signal dans le paquet reçu, α une constante donnée. Le nœud juge un lien stable si la valeur de la métrique est supérieure au seuil fixé sinon il est déclaré instable. La stabilité des positions des nœuds mesure la durée d'existence du lien. Ici, l'hypothèse de base est qu'un lien qui a existé longtemps a plus de chance

de rester actif dans le futur qu'un nouveau lien. Ce qui n'est pas toujours vérifié. En fait, tout dépend des vitesses et directions des deux nœuds.

Le protocole ASBM [Lim02] propose d'améliorer la méthode de calcul de la stabilité de lien du protocole SSA. Il utilise en plus de la force du signal, la dérivée de sa mesure : la force différenciée du signal (*Differentiated Signal Strength DSS*). Cette métrique indique l'évolution de la force du signal et permet de connaitre le mouvement relatif entre deux nœuds adjacents ; en supposant que la force du signal augmente lorsque les nœuds s'approchent et diminue lorsqu'ils s'éloignent.

$$DSS_b = SS_{cumulative_b} - prevSS_{cumulative_b} \tag{2.2}$$

où $SS_{cumulative_b}$ et $prevSS_{cumulative_b}$ sont respectivement les valeurs cumulatives actuelles et précédentes de la force du signal reçu. Un lien est considéré stable si la force du signal reçu est supérieure au seuil fixé et sa dérivée est supérieure à 0 (la force du signal augmente). En fixant un seuil inférieur à ceux des protocoles ABR et SSA, le protocole ASBM [Lim02] peut choisir des liens ayant un faible signal mais dont la valeur augmente (*ie* les nœuds se rapprochent).

Cependant, avec cette approche, un lien $L_{(i,j)}$ établi entre deux nœuds proches (ayant donc un signal fort) peut être considéré comme instable s'ils s'éloignent même légèrement dans le temps. Pour résoudre ce problème, la méthode ESM [LL06] définit deux seuils Thr_1 et Thr_2 avec $Thr_1 \geq Thr_2$. Lorsque la force du signal est supérieure au seuil Thr_1, le lien est toujours considéré stable car cela indique que la distance entre les nœuds est faible. La méthode proposée dans ESM [LL06] est utilisée pour déterminer la stabilité d'un lien dont la force du signal est comprise entre les seuils Thr_1 et Thr_2. Dans ce mécanisme, un lien stable est un lien établi entre deux nœuds très proches ou entre deux nœuds à distance moyenne mais qui se rapprochent l'un de l'autre.

Une approche similaire à celle d'ABR est proposée pour calculer la qualité et le taux de pertes d'un lien dans les deux sens de la communication [DABM03]. La métrique est nommée ETX *Expected Transmission Count*. Pour un lien, elle correspond au nombre de transmissions avant qu'un paquet soit correctement reçu. La métrique ETX d'une route est égale à la somme des ETXs de ses liens.

A chaque période τ, un nœud diffuse dans son voisinage un paquet *probe*. Après une durée ω, chaque voisin de ce nœud diffuseur calcule le taux de réception des paquets probe égal à $\frac{n_\omega}{(\omega/\tau)}$; avec n_ω, le nombre de paquets probe reçus.

Notons d_f le taux de livraison de paquets probe du nœud a vers b et d_r celui de b vers a. La métrique ETX du lien $L_{a \leftrightarrow b}$ est :

$$ETX = \frac{1}{d_f \times d_r} \tag{2.3}$$

Notons que cette méthode ne tient pas compte de la différence de taille entre les paquets probe et de données. Par ailleurs, les paquets probe sont émis en diffusion alors que les données sont transmises en *unicast*. Or, les paquets en diffusion utilisent une modulation et un codage plus robustes que ceux transmis en *unicast*. Ce qui entraine un problème d'incohérence dans le calcul. De plus, comme les approches précédentes, la méthode nécessite un échange régulier et continuel de paquets probe. Elle s'appuie aussi sur l'hypothèse qu'un lien fiable durant une période donnée, le sera dans le futur. Ce qui n'est pas toujours vrai dans un MANET.

D'une manière générale, les protocoles utilisant la métrique de la force du signal s'appuient sur un historique pour déterminer la stabilité des liens en supposant qu'un lien stable à l'instant présent le restera dans le futur. Ce qui présente une limitation importante car l'historique ne reflète pas tous les changements possibles de l'état des liens dans le futur. De plus, le calcul de la métrique nécessite des échanges réguliers de messages entre les nœuds, ce qui augmente l'*overhead*.

2.2.2 Fiabilité reposant sur la mobilité des nœuds

Ces mécanismes s'appuient sur l'état actuel du lien établi entre deux nœuds adjacents et sur leur modèle de mobilité pour prédire leurs futures positions et ainsi déduire les métriques prévisionnelles (fiabilité et durée de vie résiduelle) du lien. La fiabilité de liens est utilisée dans un protocole de routage comme métrique dans le but de réduire le nombre de défaillances de routes. Alors que la durée vie résiduelle est généralement utilisée par un protocole de routage afin d'anticiper les pannes de routes. Dans ce cas, la source procède à une nouvelle découverte de routes avant la fin de la durée de vie résiduelle prédite de la route utilisée (qui correspond au minimum de la durée de vie tous ses liens).

Les modèles de mobilité sont utilisés pour caractériser le déplacement d'un nœud dans un réseau MANET. Le choix de type de mobilité dépend de l'application visée. Les modèles de mobilité proposés peuvent être divisés en deux groupes :

- Les modèles de mobilité individuelle dans lequel chaque nœud se déplace indépendamment des autres. Les modèles *Random Waypoint*, *Random Direction*, *Gauss-Markov* et *Semi-Smooth Markov* sont des exemples de mobilité individuelle.
- Les modèles de mobilité de groupe partagent le réseau en différents groupes de nœuds. Les déplacements des nœuds appartenant à un même groupe sont alors corrélés entre eux. Les modèles RPGM (*Reference Point Group Model*) et *Sanchez* mettent en œuvre ce type de mobilité.

Notons que les choix des vitesses et des directions des nœuds peuvent être soit aléatoire soit déterministe (en utilisant des traces) soit hybride (déplacement de véhicules sur un réseau routier en utilisant des cartes). Dans ce document, nous nous intéressons à l'étude de la fiabilité des modèles de mobilité aléatoire individuelle.

Les méthodes de calcul de la fiabilité reposant sur la mobilité des nœuds utilise un système de localisation qui permet à chaque nœud de connaitre sa position dans l'espace.

Dans [SLG00], les auteurs proposent un protocole de routage qui initie une nouvelle découverte de route avant l'occurrence d'une défaillance de lien sur la route utilisée. Le mécanisme repose sur une méthode analytique qui tente de prédire la durée de vie restante du lien. La future position d'un nœud i peut être calculée en fonction de sa position actuelle (x_i, y_i), la vitesse v_i et la direction θ_i. Ainsi, la durée de vie restante d'un lien $L_{(i,j)}$ (*Link Expiration Time* $LET_{L_{(i,j)}}$) en fonction de la portée de la transmission des nœuds est formulée comme suit [SLG00] :

$$LET_{L_{(i,j)}} = \frac{-(ab+cd) + \sqrt{(a^2+b^2)r^2 - (ad-bc)}}{(a^2+c^2)} \tag{2.4}$$

Où $a = v_i \cos\theta_i - v_j \cos\theta_j$; $b = x_i - x_j$; $c = v_i \sin\theta_i - v_j \sin\theta_j$; et $d = y_i - y_j$. Notons que la durée de vie résiduelle $LET_{L_{(i,j)}} = \infty$ si les nœuds i et j se déplacent dans le même sens avec la même vitesse ($v_i = v_j$ et $\theta_i = \theta_j$).

Notons que cette méthode analytique est valable uniquement lorsque la vitesse et la direction des nœuds restent constantes pendant toute la durée de la communication, ce qui n'est pas réaliste dans les réseaux mobiles ad hoc.

Les méthodes de calcul de la fiabilité et de la disponibilité d'un lien sans fil reposant sur des modèles de mobilité *macroscopiques* sont proposées dans [YAA10, XBJ07, SDJ01, MZ99, DFH06, CCGL06].

Un modèle analytique d'estimation de la disponibilité de liens où les nœuds se déplacent de façon aléatoire est proposé dans [SDJ01]. La durée de la communication T qui est décomposée en plusieurs intervalles de temps appelés *époque*. Durant une époque donnée, un nœud se déplace dans une direction fixée avec une vitesse constante. Dans ce modèle de mobilité, les longueurs des époques sont exponentiellement distribuées avec une moyenne de λ^{-1}. Cependant, cet algorithme ne peut pas calculer avec précision la disponibilité du lien, il permet simplement de refléter une tendance générale [SDJ01].

[YAA10] propose une méthode analytique de calcul de fiabilité de liens entre deux nœuds qui se déplacent selon le modèle de mobilité *Random Walk Mobility*. Dans cette approche, la durée de communication T est décomposée en plusieurs époques de longueurs égales Δt. Pour Δt suffisamment petit, le mouvement relatif entre deux nœuds adjacents peut être considéré comme linéaire pendant un intervalle $[t, t+\Delta t]$, c'est-à-dire que la norme de la vitesse relative et sa direction restent constantes. Au début de chaque époque Δt, le nœud choisit au hasard une vitesse uniformément répartie dans $[0, v_{max}]$ et une direction uniformément répartie dans $[0, 2\pi]$, il se déplace ensuite en fonction de ces paramètres durant une durée Δt. La fiabilité $R_{L_{(a,b)}}$ du lien établi entre deux nœuds a et b durant l'intervalle $[t, t+\Delta t]$

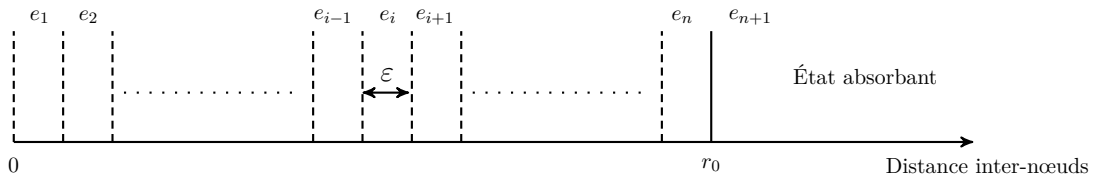


FIGURE 2.1 – Ensemble des états de la chaine de Markov : $E = E_{S_1} \cup E_{S_2}$

est formulée comme la probabilité que le nœud b soit hors de la portée r du nœud a (ie $d_{(a,b)}(t, t+\Delta t) \geq r$) sachant qu'il y était à l'instant t.

$$R_{L_{(a,b)}}(t, t+\Delta t) = 1 - \left[\frac{1}{\pi \times r^2} \times 2v\Delta t \times \left(r - \frac{\pi v \Delta t}{8}\right)\right] \tag{2.5}$$

La fiabilité ainsi obtenue est une valeur moyenne en fonction du modèle de mobilité et de la portée de la transmission r des nœuds. Elle ne tient pas compte de la distance initiale inter-nœud. Cette méthode analytique peut être utilisée pour comparer les protocoles de routage réactifs et proactifs en termes de débit et de messages de contrôle [YAA10] ou évaluer l'efficacité d'une stratégie de recouvrement [BP11a, BP11b]. Cependant, elle n'est pas adaptée pour être introduite dans un protocole de routage car la méthode donne la même valeur de fiabilité pour tous les liens. Ce qui ne permet pas de différentier les liens adjacents d'un nœud durant la découverte de routes. Par conséquent, les routes construites en utilisant comme critère de sélection la fiabilité obtenue par cette méthode analytique sont identiques à celles établies par la métrique classique du *minimum de sauts*. En réalité, la fiabilité d'un lien entre deux nœud dépend de leur distance initiale et décroît lorsque celle-ci augmente. Pour être utilisable dans un protocole de routage, la métrique fiabilité doit donc être formulée en fonction de la distance initiale inter-nœud.

Une approche intéressante pour calculer les métriques (fiabilité et disponibilité) d'un lien en fonction de la distance initiale inter-nœud pour le modèle *Random Walk Mobility (RWM)* est proposée dans [XBJ07]. Elle s'appuie sur une chaine de Markov qui décrit l'évolution de la distance inter-nœud. Cette chaine de Markov est composée de $(n+1)$ états repartis entre deux sous-ensembles :E_{S1} et E_{S2} (figure 2.1). Le premier sous-ensemble E_{S1} contient tous les états possibles entre deux nœuds dont la distance est inférieure à la portée théorique de transmission r_0. La portée r_0 est divisée en n segments de même longueur ϵ : $r_0 = n \times \epsilon$. Le sous-ensemble E_{S1} est donc composée des (n) premiers états : $E_{S1} = \{e_1, e_2, \ldots, e_i, \ldots, e_n\}$. Le second sous-ensemble contient uniquement l'état absorbant $(n+1)$ qui modélise le cas où la distance entre les nœuds est supérieure à r_0. Malheureusement, les expressions de la fiabilité et de la disponibilité contiennent des intégrales qui n'ont pas de solutions approchées.

[ZW07a] propose une adaptation de la méthode analytique précédente pour calculer la fiabilité de lien entre deux nœuds qui se déplacent selon le modèle de mobilité *Semi-Markov Smooth (SMS)*. Contrairement à la méthode précédente, l'adaptation

prend en compte les erreurs du canal de propagation en introduisant la notion de *portée effective de transmission* R_e *(ETR Effective Transmission Range)*. Celle-ci est définie comme la distance maximale pour laquelle la probabilité, qu'un paquet ne soit pas altéré par les erreurs du canal, est supérieure ou égale à 0.99. Mais, cette définition de la portée ne tient pas compte du nombre de retransmissions de niveau MAC. En conséquence, elle est appropriée uniquement lorsqu'il n'y a pas de retransmission. De plus, la notion de portée effective de transmission est inopportune même lorsque sa valeur est exprimée en fonction du nombre de retransmissions m. En effet, dans le modèle d'accès DCF du IEEE 802.11, la valeur de m dépend en général de la taille du paquet à transmettre ($m = 7$ pour les trames courtes et $m = 4$ pour les trames longues avec utilisation de RTS/CTS). Ce qui implique que la portée R_e d'un nœud varie en fonction de la valeur de m (donc de la taille des paquets). Par exemple un nœud n_i peut communiquer en même temps avec les nœuds n_j avec $m = 7$ et n_k avec $m = 4$.

Les méthodes analytiques prédictives présentent l'avantage de ne générer aucun *overhead* supplémentaire lors du calcul de la métrique dans le protocole de routage. C'est pourquoi, nous proposons de les utiliser au niveau du routage. Dans ces méthodes, chaque nœud détermine sa position à l'aide d'un système de localisation dans un repère cartésien. Cependant, les méthodes analytiques présentées dans cette section ne prennent pas en compte ou le font dans un cas particulier les effets des atténuations du signal, les interférences et les collisions comme des causes de rupture lien.

Dans la prochaine section, nous proposons une méthode analytique de calcul de fiabilité qui tient compte des différents facteurs de la communication sans fil. L'originalité de notre approche est de formuler la fiabilité de lien conjointement en fonction de la portée de transmission et des probabilités de pertes au niveau des couches physique et MAC.

2.3 Proposition : Modèle analytique de calcul de la fiabilité d'un lien ad hoc

Nous proposons en premier lieu un cadre général pour le calcul de fiabilité dans un réseau MANET où chaque nœud se déplace aléatoirement et indépendamment des autres. Ensuite, nous nous intéressons aux modèles *Random Walk Mobility (RWM)* et *Random Way Point Mobility (RWP)* en proposant une formulation analytique pour le calcul de la fiabilité pour chacun de ces deux modèles. Nous validons ensuite ces formulations analytiques par simulation.

Dans notre formulation, la fiabilité d'un lien dépend du modèle de mobilité des nœuds et de différents facteurs physiques comme la portée de la transmission des nœuds, la distance initiale inter-nœuds. Contrairement aux méthodes citées précédemment, notre proposition prend en compte l'influence des interférences, des collisions et des atténuations du signal comme des causes possibles d'une rupture de lien.

2.3.1 Modélisation de la fiabilité de lien

La fiabilité d'un lien entre deux nœuds mobiles est définie sur un intervalle de temps $I = [t, t + T]$ dont la longueur T correspond à la durée de la communication souhaitée. Nous décomposons cette longueur T en k époques.

2.3.1.1 Définitions

La fiabilité d'un lien $L_{(a,b)}$ entre les nœuds a et b durant une époque donnée est la probabilité que le nœud b reçoive correctement tout message m envoyé vers lui par le nœud a et inversement. En raison des propriétés des communications sans fil, le nœud b sera capable de recevoir un tel message si et seulement si : 1) il est dans la zone de couverture théorique du nœud a et 2) le message m n'est pas supprimé suite aux collisions successives et 3) le message m n'a pas été supprimé à cause des erreurs successives dues au canal de propagation (atténuations par la distance, présence d'obstacles).

La fiabilité d'un lien $L_{(a,b)}$ existant à l'époque 0 (instant initial t) entre les nœuds a et b, sur l'intervalle I notée $R_{L_{(a,b)}}(k)$ est la probabilité que ce lien continue d'exister jusqu'au moins à l'époque k sans interruption.

Pour déterminer cette fiabilité $R_{L_{(a,b)}}(k)$, nous devons modéliser trois paramètres sur la durée de l'intervalle de communication T qui sont :

- l'évolution de la distance entre les nœuds a et b,

- les suppressions de paquets dues aux collisions inter-paquets,
- les suppressions de paquets dues aux erreurs liées au canal de propagation.

2.3.1.2 Formulation de la fiabilité

L'évolution de la distance inter-nœud dépend du modèle de mobilité utilisé. Dans un modèle de mobilité individuelle, au début de chaque époque, un nœud choisit aléatoirement une vitesse et une direction qu'il conserve durant cette époque. Les modèles de mobilité individuelle sont donc sans mémoire, c'est-à-dire que la position d'un nœud à un instant donné j dépend de sa position à l'instant précédent $(j-1)$, de la vitesse et de la direction choisies à cet instant $(j-1)$. En conséquence, la distance $d_{(a,b)}(j)$ entre les nœuds a et b à une époque j dépend de leur distance $d_{(a,b)}(j-1)$ et des vitesses et directions choisies par les nœuds a et b à la fin de l'époque $(j-1)$. Notons (D_j) la variable aléatoire représentant la distance $d_{(a,b)}(j)$ avec $j \in T = \{0, 1, 2 \cdots k\}$. Le processus stochastique $\{D_j\}_{j \in T}$ décrit donc l'évolution de la distance entre les nœuds a et b.

Nous déduisons alors que le processus $\{D_j\}_{j \in T}$ est un processus de Markov à temps discret en utilisant sa propriété sans mémoire et la discrétisation de la durée de communication T. Pour construire l'ensemble des états E de cette chaine de Markov, nous utilisons l'approche proposée en [XBJ07]. Le portée théorique de transmission r_0 est divisée en n petits segments de longueurs égales. La longueur de chaque segment est égale ε mètres. L'ensemble des états E est composée de $(n+1)$ états repartis en deux sous-ensembles :E_{S1} et E_{S2} (figure 2.1). Le premier sous-ensemble contient les (n) premiers états qui modélisent les états possibles entre deux nœuds dont la distance est inférieure à la portée théorique r_0 : $E_{S1} = \{e_1, e_2, \ldots, e_i, \ldots, e_n\}$. Le second sous-ensemble E_{S2} est composée uniquement de l'état absorbant $(n+1)$ qui représente les distances supérieures à r_0.

La réussite d'une communication entre les nœuds a et b n'est pas garantie même lorsque leur distance est inférieure à la portée théorique de transmission r_0. Dans ce cas, cette réussite dépend du modèle d'accès utilisé au niveau MAC et de l'environnement de la communication. L'échec de la transmission d'un paquet entre deux nœuds situés à portée l'un de l'autre est dû soit à une collision subie par le paquet soit à une atténuation du signal émis qui rend impossible le décodage du paquet.

La fiabilité $R_{L_{(a,b)}}(k)$ d'un lien est modélisée comme le produit entre 1) la probabilité $\bar{p}_{sColl}$ qu'il n'y ait pas eu de suppression de paquets due aux nombres de collisions successives et 2) la somme des probabilités que les nœuds a et b communiquent sans erreurs sachant que leur distance de séparation appartient au sous-ensemble E_{S1} jusqu'à l'époque k. Pour tout état e_i $(0 \leq i \leq n)$, la probabilité que les nœuds a et b communiquent sans erreurs est le produit entre 2.a) la probabilité $rd_i(k)$ que la distance inter-nœuds $d_{(i,j)}$ soit égale à i *mètres* et 2.b) la probabilité $\bar{p}_{sCanal}(i)$ qu'un paquet transmis entre deux nœuds situés à une distance i *mètres* l'un de l'autre ne

soit pas erroné après m retransmissions à cause des atténuations dues au modèle de propagation.

La fiabilité d'un lien est formulée comme suit :

$$R_L(k) = \sum_{i=1}^{n} cr_{iL}\,(k) \tag{2.6}$$

où $cr_{iL}\,(k)$ sont les éléments du vecteur $CR_L(k)$ représentent la fiabilité de communication entre deux nœuds situés à une distance i :

$$cr_{iL}\,(k) = \bar{p}_{sColl} \times rd_i(k) \times (\bar{p}_{sCanal}\,(i))^k \tag{2.7}$$

p_{sColl} probabilité de suppression d'un paquet due aux collisions inter-paquets après m retransmissions ; $\bar{p}_{sColl} = 1 - p_{sColl}$

$rd_i(k)$ probabilité que la distance inter-nœud soit égale à i mètres après k époques

$p_{sCanal}\,(i)$ probabilité de suppression d'un paquet due aux atténuations du canal de propagation après m retransmissions entre deux nœuds séparés par une distance i ; $\bar{p}_{sCanal}(i) = 1 - p_{sCanal}(i)$

Par la suite, nous étudions successivement :
- la probabilité d'évolution de la distance inter-nœuds $RD_i(k)$,
- la probabilité p_{sColl} de suppression de paquets due aux collisions inter-paquets dans IEEE 802.11,
- la probabilité $p_{sCanal}\,(i)$ de suppression due aux atténuations, du modèle de propagation, en fonction de l'environnement de déploiement du réseau.

2.3.2 Probabilité d'évolution de la distance inter-nœuds

Lorsqu'un nœud se déplace selon un modèle de mobilité aléatoire individuelle, il n'est pas possible de prédire avec exactitude sa future position puisqu'on ne connait pas à priori sa vitesse et sa direction. Il est cependant possible d'associer une probabilité à chaque position possible si l'on connait les intervalles de sélection de la vitesse et de l'angle du nœud. Le même concept est valable pour modéliser l'évolution de la distance inter-nœuds. Pour cela, nous utilisons un vecteur $RD(k)$ de taille $(n+1)$ dont chaque élément $rd_i(k)$ représente la probabilité d'être dans l'état e_i après k époques. Il est formulé comme le produit entre le vecteur des probabilités des distances initiales $P(0)$ et la matrice P_R des probabilités de transitions après k époques.

– *Random Walk :* Dans ce modèle de mobilité, les nœuds se déplacent continuellement sans aucune pause. Nous formulons le vecteur RD(k) comme suit :

$$RD(k) = P(0)P_R^k \tag{2.8}$$

– *Random Way Point :* Le modèle *Random Way Point* est une extension du modèle *Random Walk* qui introduit un temps pause T_{pause} entre deux déplacements consécutifs d'un nœud. Supposons que les temps de pause des nœuds sont égaux. Dans ce cas, la distance inter-nœuds évolue uniquement durant les temps de déplacement ($T_{Depl} = 1sec$ dans notre modélisation) et reste inchangé pendant les temps de pause. Le vecteur de probabilité de la distance inter-nœuds $RD(k)$ est :

$$RD(k) = P(0)P_R^{k_{WP}} \tag{2.9}$$

où k_{WP} représente la durée cumulée des temps de déplacements des nœuds entre 0 et k.

$$k_{WP} = \left\lceil \frac{k}{T_{Depl} + T_{Pause}} \right\rceil = \left\lceil \frac{k}{1 + T_{Pause}} \right\rceil \tag{2.10}$$

2.3.2.1 Vecteur de la probabilité initiale des distances inter-nœuds

Les éléments du $P(0)$ de taille $(n+1)$ représentent les probabilités de distribution de la distance inter-nœuds à l'époque 0.

$$P(0) = [p_1(0), p_2(0), p_3(0), \cdots, p_n(0), p_{n+1}(0)] \tag{2.11}$$

Selon la définition de la fiabilité, le lien doit exister à l'époque 0 : $p_{n+1}(0) = 0$.

La valeur des autres éléments du vecteur $P(0)$ dépend de l'objectif de la modélisation [XBJ07] :

– Si l'objectif est de calculer la fiabilité d'un lien en particulier :

$$P(0) = [p_1(0) = 0, \cdots, p_i(0) = 1, \cdots, p_n(0) = 0, p_{n+1}(0) = 0] \tag{2.12}$$

où i est la distance initiale entre les nœuds (en mètres). Ce vecteur de probabilité initiale est utilisé lorsque la métrique fiabilité doit être introduite dans un protocole de routage. C'est-à-dire qu'on connait déjà la distance entre les deux nœuds (voir section 3.2 pour l'introduction de la fiabilité comme métrique dans un protocole de routage).

– Si l'objectif est de calculer la fiabilité moyenne des liens pour un modèle de mobilité comme dans [YAA10] (voir section 2.2.2), la valeur des éléments dépend du modèle de la distribution initiale des nœuds dans le modèle de la zone. En supposant une distribution aléatoire uniformément répartie, tous les éléments sont équiprobables.

$$P(0) = \left[p_1(0) = \tfrac{1}{n}, p_2(0) = \tfrac{1}{n}, \cdots, p_n(0) = \tfrac{1}{n}, p_{n+1}(0) = 0\right] \tag{2.13}$$

2.3.2.2 Matrice de transition de la distance inter-nœuds

La matrice de transition P est une matrice carrée de taille $(n+1) \times (n+1)$ où chaque élément $p_{i,j}$ représente la probabilité de passer de l'état e_i ($d_{(a,b)} = i$ mètres) à l'état e_j ($d_{(a,b)} = j$ mètres) après une époque.

$$P_R = \begin{bmatrix} p_{1,1} & \cdots & p_{1,n} & p_{1,n+1} \\ \cdots & \ddots & \cdots & \cdots \\ p_{n,1} & \cdots & p_{n,n} & p_{n,n+1} \\ \mathbf{0} & \mathbf{\cdots} & \mathbf{0} & \mathbf{1} \end{bmatrix} \tag{2.14}$$

où $\forall i, j,\ p_{i,j} \geq 0$ et $\sum_{j=1}^{n+1} p_{i,j} = 1$.

En supposant que la distance entre deux nœuds à l'époque m est égale à i mètres ($d_m \in e_i$), leur distance d_{m+1} à l'époque suivante ($m+1$) est comprise dans :

$$[max\,(0, d_m - 2 \times v_{max})\,, d_m + 2 \times v_{max}] \tag{2.15}$$

où v_{max} est la vitesse maximale de déplacement des nœuds. Dans la pratique, la valeur de la vitesse maximale de déplacement d'un nœud dépend de l'environnement de déploiement du réseau et l'application ciblée (application civile utilisant un réseau de piétons : marché, super-marché ou route dégagée ; application militaire utilisant un réseau ad hoc de robots : terrain plat, boueux, caillouteux).

La distance entre deux nœuds peut passer en une époque de l'état e_i à un état e_j tel que :

$$j \in [max\,(1, i-\gamma)\,, i+\gamma]\,, \quad \gamma = \left\lceil \frac{2 \times v_{max}}{\epsilon} \right\rceil \tag{2.16}$$

La probabilité de transition entre les états e_i et e_j est :

$$\begin{aligned} p_{i,j} &= Pr(e_i \rightarrow e_j) = Pr\,(d_{m+1} \in e_j / d_m \in e_i) \\ &= \int_{(j-1)\epsilon}^{j\epsilon} \int_{(i-1)\epsilon}^{i\epsilon} f_{D_{m+1}/D_m}\,(d_{m+1}/d_m) \cdot f_{D_m}\,(d_m)\, dd_m dd_{m+1} \end{aligned} \tag{2.17}$$

où $f_{D_{m+1}/D_m}\,(d_{m+1}/d_m)$ est la densité de probabilité conditionnelle de la variable aléatoire D_{m+1} par rapport à D_m. Elle dépend du modèle de mobilité des nœuds.

Si ϵ [1] est suffisamment petit, la densité de probabilité conditionnelle du passage de la distance inter-nœuds d'un état e_i à un état e_j est approximativement égale à la valeur de la fonction en remplaçant chaque état par le centre du segment auquel il appartient [XBJ07] :

$$f_{D_{m+1}/D_m}\,(d_{m+1} \in e_j / d_m \in e_i) \approx f_{D_{m+1}/D_m}\left(\left(j - \frac{1}{2}\right) \times \epsilon / \left(i - \frac{1}{2}\right) \times \epsilon\right) \tag{2.18}$$

1. Par la suite, nous utilisons $\epsilon = 1$ mètre

De plus, en supposant toujours que ϵ est suffisamment petit, la densité de probabilité $f_{D_m}(d_m)$ peut être approximée par une fonction uniformément repartie dans le $i^{ème}$ segment (indépendamment de l'époque m)[XBJ07].

$$f_{D_m}(d_m) = \frac{1}{\epsilon} \tag{2.19}$$

A partir des formules 2.18 et 2.19, la formule 2.17 peut s'écrire comme suit :

$$p_{i,j} \approx \epsilon \times f_{D_{m+1}/D_m}\left(\left(j-\frac{1}{2}\right)\times\epsilon / \left(i-\frac{1}{2}\right)\times\epsilon\right) \tag{2.20}$$

Nous nous intéressons maintenant à déterminer la densité de probabilité conditionnelle du modèle de mobilité *Random Walk Mobility*.

2.3.2.2.1 Densité de probabilité conditionnelle : *Random Walk Mobility*

Nous poursuivons le travail présent en [XBJ07] en résolvant l'équation 2.17. Pour cela, nous utilisons l'expression de la densité de probabilité conditionnelle f_{D_{m+1}/D_m} en fonction de la distribution de la vitesse relative $f_{V_{r_{m+1}}}(v_{r_{m+1}})$ proposée pour le modèle de mobilité *Semi-Markov Smooth (SMS)* [ZW07a] :

$$f_{D_{m+1}/D_m}(d_{m+1}/d_m) = \int f_{D_{m+1}/D_m, V_{r_{m+1}}}\left(d_{m+1}/d_m, v_{r_{m+1}}\right)\cdot f_{V_{r_{m+1}}}\left(v_{r_{m+1}}\right) dv_{r_{m+1}} \tag{2.21}$$

Dans le modèle *Random Walk Mobility*, la vitesse relative v_{r_m} à chaque époque m entre deux nœuds est comprise entre :

- 0 : les nœuds se déplacent dans le même direction avec la même vitesse
- $2 \times v_{max}$: les nœuds se déplacent dans des directions opposées avec une vitesse $v = v_{max}$

Ces deux valeurs correspondent aux bornes de notre intégrale. Nous réécrivons l'équation précédente comme suit :

$$\begin{aligned} f_{D_{m+1}/D_m}(d_{m+1}/d_m) &= \int_0^{2\cdot v_{max}} f_{D_{m+1}/D_m, V_{r_{m+1}}}\left(d_{m+1}/d_m, v_{r_{m+1}}\right)\cdot f_{V_{r_{m+1}}}\left(v_{r_{m+1}}\right) dv_{r_{m+1}} \\ &= \int_0^{2\cdot v_{max}} f_{\Theta_{r_{m+1}}}(\theta_{r_{m+1}})\cdot\left|\frac{\partial\theta_{r_{m+1}}}{\partial d_{m+1}}\right|\cdot f_{V_{r_{m+1}}}\left(v_{r_{m+1}}\right) dv_{r_{m+1}} \\ &= \int_0^{2\cdot v_{max}} \frac{\frac{1}{\pi}\cdot d_{m+1}\cdot f_{V_{r_{m+1}}}\left(v_{r_{m+1}}\right) dv_{r_{m+1}}}{\left[4d_{m+1}^2 d_m^2 - \left[v_{r_{m+1}}^2 - (d_{m+1}^2 + d_m^2)\right]^2\right]^{\frac{1}{2}}} \end{aligned} \tag{2.22}$$

avec $v_{r_{m+1}}$ et $\theta_{r_{m+1}}$ deux variables aléatoires indépendantes représentant respectivement la vitesse relative et l'angle relatif entre les deux nœuds à l'époque $m+1$.

