ÉCOLE DE TECHNOLOGIE SUPÉRIEURE
UNIVERSITÉ DU QUÉBEC

MÉMOIRE PRÉSENTÉ À
L'ÉCOLE DE TECHNOLOGIE SUPÉRIEURE

COMME EXIGENCE PARTIELLE
À L'OBTENTION MAITRISE EN GÉNIE
CONCENTRATION RÉSEAUX DE TÉLÉCOMMUNICATIONS
M. Ing.

PAR
Djedjiga BENZID

LE RÉSEAU PRIVÉ VIRTUEL (VPN) SUR LES RÉSEAUX MAILLÉS SANS FIL WMN

MONTRÉAL, LE 11 MARS 2014

PRÉSENTATION DU JURY

CE MÉMOIRE A ÉTÉ ÉVALUÉ

PAR UN JURY COMPOSÉ DE :

M. Michel Kadoch, directeur du mémoire
Département de Génie Électrique à l'École de technologie supérieure

M. Alain April, président du jury
Département de Génie logiciel et des TI à l'École de technologie supérieure

M. Gherbi Abdelouahed, membre du jury
Département de Génie logiciel et des TI à l'École de technologie supérieure

IL A FAIT L'OBJET D'UNE SOUTENANCE DEVANT JURY ET PUBLIC

12 FÉVRIER 2014

À L'ÉCOLE DE TECHNOLOGIE SUPÉRIEURE

REMERCIEMENTS

J'aimerais, en premier lieu, témoigner ma gratitude à mon directeur de recherche Monsieur Michel Kadoch, pour son encadrement tout au long de ce travail. Je le remercie pour son temps, sa patience, ses bonnes orientations et ses précieux conseils.

Mes sincères remerciements vont également à Monsieur Alain April, président du jury, et Monsieur Gherbi Abdelouhed, membre du jury pour l'intérêt qu'ils ont porté à notre recherche en acceptant d'examiner ce travail.

Je remercie Chafika TATA qui a accepté de m'aider dans la relecture et la correction de ce mémoire, je la remercie aussi pour son appui, et pour ses conseils judicieux.

Mes profonds remerciements vont à toute ma famille et mes amis pour leur support continu qu'ils m'ont apporté tout au long de ma démarche.

RÉSEAU PRIVÉ VIRTUEL(VPN) SUR LES RÉSEAUX MAILLÉS SANS FIL WMN

Djedjiga BENZID

RÉSUMÉ

Les Réseaux Privés Virtuels (VPN) peuvent offrir une grande sécurité aux réseaux maillés sans fil (WMN). Toutefois, le déploiement conjoint des deux technologies devient problématique pour la gestion de la mobilité IP dont souffrent déjà les deux réseaux. En effet, diverses solutions ont été proposées pour assurer un handoff VPN rapide et transparent sur les réseaux sans fil. Cependant, ces solutions ne peuvent pas fonctionner convenablement sur les WMNs qui ont des caractéristiques de multi saut et une topologie dynamique. À cet effet, une nouvelle approche est proposée, l'algorithme Seamless Handoff VPN pour les réseaux maillés sans fil (SHVM). Celui-ci repose sur trois conceptions, à savoir la conception de chemin optimal, la conception de CE (Customer Edge) basés sur VRF et la conception de l'application de l'adresse statique de VPN. L'objectif de la solution proposée est de réduire le délai de handoff et de minimiser le taux de perte de paquets. Le modèle proposé est supposé être sécurisé avec la technologie MPLS-VPN. Dans le but de valider notre approche, le modèle a été simulé sur OPNET 16. Les résultats obtenus montrent que le délai et le taux de pertes de paquets sont effectivement inférieurs aux normes requises pour assurer un seamless handoff pour une application en temps réel.

Mots clés : Mobilité IP, MPLS-VPN, QoS, Seamless Handoff , VPN, WMN.

VIRTUAL PRIVATE NETWORK OVER WIRELESS MESH NETWORKS

Djedjiga BENZID

ABSTRACT

Virtual Private Network (VPN) can enhance the security of Wireless Mesh Network (WMN). However, integrating these two technologies has several issues such as managing the nodes mobility. In the literature, many solutions of VPN handoff are suggested for wireless networks. Nevertheless, these schemes are not suitable with WMN networks, because of their dynamic topology and multi-hop routing. To address these issues, a new approach is proposed in this work, called Seamless Handoff VPN for wireless Mesh networks (SHVM). This scheme is based on three conceptions, namely, optimal path, Customer Edge (CE) based on Virtual Routing and Forwarding (VRF) and VPN static address. The main objective of SHVM is to reduce the handoff delay and packet loss rate. To validate our study, the proposed model is simulated on OPNET 16. Simulation results show that delay and packet loss are in fact reduced. Hence, SHVM has improved the network QoS performance in term of packet end to end delay and jitter.

Keywords: Mobile IP, MPLS-VPN, QoS, Seamless Handoff , VPN, WMN

TABLE DES MATIÈRES

LISTE DES TABLEAUX

Page

LISTE DES FIGURES

Page

LISTE DES ABRÉVIATIONS, SIGLES ET ACRONYMES

3Com	Computers Communication Compatibility
3DES	Triple Data Encryption Standard
AAA	Authentication, Authorization, Accounting/Auditing
AES	Advanced Encryption Standard
AP	Access Point
ARP	Address resolution protocol
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
BSS ID	Basic Service Set Identifier
CE	Customer Edge
CN	Correspondent Node
CNR	Carrier-to-Noise Ratio
CoA	Care-Of-Address
DHCP	Dynamic Host Configuration Protocol
DVD	Digital Versatile Disc
ESSID	Service Set Identifier
FA	Foreign Agent
FDDI	Fiber Distributed Data Interface
FreeBSD	Free Berkeley Software Distribution
FTP	File Transfer Protocol
GRE	Generic Routing Encapsulation
IDEA	International Data Encryption Algorithm
HA	Home Agent
HTTP	HyperText Transfer Protocol
IPsec	Internet Protocol Secrity

IPX	Internetwork Packet Exchange
ISP	Internet Service Provider
LAN	Local Area Network
L2L	LAN-to-LAN
L2TP	Layer 2 Tunneling Protocol
MD	Mobile Device
MD5	Message Digest 5
MEMO	Multiple-Input Multiple-Output
MIPv6	Mobile Internet Protocol v6
MN	Mobile Node
MPBGP	MultiProtocol BGP
MPLS	Multiprotocol Label Switching
MSAS	Mobile Security Access System
NEMO	Network Mobility Basic Support
NetBEUI	NetBIOS Frames Protocol
OFDM	Orthogonal Frequency Division Multiplexing
OPNET	Optimized Network Engineering Tool
OSI	Open Systems Interconnection
PC	Post Computer
PE	Provider Edge
PDA	Personal Digital Assistant
POP3	Post Office Protocol Version 3
PTP	Picture Transfer Protocol
QoS	Quality of Service
RC4	Rivest Cipher 4
RD	Route Distinguisher
RSA	Ronald Rivest, Adi Shamir Leonard Adleman
RSVP	Resource Reservation Protocol
RTP	Real Time Protocol
SEAL	Software Encryption Algorithm

SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SNR	Signal-to-Noise Ratio
SSL	Secure Sockets Layer
TCP/IP	Transmission Control Protocol /the Internet Protocol
TE	Traffic Engineering
Telnet	Telecommunication Network
TFTP	Trivial File Transfer Protocol
UWB	Ultra Wide Band
VPN	Virtual Private Network
VRF	VPN Routing and Forwarding
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WMN	Wireless Mesh Network

INTRODUCTION

L'évolution massive de la technologie de pointe a engendré une forte demande pour la communication à haut débit dans le domaine de la télécommunication. Pour répondre et satisfaire à cette demande, les concepteurs des réseaux internet emploient de nouvelles technologies pour concevoir des infrastructures qui peuvent répondre aux exigences des utilisateurs en termes de capacité et de sécurité. Les réseaux maillés sans fil sont parmi ces nouvelles technologies. Ils sont très répandus en raison de leurs caractéristiques pratiques, telles que leurs déploiements rapides et simplifiés, ainsi que pour leur forte tolérance aux pannes et aux interférences. Ces caractéristiques font de ces réseaux une solution économique attrayante pour fournir une connexion internet à haut débit dans des infrastructures où le déploiement du réseau filaire est difficile en termes de coût et de maintenance.

Les réseaux maillés sans fil ont une topologie dynamique qui se caractérise par l'absence d'une infrastructure de sécurité et par l'utilisation de moyens de communication non protégés. Ceci les rend vulnérables aux attaques et difficiles à contrôler et à sécuriser. Plusieurs mécanismes de sécurité ont été proposés pour pallier ces failles de sécurité. La technologie MPLS-VPN en fait partie (Muogilim, Loo et Comley, 2011).

Le VPN est une technologie qui permet d'établir des connexions privées et sécurisées entre deux entités. Il peut fournir un haut débit avec une grande sécurité sans influencer les performances du réseau. Son efficacité dépend de la technologie et des protocoles qui lui sont associés lors de son déploiement. Son utilisation avec d'autres technologies comme le MPLS apporte de la sécurité et de la performance aux réseaux. La technologie MPLS permet d'améliorer les performances du réseau VPN avec une plus grande diversité de services basés sur la politique de contrôle de gestion de réseau.

En effet, le MPLS-VPN peut assurer de la sécurité pour les clients mesh mobiles à l'intérieur de leurs domaines, car le nœud mobile maintient la connexion avec le routeur CE (Customer Edge). L**e** changement de l'endroit n'a pas d'influence sur l'acheminement du trafic dans VPN MPLS BGP, mais lorsque le nœud se déplace d'un site VPN à un autre site VPN, ceci devient problématique. Cela est dû à la difficulté d'assurer un handoff VPN sur WMN.
Cependant, bien que les VPNs soient utilisés pour sécuriser les réseaux maillés sans fil, le déploiement conjoint des deux technologies devient problématique pour la gestion de la mobilité dont souffrent déjà les deux technologies.

La gestion de la mobilité permet au terminal de maintenir la connexion et de localiser celui-ci quand il se déplace dans une nouvelle zone de service. Son étude inclut deux parties, à savoir, la gestion de handoff et la gestion de la localisation.(Srivatsa et Jiang, 2008).

Le processus de handoff peut être amélioré soit par smooth handoff (Belghoul, 2005) ,en réduisant le nombre de paquets perdus, soit par seamless handoff (Chen-Han, Jen-Shun et Ko-Ching, 2005),en diminuant la charge de la signalisation, ou bien en rendant le processus plus rapide en diminuant le délai de handoff. Dans ce dernier cas, on parle d'un fast handoff(Chen-Han, Jen-Shun et Ko-Ching, 2005).

Dans la recherche antérieure, l'étude de handoff VPN sur les réseaux maillés sans fil n'est en aucun cas abordée. Néanmoins des solutions de handoff VPN sur d'autres technologies de réseaux sans fil ont été proposées pour assurer un seamless handoff sur ces réseaux. Cependant celles-ci peuvent s'avérer inefficaces sur les réseaux maillés sans fil (Zhenxia et Boukerche, 2008).

D'autre part, plusieurs approches ont été élaborées pour assurer un handoff pour les réseaux WMN(Rongsheng, Chi et Yuguang, 2007). Ces approches fonctionnent convenablement dans le cas de WMN utilisant des protocoles de routage dynamique Manet, mais lors de l'introduction de la technologie VPN sur ces réseaux, ceci devient problématique, en raison de l'utilisation de la mobilité IP. Dans les réseaux maillés sans fil, la gestion de la mobilité IP

est problématique, car cette dernière ne prend pas en charge la topologie dynamique et le multi-saut entre les routeurs *mesh* de backbone de ces réseaux. Par conséquent, une solution pour la gestion de la mobilité pour une utilisation conjointe des VPNs et des réseaux maillés sans fil s'avère primordiale. Cette dernière doit prendre en considération les caractéristiques spécifiques des VPNs, telles que le protocole de routage IP et la mobilité IP et les caractéristiques des réseaux WMN telles que le multi saut ainsi la topologie dynamique. À cet effet, la gestion de la mobilité des VPNs sur les réseaux maillés sans fil fait l'objet de notre étude. Un algorithme Seamless Handoff VPN sur les réseaux maillés sans fil (SHVM) est proposé.

Le modèle SHVM est supposé être sécurisé avec la technologie MPLS-VPN, il est composé de trois conceptions, à savoir, la conception de chemin optimal, de CE basés sur VRF et de l'application de l'adresse statique de VPN. Le SHVM est un système qui vise à assurer un handoff rapide et transparent pour les VPNs sur les réseaux maillés sans fil. Ainsi l'objectif de cette étude est de réduire le délai de handoff et le taux de perte de paquets, afin de permettre aux nœuds de VPN mobiles de se connecter rapidement et d'une façon transparente à un nouveau point d'accès.

Notre étude s'est intéressée aussi à l'influence de SHVM sur les performances de qualité de service des WMNs. Pour cela les critères tels que la gigue et le délai de bout en bout ont été déterminés. Le modèle SHVM n'était pas dépourvue de contraintes. Des problèmes ont surgi dans le choix des paramètres sans fil tels que la puissance de transmission, le débit de transfert, et la vitesse de nœud. Pour mieux évaluer ces critères, et justifier notre choix de paramètres liés au réseau maillé sans fil, une étude portant sur la variation de ces paramètres a été effectuée et simulée sur le modèle proposé. Pour valider notre étude, SHVM a été modélisé et simulé avec une application voix avec le simulateur OPNET 16.

Le présent document est composé de cinq chapitres. Le premier chapitre concerne une description des caractéristiques des réseaux maillés sans fil ainsi que les différentes contraintes liées au déploiement de ces derniers. Le deuxième chapitre nous introduit aux

réseaux privés virtuels et décrit les différentes technologies et algorithmes qui lui sont associés pour la sécurisation des réseaux de télécommunications. Le troisième chapitre est une revue de littérature. Il relate différentes solutions des handoff VPNs sur les réseaux sans fil. Le quatrième chapitre décrit l'algorithme SHVM et son implémentation sur le simulateur OPNET 16. Le cinquième chapitre présente les simulations effectuées sur le modèle proposé ainsi que l'analyse et l'interprétation des résultats obtenus de ces simulations. On conclut ce document par une conclusion relatant les différentes étapes suivies pour l'aboutissement de notre objectif. Cette conclusion est suivie par un ensemble de suggestions et de perspectives sous forme de recommandations pour les futures recherches.

CHAPITRE 1

LES RÉSEAUX MAILLÉS SANS FIL

Introduction

Les réseaux maillés sans fil sont des réseaux sans fil à plusieurs sauts (multihop), ils sont dynamiquement auto-organisés et auto configurable, ils fournissent une couverture robuste et fiable à l'accès internet sans fil avec un faible cout de déploiement et de maintenance. Les réseaux WMN sont caractérisés par de nombreuses spécificités essentielles telles que l'architecture réseau, la densité de nœud, le nombre de canaux utilisé, la mobilité des nœuds, le modèle de trafic, et la portée de transmission. Dans ce chapitre un aperçu de ces caractéristiques est abordé, vu l'impact que ces dernières peuvent avoir sur le déploiement des WMNs.

1.1 Architecture des réseaux maillés sans fil

La topologie du réseau maillé sans fil se distingue par sa fiabilité, sa robustesse, et par ses propriétés d'auto-configuration. La topologie des réseaux maillés sans fil est formée de deux types de nœuds sans fil : les clients mesh et les routeurs mesh. La figure 1.1 illustre un exemple d'un réseau maillé sans fil (Misra et Subhas Chandra Misra, 2009).

Les clients mesh

Les clients mesh sont généralement équipés d'une seule interface radio supportant les fonctions réseau maillée. Ils ne fournissent pas les fonctionnalités de pont ou de passerelle nécessaires pour l'accès internet et l'interopérabilité avec d'autres technologies du réseau. Ils sont mobiles, et ils sont limités en matière de ressources d'approvisionnement d'énergie, de capacité de traitement, et de gamme de couverture radio.

Les routeurs mesh

Les routeurs mesh peuvent être des Points d'accès (AP), des capteurs, ou de stations de base pour les réseaux cellulaires. En outre, le routeur mesh est un dispositif matériel spécial doté d'interfaces à différentes technologies radio. Ceci lui permet de travailler avec différentes technologies sans fil et d'offrir de la connexion et des services aux clients mesh.

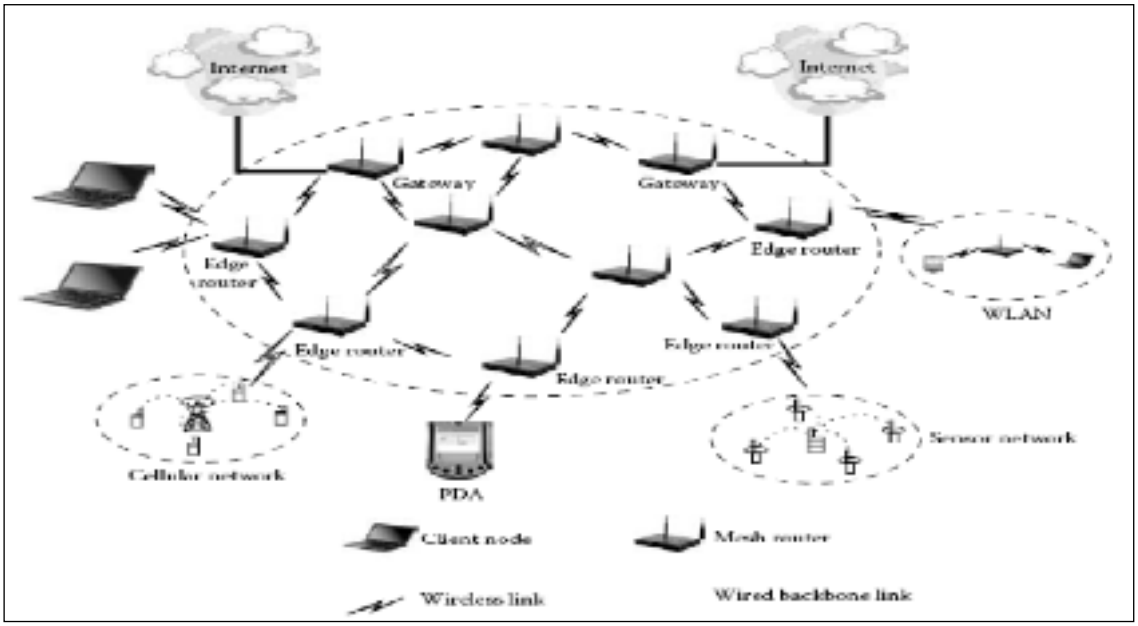

Figure 1.1 Architecture de réseau maillé sans fil
Tirée de Sudip Misra Subhas Chandra Misra (2009)

Les routeurs mesh sont plus puissants que les clients mesh en termes de capacité de traitement et de communication. Ils n'ont pas de contraintes d'approvisionnement d'énergie. L'architecture des WMNs peut être classifiée en trois types suivants :

1.1.1 Architecture d'infrastructure ou hiérarchique :

L'architecture hiérarchique, est formée de deux types de nœuds sans fil : les clients mesh et les routeurs mesh, interconnectés par le moyen d'un média sans fil. Dans l'architecture hiérarchique de WMN, les technologies des réseaux sans fil telles qu'IEEE 802.11, IEEE 802.15, IEEE 802.16, et IEEE 802.20 sont utilisées pour l'implémentation des WMNS. Un exemple de ce type d'architecture est représenté dans la figure 1.2.

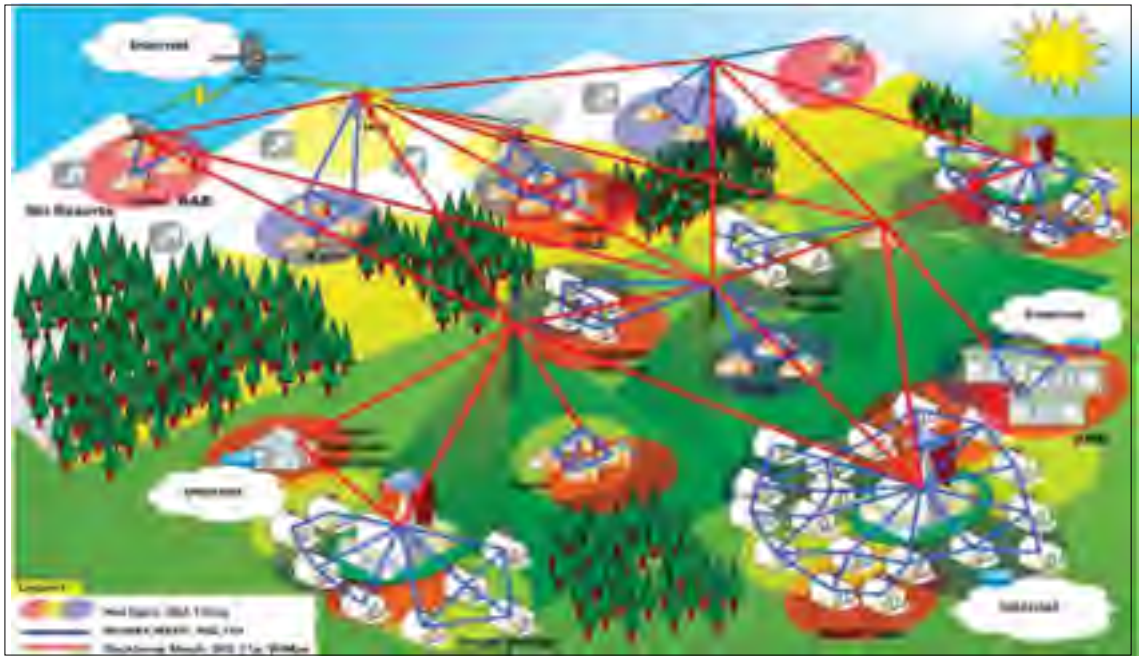

Figure 1.2 Architecture hiérarchique de réseau maillé sans fil
Tirée de Sudip Misra Subhas Chandra Misra I (2009)

Les routeurs (AP) agissent comme des passerelles de couche 3 et supportent les fonctions de maillage. Ces AP sont placées au bord du backbone et sont destinés à une connexion internet filaire à haut débit. Le réseau sans fil constitué de l'interconnexion d'AP et des routeurs *mesh*, est appelé un *backhaul*. Ces nœuds sont généralement équipés de plusieurs interfaces réseau supportant différentes technologies d'accès, ils peuvent garantir une large couverture avec moins de consommation d'énergie grâce au support de communications multi saut. Le mode d'interconnexion ad hoc entre les routeurs mesh à travers les réseaux maillés sans fil constitue le backbone de réseau maillé sans fil. Il garantit la connectivité entre les utilisateurs mobiles et les passerelles filaires.

1.1.2 Architecture WMN client

L'architecture WMN client, est un réseau maillé ad hoc. Dans ce type d'architecture un routeur mesh n'est pas requis pour fournir des connexions internet. Les nœuds clients sont

tous mobiles et constituent le réseau, ils exercent à la fois la fonction de nœud terminal du réseau et du routeur.

1.1.3 Architecture WMN hybride.

Cette architecture est la combinaison de l'architecture infrastructure et l'architecture client mesh. Les clients utilisent les routeurs mesh pour accéder au réseau, comme ils peuvent utiliser les clients mesh auxquels ils sont directement connectés. Ce type d'architecture offre une bonne connexion et bonne couverture. La figure 1.3 montre un exemple de l'architecture WMN hybride.

