Comparaison des stratégies de redondance dans les réseaux ad hoc

Amadou Baba Bagayoko, Béatrice Paillassa

Comparaison des stratégies de redondance dans les réseaux ad hoc

Amadou Baba Bagayoko — Béatrice Paillassa

Université de Toulouse
Laboratoire IRIT – ENSEEIHT UMR CNRS 5505
2, rue Camichel 31071 Toulouse, France
E-mail: {amadoubaba.bagayoko, beatrice.paillassa}@enseeiht.fr

RÉSUMÉ. *Dans ce papier, nous analysons une approche originale en combinant les processus de recouvrement de route et de chemin dans un réseau ad hoc hétérogène utilisant deux technologies sans fil Zigbee et WiFi pour améliorer la robustesse du réseau. 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 de 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. Il apparaît aussi qu'en terme de fiabilité, la gestion des pannes de la route primaire doit s'effectuer au niveau du routage par des protocoles multipath plutôt que par la couche transport.*

ABSTRACT. *This paper analyzes an original approach aiming to improve the ad hoc robustness. It combines route and path recovery process in heterogeneous ad hoc networks (Zigbee and WiFi technologies). A multi-redundancy framework based on IEEE and IEFT protocols is proposed in order to manage the fault detection on primary communication path and the fault recovery by switching traffic on an alternate path. The three recovery policies (link-to-link, end-to-end path and segment path) are studied and compared through an analytical approach. Evaluation shows segment recovery interest, and the advantage to monitor the primary path at routing level by multipath routing protocol rather than to monitor it at transport level by transport protocol.*

MOTS-CLÉS : *réseau mobile ad hoc; redondance ; multi-domiciliation; multi-technologie; processus et politique de recouvrement; robustesse; fiabilité.*

KEY WORDS: *mobile ad hoc network; redundancy; multipath; multihoming; multi-technology architecture; robustness and recovery policy; reliability.*

1. Introduction

Les réseaux sans fil sont sujets à des perturbations voire des pannes de liens en raison des caractéristiques intrinsèques de leur support de communication ; ces pannes de liens sont aggravées par les particularités de relayage et de mobilité dans les réseaux de capteurs et ad hoc. Ces réseaux requièrent donc la conception et la mise en œuvre de protocoles robustes au niveau de toutes les couches de la pile protocolaire, en particulier au niveau des fonctions d'accès et de routage. Un moyen d'améliorer la robustesse du réseau est d'apporter une certaine redondance dans le but de protéger un élément réseau de sorte qu'il soit remplacé en cas de panne. En fonction de l'objectif de la mise œuvre de la redondance, il existe différentes manières d'améliorer la fiabilité du réseau au niveau de la pile protocolaire. Il est ainsi possible de protéger un lien, une route ou un chemin. La combinaison des différents niveaux de protection est également possible.

Plus précisément, pour protéger un lien, un nœud peut utiliser deux types de technologies sans fil de différentes portées et différentes caractéristiques de puissance afin de résister aux défaillances de mode commun. Par exemple dans Bluetooth 3.0, un nœud peut communiquer simultanément avec Bluetooth et WiFi [BLU], [YUA 07] étudie les contraintes liées à l'utilisation conjointe des technologies Zigbee/WiFi.

Les protocoles de routage *multipath* assurent une protection de niveau routage (protection de route) ; contrairement aux protocoles de routage réactifs classiques (*unipath*), ils établissent deux ou plusieurs routes entre une source et une destination en fonction de la topologie du réseau. Une façon simple d'améliorer la probabilité de livraison des paquets est d'envoyer des copies multiples d'un même paquet sur des chemins différents. 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 autre approche consiste à utiliser le routage *multipath* uniquement pour assurer une reprise rapide du trafic après une rupture de route. Ainsi, lors de la découverte de route, le protocole établira un ensemble de routes classées selon un critère spécifique. La meilleure route construite appelée route primaire sera utilisée pour envoyer le trafic jusqu'à ce qu'une panne (de liens ou de nœuds) survienne sur celle-ci. Après la détection de la panne, le trafic sera basculé sur la première route secondaire. L'intérêt de la redondance de route dépend de la probabilité qu'une route secondaire soit en bon état, lorsque la route primaire tombe en panne. Pour montrer l'avantage de la redondance dans un protocole réactif, comparons simplement le temps nécessaire pour rétablir le trafic d'un protocole réactif *unipath* et d'un protocole réactif *multipath*. Soit p, la probabilité qu'une route secondaire fonctionne après une panne sur la route primaire. Notons respectivement T_{RD} et T_{FD}, les temps de découverte de route et de détection de panne. Approximons T_{RD}, le temps de découverte (une émission de requête et une émission de réponse) par deux fois T_{FD}, le temps de détection d'erreur (une émission des données en échec et une émission de message d'erreur) ($T_{RD} \approx 2\ T_{FD}$). Alors, le temps avant restauration du trafic avec un protocole sans redondance est $(T_{FD} + T_{RD})$ et $(p \times T_{FD} + (1-p) \times (2T_{FD} + T_{RD}))$ pour un protocole *multipath*. Alors, pour $p > 0{,}3$, le temps nécessaire au rétablissement du trafic avec un protocole réactif *multipath* est inférieur à celui nécessaire avec un protocole à route unique. Nous pouvons en déduire que lorsque dans un réseau mobile ad hoc, la probabilité de panne d'une route secondaire après panne de la route primaire est inférieure à 70%, le routage *multipath* améliore la