Démonstration :
Le vecteur distance inter-nœuds à l'époque *m+1* est $\overrightarrow{d_{m+1}} = \overrightarrow{d_m} + \overrightarrow{v_{r_{m+1}}}$. Nous déduisons alors sa norme en appliquant le théorème d'Al-Kashi (théorème de Pythagore généralisé) :

$$d_{m+1} = \sqrt{d_m^2 + v_{r_{m+1}}^2 - 2 \cdot d_m \cdot v_{r_{m+1}} \cdot \cos\theta_{r_{m+1}}} \tag{2.23}$$

En développant cette équation, le *cos* de l'angle relatif à l'époque $m+1$ est :

$$\cos\theta_{r_{m+1}} = \frac{d_m^2 + v_{r_{m+1}}^2 - d_{m+1}^2}{2 \cdot d_m \cdot v_{r_{m+1}}} \tag{2.24}$$

Pour déduire l'expression de l'angle $\theta_{r_{m+1}}$ à partir de l'équation précédente, nous devons passer par la fonction arccos dont le domaine de valeur est défini sur $[0, \pi]$ or l'angle $\theta_{r_{m+1}} \in [0, 2\pi]$. Nous utilisons alors un angle φ_{m+1} défini sur $[0, \pi)$ à partir de l'angle $\theta_{r_{m+1}}$ tel que :

$$\varphi_{m+1} = \begin{cases} \theta_{r_{m+1}} & \text{si} \quad 0 \leq \theta_{r_{m+1}} \leq \pi \\ -\theta_{r_{m+1}} = 2 \cdot \pi - \theta_{r_{m+1}} & \text{si} \quad \pi \leq \theta_{r_{m+1}} < 2 \cdot \pi \end{cases} \tag{2.25}$$

En utilisant la parité de la fonction cosinus ($\forall\, \alpha\ \cos(-\alpha) = \cos(\alpha)$), nous obtenons :

$$cos\varphi_{m+1} \quad = \quad \cos\theta_{r_{m+1}} = \frac{d_m^2 + v_{r_{m+1}}^2 - d_{m+1}^2}{2 \cdot d_m \cdot v_{r_{m+1}}} \tag{2.26}$$

L'angle φ_{m+1} est obtenu en appliquant une bijection réciproque à l'équation précédente :

$$\varphi_{m+1} \quad = \quad \arccos\left[\frac{d_m^2 + v_{r_{m+1}}^2 - d_{m+1}^2}{2 \cdot d_m \cdot v_{r_{m+1}}}\right] \tag{2.27}$$

Le changement de variable dans la transformation de Jacobien entre les variables aléatoires D_{m+1} et $\Theta_{r_{m+1}}$ donne :

$$f_{D_{m+1}}(d_{m+1}) = f_{\Theta_{r_{m+1}}}(\theta_{r_{m+1}}) \cdot \left|\frac{\partial\theta_{r_{m+1}}}{\partial d_{m+1}}\right| \tag{2.28}$$

La densité de probabilité de la variable $\Theta_{r_{m+1}}$ est uniformément répartie sur $[0, 2 \cdot \pi]$ d'où $f_{\Theta_{r_{m+1}}}(\theta_{r_{m+1}}) = \frac{1}{2 \cdot \pi}$. En remplaçant $f_{\Theta_{r_{m+1}}}(\theta_{r_{m+1}})$ par sa valeur et $\theta_{r_{m+1}}$ par φ_{m+1} dans l'équation précédente, nous obtenons :

$$\begin{aligned} f_{D_{m+1}/D_m, V_{r_{m+1}}}\left(d_{m+1}/d_m, v_{r_{m+1}}\right) &= \frac{1}{2 \cdot \pi} \cdot \left| \frac{\partial \varphi_{m+1}}{\partial d_{m+1}} \right| \\ &= \frac{1}{2 \cdot \pi} \cdot \left| \frac{\partial \arccos\left[\frac{d_m^2 + v_{r_{m+1}}^2 - v_{r_{m+1}}^2}{2 \cdot d_m \cdot v_{r_{m+1}}} \right]}{\partial d_{m+1}} \right| \end{aligned} \tag{2.29}$$

Nous dérivons ensuite la fonction de l'angle φ_{m+1} par rapport à d_{m+1}

$$\begin{aligned} f_{D_{m+1}/D_m, V_{r_{m+1}}}\left(d_{m+1}/d_m, v_{r_{m+1}}\right) &= \frac{1}{2 \cdot \pi} \cdot \frac{2 \cdot d_{m+1}}{\left[4 d_{m+1}^2 d_m^2 - \left[v_{r_{m+1}}^2 - \left(d_{m+1}^2 + d_m^2\right)\right]^2\right]^{\frac{1}{2}}} \\ &= \frac{\frac{1}{\pi} \cdot d_{m+1}}{\left[4 d_{m+1}^2 d_m^2 - \left[v_{r_{m+1}}^2 - \left(d_{m+1}^2 + d_m^2\right)\right]^2\right]^{\frac{1}{2}}} \end{aligned} \tag{2.30}$$

Pour calculer la densité de probabilité conditionnelle f_{D_{m+1}/D_m}, nous devons maintenant déterminer la densité de probabilité de la vitesse relative $f_{V_r}(v_r)$.

2.3.2.2.2 Densité de probabilité de la vitesse relative $f_{V_r}(v_r)$: La vitesse relative $v_{r_{m+1}}$ à l'époque $m+1$ entre deux nœuds a et b est : $\overrightarrow{v_{r_{m+1}}} = \overrightarrow{d_{m+1}} - \overrightarrow{d_m}$. Lorsque les nœuds sont dans un repère cartésien, nous pouvons écrire sa norme comme suit :

$$v_{r_{m+1}} = \sqrt{\left(X_{m+1} - X_m\right)^2 + \left(Y_{m+1} - Y_m\right)^2} \tag{2.31}$$

où X_{m+1} et Y_{m+1} sont des variables aléatoires qui représentent respectivement les projections de D_{m+1} sur l'axe des abscisses et des ordonnées. Pour m suffisamment grand ($m >> 1$), les variables X_m et Y_m peuvent être approximées par une distribution aléatoire gaussienne. Les variables aléatoires $X_{m+1} - X_m$ et $Y_{m+1} - Y_m$ suivent donc une loi normale gaussienne identique de moyenne nulle [ZW07b]. Dans ce cas, la densité de probabilité de la vitesse relative représentée par celle de la variable aléatoire $Z = \sqrt{\left(X_{m+1} - X_m\right)^2 + \left(Y_{m+1} - Y_m\right)^2}$ peut être approximée par une distribution de la loi de *Rayleigh* :

$$f_Z(z) = \frac{z}{a} \cdot e^{\frac{-z^2}{2a^2}} \quad \text{et} \quad E\{z\} = a\sqrt{\frac{\pi}{2}} \tag{2.32}$$

La distribution de la vitesse relative du modèle de mobilité *Random Walk* est alors :

$$f_{V_r}(v_r) = \frac{v_r}{\left(E\{v_r\}\sqrt{\frac{2}{\pi}}\right)^2} \cdot e^{\frac{-v_r^2}{2\left(E\{v_r\}\sqrt{\frac{2}{\pi}}\right)^2}} = \frac{\pi \cdot v_r}{2 \cdot E\{v_r\}^2} \cdot e^{\frac{-\pi \cdot v_r^2}{4 \cdot E\{v_r\}^2}} \tag{2.33}$$

Nous réécrivons donc la formule 2.22 de la densité de probabilité conditionnelle :

$$f_{D_{m+1}/D_m}\left(d_{m+1}/d_m\right) = \int_0^{2 \cdot v_{max}} \frac{\frac{d_{m+1} \cdot v_{r_{m+1}}}{2 \cdot E\{v_r\}^2} \cdot e^{\frac{-\pi \cdot v_{r_{m+1}}^2}{4 \cdot E\{v_r\}^2}}}{\left[4d_{m+1}^2 d_m^2 - \left[v_{r_{m+1}}^2 - \left(d_{m+1}^2 + d_m^2\right)\right]^2\right]^{\frac{1}{2}}} dv_{r_{m+1}}$$

$$\leq \sqrt{\frac{d_{m+1}}{d_m}} \cdot \frac{1}{E\{v_r\} \cdot 2\sqrt{2 \cdot \pi}} \left[1 - e^{\frac{-2\pi \cdot v_{max}^2}{E\{v_r\}^2}}\right]^{\frac{1}{2}} \left[\ln\left(\frac{\left|4 \cdot v_{max}^2 - (d_{m+1} - d_m)^2\right| \cdot (d_{m+1} + d_m)^2}{\left|(d_{m+1} + d_m)^2 - 4 \cdot v_{max}^2\right| \cdot (d_{m+1} - d_m)^2}\right)\right]^{\frac{1}{2}} \tag{2.34}$$

La démonstration de cette formule se trouve en Annexe A.

Nous déduisons enfin la probabilité de transition d'un état e_i vers un état e_j (avec j appartenant l'intervalle défini par l'équation 2.16) à partir des formules 2.20 et 2.34 :

$$\begin{aligned} \tilde{p_{i,j}} &\approx \epsilon \times f_{D_{m+1}/D_m}\left(\left(j - \frac{1}{2}\right) \times \epsilon / \left(i - \frac{1}{2}\right) \times \epsilon\right) \\ &\approx \epsilon \times \sqrt{\frac{2j-1}{2i-1}} \cdot \frac{1}{E\{v_r\} \cdot 2\sqrt{2 \cdot \pi}} \left[1 - e^{\frac{-2\pi \cdot v_{max}^2}{E\{v_r\}^2}}\right]^{\frac{1}{2}} \cdot \\ &\quad \left[\ln\left(\frac{\left|4 \cdot v_{max}^2 - \epsilon^2 (j-i)^2\right| \cdot (j+i-1)^2}{\left|\epsilon^2 (j+i-1)^2 - 4 \cdot v_{max}^2\right| \cdot (j-i)^2}\right)\right]^{\frac{1}{2}} \end{aligned} \tag{2.35}$$

Chaque valeur $\tilde{p_{i,j}}$ [1] obtenue à partir de l'équation précédente sera ensuite normalisée par rapport à la somme de la ligne i de la matrice P_k. Plus précisément :

$$p_{i,j} = \frac{\tilde{p_{i,j}}}{\sum_{j=1}^{n+1} \tilde{p_{i,j}}} \tag{2.36}$$

Cette équation nous permet donc d'obtenir les éléments de la matrice de transition de la distance inter-nœuds P_R.

1. Dans le cas où l'équation 2.35 n'est pas définie, $\tilde{p_{i,j}} = 0 : j = i$ ou $(j + i - 1) \cdot \epsilon = 2 \cdot v_{max}$ ou le numérateur de la fonction ln est inférieure à son dénominateur.

2.3.3 Probabilité de suppression de paquets due à des collisions inter-paquets

La méthode d'accès utilisée dans les MANETs est généralement le DCF (*Distributed Coordination Function*) qui fait partie de la famille des protocoles de type CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*). C'est une méthode d'accès probabiliste qui permet de garantir aux nœuds une égalité des chances d'accès au support de transmission. Un nœud qui souhaite émettre une trame doit d'abord écouter le support de transmission pour vérifier son activité. Il commence à émettre s'il ne détecte aucune activité sur le médium durant une durée DIFS (*Distributed Interframe Space*). Si le canal est occupé au début de l'écoute ou le devient durant la durée du DIFS, le nœud tire un nombre aléatoire appelé délai de *backoff* et attend que le médium se libère. Le délai de *backoff* est tiré dans un intervalle appelé fenêtre de contention (CW : *Contention Window*). Il correspond à un nombre entier de slots, le slot étant une unité de temps de 802.11. Après la libération du canal, le nœud attend encore une durée DIFS avant de décrémenter son délai de *backoff* slot par slot. Durant tout ce processus, le support de transmission doit rester libre. Dans le cas où une activité est détectée sur le canal, l'opération est interrompue et reprendra lorsque le médium sera de nouveau libre, c'est-à-dire que le nœud attend encore durant une durée DIFS avant de commencer la décrémentation de son timer de *backoff* dont la valeur correspond au nombre restant de slots de *backoff* lors de interruption. Le nœud peut commencer la transmission de sa trame, lorsque la valeur de son *backoff* atteint la valeur nulle. Un mécanisme d'acquittement positif est utilisé pour vérifier la bonne réception de chaque paquet. Le nœud récepteur répond par un acquittement *Ack*, après une durée d'attente SIFS (*Short Inter Frame Space*) inférieure à DIFS, à chaque paquet correctement reçu. L'émetteur suppose que le paquet émis est perdu s'il ne reçoit aucun acquittement *Ack* avant l'expiration de son timer *Ack_Timeout*. Il va alors tenter de retransmettre le paquet perdu suivant l'algorithme BEB (*Binary Exponential Backoff*). Il commence par incrémenter le nombre de tentatives infructueuses i et choisit la nouvelle valeur du délai de *backoff* entre $[0, CW_i]$ où $CW_i = 2^i \cdot CW_{min}$ est la nouvelle valeur de la fenêtre de contention.

Le nœud continue ce processus jusqu'à ce qu'il reçoive un acquittement ou que le nombre de tentatives infructueuses i atteigne la valeur maximale m fixée par le standard ($m = 6$ dans le 802.11 pour les trames courtes).

La probabilité de suppression d'un paquet est définie comme la probabilité que le nombre de retransmissions de ce paquet atteigne la valeur maximale fixée m :

$$p_{sColl} = p_c^{m+1} \tag{2.37}$$

La probabilité qu'un paquet transmis par un nœud subisse une collision est la probabilité qu'au moins un de ses voisins transmette dans le même *slot*. Elle est formulée dans [CBV03] en fonction de τ, la probabilité qu'un nœud transmette un

paquet dans un *slot* donné et du nombre de voisins du nœud émetteur N_{voisin}.

$$p_c = 1 - (1 - \tau)^{N_{voisin}} \tag{2.38}$$

$$\tau = \frac{2}{1 + CW_{min} + p_c \cdot CW_{min} \sum_{i=0}^{m-1} (2p_c)^i} \tag{2.39}$$

Les équations 2.38 et 2.39 représentent un système d'équation non-linéaire avec deux inconnues p_c et τ qui peut être résolu par les techniques numériques. L'unicité de la solution de ce système d'équation est montrée dans [Cha04]. En effet, la fonction $\tau\,(p_c)^* = 1 - (1 - p_c)^{\frac{1}{N_{voisin}}}$ obtenue en inversant l'équation 2.38 est une fonction continue monotone et strictement croissante pour $p_c \in [0, 1]$ avec $\tau\,(0)^* = 0$ et $\tau\,(1)^* = 1$. La fonction $\tau(p_c)$ de l'équation 2.39 est une fonction monotone décroissante $\tau\,(0) = 2/\,(1 + CW_{min})$ et $\tau\,(1) = 2/\,(1 + 2^m \cdot CW_{min})$. L'unicité de la solution est ainsi montrée en observant que $\tau\,(0) > \tau\,(0)^*$ et $\tau\,(1) < \tau\,(1)^*$.

La valeur de la probabilité de collision est donc déterminée en fonction des paramètres m, CW_{min} et N_{voisin}. Le nombre de voisins N_{voisin} d'un nœud dans un MANET n'est pas fixe, il évolue en cours de déploiement. Dans [YWC07], le nombre moyen de voisins $E\{N_{voisin}\}$ d'un nœud est formulé en fonction du nombre de nœuds n aléatoirement déployés et de la taille de la zone de déploiement $|A|$ (en m^2) :

$$E\{N_{voisin}\} = \frac{n \times (\pi - \frac{3\sqrt{3}}{4}) \times r^2}{|A|} \tag{2.40}$$

La figure 2.2 montre l'évolution de la probabilité de suppression d'un paquet après m retransmissions infructueuses en fonction du nombre de nœuds voisins. Nous observons que l'augmentation du nombre de retransmissions pour un nombre de voisins fixé permet de réduire la probabilité de suppression.

2.3.4 Probabilité de suppression d'un paquet due aux atténuations du canal

Dans un réseau sans fil, le signal reçu par un nœud peut être perturbé par trois types d'atténuations : l'affaiblissement par la distance (*path loss*), l'effet de masque (*shadowing*) et l'affaiblissement par multi-trajet (*multipath fading*).

Le *path loss* est un phénomène déterministe qui modélise la diminution de la puissance du signal due à l'éloignement entre les nœuds. L'atténuation du signal reçu peut être estimée par un modèle empirique d'exposant α. Le deuxième type d'atténuation appelé *shadowing* est un phénomène aléatoire dû aux atténuations

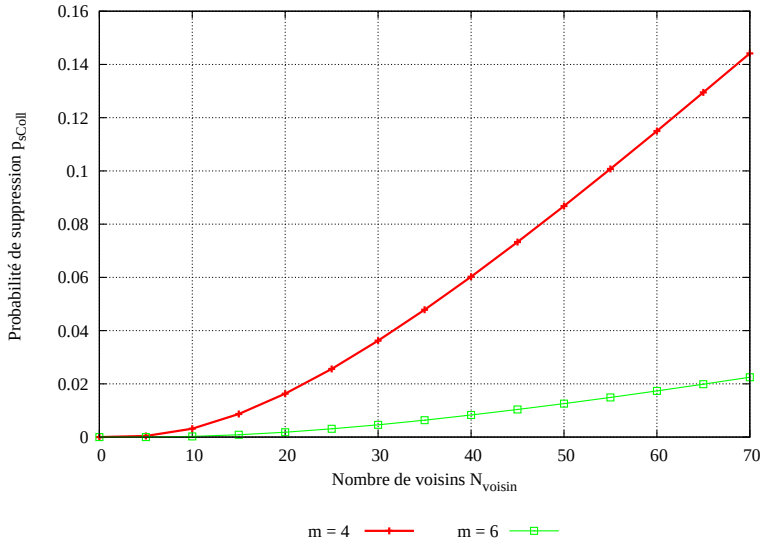


FIGURE 2.2 – Probabilité de suppression p_{sColl} vs Nombre de voisins N_{voisin}

successives. Il ajoute au modèle du *path loss* les contraintes liées aux obstacles, c'est-à-dire un affaiblissement probabiliste en fonction du milieu de propagation. Cet affaiblissement est modélisé par une variable aléatoire X_{σ_s} qui suit une loi gaussienne de moyenne nulle et variance σ_s. Enfin, le *multipath fading* modélise les variations rapides de l'amplitude du signal. Dans ce cas, l'affaiblissement est lié au fait que l'onde émise peut suivre plusieurs chemins avant de parvenir au nœud destinataire qui reçoit alors plusieurs copies. La variable aléatoire χ^2 qui modélise le multi-trajet suit une loi de *Rayleigh* avec $E\{\chi^2\} = 2\sigma_r^2$ où σ_r est le paramètre ajustable du modèle. Pour évaluer l'effet du *multipath fading* sur le signal, on utilise généralement un canal de Rice de facteur K (compris entre 6dB et 30dB)[Sch05]. Dans ce cas, le paramètre σ_r^2 est égal à $\frac{1}{2(K+1)}$.

La probabilité $\bar{p_e}(i)$ qu'un paquet émis entre deux nœuds situés à distance i ne soit pas perdu à cause des atténuations liées au canal de propagation est [Sch05] :

$$\bar{p_e}(i) = \frac{1}{2} - \frac{1}{2} erf\left(\frac{10\alpha \log_{10}(i/r_0) + 10\log_{10}(\chi^2)}{\sigma_s\sqrt{2}}\right) \tag{2.41}$$

$erf(.)$- fonction d'erreur de Gauss ; $erf(x) = \int_0^x \frac{2}{\sqrt{\pi}} e^{x^2} dx$
r_0- rayon théorique
α- exposant du *path loss*
σ_s- variance du *shadowing* modèle
χ^2- modélise le *multipath fading*

La figure 2.3 montre la probabilité de réception de paquets en fonction de la distance entre les nœuds des trois modèles d'atténuations du signal. Dans le modèle du

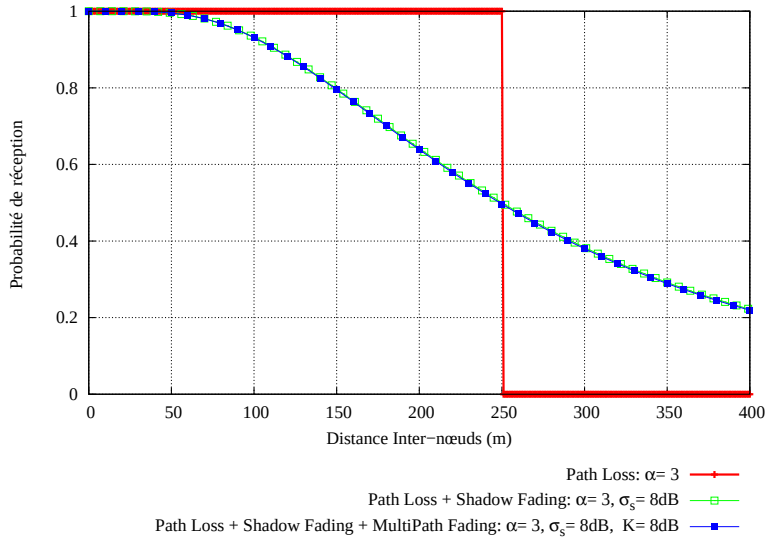


FIGURE 2.3 – Comparaison des probabilités de réception en fonction du modèle d'atténuation

path loss, deux nœuds sont toujours connectés si leur distance est inférieure au rayon théorique $r_0 = 250$ m. La probabilité décroit de 1 jusqu'à 0.5 lorsque la distance atteint r_0 lorsque les atténuations des modèles *path loss* et *shadow fading* sont ajoutées (superposées) ($\alpha = 3$, $\sigma_s = 8dB$ et $\sigma_r = 1$). Dans le cas où nous superposons les trois modèles d'atténuations en choisissant la valeur adéquate du facteur $K = 8dB$, la probabilité décroit légèrement. Elle est égale à 0.48 lorsque la distance inter-nœuds est égale au rayon théorique. Nous observons que cette probabilité n'est pas très différente de celle de la superposition des modèles *path loss* et *shadow fading*.

L'équation 2.41 modélise une perte de paquets due aux atténuations du signal pour une seule émission. Or, nous avons vu dans la section précédente qu'en cas de non d'acquittement dans le mode DCF, le nœud émetteur retransmet le paquet. Dans l'équation 2.42, nous déduisons la probabilité de suppression d'un paquet due aux atténuations du canal de propagation après m retransmissions entre deux nœuds séparés par une distance i :

$$p_{sCanal}(i) = 1 - [1 - \bar{p_e}(i)]^{m+1} \tag{2.42}$$

2.3.5 Validation du modèle analytique

Nous nous intéressons maintenant à la validation du modèle analytique de calcul de fiabilité proposé en comparant les valeurs prédites par celle-ci aux fiabilités obtenues par simulation avec le simulateur OMNeT++ [omn]. C'est un simulateur à évènements discrets orienté objet, basé sur le langage C++. Il s'appuie sur l'ex-

périence des simulateurs ns [ns] et GloMoSim [glo], pour simuler les réseaux de communication, les systèmes multi processeurs, et autres systèmes distribués. Nous utilisons la librairie inet qui permet de simuler le comportement des nœuds dans un réseau mobile ad hoc.

Différents scénarios de validation sont étudiés en fonction de l'environnement de déploiement du réseau (modèle de propagation du canal et nombre de voisins des nœuds). Nous supposons que les nœuds se déplacent selon le modèle *Random Walk* dans une zone de simulation ouverte et disposent d'une antenne omni-directionnelle de portée de transmission théorique $r_0 = 250$ mètres. Nous validons également la méthode analytique pour le modèle de mobilité *Random Way Point* (les résultats sont présentés en Annexe B). Nous utilisons la valeur par défaut définie dans le modèle d'accès DCF du nombre de retransmissions $m = 6$.

La fiabilité du lien par simulation à un instant t est une moyenne sur 10.000 expériences. Tout au long de la durée de la simulation, les nœuds s'échangent à intervalles réguliers d'une seconde des paquets de données. Pour chaque expérience, la fiabilité à un instant t est égale à 1 si elle vaut 1 à l'instant précédent $(t-1)$ et le paquet envoyé à t est correctement reçu sinon elle est égale à 0.

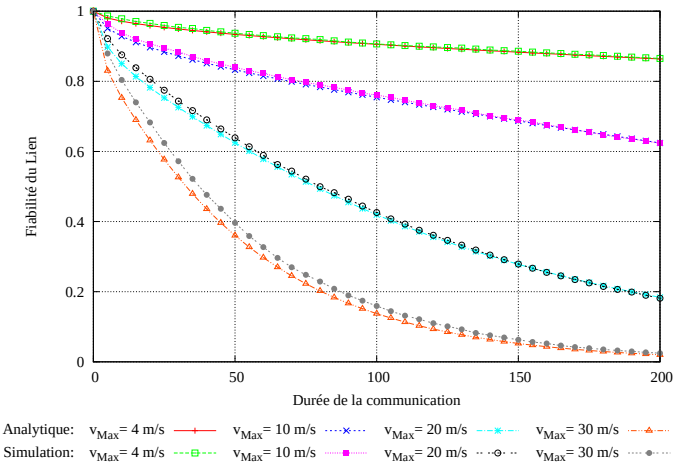
2.3.5.1 Deux nœuds

Dans un premier temps, nous validons notre modèle en l'absence d'interférence et de collision. Nous plaçons donc seulement deux nœuds dans la zone de simulation. La fiabilité du lien dépend alors de la distance initiale inter-nœuds, la vitesse maximale et du modèle de propagation.

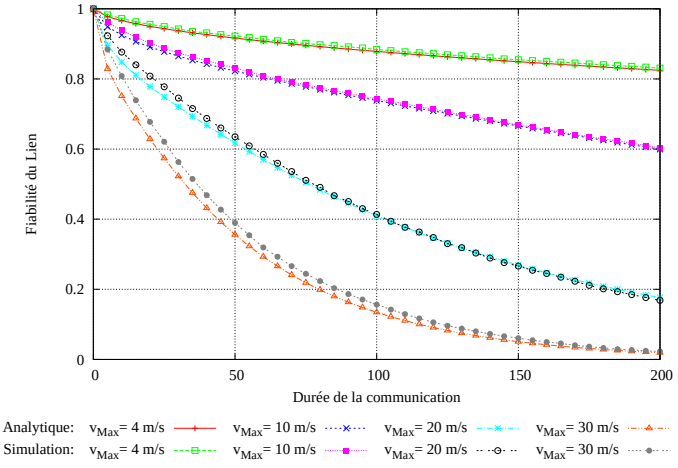
Les figures 2.4 et 2.5 présentent la fiabilité en fonction de la durée de communication pour différentes valeurs de la vitesse maximale des nœuds. Sur ces figures, des résultats attendus sont observables : la fiabilité diminue lorsque la durée et/ou la vitesse maximale augmente(nt). Notons que lorsque la vitesse $v_{max} = 4m/s$ (figure 2.5), le temps de communication de 200 s n'est pas suffisant pour voir la diminution de fiabilité ; celle-ci intervient vers 300 s.

Par ailleurs, nous constatons que l'approximation du modèle se dégrade légèrement lorsque la vitesse maximale augmente ($v_{max} > 30m/s$). Ceci provient du fait qu'il est difficile de prédire la position d'un nœud qui se déplace très rapidement en changeant à chaque instant $t = 1s$ de direction et de sens. Toutefois, notre modèle analytique reste toujours relativement correct.

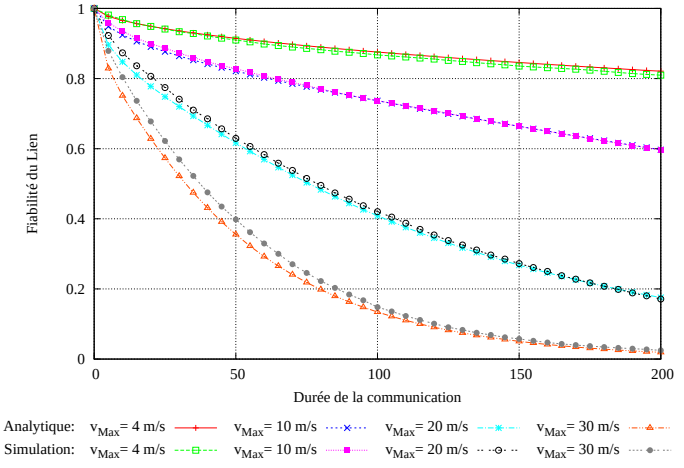
La figure 2.4 différencie la fiabilité moyenne pour les modèles de propagation *path loss (PL)*, *path loss + shadowing (PL + SM)* et *path loss + shadowing + multipath fading (PL + SM + MF)*. Les nœuds sont placés à une distance aléatoire uniformément répartie entre 0 et la portée théorique de transmission r_0 ; le vecteur P_0 de la probabilité initiale des distances inter-nœuds est déterminé par l'équation



(a) PL : $\alpha = 3$



(b) PL + SM :$\alpha = 3$, σ_s=8 dB



(c) PL + SM + MF : $\alpha = 3$, σ_s=8 dB et K = 8dB

FIGURE 2.4 – Fiabilité en fonction du temps : Distance Initiale équiprobable

2.13. Notre modèle analytique reste valide quel que soit le modèle de propagation utilisé : *path loss*, *path loss + shadowing* ou *path loss + shadowing + multipath fading*. Notons que lorsque les nœuds sont placés dans un environnement de *shadowing*, ceci entraîne une diminution de la fiabilité du lien par rapport à celle obtenue dans le modèle du *path loss*. La superposition du modèle d'atténuation *multipath fading* sur deux autres modèles ne change presque pas la fiabilité du lien.

Par la suite, nous présenterons uniquement les résultats dans un environnement d'atténuation *shadowing fading* qui est le modèle de propagation, le plus utilisé et proche de la réalité.