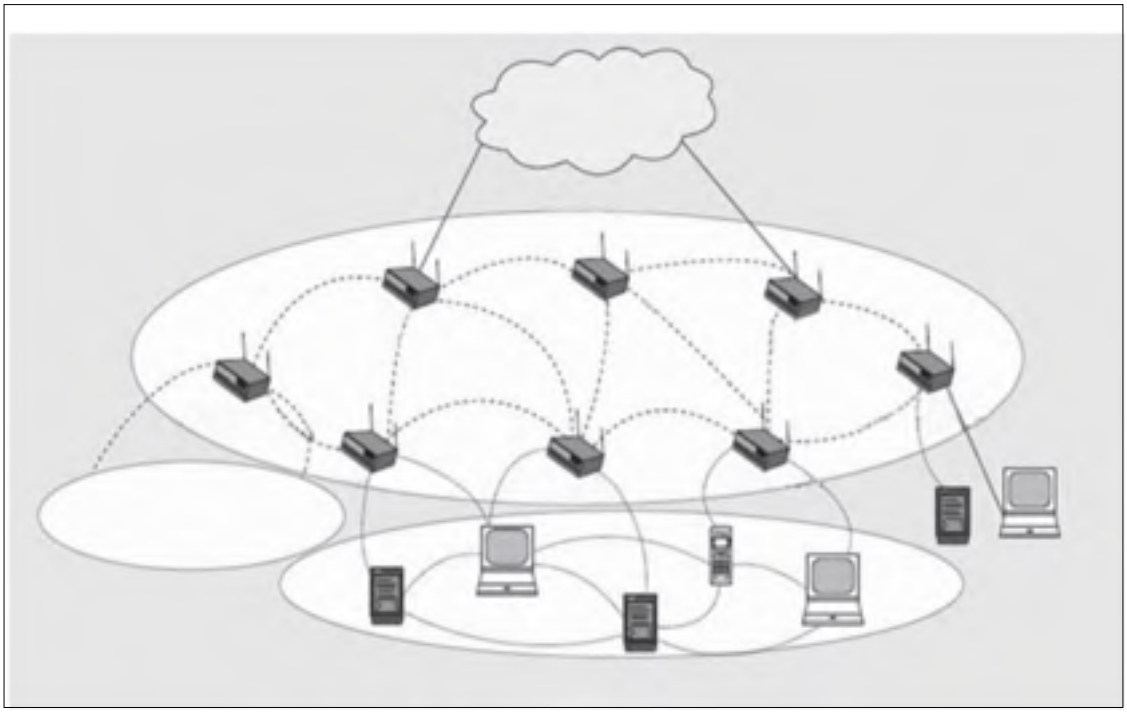

Figure 1.3 Architecture de WMNs hybride
Tirée de Zhang (2009)

1.2 Caractéristiques des réseaux maillés sans fil

Les réseaux maillés gagnent un grand intérêt grâce à leurs caractéristiques particulières qui permettent le déploiement de nouvelles applications à moindre coût. Certains des avantages

et des caractéristiques des réseaux maillés sans fil sont mis en évidence comme suit (Zhang, Zheng et Hu, 2009).

1.2.1 Communication multi-saut :

Le système de communication multi saut garantit une vaste zone de couverture et améliore la capacité du réseau. En effet, ceci permet de surmonter la contrainte de ligne de visibilité, parce que les nœuds intermédiaires transmettent l'information à leurs voisins sur de courtes liaisons sans fil en utilisant une faible puissance de transmission.

1.2.2 Réduction de couts de déploiement

L'infrastructure sans fil supportée par les réseaux maillés élimine les coûts de déploiement d'un nouveau *backhaul* filaire à travers les villes et les zones rurales.

1.2.3 Auto configuration et autogestion

Les WMNS sont auto organisés et auto configurés. En d'autres termes, les nœuds du réseau maillé établissent et maintiennent automatiquement la connectivité réseau. Ainsi, les clients mesh qui rentrent nouvellement dans le réseau maillé sont supportés de façon transparente, car les fonctions telles que la découverte de voisinage et l'apprentissage automatique de la topologie sont implémentées dans ces réseaux. Les routeurs maillés sans fil détectent rapidement la présence de nouveaux chemins, ce qui améliore la performance globale et augmente la zone de couverture.

1.2.4 Accès internet et interopérabilité

Les équipements de *backhaul* sont dotés de plusieurs interfaces réseaux qui prennent en charge à la fois Internet et la communication *peer-to-peer* , tout en garantissant l'accès aux technologies sans fil existantes des réseaux telles qu'IEEE 802.11, WiMAX, ZigBee, et les réseaux cellulaires.

1.2.5 Mobilité et consommation d'énergie

La mobilité et la consommation d'énergie varient avec la nature du nœud maillé. Ainsi les routeurs maillés et APs ont une mobilité minimale et leurs contraintes en consommation d'énergies sont réduites.

1.2.6 Fiabilité

En WMNs, les routeurs maillés sans fil fournissent des chemins redondants entre la source et la destination. Les pannes des nœuds et les bris de chemins, causés par des interférences ou par des obstacles, peuvent être évités par l'existence de multiples itinéraires redondants, ce qui donne de la robustesse au réseau envers d'éventuels problèmes.

1.2.7 Large zone de couverture

Les communications de multi saut et multicanaux fournissent une transmission pour longue distance, à travers les routeurs *mesh*, sans dégradation des performances. Contrairement, aux WLANs dont la couverture et la connectivité diminuent, quand le débit augmente pour certaines puissances de transmission.

1.3 Applications supportées par les réseaux maillés sans fil

L'usage des réseaux maillés sans fil est très répandu, particulièrement dans des infrastructures où le câblage nécessite de déployer d'énorme moyens financiers.
Parmi les applications les plus adaptées aux WMNs nous citons les suivantes :

- réseau domestique,
- réseau collectif et de voisinage,
- réseau d'entreprise,
- réseau métropolitain,
- réseau dans le domaine de transport,

- réseau médical,
- réseau de sécurité de surveillance.

1.3.1 Réseau résidentiel

Les réseaux maillés sans fil peuvent être déployés à domicile parce qu'ils supportent des applications qui consomment beaucoup de bande passante, telle que la transmission multimédia. Les nœuds du maillage peuvent être des PC de bureau, des ordinateurs portables, la télévision haute définition et des lecteurs DVD. Un AP ou les routeurs maillés peuvent être facilement ajoutés pour couvrir les zones mortes sans nécessiter de câblage ou des configurations complexes.

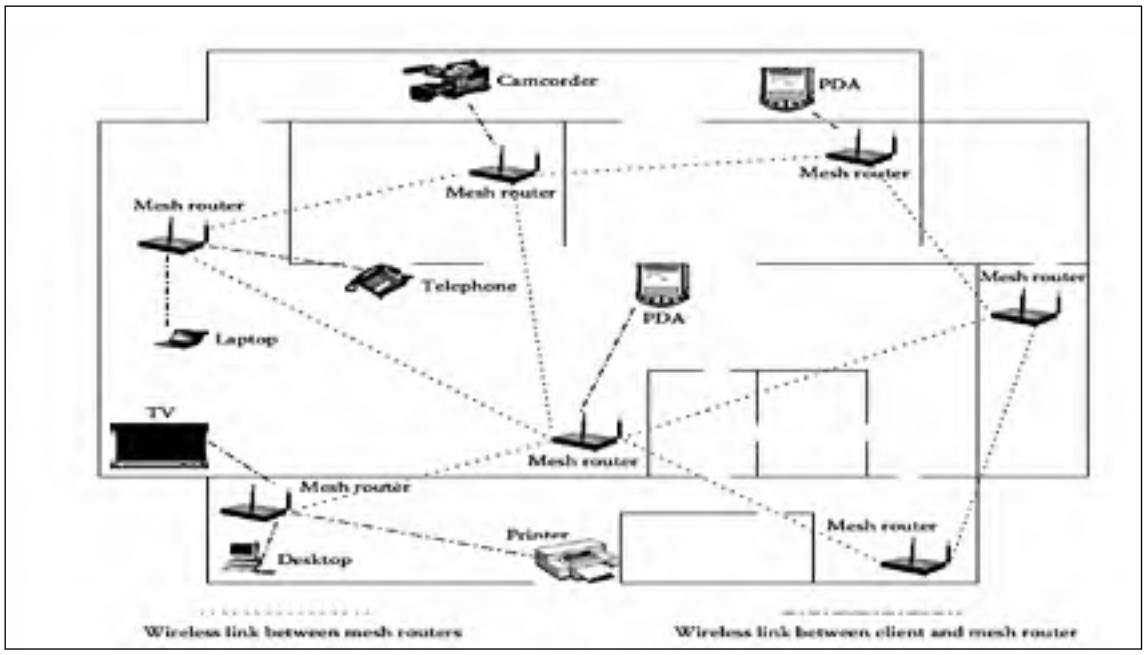

Figure 1.4 Réseau résidentiel
Tirée de Zhang (2009)

1.3.2 Réseau d’entreprise

L'adoption de réseaux maillés dans les entreprises permet le partage des ressources et l’amélioration de la performance globale grâce à la communication multi hop et le déploiement de l'infrastructure sans fil. En fait, la congestion due au goulot d'étranglement résultant de l'accès à un seul saut aux points d'accès traditionnels est éliminée. En outre, l'infrastructure peut facilement évoluer en fonction des besoins du réseau, sans nécessiter des configurations complexes et de câblage.

1.3.3 Application publique

Les réseaux maillés supportent les applications publiques métropolitaines et à grande échelle ce qui surmonte la contrainte de ligne de visibilité. L'accès à Internet sans fil sur la route, la sécurité publique, et la mise en œuvre des systèmes de transport intelligents sont très appréciés par les habitants des villes et des visiteurs, et ont déjà été déployés dans de nombreux pays.

1.3.4 La gestion des catastrophes et opérations de secours

Les WMNs peuvent être utilisés dans des endroits où la connectivité réseau spontanée est requise, telle que la gestion des catastrophes et des opérations d'urgence, car lors de catastrophes, toutes les infrastructures de communication existantes pourraient être réduites.

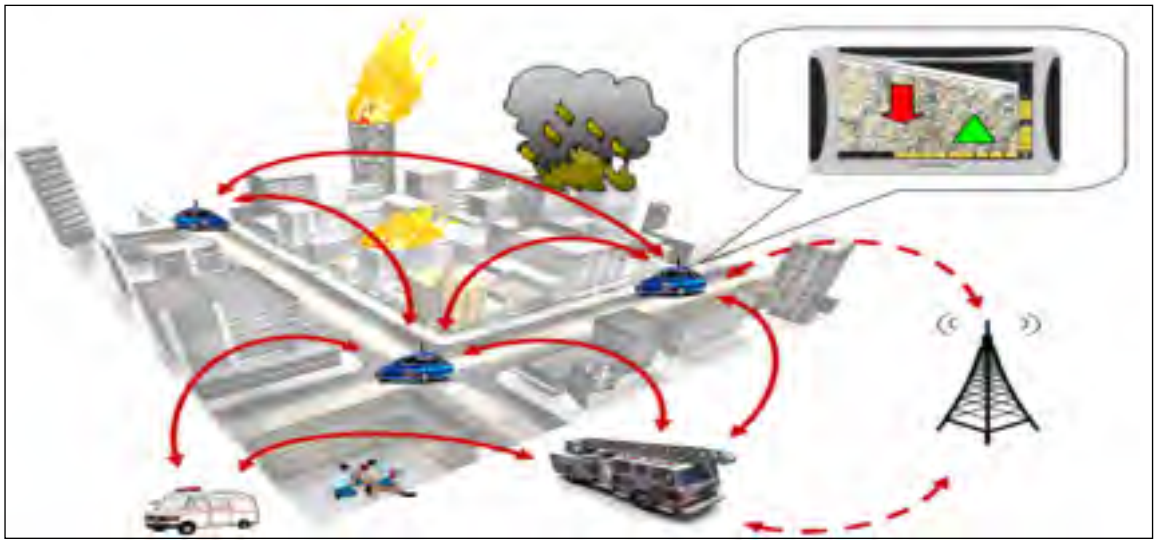

Figure 1.5 Architecture WMN pour gestion de catastrophe
Tirée de Senouci (2008)

1.3.5 Système de la sécurité de surveillance

Les WMNs offrent aux systèmes de surveillance de la sécurité situés dans différents endroits une bande passante élevée et un réseau backbone fiable nécessaire pour transmettre les données de surveillance, telles que des images, audio, et la vidéo.

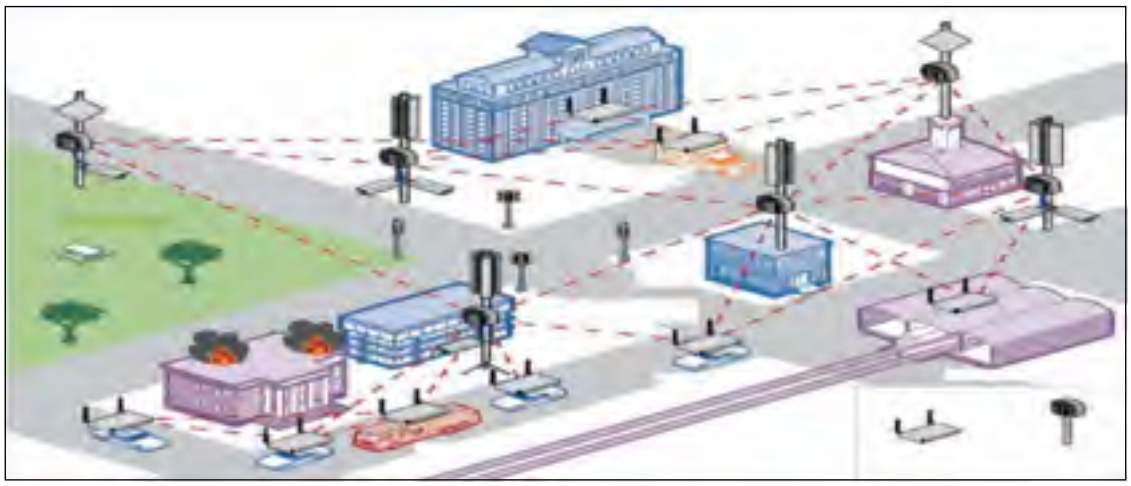

Figure 1.6 Application publique de WMN
Tirée de Misra (2009)

1.4 Contraintes des réseaux maillés sans fil

Nombreuses contraintes peuvent surgir lors de déploiement des WMNs. Les problèmes les plus fréquemment rencontrés sont illustrés comme suit (Hossain et Leung, 2008) :

1.4.1 Capacité

Dans un canal unique du réseau sans fil, la capacité du réseau se dégrade quand le nombre de sauts ou le diamètre du réseau augmente en raison de l'interférence. La capacité de WMN est affectée par de nombreux facteurs tels que l'architecture réseau, la densité des nœuds, le nombre de canaux utilisés, la mobilité des nœuds, mode de trafic, et la portée de la transmission.

1.4.2 Couche physique

La capacité du réseau dépend principalement de la technique du lien de couche physique utilisé. Le rapport du signal sur bruit (SNR) ou de la porteuse sur bruit (CNR) de la couche physique est pris en considération pour l'adaptation du lien, mais cela ne suffit pas pour décrire la qualité du signal dans le milieu sélectif en fréquence, comme dans les cas d'un canal à évanouissement. Pour surmonter les problèmes de transmission RF, d'autres techniques de la couche physique sont utilisés pour les communications sans fil. Quelques une de ces techniques sont :

- Orthogonal Frequency Division Multiplexing (OFDM),
- Ultra Wide Band (UWB),
- Multiple-Input Multiple-Output (MIMO),
- Smart Antenna.

1.4.3 Mode d'accès aux médias

Les protocoles basés sur l'adresse MAC (Medium Access Control) pour les réseaux sans fil sont limités à une communication à un seul saut. Tandis que les protocoles de routage utilisent la communication *multihop* (multi sauts).

1.4.4 Routage

Les protocoles conçus pour les réseaux ad hoc fonctionnent aussi bien sur WMNs. Toutefois, dans WMNS les routeurs mesh n'ont pas de contraintes de puissance, et les clients sont mobiles avec une puissance limitée. Ce qui rend l'élaboration des protocoles de routage efficaces pour WMNs.

1.4.5 Couche de transport

Utilisation du protocole TCP sur un réseau sans fil dégrade la performance du réseau, qui se traduit par la réduction du débit et l'iniquité pour les connexions. Cette dégradation des performances est due aux raisons suivantes:

- le taux élevé d'erreur binaire (BER) dans les réseaux sans fil par rapport aux réseaux filaires,
- une fréquence élevée de rupture de lien dans les réseaux sans fil en raison de la mobilité des nœuds dans les réseaux ad hoc.

Si les paquets sont éliminés dans le réseau à cause des raisons citées ci-dessus, le transmetteur TCP interprète mal cet événement et il le considère comme de la congestion, alors il déclenche le mécanisme de contrôle de congestion pour réduire la taille de la fenêtre de congestion. Ce qui réduit le débit effectif du réseau.

1.4.6 Équilibre de charge de la passerelle

Comme de nombreux clients dans le réseau envoient du trafic vers la passerelle, la bande passante disponible doit être utilisée de façon efficace. Le trafic envoyé par les nœuds clients se regroupe au niveau des nœuds de la passerelle dans le WMN. Si certaines des passerelles sont très chargées et d'autres passerelles sont légèrement chargées, cela crée un déséquilibre de charge entre les nœuds de la passerelle, ce qui conduit à la perte de paquets et entraîne une dégradation des performances du réseau. Par conséquent, l'équilibrage de charge entre les nœuds de la passerelle dans WMNs améliore l'utilisation de la bande passante et augmente aussi le débit du réseau.

1.5 Défis des réseaux maillés sans fil

Les facteurs essentiels influençant les performances des WMNS peuvent être résumés comme suit :

1.5.1 Technologie avancée radio sans fil

Beaucoup de technologies sans fil ont été proposées pour améliorer la capacité des WMNs tels que :

- systèmes à Radio reconfigurables,
- systèmes à smart fréquence,
- systèmes, radios cognitives,
- antennes directionnelles et smart,
- systèmes à multiple input et multiple output (MIMO),
- systèmes, multi radio et multicanaux.

Cependant, la complexité et le coût de ces technologies sont encore trop élevés pour être largement acceptés pour la commercialisation. Par conséquent, toutes technologies radio sans fil avancées requièrent une conception révolutionnaire de la suite de protocoles de

communication afin de faciliter le déploiement de WMNs et la commercialisation des produits.

1.5.2 Interopérabilité et intégration de réseaux hétérogènes

Les technologies de réseau existantes ont des capacités limitées pour intégrer différents réseaux sans fil. Ainsi, pour augmenter la performance de WMNs, et fournir l'interopérabilité entre les produits de différents fabricants, les capacités d'intégration des multiples interfaces sans fil et les fonctionnalités des routeurs correspondants aux passerelles et ponts du réseau doivent être améliorées.

1.5.3 Mise à échelle

Le réseau maillé déployé doit être en mesure de fonctionner dans de larges topologies réseau sans augmenter le nombre d'opérations de réseau de façon exponentielle. En outre, les performances du réseau ne doivent pas se dégrader quand le nombre de sauts entre l'émetteur et le récepteur augmente. Pour fournir l'extensibilité dans les WMNs, on a besoin de la couche MAC, de protocoles de routage et de protocoles de couche de transport avec minimum surcharge.

1.5.4 Les exigences de qualité de service (QoS) hétérogènes

Les services du réseau qui sont fournis par WMNs varient, d'un fichier de transfert fiable à fichier multimédia en temps réel. Ainsi, en plus de débit du réseau traditionnel et de mesures de latence de communication, des mesures de performance plus concrètes, telles que la gigue sur le délai, la capacité globale, la capacité du nœud, et les ratios de paquets perdus, doivent être considérées par les mécanismes de déploiement.

1.5.5 Connectivité dynamique et auto configuration

Afin d'éliminer les points de défaillance uniques et la congestion dans les WMNs, le backbone sans fil doit fournir des chemins redondants entre l'émetteur et le récepteur. Cependant, la topologie et la connectivité du réseau peuvent varier fréquemment en raison des pannes de route et l'épuisement de l'énergie. Par conséquent, un réseau d'auto configuration efficace, le contrôle de topologie et des algorithmes de gestion de l'alimentation sont nécessaires, pour tirer profile des avantages de la connectivité réseau autonome de WMN.

1.5.6 Support de mobilité

Pour une bonne gestion de la mobilité, il est nécessaire de concevoir une couche physique et des techniques de déploiement réseau avancées. En plus de ces techniques de pointe, un transfert à main libre à faible latence et des algorithmes de gestion de localisation sont également nécessaires pour améliorer la qualité du service au cours de la mobilité.

1.6 Outils de gestion réseau

Pour surveiller la performance globale du réseau et maintenir le fonctionnement du réseau, flexible et adaptable, des capacités de gestion de réseau sont nécessaires pour WMNs.
Les principales capacités de gestion de réseau des WMNs comprennent :

- apport de bande passante,
- installation de la politique de sécurité et la qualité de service,
- support des accords de niveau de service,
- détection et résolution d'erreurs,
- ajout et suppression des entités réseau,
- modification des fonctions de réseau,
- comptabilité, facturation et rapports.

Toutes ces fonctionnalités peuvent automatiser l'erreur de gestion dans WMNs et ainsi permettre le déploiement rapide de WMN.

Conclusion

Ce chapitre, nous a introduits aux réseaux maillés sans fil. Il a permis de mettre en évidence les avantages, les inconvénients et les caractéristiques de ces réseaux. Ces caractéristiques le rendent une technologie prometteuse, en pleine essors. Ses spécificités telles que son faible cout de déploiement et sa robustesse ont permis de fournir le haut débit même dans des zones où le câblage est difficile. Ce chapitre a relaté aussi l'usage répandu de WMN dans des différentes infrastructures. Celui-ci peut être utilisé dans des endroits où la connectivité réseau spontanée est requise, telle que la gestion des catastrophes et des opérations d'urgence, il peut être utilisé aussi pour les systèmes de la sécurité de surveillance en raison de son fiable backbone. Les contraintes et les défis liés au déploiement des réseaux maillés ont été aussi soulevés. Nous avons constaté que la capacité de WMN est affectée par de nombreux facteurs tels que l'architecture réseau, la densité de nœud, le nombre de canaux utilisé, la mobilité des nœuds, le modèle de trafic, et la portée de transmission.

Dans prochain chapitre, une étude des réseaux privés virtuels serait abordée, elle va décrire les différentes technologies et algorithmes qui sont associés aux VPNs pour la sécurisation des réseaux de télécommunications.

CHAPITRE 2

LES RÉSEAUX PRIVÉS VIRTUELS
VPN

2.1 Introduction

Un réseau privé virtuel est une extension d'un réseau privé (intranet) sur un réseau public (internet). Il permet l'échange des données entre les membres d'un groupe à travers un réseau d'interconnexion partagé ou public d'une façon sécurisée et rentable à l'aide des tunnels logiques privés comme dans une liaison pointe à point. La figure 2.1 illustre un exemple d'un réseau VPN.

Ce chapitre relate les différentes façons de déployer les VPNs, il décrit aussi les technologies et algorithmes qui sont associés aux VPNs pour une mise en œuvre d'une sécurité fiable et rentable sur les réseaux.

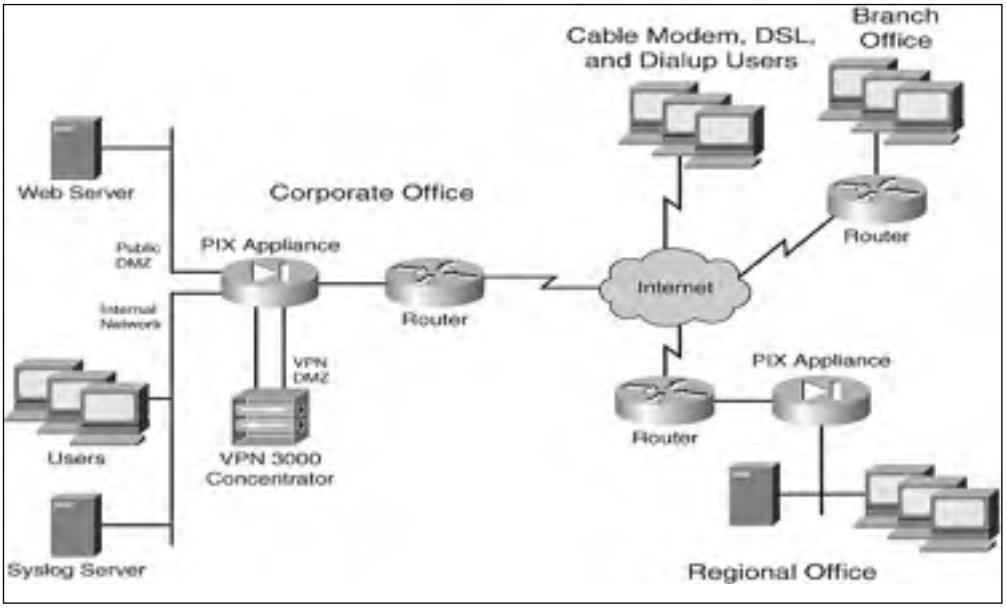

Figure 2.1 Réseau VPN
Tirée de Deal (2008)

2.2 Les types des réseaux privé virtuels

Le type de VPN est le type d'entités qui sont impliquées dans une connexion VPN réelle. On compte ci-dessus les types les plus répandus en raison de leur fréquente utilisation :

- VPN site à site,
- VPN d'accès distant,
- pare-feu VPN,
- VPN d'utilisateur à utilisateur (*user to user*),
- le réseau privé virtuel dédié.