fiabilité du réseau. L'intérêt d'utiliser la redondance est aussi valable dans un protocole de routage proactif, comme indiqué dans MP-OLSR [YIJ 08].

Une autre possibilité d'améliorer la robustesse consiste à utiliser une redondance de niveau transport (*multihoming*) mise en œuvre par un protocole comme Stream Control Transport Protocol (SCTP)[STE 07]. Le *multihoming* se réfère à une situation dans laquelle un nœud peut utiliser plusieurs interfaces (ou adresses IP) pour communiquer avec un autre nœud. Plusieurs chemins peuvent alors être associés aux interfaces de la source et de la destination, avec comme avantage, l'augmentation de la probabilité de survie d'une session en présence d'une défaillance dans le réseau. Les données sont transférées sur le chemin principal alors que les chemins alternatifs sont surveillés de sorte qu'en cas de panne du chemin primaire, SCTP puisse basculer son trafic sur l'un des chemins alternatifs.

Lorsqu'une panne survient dans un réseau ad hoc, différentes politiques de recouvrement peuvent être envisagées. Il existe trois stratégies de base qui sont : le recouvrement lien par lien, le recouvrement de bout en bout et le recouvrement par segment de route. Dans le premier type de recouvrement, en cas de panne, le trafic est basculé sur le lien alternatif, 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 disjointe de la route primaire, la récupération est un recouvrement de bout en bout. Au contraire, en cas d'éléments réseau communs (lien ou nœud) entre les 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 toutes les politiques de recouvrement sont applicables, une politique apportera un meilleur gain en terme 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 cet article, nous proposons un cadre original pour évaluer l'efficacité des mécanismes de redondance. A cet effet, pour chaque politique de recouvrement de base, nous formulons une expression analytique de la fiabilité de l'ensemble des routes (primaire et secondaire). Le reste de cet article est organisé comme suit. Dans la section 2, nous décrivons et discutons les travaux effectués sur les mécanismes de redondance. Nous détaillons notre architecture de redondance multi-niveau dans la section 3. Les politiques de recouvrement sont analysées et un modèle analytique évaluant la fiabilité de méthodes de recouvrement de panne est proposé dans la section 4. La section 5 présente l'évaluation des performances.

2. Etat de l'art

De nombreux protocoles de routage *multipath* ont été proposés par la littérature. En général, ils essaient d'établir des routes aussi disjointes que possible en nœud [LEE 01] et diffèrent selon leurs critères de sélection de route : minimum de sauts et fiabilité. Dans les réseaux ad hoc, AODV-BR [LEE 00], AOMDV [MAR 06], et MDYMO [KOL 07] qui sont des versions *multipath* des protocoles de routage standards, 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 [LEU 01], LET [DAN 08], et BSR [GUO 05], quant à eux, ils utilisent la stabilité et la fiabilité comme critère. 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.

Dans [CHA 07], deux niveaux de protection, le routage *multipath* et le *multihoming* transport, sont combinés dans un réseau mono-technologique. L'intérêt de l'architecture de redondance en termes d'augmentation de taux de livraison de paquets est montré par simulation. Toutefois, une intégration *multihoming-multipath* dans un réseau mobile ad hoc nécessite des modifications pour prendre en compte la multi-domiciliation des nœuds et coordonner les processus de recouvrement entre les deux couches. Tout d'abord, le protocole de routage considère chaque interface (une adresse IP) comme un nœud. Ainsi un nœud multi-domicilié avec plusieurs interfaces N est considéré comme N nœuds différents. Un protocole qui essaie d'établir des chemins disjoints au maximum, peut alors établir N routes sur différentes interfaces d'un même nœud. Le protocole considérera ces routes comme disjointes, car établies sur différentes adresses IP ; le déplacement de ce nœud entraîne la rupture des N routes. Il est également possible d'obtenir des routes partageant les mêmes nœuds mais utilisant différentes technologies de transmission. Dans ce cas, seul le recouvrement lien par lien est possible entre les nœuds adjacents. Cependant, lorsque la distance inter-nœud devient supérieure à celle de la technologie ayant la plus grande portée, la restauration par le schéma de recouvrement lien par lien n'est plus possible. Un autre problème d'intégration des niveaux de redondance peut survenir lorsque deux nœuds multi-domiciliés sont reliés par deux chemins transport différents, le protocole de routage n'est pas au courant de l'existence d'une route alternative, car le couple d'adresses IP source et destination utilisé par le chemin secondaire est différent de celui utilisé par le primaire. Ainsi, en cas de détection d'une rupture de la route primaire, le protocole de routage tente de reconstruire une nouvelle route bloquant ainsi la récupération de niveau transport.