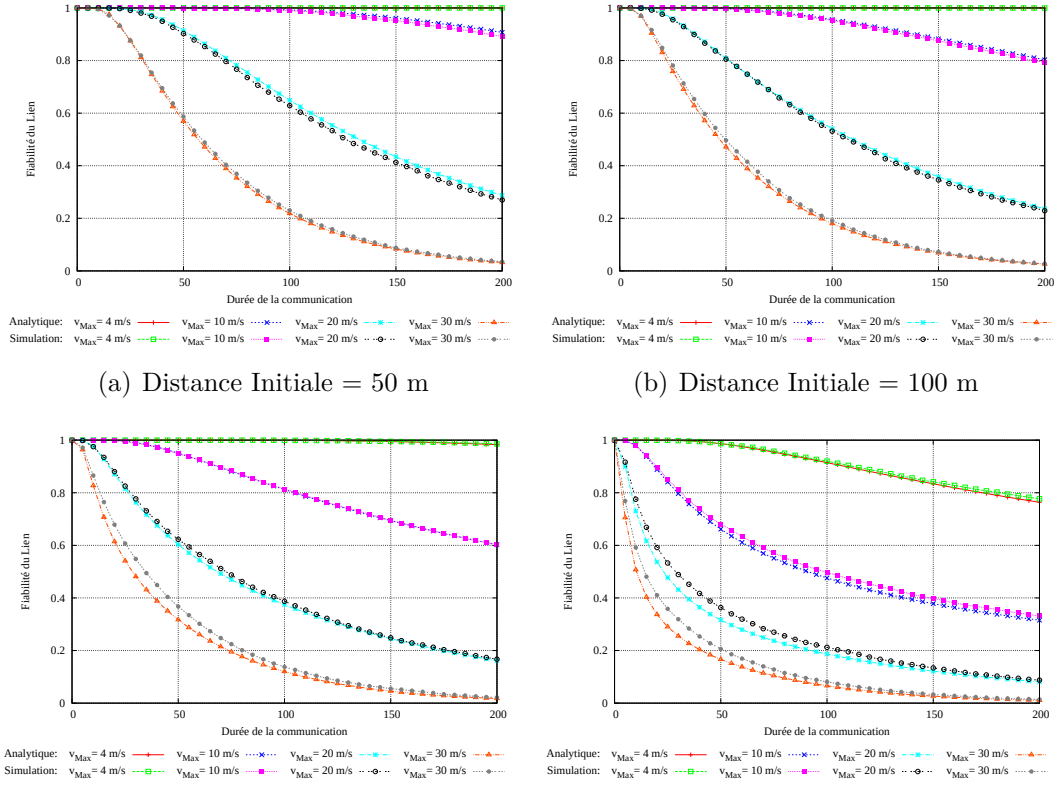
Les courbes de la figure 2.5 illustrent l'importance de la distance initiale sur la fiabilité du lien. Pour une vitesse maximale v_{max} donnée, nous comparons la fiabilité du lien pour différentes distances initiales 50 m, 100 m, 150 m et 200 m ; le vecteur P_0 est déterminé par l'équation 2.12.

Nous observons que lorsque les nœuds se déplacent avec une vitesse maximale faible ($v_{max} = 4m/s$), la distance initiale a peu d'influence sur la fiabilité des liens. Par contre, la distance initiale influence fortement la fiabilité des liens entre deux nœuds se déplaçant à $v_{max} = 10m/s$. Dans ces deux cas, l'écart entre les fiabilités augmente avec la durée de communication ; la valeur maximale est atteinte à $T = 200$ s. Contrairement aux cas précédents, l'écart entre les fiabilités décroît lorsque la durée de communication augmente pour les vitesses $v_{max} = 20m/s$ ou $30m/s$; quelle que soit la distance initiale, la fiabilité du lien converge rapidement vers 0. Ces résultats nous paraissent être les plus importants, car notre objectif est d'utiliser le modèle analytique dans un protocole de routage. Ce qui implique que le calcul de la fiabilité doit s'effectuer en connaissant la distance initiale.

2.3.5.2 Cent nœuds

Pour montrer l'influence des collisions inter-paquets sur la fiabilité des liens, nous plaçons cent nœuds dans la zone de simulation (1000m × 1000m). Ces nœuds s'échangent à intervalle réguliers d'une seconde des messages.

Nous observons sur la figure 2.6 que lorsque le nombre de retransmissions $m = 6$, les collisions inter-paquets ont très peu d'influence sur la fiabilité. Durant la simulation, un nœud a donc un nombre moyen de voisins égal à 11 nœuds (valeur obtenue à partir de l'équation 2.40 et des paramètres choisis). Dans ce cas, la probabilité p_{sColl} de suppression de paquets dues aux collisions successives est presque nulle (figure 2.2).



(a) Distance Initiale = 50 m

(b) Distance Initiale = 100 m

(c) Distance Initiale = 150 m

(d) Distance Initiale = 200 m

FIGURE 2.5 – Fiabilité en fonction du temps : Distance Initiale connue

2.3.5.3 Fiabilité d'une route

Dans cette partie, nous appliquons notre modèle analytique pour le calcul de fiabilité d'une route. Comme formulé dans l'équation 1.4, la fiabilité de la route

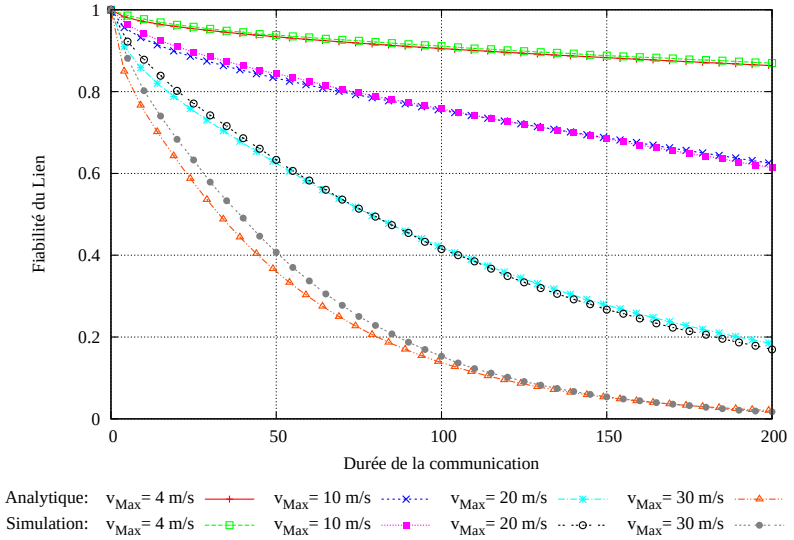


FIGURE 2.6 – Fiablité d'un lien influencée par les collisions inter-paquets

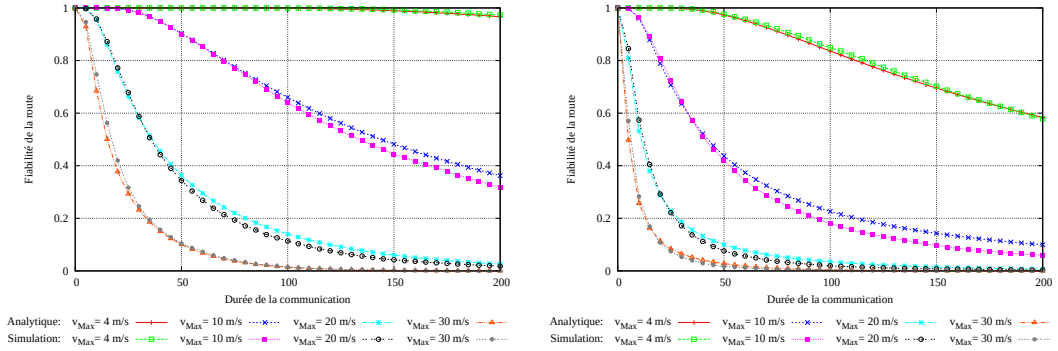
$Ro_{(n_0 \leftrightarrow n_m)}$ entre les nœuds n_0 et n_m dépend de celles des m liens et des $(m+1)$ nœuds la composant. Cependant, la fiabilité d'un nœud varie très peu dans les intervalles temporels de communications qui nous intéressent. Nous supposons que cette fiabilité est constante et est égale à 1.0 dans notre modélisation.

Lorsque les liens sont supposés indépendants, la fiabilité de la route après k époques s'écrit comme le produit de la fiabilité des m liens composant la route [BDP12, CCGL06, DFH06, MZ99, SZG+07, SLG00, YAA10] :

$$\begin{aligned} R_{Ro_{(n_0 \leftrightarrow n_m)}}(k) &= R\left(L_0(k) \cap L_1(k) \cdots \cap L_{m-1}(k)\right) \\ &= \prod_{i=0}^{m-1} R_{L_i}(k) \end{aligned} \tag{2.43}$$

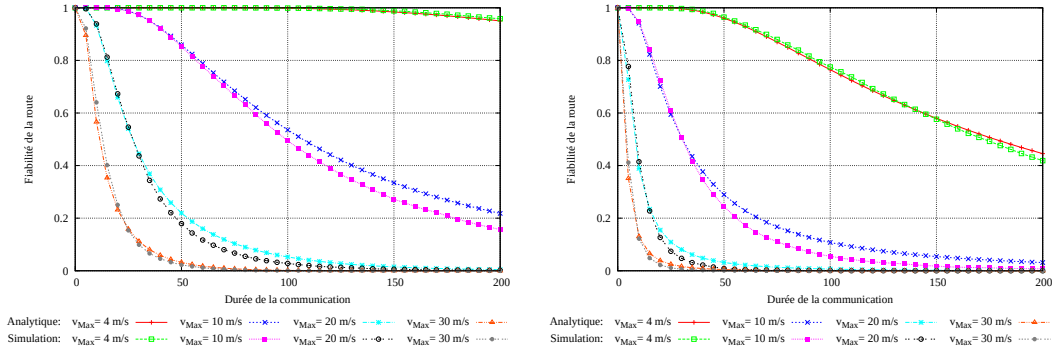
Les distances inter-nœuds choisies pour cette validation sont 150 m et 200 m. Les figures 2.7, 2.8 et 2.9 représentent la fiabilité des routes composées respectivement de deux, trois et quatre liens. Nous observons que la fiabilité prévisionnelle donne une bonne approximation de la fiabilité simulée quelle que soit la vitesse et la distance initiale inter-nœuds. Notons, cependant une légère détérioration de la validation pour les vitesses maximales de 10 m/s due aux corrélations entre les liens adjacents. La prise en compte de la corrélation entre liens adjacents dans un calcul de la fiabilité a été étudiée dans [BCF+99, Far04, ZD07] pour différents modèles de mobilité. En effet, la fiabilité d'une route composée de deux liens entre $(n_0 \leftrightarrow n_1 \leftrightarrow n_2)$ dépend de la mobilité du nœud intermédiaire n_1.

Pour prendre en compte la corrélation dans notre modèle analytique, il faut construire une nouvelle chaine de Markov. Celle-ci modélise le déplacement conjoint des nœuds de la route. En choisissant, les mêmes valeurs que dans la section précédente $\epsilon = 1$ mètre et $r_0 = 250$ mètres, le nombre d'états de la chaine de Markov est égale à 250^m où m est le nombre de liens composant la route. Ce qui entraine un coût important en termes de temps de calcul, de mémoire et d'énergie consommée au niveau des nœuds pour une faible amélioration. En conséquence, cette solution n'est pas en envisageable, pour être apportée, dans un protocole de routage.



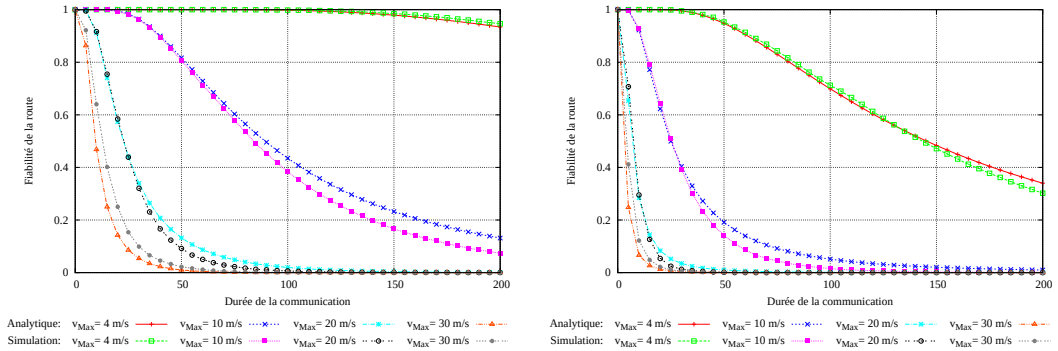
(a) Distances Initiales = 150 m (b) Distances Initiales = 200 m

FIGURE 2.7 – Route composée de deux liens



(a) Distances Initiales = 150 m (b) Distances Initiales = 200 m

FIGURE 2.8 – Route composée de trois liens



(a) Distances Initiales = 150 m (b) Distances Initiales = 200 m

FIGURE 2.9 – Route composée de quatre liens

2.4 Conclusion

Dans ce chapitre, nous avons étudié la métrique prédictive fiabilité de route. Elle permet d'améliorer les performances du réseau au niveau routage par un service de protection.

Un modèle analytique capable de prédire la fiabilité de communication entre deux nœuds adjacents se déplaçant selon les modèles *Random Walk Mobility* et *Random Way Point Mobility* a été proposé. L'originalité de notre approche est la prise en compte dans notre modèle analytique des différents facteurs de communication sans fil (les atténuations du signal et les collisions inter-paquets) en plus des déplacement des nœuds. Dans cette méthode, le calcul de métrique ne génère aucun overhead supplémentaire contrairement aux méthodes reposant sur l'historique de la communication qui s'appuient sur l'hypothèse selon laquelle un lien fiable durant une période donnée, le sera dans le futur. Ce qui n'est pas toujours vrai dans un réseau mobile ad hoc. Ceci qui est un atout intéressant. Par ailleurs, notre méthode est plus adaptée au calcul de la fiabilité de lien dans un réseau mobile que les métriques reposant sur la qualité du lien comme ETX [DABM03].

La comparaison entre les fiabilités observées et prédites des liens montre la validité du modèle analytique proposé. La fiabilité d'un lien entre deux nœuds diminue lorsque leur distance initiale et/ou leur vitesse maximum augmentent. Les fiabilités de routes obtenues avec l'hypothèse d'indépendance donne une bonne approximation de la fiabilité de route obtenue par simulation. Nous avons aussi étudié l'influence de la distance initiale inter-nœuds sur la fiabilité des liens et des routes.

Dans le prochain chapitre, nous étudierons l'utilisation de métriques prédictives dans un protocole de routage.

Chapitre 3

Routage robuste et Métriques prédictives

Table des matières

Dans le chapitre précédent, nous avons proposé une méthode analytique pour le calcul de la fiabilité de liens et de routes. L'objectif de ce chapitre est d'étudier l'utilisation des métriques prédictives dans un protocole de routage réactif.

En introduction, nous motivons le choix du protocole IETF DYMO[CP10]. Ensuite, nous décrivons brièvement le protocole.

La deuxième section est consacrée à l'utilisation de la fiabilité obtenue comme métrique dans un protocole de routage réactif. Nous présentons notamment les modifications à effectuer sur les paquets de découverte et le choix de la durée de l'intervalle de calcul de la fiabilité.

Le choix de la fiabilité comme métrique de routage permet d'augmenter la durée de vie des routes construites. Nous remarquons qu'elle augmente aussi le nombre moyen de sauts des routes car celles-ci sont construites avec des liens courts. Pour remédier à cet inconvénient, nous proposons dans la troisième section, une métrique qui permet de concilier de manière conjointe les deux critères antagonistes : la fiabilité et le minimum de sauts. Le critère de sélection d'une route ne repose plus uniquement sur la fiabilité des liens qui la composent, mais sur une combinaison entre la fiabilité des liens et la probabilité de ne pas utiliser des relais inutiles. La route construite est celle qui offre le meilleur compromis entre ces deux métriques. Un nœud intermédiaire utilisé comme relais lors de la phase de découverte peut devenir inutile à certains instants durant la communication. L'objectif est donc de réduire les chances de choisir des relais inutiles lors de la découverte.

La quatrième section est consacrée à l'évaluation comparative des deux métriques proposées (la fiabilité et la combinaison fiabilité-minimum de sauts) par rapport à la métrique par défaut (le minimum de sauts). Nous présentons les paramètres de simulation utilisés et les critères de performances. Puis, nous comparons les trois métriques en fonction des critères de performances choisis. Nous en déduisons l'apport des métriques prédictives dans l'amélioration des performances du protocole de routage.

3.1 Introduction

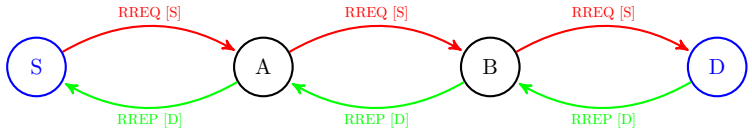
Pour utiliser les métriques prédictives, nous choisissons le protocole DYMO [CP10]. C'est le dernier né des protocoles de routage pour les réseaux MANETs de l'IETF. Actuellement, il est en cours de standardisation. Inspiré du protocole AODV [PBRD03], c'est un protocole réactif qui utilise la stratégie de routage par la destination. Pour éviter des boucles de routes et mettre à jour les routes existantes, chaque nœud DYMO maintient un numéro séquence. La gestion des numéros de séquence et l'algorithme d'évitement de boucle de routage sont assez semblables à ceux introduits par le protocole AODV.

La principale nouveauté introduite par DYMO est la notion d'accumulation de routes. L'objectif est de réduire le temps moyen d'acquisition des routes et de diminuer le surcoût du routage. Pour mettre en œuvre cette notion, chaque nœud ajoute ses informations de routage à chaque paquet de routage (RREQ et RREP) qu'il transmet. Un paquet de routage contient donc les informations sur tous les nœuds qu'il a traversés. A la réception d'un paquet de routage, un nœud DYMO vérifie si celui-ci lui permet soit d'apprendre de nouvelles routes soit de mettre à jour des routes existantes. La métrique par défaut utilisée est le minimum de sauts.

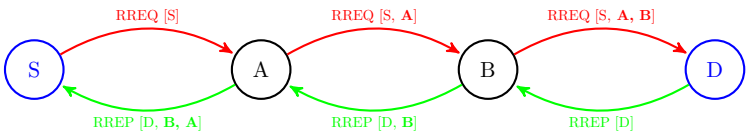
La figure 3.1 compare les découvertes des protocoles AODV et DYMO. Dans AODV, la découverte permet à chaque nœud d'établir des routes vers ses voisins directs, la source S et la destination D. Avec l'accumulation de routes, chaque nœud DYMO obtient une route vers tous les nœuds entre S et D. Dans ce cas, le nœud S n'initie pas de découverte lorsqu'il désire joindre B. Alors que dans le protocole AODV, une nouvelle découverte est nécessaire pour établir une telle communication.

Comme dans AODV, un nœud DYMO associe un ensemble de minuteurs à chaque route construite (voir Tableau 3.1).

Le minuteur ROUTE_AGE_MIN_TIMEOUT correspond à la durée de vie minimale d'une route construite. L'échec de conservation d'une route durant au moins



(a) AODV : Contenus des RREQs et RREPs



(b) DYMO : Contenus des RREQs et RREPs

FIGURE 3.1 – Comparaison des découvertes de routes entre S et D : AODV et DYMO

cette durée entraine des pertes de messages ou le transfert de plusieurs copies d'un même message.

Les numéros de séquence DYMO, qui assurent l'évitement de boucles, sont sensibles au délai. Ils doivent être renouvelés à chaque ROUTE_SEQNUM _AGE_MAX. En conséquence, la durée de vie maximale d'une route est égale à la valeur de ce minuteur. L'inconvénient de cette approche est l'augmentation du nombre messages de contrôle et des pertes de données, si les nœuds d'extrémité désirent toujours communiquer après l'expiration du minuteur.

La minuterie ROUTE_USED est utilisée pour détecter l'état d'une route (active ou non). Une route est active si elle a été utilisée pour transmettre des données, il y a une durée inférieure à la valeur de ROUTE_USED_TIMEOUT. C'est-à-dire que son minuteur ROUTE_USED n'a pas encore expiré. Chaque fois qu'une route active est utilisée pour transmettre des données, sa minuterie ROUTE_USED est réinitialisée. La route devient inactive à l'expiration de cette minuterie. Une minuterie ROUTE_NEW est associée à chaque nouvelle route créée. Elle est initialisée à la même valeur que la minuterie précédente.

Sur la figure 3.1(b), si le nœud S n'émet aucune donnée dont la destination est le nœud B, sa route vers B sera déclarée inactive après 5 secondes. Les minuteries ROUTE_NEW et ROUTE_USED auront expirées.

La déclaration d'inactivité d'une route entraine le lancement de sa minuterie ROUTE_DELETE. Elle est initialisée à ROUTE_DELETE_TIMEOUT. Après ce délai sans émission de données par la route, celle-ci est supprimée de la table de routage. Dans notre exemple, si le nœud S n'envoie toujours pas de données vers B, la route sera supprimée après 10 secondes. Le temps de suppression d'une route jamais utilisée pour un transfert de données est égale à 15 secondes (ROUTE_DELETE_TIMEOUT + ROUTE_TIMEOUT) .

L'utilisation conjointe des minuteurs ROUTE_USED et ROUTE_DELETE permet d'identifier et de supprimer les routes inactives. Ce qui permet, par ailleurs, de réduire les chances qu'un nœud intermédiaire informe une source qu'il possède une route (génération de RREP en réponse à un RREQ) qui est en fait déjà rompue.

Nom	Valeur
ROUTE_TIMEOUT	5 secondes
ROUTE_AGE_MIN_TIMEOUT	1 seconde
ROUTE_SEQNUM_AGE_MAX	60 secondes
ROUTE_USED_TIMEOUT	ROUTE_TIMEOUT
ROUTE_DELETE_TIMEOUT	2 * ROUTE_TIMEOUT

TABLE 3.1 – Valeurs par défaut des minuteries du protocole DYMO

La principale difficulté d'association de minuteurs aux routes est le dimensionnement correct de leurs valeurs. Ces valeurs dépendent du modèle de mobilité des nœuds et de leurs vitesses.

Les ruptures de routes entre nœuds adjacents peuvent être détectées par un des mécanismes présentés au chapitre 1 section 1.2.1.2.2.1. Dans la section consacrée à l'évaluation de performances, nous précisons et expliquons notre choix de mécanisme de détection.

3.2 Utilisation de la fiabilité dans un protocole réactif

Dans cette section, nous nous intéressons à l'introduction de la fiabilité déduite de ce modèle analytique comme métrique dans un protocole de routage réactif *unipath*.

Nous présentons notamment les modifications à apporter aux paquets de découverte de routes (*Route Request – RREQ* et *Route Reply – RREP*) et l'algorithme de traitement de ces paquets. Ensuite, nous discuterons le choix de la durée de définition de la fiabilité des liens.

3.2.1 Modifications sur les paquets de routage et dans l'algorithme

Pour introduire la fiabilité dans un protocole réactif, il est nécessaire d'ajouter respectivement un et deux champs aux paquets de découverte *RREP* et *RREQ*. Le champ supplémentaire commun ajouté aux deux paquets de découverte est le champ fiabilité de route (*fr*). Durant la phase de recherche de route, ce champ contient à tout moment la fiabilité de la route entre la source n_0 et le nœud émetteur n_j de la requête *RREQ* et est modifié à chaque saut. Alors que le champ fiabilité de route d'un paquet de réponse de route notée *RREP.fr* est enregistré par la destination n_m (reste inchangé durant son parcours entre n_m et n_0) et contient la fiabilité de la route entre la source n_0 et la destination n_m. C'est-à-dire que nous supposons que la meilleure route en terme de fiabilité entre la source n_0 et la destination n_m (ou inversement) est la même au moment de la recherche de routes (diffusion de RREQs) qu'au moment de la réponse de routes (transmission de RREPs). Dans les protocoles réactifs standards IETF qui nous intéressent, la durée de découverte de routes T_{DR} doit être inférieure à 2 secondes. Notre hypothèse est donc valable car les fiabilités d'un lien aux instants k_0 et $k_0 + T$ (avec $T \leq 2$ secondes) sont presque égales (voir section 2.3.5). Le second champ ajouté aux paquets *RREQ* est le champ *position du nœud émetteur (pne)* dans lequel un nœud n_j insert ses coordonnées $\left(X_{n_j}, Y_{n_j}\right)$ avant de diffuser la requête. Les coordonnées d'un nœud sont obtenues grâce à un système de localisation.

L'algorithme simplifié de la phase de diffusion des requêtes de route est donné en *Algorithme* 1. Lorsqu'une source n_0 désire joindre une destination n_m pour laquelle, elle ne possède pas de route, elle crée une requête de route RREQ. La source met le champ *fiabilité de route - fr* de cette requête à 1 et y ajoute sa position actuelle $RREQ.pne = (X_{n_0}, Y_{n_0})$ avant de la diffuser dans son voisinage. Un nœud n_j ($1 \leq j \leq m$) qui reçoit un paquet de requête n'introduisant pas de boucle dans le routage (détectée grâce aux numéros de séquence), calcule la fiabilité du lien L_{j-1} entre lui et le nœud n_{j-1} émetteur de cette requête à partir de la distance calculée $d_{L_{j-1}}$.

Le nœud n_j met à jour sa table de route (tr) en acceptant la nouvelle route si celle-ci respecte les trois conditions d'acceptations : 1) il ne possède pas de route vers la source n_0 ou 2) la nouvelle route est plus fiable que celle qu'il possède *ie* $R_{L_{j-1}} \times RREQ.fr > tr.Ro_{n_0 \leftrightarrow n_j}$ ou 3) les deux routes ont la même fiabilité mais la nouvelle route compte moins de sauts. Sinon le paquet de requête est supprimé. Les champs *RREQ.fr* et *RREQ.pne* sont mis à jour avant la diffusion par le nœud n_j si celui-ci est un nœud intermédiaire (*ie* $j \neq m$). Dans le cas où n_j est le nœud destinataire, il crée un paquet de réponse de route dont la fiabilité de route est égale à celle de la nouvelle route. La source et les nœuds intermédiaires appliquent les mêmes conditions d'acceptation aux paquets RREP reçus.

Notations :
tr : table de routage
fr : fiabilité de la route
$Ro_{n_0 \leftrightarrow n_j}$ *: route entre les nœuds* n_0 *et* n_j
hc : Nombre de sauts
Initialisation :

1. Calculer la distance du lien $d_{L_{j-1}}$
   - $d_{L_{j-1}} = distance(pos_{n_j}, RREQ.pne)$
2. Calculer la fiabilité du lien L_{j-1}
   - $R_{L_{j-1}} = fiabilite(d_{L_{j-1}}, T)$
3. Calculer la fiabilité de la route $Ro_{n_0 \leftrightarrow n_j}$
   - $Ro_{n_0 \leftrightarrow n_j} = R_{L_{j-1}} \times RREQ.fr$

Si ($tr_{n_j}\left(Ro_{n_0 \leftrightarrow n_j}\right) = null$ OU $tr_{n_j}\left(Ro_{n_0 \leftrightarrow n_j}\right).fr < Ro_{n_0 \leftrightarrow n_j}$
OU
$\left(tr_{n_j}\left(Ro_{n_0 \leftrightarrow n_j}\right).fr == Ro_{n_0 \leftrightarrow n_j}\right.$ ET $\left.tr_{n_j}\left(Ro_{n_0 \leftrightarrow n_j}\right).hc > RREQ.hc + 1\right)$
) **Alors**
  Accepter la nouvelle route et Modifier en conséquence la table de routage (tr)
  - $tr_{n_j}\left(Ro_{n_0 \leftrightarrow n_j}\right).fr = Ro_{n_0 \leftrightarrow n_j}$
  - $tr_{n_j}\left(Ro_{n_0 \leftrightarrow n_j}\right).hc = RREQ.hc + 1$

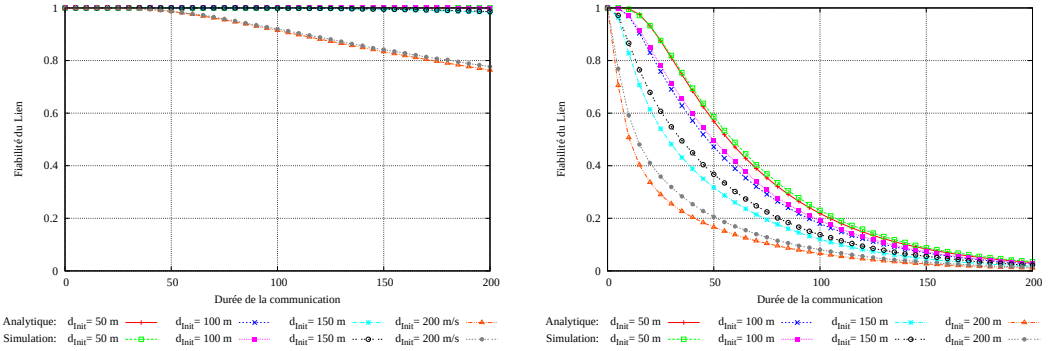
  Si ($n_j \neq n_m$) **Alors**
    $RREQ.fr = tr_{n_j}\left(Ro_{n_0 \leftrightarrow n_j}\right).fr$
    $RREQ.pne = pos_{n_j}$
    $RREQ.hc = tr_{n_j}\left(Ro_{n_0 \leftrightarrow n_j}\right).hc$
    Diffuser la requête RREQ dans son voisinage
  Sinon
    n_j est la destination ; Créer un paquet RREP
    $RREP.fr = tr_{n_j}\left(Ro_{n_0 \leftrightarrow n_j}\right).fr$
    Transmettre ce paquet au nœud n_{j-1}
  Fin Si

Sinon
  n_j supprime le paquet $RREQ$
Fin Si

Algorithme 1: Métrique fiabilité :Traitement d'un $RREQ$ par n_j en provenance de n_{j-1}

3.2.2 Importance du choix de la durée de l'intervalle T

Durant la phase de découverte, les routes sont choisies à chaque saut en fonction de la fiabilité des liens les composant. Rappelons que la fiabilité est définie sur un intervalle, la fiabilité d'un lien dépend donc de la durée de cet intervalle. Le choix de cette durée aura par conséquent un impact important sur les routes construites. Pour appuyer cette analyse, nous illustrons la phase de découverte entre les nœuds



(a) $v_{max} = 4$ m/s (b) $v_{max} = 30$ m/s

FIGURE 3.2 – Importance du choix de la durée T

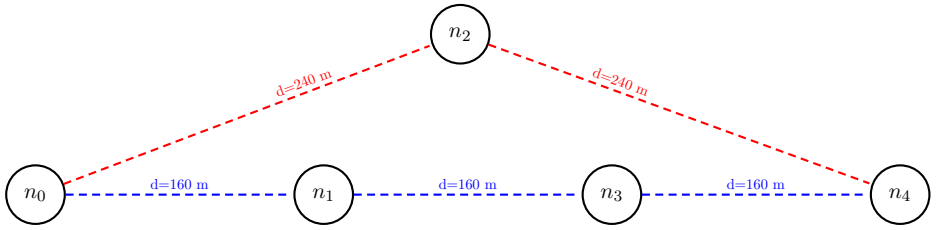


FIGURE 3.3 – Comparaison des métriques *minimum de sauts* et *fiabilité de route*

n_0 et n_4 (figure 3.3) dans le cas où tous les nœuds se déplacent respectivement avec les vitesses v_{max} 4 et 30 m/s. Quelles que soient les vitesses des nœuds, la route établie par la métrique *minimum de saut* est $Ro_1 = (n_0 \leftrightarrow n_2 \leftrightarrow n_4)$. Les routes construites avec la métrique *fiabilité de route* dépendent du choix de la durée de communication T.