- **Accès à distance via internet**

Comme son nom l'indique, le VPN d'accès distant fournit à tout moment l'accès à distance aux ressources d'une organisation sur l'Internet public, tout en préservant la confidentialité des informations. Les VPNs à accès distant sont généralement utilisés pour des connexions à faible bande passante ou de connexions à haut débit.

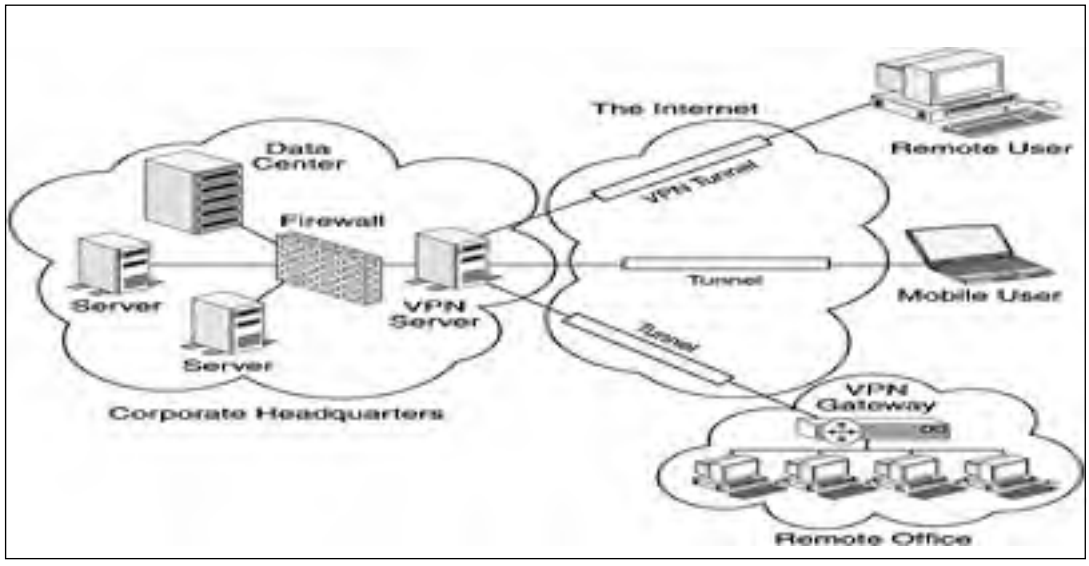

Figure 2.2 VPN à accès distant via Internet.
Tirée de Gupta (2003)

- **Le réseau privé virtuel de site à site**

Pour ce type de réseau VPN on compte deux façons de déploiement qui sont les suivantes :

1) Le réseau privé virtuel de site à site interne

Appelé aussi Connexion d'ordinateurs sur un intranet. Le réseau privé virtuel de site à site interne, est un VPN qui utilise une connexion en mode tunnel entre deux passerelles VPN, pour protéger le trafic entre deux ou plusieurs sites. Les emplacements de site à site sont communément référés à LAN-to-LAN (L2L).

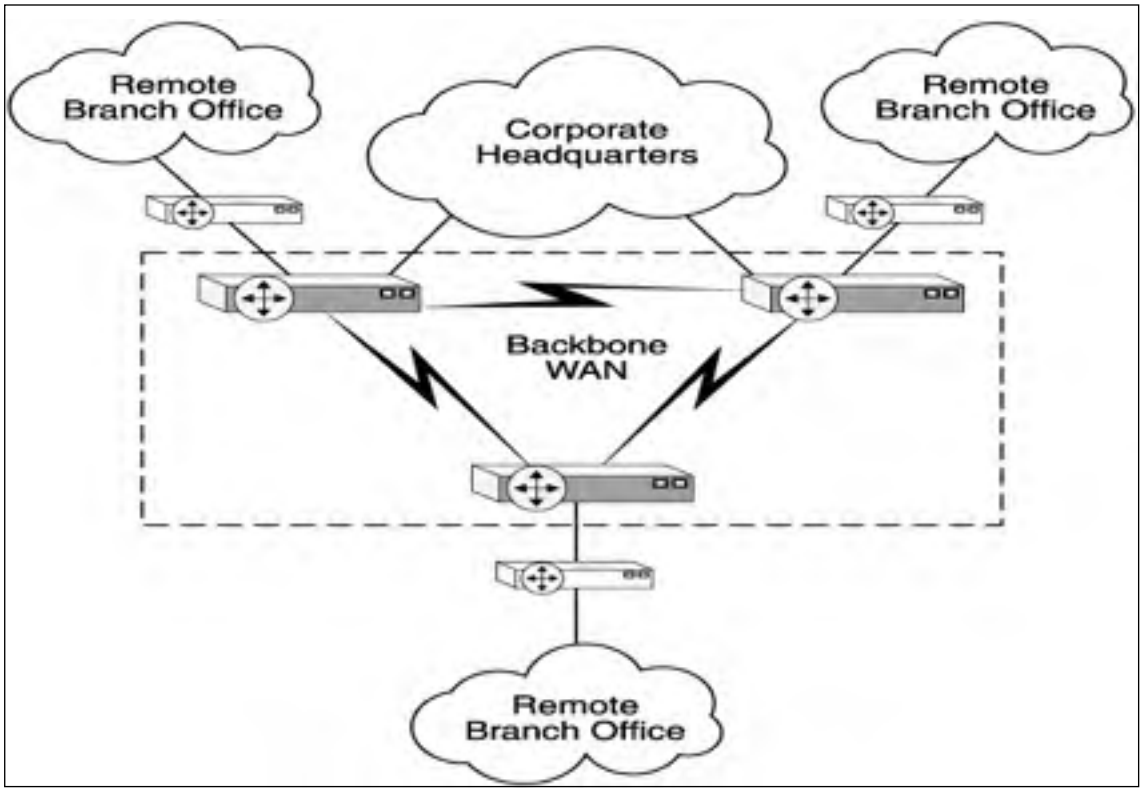

Figure 2.3 VPN de site à site via Backbone WAN.
Tirée de Gupta (2003)

2) Le réseau privé virtuel Site-to-Site par Internet

La technologie VPN de site à site utilise la connectivité locale ISP sur les sites des bureaux distants et un seul circuit à grande vitesse au bureau central. Ceci permet à une entreprise d'éliminer les coûts récurrents mensuels des circuits à grande vitesse, tels que le frame relay, et le maintien d'une architecture de routage WAN.

Le réseau privé virtuel d'utilisateur à utilisateur

Un VPN de type utilisateur à utilisateur est essentiellement un mode de transport de connexion de VPN entre deux appareils. Deux appareils peuvent être un routeur et un serveur TFTP. Un utilisateur utilisant Telnet peut accéder à un routeur, ou à plusieurs paires de connexions.

Le réseau privé virtuel Pare-feu

Un pare-feu VPN est essentiellement un VPN de l'accès distant, ou une L2L renforcés avec une sécurité supplémentaire et des fonctions de pare-feu. Les Pare-feu VPN sont généralement utilisés, lorsqu'un côté de la connexion VPN a besoin de la sécurité améliorée.

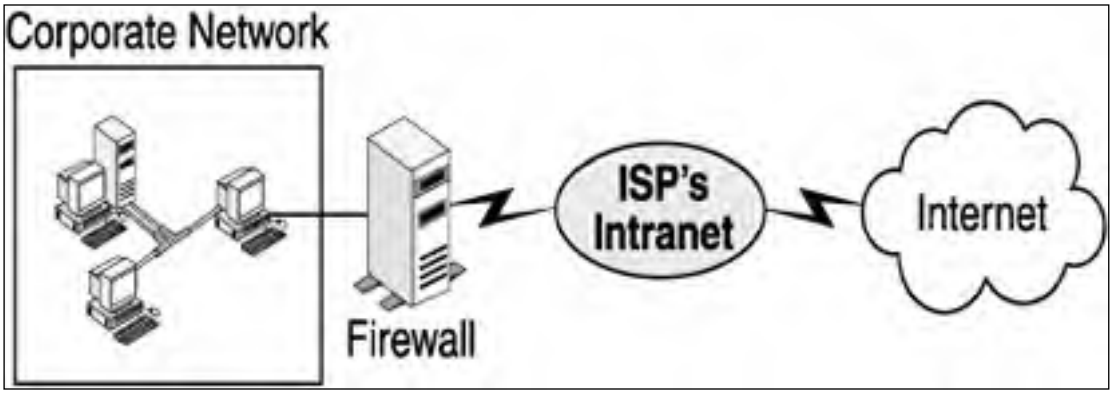

Figure 2.4 VPN avec Firewall
Tirée de Gupta (2003)

Le réseau privé virtuel dédié

Cette méthode utilise des lignes dédiées pour raccorder une filiale à un réseau d'entreprise local (LAN). Les connexions locales ISP et Internet sont utilisés pour créer un VPN entre le routeur de la succursale et le routeur concentrateur de l'entreprise.

2.3 Les exigences de base de réseau privé virtuel

Pour garantir la confidentialité et l'intégrité des données lors de leur passage sur l'Internet, des mesures et des mécanismes de sécurité sont également utilisés pour assurer le transfert de ces données en toute sécurité à travers un milieu non sécurisé.

Les mécanismes de sécurité les plus importants pour les réseaux privés virtuel sont les suivants :

- authentification,
- mode d'encapsulation,
- chiffrement des données,
- intégrité des paquets,
- gestion des clés,
- la non-répudiation,
- support de protocole et applications,
- gestion des adresses.

- **Authentification**

L'authentification vérifie l'équipement de l'utilisateur ou l'identité de l'utilisateur lors de l'établissement d'une connexion VPN dans un réseau. Il existe deux catégories générales d'authentification :

1) authentification de l’équipement,
2) authentification de l’utilisateur.

1. Authentification de l’équipement

L’authentification de l’équipement permet de restreindre l'accès VPN au réseau pour fournir des informations d'authentification à partir d'un périphérique VPN distant. Une ou plusieurs clés sont configurées et utilisées pour authentifier l'identité d'un périphérique. Les Clés pré-partagées sont généralement utilisées dans un VPN de petit environnement. Les9-* signatures numériques, ou les certificats numériques sont utilisés pour l'authentification des équipements dans des déploiements de grand VPN.

2. Authentification de l'utilisateur

De nombreuses implémentations VPN ajoutent une couche supplémentaire d'authentification, appelée l'authentification des utilisateurs, afin de vérifier si une connexion VPN est autorisée par un utilisateur à l'aide d'un équipement spécifique, où l'utilisateur doit fournir un nom d'utilisateur et un mot de passe. Ce mot de passe peut-être un mot de passe statique ou un mot de passe instantané.

Chiffrement des données

Le chiffrement est le processus de modification des données dans un format qui peut être lu que par le destinataire prévu. Pour lire le message, le destinataire des données doit avoir la clé de déchiffrement correct. Le cryptage des données est utilisé pour résoudre les problèmes de l'écoute. Le cryptage des données comprend essentiellement des données des utilisateurs et une valeur de la clé de déchiffrement et il fonctionne grâce à un algorithme de chiffrement tel que les chiffrements DES, 3DES, AES, Blowfish, RSA, IDEA, SEAL, et RC4.

Intégrité d'un paquet

En raison de falsification de paquets possible ou d'usurpation de paquets, certaines implémentations VPN utilisent l'authentification des paquets. SHA et MD5 sont deux des fonctions les plus courantes de hachage utilisées pour vérifier l'intégrité des paquets.

Gestion des clés

Pour utiliser le cryptage, la solution VPN doit fournir une sorte de mécanisme de chiffrement de clé pour créer la session tunnel. La solution doit générer et régénérer des clés de chiffrement pour les données chiffrées sur un accord mutuel de façon périodique afin que la sécurité et la confidentialité puissent être maintenues.

La non-répudiation

La non-répudiation ou la comptabilité est l'enregistrement de la session VPN. Cela pourrait inclure l'identité des deux dispositifs pour établir la connexion, la durée de la connexion qui a été utilisée, la quantité d'information qui a été transmise, le type d'informations traversé pendant la connexion, etc. Cela peut ensuite être utilisé pour détecter les attaques et pour l'accès à des fins de gestion, telles que la création des lignes de base et la recherche de problèmes de bande passante.

L'autorisation

L'autorisation est le processus d'octroi ou de refus de l'accès aux ressources situées dans un réseau après que l'utilisateur ait été identifié et authentifié.

Gestion des adresses

Un client VPN doit avoir une adresse sur l'intranet et s'assurer que les adresses utilisées dans l'intranet sont gardées confidentielles. Pour cela une solution commune consiste à utiliser un serveur DHCP externe ou un serveur AAA (authentification, autorisation et comptabilité) pour l'attribution d'une adresse à l'utilisateur. En outre, certaines informations pour permettre au client d'accéder aux ressources sur le réseau protégé doivent être fournies. Par exemple, les informations de routage, la résolution de nom de la source, et de la sécurité ainsi que des filtres de sécurité pour assurer la protection des données internes de toute utilisation non autorisée.

2.4 Les implémentations des réseaux privés virtuels

Des méthodes d'implémentation les plus populaires de VPN sont :

- GRE,
- IPsec,
- PTP,
- L2TP,
- MPLS,
- SSL.

2.4.1 Le protocole de sécurité IP (IPSec)

Développé par l'IETF, IPSec est un standard qui garantit la sécurité de transmission et l'authentification des utilisateurs sur les réseaux publics. IPSec fonctionne à la couche réseau de systèmes (OSI). Par conséquent, il peut être mis en œuvre indépendamment des applications qui s'exécutent sur le réseau. IPsec offre la confidentialité des données, en utilisant le chiffrement pour protéger les données contre les tentatives d'écoute. Des algorithmes de chiffrement utilisés comprennent DES, 3DES et AES.

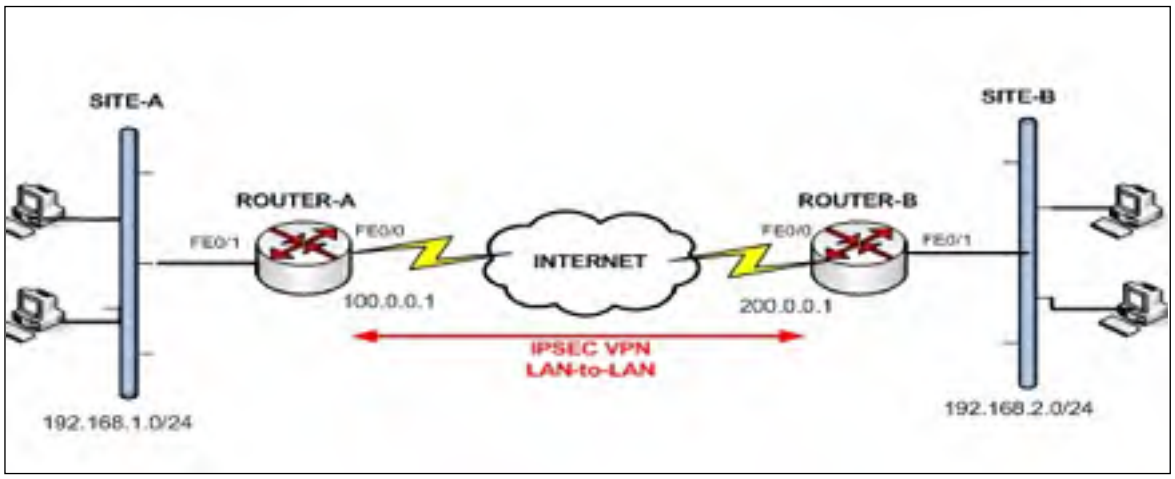

Figure 2.5 VPN-IPSec
Tirée de http://www.ipworld.vn
Consulté le 28 septembre 2013

2.4.2 Le protocole point-to-point tunneling (PPTP)

Le PPTP est une transmission sécurisée du trafic Windows. Développé par Microsoft, 3Com, et Ascend Communications. Il fonctionne à la couche 2 (couche de liaison de données) du modèle OSI. PPTP est une extension du protocole Point-to-Point (PPP). Par conséquent, il utilise les fonctionnalités de PPP telles que l'encapsulation multiple des protocoles, comme IP, IPX et NetBEUI, .et les protocoles PAP, CHAP et MS-CHAP pour authentifier les appareils PPTP.

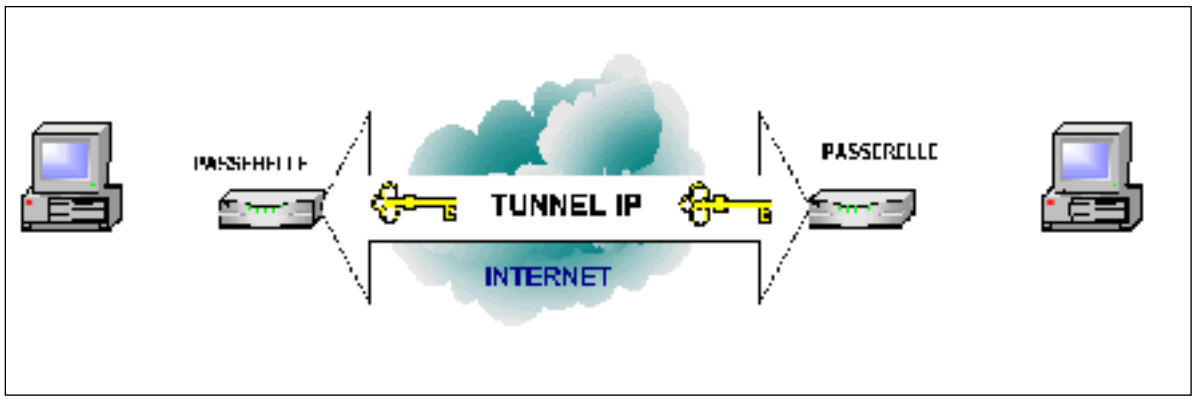

Figure 2.6 VPN PPTP
Tirée de http://www.labo-microsoft.org
Consulté 28 octobre 2013

2.4.3 Le protocole de tunneling de couche 2 (L2TP)

Développé par System Cisco, L2TP est une combinaison de Layer 2 Forwarding (L2F) et PPTP. Il est à base d'une technologie PPP, par conséquent, il utilise des fonctionnalités de celui-ci, telle que la gestion de contrôle de session, la répartition et l'affectation des adresses, et du routage. L2TP permet au trafic multi protocole d'être chiffré, puis être envoyé sur n'importe quel support qui soutient le cheminement point à point de L2TP. Il utilise UDP comme une méthode d'encapsulation pour des travaux d'entretien du tunnel et les données utilisateur. Les paquets L2TP sont protégés par ESP IPsec en mode transport. Par conséquent, la mise en œuvre L2TP inclura l'utilisation de IPsec.

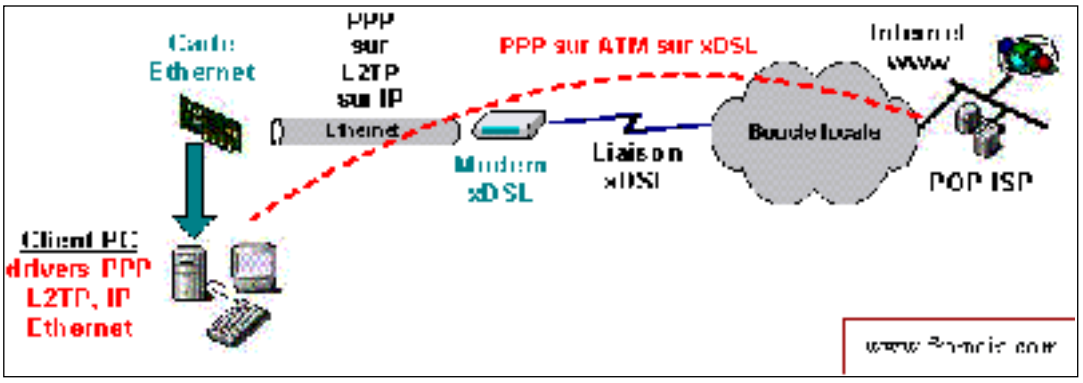

Figure 2.7 VPN-L2TP

Tirée de http://www.frameip.com
consulté le 28 sept 2013

2.4.4 Couche de sockets sécurisée SSL

La technologie VPN SSL fonctionne à la couche session du modèle de référence OSI. Elle a été conçue pour les solutions d'accès distant et ne fournit pas de connexion de site à site. VPN SSL offre un accès sécurisé aux applications principalement basé sur le Web. Par conséquent, les applications telles que Telnet, FTP, SMTP, POP3, la téléphonie IP et le

contrôle de bureau à distance ne fonctionnent pas avec les VPN SSL. Cependant des logiciels comme, Java ou Activex peuvent être utilisés pour améliorer le VPN SSL.

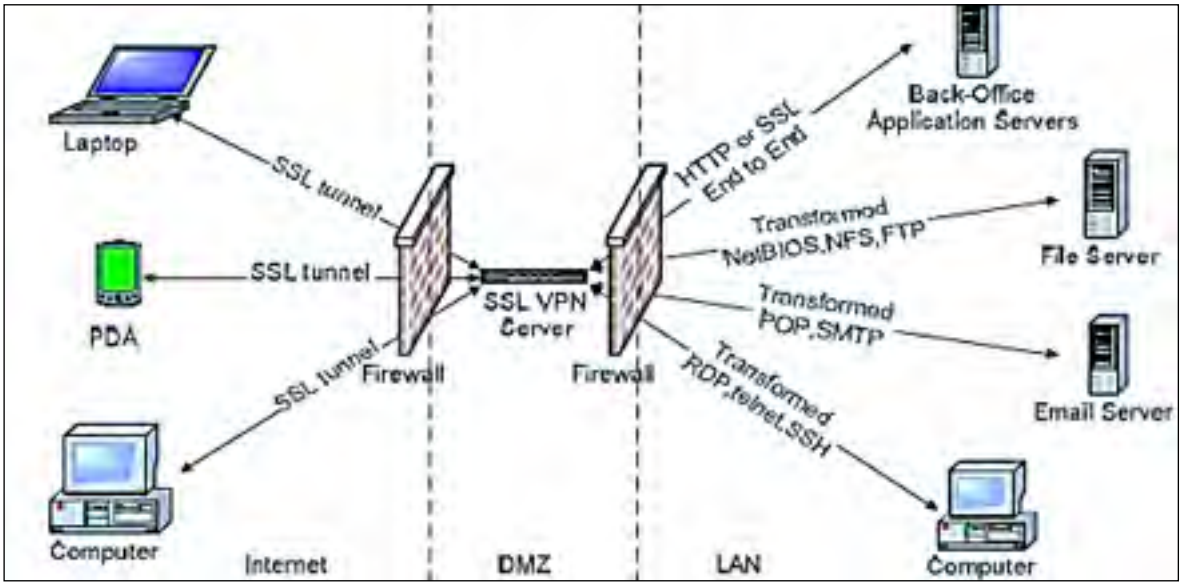

Figure 2.8 La technologie VPN SSL
Tirée de Yu (2009)

2.4.5 Les réseaux privés virtuels avec MPLS

MPLS VPN est défini dans le RFC 2547, il utilise MPLS et MPBGP (MultiProtocol BGP) pour transmettre des données privées et le VPN pour le routage d'informations. Pour éviter que les adresses se chevauchent, dans l'environnement MPLS VPN, une route globale RD unique (Route Distinguisher) est associée à la plage d'adresse privée de chaque entreprise, pour former une adresse VPNv4 qui est acheminée par MPBGP entre les routeurs *Provider Edge* (PE). Pour chaque entreprise, RD est différent, donc l'espace d'adressage privé est isolé. Comme le routage doit être séparé et privé pour chaque client (VPN) sur un routeur PE, chaque VPN doit avoir sa propre table de routage. Cette table de routage privé est appelée la table de routage VRF. L'interface du routeur PE vers le routeur CE ne peut appartenir qu'à un seul VRF. La figure 2.1 illustre un exemple d'un réseau MPLS-VPN.

Figure 2.9 Exemple de MPLS-VPN
Tirée de http://www.zetta.net.
Consulté le 30octobre 2013

Les opérateurs de MPLS VPN BGP offrent une grande flexibilité à leurs clients. Un des plus grands avantages est qu'ils peuvent utiliser des LSP avec la priorité des classes. Cela permet à un utilisateur de travailler avec des classes de service correspondant à ces priorités. Ces VPNs assurent la sécurité des données et veille à ce que le réseau soit isolé des autres réseaux

Conclusion

Ce chapitre nous a permis de connaitre les implémentations de VPN les plus répandues en raison de leurs applications courantes. Ces implémentations sont mises en œuvres en fonction des besoins de l'entreprise en terme de sécurité. Chaque solution utilise des algorithmes et des mécanismes spécifiques. Ces mécanismes et algorithmes ont été aussi décrits dans ce chapitre. Ces derniers assurent la confidentialité et l'intégrité des données lors de leur passage sur l'Internet. Le chapitre qui suit, est une revue de littérature, elle relate les différentes solutions proposées de VPN sans fil proposées dans la littérature.