Pour permettre l'intégration de la protection *multihoming-multipath*, la première solution est d'identifier chaque nœud multi-domicilié par un identifiant. Cet identifiant peut être un identifiant HIP [MOS 06] ou encore, un identifiant SHIMv6, si IPv6 est présent. Cependant, même lorsque les nœuds sont identifiés de façon unique, la source ne peut pas utiliser le chemin secondaire après une rupture, car le routage est incapable d'utiliser les informations disponibles au niveau transport ; il est nécessaire d'utiliser un mécanisme de *Cross-Layer* entre les fonctions routage et transport. L'inter-couche définie assurera les services de stockage et de récupération et de partage des données. L'interface notée DCLI (Distributed Cross Layer Interface) est présente sur tous les nœuds (figure 1).

3. Architecture de redondance multi-niveau

L'architecture de redondance multi-niveau qui utilise deux technologies sans fil (IEEE 802.11 et 802.15.4) dans un réseau ad hoc est présentée en figure 1. Elle s'appuie sur des protocoles

standardisés IEEE et IETF. Dans [BAG 09], nous avons montré l'intérêt de la redondance dans un réseau ad hoc en terme de fiabilité. Nous avons aussi observé qu'une redondance supérieure à deux n'était pas souhaitable car elle augmente inutilement la complexité de l'architecture pour une amélioration très faible de la fiabilité d'acheminement. Nous proposons donc une architecture de redondance double avec une double technologie (Zigbee et WiFi) et deux routes différentes. La route primaire utilisera des liens Zigbee alors que les liens WiFi assurent leur protection. Le protocole transport est en charge de la multi-domiciliation. Le routage *multipath* établit des routes à la demande. Selon la topologie, ces routes peuvent être soit disjointes de bout en bout soit disjointes sur certains segments de routes. Un nœud peut posséder soit une seule soit deux technologies (WiFi et Zigbee), dans ce cas, il est capable de recevoir et d'envoyer des données vers / depuis les deux technologies.

La gestion du recouvrement d'une route après une panne est composée de différentes étapes [FAR 06] : la détection de la panne, la notification de la panne, l'opération de restauration, et la reprise du trafic. Ces processus peuvent être mis en œuvre à différents niveaux de l'architecture selon la politique de recouvrement choisi. Nous distinguons trois politiques de recouvrement 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 la politique de recouvrement lien par lien, chaque lien Zigbee de la route primaire est protégé par un lien WiFi (figure 2.a). En cas de rupture d'un lien Zigbee entre deux nœuds voisins,

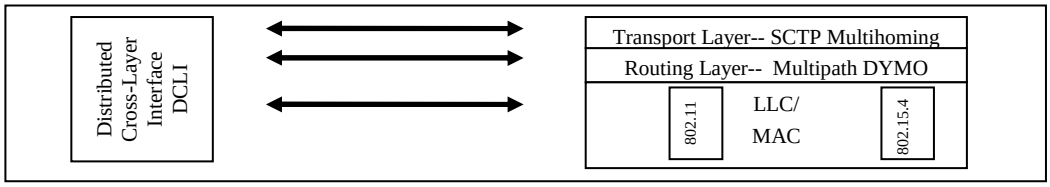
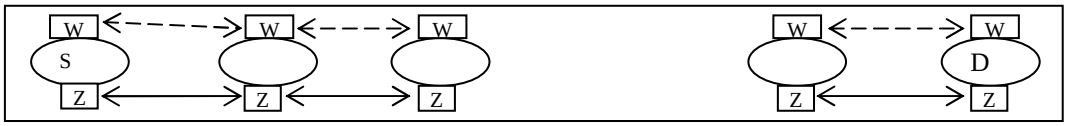
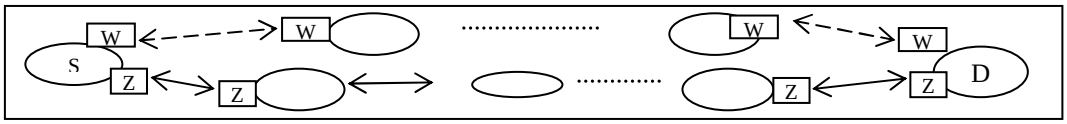


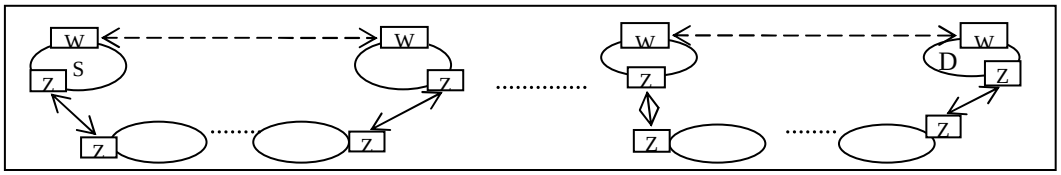
Figure 1. *Architecture de redondance multi-niveaux double technologie*