- $v_{max} = 4$ m/s : Pour les durées $T \leq 50$ secondes, la même route Ro_1 sera établie par la métrique *fiabilité de route*, car tous les liens ont une fiabilité égale à 1,0. Alors que la route $Ro_2 = (n_0 \leftrightarrow n_1 \leftrightarrow n_3 \leftrightarrow n_4)$ sera construite si la durée T est supérieure à 50 secondes (voir figure 3.2(a)).
- $v_{max} = 30$ m/s : L'utilisation de la métrique *fiabilité de route* construit la route Ro_2 pour T inférieure ou égale à 100 secondes. Elle conduira au choix de la même route Ro_1 (avec le *minimum de sauts*) parce que tous les liens ont des fiabilités presque nulles (voir figure 3.2(b)).

L'objectif du critère fiabilité est de construire de meilleures routes qu'avec la métrique *minimum de saut* en permettant à un chaque nœud intermédiaire de choisir le meilleur relais parmi ses voisins ; c'est-à-dire le voisin avec lequel le lien établi a la plus faible probabilité de se rompre. A partir de l'analyse précédente, nous déduisons que la durée doit être comprise entre 50 et 100 secondes pour les vitesses maximum de déplacement qui nous intéressent.

Un choix adéquat de la durée T permet donc de réduire la probabilité de panne des routes construites. Cependant, nous observons que les longueurs des routes (en

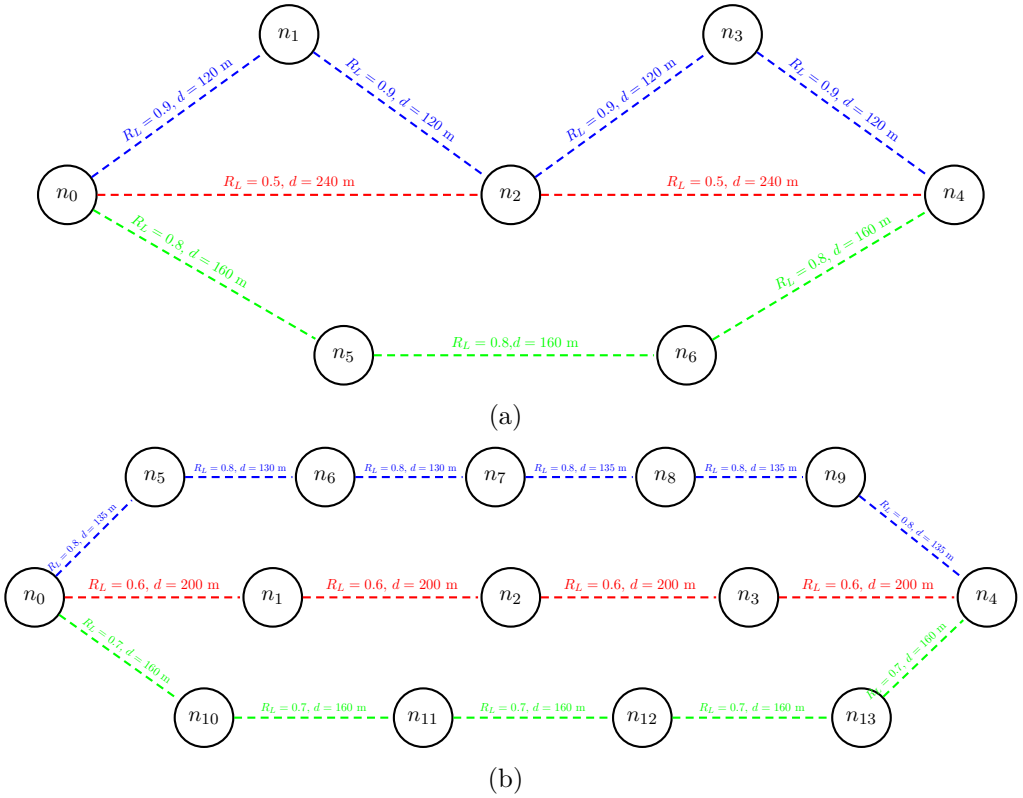
nombre de sauts) risquent d'augmenter dans certains cas. Pour résoudre cet inconvénient, dans la prochaine section, nous proposons une nouvelle métrique qui permet d'assurer un compromis entre les métriques *fiabilité de route* et *minimum de sauts*.

3.3 Proposition d'une métrique de routage combinant le minimum de sauts et la fiabilité

3.3.1 Analyse des métriques fiabilité et minimum de sauts

Dans le routage classique, le critère de sélection d'une route est le minimum de sauts. L'utilisation de ce critère présente l'avantage d'utiliser le minimum de nœuds intermédiaires. Cependant, nous avons montré précédemment que cela risque de diminuer la qualité des liens utilisés pour construire la route en termes de bande passante et de fiabilité. Puisque la route est construite sur les liens les plus longs. L'utilisation de la fiabilité comme métrique permet d'établir des routes qui durent le plus longtemps. Cependant, il y a un risque d'augmentation du nombre moyen de sauts des routes car celles-ci sont établies sur des liens courts.

Nous proposons donc une métrique de routage pour construire des routes fiables avec un nombre de sauts optimisé. Cette métrique tire profit des avantages des deux métriques antagonistes : *fiabilité de route* et *minimum de sauts*. Nous montrons l'utilité d'une telle métrique et discutons son utilisation au sein d'un protocole de routage réactif.



(a)

(b)

FIGURE 3.4 – Métrique combinant *fiabilité* et *minimum de sauts*

Illustrons la découverte de route entre les nœuds n_0 et n_m sur les topologies de la figure 3.4.

Les routes construites par la métrique *minimum de sauts* sur les deux topologies sont respectivement $Ro_1(a) = (n_0 \leftrightarrow n_2 \leftrightarrow n_4)$ et $Ro_1(b) = (n_0 \leftrightarrow n_1 \leftrightarrow n_2 \leftrightarrow n_3 \leftrightarrow n_4)$ alors qu'un protocole utilisant la métrique *fiabilité de route* établira les routes $Ro_2(a) = (n_0 \leftrightarrow n_1 \leftrightarrow n_2 \leftrightarrow n_3 \leftrightarrow n_4)$ et $Ro_2(b) = (n_0 \leftrightarrow n_5 \leftrightarrow n_6 \leftrightarrow n_7 \leftrightarrow n_8 \leftrightarrow n_9 \leftrightarrow n_4)$.

Nous observons qu'aucune des deux métriques n'établit les routes qui possèdent le meilleur compromis entre la métrique fiabilité et le nombre de sauts à savoir $R_3(a) = (n_0 \leftrightarrow n_5 \leftrightarrow n_6 \leftrightarrow n_4)$ et $R_3(b) = (n_0 \leftrightarrow n_{10} \leftrightarrow n_{11} \leftrightarrow n_{12} \leftrightarrow n_{13} \leftrightarrow n_4)$.

En fait, la métrique *fiabilité de route* construit la route la plus longue car elle est calculée à chaque saut et tient compte uniquement de l'état du lien adjacent. De plus, elle conduit souvent à choisir soit des relais inutiles au moment de la découverte (cas de n_1 entre n_0 et n_2 sur la figure 3.4(a)) soit des relais qui ont de forte chance de devenir inutile durant la communication.

Nous définissons l'utilité d'un relais n_{i+1} entre les nœuds n_i et n_{i+2} comme le pourcentage de temps durant lequel il est indispensable pour assurer la communication entre n_i et n_{i+2}. L'inutilité du relais n_{i+1} est égale à la probabilité que les nœuds n_i et n_{i+2} puissent communiquer directement.

Comme le routage utilisé est réactif, le relais devenu inutile continuera à être utilisé jusqu'à une nouvelle découverte de route. Outre l'inefficacité d'une telle communication, elle peut entrainer des collisions, des interférences inter-paquets et une augmentation du délais.

Pour réduire le nombre de sauts, il faut réduire la probabilité d'utiliser un relais inutile durant la communication.

3.3.2 Formulation de la métrique

La métrique que nous proposons est le produit entre la fiabilité des liens composant la route et la probabilité de ne pas utiliser de relais inutile entre les nœuds à deux sauts. La valeur de la métrique après k époques de la route $Ro_{(n_0 \leftrightarrow n_m)}$ entre une source n_0 et une destination n_m composée de m liens adjacents est formulée :

$$\begin{aligned} NM_{P_{(n_0 \leftrightarrow n_m)}}(k) &= R_{Ro_{(n_0 \leftrightarrow n_m)}}(k) \times \prod_{i=0}^{m-2} \left[1 - IR_{n_{i+1}}(k)\right] \\ &= R_{L_{m-1}}(k) \prod_{i=0}^{m-2} R_{L_i}(k) \times \left[1 - IR_{n_{i+1}}(k)\right] \end{aligned} \quad (3.1)$$

où $\forall\ i\ R_{L_i}(k)$ est obtenue par l'équation 2.6 et $IR_{n_{i+1}}(k)$ la probabilité que le nœud n_{i+1} devienne un relais inutile.

Pour calculer cette probabilité, nous utilisons une chaine de Markov pour décrire l'évolution de la communication entre les nœuds n_i et n_{i+2} entre les époques 0 et k. Elle est composée de $(2\times n+1)$ états que nous décomposons en trois sous-ensembles : $E_{S1} = \{e_1, e_2, \ldots, e_i, \ldots, e_n\}$, $E_{S2} = \{e_{n+1}, e_{n+2}, \ldots, e_{2\times n}\}$ et $E_{S3} = \{e_{2\times n+1}\}$. Le sous-ensemble E_{S1} indique qu'il est possible d'établir une communication directe entre les nœuds. Dans le cas où l'état de communication appartient au deuxième sous-ensemble, il est nécessaire d'avoir le relais n_{i+1} pour communiquer entre les nœuds n_i et n_{i+2}. Le troisième sous-ensemble E_{S3} contient l'état absorbant et indique que les nœuds n_i et n_{i+2} ne peuvent pas communiquer à l'aide du seul relai n_{i+1}.

L'inutilité du relais n_{i+1} entre les époques 0 et k est :

$$\begin{aligned} IR_{n_{i+1}}(k) &= Pr\left[d_{(n_i,n_{i+2})}(k) \in ES_1 | d_{(n_i,n_{i+2})}(0) \in (ES_1 \cup ES_2)\right] \\ &= \sum_{i=1}^{n} cr_{i\ 2L}\,(k) \end{aligned} \tag{3.2}$$

où $cr_{i\ 2L}\,(k)$ sont les éléments du vecteur $CR_{2L}(k)$ représentent la probabilité de communication entre deux nœuds situés à une distance i :

$$cr_{i\ 2L}\,(k) = \begin{cases} \bar{p}_{sColl} \times rd_{i\ 2L}(k) \times (\bar{p}_{sCanal}\,(i))^k & \text{si} \quad 1 \leq i \leq n \\ rd_{i\ 2L}(k) & \text{si } n+1 < i \leq 2\times n+1 \end{cases} \tag{3.3}$$

Le vecteur $RD_{2L}(k)$ de taille $(2 \times n + 1)$ dont chaque élément $rd_{i\ 2L}(k)$ représente la probabilité d'être à l'état i à l'instant k est :

$$RD_{2L}(k) = P(0)P_R^k \tag{3.4}$$

où $P(0)$ représente la distance initiale entre les nœuds n_i et n_{i+2} (voir section 2.3.2.1). La matrice P_R est la matrice de probabilité de transition entre les $(2 \times n + 1)$ états de la chaine de Markov entre les instants 0 et k.

$$P_R = \begin{bmatrix} p_{1,1} & \cdots & p_{1,n} & p_{1,n+1} \cdots & p_{1,2n} & p_{1,2n+1} \\ \ldots & \ddots & \ldots & \ldots & \ldots & \ldots \\ p_{n,1} & \cdots & p_{1,n} & p_{1,n+1} \cdots & p_{n,2n} & p_{n,2n+1} \\ \ldots & \ddots & \ldots & \ldots & \ldots & \ldots \\ \ldots & \ddots & \ldots & \ldots & \ldots & \ldots \\ p_{2n,1} & \cdots & p_{2n,n} & p_{2n,n+1} \cdots & p_{2n,2n} & p_{2n,2n+1} \\ \mathbf{0} & \cdots & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{1} \end{bmatrix} \tag{3.5}$$

où $p_{i,j}$ est obtenu par l'équation 2.35 avec $\forall i, j,\ p_{i,j} \geq 0$ et $\sum_{j=1}^{n+1} p_{i,j} = 1$.

En utilisant cette nouvelle métrique, les routes construites $R_3(a)$ et $R_3(b)$ seront optimales sur les topologies de la figure 3.4.

L'introduction de la nouvelle métrique dans le routage nécessite l'ajout d'un troisième champ aux paquets *RREQ* par rapport à la métrique fiabilité. Ce champ noté *pnpe* indique la position du nœud précédent le nœud émetteur. A la réception d'un paquet RREQ, un nœud pourra déterminer la probabilité d'utiliser un relai inutile.

3.4 Evaluation des performances

Dans cette section, nous présentons les paramètres choisis pour le modèle de simulations. Nous utilisons le simulateur à évènements discrets OMNeT++ [omn]. Ensuite, nous nous intéressons aux critères de performances que nous évaluons.

3.4.1 Modèle de simulation

Pour faire l'évaluation comparative, nous choisissons une topologie de 50 nœuds. A l'initialisation, les nœuds sont aléatoirement placés dans une zone de simulation de taille 1000 m * 1000 m. Ensuite, ils se déplacent selon le modèle de mobilité *Random Walk*. Nous étudions les vitesses maximales utilisés dans le chapitre précédent à savoir 4, 10, 20 et 30 m/sec. Pour chaque vitesse maximale, 50 scénarios sont simulés. Le temps de simulation est de 900 secondes.

Dans cette évaluation, nous utilisons 4 sources qui émettent un trafic constant (CBR *Constant Bit Rate*). Le taux d'envoi de chaque source est égale à 4 paquets/sec de taille 512 octets.

Chaque nœud possède un débit nominal de 2 mégabits/sec. La taille des tampons d'interfaces est fixée à 50 paquets. La portée théorique est égale à 250 mètres. Le modèle de propagation choisi est *Shadowing fading* avec $\alpha = 3$, $\sigma_s = 2$ dB.

Le mécanisme de détection, de panne entre nœuds adjacents, est la notification de liaison (Link Layer Feedback LLF). Nous avons montré au chapitre 1 section 1.2.1.2.2.1, qu'elle offre le meilleur compromis en termes de durée de détection et de surcoût généré.

Concernant la durée T de l'intervalle, nous avons montré au chapitre précédent qu'elle doit être comprise entre 50 et 100 secondes. Sinon, la métrique fiabilité est susceptible de construire les mêmes routes que le minimum de sauts. Or, le protocole DYMO conseille une durée de vie maximale d'une route égale à ROUTE_AGE_MIN_TIMEOUT = 60 secondes. Nous choisissons par conséquent cette valeur pour la durée T. Pour réduire le surcoût du routage, une route active ne sera supprimée qu'à la réception d'un paquet RERR.

3.4.2 Critères de performances

Pour chaque critère, nous donnons sa description, son utilité et les facteurs qui influencent la valeur.

Durée T	60 secondes
Durée de la simulation	900 secondes
Zone de la simulation	1000 m * 1000 m
Nombre de nœuds	50
Nombre de sources	4
Taux d'envoi (Trafic CBR)	4 paquets/secondes
Taille des paquets	512 octets
Rayon théorique	250 m
Modèle de propagation	Shadowing fading : $\alpha = 3$, $\sigma_s = 2$ dB
Modèle d'accès	CSMA/CA – DCF 802.11
Débit nominal	2 Mbps
Mécanisme de détection	Link Layer Feedback LLF
Modèle de mobilité	Random Walk
Vitesses maximales v_{max}	4, 10, 20 et 30 m/sec

TABLE 3.2 – Paramètres de simulation

– **Taux de livraison de paquets (PDR Packet Delivery Ratio) (en %) :** C'est la proportion de paquets de données délivrées à la destination par rapport à ceux émis par les sources. Cette métrique dépend du nombre de rupture de routes, du temps de restauration T_R et de la taille des files d'attentes. Intuitivement le taux de livraison de paquets décroit lorsque la vitesse maximale des nœuds augmente.

– **Surcoût normalisé du routage (Normalized Routing Overhead) (en %) :** est défini comme le rapport entre la taille du surcoût total (en octets) et la somme de la taille des paquets arrivés à destination (en octets). Le surcoût total induit par le routage est :
  – La somme de la taille des paquets de contrôle (RREQ, RREP, RERR) en octets. Notons qu'à chaque relayage, une transmission de paquets de contrôle est comptabilisée.
  – Le surcoût du routage sur les paquets de données (Entêtes).

  Le surcoût du aux paquets de paquets de contrôle augmente lorsque le nombre de détection de rupture de routes augmente. En effet, après chaque détection de communication entre nœuds adjacents, il y a diffusion messages RERR jusqu'à la source. Ensuite, celle-ci procède à une nouvelle découverte de routes qui entraîne d'autres circulations de RREQs et de RREPs dans réseau.

– **Délai de bout en bout (en sec) :** Durée entre la demande d'émission d'un paquet de données par la couche transport de la source et sa réception par celle de la destination. Ce temps inclut toutes les durées d'attente causées respectivement par le routage (pour d'éventuelles découvertes de routes), les retransmissions de niveau MAC, les files d'attente des différentes couches (transport, routage, MAC).
  Cette métrique est corrélée avec le nombre découverte de routes réussie.

– **Nombre moyen de sauts par paquets :** indique le nombre moyen de nœuds traversés par les paquets de données.

– **Le nombre moyen de relais inutiles par paquets :** indique le nombre de nœuds non nécessaire utilisés pour assurer le relayage.

3.4.3 Résultats et interprétations

Dans cette évaluation, des résultats attendus sont observables , quelle que soit la métrique utilisée : lorsque la vitesse v_{max} augmente, le taux de livraison diminue alors que le surcoût normalisé et le nombre de rupture de routes augmentent.

Quelle que soit la valeur de v_{max}, la métrique fiabilité obtient le meilleur taux de livraison (figure 3.5). En effet, les routes sont construites avec des liens courts lorsque le critère de sélection est la fiabilité. Dans ce cas, le nombre de ruptures de routes est inférieur à ceux des autres métriques (minimum de sauts et combinaison fiabilité-minimum de sauts) (figure 3.6). Le gain en termes de taux de livraison des deux métriques proposées par rapport à la métrique classique (minimum de sauts) croît lorsque la vitesse v_{max} augmente. Ce qui est un résultat intéressant, lorsque nous nous intéressons au déploiement de réseaux très mobiles.

Cependant l'utilisation de ces deux métriques augmente le nombre de relais inutiles (figure 3.9). Surtout, la fiabilité qui en utilise un nombre important. Ceci entraine une augmentation du temps de parcours d'un paquet entre la source et la destination. Nous observons que quelle que soit la valeur de v_{max}, le délai de bout en bout de la métrique fiabilité est le plus grand, la métrique minimum de sauts, le plus faible.

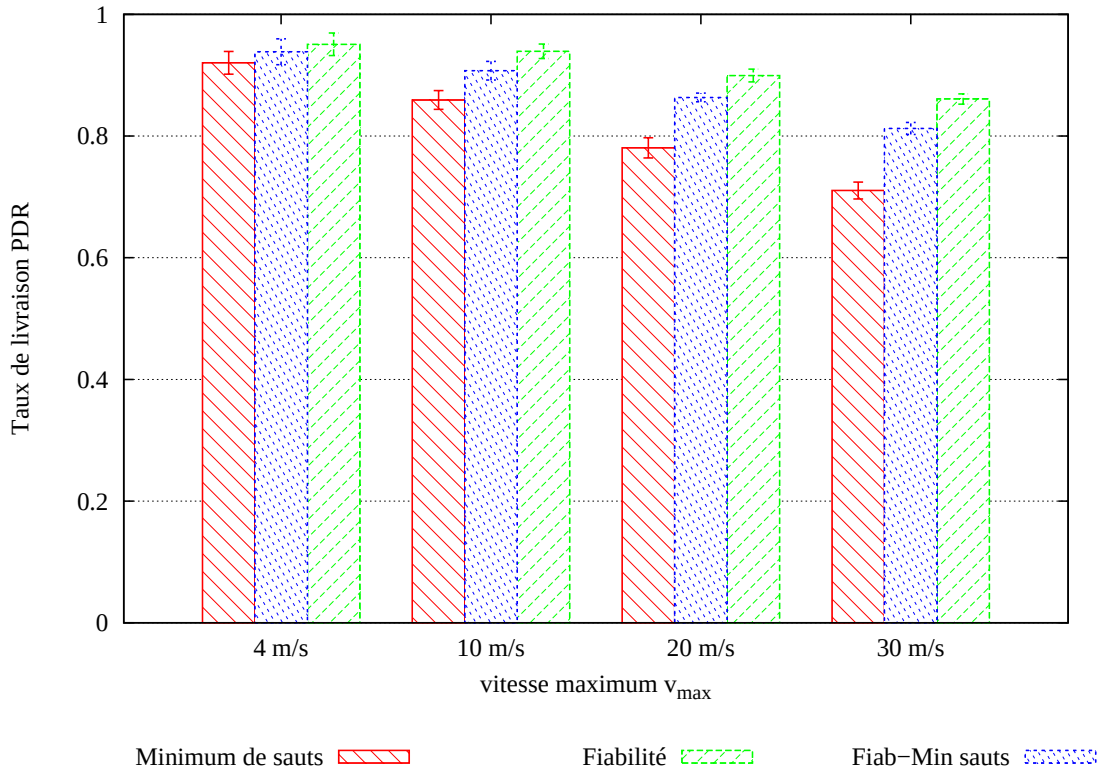


FIGURE 3.5 – Taux de livraison

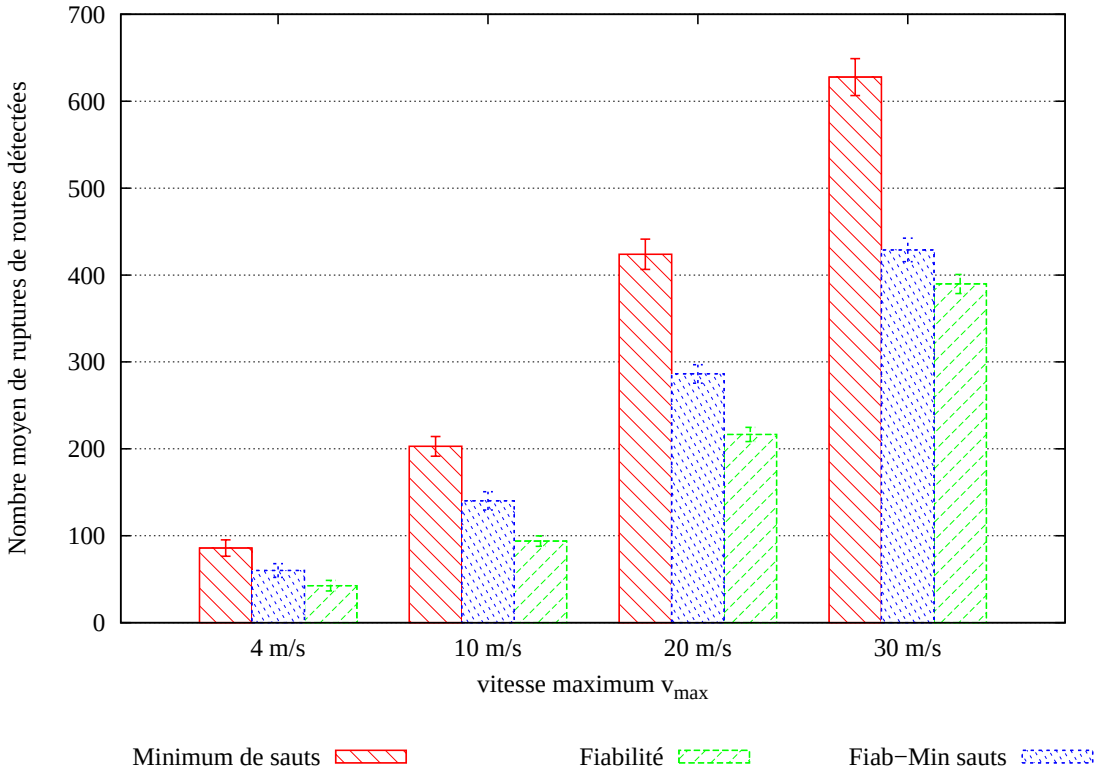


FIGURE 3.6 – Nombre moyen de ruptures de routes

Lorsque v_{max} augmente, l'écart entre les délais de bout en bout se resserre. En effet, l'utilisation de la métrique minimum de sauts conduit à l'augmentation du temps moyen d'attente des paquets à la source avant l'obtention d'une route. De plus, la probabilité que les paquets émis par la source sans attente (sur des routes) soient perdus durant le routage augmente. Ceci est dû à la réduction de la durée de vie des routes.

Nous observons sur la figure 3.10, que la métrique fiabilité possède le meilleur surcoût normalisé pour toutes les valeurs v_{max} étudiées.