CHAPITRE 3

REVUE DE LITTÉRATURE

3.1 Introduction

Les réseaux maillés sans fil sont très répandus en raison de leur faible coût de déploiement. Ces derniers se distinguent par leur nature dynamique auto-organisée et auto configurée, et fournissent une couverture robuste et fiable de l'accès à Internet. Le déploiement des VPNs sur les WMNs est peu abordé dans la littérature. (Muogilim, Loo et Comley, 2011) Sont les seuls auteurs, à notre connaissance à avoir traité un tel sujet. Les auteurs ont proposé MPLS-VPN comme techniques de sécurité pour pallier la contrainte de sécurité dont souffrent les WMNs et ont prouvé que la technologie MPLS-VPN sur les réseaux maillés sans fil non seulement apporte de la sécurité à ces réseaux, mais leur fournit aussi de la qualité de service.

En effet le MPLS-VPN peut assurer de la sécurité pour les clients mesh mobiles à l'intérieur de leurs domaines. D'après (Zhang et al., 2006), lorsque la plage de la mobilité est limitée dans le site, le nœud mobile maintient la connexion avec le routeur CE. Dans ce cas, le changement de l'endroit n'a pas d'influence sur l'acheminement du trafic dans VPN MPLS BGP. Toutefois, lorsque le nœud mesh se déplace d'un site VPN à un autre site, ceci devient problématique, car il est difficile d'assurer un handoff VPN sur WMN où la gestion de mobilité IP est déjà une contrainte.

Comme la gestion de la mobilité des VPNs sur les réseaux maillés sans fil n'est en aucun cas abordée dans la littérature, notre étude va explorer les articles qui ont soulevé la problématique de handoff VPN sur d'autres technologies de réseaux sans fil. Toutefois, un survol sur la solution de la gestion de la mobilité IP sur WMN proposées dans la recherche serait présenté dans ce chapitre. Ceci va nous permettre de déterminer les besoins de WMNs en termes de gestion de la mobilité IP, afin de pouvoir trouver une solution qui permet d'assurer un seamless handoff pour VPN sur WMN.

3.2 Les solutions de Handoff VPN sur les réseaux sans fil

La technologie VPN sur les réseaux sans fil a été utilisée sur plusieurs technologies sans fil. tel que la technologie WIMAX (Dhaini, Ho et Jiang, 2010) , où un Framework a été proposé pour améliorer la sécurité au niveau de la couche de liaison , les auteurs (Munasinghe et Shahrestani, 2005) et (Kadlec, Kuchta et Vrba) ont étudié l'utilisation de VPN sur la technologie WLAN 802.11b et 802.11g. Dans cette étude les performances de la qualité de services ont été déterminées, pour étudier l'impact de VPN sur les WLAN. (Namhi et al., 2006), quant à eux, ont proposé une solution qui permet l'utilisation de VPN sur le GSM, GPRS, le WLAN ou l'UMTS.

Cependant, bien que le VPN assure de la sécurité aux réseaux sans fil, son utilisation n'est pas dépourvue de défis sur ce type de réseaux, particulièrement lorsqu'il s'agit de la gestion de la mobilité. Plusieurs solutions ont été proposées pour pallier à cette contrainte. Ces solutions consistent à assurer un handoff VPN sans rupture de service sur les réseaux sans fil.

Cette partie présente ces différentes solutions proposées dans la littérature pour assurer un handoff VPN dans les réseaux sans fil. Ces méthodes visent à minimiser le délai de handoff et la perte de paquets engendrés par la perte de la connexion lors de la mobilité d'un nœud dans le réseau.

(Zhang et al., 2006) ont proposé des méthodes pour seamless handoff pour MPLS-VPN-BGP. Ces approches sont basées sur la mobilité MIPV6 et la théorie NEMO (Network Mobility). Elles permettent d'avoir de la connexion transparente à l'hôte mobile et au site mobile qui se déplacent d'un site VPN vers un autre.

La mobilité MIPV6 est un protocole qui permet aux nœuds de demeurer accessibles lorsqu'ils se déplacent d'un réseau à un autre. Ce protocole permet au nœud mobile d'être localisé par son adresse CoA, quel que soit son point de rattachement.

Le protocole NEMO, assure la continuité de service, la connectivité et l'accessibilité pour tout le réseau mobile, même quand le routeur mobile change son point d'attache (D. Johnson, 2004)

(Byun et Lee, 2008) Proposent une architecture basée sur BGP/MPLS VPN pour étendre l'utilisation de L3VPN aux utilisateurs mobiles. L3VPN étant un VPN de couche 3 qui concerne MPLS VPN BGP. Cette architecture a permis de réduire la latence de handoff, le taux de perte de paquets et le délai de bout en bout. L'architecture proposée est représentée sur la figure 3.6. Elle est composée de routeurs PE (Provider Edge) supportant le mécanisme de BGP / MPLS VPN et de VPN Virtuel, de routeurs CE (Customer Edge) supportant le VPN IPSec et d'une entité PNS (Provider Provisioned VPN Network Server) supportant la plate-forme de fournisseur de services. En effet, quand le Mobile Node (MN) se déplace vers un site visité, le PNS fournit le Foreign CE (FCE) et un PE sélectionné avec des informations nécessaires. Ces informations sont sur la topologie VPN utilisée, route cible (Route Target), et la Route Distinguisher (RD), elles permettent au PE de mettre en place un BGP / MPLS VPN pour l'utilisateur mobile. Les PEs mettent à jour leur table VRF avec les informations de routage reçues, et les transmettent aux CEs auxquels ils sont attachés. Si le CE du réseau d'origine de l'utilisateur mobile reçoit les informations de routage pour cet utilisateur mobile, il les transmet à HA. Le HA met à jour sa table d'entrée de gestion d'association de mobilité, de telle sorte que le CoA du MN soit fixé sur l'adresse de CE. L'architecture proposée par les auteurs est composée aussi d'un serveur de comptabilité, d'autorisation et d'authentification pour le réseau visité (AAAF) et d'un serveur de comptabilité, d'autorisation et d'authentification pour le fournisseur de services (AAAP). Ces serveurs échangent entre eux la comptabilité, l'autorisation et l'authentification (AAA) des utilisateurs VPN mobiles.
L'User Profile Server (UPS) quant à lui, conserve les informations sur le profil de service de l'utilisateur concernant le VPN.

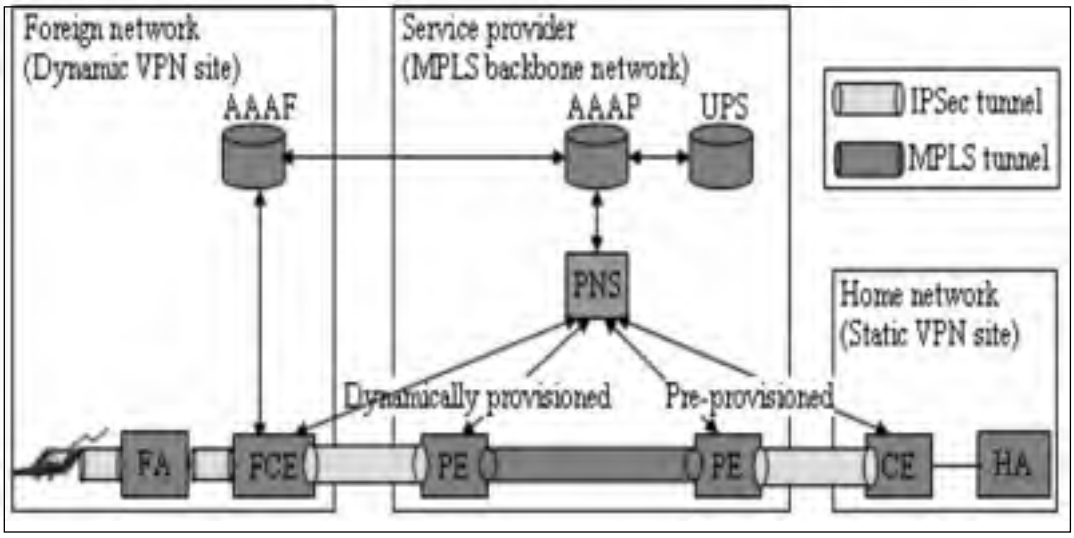

Figure 3.1 Architecture de réseau et de tunnels mobile BGP / MPLS
Tirée de Byun (2008)

Entre le CE et PE, un tunnel IPSec est établi afin de fournir de la sécurité nécessaire pour un VPN sur le circuit de fixation dynamique. L'architecture proposée dans cet article a été simulée en utilisant le simulateur OPNET 11. Le délai de handoff, le débit moyen pendant le handoff, et le délai de bout en bout ont été mesurés. Les résultats de la simulation montrent que les mécanismes de VPN mobiles proposés sont meilleurs que ceux des mécanismes ultérieurs de VPN mobiles. Les résultats ont montré aussi que les mécanismes proposés dans cet article ont réduit la charge de tunnel IPSec sur le nœud de l'utilisateur mobile et ont permis également au trafic d'être livré par des chemins optimisés entre les utilisateurs de VPN (mobile) sans encourir une surcharge supplémentaire du tunnel IPSec.

(Chen-Han, Jen-Shun et Ko-Ching, 2005) proposent une architecture pour handoff transparent (seamless handoff) pour VPN mobiles. Afin de réduire les délais causés par le handoff lors de la mobilité VOIP. Ces délais causés par le handoff sont le délai de la couche liaison, délai de réauthentification d'accès, délai d'association de la couche IP et le délai de l'enregistrement et d'authentification de la couche application. Pour minimiser ces délais les trois techniques suivantes ont été employées.

- VPN avec une adresse IP statique privée,

- multi-homing,
- Mobile Agent.

Le rôle de technologie VPN est de réduire le délai d'attribution d'adresse IP dynamique, car le VPN permet au MN d'utiliser la même adresse IP pendant le handoff. L'utilisation du concept de multi homing permet d'éliminer la perte de paquets au cours de handoff et de minimiser le temps d'interruption car ce concept a la capacité de supporter de multiples adresses IP en un seul point de terminaison. Le rôle de la technologie Mobile Agent (MA) dans les services VoIP consiste à réduire les paquets de contrôle et le traitement de l'authentification basée sur SIM via le tunnel VPN. La figure 3.2 illustre l'architecture proposée. Dans cette architecture des tunnels VPN (L2TP) sont construits entre le L2TP Network Server (LNS) et tous les concentrateurs d'accès L2TP (LACs). Le LNS fonctionne comme un proxy de service pour transmettre les demandes de service à partir du MN vers le serveur d'application. Les demandes de service et de l'authentification ainsi que les paquets de données sont protégées par des tunnels IPSec quand ils sont transmis entre le MN et LNS.

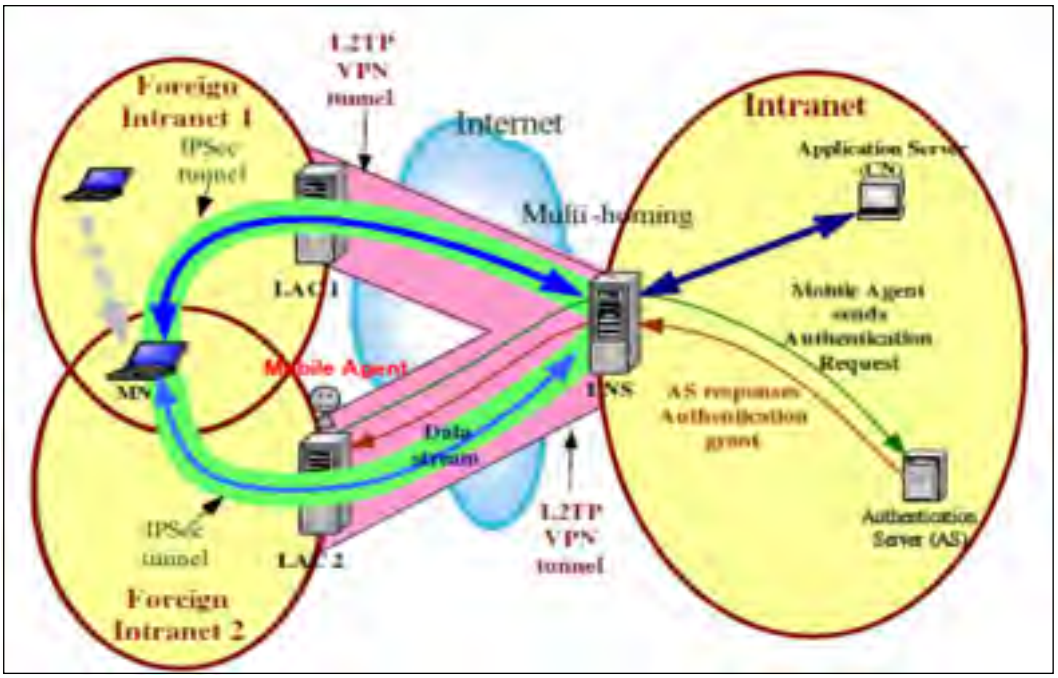

Figure 3.2 Architecture d'un seamless handoff pour Mobile VPN
Tirée de Chen-Han (2005)

(Oya et al., 2010) Proposent la méthode VIRP (Virtual IPsec Redundancy Protocol) pour optimiser le routage du protocole MOBIKE. MOBIKE (Mobility and Multi homing extension to Internet Key Exchange (IKEv2), est un protocole qui permet à IKEv2 et au tunnel IPSec de changer leurs adresses IP associées. Un client de réseau privé virtuel mobile (VPN) pourrait utiliser MOBIKE pour maintenir la connexion avec la passerelle VPN actif tout en se déplaçant d'une adresse à une autre (Eronen, 2006). Cette méthode a pour objectif d'utiliser une seule passerelle IPsecGW appropriée afin d'éviter le routage triangulaire après chaque handoff. La méthode VIRP permet aussi d'éviter que les sessions IPsec soient déconnectées lorsque le IPsecGW impliqués dans ces sessions tombe en panne. La durée de rupture de communication causée par la commutation d'IPsecGW, ainsi que le temps nécessaire pour effectuer l'optimisation de routage ont été évalués.
En utilisant des Pics ayant plusieurs cartes réseau, le temps nécessaire pour basculer les interfaces a été mesuré aussi.

les résultats montrent que la méthode suggérée a permis de déterminer la durée d'interruption de communication et le temps nécessaire pour compléter l'optimisation de routage après handoff. L'étude a montré que ce temps du traitement dépend de la puissance des terminaux, du système d'exploitation et des logiciels utilisés. De ce fait le temps d'interruption peut être court quand les terminaux sont assez puissants. La durée de l'interruption de la communication après panne peut être plus courte que le temps de déconnexion de TCP pour un navigateur web ordinaire en utilisant IPsecGWs.

(Bontozoglou et al., 2012) Proposent un cadre générique, basé sur un banc d'essai, qui permet de tester l'algorithme MADM. L'algorithme MADM permet de déterminer des critères décisionnels de déclenchement d'un handoff et de choisir le meilleur réseau auquel un nœud mobile doit se connecter lors de sa mobilité. L'architecture du système proposé est illustrée dans la figure 3.3. Elle est divisée en deux parties principales à savoir, le côté du terminal et le côté réseau. Le côté terminal fonctionne comme passerelle indépendante du média (MIG : Medium Independent Gateway), il fournit une connectivité permanente pour le

client final. Le côté réseau comprend un MIG-Manager qui s'exécute en tant que service dans le réseau, il conseille et aide dans le processus HO (hand-over).

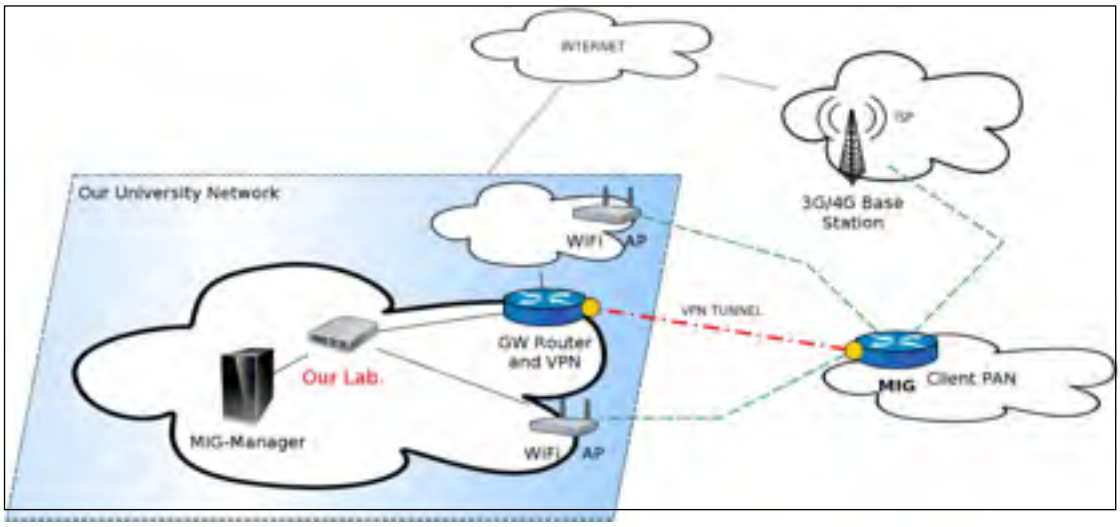

Figure 3.3 Architecture du système à haut niveau
Tirée de Bontozoglou (2012)

La liaison entre les deux côtés mentionnés est établie sur un tunnel OpenVPN qui est également utilisé pour le traitement de la continuité de la session.

MIG côté client, se compose de différents éléments où chacun est responsable d'une tâche spécifique

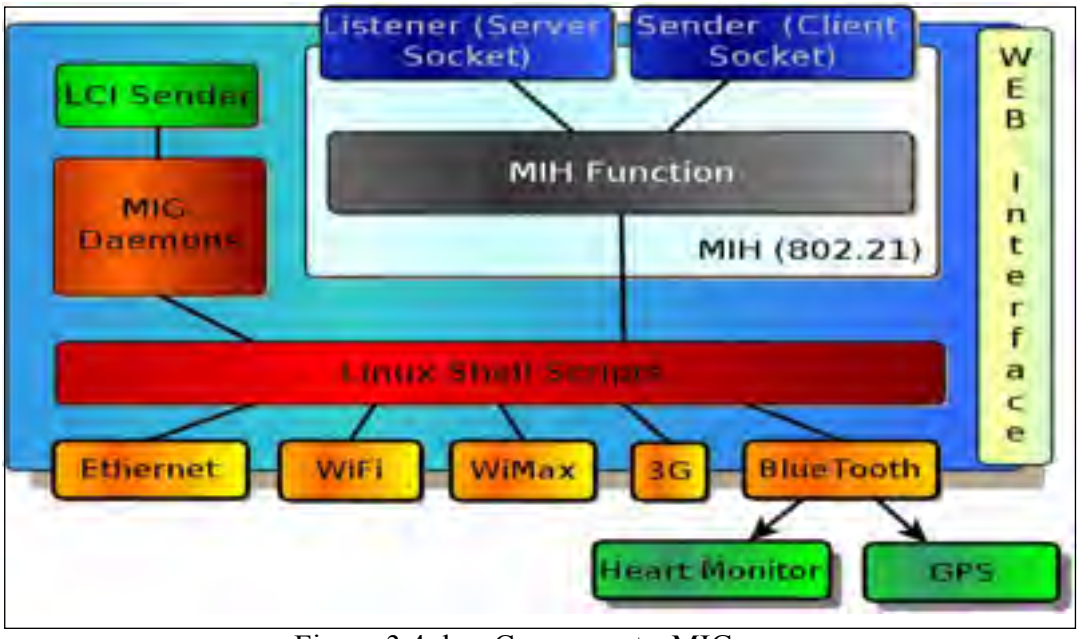

Figure 3.4 les Components MIG
Tirée de Bontozoglou (2012)

La fonctionnalité de contrôle de base sur le matériel disponible est fournie à partir de la couche supérieure. Deux catégories d'expériences ont été réalisées sur ce modèle. La première est sur le fonctionnement du système qui a été réalisée dans un scénario en banc d'essai. La deuxième catégorie concerne les expériences réalisées sur l'analyse comparative de la continuité de la session et les temps de handoff. La série d'expériences de performance handoff a été effectuée en environnement intérieur. Les résultats de cette expérience montrent que des délais de handoff pour l'utilisateur en itinérance des réseaux filaires et sans fil final en ont été satisfaisants.

(Evers et Seitz, 2006) proposent un mécanisme qui permet aux nœuds mobiles de changer leur technologie d'accès réseau d'une façon transparente au cours d'une session. Le mécanisme présenté dans cet article utilise un serveur proxy central qui est connecté à Internet et qui cache tous les nœuds mobiles (provenant de l'intérieur d'un VPN) en faisant la translation d'adresse réseau. Sa mission est d'agir comme un «serveur relais" qui se connecte à des serveurs sans être affecté par la mobilité. Le lien mobile, non fiable en raison de handoff, est isolé aux deux extrémités. Toutes les erreurs qui résultent d'un handoff sont

transparentes et cachées aux applications sur les serveurs et les applications s'exécutant sur le nœud mobile.

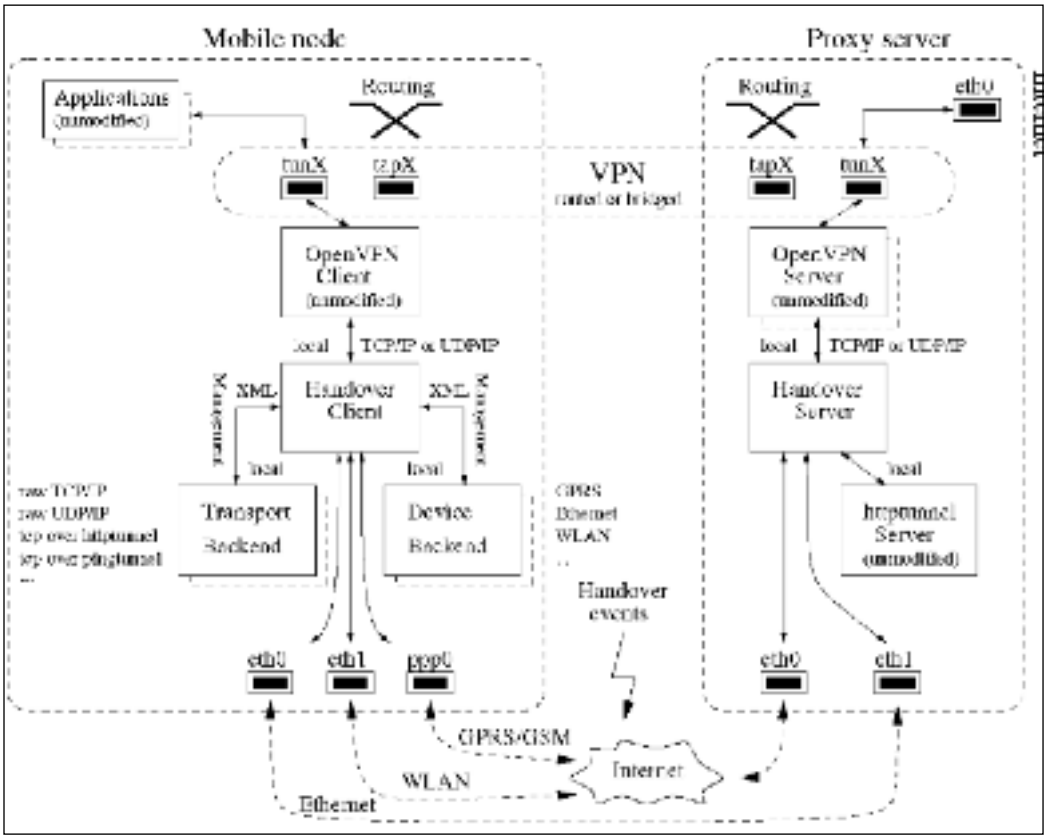

Figure 3.5 Infrastructure de VPN basé sur seamless handoff
Tirée de Evers (2006)

L'architecture de la figure 3.5 montre une infrastructure de VPN handoff. Sur le nœud mobile, tous les flux de données IP sont acheminés sur une interface réseau virtuelle (tunX utilisant OpenVPN sur GNU / Linux). Le flux de données ainsi obtenu est traité par le client handoff en cours d'exécution sur le nœud mobile. Celui-ci reçoit le flux de données du client VPN et le protège contre la perte de données pour la transmission sur les liaisons mobiles. Cela est réalisé grâce au mécanisme de segmentation / de rassemblement, en combinaison avec l'utilisation d'acquittements, pour fournir une agrégation de canaux et rendre le handoff plus souple. Toutes les technologies d'accès aux réseaux disponibles sont triées selon le critère choisi par l'utilisateur. Le "handoff manager" dans le client handoff possède une

connaissance approfondie de tous les liens sortants ainsi que leurs débits de données possibles et leurs coûts. Il décide si un lien doit être connecté et quel type de données doit être transmis. Le système est testé en termes de latence, de débit de données et de la charge. Il a été démontré que le sous-système de transfert a ajouté environ 0,2 ms pour le temps aller-retour d'une connexion OpenVPN direct.