(a) *Recouvrement Lien par Lien*



(b) *Recouvrement de bout en bout*



(c) *Recouvrement par Segment de route*

Figure 2. *Politiques de Recouvrement (Lien par lien, de bout en bout, par segment de route)*

le trafic est immédiatement basculé sur le lien WiFi existant entre les nœuds ; si celui-ci n'est pas en panne. Contrairement à la route primaire, la route secondaire utilisée après la panne est une route multi-technologie. Elle utilise les liens Zigbee de la route primaire en bon état, et remplace ceux rompus par les liens WiFi. Dans ce schéma de recouvrement, chaque nœud doit être multi-domicilié.

Pour le recouvrement de bout en bout, la route primaire est établie sur les liens Zigbee, tandis que la secondaire est entièrement composée de liens WiFi (figure 2.b). Les routes établies sont disjointes en nœuds et en technologie. Contrairement au scénario précédent, à un instant donné, une route utilise une et une seule technologie de transmission. Seules la source et la destination doivent être multi-domiciliées ; les nœuds intermédiaires peuvent n'avoir qu'une seule technologie.

Dans le recouvrement par segment de route, l'ensemble des routes entre la source et la destination est composé de plusieurs sous-réseaux de routes. Chaque sous-réseau de routes est constitué de deux segments disjoints ayant aussi des technologies différentes. En raison de la différence entre la portée de transmission des deux technologies considérées, le sous-réseau de route est composé d'un ensemble de liens Zigbee sur la route principale et d'un lien WiFi pour la route secondaire (figure 2.c). Les nœuds de bordure (entrée et sortie) d'un sous-réseau doivent être multi-domiciliés ; les nœuds intermédiaires du réseau peuvent être mono-technologie.

4. Analyse des politiques de recouvrement

Dans cette section, nous analysons les avantages de l'architecture proposée avec plusieurs politiques de recouvrement et proposons une formulation analytique de leur fiabilité. Nous utilisons l'approche des blocs de diagrammes de fiabilité. Le terme *Two-Terminal Reliability* (2TR) est défini comme la probabilité qu'un chemin de communication existe entre la source et la destination.

Un réseau mobile ad hoc est modélisé sous la forme d'un graphe G = (N, L) où N= {1,2, …|N|} constitue l'ensemble des nœuds du réseau, L représente l'ensemble de liens. *L.Z (i, i +1)* et *L.W (i, i +1)* sont respectivement les liens Zigbee et WiFi reliant les nœuds *i* et *(i +1)*.

La fiabilité d'un lien entre les nœuds *i* et *(i +1)* durant l'intervalle *[t, t + T]* est la probabilité que les nœuds *i* et *(i +1)* puissent communiquer continuellement durant cet intervalle. La fiabilité est donc une grandeur mesurée sur un intervalle contrairement à la disponibilité qui est une grandeur instantanée liée à des cycles de panne-restauration. $R_{L.Z\ (i,\ i\ +1)}$ et $R_{L.W\ (i,\ i\ +1)}$ sont respectivement la fiabilité du lien actif utilisant la technologie Zigbee, WiFi. La fiabilité du nœud *i* est notée $R_{Nod\ (i)}$.

4.1. *Recouvrement lien par lien*

La fiabilité du recouvrement lien par lien notée $2TR_{L2L}(Z_N, W_N)$ (Two Terminal Reliability with Link-to-Link) dans laquelle N liens Zigbee sont protégés par N liens WiFi est:

$$2TR_{L2L}(Z_N, W_N) = R_{Nod\ (N)} \times \prod_{j=0}^{N} \left(R_{Nod\ (j)} \times R_{ZW\ (j,j+1)} \right). \quad [1]$$

$R_{ZW(j,j+1)}$ la fiabilité de l'ensemble des liens reliant les nœuds *j* et *(j+1)* est :

$$R_{ZW(j,j+1)} = 1-(1- R_{L.Z(j,j+1)}) \times (1- R_{L.W(j,j+1)}). \quad [2]$$

La rupture de la route primaire est détectée par les entités de la couche liaison des deux nœuds adjacents au lien rompu. Chacun de ces nœuds localise la panne puis envoie une notification de panne à sa couche gestionnaire de pannes, DCLI. Ensuite, cette entité notifie la panne à la couche réseau qui supprime toutes les routes contenant le lien rompu. Le recouvrement est assuré par le DCLI du nœud amont dans le sens source-destination qui bascule le trafic sur le lien WIFI alternatif, s'il n'est pas rompu.