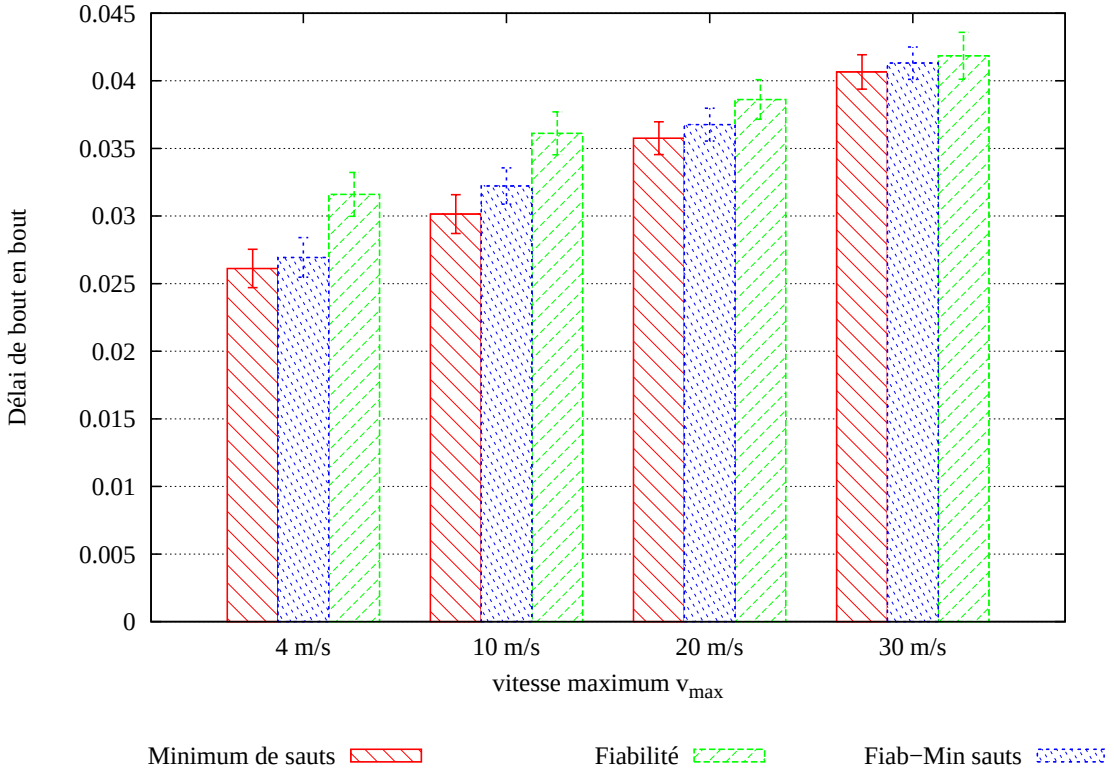


FIGURE 3.7 – Délai de bout en bout

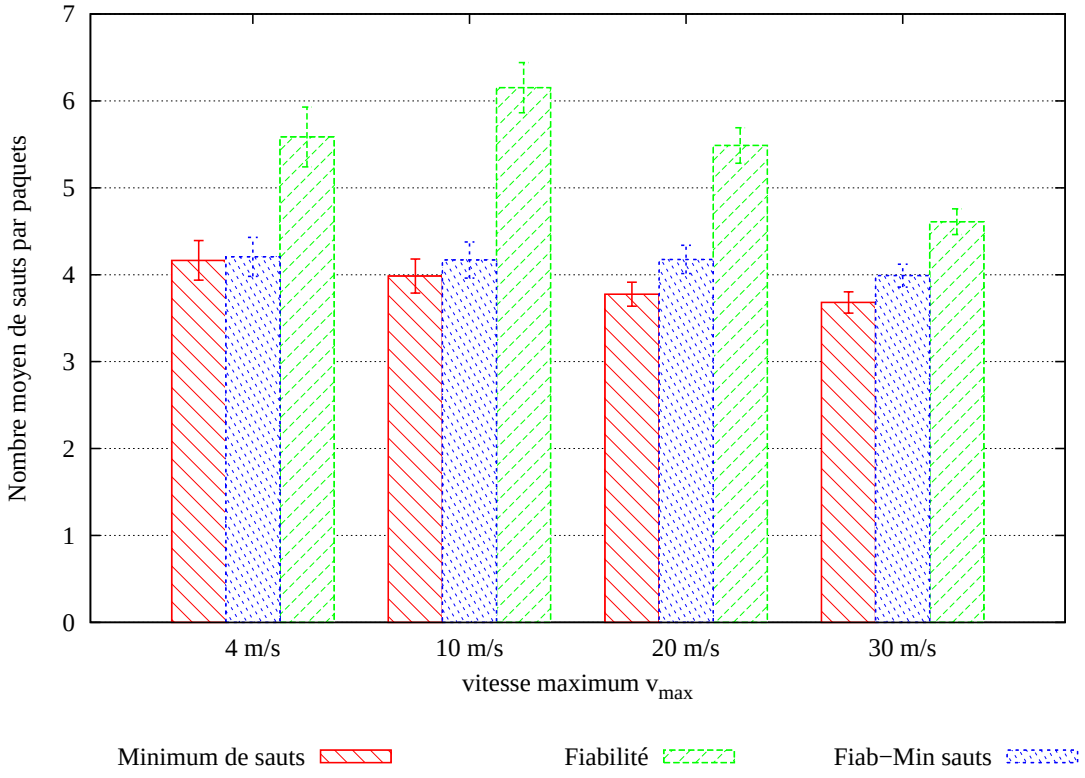


FIGURE 3.8 – Nombre de sauts par paquets

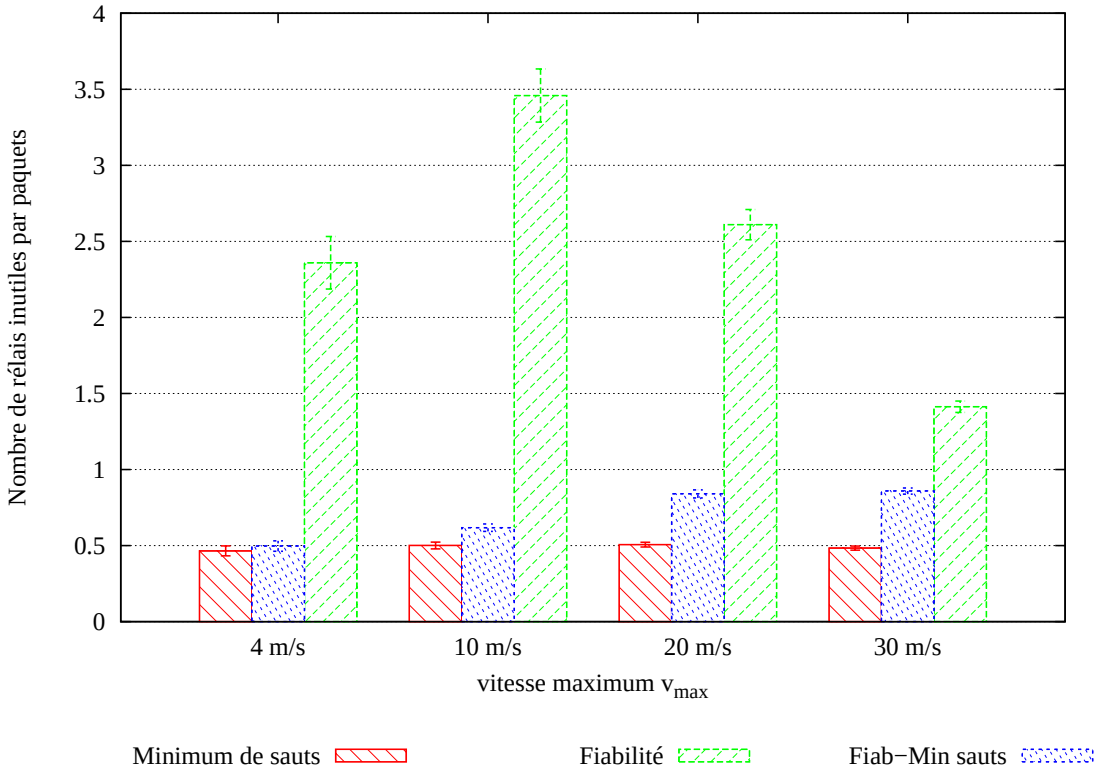


FIGURE 3.9 – Nombre de relais inutile par paquets

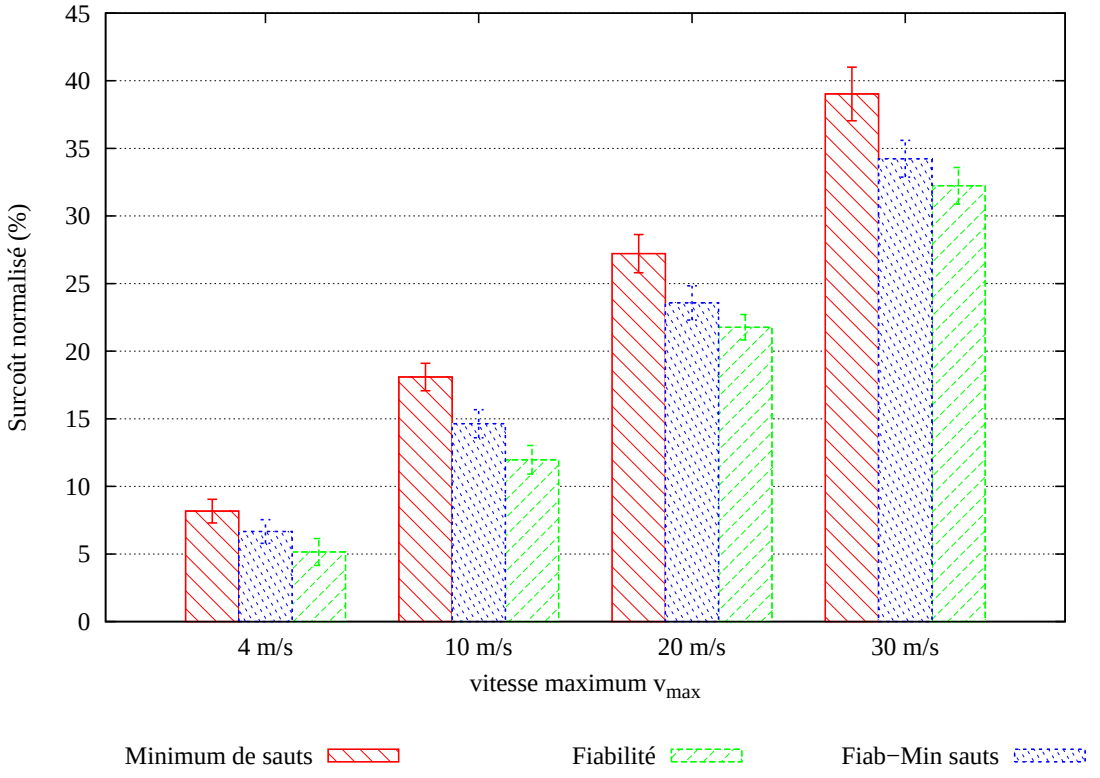


FIGURE 3.10 – Surcoût normalisé

3.5 Conclusion

Ce chapitre étudie l'apport des métriques prédictives dans le routage. Nous avons choisi le protocole DYMO[CP10] comme base de cette évaluation. Ce choix est motivé par l'option d'accumulation de routes proposée qui permet de réduire le surcoût et le délai d'obtention des routes par rapport aux protocoles AODV[PBRD03] et DSR[JHM07].

Nous nous sommes ensuite intéressés à l'introduction de la fiabilité dans un protocole de routage réactif, puis avons analysé l'influence du choix de la durée de la communication sur les routes construites. Cette durée doit être comprise entre 50 secondes et 100 secondes, pour une meilleure utilisation de la fiabilité comme métrique de routage.

Bien que la fiabilité nous permette d'améliorer la durée de vie des routes, nous observons qu'elle augmente le nombre moyen de sauts utilisés. A partir cette observation, nous avons proposé une nouvelle métrique qui permet de concilier de manière conjointe les métriques fiabilité et minimum de sauts. Elle assure un bon compromis entre le taux de livraison de paquets et le nombre moyen de sauts.

Pour une mobilité faible $v_{max} \leq 4$ m/s, il n'est pas très utile d'utiliser des métriques prédictives, car leur utilisation augmente le délai de bout en bout et la consommation d'énergie pour un gain faible en termes de taux de livraison (de l'ordre 1.5% et 3% pour respectivement les métriques la combinaison fiabilité-minimum et la fiabilité de routes).

Elles sont sont cependant très utiles dans réseau ad hoc à moyenne ou à forte mobilité $v_{max} \geq 10$ m/s . Leur utilisation améliore les performances du routage en termes de taux de livraison et de surcoût normalisé. Notons que quelle que soit la valeur v_{max}, la métrique fiabilité-minimum de sauts assure le meilleur compromis entre d'une part le taux de livraison et d'autre part le délai de bout en bout et le surcoût normalisé.

Deuxième partie

Approche de robustesse par redondance

Chapitre 4

Redondance dans le routage

Table des matières

Dans le chapitre 1, nous avons présenté les concepts de base de la redondance au niveau routage. Ce chapitre étudie la redondance des routes dans le but d'améliorer les performances du réseau en réduisant le temps de restauration. La redondance de routes est mise œuvre par les protocoles *multipath*.

En introduction, nous présentons les limites du routage *unipath* en termes de temps de restauration et de délai de bout en bout.

La deuxième section propose un état de l'art des différents protocoles *multipath* en mettant l'accent sur deux paramètres importants à savoir : le processus de recouvrement et le degré de similitude entre les routes construites. L'influence de ces deux paramètres sur les types de pannes supportés par la redondance est ensuite analysée.

Dans la troisième section, nous proposons une comparaison des deux approches (protocoles *unipath* et *multipath*) en termes de temps de recouvrement, de fiabilité et d'efficacité de communication. Nous en déduisons l'intérêt de la redondance en

fonction du mécanisme de détection de panne entre nœuds adjacents. Nous proposons également une formulation analytique du temps de restauration et de la fiabilité des deux catégories de recouvrement des protocoles *multipath*.

4.1 Introduction

La principale limitation des protocoles standards est qu'ils ne construisent qu'une seule route entre la source et la destination. Ce sont des protocoles *unipath*. Après l'occurrence d'une panne de communication sur une route active, une restauration doit être mise en œuvre pour trouver une route. Un nœud intermédiaire ayant détecté une rupture de communication de sa route active vers une destination, supprime tous les paquets de données cette destination car il ne dispose pas d'une route alternative. Tous les paquets de données émis par la source avant qu'elle ne soit informée de l'état de panne (phases de détection + corrélation + notification) n'atteindront pas leur destination. Ensuite, la source bloque le trafic en fonction de la quantité de trafic généré par l'application et la taille de ses files d'attente. Ce qui peut entrainer des pertes et des congestions.

Pour reprendre la transmission, la source sera obligée de lancer une nouvelle découverte de route. Le temps d'attente de réponse entraîne une augmentation du délai de bout en bout des paquets et la découverte de route génère des messages de contrôle supplémentaires.

Pour réduire le temps de restauration de service et ainsi augmenter le taux de livraison des paquets (PDR), des protocoles de routage *multipath* s'appuyant sur les protocoles standard *unipath* ont été proposés : AODV-BR [LG00], SMR [LG02], AOMDV [MD01, MD06], AODVM [YKT03], DYMOM [KPK+07] MDYMO[NCM07] et MP-OLSR. Ces études montrent l'avantage par simulation de l'approche en termes de taux de livraison des paquets de données (Packet Delivery Ratio PDR), de messages de contrôle générés (*overhead*), de délai de bout en bout des paquets de données. En complément à ces travaux, nous proposons une comparaison analytique des approches *unipath* et *multipath* en termes de temps de restauration et de fiabilité. Nous en déduisons les conditions dans lesquelles l'approche *multipath* améliore les performances du réseau.

4.2 Protocoles de routage *multipath*

4.2.1 État de l'art

Dans cette partie, nous présentons et décrivons les principaux protocoles de routage *multipath* en réseaux mobiles ad hoc.

4.2.1.1 AODV-Backup Route (AODV-BR)

Le protocole AODV-BR [LG00] utilise les avantages de la diffusion sans fil pour mettre en place des nœuds primaires et des nœuds de secours entre la source et la destination par découverte. Son processus de découverte de routes reste identique à celui proposé par le protocole AODV (cycle de requête de routes RREQ/ réponse de routes RREP, suppression des copies d'un RREQ déjà reçu par les nœuds intermédiaires, sauvegarde d'une seule route dans la table de routage par destination). Cependant, contrairement au protocole AODV où les nœuds ne traitent que les paquets qui leur sont destinés (adresse de diffusion ou son adresse IP), un nœud dans le protocole AODV-BR traite tous les paquets de réponse de routes RREP reçus (même ceux qui ne lui pas sont destinés).

Les nœuds primaires reçoivent la réponse de route RREP après avoir diffusé la requête de route RREQ. Les nœuds de secours sont les voisins des nœuds primaires ; ils n'appartiennent pas à la route de retour empruntée par la réponse mais l'entendent à cause du caractère de diffusion des communications sans fil. Lorsqu'un nœud de secours entend une réponse de route destinée à un de ses voisins, il enregistre l'émetteur du paquet RREP comme le prochain nœud pour atteindre la destination dans sa table alternative.

Dans AODV-BR, une découverte de routes permet aux nœuds primaires de construire (ou de mettre à jour) leur table primaire et aux nœuds de secours de mettre en place leur table alternative.

Lorsqu'un nœud primaire détecte une rupture de communication avec un voisin dans sa table primaire, il diffuse sa donnée pour demander un routage de secours (indiqué dans l'entête du paquet de données). Cette donnée sera relayée en routage de secours lorsqu'elle est reçue par un nœud de secours possédant dans sa table alternative une route pour atteindre la destination. Dans le cas où la communication entre le nœud de secours et son prochain saut (qui est un nœud primaire) n'est pas rompue, la transmission de la donnée (ré)basculera sur la route primaire jusqu'à atteindre une autre défaillance de communication entre deux nœuds primaires adjacents. Après la détection de cette panne, le nœud primaire en amont de la panne procédera comme précédemment en demandant un routage de secours.

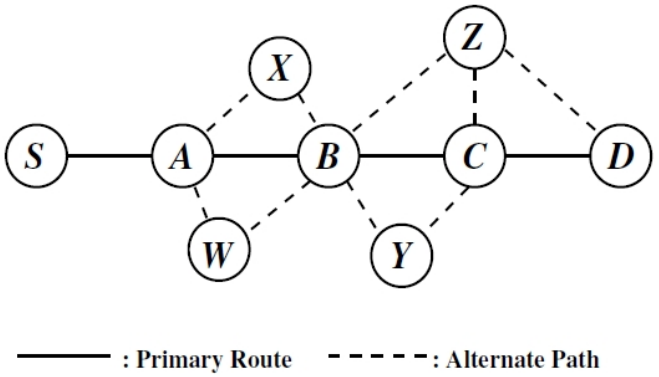


FIGURE 4.1 – Protocole AODV-BR (Source article AODV-BR[LG00])

Cette approche ne considère que des nœuds de secours à un saut des nœuds primaires, ce qui augmente les probabilités de collisions lorsque les paquets circulent simultanément sur les routes primaires et secondaires. Un même paquet de données peut être relayé en routage de secours par plusieurs nœuds de secours (par exemple les nœuds X et W) se trouvant dans la voisinage du nœud primaire A ayant détecté une panne de communication avec le nœud B (figure 4.1). Ce qui entraîne une mauvaise utilisation des ressources et peut être facteur d'autres collisions.

Par ailleurs, le protocole AODV-BR oblige la couche routage à traiter tous les paquets reçus au niveau MAC au lieu de permettre à celle-ci de supprimer immédiatement les paquets inutiles (ceux donc l'adresse MAC ne correspondent pas au sien). Ce processus entraîne une augmentation de la taille de files d'attente au niveau routage, une utilisation supplémentaire du temps CPU et une perte de temps.

4.2.1.2 Split Multipath Routing (SMR)

Le protocole multipath SMR [LG02] est inspiré du protocole DSR, il essaie d'établir des routes aussi disjointes que possible sans aucune exigence. Le protocole n'utilise pas l'amélioration *cache de routes* proposée dans le protocole DSR. Ainsi, durant la phase de découverte, un nœud intermédiaire SMR ne génère jamais de réponse de routes RREP même s'il possède une route vers la destination de la requête reçue. Un nœud intermédiaire rediffuse la première requête reçue de chaque voisin qui ne crée pas de boucle dans le routage (*ie* son identifiant n'existe pas le *enregistrement de route*) et qui lui permet d'apprendre une meilleure route vers la source.

Une destination SMR répond immédiatement à la première requête de route RREQ reçue par un paquet RREP dans le but d'optimiser le temps d'acquisition des routes par la source. Ensuite, la destination se met en attente pour recevoir le maximum de requêtes de routes. Après l'expiration d'un temporisateur, la destina-

tion choisit la route la plus disjointe de la première reçue en utilisant le degré de similitude. Le degré de similitude entre deux routes est définie comme le nombre de nœuds communs entre les deux routes.

A l'instar du protocole DSR, le protocole SMR utilise la stratégie de routage par la source entre les nœuds d'extrémité. En cas de panne de communication détectée, les nœuds intermédiaires remontent la notification de pannes à la source car le protocole n'utilise pas de caches de routes. La source basculera ensuite le trafic sur la route secondaire. On dit que le protocole SMR procède à un recouvrement de bout en bout.

4.2.1.3 Protocoles AODVM et DYMOM

Les protocoles AODV *Multipath* [YKT03] et DYMO *Multipath* [KPK+07] choisissent de construire plusieurs routes (primaire et secondaires) disjointes en nœuds. Les nœuds intermédiaires ne sont pas autorisés à créer des paquets RREP pour répondre à la source même s'ils possèdent des routes vers la destination de la requête de routes RREQ reçue.

La différence entre les protocoles AODVM et DYMOM se situe au niveau des mécanismes mis en œuvre pour assurer l'établissement des routes disjointes en nœuds.

Le protocole DYMOM utilise l'option d'accumulation de routes pour permettre à la destination de disposer pour chaque requête reçue des informations sur l'ensemble de nœuds intermédiaires qu'elle a traversés. A partir de ces informations, une destination DYMOM peut calculer le degré de similitude entre les routes. Ensuite, elle répond uniquement à celles qui permettent de construire des routes disjointes.

Dans le protocole AODVM[YKT03], les nœuds intermédiaires enregistrent chaque paquet RREQ reçu dans leur *table de RREQ*. Une destination AODVM repond à toutes les requêtes reçues. A la réception d'un paquet RREP, un nœud intermédiaire le retransmet sur la route la plus courte de sa *table de RREQ* lui permettant de joindre la source de la découverte de routes. Ensuite, il supprime de sa *table de RREQ* le voisin auquel il a transmis le paquet RREP. Pour garantir que les routes construites soient disjointes en nœuds, un nœud intermédiaire I écoute tous les paquets émis par ses voisins enregistrés dans sa *table de RREQ*. Le nœud I supprime de sa *table de RREQ* un voisin qu'il entend transmettre une réponse de route RREP.

Les routes construites sont disjointes en nœuds car chaque nœud intermédiaire participe au plus à une route. En cas de rupture de la route primaire, les protocoles AODVM et DYMOM procèdent à un recouvrement de bout en bout car les routes alternatives sont disponibles uniquement au niveau de la source des données.

4.2.1.4 Protocoles AOMDV et MDYMO

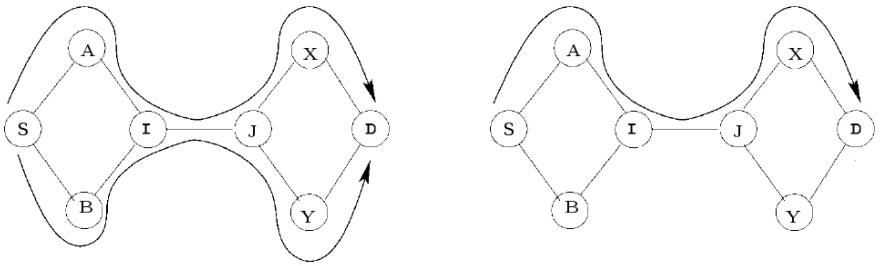
Les protocoles AOMDV [MD01, MD06] et MDYMO [NCM07] construisent des routes disjointes en nœuds ou en liens en fonction des exigences formulées par la source des données. Ils enrichissent leur protocole *unipath* de base (respectivement AODV et DYMO) en leur ajoutant deux notions supplémentaires : *nombre de sauts annoncé* et *dernier nœud*.

Le champ *nombre de sauts annoncé* d'un nœud i pour une destination D représente le nombre de sauts de la route la plus longue entre les deux nœuds. L'utilisation combinée de cette notion et des numéros de séquence permet d'adapter l'invariant des protocoles *unipath* dans le contexte de la redondance de routes, en évitant des boucles dans le routage. A réception d'un paquet RREQ dont le numéro de séquence est supérieur au sien, avant de le diffuser dans son voisinage, un nœud intermédiaire AOMDV ou MDYMO enregistre le nombre de sauts pour atteindre la source dans son champ *nombre de sauts annoncé*. La valeur du champ *nombre de sauts annoncé* d'un nœud reste inchangée jusqu'à ce qu'il reçoive une nouvelle requête RREQ de numéro de séquence supérieur. Les protocoles *multipath* diffèrent des protocoles *unipath* au niveau du traitement des copies de paquets de RREQ par les nœuds intermédiaires. Contrairement aux protocoles standards où toutes les copies d'un même RREQ (un RREQ possède un identifiant unique) sont systématiquement supprimées par un nœud intermédiaire, les nœuds AOMDV et MDYMO examinent les duplicatas RREQ pour savoir s'ils peuvent former des routes alternatives de retour sans risque de boucle et disjointes de celles déjà enregistrées en liens ou en nœuds.

Une route alternative apprise grâce à une copie de paquet de RREQ présente un risque de boucle si le nombre de sauts entre la source et le nœud intermédiaire est supérieur au champ *nombre de sauts annoncé* du nœud. Une route alternative ne présentant pas de risque de boucle sera ensuite analysée pour connaitre le degré de similitude entre elle et les autres routes déjà construites en utilisant la notion de *'Last hop'*. Le *'Last hop'* d'une route entre une source S et une destination D fait référence au nœud précèdent immédiatement la destination.

Une condition nécessaire pour avoir deux routes disjointes est : qu'elles aient des *'prochains nœuds'* différents et des *'derniers nœuds'* différents. Cependant cette condition n'est pas suffisante (figure 4.2(a)). En effet, les deux routes $R_{Pri} = (S \leftrightarrow A \leftrightarrow I \leftrightarrow J \leftrightarrow X \leftrightarrow D)$ et $R_{Sec} = (S \leftrightarrow B \leftrightarrow I \leftrightarrow J \leftrightarrow Y \leftrightarrow D)$ respectent cette condition.

Cependant, elles ne sont pas disjointes en liens (lien commun $I \leftrightarrow J$). Pour construire des routes disjointes, tous les nœuds doivent assurer que toutes les routes partant d'eux vers la destination aient des *'prochains sauts'* différents et des *'derniers sauts'* différents. Dans le figure 4.2, il n'est pas possible de construire de route



(a) (b)

FIGURE 4.2 – Protocole AOMDV (Source article AOMDV 2006)

alternative disjointe en lien de la route primaire R_{Pri}, car :

$$\begin{aligned} (prochain\ saut_I)_{R_{Pri}} &= (prochain\ saut_I)_{R_{Sec}} = J \\ &\text{et} \\ (dernier\ saut_J)_{R_{Pri}} &= (dernier\ saut_J)_{R_{Sec}} = I \end{aligned}$$

Pour limiter l'*overhead*, un nœud intermédiaire ne transmet jamais les copies de paquets RREQ reçus. Lorsque la destination reçoit un RREQ, elle procède comme les nœuds intermédiaires en créant des routes de retour vers la source du paquet RREQ. La destination génère alors un paquet RREP en réponse à chaque copie de paquet RREQ reçu qui lui permet de créer une route alternative sans risque de boucle. Un nœud intermédiaire AOMDV ou MDYMO ne duplique jamais un RREP. Cependant lorsqu'il reçoit une copie de RREP, le nœud vérifie s'il possède dans sa table une route non utilisée par un autre RREP pour atteindre la destination de ce paquet RREP (*ie* la source de la découverte).

4.2.1.5 Multipath OLSR (MP-OLSR)

Basé sur le protocole de routage proactif OLSR [CJ03], MP-OLSR est un protocole de routage *multipath* hybride. Le fonctionnement de base du protocole MP-OLSR comporte deux parties principales : la détection de la topologie du réseau (*topology sensing*) et le calcul de routes (*routes computation*). MP-OLSR est un protocole hybride dans le sens où les informations sur la topologie s'obtiennent de manière proactive alors que le calcul de routes s'effectue à la demande, comme, pour les protocoles réactifs.

A l'instar du protocole OLSR, la découverte de la topologie du réseau qui permet aux nœuds d'obtenir les informations sur la topologie du réseau s'effectue par des émissions périodiques des messages de contrôle TC (*Topology Control*) et des messages *Hello*. Le calcul de routes entre deux nœuds d'extrémité s'effectue uniquement à la demande, lorsque la source possède des paquets de données à envoyer.

Ce calcul permet à la source d'obtenir un ensemble de routes vers la destination. Pour envoyer les paquets de données, le protocole MP-OLSR utilise le routage par la source (*source routing*), c'est-à-dire que chaque paquet de données émis contient la liste de tous les nœuds à traverser depuis la source jusqu'à la destination.

4.2.1.6 On-demand Routing protocol with Backtracking (ORB) [TCC06]

Le protocole ORB [TCC06] construit des routes multiples non identiques sans autre exigence sur leur degré de similitude, par découverte et utilise la technique des caches de données lors de la phase d'acheminement des données (*Data Delivery*). Comme les autres protocoles réactifs, une source S souhaitant transmettre des données à une destination D vers laquelle elle ne possède pas de route, initie une découverte de routes.

Un nœud intermédiaire i qui reçoit une requête de route *RREQ* d'un voisin j procède comme suit :

- C'est la première requête reçue lors de cette découverte. Le nœud i crée une nouvelle entrée dans sa table de routage ayant pour destination la source S. Pour cette entrée, il incrémente le nombre de saut hc de la requête et affecte cette valeur à son champ hc_S^i, puis enregistre le nœud voisin j comme son nœud primaire de retour. Après ces modifications, le nœud i rediffuse la requête *RREQ* en mettant à jour son champ hc.

- Sinon, la requête reçue est une copie. Un nœud traite une copie de paquet RREQ dont le nombre de saut incrémenté est inférieur à celle de la route déjà connue c'est-à-dire $hc_s^j < i.hc$. Dans ce cas, le nœud j est ajouté à la liste des nœuds alternatifs de retour (*ARNL*) vers la source S. Pour réduire le nombre de messages de contrôle, un nœud intermédiaire ORB ne transmet jamais une copie de RREQ, elles sont supprimées.

La destination génère une réponse de route RREP à la réception de chaque *RREQ* tant que le nombre de routes créées est inférieur à K (nombre maximum de routes maintenues par la destination). Lorsqu'il reçoit un premier paquet *RREP* d'un voisin j, un nœud intermédiaire i enregistre ce nœud voisin comme son nœud primaire d'acheminement ensuite il retransmet le paquet vers son nœud primaire de retour (*prn*). Les nœuds émetteurs des copies de *RREP* sont enregistrés dans la liste des nœuds primaires *AFNL (Alternate Forward Node List)*. Un nœud intermédiaire qui reçoit plus d'une réponse *RREP* par découverte se déclare comme *checkpoint* pour cette destination (*ie* il met son champ *cp* pour cette entrée à *'vrai'*).

Notons qu'un nœud intermédiaire ORB transmet une seule réponse RREP par découverte de routes même s'il possède plusieurs routes pour joindre la destination *ARNL* non vide : pas de duplication de réponses RREP ni de transmission de copies de RREP sur les routes secondaires comme dans AOMDV et MDYMO. Un nœud

Dest	*hc*	*prn*	*ARNL*	*pfn*	*AFNL*	*cp*	*k*	*db*
Identifiant de la destination	Nombre de sauts	Nœud primaire de retour	Liste des nœuds secondaires de retour	Nœud primaire d'acheminement	Liste des nœuds secondaires de retour	(*Ckeckpoint flag*)	Nombre de RREP transmis par la destination *d*	Buffer des données

TABLE 4.1 – Table de routage d'un nœud i

utilise sa liste *ARNL* uniquement lorsqu'il détecte une panne de communication avec son nœud primaire de retour.

A la réception des réponses de routes, la source commence la phase d'acheminement (*Data Delivery*) vers la destination en transférant ses données à son nœud primaire d'acheminement (*pfn*). Durant cette phase, les nœuds *checkpoint* bufférisent chaque paquet de données reçu durant une période T_c prédéfinie ; ensuite transmettent le paquet de données à leur nœud primaire d'acheminement (la route primaire). Lorsque la route primaire tombe en panne (détectée par le *checkpoint* lui-même ou à la réception d'un *RERR*), le nœud *checkpoint* vérifie si la durée du compteur de son buffer n'est pas encore écoulée et s'il possède une ou plusieurs routes secondaires (dans son *AFNL*) : il remplace son nœud primaire de retour *prn*(*Primary return node*) par le premier nœud de la liste *ARNL* et envoie la donnée par la route secondaire. Dans le cas contraire, il indique qu'il n'est plus *chechkpoint* (*cp=NULL*) et supprime le paquet de données.

4.2.1.7 Protocoles *multipath* utilisant la fiabilité

Les protocoles *multipath* précédents utilisent comme critère de sélection le minimum de sauts. Ils considèrent qu'une route est meilleure qu'une autre, quand elle comporte moins de nœuds. Comme le nombre d'éléments réseau qui composent la route est minimal, on peut considérer que cela diminue la probabilité de rupture de la route. Cependant, utiliser uniquement comme critère le plus court chemin peut conduire à la réduction de la qualité de la route en termes de fiabilité et de bande passante, parce que moins il y a de sauts, plus les nœuds sont éloignés et plus la qualité du lien décroît.

MP-DSR [LLP+01], LET [DZSN08], BSR [GYS05], quant à eux, utilisent la fiabilité prévisionnelle et la durée de vie prédite comme critère. Ils permettent ainsi d'améliorer le taux de livraison des paquets (PDR). MP-DSR établit un ensemble de routes qui peuvent satisfaire à une exigence minimum de fiabilité de bout en bout. Les protocoles LET et BSR construisent un ensemble de routes qui assurent la meilleure fiabilité de bout en bout.

Cette approche peut être intéressante lorsque le protocole de routage est utilisé pour faire un partage de charge entre les différentes routes. Cependant, elle n'est pas adaptée pour améliorer la robustesse, où la route secondaire est utilisée unique-

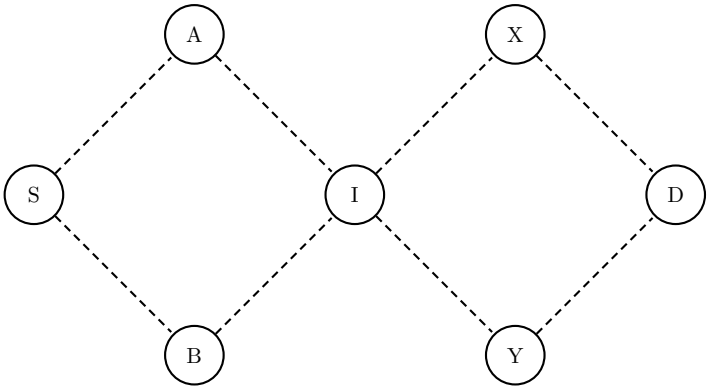


FIGURE 4.3 – Topologie exemple

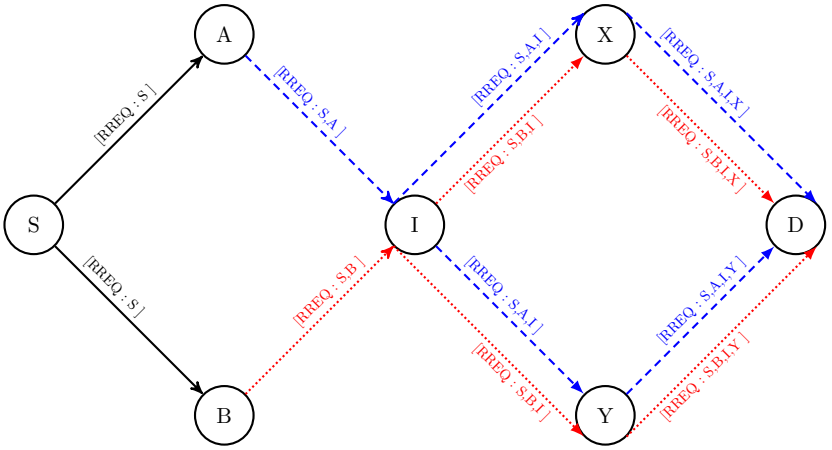
ment après la défaillance de la route primaire. La route la plus fiable construite à chaque découverte, est choisie comme route primaire. En conséquence, il y a très peu de chance qu'une route secondaire soit en bon état après la rupture d'une route primaire ; car la route secondaire possède une fiabilité inférieure à celle de la route primaire.