3.3 Solution de handoff sur les réseaux maillés sans fil

Dans les réseaux maillés sans fil, la gestion de la mobilité IP est problématique, car cette dernière ne prend pas en charge la topologie dynamique et le routage multi-saut entre les routeurs mesh de backbone de ces réseaux. À cet effet, les articles choisis dans cette partie vont se focaliser sur les solutions proposées dans la recherche pour adapter la mobilité IP aux WMN.

(Srivatsa et Jiang, 2008) proposent un système hybride de handoff sur WMN qui prend en considération les connexions multi saut pour le backbone et les mesh clients. La solution proposée consiste à rajouter des fonctionnalités supplémentaires relatives à la mobilité IP pour que le routeur visité FA (Foreign Agent) et le nœud mobile MN puissent se connecter entre eux à travers de multiples routeurs mesh du réseau WMN.

Pour cela quatre nouveaux messages de signalisation pour le support de handoff dans WMN ont été introduits, à savoir, Gateway Request (GTWREQ), Gateway Reply (GTWREP), Registration (REG), Registration Acknowledgement (rack). Ces messages permettent la détection de l'emplacement de MN, la gestion et la mise à jour d'adresses CoA. Une fois associé au nouveau routeur *mesh*, le MN envoie d'abord le message *Gateway Request* pour demander une adresse IP CoA. Ce message est transmis par le routeur *mesh* associé à la passerelle de MN. La passerelle répond avec le message *Gateway Reply* qui contient l'adresse CoA. Lorsque le MN reçoit l'adresse *CoA*, il compare l'adresse *CoA* reçue avec l'adresse CoA dont il dispose. Si les adresses CoA sont identiques, ceci signifie que MN n'a pas changé sa passerelle vers l'internet. Dans ce cas, même si elle a changé à un nouveau

routeur maillé associé, il ne lance pas un handoff. Dans le cas échéant, le MN envoie un *Registration* message à la passerelle pour qu'il mette à jour sa nouvelle adresse CoA. La passerelle mesh (FA) transmet le message à HA en suivant la procédure d'enregistrement de Mobile IP standard. Le message *Registration* contient l'adresse du réseau d'accueil du MN, l'adresse IP du routeur mesh avec laquelle le MN est associée, et CoA reçu de la passerelle. Après que CoA ait mis à jour par HA, les paquets de données seront envoyés à la nouvelle passerelle. Le système proposé de handoff a été simulé sur OPNET 12. Le délai de handoff a été déterminé et comparé à celui de WLAN. Les résultats ont montré que le délai de handoff augmente avec le nombre de sauts le long du chemin qui relie MN à l'Internet, en particulier dans le cas clients du réseau maillé.

(Rongsheng, Chi et Yuguang, 2007) proposent un système de gestion de la mobilité dans WMN, appelée Mesh Mobility Management (M3). Ce système prend en considération certaines fonctionnalités de WMNs, comme le multihop et la topologie mesh, afin de mieux intégrer la micro-mobilité IP dans WMNs et offrir un seamless handoff au nœud mobile.

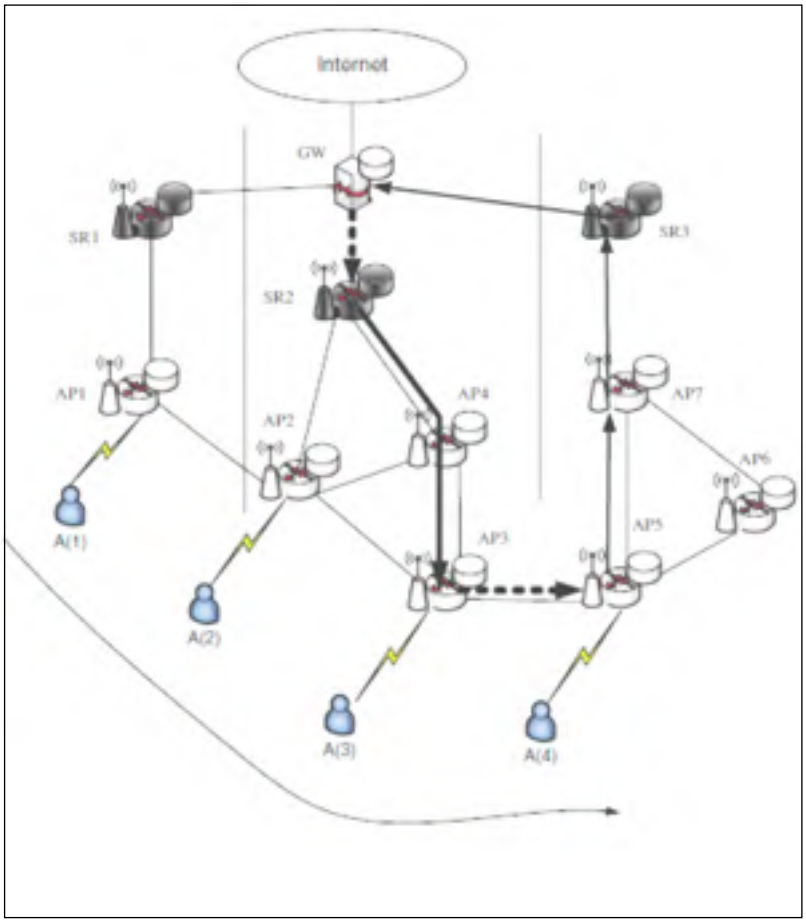

Figure 3.6 Architecture de Modèle proposé
Tirée de Rongsheng et Chi et Yuguang (2007)

Comme le montre la figure 3.6. Une architecture de trois niveaux a été utilisée. Trois points d'accès Superior router (SR) sont connectés à la passerelle. Ils sont chargés de collecter des informations de localisation des clients mobiles dans les cellules de AP. les SRs agissent comme les délégués de la passerelle et partagent le trafic de signalisation. Dans ce schéma, la technique de tunneling est utilisée pour transmettre les paquets en aval. Pour les paquets en amont, les points d'accès utilisent des routes par défaut pour transmettre les paquets à la passerelle. Lors de la réception d'un message de demande de handoff à partir du client mobile indiquant le premier ID de point d'accès, le nouveau point d'accès envoie un message de demande de transfert à l'ancien point d'accès. L'ancien AP renvoie les informations d'abonné correspondant au nouvel AP après réception du message de demande de handoff. Pendant ce temps, il ajoute une entrée temporaire dans sa table de routage avec l'adresse de destination

de ce client mobile. La Mise à jour de l'information de localisation du client mesh au niveau des routeurs supérieure est retardé jusqu'à ce qu'à une certaine période, et les informations de localisation à la passerelle est mis à jour par le routeur supérieur. Cependant, bien que l'architecture hiérarchique diminue le retard lors de la demande des informations de localisation du client au niveau de la passerelle et augmente l'évolutivité du réseau maillé, il introduit surcharge de l'encapsulation et décapsulation.

(Zhenxia et Boukerche, 2008) Proposent un schéma pour assurer la gestion de la mobilité intra-domaine à l'intérieur de WMNs. Ce schéma assure un *seamless handoff* pour les applications en temps réel. L'architecture de réseau maillé proposé, adopte un protocole de routage hybride, qui implique à la fois, le routage de la couche liaison et le routage de la couche réseau (couche 3). La solution proposée assure le seamless handoff pour l'application à temps réel. Elle permet d'éviter la latence de mise à jour de localisation, et diminue le coût du temps d'établissement de nouveaux chemins de routage après handoff. Pendant le handoff, le client mesh envoie un message ARP avec une adresse MAC du nouvel AP au nœud correspondant. Après avoir reçu ce message ARP, le nœud correspondant dresse une carte de l'adresse MAC du nouvel AP pour l'adresse IP du client mesh, et tous les paquets suivants sont transmis à la nouvelle adresse MAC du nouvel AP, directement sans ré-routage. Ensuite, le client envoie un message de dissociation de l'ancien AP avec l'adresse MAC du nouvel AP. Ainsi, l'ancien AP peut établir un tunnel pour envoyer au nouvel AP les paquets qui sont envoyés au client temporellement. Le simulateur de réseau - NS2 a été utilisé pour simuler la solution proposée. Les résultats obtenus de délai de handoff ont montré que l'algorithme de routage a permis d'éviter les mise à jour de localisation dans le serveur de site central pendant le processus de handoff. Par conséquent, un handoff plus rapide peut être réalisé avec un coût de moindre frais.

3.4 **Conclusion**

La plupart des approches proposées dans cette revue de littérature relatives au handoff VPN sans fil sont liées à la gestion de la mobilité IP. Ces solutions visent à assurer le Seamless Handoff en diminuant le délai de handoff et le taux de perte de paquets et en résolvant le problème de routage triangulaire de MIPv4 et la perte de connexion. Le problème de routage triangulaire est résolu avec l'optimisation de routage. Dans ce contexte (Byun et Lee, 2008) ont proposé la méthode NEMO et MIPv6. Néanmoins cette solution de handoff de Mobilité IPv6 permet de minimiser la période d'interruption de service mais elle ne contribue pas à la réduction de perte de paquets (Lin, Yang et Wu, 2005).

La perte de paquet est résolue en utilisant de multi homing proposé dans (Lin, Yang et Wu, 2005). Cette solution consiste à doter le MN avec deux interfaces radio LAN. Ceci permet à MN de recevoir des données à partir de multiples points d'accès simultanément, dans la couche IP, ce qui assure à MN un déplacement sans interruption de service. L'utilisation de VPN (Lin, Yang et Wu, 2005) a été également proposée pour réduire le délai de handoff. Dans ce cas ci, le MN se voit attribué une adresse privée statique. Ce qui lui permet d'utiliser la même adresse après handoff. Cette solution aide MN à non seulemet à garder la connexion VPN, mais aussi à diminuer le délai d'attribution d'adresses, car il n'aura pas besoin de s'authentifier. Néanmoins, ces solutions de mobilité IP pour VPN sur réseaux sans fil peuvent causer une dégradation significative des performances lorsqu'ils sont appliqués sur WMNs, car ces systèmes ne prennent pas en charge la connexion multi-sauts entre les routeurs mesh dans le backbone sans fil et la topologie dynamique des WMNs. (Srivatsa et Jiang, 2008). D'autre part, plusieurs mécanismes de seamless handoff pour WMN ont été proposés, tels que l'algorithme de routage, la solution hybride et la répartition des Gateway pour fournir des seamless handoff ou des fast handoff. Bien que, ces approches de la mobilité IPv4 ont pris en charge les caractéristiques de WMN, celles-ci restent insuffisantes car elles introduisent une surcharge de l'encapsulation et de la décapsulation. Telles que l'approche M3 (Rongsheng, Chi et Yuguang, 2007).

Le prochain chapitre va décrire notre nouvelle approche pour le seamless handoff qui est modélisée et appliquée pour MPLS-VPN sur les réseaux maillés sans fil pour assurer un seamless handoff VPN.

CHAPITRE 4

ALGORITHME DE SEAMLESS HANDOFF VPN SUR WMN SHVM

4.1 Introduction

Les réseaux maillés sans fil gagnent une grande popularité grâce à leurs aspects pratiques. Bien qu'ils soient attrayants, ces réseaux possèdent des défis qui doivent être résolus(Misra et Subhas Chandra Misra, 2009). Cependant le défi tel que la gestion de la mobilité s'impose dans les WMNs. Des solutions tels qu'un handoff à faible latence et des algorithmes de gestion de la localisation sont proposés pour améliorer la qualité du service au cours de la mobilité (Leung, 2007).

Dans les réseaux maillés sans fil, le processus de handoff peut être amélioré soit par smooth handoff (Belghoul, 2005), en réduisant le nombre de paquets perdus, soit par seamless handoff (Chen-Han, Jen-Shun et Ko-Ching, 2005) en diminuant la charge de la signalisation, ou bien en rendant le processus plus rapide en diminuant le délai de transfert. Dans ce dernier cas, on parle d'un fast handoff(Chen-Han, Jen-Shun et Ko-Ching, 2005).
Dans ce chapitre, une nouvelle approche pour le seamless handoff est modélisée et appliquée pour VPN sur les réseaux maillés sans fil. Cette méthode suggérée permet de diminuer le délai de handoff et la perte de paquets sur les réseaux maillés sans fil.

4.2 Description de l'algorithme Seamless Handoff VPN pour WMN(SHVM)

Cette section décrit l'algorithme proposé SHVM. Elle explique les différentes conceptions utilisées pour permettre au nœud mobile de se connecter rapidement à un nouveau point d'accès.

Pour réaliser un seamless handoff, le délai et la perte de paquets doivent être réduits pendant le handoff (Chen-Han, Jen-Shun et Ko-Ching, 2005).

Le délai de handoff peut être divisé en quatre sous délais. (Chen-Han, Jen-Shun et Ko-Ching, 2005). À savoir le délai de commutation radio qui est un délai de la couche de liaison, délai de réauthentification d'accès, délai d'association de la couche IP et le délai de l'enregistrement et d'authentification.

L'algorithme proposé a pour objectif de diminuer certains de ces délais, afin d'offrir un seamless handoff au client VPN mobile. Notre approche est basée sur trois conceptions. La première conception consiste à utiliser le principe de multi-path dans le but d'optimiser le chemin emprunté par le nœud mobile afin qu'il puisse se connecter au VPN approprié. Cette conception vise à réduire le temps de déconnexion de service et de perte de paquets. La deuxième conception a pour rôle de réduire le délai d'authentification qui consiste à utiliser la technologie VPN-MPLS, où les routeurs de clients CE sont basés sur plusieurs VRFs.

La troisième conception consiste en l'application de la technologie VPN sur les WMNS pour réduire le délai d'attribution d'adresse IP (Chen-Han, Jen-Shun et Ko-Ching, 2005).
Pour concrétiser notre approche, un modèle est proposé et est implémenté sur une architecture MPLS-VPN. Ce modèle est représenté dans la Figure 4.1

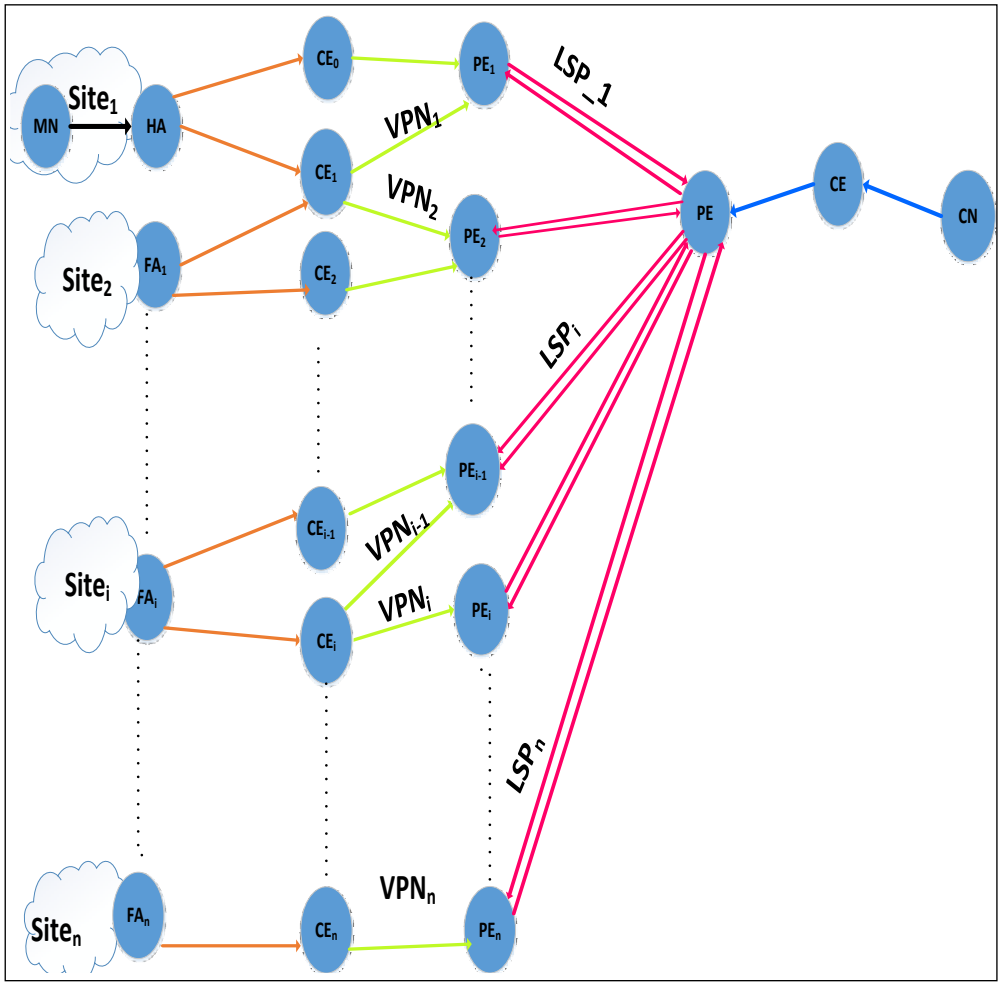

Figure 4.1 Modèle de handoff VPN

Le modèle est constitué de routeurs PE (Provider Edge), supportant la technologie MPLS_VPN. Ces PEs ont la fonctionnalité de passerelle et permettent au nœud mobile (MN) se trouvant dans un site VPN d'avoir accès au nœud correspondant (CN) se trouvant dans un autre site VPN distant.

Le routeur PE est assigné au réseau auquel CN est connecté. Il est configuré de manière à supporter plusieurs VPN.

Les routeurs PE_i sont associés au réseau auquel MN est connecté. À chaque PE_i on associe une VRF_i , qui est désignée par un nom VPN_i.

Les CE_i quant à eux sont directement connectés à plusieursPE_i. Ceci leurs permet de supporter différents VPN_i.

Les routeurs CE_i jouent le rôle de routeurs de relai entre HA et PE_1 et FA_i et PE_i. Cette connexion assurera donc un accès à internet. Ces routeurs n'ont aucune connaissance préalable de la configuration des MPLS/VPN.

Les routeurs HA et FA_i sont implémentés pour gérer la mobilité IPv4 de MN, ils sont connectés à plusieursCE_i. De cette connexion résulte différents sites supportant plusieurs VPN_i .

4.3 Fonctionnement du modèle Handoff VPN

Cette section explique comment les VPN sont assignés entre les PE_i et CE_i ainsi que la façon dont les PE_i sont sélectionnés. Elle permet aussi de montrer le rôle des CE_i dans le modèle proposé et la façon dont les CE_i doivent être configurés et placés dans l'aire du réseau, afin d'assurer la continuité de service pour un nœud mobile.

Comme il a été déjà mentionné ci-dessus, à chaque PE_i est associé uneVRF_i, qui est désignée par un nom VPN_i. De ce fait, en considérant le modèle illustré dans la figure 4.1, on constatera les cas de connexions aux VPN suivantes :
Si CE_1 est connecté à PE_1 et PE_2, ceci implique que CE_1 supporte VPN_1 et VPN_2.
Si CE_2 est connecté à PE_2 et PE_3 ceci implique CE_2 supporte VPN_2 et VPN_3.
Par conséquent le site1 attaché à HA relié à CE1 va supporter VPN_1 et VPN_2, et le site 2 attaché à FA_1 relié à CE_2 et CE_1 va supporter VPN_1, VPN_2, VPN_3

Pour le cas général, on peut déduire ce qui suit:

- CE_{i-1} supportera VPN_{i-1} et VPN_i,

- Un $site_i$ donné, qui est connecté à un FA_i relié à la fois à CE_i et à CE_{i-1} va supporter VPN_{i-1} et VPN_i.

Soit ψ un ensemble de VPNs $dusite_i$, $\psi = \{VPN_{i+1,}VPN_i, VPN_{i-1}\}$ et Φ un autre ensemble de VPNs $dusite_{i-1}, \Phi = \{VPN_i, VPN_{I-1}, VPN_{i-2},\}$.

L'intersection entre les deux ensembles donne: $\psi \cap \Phi = \{VPN_i, VPN_{i-1}\}$. Ceci implique qu'il existe toujours deux VPNs communs supportés par les deux sites.

Par exemple, un nœud mobile MN appartenant au $site_{i-1}$ et ayant une connexion VPN_{i-2} . Ce nœud va se déplacer de son $site_{i-1}$ pour se rendre au$site_i$, en s'éloignant de son site d'accueil, le MN va utiliser un autre chemin plus optimal pour transmettre ses données, par conséquent il va basculer vers le CE le plus proche de sa localisation. Si MN bascule de CE_{i-1} vers CE_i, Ceci dit qu'il va se connecter à VPN_{i-1} ou au $VPN_{i,}$ selon la table de routage de CE_i. Notons, que quand ce nœud mobile arrive au$site_i$, il ne va pas être déconnecté du VPN précédant. Ce dernier va continuer à utiliser ce même VPN qui est supporté par les deux sites.

L'analyse suivante va expliquer l'importance de configurer les CE_i sur plusieurs VPN et de les répartir d'une façon à assurer la continuité de la connexion réseau. Pour ce faire, un contre-exemple sera présenté afin de démontrer cette importance.

Soit le modèle illustré dans la figure 4.2. Dans ce cas les routeurs relais ne sont pas tous des CE. De plus, chacun d'eux ne pourra supporter plus d'un VRF.

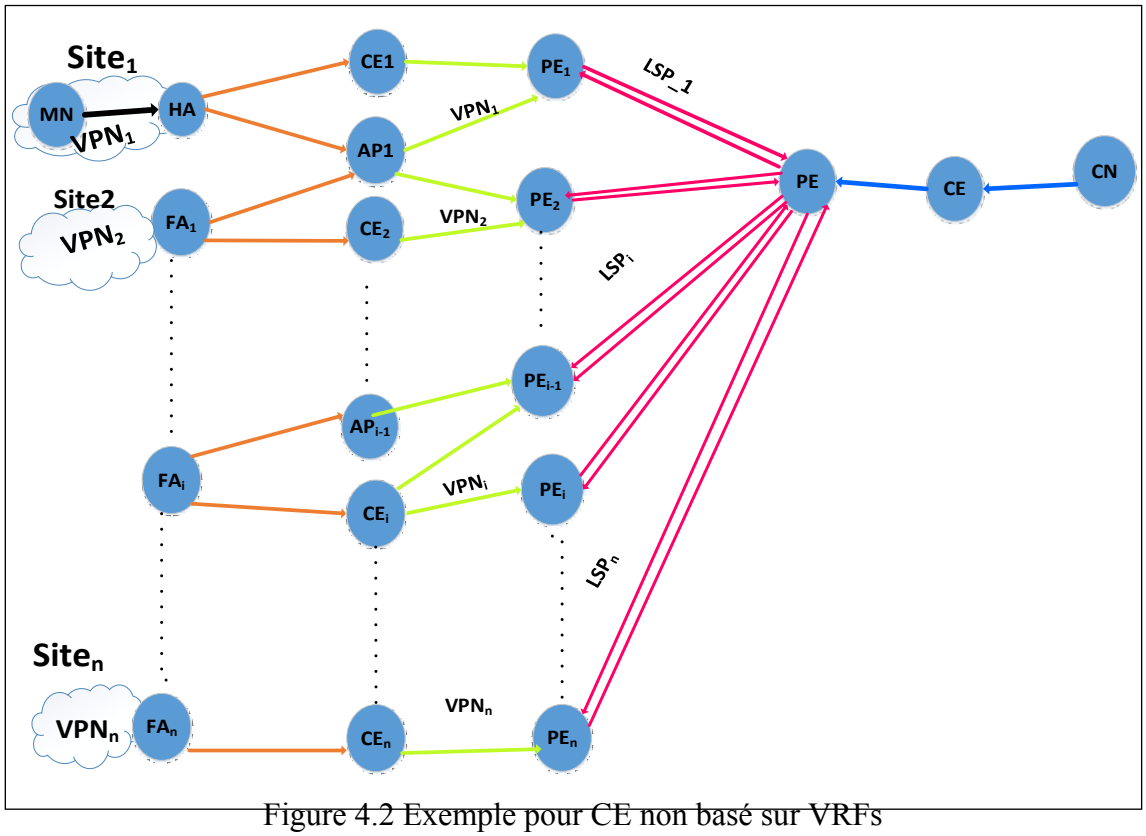

Figure 4.2 Exemple pour CE non basé sur VRFs

Dans le cas où CE_1 va supporter seulement un VPN, ceci implique automatiquement qu'il ne va supporter que VPN_1. Par conséquent le $site_1$ attaché à HA, qui est relié à CE_1 va supporter VPN_1. CE_2 quant à lui, serait connecté à PE_2 et PE_3 mais il va supporter que VPN_2 et le $site_2$ attaché à FA_1, qui est relié à CE_2 et AP_1 va supporter VPN_2.