Le principal avantage de cette politique est une bonne résistance à un environnement bruyant. En outre, comme le domaine de recouvrement est très court (un lien), elle assure un recouvrement rapide. Toutefois, elle ne résiste pas à une panne de nœud sur le chemin primaire. Le recouvrement lien par lien est adapté à des protocoles de routage de type *hop-by-hop* avec une faible mobilité.

4.2. *Recouvrement de bout en bout*

La fiabilité du recouvrement de bout en bout nommée $2TR_{E2E}(Z_N, W_M)$ (Two Terminal Reliability with End-to-End) dépend des fiabilités $2TR(Z_N)$ des N liens Zigbee (Two Terminal Reliability on N Zigbee links) et de $2TR(W_M)$ des liens M WiFi (Two Terminal Reliability on M WiFi links). Notons respectivement la source et la destination, *nod(0) et nod (dst).*

$$2TR_{E2E}(Z_N, W_N) = R_{nod\ (0)} \times R_{nod\ (dst)} \times [1-(1-2TR(Z_N)) \times (1-2TR(W_N)). \quad [3]$$

$$2TR(Z_N) = R_{L.Z\ [nod(0),\ nod(1)\ ]} \times \prod_{j=1}^{N-1} \left(R_{L.Z(\ j,j+1)} \right) \times \left(R_{Nod\ (j)} \right). \quad [4]$$

$$2TR(W_M) = R_{L.W\ [nod(0),\ nod(1)\ ]} \times \prod_{j=1}^{M-1} \left(R_{L.W(\ j,j+1)} \right) \times \left(R_{Nod\ (j)} \right). \quad [5]$$

Comme précédemment, les couches liaison des nœuds adjacents au lien rompu détectent l'état de panne, et le notifient au DCLI qui à son tour informe la couche réseau pour supprimer toutes les routes utilisant le lien rompu. Ensuite, la couche réseau du nœud adjacent en amont envoie une notification de panne inter-nœud via un message d'erreur de route (Route Error-- RERR) vers les sources. Quand un nœud intermédiaire reçoit un RERR, il réalise la notification de panne intra-nœud et, enfin, la notification de panne inter-nœud. Enfin, lors de la réception d'un RERR, la source procède à l'opération de restauration. L'entité DCLI de la source effectue le changement de route sur la route secondaire. Après cela, la couche de transport peut effectuer la reprise du trafic.

La politique de recouvrement de bout en bout résiste aux défaillances simultanées de plusieurs éléments réseau (liens, nœuds) sur le chemin primaire. Le processus de recouvrement peut être effectué par divers type de protocoles de routage (routage source et hop-by-hop). 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. Comme le domaine de recouvrement est le chemin complet, la durée totale du processus de recouvrement est importante et, en cas de panne de lien simultanée sur le chemin primaire et sur le chemin secondaire, aucun recouvrement n'est possible.

4.3. *Recouvrement par segment de route*

Considérons un réseau composé de M liens WiFi et divisé en M sous-réseaux. Un sous-réseau commence par un nœud avec une carte WiFi et se termine au prochain nœud sur la route ayant une carte WiFi. Chaque sous-réseau composé de *n* liens Zigbee est caractérisé par une fiabilité notée 2TR (Z_n, W_1). La valeur de *n* dépend de la portée de transmission des deux technologies considérées. Ainsi, la fiabilité du recouvrement de type segment $2TR_S(Z_N, W_M)$ (Two Terminal Reliability with Segment) est une multiplication de la fiabilité des M sous-réseaux.

$$2TR_S(Z_N, W_M) = R_{Nod(M)} \times \prod_{j=0}^{M-1} \left(R_{Nod(j)} \times 2TR(Z_n, W_1)\right). \quad [6]$$

N est le nombre de liens Zigbee entre une source et une destination N = *n* × M, où *n* est le nombre de liens Zigbee entre les nœuds de bordure (entrée et sortie) d'un sous-réseau.

$$2TR(Z_n, W_1) = 1-[1-2TR(Z_n)] \times [1-2TR(W_1)]. \quad [7]$$

La gestion du recouvrement est similaire à celle du recouvrement lien par lien à l'exception de l'opération de restauration. Contrairement au recouvrement lien par lien, le nœud qui effectue cette étape, bascule le trafic sur un segment composé de liens WiFi (s'il existe encore) plutôt que sur un unique lien. Notons qu'avec cette technique, la panne est transparente à la source. Le domaine de recouvrement est plus petit que l'ensemble de la route (pour une route avec au moins 2 segments) ; en général son recouvrement est plus rapide que celui de bout en bout. Le recouvrement par segment fournit une meilleure protection que celle proposée par le recouvrement de bout en bout. En effet, lorsque deux pannes simultanées surviennent sur la route primaire et la route secondaire, aucune reprise n'est possible avec le recouvrement de bout en bout ; alors que le recouvrement par segment isolera le segment en panne sur la route primaire pour le remplacer par un segment secondaire.