4.2.2 Degré de similitude et stratégie de routage

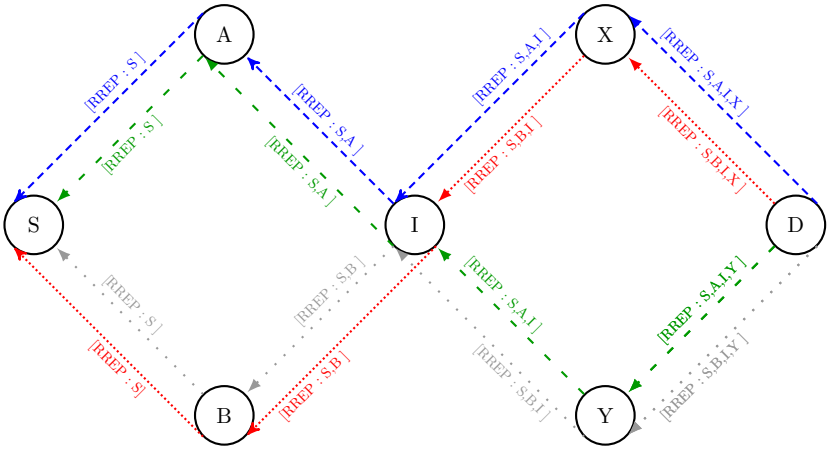
L'utilisation de la stratégie de routage par la source dans le contexte *multipath* permet une simplification du calcul du degré de similitude entre les routes primaire et secondaires. Cependant, dans le contexte *multipath*, la gestion des caches de routes par les nœuds intermédiaires est assez complexe. A cet effet, dans les protocoles *multipath*, les nœuds intermédiaires n'utilisent pas des caches de routes. Dans cette stratégie, le champ enregistrement de routes de chaque requête de routes RREQ reçue par la destination contient l'ensemble des nœuds traversés depuis la source jusqu'à elle. Le calcul du degré de similitude entre deux routes s'effectue par la destination et consiste à une recherche de chaque nœud de la route primaire dans le champ enregistrement de la seconde route. En cas de non utilisation des caches de routes par les nœuds intermédiaires, seule la source est capable de procéder au recouvrement (recouvrement de bout en bout).

Pour construire le maximum de routes, les nœuds intermédiaires diffusent toutes les requêtes RREQ reçues dans leur voisinage et la destination émet une réponse de routes à chaque requête reçue (figures 4.4(a) et 4.4(b)). Ce qui entraîne une génération et une transmission d'un nombre important de messages de contrôle.

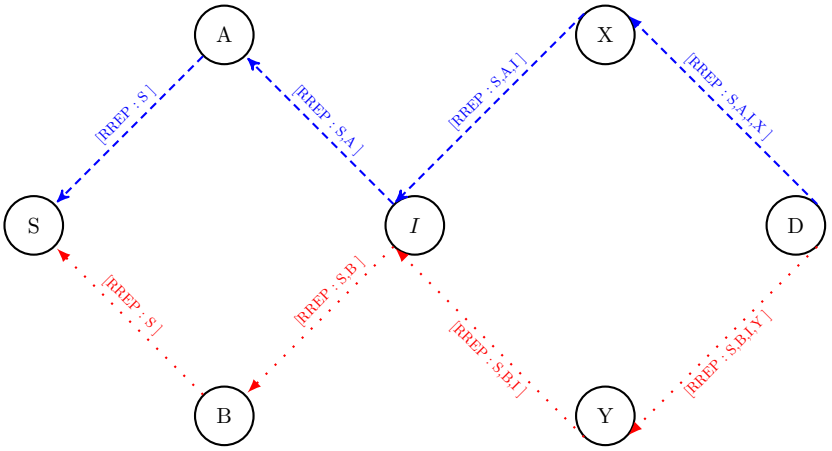
Pour limiter le nombre de messages de contrôle, d'autres protocoles (comme SMR [LG02]) proposent de ne transmettre que les requêtes reçues des voisins différents. Cette approche présente l'inconvénient de réduire le nombre de routes apprises (donc construites) par la destination et la source (figure 4.4(c) : deux routes).



(a) Phases de requêtes de routes disjointes en liens ou non

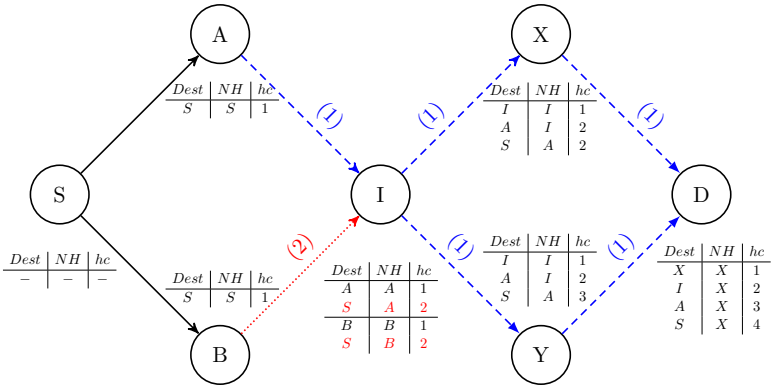


(b) Maximum de routes possibles : Phases de réponses de routes $R_{Pri} = (S \leftrightarrow A \leftrightarrow I \leftrightarrow X \leftrightarrow D)$, $R_{Sec1} = (S \leftrightarrow A \leftrightarrow I \leftrightarrow Y \leftrightarrow D)$, $R_{Sec2} = (S \leftrightarrow B \leftrightarrow I \leftrightarrow X \leftrightarrow D)$, $R_{Sec3} = (S \leftrightarrow B \leftrightarrow I \leftrightarrow Y \leftrightarrow D)$

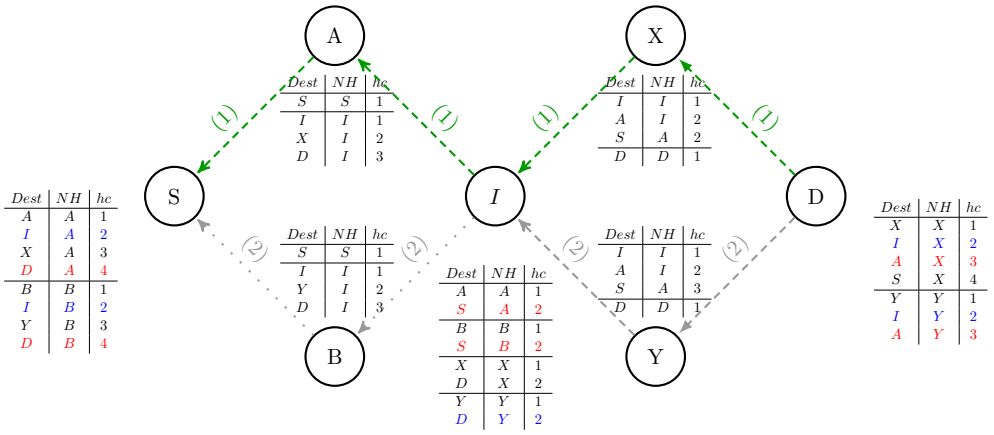


(c) Routes disjointes en lien : Phases de réponses de routes $R_{Pri} = (S \leftrightarrow A \leftrightarrow I \leftrightarrow X \leftrightarrow D)$ et $R_{Sec} = (S \leftrightarrow B \leftrightarrow I \leftrightarrow Y \leftrightarrow D)$

FIGURE 4.4 – Routage par la source : Découverte de routes entre S et D



(a) Phases de requêtes de routes disjointes en liens ou non disjointes



(b) Phases de réponses de routes disjointes en liens ou non disjointes

FIGURE 4.5 – Routage par destination : Découverte de routes entre S et D

La principale difficulté dans la stratégie de routage par destination est le calcul du degré de similitude entre les routes construites. Une première approche consiste à utiliser l'option d'accumulation des routes pour permettre à la destination de disposer des informations sur tous les nœuds traversés par chaque requête de routes (comme dans DYMOM [KPK+07]). Dans ce cas, la destination reste le nœud responsable du calcul du degré de similitude. Outre l'augmentation de la taille des paquets de requêtes, cette solution permet de construire toutes les routes possibles uniquement lorsqu'elles doivent être disjointes en nœuds.

Une autre solution est de partager le contrôle du degré de similitude entre les nœud traversés par les requêtes et leurs réponses. Ceci nécessite la mise en place d'algorithmes efficaces (AOMDV [MD01, MD06] et AODVM[YKT03]) (figure 4.5).

Si l'objectif du protocole *multipath* est la construction des routes disjointes en nœuds : la stratégie de routage par la source est la plus efficace en termes de calcul (simplification du calcul du degré de similitude).

Cependant, lorsque les routes construites doivent être disjointes en liens ou non disjointes, la stratégie de routage par destination génère moins de messages de

contrôle et construit plus de routes que la stratégie de routage par la source (voir les figures 4.4 et 4.5). De plus, si un recouvrement par segment est mis en œuvre, la stratégie de routage distribué procède à un recouvrement plus rapide.

4.3 Analyse comparative

Dans cette section, nous proposons une comparaison analytique entre les protocoles *unipath* et *multipath* en termes de temps de restauration et de fiabilité. L'objectif de la section est de répondre aux questions suivantes :

- Qu'apporte la redondance de routes et quand est-elle intéressante ?
- Quels sont les avantages et les inconvénients des deux schémas de recouvrement ?
- Quel type de recouvrement choisir en fonction du mécanisme de détection de panne de liens ?

Dans la première partie, nous montrons l'apport de la redondance de routes en termes de temps de restauration. Pour cela, une formulation analytique du temps de restauration des protocoles *unipath* et*multipath* est proposée. Nous en déduisons le choix de mécanismes adaptés pour la détection de panne de communication entre nœuds adjacents en nous appuyant sur deux critères : le temps de restauration de service et l'*overhead* de niveau routage généré. Pour améliorer l'efficacité de la redondance de routes, nous proposons de maintenir la route secondaire lorsque la primaire est utilisée. Nous montrons analytiquement l'avantage de cette proposition.

La seconde partie étudie les deux approches de recouvrement en termes de fiabilité. Nous formulons une expression analytique de la fiabilité des deux schémas de recouvrement (recouvrement de bout en bout et segmenté).

4.3.1 Temps de restauration de service : *Unipath* et *Multipath*

Si la redondance de routes est utilisée pour assurer une reprise rapide du trafic, son intérêt dépend de la probabilité qu'une route secondaire soit en bon état, lorsque la route primaire tombe en panne. Pour montrer analytiquement l'avantage de la redondance de routes, il est nécessaire de comparer les temps de restauration d'un protocole *unipath* et d'un protocole *multipath*. Pour cela, nous formulons le temps de restauration de deux types de recouvrement d'un protocole *multipath* : recouvrement de bout en bout et recouvrement segmenté.

Dans cette analyse, nous supposons que le nœud responsable du recouvrement d'un protocole *multipath* possède deux routes (une primaire Ro_{pri} et une secondaire Ro_{sec}) disjointes en nœud ou en lien en fonction du type de recouvrement.

Notations

$T_{R_{UP-Reac}}$ –	Temps de restauration de service d'un protocole *Unipath* réactif
$T_{R_{MP}}$ –	Temps de restauration de service d'un protocole *Multipath*
$p_{secVald}$ –	Probabilité qu'une route secondaire fonctionne après une panne sur la route primaire ($0 \leq p_{secVald} \leq 1$)
$p_{use-Sec}$ –	La probabilité d'utiliser une route secondaire après une panne sur la route primaire
T_d –	Temps de la détection des pannes
T_c –	Temps de la corrélation des pannes
T_n –	Temps de la notification des pannes
T_{or} –	Temps de l'opération de recouvrement des pannes
$T_{DR} = T_{or}$ –	Temps de découverte de la route d'un protocole réactif (*Unipath* ou *Multipath*)
T_{rt} –	Temps de la reprise du trafic

L'occurrence d'une panne sur une route active entraîne une restauration de service. La restauration de service est composée des cinq phases : la détection, la corrélation, la notification et l'opération de recouvrement de pannes, et la reprise du trafic.

La détection de la panne de communication est mise en œuvre par les mécanismes présentés dans le chapitre 1 soit uniquement par la couche routage soit par un cross-layer entre la couche routage et la sous-couche MAC. Quant à la notification de pannes dans un protocole réactif, elle consiste à une génération et une diffusion de message d'erreur *RERR* depuis le nœud détecteur jusqu'au nœud responsable du recouvrement.

4.3.1.1 Routage *unipath*

Dans un protocole *unipath*, le nœud responsable du recouvrement est la source S. Après la réception de la notification, elle procédera à une opération de recouvrement qui consiste à initier une nouvelle découverte de routes vers la destination. Cette découverte sera effectuée par une émission de requête *RREQ* par la source vers la destination et une émission de réponse *RREP* par la destination vers la source.

La durée de la restauration de service d'un protocole réactif *unipath* est formulée comme suit (cf. Chapitre 1 formule 1.8) :

$$\begin{aligned} T_{R_{UP-Reac}} &= T_{d_{Route(S)}} + T_{or} + T_{rt} \\ &= T_{d_{(n_i,n_{i+1})}} + T_{n[n_i \to S]} + T_{or} + T_{rt} \\ &= T_{d_{(n_i,n_{i+1})}} + T_{RERR[n_i \to S]} + T_{or} + T_{rt} \end{aligned} \quad (4.1)$$

Où n_i est le nœud détecteur de la panne et initiateur de la phase de notification.

En supposant que la panne s'effectue à mi-chemin entre la source et la destination, la durée de la notification de pannes (entre les nœuds i et S) être approximée par la moitié du temps nécessaire au parcours d'un message de contrôle ($RREQ$ ou $RREP$) entre la source S et la destination D (ou inversement).

$$T_{RERR[n_i \to S]} \approx \frac{T_{RREQ[S \to D]}}{2} \approx \frac{T_{RREP[D \to S]}}{2} \tag{4.2}$$

La durée du recouvrement de pannes correspond au temps nécessaire à une découverte de routes (une émission de requête RREQ et une émission de réponse RREP).

$$\begin{aligned} T_{or} = T_{DR} &= T_{RREQ[S \to D]} + T_{RREP[D \to S]} \\ &\approx 4 \times T_{RERR[n_i \to S]} \end{aligned} \tag{4.3}$$

4.3.1.2 Routage *multipath*

La restauration de service d'un protocole *multipath* est un peu différente de celle d'un protocole *unipath*. Tout dépend de l'état (panne ou non) de la route secondaire Ro_{sec} lorsque nœud responsable du recouvrement reçoit la notification de panne de la route primaire Ro_{pri}.

Lorsque le nœud responsable du recouvrement d'un protocole *multipath* reçoit cette notification, il bascule immédiatement le trafic sur la route secondaire (phase de reprise du trafic) sans lancer une nouvelle découverte de route. Dans les protocoles *multipath* présentés précédemment, la source procède ainsi dans tous les cas, car au moment de la réception de la notification, elle ne connait pas l'état de la route secondaire. En effet, ces protocoles n'utilisent aucun mécanisme pour vérifier la validité d'une route secondaire Ro_{sec}.

La durée de la restauration de service d'un protocole *multipath* est formulée en fonction de l'état de la route secondaire. Notons $p_{secVald}$ la probabilité que la route secondaire soit en bon état au moment de la réception des messages d'erreur RERR par le nœud de recouvrement N_{rec}. Le temps nécessaire à la restauration de service d'un protocole *multipath* est :

$$T_{RS_{MP}} = \left(T_{d_{Route(N_{rec})}}\right)_{Pri} + [p_{secVald} \times \{T_{RS_{MP}}\}_{Cas1}] + [(1 - p_{secVald}) \times \{T_{RS_{MP}}\}_{Cas2}] \tag{4.4}$$

Cas 1 : La route secondaire Ro_{sec} est en bon état au moment de la réception de la notification de pannes $RERR$ par le nœud responsable du recouvrement N_{rec}.

$$\{T_{RS_{MP}}\}_{Cas1} = T_{rt} \tag{4.5}$$

Le nœud N_{rec} bascule immédiatement la communication sur sa route secondaire.

Cas 2 : La route secondaire Ro_{sec} est déjà rompue mais le nœud responsable du recouvrement N_{rec} n'est pas au courant de cette information. Dans un premier temps, il basculera le trafic de données sur sa route secondaire qui devient alors active. L'émission de données conduira à une détection de pannes de communication par les nœuds adjacents à l'élément défaillant (lien ou nœud). Après la phase de corrélation, les messages d'erreurs de routes *RERR* vont informer la source de l'état de pannes de la route secondaire qui initiera une nouvelle découverte puis effectuera une reprise du trafic.

$$\begin{aligned} \{T_{RS_{MP}}\}_{Cas2} &= (T_{rt} + T_{d_{Route}})_{Sec} + T_{or} + T_{rt} \\ &= \left(T_{rt} + T_{d_{(n_j,n_{j+1})}} + T_{n[n_j \to S]}\right)_{Sec} + T_{or} + T_{rt} \end{aligned} \tag{4.6}$$

Où le nœud n_j détecte la panne de route secondaire et initie la phase de notification.

Note : Pour plus details sur les équations 4.8, 4.9, 4.11 et 4.23 ; leurs démonstrations sont données en annexe, section C.

4.3.1.2.1 Recouvrement de bout en bout

Dans cette stratégie de recouvrement, le nœud responsable du recouvrement N_{rec} est la source des données S. Donc, son temps de restauration est :

$$\begin{aligned} T_{RS_{MP(E2ER)}} &= \left[\left(T_{d_{Route(S)}}\right)_{Pri} + T_{or} + T_{rt}\right] - (p_{secVald} \times T_{or}) \\ &\quad + [(1 - p_{secVald}) \times (T_{rt} + T_{d_{Route}})_{Sec}] \qquad (4.7) \\ &= \left[(1 - p_{secVald}) \times T_{RS_{UP-Reac}}\right] + \left(T_{rt} + T_d + T_{n[j \to S]}\right) \qquad (4.8) \end{aligned}$$

Avec $T_{d_{(n_j,n_{j+1})}} = T_{d_{(n_j,n_{j+1})}} = T_d$ et $T_{n[n_j \to S]} = T_{n[n_j \to S]}$ (en supposant que les nombres de sauts entre $n_i \to S$ et $n_j \to S$ sont égaux).

4.3.1.2.2 Recouvrement par segment de routes

Dans ce cas, le basculement du trafic sur la route secondaire est assuré par un nœud intermédiaire NI qui est situé entre le nœud détecteur n_i et la source S.

$$\begin{aligned} T_{RS_{MP(SR)}} &= \left[\left(T_{d_{Route(NI)}}\right)_{Pri} + T_{or} + T_{rt}\right] - (p_{secVald} \times T_{or}) \\ &\quad + [(1 - p_{secVald}) \times (T_{rt} + T_{d_{Route}})_{Sec}] \end{aligned} \tag{4.9}$$

Le temps de restauration du recouvrement par segment est inférieur à celui de la stratégie de bout en bout sachant que le nœud NI est plus proche du nœud détecteur n_i que la source S.

$$\begin{aligned} T_{n[n_i \to NI]} &< T_{n[n_i \to S]} \\ T_{d_{(n_i,n_{i+1})}} + T_{n[n_i \to NI]} &< T_{d_{(n_i,n_{i+1})}} + T_{n[n_i \to S]} \\ \left(T_{d_{Route(NI)}}\right)_{Pri} &< \left(T_{d_{Route(S)}}\right)_{Pri} \\ T_{RS_{MP(SR)}} &< T_{RS_{MP(E2E)}} \end{aligned} \tag{4.10}$$

Après avoir formulé le temps de restauration de service des types de recouvrement d'un protocole *multipath*, nous nous intéressons par la suite à montrer analytiquement l'avantage de la redondance de routes.

4.3.1.3 Avantage de la redondance de routes

Pour évaluer l'avantage du routage *multipath* en termes de réactivité aux changements de la topologie, nous comparons les temps de recouvrement d'un protocole *unipath* (équation 4.1) et d'un protocole *multipath* avec stratégie de recouvrement de bout en bout (équation 4.8). La durée de la restauration d'un protocole *unipath* est supérieure à celle d'un protocole *multipath* si :

$$p_{secVald} \geq \frac{T_{rt} + T_d + T_n}{T_d + T_n + T_{or} + T_{rt}} \tag{4.11}$$

Dans un protocole de routage, la phase de reprise du trafic est presque instantanée ($T_{rt} \approx 0$). L'équation précédente peut donc être réduite comme suit :

$$p_{secVald} \geq \frac{T_d + T_n}{T_d + T_n + T_{or}} = \frac{T_d + T_{RERR}}{T_d + T_{RERR} + T_{DR}} \tag{4.12}$$

La valeur de la probabilité $p_{secVald}$ dépend du type de mécanismes de détection utilisés par le protocole de routage. A la suite, nous étudions la valeur de cette probabilité $p_{secVald}$ en fonction de trois mécanismes de détection présentés dans le chapitre précédent : utilisation de la notification de la couche liaison *NNL*, les messages *Hello*, les acquittements de niveau routage *ANR*.

4.3.1.3.1 Notification de la couche liaison Au chapitre 1, nous avons formulé le temps de détection de ce mécanisme comme suit (équation 1.15) :

$$E\left\{T_{d_{(n_i,n_{i+1})}}\right\}_{(NNL)} = T_{att-Paq} + T_{retrans-Data} \tag{4.13}$$

Le temps $T_{att-Paq}$ correspond au temps de parcours d'une donnée entre la source et le nœud détecteur. Il est approximativement égale à la durée de la phase de notification (émission d'un message d'erreur *RERR* par le nœud détecteur vers la source).

$$T_{att-Paq} \approx T_{RERR} \tag{4.14}$$

La durée des sept émissions infructueuses du paquet de données $T_{retrans-Data}$ est très petite (de l'ordre de la milliseconde) comparée à $T_{att-Paq}$. Nous pouvons réécrire, le temps de détection comme suit :

$$E\left\{T_{d_{(n_i,n_{i+1})}}\right\}_{(NNL)} \approx T_{att-Paq} \approx T_{RERR} \approx \frac{T_{DR}}{4} \tag{4.15}$$

En utilisant les équations 4.3 et 4.15 dans la formule 4.12, nous obtenons :

$$\begin{aligned} \{p_{secVald}\}_{(NNL)} &\geq \frac{T_d + T_{RERR}}{T_d + T_{RERR} + T_{DR}} = \frac{\frac{T_{DR}}{2}}{\frac{T_{DR}}{2} + T_{DR}} \\ \{p_{secVald}\}_{(NNL)} &\geq \frac{1}{3} \end{aligned} \tag{4.16}$$

La restauration de service d'un protocole *multipath* est plus rapide que celle d'un protocole *unipath* si la probabilité que la route secondaire soit en bon en état après la panne de la route primaire est supérieure à 1/3.

4.3.1.3.2 Mécanismes de détection par le protocole de routage Un protocole de routage détecte les ruptures de communication sur les routes actives en utilisant soit les messages *Hello* soit les acquittements de niveau routage. Dans ces deux mécanismes, la maintenance des routes actives s'effectue de manière périodique. Les détections de pannes ne sont pas liées uniquement à l'émission des paquets de données comme précédemment.

La valeur de la probabilité $p_{secVald}$ est bornée comme suit pour que la durée de la restauration des protocoles *multipath* soit inférieure à celle des protocoles *unipath* (équations 4.3 et 4.12) :

$$\begin{aligned} p_{secVald} &\geq \frac{T_d + T_{RERR}}{T_d + T_{RERR} + T_{DR}} = \frac{T_d + \frac{T_{DR}}{4}}{T_d + \frac{T_{DR}}{4} + T_{DR}} \\ p_{secVald} &\geq \frac{(4 \times T_d) + T_{DR}}{(4 \times T_d) + (5 \times T_{DR})} \end{aligned} \tag{4.17}$$

La valeur de la probabilité $p_{secVald}$ dépend de la durée du processus de détection de pannes T_d et celle de la découverte de routes T_{DR}.

- *Message Hello :* La valeur moyenne du temps de détection d'un protocole de routage utilisant les messages *Hello* a été formulée dans l'équation 1.12 et 1.13.

$$E\left\{T_{d_{(n_i,n_{i+1})}}\right\}_{(Hello)} = 1.5 \text{ sec} \tag{4.18}$$

  En remplaçant T_{DR} par sa valeur moyenne pour la détection avec les messages *Hello* dans l'équation 4.17, nous obtenons :

$$\{p_{secVald}\}_{(Hello)} \geq \frac{6 + T_{DR}}{6 + (5 \times T_{DR})} \tag{4.19}$$

- *Acquittement de niveau routage :* Ce mécanisme de détection a été proposée dans le protocole de routage DSR [JHM07]. Au chapitre 1, nous avons formulé le temps moyen avant la détection dans ce mécanisme dans les équations 1.16 et 1.17.

$$E\left\{T_{d_{(i,i+1)}}\right\}_{(ANR)} = 0.125 \text{ sec} \tag{4.20}$$

En remplaçant le durée de la détection par sa valeur dans l'équation 4.17, nous obtenons :

$$\{p_{secVald}\}_{(ANR)} \geq \frac{0.5 + T_{DR}}{0.5 + 5 \times T_{DR}} \tag{4.21}$$

4.3.1.4 Choix du type de routage en fonction du mécanisme de détection utilisé

Nous comparons le routage *unipath* et *multipath* en termes de temps de restauration en fonction du mécanisme utilisé pour détecter les pannes entre nœuds adjacents.

La figure 4.6 montre l'influence de la durée de la découverte de routes T_{DR} sur la probabilité $p_{secVald}$ (équations 4.16, 4.19 et 4.21).

Lorsque les pannes sont détectées par les notifications de la couche liaison, la valeur de la probabilité est indépendante de la durée de la découverte de routes T_{DR}. Elle doit être supérieure ou égale à 1/3 pour que la restauration s'effectue plus rapidement dans l'approche *multipath* que dans le routage *unipath*.

Concernant les deux autres mécanismes, tout dépend du temps de la découverte de route. Nous observons que lorsque la durée de découverte augmente, la valeur exigée pour la probabilité $p_{secVald}$ décroît. L'avantage d'utiliser de la redondance de routes est fortement corrélé avec la durée de la découverte T_{DR}. Plus cette durée est grande, meilleure sera la redondance de routes.

Dans les protocoles *unipath* AODV [PBRD03] et DYMO [CP10] comme dans leurs extensions *multipath*, la durée de la découverte de route doit être inférieure à 2 sec. C'est-à-dire une nouvelle découverte de routes est initiée en cas de réception de réponse *RREP* par la source après cette durée. Les bornes inférieures de la probabilité $p_{secVald}$ en fonction des mécanismes de détection sont respectivement :

$$\{p_{secVald}\}_{(NNL)} \geq \frac{1}{3}$$

$$\{p_{secVald}\}_{(Hello)} \geq 0.5$$

$$\{p_{secVald}\}_{(ANR)} \geq \frac{5}{21}$$

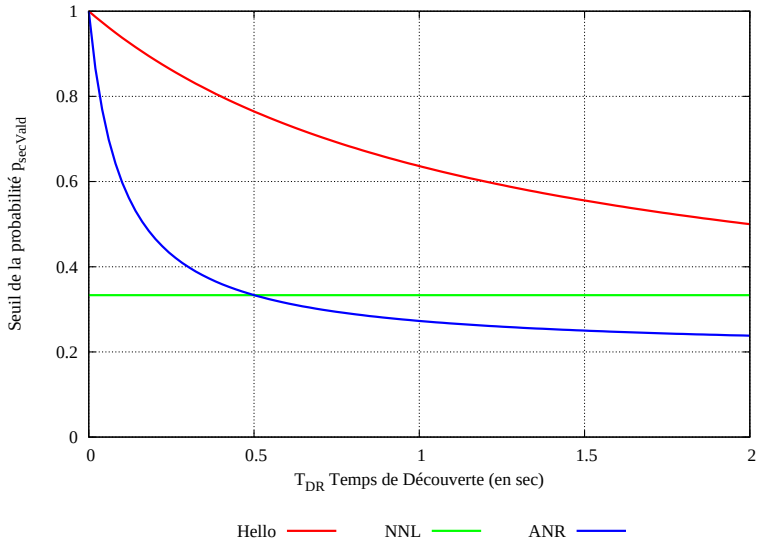


FIGURE 4.6 – Seuil de la probabilité $p_{secVald}$ vs Durée de la découverte de routes T_{DR}

Contrairement à ce qu'on aurait pu penser intuitivement, le routage *multipath* n'améliore pas toujours les performances du réseau par rapport au routage *unipath*. Lorsque les pannes entre nœuds adjacents sont détectées par les mécanismes de niveau routage (*Hello* et *acquittement de route ANR*), il serait intéressant d'avoir une approche adaptative pour les constructions ou non de plusieurs routes. Par exemple, utiliser un routage *unipath* si le temps de découverte $T_{DR} < 0.5$ sec ; sinon un protocole de routage *multipath*.

Nous avons montré au chapitre 1 que l'utilisation des notifications de la couche liaison est la meilleure technique en termes en compromis entre le temps de restauration et de coût quelle que soit l'approche de routage *unipath* ou *multipath*. Nous appuierons donc sur ce mécanisme aussi bien en routage *unipath* qu'en routage *multipath*. Dans ce cas, nous n'avons pas besoin d'auto-adaptabilité car l'avantage ne dépend pas de la durée de la découverte. Pour améliorer l'approche *multipath*, il faut mettre en place des techniques qui permettent d'éviter d'utiliser des routes secondaires rompues.

4.3.1.5 Proposition : Maintenir les routes secondaires

Pour améliorer le gain des protocoles *multipath* en termes de rapidité de restauration, il est nécessaire de mettre en place des mécanismes permettant d'augmenter la probabilité $p_{secVald}$. Une solution consiste à maintenir les routes secondaires. Dans ce cas, la source dispose à tout moment de l'état (presque effectif ou courant) de la route secondaire. Quand elle reçoit la notification de pannes, le trafic est basculé sur

sa route secondaire si celle-ci n'est pas rompue sinon la source va initier une nouvelle découverte de routes.

D'une manière générale, la formule 4.4 s'écrire comme suit :

$$\begin{aligned} T_{RS_{MP(Gen)}} &= \left(T_{d_{Route(N_{rec})}}\right)_{Pri} + p_{secVald} \times \{T_{RS_{MP}}\}_{Cas1} + (1 - p_{secVald}) \\ &\times \{p_{useSecInvald} \times (T_{rt} + T_{d_{Route}})_{Sec} + T_{or} + T_{rt}\}_{Cas2} \end{aligned} \tag{4.22}$$

Où $p_{useSecInvald}$ est la probabilité d'utiliser une route secondaire invalide après la panne de la primaire.