Finalement, nous déduisons que $site_{i-1}$ serait connecté à VPN_{i-1}, et le $site_i$ connecté à FA_i va supporter VPN_i. À cet effet, quand un nœud mobile appartenant au $site_{i-1}$ et ayant connexion VPN_{i-1} se déplace vers le $site_i$ de VPN_i, il va être déconnecté, car il ne peut pas s'authentifier au VPN_i. Celui-ci le considère comme un nœud illégal. Ce qui cause une rupture de service pour MN.

De ces démonstrations, découlent deux conceptions, la première appelée conception de multi chemin, permet au MN d'utiliser un chemin optimal pour sélectionner un PE plus proche, et

la deuxième conception appelée CE basé sur les VRFs , permet au MN de rester connecté au VPN après handoff.

4.1.1 Conception du chemin optimal

Quand MN veut établir un VPN avec le CN, il doit sélectionner un PE. Le PE est déterminé de manière dynamique, grâce au protocole de routage IP dynamique OSPF utilisé entre le PE et le CE et dans tout le réseau mesh. Par exemple, parmi les PEs qui peuvent satisfaire les besoins de l'utilisateur mobile, le PE le plus proche du FA auquel est connecté le MN est sélectionné. Autrement dit le VPN qu'établit le MN avec le CN dépend du chemin qu'il emprunte pour atteindre celui-ci.

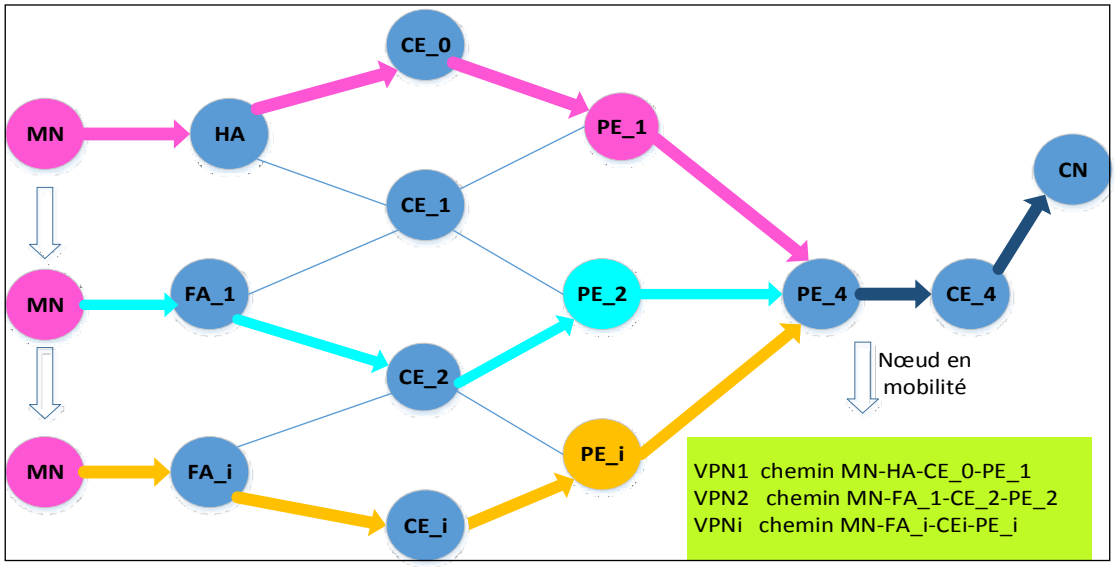

Figure 4.3 Sélection de PE

La figure 4.3 montre un exemple de différents chemins que peut emprunter MN pour sélectionner un PE (VPN). Le protocole de routage OSPF va choisir le chemin optimal en se basant sur le chemin le plus court. Cette approche de chemin optimal permet à MN de trouver rapidement un nouveau AP et de se connecter à lui. Ceci lui permet aussi de

sélectionner un VPN approprié dans la zone réseau dans laquelle il est situé après chaque handoff.

4.1.2 Conception de CE basé sur les VRFs

En utilisant la conception de CE basé sur les VRFs, MN ne va pas perdre sa connexion VPN avec CN lors de handoff. Les CEs ont connaissance de plusieurs VRFs et offrent aux sites la possibilité de supporter différents VPN. À cet effet MN change de site en se déplaçant mais ne change pas de VPN. S'il a besoin de changer de VPN, cela se produira sans rupture de service. En gardant son ancienne connexion, le MN n'aura pas besoin de demander un accès ou d'établir une nouvelle connexion, donc, il n'aura pas besoin de s'authentifier. Ceci réduit ou élimine le délai d'authentification, par conséquent le délai de handoff.

L'utilisation de ces deux conceptions, minimisent le temps d'interruption de service et le taux de perte de paquets. Ce qui permet d'assurer un seamless handoff pour les VPNs sur réseaux maillés sans fil.

4.1.3 Conception d'utilisation de la technologie VPN

La technologie VPN attribue au client VPN une adresse privée statique (Chen-Han, Jen-Shun et Ko-Ching, 2005) .Cette caractéristique contribue à diminuer le délai de liaison de la couche IP, qui est causé par l'attribution d'adresse IP dynamique. En effet en attribuant à MN une adresse IP privée statique, le MN va l'utiliser pendant le handoff.

Quand le nœud mobile s'associe à un autre point d'accès, il n'aura pas besoin de se ré-authentifier car il va utiliser la même adresse privée qui lui a été déjà attribuée. Par conséquent les messages d'échange pour ouvrir une session seront éliminés ce qui réduit le délai de réauthentification pour le MN (Chen-Han, Jen-Shun et Ko-Ching, 2005).

4.4 Structure de l'algorithme SHVM

Dans cette partie nous présentons l'algorithme proposé de Handoff VPN. Afin de permettre une bonne compréhension de l'algorithme, certains de ses éléments qui le constituent seront définis. Notons que les formules ainsi que certaines définitions utilisées dans cette partie ont été tirées de la documentation du simulateur OPNET. Ces définitions sont comme suit :

4.4.1 Définitions

- condition PRx_1<PTh

Cette condition permet à MN prendre la décision de déclencher un handoff et de chercher un nouveau point d'accès pour s'y associer à lui.
PTh définit la valeur de la puissance seuil reçue (sensibilité du récepteur) du récepteur elle est exprimée en dBm.

La puissance PRx_1 est la puissance reçue de nœud mobile, elle calculée suivant la formule 4.1.

$$P_{Rx1} = \frac{G_{Rx} * G_{Tx} * P_{Tx}}{\left(4\pi f \frac{D1}{c}\right)^2} \quad (4.1)$$

Avec :

- PRx= puissance de réception de nœud mobile,
- GRx= gain de réception,
- GTx= gain de transmission,
- Dans notre cas GRx et GTx sont égales à zéro dB car il n'y a eu l'utilisation d'antennes,
- PTx est la puissance de transmission,
- D1 est la distance entre HA et MN,

- λ est la longueur d'onde,
- c, est la vitesse de la lumière,

$$\lambda = \frac{f_{min}}{B/2} \tag{4.2}$$

- f_{min} est la fréquence minimale,
- $B/2$ est la bande passante utilisée lors de la transmission.

D1 est calculée selon la formule 2, elle est comme suit :
Si le nœud mobile (MN) et le point d'accès (AP) auquel il est connecté sont désignés respectivement par leurs coordonnées cartésiennes (ax, ay) (bx, by).

La distance qui sépare le MN et l'AP est calculée selon la formule Pythagore.

$$D1 = \sqrt{(dx^2 + dy^2)} \tag{4.3}$$

Avec $\begin{cases} dx = bx - by \\ dy = by - ay \end{cases}$

- condition PRx_2>PTh

Cette condition définit la fin de handoff et le début d'association au nouveau point d'accès FA et PTh désigne toujours la puissance seuil.

PRx2 est la puissance de réception de nœud mobile reçue de nouveau point d'accès. Cette puissance est calculée avec la formule 4.4. Cette formule est identique à la formule 4.1 utilisée pour calculer $PR_{x1,}$ on a seulement la distance D1 qui a été changée par distance D2.

$$P_{Rx2} = \frac{G_{Rx}\ G_{Tx}P_{Tx}}{\left(4\pi f \frac{D2}{c}\right)^2} \quad (4.4)$$

D2 est la distance qui sépare MN du nouveau point d'accès. D2 est calculée avec la formule2 en utilisant les coordonnées cartésiennes de MN et du nouvel AP.

- la condition si PE[i] donc VPN[i]

Cette condition permet de sélectionner un VPN avec un chemin optimal. Dans cette partie les deux conceptions de chemin optimal et de CE basé sur les VRFs sont appliqués.

4.5 **Présentation de l'algorithme**

L'algorithme de handoff VPN est représenté dans la figure 4.4. Initialement le MN sera attaché au routeur d'accueil HA, un VPN_1 est établi entre lui et le CN situé dans un autre réseau privé. Le MN va suivre une trajectoire d'une longueur TRj, initialisée à zéro.

Quand le nœud mobile commence à se déplacer, l'état (roaming) est activé. Le MN évalue la distance DIST qui le sépare de son point de départ. DIST est le résultat que donne la fonction Distance présentée dans la figure 4.6

Tant que le MN est en état roaming il doit comparer la distance DIST à TRj et tant que DIST < TRj, le MN doit effectuer les trois phases suivantes :

```
1 Data: AP=FA; Roaming=Enabled; DIST=0;
2 while (roaming = Enable) do
3    Get DIST
4    while (DIST <TRj) do
5       Get power function            /* calculating the transmit power */
6       if (PRX1 < PTh) then          /* PTh= threshold power */
7          ScanMode = Enable          /* state allowing the mobile node to find a new AP*/
8          if (AP = Found) then
9             Get Power fuction
10               if (PRX2 > PTh and AP=AF) then
11                  ScanMode= Disabled
12               end
13         end
14      end
15   end
16 end
```

Figure 4.4 Algorithme de Handoff VPN

1) Phase 1: Mode Roaming

Dans cette phase, le MN évalue sa puissance reçue PRx1 à chaque fois qu'il détecte un changement dans sa position qui le sépare de HA.

La fonction de calcul de la puissance reçue de MN est représentée par la Figure 4.5.PRx est le résultat que renvoie cette fonction de la puissance.

La puissance de réception varie en fonction de la distance D. La fonction de la distance est représentée par la Figure 4.6.

```
Power function
1 Input: double GTx,GRx, λ,PTx ,B,fmin;C const; C= 3.0E+08
2 Function power(D: double)
3 |   get(double x1,double y1, double x2,double y2)
4 |   D=dist(x1,y1,x2,y2).
5 |   fc=fmin+B/2.
6 |   λ=fc/[B/2]
7 |   PRx=(PTx*GRx*GTx)/[(4*π*λ/D)*(4*π*λ/D)]
8 |   return PRx;
9 end
```

Figure 4.5 Fonction de la puissance

```
Distance function
  Function Distance function(double xa,double ya, double xb,double yb)
  |   double dx, dy;
  |   dx = xb-xa;
  |   dy = yb-xb;
  |   D=sqrt dx*dx+dy*dy;
  |   return D;
  end
```

Figure 4.6 Fonction de calcul de la distance

À chaque changement dans la distance qui sépare MN d'AP, la puissance de réception de MN est réévaluée et comparée à la puissance seuil PTh.

Si la puissance de réception de MN diminue et devient inférieure à PTh, le nœud mobile entre dans l'état ModeScan. Dans le cas échéant, MN reste connecté à HA ou à l'ancien AP. La connexion VPN quant à elle reste toujours établie entre le MN et CN.

2) Phase 2 : Mode Scan

Pendant cette phase le MN cherche un nouvel AP dans son voisinage pour qu'il se connecte à lui. En effet selon le standard (802.11), périodiquement, les AP_S de tout le réseau envoient des balises de niveau de liaison contenant ESSID pour mesurer la force du signal. Ainsi en entrant dans le ModeScan, le MN commence par diffuser des requêtes de sondage (Probe request) contenant des informations sur son ESSID et son débit. Par la suite, MN écoute le réseau et attend une réponse de l'un des APs sur le réseau. En recevant, la première balise le MN, peut ainsi réévaluer la distance qui le sépare de nouvel AP, et déterminer la puissance reçue.

La fonction de calcul de puissance est de nouveau appelée pour calculer la puissance PRx2. PRx2 est le résultat renvoyé par la fonction calcul de puissance de la figure 4.5

Si la puissance PRx2 reçue de la part de nouvel AP est plus importante que la puissance de seuil PTh, le MN doit s'assurer qu'il s'agit d'un routeur FA (foreign Agent) avant qu'il s'associe à lui. Dans le cas échéant le MN reste en ModeScan jusqu'à ce qu'il trouve un réseau qui prend en charge sa mobilité IP. Dans ce mode bien que le MN soit déconnectée du premier AP il reste toujours connecté au VPN. Pour cela la fonction VPN est appelée. Cette fonction est représentée dans la figure 4.7.

Dans cette phase la conception de CE basé sur les VRFs est appliqué. Tel qu'il est décrit dans la section 4.1.2, le MN passe d'un site à un autre, mais il garde sa connexion VPN, le temps qu'il trouve un nouvel AP.

3) Phase 3 : Association au nouvel AP

Une fois AP trouvé, MN s'associe à cet AP et se désassocie de HA. En appliquant le standard de MIPV4, le routeur AP qui est foreign agent attribue au MN, une adresse temporaire d'hébergement (CoA). Lors de son acquisition de la nouvelle adresse, MN

envoie un message de demande d'enregistrement à l'agent d'accueil HA, ensuite il l'informe de sa nouvelle adresse en lui envoyant un message Binding Update. Ceci permet aux agents MIP de modifier leurs listes de liaison de MN à la nouvelle adresse CoA. Lorsque HA reçoit le message de mise à jour de MN via FA, il obtient l'adresse de MN et envoie un message de réponse Binding Ackowledgement pour confirmer la mise à jour. HA met à jour le cache de liaison correspondant avec la nouvelle CoA afin d'acheminer correctement les paquets destinés vers MN.

4) Phase 4 : Association au VPN

Une fois associé au nouveau FA, le MN peut établir un nouveau VPN avec le CN afin de pouvoir lui transmettre les données. Si le MN transmet les données à CN, la conception de chemin optimal sera appliquée. MN cherche le chemin le moins couteux pour se connecter au CN tel qu'il est décrit dans la section 4.2. Si PE_i est sélectionné, alors un VPN_i sera utilisé. En se basant sur le standard de la mobilité IP (Perkins, 2002), la réception de données pour MN serait comme suit :

Le CN transmet les données à HA via VPN_1. Le HA les intercepte, encapsule les données et les transmet à FA auquel est connecté MN, à travers un tunnel établi au préalable. Le FA décapsule les données reçus par HA et les transmet à son tour au MN.

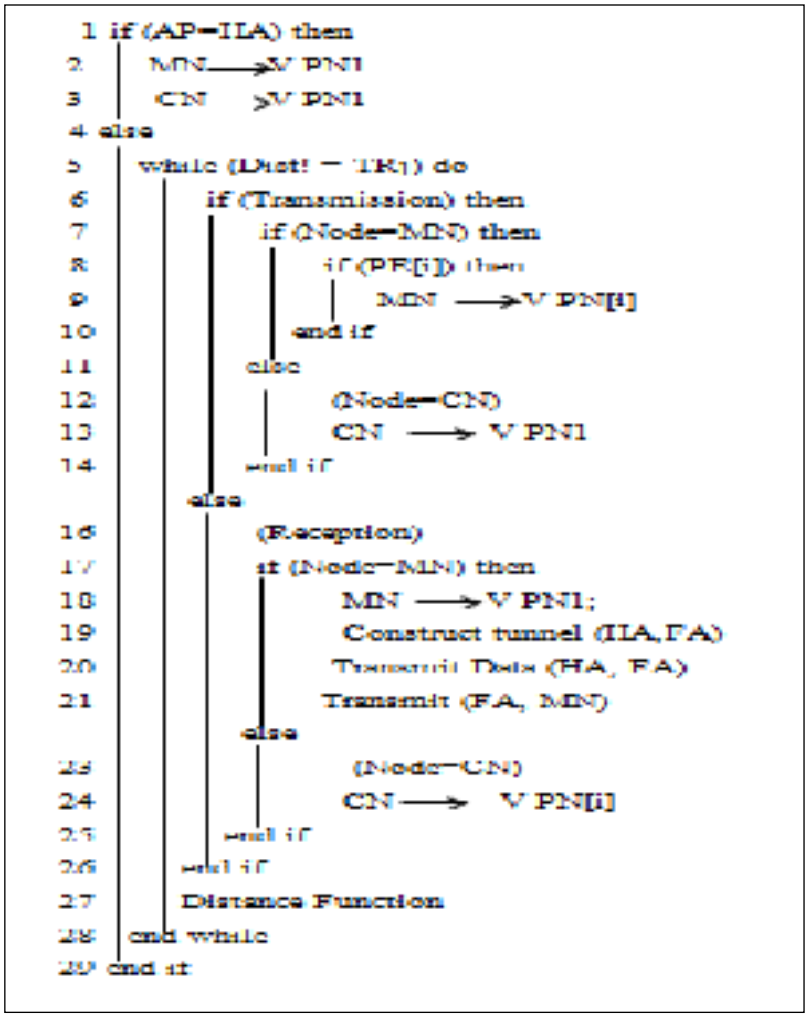

Figure 4.7 Fonction VPN

4.6 **Conclusion**

Pour gérer la mobilité dans les VPNs sur les réseaux maillés sans fil l'algorithme SHVM est proposé. Celui-ci repose sur trois conceptions qui visent à réduire le délai de handoff et la perte de paquets. La première conception du chemin optimal consiste à réduire le temps de rupture de service et de perte de paquets. La deuxième conception de CE supportant plusieurs VRFs permet de réduire le délai de réauthentification et la dernière conception est celle reliée à l'utilisation de VPN, elle permet de réduire le délai d'attribution d'adresse IP. Dans ce chapitre nous avons présenté le fonctionnement de ces conceptions et comment elles peuvent

être utilisées pour qu'elles soient efficaces. Nous avons expliqué le rôle de chacun d'elles et leur contribution pour diminuer le délai de handoff.

La conception de chemin optimal vise à avoir une connexion rapide en sélectionnant un PE plus proche de FA auquel est connecté MN. Ceci est possible grâce à la façon dont sont répartis les différentes CE sur l'aire du réseau.

La conception de CEs basés sur VRFs permet au nœud mobile de se déplacer d'un site à un autre sans rupture de service. Ceci contribue à diminuer le temps de rupture de service ainsi que la perte de paquets.

La dernière conception, qui est une simple application de VPN, consiste à diminuer le délai d'attribution d'adresse qui contribue à offrir un fast handoff.

Le prochain chapitre va décrire les différents scénarios de la simulation qui a été effectuée afin de valider notre étude. À travers les différents scénarios de la simulation nous avons montré la performance de l'algorithme SHVM. Pour cela le simulateur OPNET 16 est utilisé afin d'implémenter le modèle proposé.

CHAPITRE 5

SIMULATIONS DE L'ALGORITHME SHVM

Introduction

Pour valider notre étude, l'algorithme proposé SHVM est modélisé et implémenté dans OPNET 16. Pour cela deux parties principales de scénarios ont été élaborées, à savoir le scénario de référence et les scénarios de l'influence des paramètres WLAN.

Le scénario de référence permet d'évaluer l'efficacité des conceptions de seamless handoff, sur quoi est basé le modèle proposé. Pour cela, certains critères tels que le taux de pertes de paquets et le délai de handoff ont été déterminés lors des simulations effectuées sur ce scénario. L'impact de la gigue et le délai de bout en bout ont aussi fait partie de l'étude dans ce scénario, et ceci afin de permettre l'évaluation de l'efficacité du modèle proposé en terme de performance de qualité service dans le réseau.

La deuxième partie relate les étapes intermédiaires qui ont mené au choix définitif des paramètres WLA du modèle proposé. Parmi ces paramètres qui ont eu une grande influence sur la conception sur l'architecture proposée, on cite la puissance de transmission, le débit de transfert, et la vitesse de nœud. Pour mieux évaluer ces critères, et justifier notre choix des paramètres reliés au réseau maillé sans fil, une étude sur la variation de ces paramètres a été effectuée et simulée notre approche. En effet l'étude dans cette partie, consiste à assigner des canaux dynamique à tous les nœuds sans fil du réseau et à faire varier la vitesse du nœud mobile, la puissance et le *data rate* des routeurs concernés par la mobilité IP. Dans ces scénarios le taux de perte de paquets a été déterminé afin d'étudier l'impact de ces paramètres WLAN sur le modèle proposé.

Pour pouvoir discuter et analyser les résultats obtenus des scénarios simulés, des métriques de performances sont utilisées et définies ci-dessous. Certaines de leur définition sont tirées de la documentation du simulateur OPNET.

5.1 Les métriques de performances

Dédit VPN

Cette statistique mesure la quantité de trafic VPN sortant par le PE de sortie (EGRESS), cette statistique est mesurée en paquets par seconde.

Gigue

Est la variation de latence ou le délai de transmission de bout en bout des paquets.
Pour deux paquets consécutifs quittant la source à t1 & t2 et sont reçus par destination à l'instant t3 et t4, la gigue serait = (t4 - t3) - (t2 - t1).

Délai de bout en bout

Est le délai total des paquets de voix, appelé aussi "mouth-to-ear" de (bouche-à-oreille) est la durée entre le temps ou le nœud émetteur remet le paquet à RTP (Real Time Protocol) et le temps le récepteur le reçoit de RTP.il est défini comme suit :

Délai de bout en bout = Délai de réseau + Le délai de codage + Le délai de décodage + délais de compression +de décompression.

1) délai de réseau est la durée entre le temps ou le nœud émetteur remis le paquet à RTP (*Real Time Protocol*) et le temps où le récepteur le reçoit de RTP.

2) le délai de codage sur le nœud transmetteur, est calculé à partir du système d'encodage.

Le délai total de handoff

le délai de handoff se compose de deux parties (Zhenxia et Boukerche, 2008):

1) Le délai de la couche liaison, est le temps où MN se réassocie avec un nouvel AP dans la couche de liaison. Dans notre cas, ceci correspond au moment où le MN se déconnecte de son AP pour se connecter à son nouvel AP. Pour cela les statistiques de Throughput au niveau de la couche MAC des interfaces WLAN des routeurs HA et FAs auxquelles est connecté MN sont utilisées. Ceci consiste à déterminer le temps entre le moment où le throughput commence à diminuer sur l'interface relié à MN de l'ancien AP et le moment ou le nouveau AP commence à acheminer les paquets sur son interface relié à MN.

2) Le délai de la couche réseau est la durée entre le moment où le client mobile décide de commencer un handoff et le moment où le nœud correspondant reçoit le premier paquet.

Ceci revient à étudier la période où le débit du trafic reçu par CN diminue et atteint son minimum et la période où le débit du trafic reçu commence à augmenter. Pour cela les statistiques du trafic RTP reçus du nœud correspondant sont utilisées. Ceci consiste à localiser la zone d'intersection entre le temps du dernier paquet envoyé par HA et le temps du premier paquet reçu par CN de FA.

Pour permettre de déterminer le délai de handoff, un agrandissement a été effectué sur certaines zones des graphes de ces statistiques, jugées significatives pour déterminer le délai handoff.

Paquets perdus

Est le nombre de datagrammes IP perdu par tous les nœuds du réseau sur toutes les interfaces IP.

Throughput

Est le Trafic total en bits/s, reçu et transmis par la couche MAC à la couche supérieure.

5.2 Les critères de la qualité de service de la voix

La qualité de service pour un flux voix sur IP nécessite les critères illustrés dans le tableau 5.1 (YOUNES 2009). Celui-ci illustre les normes tolérées pour le délai de bout en bout, la gigue et le taux de pertes de paquets.