5. Evaluation de performances

Nous avons formulé analytiquement la fiabilité pour le recouvrement lien par lien, de bout en bout et par segment de routes durant l'intervalle de temps *[t; t + T]*. Les nœuds source et

destination communiquent selon les topologies des figures 2.a, 2.b et 2.c; où un lien WiFi correspond à deux liens Zigbee.

Dans les formules de fiabilité de recouvrement [1], [3], et [6], le paramètre de fiabilité de lien entre deux nœuds adjacents *i* et *(i +1)* est fonction de la durée de la communication, la portée de la technologie, et le modèle de mobilité. Concernant l'impact des interférences, nous supposons que tout au long de la simulation, les nœuds adaptent leurs puissances afin de conserver une même portée de transmission, même si la qualité du signal diminue ou augmente.

Les nœuds se déplacent selon le modèle de mobilité *Random Walk* pendant un temps *T* de communication qui se décompose en somme de Δt époque. 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 [YEZ 10]. 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. En considérant les hypothèses précédentes, dans [YEZ 10] les auteurs formulent la probabilité que le nœud *(i +1)* soit en dehors de la portée *r* du nœud *i* à l'instant $(t + \Delta t)$ (c'est-à-dire $d_{i,(i+1)}(t+\Delta t) > r$) en sachant que le nœud *(i +1)* était dans la portée du nœud *i* à l'instant *t*. Si nous négligeons les interférences et les effets de fading, nous pouvons déduire $R_L(t, t + \Delta t)$ la fiabilité du lien durant $[t; t + \Delta t]$:

$$R_L(t,t+\Delta t) = 1 - \left[\frac{1}{\pi r^2} \times 2v\Delta t \times \left(r - \frac{\pi v \Delta t}{8} \right) \right]. \qquad [8]$$

Précisons, la fiabilité des liens WiFi et Zigbee ($R_{L.W\,(i,\,i+1)}$ et $R_{L.Z\,(i,\,i+1)}$) dans $[t; t + \Delta t]$ avec les paramètres r_{WiFi} = 150 mètres, r_{Zigbee}=75 mètres, v_{max} = 5 mètres / sec et Δt = 0,01 sec.

Notons qu'un lien WiFi est toujours plus fiable qu'un lien Zigbee car la portée WiFi est le double de celle de Zigbee. Dans cette évaluation, tous les nœuds sont fiables; $R_{Nod(i)}=1; \forall\, i \in N$.

Les figures 3, 4, 5, 6, et 7 permettent de comparer les trois schémas de recouvrement en fonction de la durée de communication pour respectivement N = 4, 6, 8, 10 nombre de liens Zigbee entre la source et la destination.

Des résultats attendus sont observables. Sur toutes les figures, pour les trois schémas de recouvrement, la fiabilité de la route diminue lorsque la durée de communication augmente, et quand N augmente, la fiabilité des routes diminue parce que plus il y a de liens entre la source et la destination, plus la probabilité de rupture de la route augmente.

Concernant les politiques de recouvrement, nous observons que le recouvrement par segment est toujours le meilleur schéma quelle que soit la valeur de N (nombre de liens Zigbee). Ceci pour deux raisons: il possède un domaine de recouvrement plus petit que le recouvrement de bout en bout et par rapport au recouvrement lien par lien, ses routes possèdent moins de liens.

Notons *TI*, le temps d'intersection entre la fiabilité du recouvrement de bout en bout et celle du recouvrement de type lien par lien. Nous remarquons que *TI* augmente en fonction du nombre nœuds intermédiaires. *(TI (N = 4) = 32,4 sec; TI (N = 6) = 36.2sec; TI (N= 8) = 37,2 sec et TI (N = 10) = 38 sec).*

Le recouvrement lien par lien est meilleur que le recouvrement de bout en bout pour des durées de communication courtes et moyennes, alors que le recouvrement de bout en bout est plus fiable que le schéma de recouvrement lien par lien pour des durées de communication longues. Cela est

dû à l'augmentation de la corrélation des pannes entre les liens Zigbee et WiFi en fonction de la durée de communication.

L'analyse des trois politiques présentées dans un réseau sans mobilité donne des résultats semblables. Seule la méthode de calcul de la fiabilité des liens change. La fiabilité d'un lien sera fonction du modèle de propagation et des puissances d'émission et de réception des nœuds.

D'autre part, quelles que soient les longueurs des segments dans le recouvrement par segment, les conclusions de notre analyse restent valables.

A partir de ces résultats, une comparaison globale entre les trois politiques de recouvrement est synthétisée dans le tableau 1. Il comprend la valeur de la fiabilité (amélioration de la fiabilité), déduite à partir des résultats de simulation ci-dessus, mais aussi du type de panne pris en charge, (défaillance d'un nœud sur le chemin principal, pannes simultanées), et le temps de recouvrement présenté dans les sections précédentes.