L'objectif de la maintenance d'une route secondaire est de diminuer la probabilité $p_{useSecInvald}$.

$$p_{secVald} \geq \frac{p_{useSecInvald} \times (T_d + T_n)}{T_{or} + p_{useSecInvald} \times (T_d + T_n)} \tag{4.23}$$

Les bornes inférieures des mécanismes de détection deviennent alors :

$$\{p_{secVald}\}_{(NNL)} \geq \frac{p_{useSecInvald} \times T_{DR}}{T_{DR} \times (p_{useSecInvald} + 2)} = \frac{p_{useSecInvald}}{(p_{useSecInvald} + 2)} \tag{4.24}$$

$$\{p_{secVald}\}_{(Hello)} \geq \frac{p_{useSecInvald} \times (6 + T_{DR})}{(6 \times p_{useSecInvald}) + T_{DR} \times (p_{useSecInvald} + 4)} \tag{4.25}$$

$$\{p_{secVald}\}_{(ANR)} \geq \frac{p_{useSecInvald} \times (0.5 + T_{DR})}{(0.5 \times p_{useSecInvald}) + T_{DR} \times (p_{useSecInvald} + 4)} \tag{4.26}$$

L'intérêt de maintenir la route secondaire durant l'utilisation de la route primaire dont la panne est détectée par les notifications de la couche liaison est montré sur la figure 4.7. Nous remarquons que lorsque la source n'utilise jamais de route secondaire déjà rompue ($p_{useSecInvald} = 0$), le temps de recouvrement routage *multipath* est toujours inférieure à celui d'un protocole *unipath*.

Une première approche pour la maintenance des routes secondaires est d'utiliser les messages *Hello* entre chaque pair de nœuds adjacents. L'inconvénient de cette approche est le nombre de messages de contrôle *Hello* utilisé sur une route qu'on n'est pas certain d'utiliser. Les routes secondaires peuvent être aussi maintenues par des messages périodiques émis par la source vers la destination. L'efficacité de ce mécanisme va dépendre de la durée de la période d'émission de ces messages de contrôle. Ce mécanisme est utilisé notamment par le protocole transport SCTP pour assurer la maintenance de ses chemins secondaires.

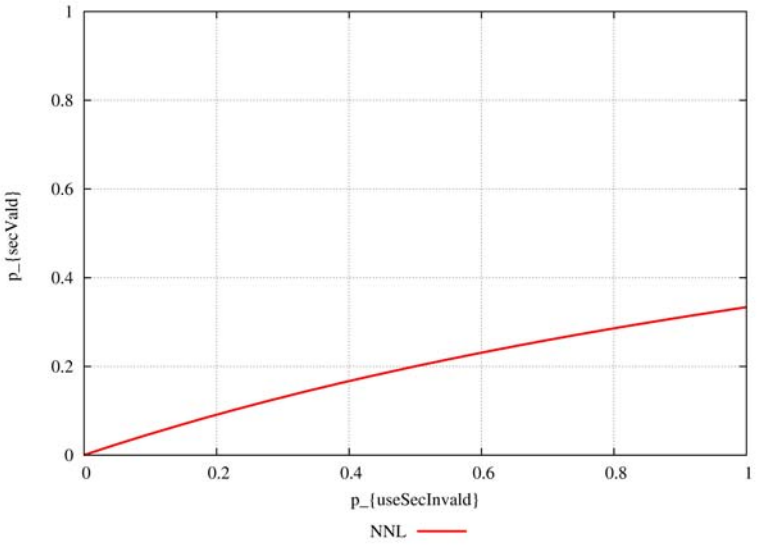


FIGURE 4.7 – $p_{secVald}$ VS $p_{useSecInvald}$

4.3.2 Modélisation analytique de la fiabilité des politiques de recouvrement

Lorsqu'une panne survient dans un réseau mobile ad hoc, en fonction de l'élément réseau protégé, différentes politiques de recouvrement peuvent être envisagées. Il existe trois stratégies de base qui sont : le recouvrement lien par lien (*link-to-link recovery*), le recouvrement de bout en bout (*end-to-end recovery*) et le recouvrement par segment de route (*segment recovery*). Dans le premier type de recouvrement, en cas panne, le trafic est basculé sur le lien alternatif (protection de lien), tandis que pour les deux autres, le trafic est redirigé soit sur une route entière secondaire soit sur un segment de route secondaire. Lorsque la nouvelle route est entièrement disjointe de la route primaire, la récupération est un recouvrement de bout en bout. Au contraire, en cas de nœuds communs deux routes, c'est une protection de segment de route qui est utilisée. De toute évidence, la mise en œuvre d'une politique de recouvrement dépend de la topologie du réseau. Dans les réseaux de faible densité, où la probabilité d'obtenir un grand nombre de routes disjointes est faible, la robustesse obtenue avec un recouvrement de bout en bout n'est pas très intéressante. Toutefois, lorsque dans une topologie de réseau où toutes les politiques de recouvrement sont applicables, une politique apportera un meilleur gain en termes de la fiabilité qu'une autre. Le problème est alors de déterminer le bon niveau de protection en fonction des différentes topologies et des caractéristiques ad hoc (portée de transmission, mobilité).

Dans cette section, nous proposons un cadre original pour évaluer l'efficacité des mécanismes de redondance. Au chapitre 1, nous avons montré que le recouvrement lien par lien n'a aucun avantage en termes de robustesse dans un réseau MANET homogène (c'est-à-dire que tous les nœuds utilisent la même technologie) (voir sec-

tion 1.2.2.2). Dans [BP11a, BP11b], nous étudié, formulé et comparé les fiabilités trois politiques dans une architecture hétérogène (WiFi/Zigbee) proposée. Dans ces travaux, nous nous intéressés à une topologie particulière.

Dans cette section, nous nous intéressons à un réseau mobile homogène. A cet effet, nous formulons une expression analytique de la fiabilité de l'ensemble des routes (primaire et secondaire) des politiques de recouvrement de bout en bout et par segment de routes. Ensuite, nous évaluons les performances de ces schémas de recouvrement en fonction de la durée de la communication.

4.3.2.1 Formulation analytique

Nous utilisons l'approche des blocs de diagrammes pour formuler la fiabilité des schémas de recouvrement. La fiabilité d'un système composé d'équipements élémentaires en série est égal au produit des fiabilités de ces équipements élémentaires. Lorsque les équipements sont en parallèle, ce sont les défiabilités qui se multiplient.

Dans un réseau, les équipements élémentaires sont les nœuds et les liens. Au chapitre 1, nous avons formulé la fiabilité d'une route construite par un protocole *unipath* entre les nœuds n_0 et n_m (équation 1.4). Cette fiabilité est égale au produit des fiabilités de tous les équipements élémentaires composant la route. L'expression de cette fiabilité est utile pour formuler la fiabilité des schémas de recouvrement. Comme dans la section précédente consacrée au temps de restauration, nous supposons que le réseau est assez dense pour construire à chaque découverte deux routes : une primaire Ro_{pri} et une secondaire Ro_{sec}.

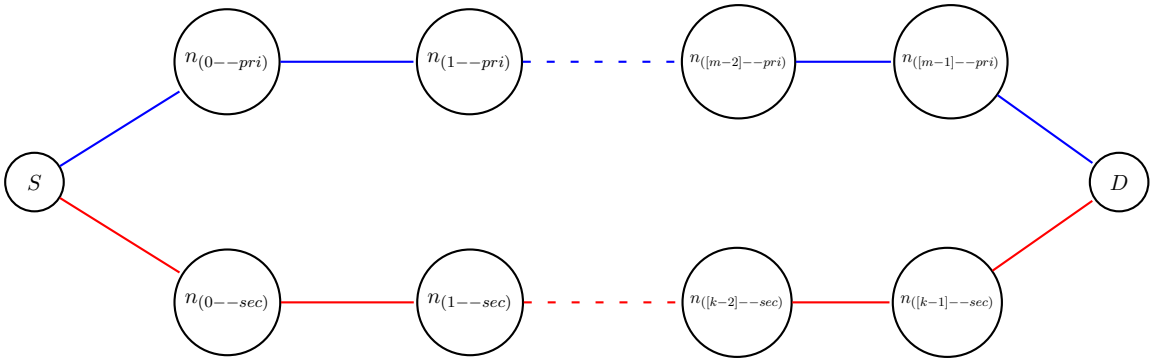
Notons respectivement la fiabilité d'un nœud n_i et celle du lien entre n_i et n_{i+1}, R_{n_i} et R_{L_i}.

4.3.2.1.1 Recouvrement de bout en bout La fiabilité du recouvrement de bout en bout nommée $R_{E2E_{(S\leftrightarrow D)}}$ dépend de celle des routes disjointes (primaire et secondaire) construites entre les nœuds source S et destination D (figure 4.8(a)). Il existe deux équipements élémentaires communs à ces deux routes qui sont les nœuds d'extrémité : S et D. Après une décomposition des routes en série/parallèle, nous obtenons :

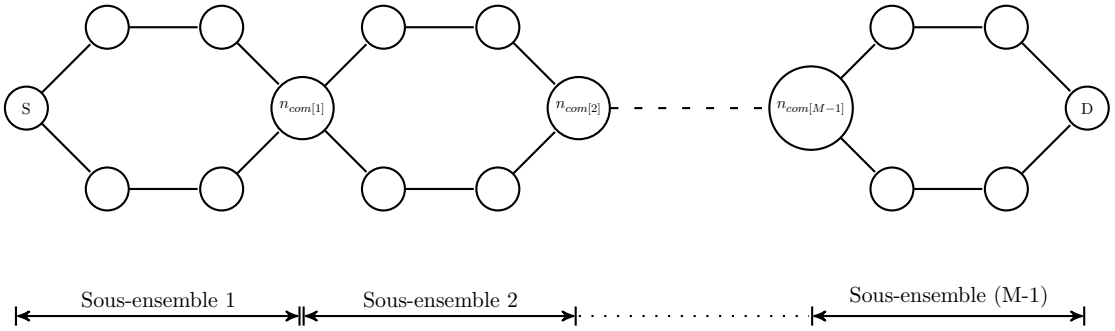
$$R_{E2E_{(S\leftrightarrow D)}} = R_S \times R_D \times \left[1 - \left(1 - \tilde{R}_{Ro_{pri_{(S\leftrightarrow D)}}}\right) \times \left(1 - \tilde{R}_{Ro_{sec_{(S\leftrightarrow D)}}}\right)\right] \quad (4.27)$$

Où :

- La fiabilité $\tilde{R}_{Ro_{pri_{(S\leftrightarrow D)}}}$ est égale au produit des fiabilités de tous les équipements élémentaires qui composent **la route primaire** sauf celles des nœuds



(a) Recouvrement de bout en bout



(b) Recouvrement par segment de routes

FIGURE 4.8 – Politiques de recouvrement

source S et destination D. Nous supposons que la route primaire est composée de m liens, et notons les nœuds de cette route $n_{(j--pri)}$, $\forall\ (0 \leq j \leq m-1)$.

$$\tilde{R}_{Ro_{pri}(S\leftrightarrow D)} = R_{L_{\left[S,n_{(0--pri)}\right]}} \times \left[\prod_{j=0}^{m-1} R_{n_{(j--pri)}} \times R_{L_{(j--pri)}}\right] \times R_{L_{\left[n_{([m-1]--pri)},D\right]}} \quad (4.28)$$

- La fiabilité $\tilde{R}_{Ro_{sec}(S\leftrightarrow D)}$ est égale au produit des fiabilités de tous les équipements élémentaires qui composent **la route secondaire** sauf celles des nœuds source S et destination D. Nous supposons que la route secondaire possède k liens, et notons les nœuds appartenant à cette route $n_{(j--sec)}$, $\forall\ (0 \leq j \leq k-1)$.

$$\tilde{R}_{Ro_{sec}(S\leftrightarrow D)} = R_{L_{\left[S,n_{(0--sec)}\right]}} \times \left[\prod_{j=0}^{k-1} R_{n_{(j--sec)}} \times R_{L_{(j--sec)}}\right] \times R_{L_{\left[n_{([k-1]--sec)},D\right]}} \quad (4.29)$$

La politique de recouvrement de bout en bout résiste aux défaillances simultanées de plusieurs éléments réseau (liens, nœuds) sur la route primaire. Ce processus de

recouvrement peut être effectué par les deux stratégies de routage (routage par source et par destination). Bien que la complexité du processus de recouvrement soit simplifiée, car elle est mise en œuvre uniquement par les nœuds d'extrémité, cette politique souffre de quelques inconvénients. En cas de pannes simultanées de lien sur la route primaire et sur la route secondaire, aucun recouvrement n'est possible ; une nouvelle découverte de route est nécessaire pour rétablir la communication.

4.3.2.1.2 Recouvrement par segment de routes Le recouvrement par segment de route est mise œuvre lorsque les routes (primaire et secondaire) sont disjointes en liens (figure 4.8(b)). Ce qui implique qu'elles possèdent au moins un autre nœud commun en plus de la source et de la destination. Pour formuler sa fiabilité, il faut décomposer l'ensemble des routes en $(M-1)$ sous-ensembles ; où M est le nombre de nœuds communs aux routes primaire et secondaire. Le premier sous-ensemble commence par la source S (notée $n_{com[0]}$) et termine par le premier nœud intermédiaire commun (noté $n_{com[1]}$) aux deux routes. De plus, ce nœud $n_{com[1]}$ débute le deuxième sous-ensemble qui s'achève au prochain nœud commun $n_{com[2]}$. On procède ainsi de suite jusqu'à atteindre la destination D (notée $n_{com[M]}$).

La fiabilité de chaque sous-ensemble est formulée comme celle de la politique du recouvrement de bout en bout. Étant donné que les sous-ensembles sont en série, la fiabilité de l'ensemble des routes est le produit des fiabilités des sous-réseaux divisé par le produit des fiabilités des nœuds intermédiaires communs. Le but de cette division est d'éviter de prendre en compte la fiabilité d'un nœud intermédiaire commun deux fois : une première fois avec le sous-ensemble qu'il termine et une seconde fois avec le sous-ensemble qu'il débute.

La fiabilité du recouvrement par segment de routes de l'ensemble des routes décomposé en $(M-1)$ sous-ensembles est égale à :

$$R_{SR_{(S\leftrightarrow D)}} = R_{SR_{\left(n_{com[0]}\leftrightarrow n_{com[M]}\right)}} = \frac{\prod_{i=0}^{M-1} R_{E2E_{\left(n_{com[i]}\leftrightarrow n_{com[i+1]}\right)}}}{\prod_{i=1}^{M-1} R_{n_{com[i]}}} \tag{4.30}$$

où la fiabilité $R_{E2E_{\left(n_{com[i]}\leftrightarrow n_{com[i+1]}\right)}}$ est donnée par l'équation 4.27.

Notons que, lorsque $M=2$ (*ie* les seuls nœuds en commun aux deux routes sont la source S et la destination D), les équations 4.27 et 4.30 sont équivalentes.

Le recouvrement par segment fournit est une meilleure protection que celle proposée par le recouvrement de bout en bout. En effet, aucune reprise n'est possible avec le recouvrement de bout en bout, en cas de pannes simultanées sur la route primaire et sur la route secondaire. Alors que dans le recouvrement par segment, une reprise immédiate est possible dans le cas où les liens défaillants n'appartiennent pas

au même sous-ensemble. Le recouvrement consiste donc à isoler le segment en panne sur la route primaire pour le remplacer par un segment secondaire non défaillant.

4.3.2.2 Évaluation de performances

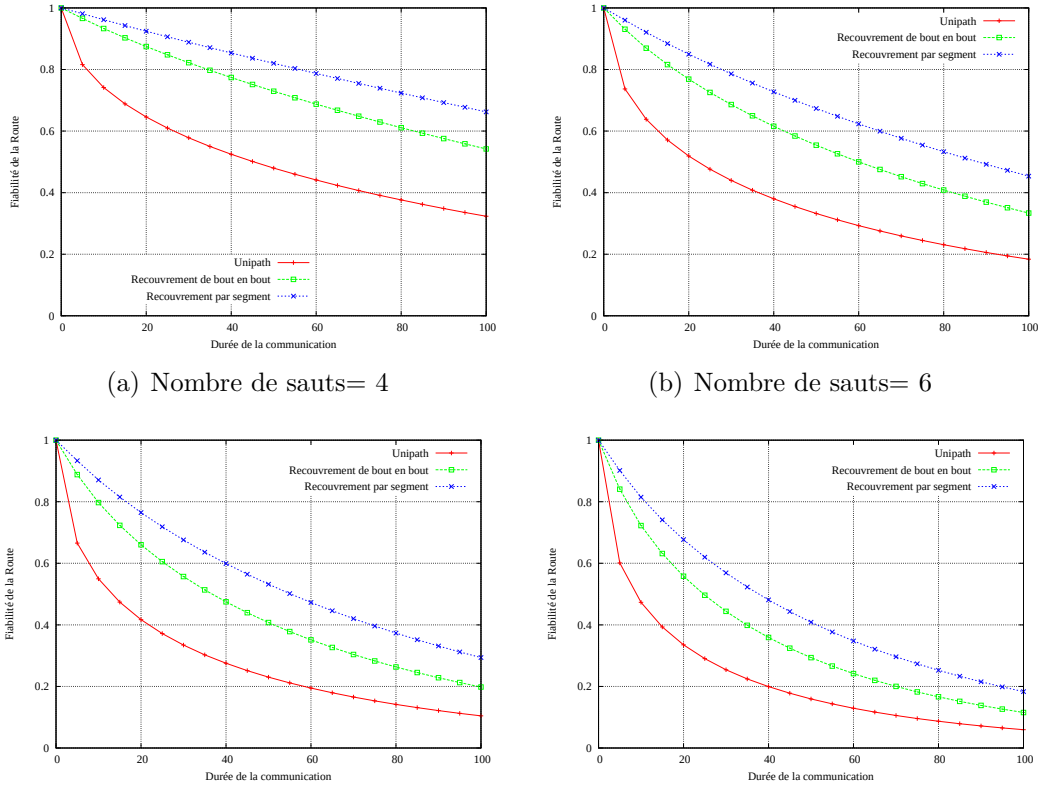
Après avoir formulé la fiabilité des politiques de recouvrement, nous nous intéressons maintenant à leur évaluation dans un réseau mobile ad hoc. Les équations 4.27 et 4.30 dépendent de la fiabilité des liens et des nœuds. Au chapitre 2, nous avons proposé une méthode analytique de calcul de la fiabilité de liens entre deux nœuds mobiles. La fiabilité d'un lien dépend de différents facteurs comme le modèle de mobilité, l'environnement de propagation et la distance initiale inter-nœuds.

Dans les politiques de recouvrement, les distances inter-nœuds ne sont pas connues à priori. Nous utilisons donc des fiabilités moyennes qui sont calculées en supposant une distribution aléatoire uniforme (voir section 2.3.2.1). Concernant la fiabilité d'un nœud, elle varie très peu pendant les durées de communications qui nous intéressent. En conséquence, dans notre évaluation, nous supposons qu'elle reste constante et est égale à 1 : $\forall\ j\ R_{n_j} = 1$.

L'objectif de l'évaluation est de comparer les deux politiques de recouvrement dans un réseau où elles peuvent toutes les deux être mises en œuvre. Nous supposons donc qu'à chaque découverte de routes, les hypothèses suivantes sont vérifiées :

- Dans les deux politiques de recouvrement, les routes primaire et secondaire possèdent le même nombre de sauts.
- Pour le recouvrement par segment de routes, un seul nœud intermédiaire commun deux routes existe (c'est-à-dire que $M = 3$ donc les routes sont divisées en 2 sous-ensembles). Ce nœud intermédiaire se trouve à mi-chemin entre la source et la destination.

Les courbes de la figure 4.9 comparent les fiabilités des routes des politiques de recouvrement et d'un protocole *unipath* pour une vitesse $v_{max} = 10$ m/s en fonction de la durée de la communication pour respectivement 4, 6, 8, 10 sauts entre la source et la destination. Quelle que soit la stratégie adoptée, la fiabilité diminue lorsque le nombre de sauts augmente. Concernant les politiques de recouvrement, nous observons que le recouvrement par segment est la meilleure politique quel que soit le nombre de sauts. Le recouvrement de bout en bout obtient toujours une meilleure fiabilité qu'un protocole *unipath*.



(a) Nombre de sauts= 4

(b) Nombre de sauts= 6

(c) Nombre de sauts= 8

(d) Nombre de sauts= 10

FIGURE 4.9 – Comparaison de la fiabilité des routes des protocoles *unipath* et *multipath* (recouvrement de bout en bout et par segment de routes) : $v_{max} = 10$ m/s

4.4 Conclusion

Dans ce chapitre, nous étudié la redondance de routes qui améliore les performances du routage en réduisant le temps de restauration.

En introduction, nous montrons les limites du routage *unipath*. En effet, dans un protocole *unipath*, une source conserve une seule route par destination. Lorsque celle-ci est rompue, une nouvelle découverte est nécessaire pour rétablir la communication. L'inconvénient de cette approche est une augmentation du temps de restauration qui entraine en conséquence une diminution du taux de livraison et une augmentation du délai de bout en bout.

Dans la deuxième section, nous étudié et analysé les protocoles de routage *multipath* proposés dans les réseaux MANETs en fonction du degré de similitude entre les routes et de la stratégie de routage. Nous en déduisons une meilleure efficacité de la stratégie de routage par la source pour construire les routes disjointes en nœuds. La stratégie par destination est plus adaptée pour établir des routes disjointes en lien ou non disjointes.

La troisième section est consacrée à une analyse comparative en termes de temps de restauration et de fiabilité, des protocoles *unipath* et deux politiques de recouvrement des protocoles *multipath*.

- En termes de temps de restauration, l'intérêt de la redondance de routes dépend de la probabilité $p_{secVald}$ de fonctionnement d'une route secondaire après la rupture de communication sur la route primaire. Pour chacun des trois mécanismes de détection de panne de liens, nous avons analysé l'avantage du routage *multipath*. Le routage *multipath* n'améliore pas toujours le temps de restauration par rapport à un routage *unipath*.
  Dans les notifications de niveau de liaison, le routage *multipath* possède un meilleur temps de restauration si la probabilité $p_{secVald}$ est supérieure ou égale 1/3. Concernant les deux autres mécanismes (protocoles *Hello* et *acquittement de niveau routage*), l'intérêt de la redondance de routes est fortement corrélé avec la durée de la découverte T_{DR}. Plus, cette durée est grande, meilleur est le gain de la redondance de routes. Dans ces deux mécanismes, il serait intéressant d'avoir une approche adaptative pour les constructions ou non de routes multiples. A partir des formulation, nous proposons d'utiliser un routage *unipath* si le temps de découverte $T_{DR} < 0.5$ sec ; sinon un protocole de routage *multipath*.
  Pour améliorer la probabilité $p_{secVald}$, nous avons proposé de maintenir la route secondaire.

- La comparaison en termes de fiabilité montre que le recouvrement par segment de routes est la meilleure politique pour fournir un service robuste aux applications.

Conclusions et Perspectives

A Conclusions Générales

Un réseau mobile ad hoc est une instance de réseau sans fil composée de nœuds mobiles auto-configurés qui communiquent entre eux sans avoir recours à une infrastructure centrale préexistante. Les communications entre nœuds d'extrémité sont perturbées par des pannes de liens et de nœuds en raison des caractéristiques intrinsèques de leur support de communication. Ces défaillances de communication sont aggravées par les particularités de relayage et de mobilité des nœuds. Ces réseaux requièrent donc la conception et la mise œuvre des protocoles robustes au niveau de toutes les couches protocolaires, en particulier au niveau des fonctions d'accès et de routage.

Dans cette thèse, nous proposons d'améliorer les performances des communications dans un réseau mobile ad hoc en utilisant des politiques de robustesse. Nous proposons et étudions deux architectures de communication qui fournissent chacune, deux politiques couplées de robustesse à savoir la protection et la restauration de service. Notons que quelle que soit la technique de protection, une restauration est nécessaire dans un réseau mobile ad hoc.

Les deux architectures proposées diffèrent selon la politique de protection choisie ; mais utilisent la politique de même restauration. Celle-ci est mise œuvre par le protocole de routage. Les pannes de communication entre nœuds adjacents sont détectées à partir des notifications de la couche liaison. Ce mécanisme assure les meilleurs temps et coût de la restauration, par rapport aux autres mécanismes de détection de pannes de liens.

Concernant, la protection de service mise en place à l'initialisation de la communication, les deux solutions proposées sont :

- **Solution 1 : Protection par une analyse prédictive**

  L'architecture proposée s'appuie sur un protocole de routage réactif dont le critère de sélection de routes est modifié. L'idée est d'utiliser des métriques capables de prédire l'état futur des routes dans le but d'améliorer leur durée de

vie. Pour cela, deux métriques prédictives reposant sur la mobilité des nœuds sont proposées : fiabilité des routes et combinaison fiabilité-minimum de sauts. Le calcul de ces métriques prédictives s'appuie sur une méthode analytique qui prédit l'état futur des communications. Leur utilisation améliore les performances du routage en termes de taux de livraison de paquets et de surcoût normalisé.

- **Solution 2 : Protection par redondance de routes**

  Dans cette solution, l'architecture s'appuie sur un protocole de routage *multi-path*. Nous avons montré qu'en termes de robustesse, il n'est donc pas nécessaire d'utiliser une redondance de niveau transport dans un MANET où les nœuds sont mono-domiciliés. La redondance de routes améliore la robustesse de la communication en réduisant le temps de restauration et en conséquence le taux de livraison et le délai de bout en bout des paquets.
  A partir de nos expressions analytiques, nous déduisons qu'un protocole *multi-path* avec une politique de recouvrement segmenté donne les meilleurs résultats en termes de temps de restauration et de fiabilité.

B Perspectives

Les perspectives pour les travaux présentés dans cette thèses sont nombreuses.

1. Une premier axe de recherche intéressant serait d'étendre l'utilisation des métriques prédictives proposées dans un protocole de routage proactif *unipath* type OLSR [CJ03]. Le choix des MPRs (MultiPoint Relays) pourrait reposer sur des métriques prédictives. Le MPR choisi pourra être le nœud possède qui le plus de voisins à 2 sauts durant l'intervalle de prédiction.

2. Il serait intéressant d'étendre la méthode analytique de calcul de la fiabilité de lien à d'autres modèles de mobilité, notamment :

   - Le modèle *Random Way Point* où les temps de pause T_{Pause} entre deux déplacements consécutifs d'un nœud ne sont pas connus à priori,
   - Les modèles de mobilité de groupes, en particulier le modèle RPGM (*Reference Point Group Mobility*).

3. Une perspective de recherche est d'étudier l'utilisation conjointe des deux solutions de protection proposées dans une même architecture pour le partage charge. Dans ce cas, à chaque découverte de routes, la source construit les N routes les plus fiables.

Annexe

A Démonstration équation 2.34

$$f_{D_{m+1}|D_m}\left(d_{m+1}|d_m\right) = \int_0^{2\cdot v_{max}} \frac{\frac{d_{m+1}\cdot v_{r_{m+1}}}{2\cdot E\{v_r\}^2}\cdot e^{\frac{-\pi\cdot v_{r_{m+1}}^2}{4\cdot E\{v_r\}^2}}}{\left[4d_{m+1}^2 d_m^2 - \left[v_{r_{m+1}}^2 - \left(d_{m+1}^2+d_m^2\right)\right]^2\right]^{\frac{1}{2}}} dv_{r_{m+1}}$$

$$= \frac{d_{m+1}}{2\cdot E\{v_r\}^2}\int_0^{2\cdot v_{max}} v_{r_{m+1}}\cdot\left[\frac{e^{\frac{-\pi\cdot v_{r_{m+1}}^2}{2\cdot E\{v_r\}^2}}}{4d_{m+1}^2 d_m^2 - \left[v_{r_{m+1}}^2 - \left(d_{m+1}^2+d_m^2\right)\right]^2}\right]^{\frac{1}{2}} dv_{r_{m+1}} \tag{31}$$

Procédons à un changement de variable, en posant : $X = v_{r_{m+1}}^2 \Rightarrow dX = 2\cdot v_{r_{m+1}}\cdot dv_{r_{m+1}}$ donc $v_{r_{m+1}}^2 \in [0, 2\cdot v_{max}] \Rightarrow X \in [0, 4\cdot v_{max}^2]$

$$\begin{aligned} f_{D_{m+1}|D_m}\left(d_{m+1}|d_m\right) &\approx \frac{d_{m+1}}{2\cdot E\{v_r\}^2}\int_0^{4\cdot v_{max}^2}\left[\frac{e^{\frac{-\pi\cdot X}{2\cdot E\{v_r\}^2}}}{4d_{m+1}^2 d_m^2 - \left[X - \left(d_{m+1}^2+d_m^2\right)\right]^2}\right]^{\frac{1}{2}} dX \\ &\approx \frac{d_{m+1}}{2\cdot E\{v_r\}^2}\int_0^{4\cdot v_{max}^2} f(X)\cdot g(X) dX \end{aligned} \tag{32}$$

avec $f(X) = \left[e^{\frac{-\pi\cdot X}{2\cdot E\{v_r\}^2}}\right]^{\frac{1}{2}} dX$ et $g(X) = \left[\frac{1}{4d_{m+1}^2 d_m^2 - \left[X - \left(d_{m+1}^2+d_m^2\right)\right]^2}\right]^{\frac{1}{2}} dX$

La fonction $f(X)\cdot g(X)$ étant positive, nous pouvons borner la densité conditionnelle de probabilité $f_{D_{m+1}|D_m}$ en utilisant l'inégalité de Cauchy-Schwarz :

$$\int_a^b |f(x)\cdot g(x)|\, dx \leq \left[\int_a^b |f(x)|^2\, dx\right]^{\frac{1}{2}}\cdot\left[\int_a^b |g(x)|^2\, dx\right]^{\frac{1}{2}} \tag{33}$$

Nous obtenons donc

$$f_{D_{m+1}|D_m} \leq \frac{d_{m+1}}{2\cdot E\{v_r\}^2}\cdot A\cdot B \tag{34}$$

avec $A^2 = \int_0^{4\cdot v_{max}^2} |f(X)|^2\, dX$ et $B^2 = \int_0^{4\cdot v_{max}^2} |g(X)|^2\, dX$

Calculons A^2 et B^2 :

$$\begin{aligned} A^2 &= \int_0^{4\cdot v_{max}^2} e^{\frac{-\pi\cdot X}{2\cdot E\{v_r\}^2}} dX = \left[\frac{-2\cdot E\{v_r\}^2}{\pi}\cdot e^{\frac{-\pi\cdot X}{2\cdot E\{v_r\}^2}}\right]_0^{4\cdot v_{max}^2} \\ &= \frac{2\cdot E\{v_r\}^2}{\pi}\cdot\left[1-e^{\frac{-2\pi\cdot v_{max}^2}{E\{v_r\}^2}}\right] \end{aligned} \tag{35}$$

$$\begin{aligned} B^2 &= \int_0^{4\cdot v_{max}^2} \frac{1}{(2\cdot d_{m+1}d_m)^2-\left[X-(d_{m+1}^2+d_m^2)\right]^2} dX \\ &= \frac{1}{2\cdot(2\cdot d_{m+1}d_m)}\cdot\left[\ln\left|\frac{2\cdot d_{m+1}d_m+\left[X-\left(d_{m+1}^2+d_m^2\right)\right]}{2\cdot d_{m+1}d_m-\left[X-(d_{m+1}^2+d_m^2)\right]}\right|\right]_0^{4\cdot v_{max}^2} \\ &= \frac{1}{4\cdot d_{m+1}d_m}\cdot\left[\ln\left|\frac{X-(d_{m+1}-d_m)^2}{(d_{m+1}+d_m)^2-X}\right|\right]_0^{4\cdot v_{max}^2} \\ &= \frac{1}{4\cdot d_{m+1}d_m}\cdot\ln\left[\frac{\left|4\cdot v_{max}^2-(d_{m+1}-d_m)^2\right|\cdot(d_{m+1}+d_m)^2}{\left|(d_{m+1}+d_m)^2-4\cdot v_{max}^2\right|\cdot(d_{m+1}-d_m)^2}\right] \end{aligned} \tag{36}$$

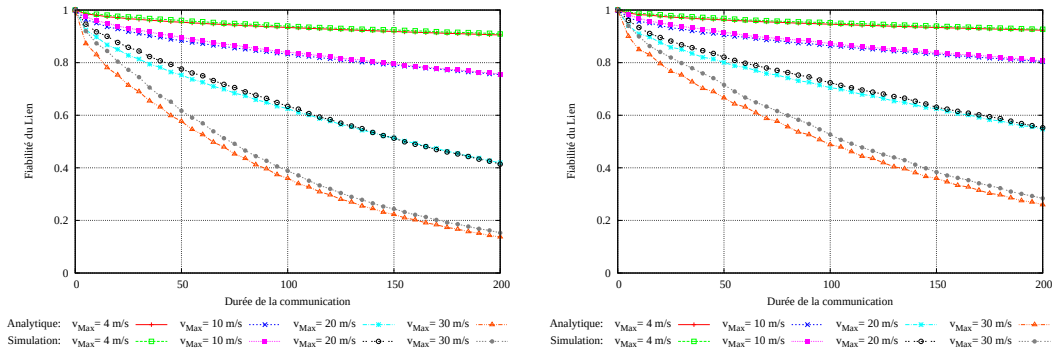
$$\text{car } \int\frac{1}{a^2-f(x)^2}dx=\frac{1}{2\cdot a}\ln\left|\frac{a+f(x)}{a-f(x)}\right| \quad \text{lorsque} \quad f'(x)=1$$

En remplaçant A^2 et B^2 dans l'équation 34, on obtient :

$$\begin{aligned} f_{D_{m+1}|D_m}(d_{m+1}|d_m) &\leq \frac{d_{m+1}}{2\cdot E\{v_r\}^2}\cdot\left[\frac{2\cdot E\{v_r\}^2}{\pi}\cdot\left(1-e^{\frac{-2\pi\cdot v_{max}^2}{E\{v_r\}^2}}\right)\right]^{\frac{1}{2}}\cdot \\ &\quad \left[\frac{1}{4\cdot d_{m+1}d_m}\cdot\ln\left(\frac{\left|4\cdot v_{max}^2-(d_{m+1}-d_m)^2\right|\cdot(d_{m+1}+d_m)^2}{\left|(d_{m+1}+d_m)^2-4\cdot v_{max}^2\right|\cdot(d_{m+1}-d_m)^2}\right)\right]^{\frac{1}{2}} \\ f_{D_{m+1}|D_m}(d_{m+1}|d_m) &\leq \sqrt{\frac{d_{m+1}}{d_m}}\cdot\frac{1}{E\{v_r\}\cdot 2\sqrt{2\cdot\pi}}\left[1-e^{\frac{-2\pi\cdot v_{max}^2}{E\{v_r\}^2}}\right]^{\frac{1}{2}}\cdot \\ &\quad \left[\ln\left(\frac{\left|4\cdot v_{max}^2-(d_{m+1}-d_m)^2\right|\cdot(d_{m+1}+d_m)^2}{\left|(d_{m+1}+d_m)^2-4\cdot v_{max}^2\right|\cdot(d_{m+1}-d_m)^2}\right)\right]^{\frac{1}{2}} \text{ CQFD} \end{aligned} \tag{37}$$

B Validation de la méthode analytique pour le modèle de mobilité *Random Way Point*

Nous validons notre méthode analytique dans le cas où les nœuds se déplacent selon le *Random Way Point* pour différentes valeurs de temps de pause. Le modèle de propagation est *path loss*.