Tableau 5.1 Les critères de la qualité de service pour un flux voix sur IP

Métrique	**Excellent**	**Acceptable**	**Tolérable**
Le délai de bout en bout	100 et 150 ms	150 ms et 250 ms	< 400 msec
La gigue de délai	40 ms	40 ms et 75 ms.	
Le taux de pertes de paquets	< 5 %		

pour le délai de handoff, la valeur ne doit pas dépasser 120ms pour les applications à temps réel (Zhenxia et Boukerche, 2008).

5.3 Scénario de référence

Cette partie consiste à décrire le modèle de référence. Celui-ci est modelé sur OPNET 16 pour permettre l'étude de handoff VPN sur les réseaux maillé sans fil. Pour cela des paramètres tels que le délai de handoff, les pertes de paquets, le délai de bout en bout ainsi que la gigue ont été déterminés durant la simulation du scénario de référence.

Le modèle de référence est composé de deux sous réseaux. Le subnet_1 et le subnet_0, les deux sous réseaux sont connectés entre eux via un backbone internet comme illustré dans la figure 5.1.

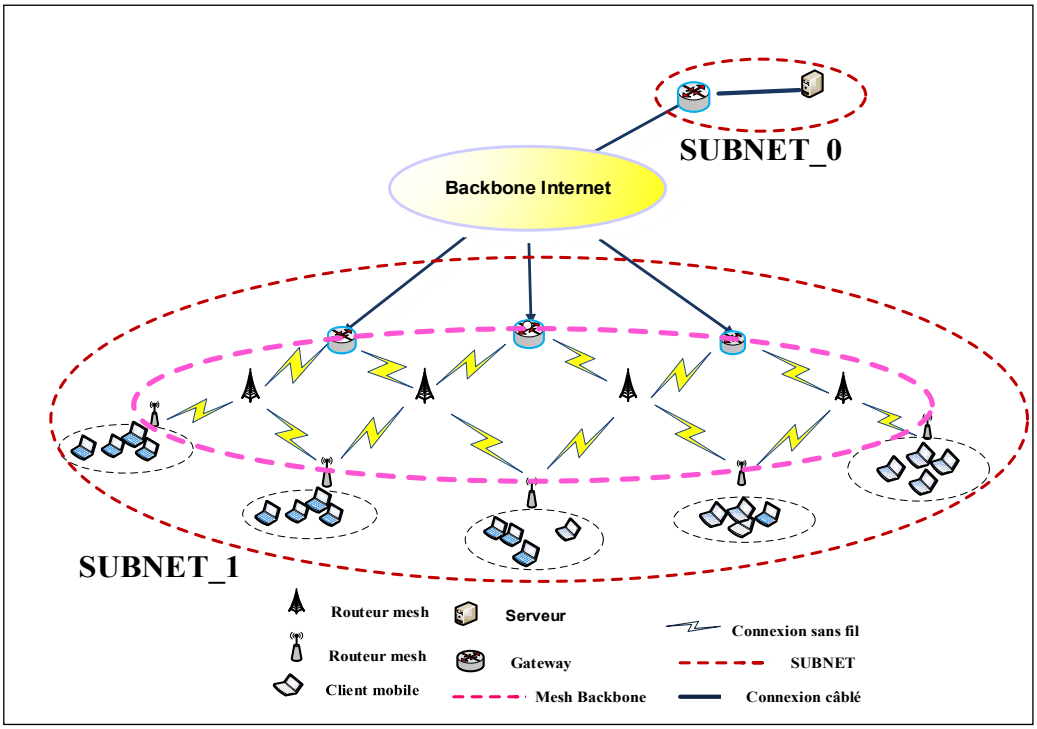

Figure 5.1 Modèle de référence

Le Subnet_0 est le sous réseau d'Ethernet qui contient l'application voix, il est constitué d'un serveur et d'un routeur. Ce routeur est relié au backbone internet avec une ligne dédiée T1, d'un débit de transmission de 1,544 Mbps. Ce routeur sert de passerelle pour le serveur d'application.

Le serveur est relié au routeur par un lien Ethernet 100BaseT, le routeur et le serveur ne sont dotés que d'interfaces IP.

Le Subnet_1 est le sous réseau contenant l'architecture WMN où la technologie des réseaux sans fil IEEE 802.11g a été utilisée.

Le sous-réseau subnet_1 est constitué de stations (client) mobiles et d'un backbone de routeurs mesh, comme le montre la figure 5.1. Le réseau WMN est réparti sur une aire d'infrastructure de 5000 x 5000 m^2, La portée de chaque nœud est de 750 m.

Des routeurs fixes sont placés au bord du backbone WMN reliés à l'internet par une connexion câblée, à l'aide d'une ligne dédiée T1 dont le débit de transmission est de 1,544 Mbps. Ces routeurs assurent l'accès internet au réseau maillé sans fil. Ils sont dotés de deux interfaces WLAN et une interface IP.

Huit routeurs mesh mobiles statiques sans fil forment le backbone mesh et assurent le relai entre les passerelles et les nœuds mobiles. Les routeurs mesh mobiles ne sont dotés que d'interfaces WLAN.

Dans cette architecture, 16 stations WLAN mobiles ont été utilisées. Un point d'accès sans fil est associé à chaque ensemble de quatre stations mobiles formant ainsi quatre sous réseau WLAN. Les paramètres par défaut offert par OPNET ont été utilisés pour configurer l'application, le profil de l'application utilisé est exécuté en série, et le temps départ de celle-ci est constant (200 secondes) et sa durée est jusqu'à la fin de la simulation.

Tableau 5.2 les paramètres de l'application de la voix

Nom de la destination	Voice Destination
Système d'encodage	G.729A
Trames de voix par paquet	20
Type de service	Best Effort

Dans ce modèle nous avons introduit la technologie MPLS_VPN où l'adressage IP auto assigné est appliqué sur tous les nœuds suivant leur BSS ID.
Le backbone internet joue le rôle des routeurs P (Provider), les routeurs d'accès internet t jouent le rôle de PE (Provider Edge) et les routeurs de relais ont le rôle de CE (customer Edge). Dans ce réseau trois zones sont créés :

1) Zone MPLS: Est constituée de routeurs P et de routeurs PE, ces routeurs sont configurés pour supporter le protocole MPLS. Entre les PE les P, le protocole OSPF et le protocole

RSVP sont utilisés. les routeur P qui sont placés au cœur du backbone MPLS jouent le rôle de LSR et transportent les paquets étiquetés.

2) Zone MP-iBGP : Est composée de routeurs PE, ces derniers sont configurés avec des adresses loopback et de protocole MP-IBGP. Les routeurs PE_1, PE_2, PE_3 sont reliés au routeur PE_0 avec MP-IBGP. Le temps de départ IBGP est configuré à 160 s. Les PEs sont configurés pour supporter les VRFs. Le tableau montre les différents VRF supportés par différents PEs. Les routeurs PEs jouent le rôle de relai entre les CEs et les routeurs P.

3) Zone utilisateurs : elle est composée de routeurs CE, de routeurs mesh et de clients mobiles. Le protocole de routage dynamique OSPF est utilisé entre les PEs et les CEs et dans tout le reste du réseau mesh. Les CEs ne supportent pas le MPLS, ils vont juste établir le lien avec le PE auquel ils sont reliés et partager leurs routes avec celui-ci.

En effet les CEs du réseau mesh donnent des informations de routage des clients aux PEs auxquels ils sont connectés. Ces derniers mettent à jour leurs tables VRF et communiquent ces informations au routeur PE_0 à l'aide des LSP qui sont créés entre lui et les autres routeurs PEs. Le PE_0 à son tour fournit le serveur CN des nouvelles informations de routage. Le temps de départ de LSP est configuré d'une façon à ce qu'il soit inférieur au temps de départ IBGP, pour cela il a été fixé à 150s.

Tableau 5.3 Configuration des VPNs

VPN	PE_0	PE_1	PE_2	PE_3
VPN_10	✓	✓		
VPN_20	✓		✓	
VPN_30	✓			✓

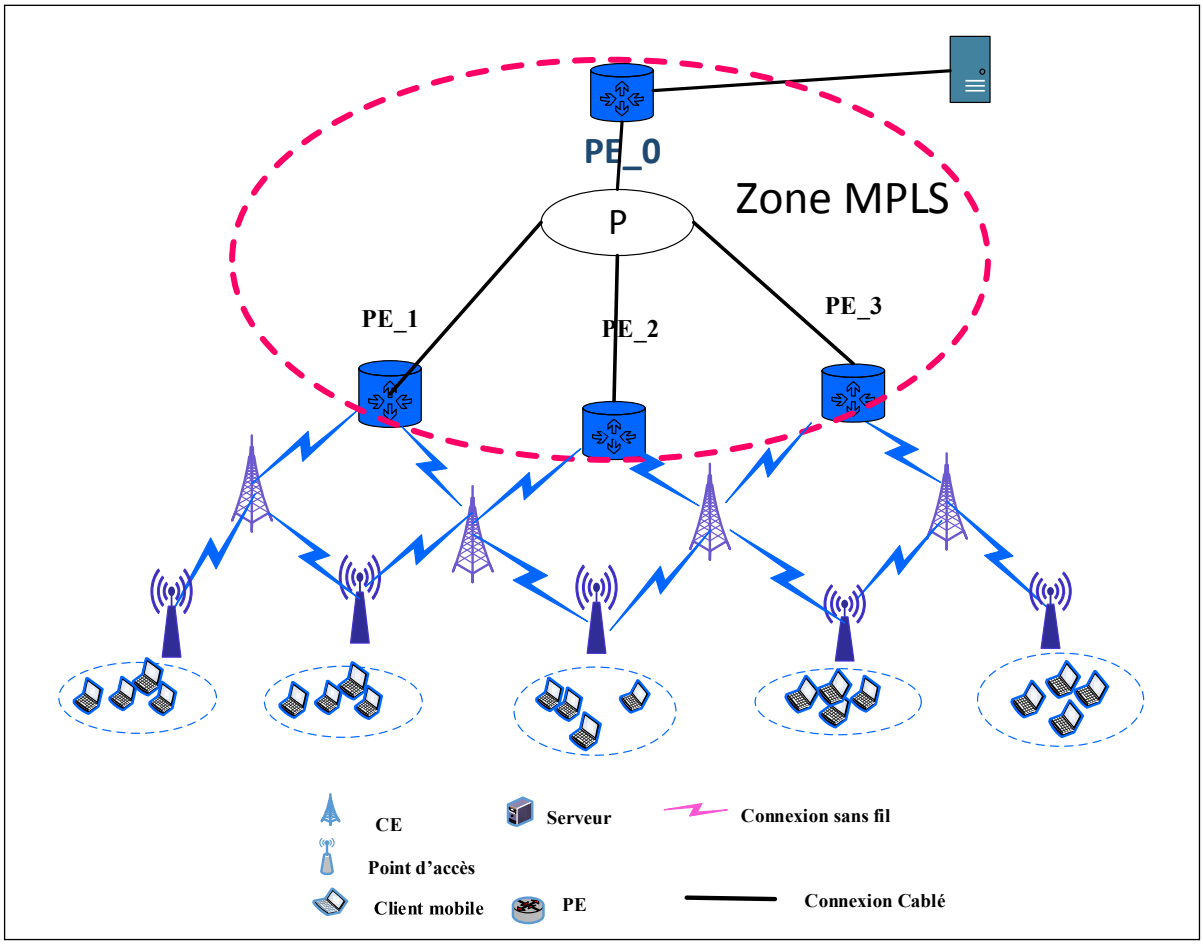

Figure 5.2 Zone MPLS dans l'architecture du réseau maillé sans fil

Le protocole de routage IP dynamique OSPF est utilisé entre PE et CE et dans tout le sous-réseau subnet_1 et subnet_0. Sur toutes les interfaces des PE directement reliées avec les CE, on a assigné à l'interface de PE une VRF. Dans ce modèle toutes les stations mobiles suivent une trajectoire aléatoire (default random waypoint) sur une aire de 750m sur 750 m avec une vitesse de 5 m/s. Une station d'entre elles supporte le profil de l'application voix et suit une trajectoire constante avec une vitesse de 2K/h. Cette station se déplace du site 2 pour arriver au site 5. Tel que la montre la figure 5.4.

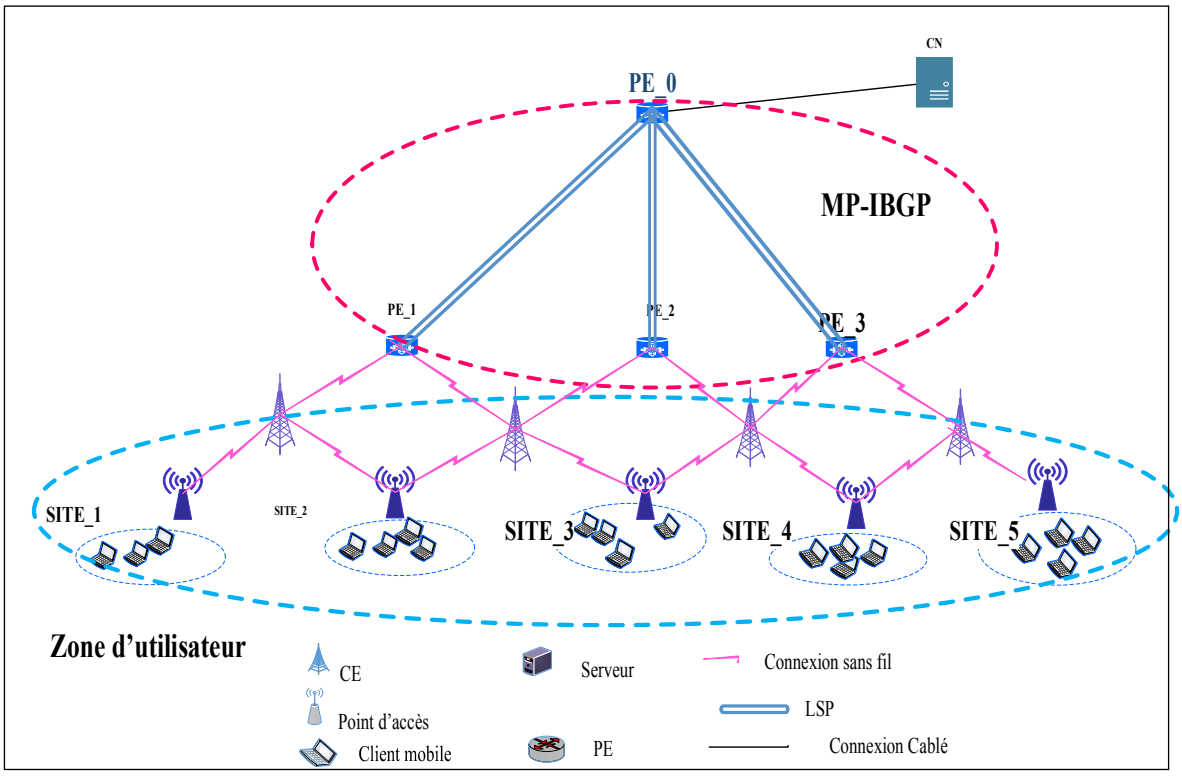

Figure 5.3 Zone utilisateur et zone MP-IBGP de l'architecture SHVM

Dans ce cas-ci la mobilité IP est introduite. Le client mobile utilise le service de l'agent d'accueil HA et des routeurs agents visités FA (1, 2,3) pour la transmission et la réception de ses données. Les routeurs FAs (foreign Agent) et HA sont configurés avec différents BSS ID. Ces derniers jouent le rôle de points d'accès pour le client mobile ainsi que pour d'autres nœuds mobiles.

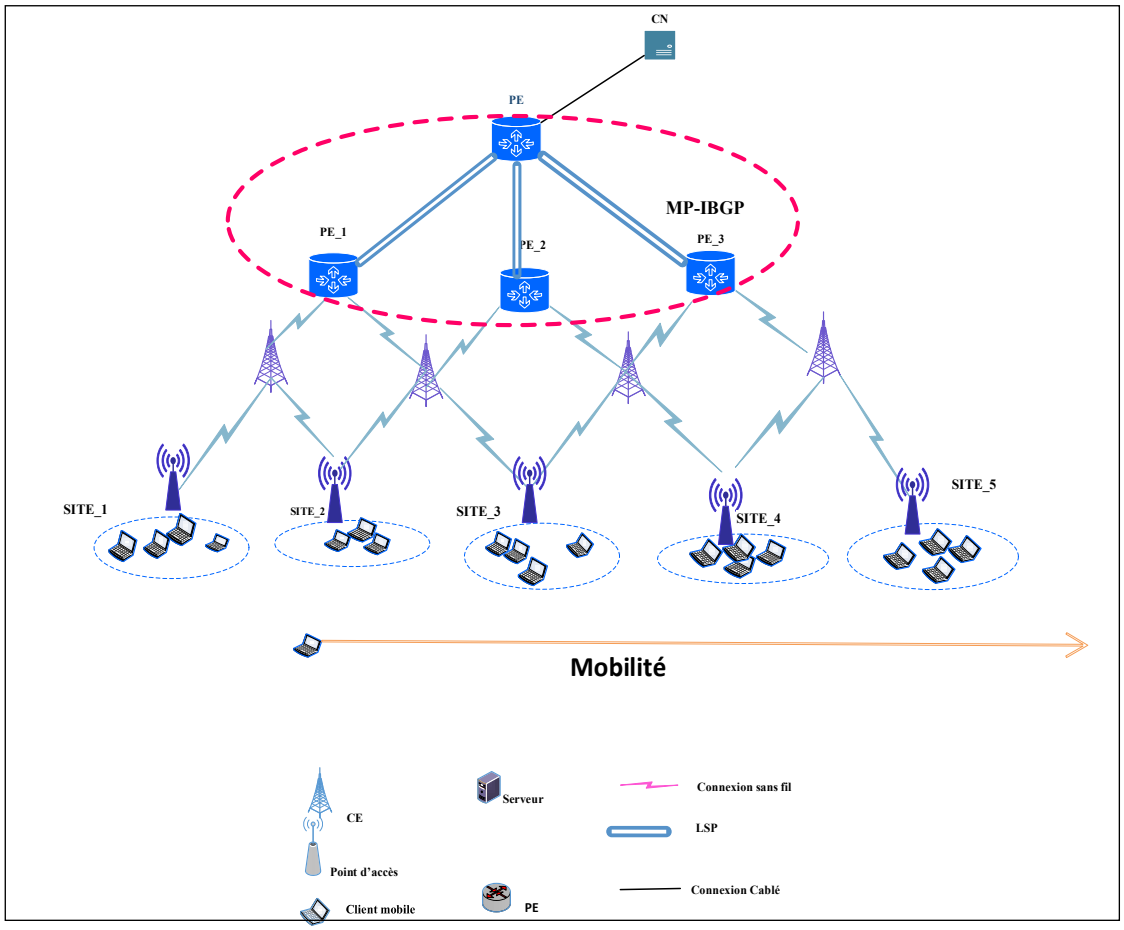

Figure 5.4 MPLS-VPN sur WMN avec nœud mobile

Dans ce modèle de référence un serveur situé dans le réseau subnet_0 envoie du trafic au Client mobile. Étant donné que le client mobile se déplace le long de la trajectoire, il change de point d'accès et change d'agent mobile. Les paquets lui seront envoyés par tunnel aux différents foreign agents selon le standard de la mobilité IP(Perkins, 2002).

Tableau 5.4 Paramètre de configurations du scénario de référence

Nœud	**Taux des données (Mbps)**	**Puissance de transmission (W)**	**Assignement du canal**
HA	1	0.02	dynamique
FA_1	1	0.009	dynamique
FA_2	1	0.009	dynamique
FA_3	1	0.05	dynamique
Client mobile	1	0.1	dynamique
Stations locales mobile	5.5 Mbps	0.0001	1, 6,11

5.4 Les résultats et les analyses des scénarios

Cette section est composée de deux parties. La première partie comprend le scénario du modèle de référence destiné à étudier l'algorithme proposé en termes de délai de handoff et perte de paquets, ainsi que les performances de qualité de service du modèle. La deuxième partie concerne l'étude de l'influence des paramètres de WLAN sur le modèle proposée.

5.4.1 Résultats et Analyses

Cette partie est consacrée à la présentation des résultats des simulations effectuées sur le modèle SHVM à l'aide de simulateur OPNET 16,comme elle est destinée aussi à l'interprétation et l'analyses de résultats obtenus.

5.4.1.1 Résultats et analyses du scénario de référence

a) Résultats du délai de handoff

Comme il a été mentionné dans la section 5.1, le délai de handoff se compose de deux délais, à savoir le délai de la couche de liaison et le délai de la couche réseau.

1) Résultats du délai de la couche de liaison

Pour déterminer le délai de handoff de la couche de liaison, les statistiques de *throughput* du simulateur OPNET sont utilisées. Le résultat de ces statistiques est montré dans le graphe de figure 5.5.

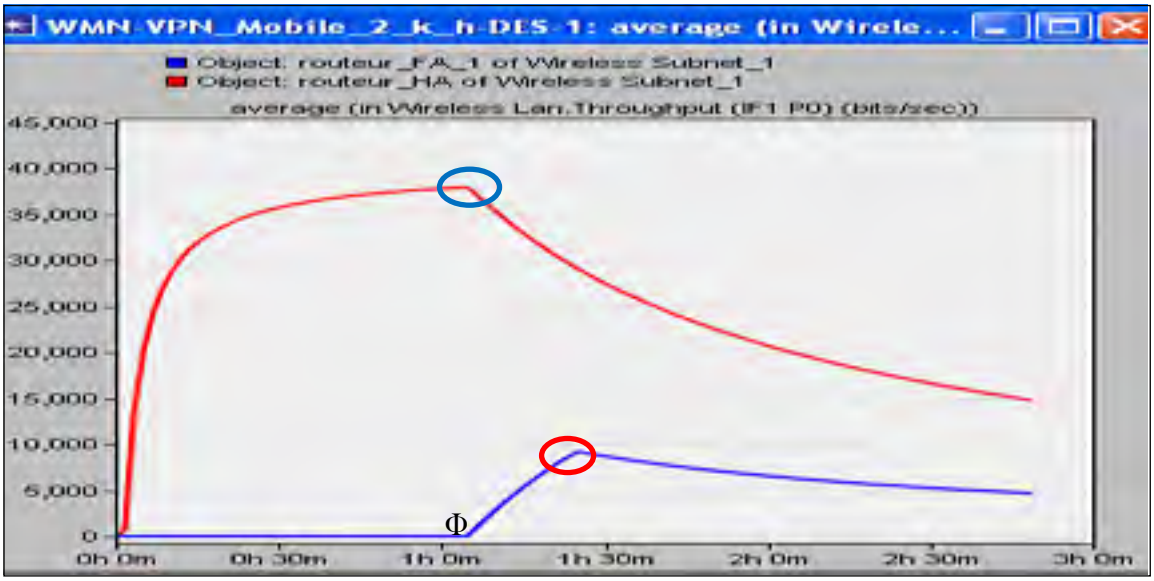

Figure 5.5 Trafics reçus et envoyés de FA_1 et HA_1 vs. Le temps

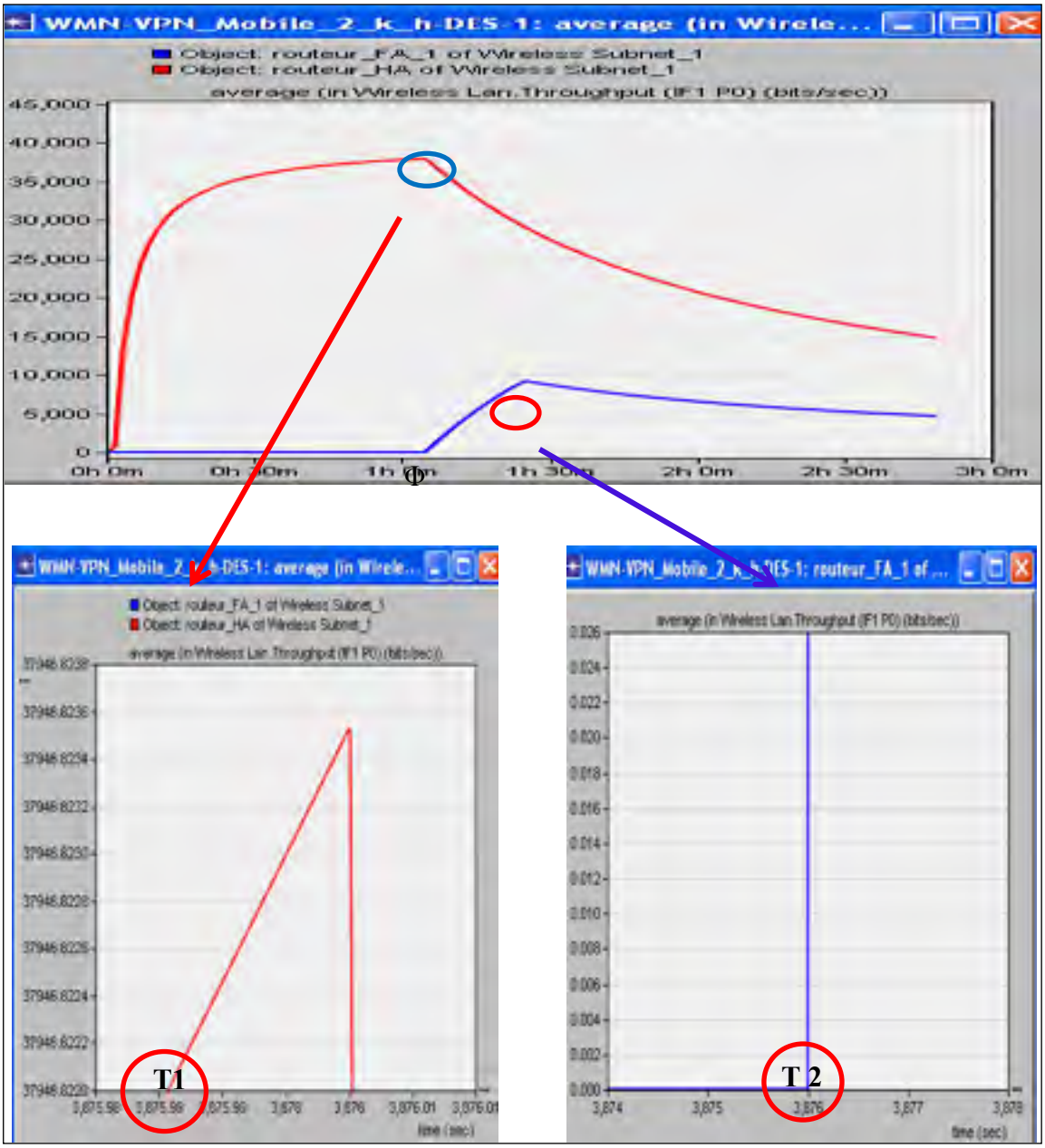

Figure 5.6 Agrandissement des portions des graphes des *throughput* de HA et FA

Le graphe de la figure 5.5 représente le taux du trafic acheminé, par les interfaces WLAN MAC de HA et FA_1 reliés à MN.