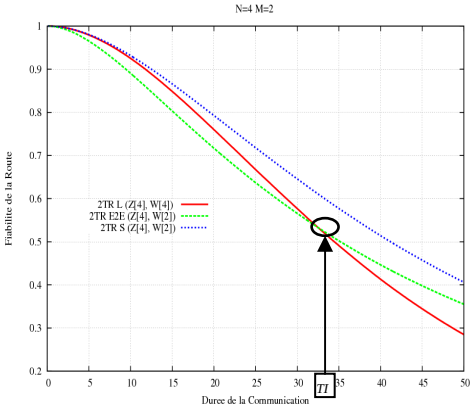


Figure 3. *Fiabilité de la route N=4 Liens Zigbee vs Durée de la communication*

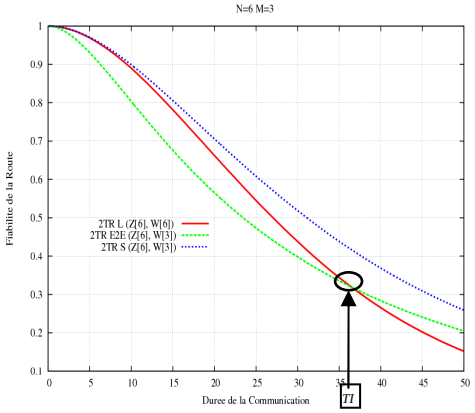


Figure 4.*Fiabilité de la route N=6 Liens Zigbee vs Durée de la communication*

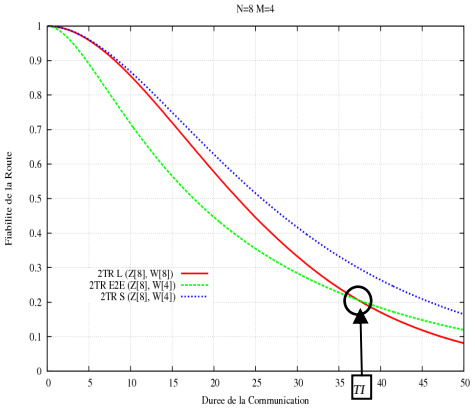


Figure 5. *Fiabilité de la route N=8 Liens Zigbee vs Durée de la communication*

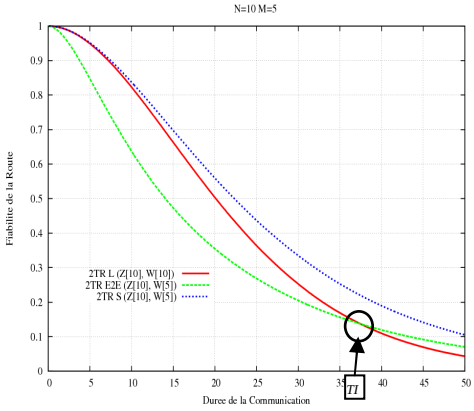


Figure 6. *Fiabilité de la route N=10 Liens Zigbee vs Durée de la communication*

Tableau 1. *Comparaison des différents schémas de recouvrement*

		Lien par lien	**De bout en bout**	**Segment de route**
Temps de Recouvrement		+++	+	++
Panne de nœud sur le chemin primaire		Non	Oui	Non
Panne simultanée : chemins primaire et secondaire		Nœud : Non Lien: Oui	Nœud: Non Lien: Non	Nœud: Non Lien: Oui
Gain en fiabilité	courtes et moyennes durées	++	+	+++
	Longues durées	+	++	+++

6. Conclusion

Ce document étudie les principaux mécanismes de protection présents dans la littérature pour améliorer la robustesse des routes dans un réseau mobile ad hoc. Nous proposons une approche originale en intégrant deux types de redondance (*multipath* et *multihoming*) avec une double technologie (WiFi et Zigbee) dans les réseaux ad hoc, ainsi améliorer la fiabilité du réseau.

Trois politiques de recouvrement sont analysées, le recouvrement lien par lien, le recouvrement de bout en bout et le recouvrement par segment de route. Leurs fiabilités sont formulées et évaluées.

La fiabilité d'une route dépendant de la fiabilité de tous les éléments réseau la composant, les principaux paramètres de l'évaluation sont donc la longueur de la route et la fiabilité des liens qui dépend des paramètres comme la portée et la mobilité des nœuds. Toutefois, quelle que soient les valeurs des paramètres, les résultats de l'analyse indiquent que le recouvrement de bout en bout et le recouvrement par segment améliorent la fiabilité de la communication par rapport une approche sans redondance. Néanmoins, d'autres critères doivent être pris en compte pour l'analyse d'une politique de recouvrement comme la topologie du réseau (routes disjointes ou non) et les caractéristiques du nœud (multi-domicilié ou non), et les exigences de l'application utilisatrice en terme de robustesse. Dans ce papier, nous proposons une classification d'intérêt des politiques de recouvrement en fonction de la durée de communication, les catégories de pannes supportées et le temps nécessaire au recouvrement. Ainsi, lorsqu'une application utilisatrice requiert un temps de recouvrement le plus court possible (par exemple processus à temps réel), le recouvrement lien par lien sera préféré car il assure un meilleur temps de recouvrement. Lorsque l'application souhaite optimiser la fiabilité des routes utilisées, le recouvrement par segment est préférable.