(a) T_{Pause} = 1 seconde (b) T_{Pause} = 2 secondes

FIGURE 10 – Random Way Point : fiabilité en fonction du temps, distance initiale équiprobable

C Démonstration des formules du chapitre 4

C.1 Formule 4.8

$$
\begin{aligned}
T_{RS_{MP(E2ER)}} &= \left(T_{d_{Route(N_{rec})}}\right)_{Pri} + (p_{secVald} \times T_{rt}) \\
&\quad + (1 - p_{secVald}) \times [(T_{rt} + T_{d_{Route}})_{Sec} + T_{or} + T_{rt}] \\
&= \left[\left(T_{d_{Route(S)}}\right)_{Pri} + T_{or} + T_{rt}\right] + (p_{secVald} \times T_{rt}) + (T_{rt} + T_{d_{Route}})_{Sec} \\
&\quad - (p_{secVald} \times T_{rt}) - p_{secVald} \times [(T_{d_{Route}})_{Sec} + T_{or} + T_{rt}] \\
&= \left[\left(T_{d_{Route(S)}}\right)_{Pri} + T_{or} + T_{rt}\right] - p_{secVald} \times [(T_{d_{Route}})_{Sec} + T_{or} + T_{rt}] \\
&\quad + (T_{rt} + T_{d_{Route}})_{Sec} \\
&= \left[\left(T_{d_{Route(S)}}\right)_{Pri} + T_{or} + T_{rt}\right] - p_{secVald} \times [(T_{d_{Route}})_{Sec} + T_{or} + T_{rt}] \\
&\quad + (T_{rt} + T_{d_{Route}})_{Sec} \\
&= \left(T_{d_{(n_i,n_{i+1})}} + T_{n[n_i \to S]} + T_{or} + T_{rt}\right) - p_{secVald} \times \left(T_{d_{(n_j,n_{j+1})}} + T_{n[n_j \to S]} + T_{or} + T_{rt}\right) \\
&\quad + \left(T_{rt} + T_{d_{(n_j,n_{j+1})}} + T_{n[n_j \to S]}\right) \\
&= (1 - p_{secVald}) \times (T_d + T_n + T_{or} + T_{rt}) + \left(T_{rt} + T_d + T_{n[j \to S]}\right) \\
&= \left[(1 - p_{secVald}) \times T_{RS_{UP-Reac}}\right] + \left(T_{rt} + T_d + T_{n[n_j \to S]}\right)
\end{aligned}
$$

Avec $T_{d_{(n_j,n_{j+1})}} = T_{d_{(n_i,n_{i+1})}} = T_d$ et $T_{n[n_i \to S]} = T_{n[n_j \to S]}$ (en supposant que les nombres de sauts entre $n_i \to S$ et $n_j \to S$ sont égaux).

C.2 Démonstration : formule 4.9

$$
\begin{aligned}
T_{RS_{MP(SR)}} &= \left(T_{d_{Route(N_{rec})}}\right)_{Pri} + (p_{secVald} \times T_{rt}) + (1 - p_{secVald}) \times \left[\left(T_{rt} + T_{d_{Route}}\right)_{Sec} + T_{or} + T_{rt}\right] \\
&= \left[\left(T_{d_{Route(NI)}}\right)_{Pri} + T_{or} + T_{rt}\right] + (p_{secVald} \times T_{rt}) + \left(T_{rt} + T_{d_{Route}}\right)_{Sec} \\
&\quad - (p_{secVald} \times T_{rt}) - p_{secVald} \times \left[\left(T_{rt} + T_{d_{Route}}\right)_{Sec} + T_{or}\right] \\
&= \left(T_{d_{Route(NI)}}\right)_{Pri} + (p_{secVald} \times T_{rt}) + [(1 - p_{secVald}) \times (T_{or} + T_{rt})] \\
&\quad + \left[(1 - p_{secVald}) \times \left(T_{rt} + T_{d_{Route}}\right)_{Sec}\right] \\
&= \left[\left(T_{d_{Route(NI)}}\right)_{Pri} + T_{or} + T_{rt}\right] + (p_{secVald} \times T_{rt}) - (p_{secVald} \times T_{rt}) - (p_{secVald} \times T_{or}) \\
&\quad + \left[(1 - p_{secVald}) \times \left(T_{rt} + T_{d_{Route}}\right)_{Sec}\right] \\
&= \left[\left(T_{d_{Route(NI)}}\right)_{Pri} + T_{or} + T_{rt}\right] - (p_{secVald} \times T_{or}) + \left[(1 - p_{secVald}) \times \left(T_{rt} + T_{d_{Route}}\right)_{Sec}\right]
\end{aligned}
$$

C.3 Démonstration de la formule 4.11

$$\begin{aligned} T_{RS_{UP-Reac}} - T_{RS_{MP(E2ER)}} &= p_{secVald} \times T_{RS_{UP-Reac}} - \left(T_{rt} + T_{d_{(n_j,n_{j+1})}} + T_{n[n_j \to S]}\right) \\ &= p_{secVald} \times \left(T_{d_{(n_i,n_{i+1})}} + T_{n[n_i \to S]} + T_{or} + T_{rt}\right) \\ &\quad - \left(T_{rt} + T_{d_{(n_j,n_{j+1})}} + T_{n[n_j \to S]}\right) \end{aligned} \tag{38}$$

$$\begin{aligned} T_{RS_{Unip}} - T_{RS_{MP}} &\geq 0 \\ p_{secVald} \times \left(T_{d_{(n_i,n_{i+1})}} + T_{n[n_i \to S]} + T_{or} + T_{rt}\right) - \left(T_{rt} + T_{d_{(n_j,n_{j+1})}} + T_{n[n_j \to S]}\right) &\geq 0 \\ p_{secVald} \geq \frac{T_{rt} + T_{d_{(n_j,n_{j+1})}} + T_{n[n_j \to S]}}{T_{d_{(n_i,n_{i+1})}} + T_{n[n_i \to S]} + T_{or} + T_{rt}} & \\ p_{secVald} \geq \frac{T_{rt} + T_d + T_n}{T_d + T_n + T_{or} + T_{rt}} & \end{aligned} \tag{39}$$

Avec $T_{n[n_i \to S]} = T_{n[n_j \to S]}$ et $T_{d_{(n_i,n_{i+1})}} = T_{d_{(n_j,n_{j+1})}}$.

C.4 Démonstration de la formule 4.23

$$\begin{aligned} T_{RS_{MP(E2ER)}} &= \left(T_{d_{Route(N_{rec})}}\right)_{Pri} + p_{secVald} \times \left\{T_{RS_{MP}}\right\}_{Cas1} \\ &\quad + (1 - p_{secVald}) \times \left\{p_{useSecInvald} \times \left(T_{rt} + T_{d_{Route}}\right)_{Sec} + T_{or} + T_{rt}\right\}_{Cas2} \\ &= \left(T_{d_{Route(S)}}\right)_{Pri} + (p_{secVald} \times T_{rt}) + (1 - p_{secVald}) \times \left[p_{useSecInvald} \times \left(T_{rt} + T_{d_{Route}}\right)_{Sec} + T_{or} + T_{rt}\right] \\ &= \left(T_{d_{Route(S)}}\right)_{Pri} + (p_{secVald} \times T_{rt}) + (1 - p_{secVald}) \times [T_{or} + T_{rt}] \\ &\quad + (1 - p_{secVald}) \times \left[p_{useSecInvald} \times \left(T_{rt} + T_{d_{Route}}\right)_{Sec}\right] \\ &= \left(T_{d_{Route(S)}}\right)_{Pri} + (p_{secVald} \times T_{rt}) + T_{or} + T_{rt} - (p_{secVald} \times T_{or}) - (p_{secVald} \times T_{rt}) \\ &\quad + (1 - p_{secVald}) \times \left[p_{useSecInvald} \times \left(T_{rt} + T_{d_{Route}}\right)_{Sec}\right] \\ &= \left[\left(T_{d_{Route(S)}}\right)_{Pri} + T_{or} + T_{rt}\right] - (p_{secVald} \times T_{or}) + (1 - p_{secVald}) \times \left[p_{useSecInvald} \times \left(T_{rt} + T_{d_{Route}}\right)_{Sec}\right] \\ &= T_{RS_{UP-Reac}} - p_{secVald} \times \left[T_{or} + p_{useSecInvald} \times \left(T_{rt} + T_{d_{Route}}\right)_{Sec}\right] + \left[p_{useSecInvald} \times \left(T_{rt} + T_{d_{Route}}\right)_{Sec}\right] \end{aligned} \tag{40}$$

$$\begin{aligned} T_{RS_{UP-Reac}} - T_{RS_{MP(E2ER)}} &= p_{secVald} \times \left[T_{or} + p_{useSecInvald} \times \left(T_{rt} + T_{d_{Route}}\right)_{Sec}\right] - \left[p_{useSecInvald} \times \left(T_{rt} + T_{d_{Route}}\right)_{Sec}\right] \\ &= p_{secVald} \times [T_{or} + p_{useSecInvald} \times (T_{rt} + T_d + T_n)] - [p_{useSecInvald} \times (T_{rt} + T_d + T_n)] \end{aligned} \tag{41}$$

$$T_{RS_{Unip}} - T_{RS_{MP}} \geq 0$$

$$p_{secVald} \times [T_{or} + p_{useSecInvald} \times (T_{rt} + T_d + T_n)] - [p_{useSecInvald} \times (T_{rt} + T_d + T_n)] \geq 0$$

$$p_{secVald} \geq \frac{p_{useSecInvald} \times (T_{rt} + T_d + T_n)}{T_{or} + p_{useSecInvald} \times (T_{rt} + T_d + T_n)}$$

$$p_{secVald} \geq \frac{p_{useSecInvald} \times (T_d + T_n)}{T_{or} + p_{useSecInvald} \times (T_d + T_n)} \tag{42}$$

Bibliographie

[ATC+09] A. Ariza, A. Trivio, E. Casilari, J.-C. Cano, C.T. Calafate et P. Manzoni : Assessing the impact of link layer feedback mechanisms on manet routing protocols. *In Computers and Communications, 2009. ISCC 2009. IEEE Symposium on*, pages 770 –775, juillet 2009.

[Bag11] M. Bagnulo : Threat Analysis for TCP Extensions for Multipath Operation with Multiple Addresses. RFC 6181 (Informational), mars 2011.

[BCF+99] S. Basagni, I. Chlamtac, A. Faragó, V. R. Syrotiuk et R. Talebi : Route selection in mobile multimedia ad hoc networks. *In Proceedings of the Sixth IEEE International Workshop on Mobile Multimedia Communications, MoMuC'99*, pages 97–103, San Diego, CA, novembre 1999.

[BDP12] Amadou Baba Bagayoko, Riadh Dhaou et Béatrice Paillassa : An efficient metric for reliable routing with link dependencies (regular paper). *In IEEE Vehicular Technology Conference (VTC), Quebec City, 03/09/2012-06/09/2012*, septembre 2012.

[BP11a] Amadou Baba Bagayoko et Béatrice Paillassa : Analysis of Robustness in Heterogeneous Ad Hoc Networks (regular paper). *In International Wireless Communications and Mobile Computing Conference (IWCMC), istambul,Turkey, 05/07/2011-08/07/2011*, juillet 2011.

[BP11b] Amadou Baba Bagayoko et Béatrice Paillassa : Comparaison des stratégies de redondance dans les réseaux ad hoc (regular paper). *In Colloque Francophone sur l'Ingéniérie des Protocoles(CFIP), sainte maxime,France, 10/05/2011-13/05/2011*, mai 2011.

[BPD11] Amadou Baba Bagayoko, Béatrice Paillassa et Riadh Dhaou : Practical Link Reliability for Ad-hoc Routing Protocol (regular paper). *In IEEE Vehicular Technology Conference (VTC), San Francisco, 05/09/2011-08/09/2011*, pages 1–5. IEEE Computer Society - Conference Publishing Services, septembre 2011.

[CBV03] P. Chatzimisios, A. C. Boucouvalas et V. Vitsas : Ieee 802.11 packet delay - a finite retry limit analysis. *In In Proceedings of the IEEE Global Telecommunications Conference Globecom*, pages 950–954, décembre 2003.

[CCGL06] G. Carofiglio, C. Chiasserini, M. Garetto et E. Leonardi : Analysis of route stability under the random direction mobility model. *SIGMETRICS Perform. Eval. Rev.*, 34:36–38, décembre 2006.

[Cha04] Periklis Chatzimisios : *Performance modelling and enhancement of wireless communication protocols*. Thèse de doctorat, School of Design, Engineering & Computing, Bournemouth University, décembre 2004.

[CJ03] T. Clausen et P. Jacquet : The optimized link state routing protocol (OLSR). RFC 3626, octobre 2003.

[CNRS98] E. Crawley, R. Nair, B. Rajagopalan et H. Sandick : A Framework for QoS-based Routing in the Internet. RFC 2386 (Informational), août 1998.

[CP10] Ian D. Chakeres et Charles E. Perkins : Dynamic manet on-demand (dymo) routing. Published Online, juillet 2010. Expiration : Janvier 2011.

[DABM03] Douglas S. J. De Couto, Daniel Aguayo, John Bicket et Robert Morris : A high-throughput path metric for multi-hop wireless routing. *In Proceedings of the 9th ACM International Conference on Mobile Computing and Networking (MobiCom '03)*, San Diego, California, septembre 2003.

[DFH06] O. Daescu, G. Fasui et K. Haridoss : Gara : a geometry aided routing algorithm : Research articles. *Wirel. Commun. Mob. Comput.*, 6:259–268, mars 2006.

[DRWT97] Rohit Dube, Cynthia D. Rais, Kuang-Yeh Wang et Satish K. Tripathi : Signal stability-based adaptive routing (ssa) for ad hoc mobile networks. *In IEEE Personal Communications Magazine*, pages 36–45. IEEE, février 1997.

[DZSN08] Arash Dana, Ahmad Khadem Zadeh et Seyed Ali Sadat Noori : Backup path set selection in ad hoc wireless network using link expiration time. *Comput. Electr. Eng.*, 34(6):503–519, novembre 2008.

[Far04] A. Farago : Availability estimation of routes, trees and subnetworks for end-to-end qos. *In Global Telecommunications Conference, 2004. GLOBECOM '04. IEEE*, volume 6, pages 3583 – 3587 Vol.6, nov.-3 dec. 2004.

[FB06] Adrian Farrel et Igor Bryskin : *GMPLS : Architecture and Applications*. Morgan Kaufmann, première édition, 2006.

[FRH+11] A. Ford, C. Raiciu, M. Handley, S. Barre et J. Iyengar : Architectural Guidelines for Multipath TCP Development. RFC 6182 (Informational), mars 2011.

[glo] *Global Mobile Simulator- glomosim*. http ://pcl.cs.ucla.edu/projects/glomosim.

[GMS+06] C. Gomez, D. Mediavilla, P. Salvatella, X. Mantecon et J. Paradells : A study of local connectivity maintenance strategies of manet reactive routing protocol implementations. *In Wireless Communication Systems, 2006. ISWCS '06. 3rd International Symposium on*, pages 228 –232, septembre 2006.

[GYS05] Song Guo, Oliver Yang et Yantai Shu : Improving source routing reliability in mobile ad hoc networks. *IEEE Trans. Parallel Distrib. Syst.*, 16(4):362–373, avril 2005.

[IEC74] IEC : IEC - International Electrotechnical Commission- Standard 271, List of basic terms, definitions and related mathematics for reliability, janvier 1974.

[IEE90] IEEE : IEEE Standard Glossary of Software Engineering Terminology, septembre 1990.

[JHM07] D. Johnson, Y. Hu et D. Maltz : The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4. RFC 4728 (Experimental), février 2007.

[KHF06] E. Kohler, M. Handley et S. Floyd : Datagram Congestion Control Protocol (DCCP). RFC 4340 (Proposed Standard), March 2006. Updated by RFCs 5595, 5596.

[KPK+07] G. Koltsidas, F.-N. Pavlidou, K. Kuladinithi, A. Timm-Giel et C. Gorg : Investigating the performance of a multipath dymo protocol for ad-hoc networks. *In Personal, Indoor and Mobile Radio Communications, 2007. PIMRC 2007. IEEE 18th International Symposium on*, pages 1–5, septembre 2007.

[LG00] S. J. Lee et M. Gerla : AODV-BR : backup routing in ad hoc networks. *Wireless Communications and Networking Conference, 2000. WCNC. 2000 IEEE*, 3:1311–1316, 2000.

[LG02] S. J. Lee et M. Gerla : Split multipath routing with maximally disjoint paths in ad hoc networks. *Communications, 2001. ICC 2001. IEEE International Conference on*, 10:3201–3205 vol.10, août 2002.

[Lim02] Geunhwi Lim : Link stability and route lifetime in ad-hoc wireless networks. *In Proceedings of the 2002 International Conference on Parallel Processing Workshops*, Washington, DC, USA, 2002. IEEE Computer Society.

[LL06] Min-Gu Lee et Sunggu Lee : A link stability model and stable routing for mobile ad-hoc networks. *In EUC*, pages 904–913, 2006.

[LLP+01] Roy Leung, Jilei Liu, Edmond Poon, Ah-Lot Charles Chan et Baochun Li : Mp-dsr : A qos-aware multi-path dynamic source routing protocol for wireless ad-hoc networks. *In LCN*, pages 132–141. IEEE Computer Society, 2001.

[MD01] M. K. Marina et S. R. Das : On-demand multipath distance vector routing in ad hoc networks. *Network Protocols, 2001. Ninth International Conference on*, pages 14–23, 2001.

[MD06] Mahesh K. Marina et Samir R. Das : Ad hoc on-demand multipath distance vector routing. *WCMC 2006, Wireless Communications and Mobile Computing*, 6(7):969–988, 2006.

[MZ99] A. Bruce McDonald et Taieb Znati : A mobility based framework for adaptive clustering in wireless ad-hoc networks. *IEEE Journal on Selected Areas in Communications*, 17:1466–1487, août 1999.

[NCM07] M. Nacher, C.T. Calafate et P. Manzoni : Multipath extensions to the dymo routing protocol. *In Mobile Wireless Communications Networks, 2007 9th IFIP International Conference on*, pages 1 –5, septembre 2007.

[ns] *The Network Simulator NS (ns-2)*. http ://www.isi.edu/nsnam/ns.

[omn] *OMNet++ Network Simulation Framework*. http ://ieeexplore.ieee.org/xpls/abs_all.jsp ?arnumber=916672.

[PB94] C. E. Perkins et P. Bhagwat : Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. *ACM SIGCOMM Computer Communication Review*, 24(4):234–244, 1994.

[PBRD03] C. Perkins, E. Belding-Royer et S. Das : Ad hoc On-Demand Distance Vector (AODV) Routing. RFC 3561 (Experimental), juillet 2003.

[PNBS99] Ratish J. Punnoose, Pavel V. Nikitin, Josh Broch et Daniel D. Stancil : Optimizing wireless network protocols using real-time predictive propagation modeling. *In In Radio and Wireless Conference (RAWCON*, 1999.

[Pos80] J. Postel : User Datagram Protocol. RFC 768 (Standard), août 1980.

[Pos81] J. Postel : Transmission Control Protocol. RFC 793 (Standard), septembre 1981. Updated by RFCs 1122, 3168, 6093.

[RAB00] *Route-lifetime assessment based routing (RABR) protocol for mobile ad-hoc networks*, volume 3, 2000.

[Sch05] M. Schwartz : *Mobile Wireless Communications*. CAMBRIDGE, première édition, 2005.

[SDJ01] Jiang Shengming, He Dajiang et Rao Jianqiang : A prediction-based link availability estimation for mobile ad hoc networks. *INFOCOM 2001. Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, 3:1745–1752 vol.3, avril 2001.

[SLG00] W. Su, S.-J. Lee et M. Gerla. : Mobility prediction in wireless networks. *In the Proc. of IEEE Military Communications Conference*, 0:491–495, octobre 2000.

[Ste07] R. Stewart : Stream Control Transmission Protocol. RFC 4960 (Proposed Standard), septembre 2007. Updated by RFCs 6096, 6335.

[SXM+00] R. Stewart, Q. Xie, K. Morneault, C. Sharp, H. Schwarzbauer, T. Taylor, I. Rytina, M. Kalla, L. Zhang et V. Paxson : Stream Control Transmission Protocol. RFC 2960 (Proposed Standard), octobre 2000. Obsoleted by RFC 4960, updated by RFC 3309.

[SZG+06] Dong Shi, Xinming Zhang, Xuemei Gao, Wenbo Zhu et Fengfu Zou : Routing based on ad hoc link reliability. *In Frontiers of High Performance Computing and Networking ISPA 2006 Workshops*, volume 4331 de *Lecture Notes in Computer Science*, pages 341–350. Springer Berlin Heidelberg, 2006.

[SZG+07] Dong Shi, Xinming Zhang, Xuemei Gao, Wenbo Zhu et Fengfu Zou : A link reliability-aware route maintenance mechanism for mobile ad hoc networks. *In Proceedings of the Sixth International Conference on Networking*, pages 8–, Washington, DC, USA, 2007. IEEE Computer Society.

[TCC06] Hua-Wen Tsai, Tzung-Shi Chen et Chih-Ping Chu : An on-demand routing protocol with backtracking for mobile ad hoc networks. *Wirel. Pers. Commun.*, 38:279–300, août 2006.

[Toh96] Chai-Keong Toh : A novel distributed routing protocol to support ad hoc mobile computing. *In Proc. IEEE 15th Annual International Phoenix Conference on Computers and Communications, IEEE IPCCC 1996, March 27-29, Phoenix, AZ, USA*, pages 480–486. IEEE, IEEE, mars 1996.

[XBJ07] Sanlin Xu, Kim L. Blackmore et Haley M. Jones : An analysis framework for mobility metrics in mobile ad hoc networks. *EURASIP J. Wirel. Commun. Netw.*, janvier 2007.

[YAA10] Zhenzhen Ye, Abouzeid et Alhussein A. : A unified model for joint throughput-overhead analysis of random access mobile ad hoc networks. *Comput. Netw.*, 54:573–588, mars 2010.

[YKT03] Z. Ye, S. V. Krishnamurthy et S. K. Tripathi : A framework for reliable routing in mobile ad hoc networks. *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE*, 1:270–280 vol.1, 2003.

[YWC07] Chang Wu Yu, Tung-Kuang Wu et Rei Heng Cheng : A low overhead dynamic route repairing mechanism for mobile ad hoc networks. *Comput. Commun.*, 30:1152–1163, mars 2007.

[YWL07] Wei Yuan, Xiangyu Wang et Jean-Paul M G Linnartz : A coexistence model of ieee 802.15.4 and ieee 802.11b/g. *Scenario*, pages 2–6, 2007.

[ZD07] Hui Zhang et Yu-Ning Dong : A novel path stability computation model for wireless ad hoc networks. volume 14, pages 928 –931, dec 2007.

[ZW07a] Ming Zhao et Wenye Wang : Analyzing topology dynamics in ad hoc networks using a smooth mobility model. *In the Proc. of IEEE Global Telecommunications Conference*, pages 1206–1210, mars 2007.

[ZW07b] Ming Zhao et Wenye Wang : Analyzing topology dynamics in ad hoc networks using a smooth mobility model. *In the Proc. of IEEE Wireless Communications and Networking Conference*, pages 3279–3284, mars 2007.

Résumé :

Les réseaux sans fil sont sujets à des perturbations voire des pannes de liens et de nœuds en raison des caractéristiques intrinsèques de leur support de communication ; ces pannes sont aggravées par les particularités de relayage et de mobilité des nœuds dans les réseaux ad hoc. Ces réseaux requièrent donc la conception et la mise œuvre des protocoles robustes au niveau de toutes les couches protocolaires.

Dans cette thèse, nous choisissons une approche de robustesse pour améliorer les performances des communications dans un réseau mobile ad hoc. Nous proposons et étudions deux architectures de protection (protection par une analyse prédictive et protection par redondance de routes) qui sont couplées avec une restauration de niveau routage. Concernant la phase de détection, le protocole de routage utilise les notifications de niveau liaison pour détecter les pannes de liens.

La première solution repose sur un protocole de routage réactif *unipath* dont le critère de sélection de routes est modifié. L'idée est d'utiliser des métriques capables de prédire l'état futur des routes dans le but d'améliorer leur durée de vie. Pour cela, deux métriques prédictives reposant sur la mobilité des nœuds sont proposées : la fiabilité des routes et une combinaison fiabilité-minimum de sauts. Pour calculer ces métriques prédictives, nous proposons une méthode analytique de calcul de la fiabilité de liens entre nœuds. Cette méthode prend compte le modèle de mobilité des nœuds et les caractéristiques de la communication sans fil notamment les collisions inter-paquets et les atténuations du signal. Les modèles de mobilité étudiés sont les modèles *Random Walk* et *Random Way Point*. Nous montrons l'impact de ces métriques sur les performances en termes de taux de livraison de paquets, de surcoût normalisé et de ruptures de routes.

La seconde solution est une protection par redondance de routes qui s'appuie sur un protocole de routage *multipath*. Dans cette architecture, l'opération de recouvrement consiste soit à un basculement sur une route secondaire soit à une nouvelle découverte. Nous montrons que la redondance de routes améliore la robustesse de la communication en réduisant le temps de restauration. Ensuite, nous proposons une comparaison analytique entre les différentes politiques de recouvrement d'un protocole *multipath*. Nous en deduisons qu'un recouvrement segmenté donne les meilleurs résultats en termes de temps de restauration et de fiabilité.

Mots clés : réseaux ad hoc, robustesse, mobilité, redondance, multipath, fiabilité, métrique de routage

---

Abstract :

Due to the unreliability characteristics of wireless communications, and nodes mobility, Mobile Ad hoc Networks (MANETs) suffer from frequent failures and reactivation of links. Consequently, the routes frequently change, causing significant number of routing packets to discover new routes, leading to increased network congestion and transmission latency. Therefore, MANETs demand robust protocol design at all layers of the communication protocol stack, particularly at the MAC, the routing and transport layers.

In this thesis, we adopt robustness approach to improve communication performance in MANET. We propose and study two protection architectures (protection by predictive analysis and protection by routes redundancy) which are coupled with a routing level restoration. The routing protocol is responsible of the failure detection phase, and uses the mechanism of link-level notifications to detect link failures.

Our first proposition is based on *unipath* reactive routing protocol with a modified route selection criterion. The idea is to use metrics that can predict the future state of the route in order to improve their lifetime. Two predictive metrics based on the mobility of nodes are proposed : the routes reliability and, combining hop-count and reliability metrics. In order to determine the two predictive metrics, we propose an analytical formulation that computes link reliability between adjacent nodes. This formulation takes into account nodes mobility model and the the wireless communication characteristics including the collisions between packets and signal attenuations. Nodes mobility models studied are *Random Walk* and *Random Way Point*. We show the impact of these predictive metrics on the networks performance in terms of packet delivery ratio, normalized routing overhead and number of route failures.

The second proposition is based on *multipath* routing protocol. It is a protection mechanism based on route redundancy. In this architecture, the recovery operation is either to switch the traffic to alternate route or to compute a new route. We show that the routes redundancy technique improves the communication robustness by reducing the failure recovery time. We propose an analytical comparison between different recovery policies of *multipath* routing protocol. We deduce that segment recovery is the best recovery policy in terms of recovery time and reliability.

Keywords : ad hoc networks, robustness, mobility, redundancy, multipath, reliability, routing protcol metrics