Un autre résultat intéressant et original que nous pouvons déduire de l’article, concerne les protocoles de communication. Il semble préférable de gérer la protection au niveau de routage plutôt qu'au niveau transport. Le protocole de routage prendrait en charge de la détection de la panne, le recouvrement de la route et aussi la reprise du trafic. Ainsi, le protocole de transport SCTP ne surveillera plus les chemins secondaires. Nous proposons d'utiliser un protocole de transport *multihoming* pour la gestion des adresses multiples, le contrôle de congestion et la reprise du trafic. Ainsi, un protocole tel que MP-TCP étudié par l'IETF serait préférable à SCTP avec les protocoles de routage *multipath*.

La suite de ce travail considère une méthode de calcul de fiabilité qui intègre l’hétérogénéité de la fiabilité des liens. Cette méthode prend en compte la distance initiale inter-nœuds. Les

techniques de recouvrement et la méthode analytique seront combinées au sein d'un protocole de routage *multipath* basé sur la fiabilité.

7. Bibliographie

[BAG 09] Bagayoko A.B., Paillassa B., Betous-Almeida C., « Transport and Routing Redundancy for MANETs Robustness » *Parallel and Distributed Processing with Applications, 2009 IEEE International Symposium on (ISPA'09), Chengdu, Sichuan, China,* Août 2009, p. 348 – 353.

[BLU] Bluetooth SIG Technology. Diponible sur www.bluetooth.org

[CHA 07] Charoenpanyasak S., Paillassa B., « SCTP multihoming with Cross Layer Interface in Ad Hoc Multihomed Networks » *IEEE WiMob'07, White Plains, New York USA,* Oct 2007, p. 46-52.

[DAN 08] Dana A., Zadeh A.K., Sadat-Noori S., « Backup path set selection in ad hoc wireless using link expiration time » *Computers and Electrical Engineering, Vol. 34 Issue 6,* Nov. 2008, p. 503-519.

[FAR 06] Farriel A., Bryskin I., *GMPLS Architecture and Applications,* Editions Morgan Kaufmann, Elsevier Inc, 2006.

[GUO 05] Guo S., Yang O., Shu Y., « Improving source routing reliability in mobile ad hoc networks » *IEEE Parallel and Distributed Systems, Vol. 16, n°4,* Av 2005, p. 362-373.

[KOL 07] Koltsidas G., Palvidou F., Kuladinithi K., Timm-Giel A., Gorg C., « Investigating the performance of multipath protocol for ad-hoc networks » *IEEE PIMRC 2007, Athens,* Sept 2007, p.1-5.

[LEE 00] Lee S.J., Gerla M., « AODV-BR: Backup Routing in Ad hoc Networks » *IEEE Wireless Communication and Networking Conference (WCNC'00), Chicago,* Sept. 2000, p. 1311-1316.

[LEE 01] Lee S.J., Gerla M., « Split Multipath Routing with Maximally Disjoints Paths in Ad Hoc Networks » *IEEE ICC 2001, Vol. 10, Helsinki,* Juin 2001, p. 3201-3205.

[LEU 01] Leung R., Liu J., Poon E., Chan A.C., Li B., « MP-DSR: A QoS-Aware Multi-Path Dynamic Source Routing Protocol for Wireless Ad-Hoc Networks » *IEEE LCN'01, Tampa,* Nov.2 001 , p 132-142.

[MAR 06] Marina M.K., Das S.R., « Ad hoc on-demand multipath distance vector routing » *Wireless Communications and Mobile Computing (WCMC'06), Vol. 6, Issue 7,* Nov. 2006, p. 969–988.

[MOS 06] Moskowitz R., Nikander P., «Host Identity Protocol (HIP) Architecture", RFC 4423, Mai 2006.

[STE 07] Stewart R., « Stream Control transmission Protocol » *RFC 4960, IETF,* Sept. 2007.

[YEZ 10] Ye Z., Abouzeid A., «A unified model for joint throughput-overhead analysis of mobile ad hoc networks » *Computer Networks,* Elsevier Inc. *Vol. 54, Issue 4,* Mars 2010, p. 573-588

[YIJ 08] Yi J., Cizron E., Hamma S., Parrein B., "Simulation and performance analysis of MP-OLSR for mobile ad-hoc networks" *IEEE WCNC 2008, Las Vegas,* 31 Mars-3 Avril 2008, p. 2235-2240.

[YUA 07] Yuan W., Wang X., Linnartz J-P., « A Coexistence Model of IEEE 802.15.4 and IEEE 802.11 b/g » *IEEE 14th SCVT'07, Delft, The Netherlands,* November 2007, p. 1-5.