D'après ces graphe, le trafic transitant par HA augmente durant un l'intervalle du temps de [0, 3875.9925] s. Or, pour le même intervalle, le graphe de *throughput* de FA_1, illustre qu'il n'y a aucun trafic qui passe dans FA_1. Ceci prouve que pour cette période, le MN est connecté à HA et non pas à FA_1. Cependant, à partir du temps égal à 387.9925s, le taux du trafic commence à augmenter pour FA_1 et à diminuer pour HA. Cela montre que le MN s'est connecté à FA_1 et que son trafic est acheminé par celui-ci. Cette durée entre connexion et du MN de HA et sa connexion à FA_1 peut être utilisée afin de déterminer le délai de handoff pour la couche de liaison pour MN. Dans le graphe la figure 5.5, cette durée est représenté par Φ où un agrandissement a été effectué sur les zone des trafics de HA et FA. L'agrandissement de ces zones est illustré respectivement dans les graphes de la figure 5.6

Soit T1, le temps où le taux de trafic dans HA commence à diminuer, celui-ci est assimilé au temps de déconnexion de MN de HA. T2 est le temps où FA_1 commence à acheminer le trafic de MN, ce temps est assimilé au temps de connexion de MN à FA_1.

Soit T le délai de handoff de la couche de liaison pour MN. Ce temps de handoff est la différence entre le temps de déconnexion du MN de HA(T2) et le temps de sa connexion à FA_1(T1).

$$T = T2 - T1. \qquad (5.1)$$

D'après le graphe de la figure 5.6 et la figure 5.7, T2 = 3876s, et T1= 3875,99s.
Donc le temps de handoff pour la couche de liaison est :
T = 3876-3875,99= 0,010 s = 10 ms.

D'après (Zhenxia et Boukerche, 2008) le temps de délai de handoff pour la couche MAC est fixé à entre 40-50ms.

2) Résultat du délai de la couche réseau

Les graphes des statistique RTP du trafic reçu du nœud correspondant CN sont utilisés pour déterminer le délai de la couche réseau.

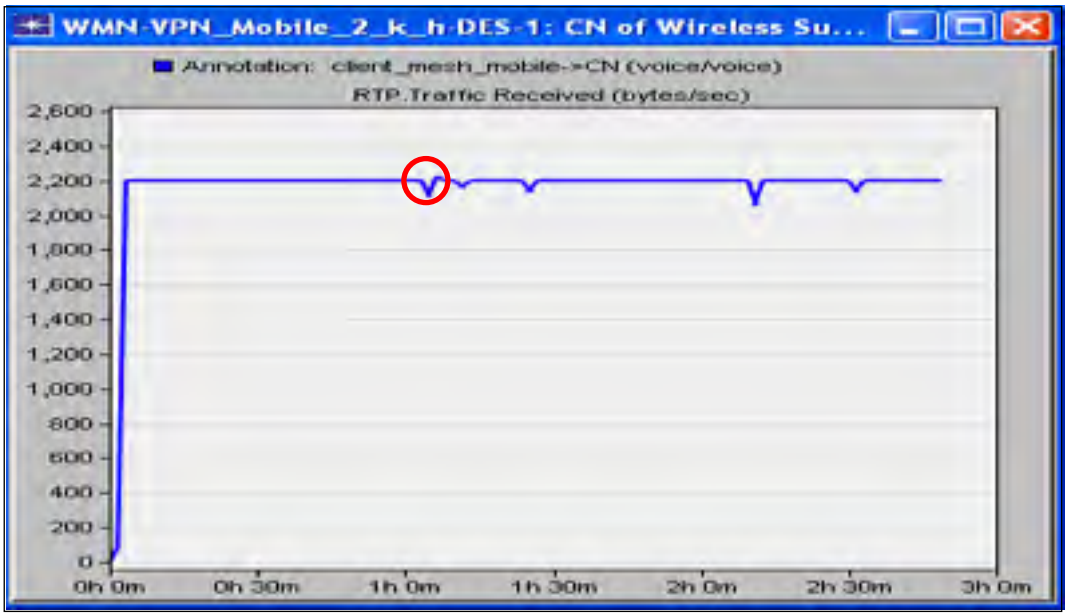

Figure 5.7 Trafic RTP reçu de CN Vs le temps

La zone entourée en rouge dans la figure 5.7 montre que le taux du trafic RTP reçu par CN diminue pour un certain laps de temps, pour croître de nouveau pour atteindre sa valeur initiale.

En effet, quand la puissance entre MN et HA diminue, MN ne sera pas en mesure d'acheminer le trafic de HA vers CN, ce qui explique la diminution du taux de trafic envoyé à CN. Comme le signal reçu de la part de FA_1 est supérieur à celui reçu de HA, le MN ne tarde pas à se connecter à FA_1. De ce fait, à partir du moment où MN se connecte à FA_1, celui-ci se charge d'acheminer le trafic de MN vers CN.

Nous assumons que la différence entre le temps où CN reçoit le dernier paquet envoyé par HA et le temps où CN reçoit le premier paquet envoyé par FA, correspond au délai de handoff de couche réseau. Pour calculer ce temps, un agrandissement a été effectué sur la zone entourée en rouge sur graphe de la figure 5.8. L'agrandissement est illustré sur le graphe de la même figure.

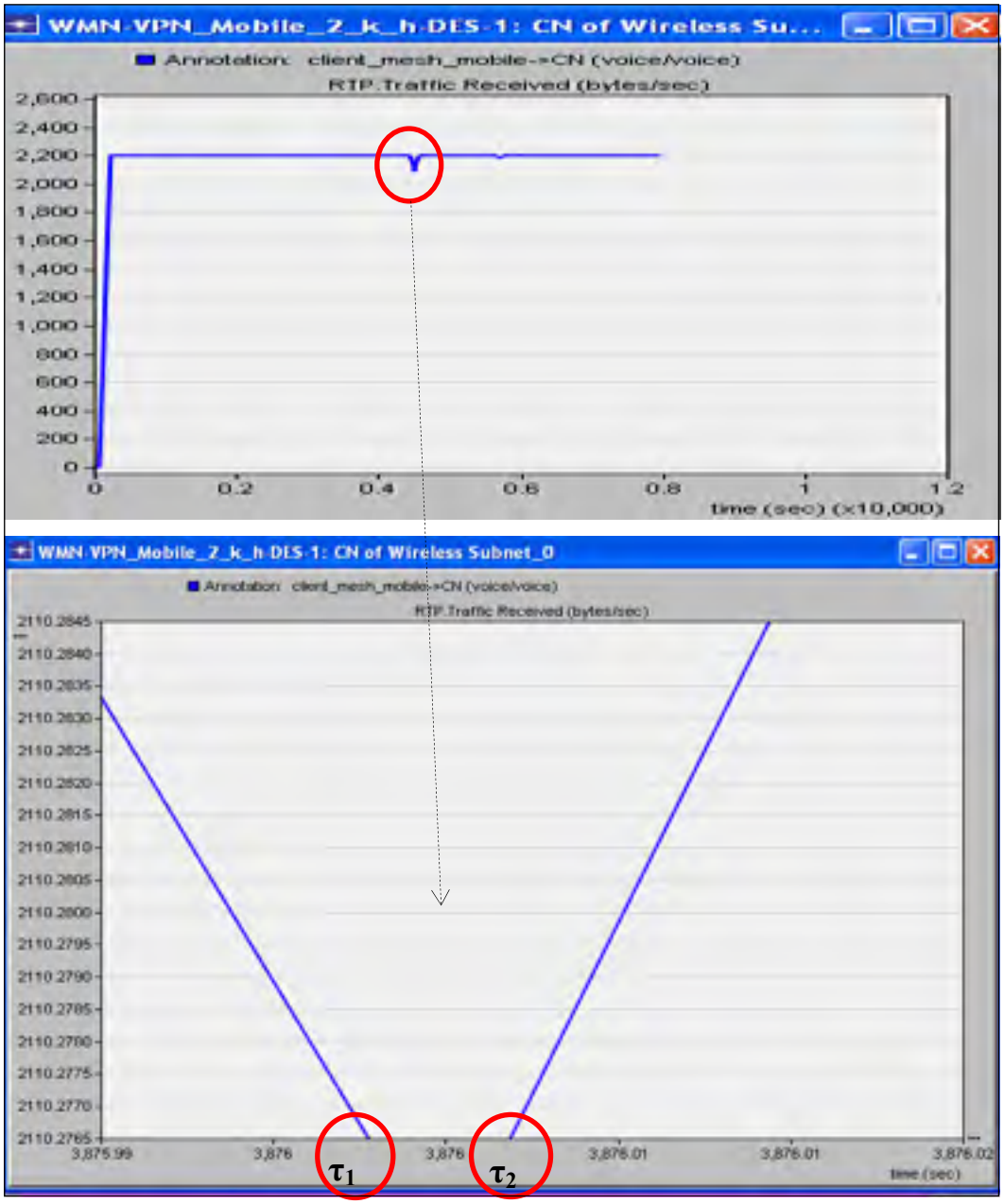

Figure 5.8 Agrandissement d'une portion du graphe du trafic RTP reçu de CN

Soit τ, le temps de handoff de la couche réseau, τ_1 et τ_2 sont les temps des deux plus bas trafics reçus par CN, τ_1 correspond temps transmission du dernier paquet envoyé de HA à CN. Ce temps correspond à la valeur 3876,0025 s du graphe de la figure 5.8.

τ_2 correspond au moment où le CN reçoit son premier paquet juste après le handoff.

Sur le graphe de la figure 5.8 ceci correspond à la valeur 3876,0075. Comme déjà défini ci-dessus dans la section 5.1, le temps de handoff va correspondre à

$$\tau = \tau_1 - \tau_2 \tag{5.2}$$

D'où $\tau = 5ms$.

La figure 5.9 illustre le calcul du délai total de handoff, celui-ci est égal à la somme de délai de la couche de liaison T et de délai de la couche réseau τ, comme il a été défini dans la section 5.1.

$$\text{Délai total de handoff} = T + \tau \tag{5.3}$$

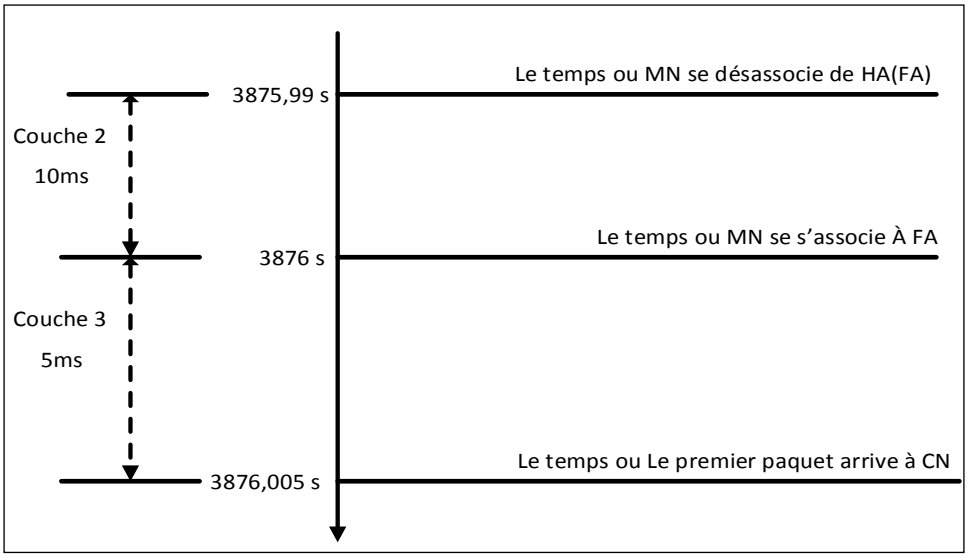

Figure 5.9 Méthode de calcul de délai total de handoff

À cet effet le délai total de handoff est égal T+ τ = 15 ms.

D'après(Zhenxia et Boukerche, 2008) le délai de handoff pour une application en temps réel ne doit pas dépasser 102ms.

Le résultat obtenu de délai de handoff, montre que le modèle proposée répond aux normes exigées en termes de délai pour une application à temps réel. Notre objectif pour un délai de handoff minimal est atteint, grâce à l'application de la conception du chemin optimal. Cette approche de chemin optimal permet à MN d'utiliser le meilleur chemin parmi plusieurs chemins disponibles, ceci aide MN à trouver rapidement un nouvel AP et de se connecter à lui. Ceci lui fournit aussi la possibilité de sélectionner un VPN approprié dans la zone réseau dans laquelle il est situé après chaque handoff. Ce qui a contribué à réduire le délai de handoff.

b) Perte de paquets

Afin de déterminer le ratio de paquet perdus, les statistiques *data dropped* et de *throughput* sont utilisées. Ces statistiques sont illustrées par les graphes de la figure 5.10

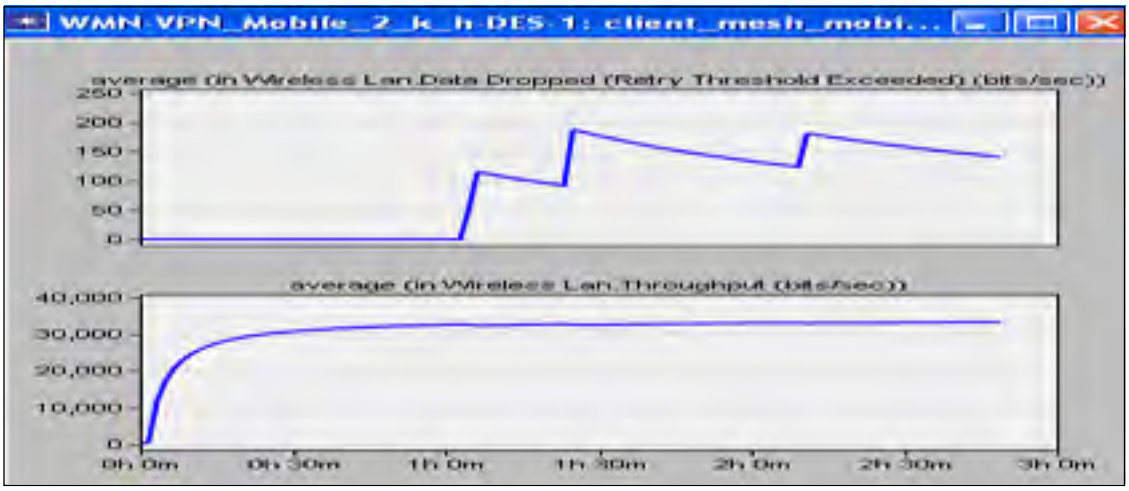

Figure 5.10 Graphes de données perdues et du taux de trafic moyen reçu de MN

Les graphes de la figure 5.10, illustrent la perte de paquet et le *throughput* de MN en débit/s en fonction du temps exprimé en minutes.

Le graphe de *throughput* montre que la plus grande valeur moyenne atteinte pour le nœud mobile MN est de 33253,6959 bits/s.

D'après le graphe de *data dropped*, la plus grande valeur moyenne des données perdues est 146,3627 bits/s. par conséquent le ratio de perte de paquets est de 0.00440. Ceci est équivalent à 0.44%. Cette valeur est inférieure à la norme tolérée pour les applications voix qui est de 5%. Ceci montre que l'objectif de la continuité de la connexion est atteint, grâce à l'application de la conception CE basé sur les VRFs qui a contribué à minimiser le temps d'interruption de service et le taux de perte de paquets.

c) Délai de bout en bout

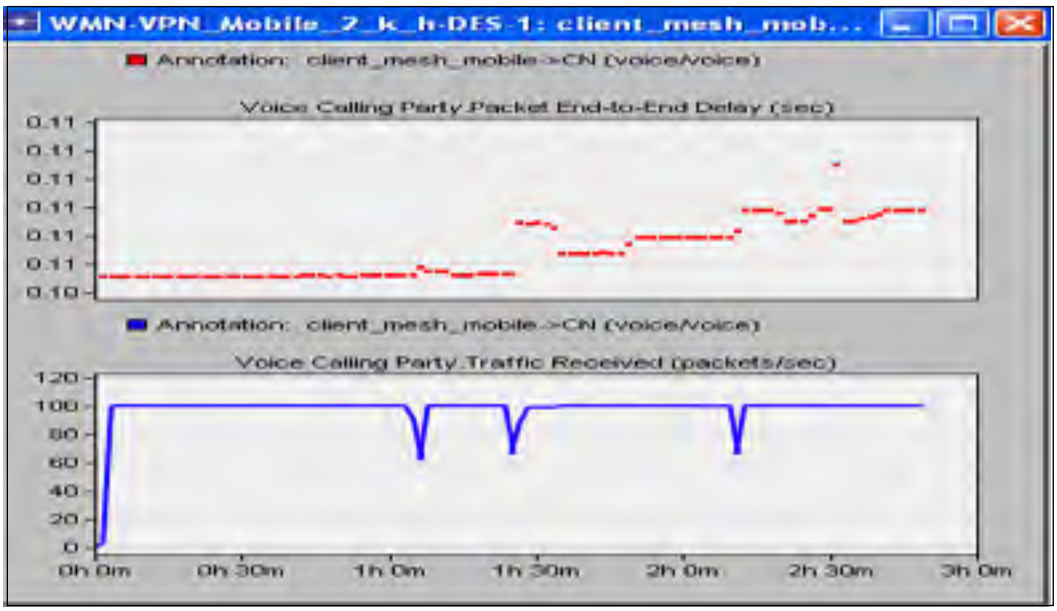

Figure 5.11 Délai de bout en bout et trafic reçu de l'application voix

La figure 5.11, représente le délai de bout en bout mesuré en seconde, en fonction du temps mesuré en minute

Les résultats des graphes de la figure 5.11, montrent que le délai de bout en bout augmente avec la mobilité du nœud. Selon, le standard de la mobilité IP (Perkins, 2002), quand le nœud mobile est dans la zone visitée, il envoie les données via le FA de sa localité, mais pour la réception de ses informations, le routage triangulaire est utilisé. En effet, le CN envoie les données destinées à MN par l'intermédiaire de HA qui à son tour les envoie à MN via d'un tunnel préétabli entre le FA et le HA. Par conséquent, plus la distance entre le MN et le HA augmente, plus le nombre de saut n'augmente et le délai que met le MN pour recevoir les données augmente aussi. Toutefois, les résultats obtenus montrent que l'utilisation du standard de la mobilité IP n'a pas d'impact significatif sur le délai, étant donné que la plus grande valeur enregistrée pour le délai de bout en bout est de106 ms, qui est une valeur excellente en termes de critère de qualité de service dont la valeur varie entre 100 et 150ms (tableau 5.1section 5.1). Notre approche a permis de tirer profit de l'utilisation de la mobilité indirecte. En effet, en utilisant la mobilité IPv4, un tunnel est établi entre HA et FA pour l'acheminement des données de HA à MN, ceci, pouvait engendrer un délai transmission des données et la surcharge dans le réseau, à cause de l'encapsulation et de la décapsulation des données transmises et en raison de l'augmentation de la distance entre HA et MN. Toutefois, avec l'application de notre approche, ces contraintes ont été évitées, ce qui a permis un acheminement de données d'une façon sécuritaire avec le tunnel établi entre HA et FA sans l'ajout de délai de bout en bout.

d) Résultat de la gigue

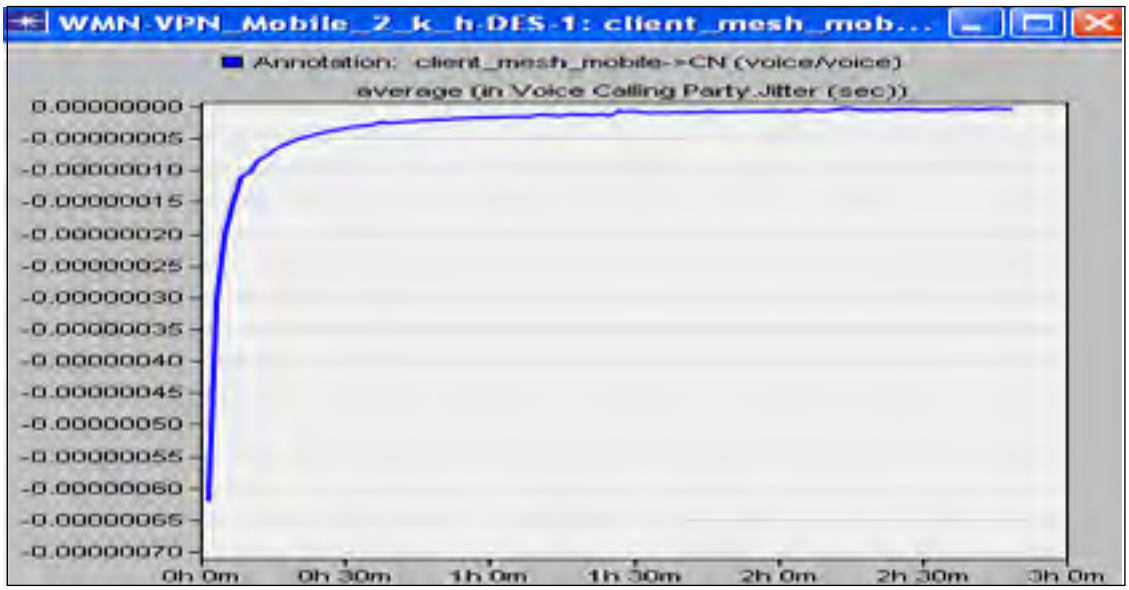

Figure 5.12 Graphe de la gigue de MN vs temps

La figure 5.12 montre le graphe de la gigue mesurée en seconde, en fonction du temps mesuré en heure. La plus grande valeur moyenne de la gigue enregistrée est de 0,03µs. Cette valeur est constatée au début de la simulation. D'autre part la plus petite valeur moyenne enregistrée de la gigue est de 0.006µs. Celle-ci demeure constante tout au long de la simulation. Ceci montre qu'il n'y a pas de délai entre les paquets reçus par MN. Cependant, bien que la mobilité IP indirecte soit utilisée pour la réception de données pour MN, les performances du réseau ne sont pas affectées par la gigue. L'application de la conception de multi-chemin et le concept de CE basé sur VRF, a non seulement aidé à effectuer un seamless handoff, mais a permis aussi aux paquets de MN d'être reçu par celui-ci sans délai supplémentaire à leurs destination.

e) les Résultats de la charge VPN

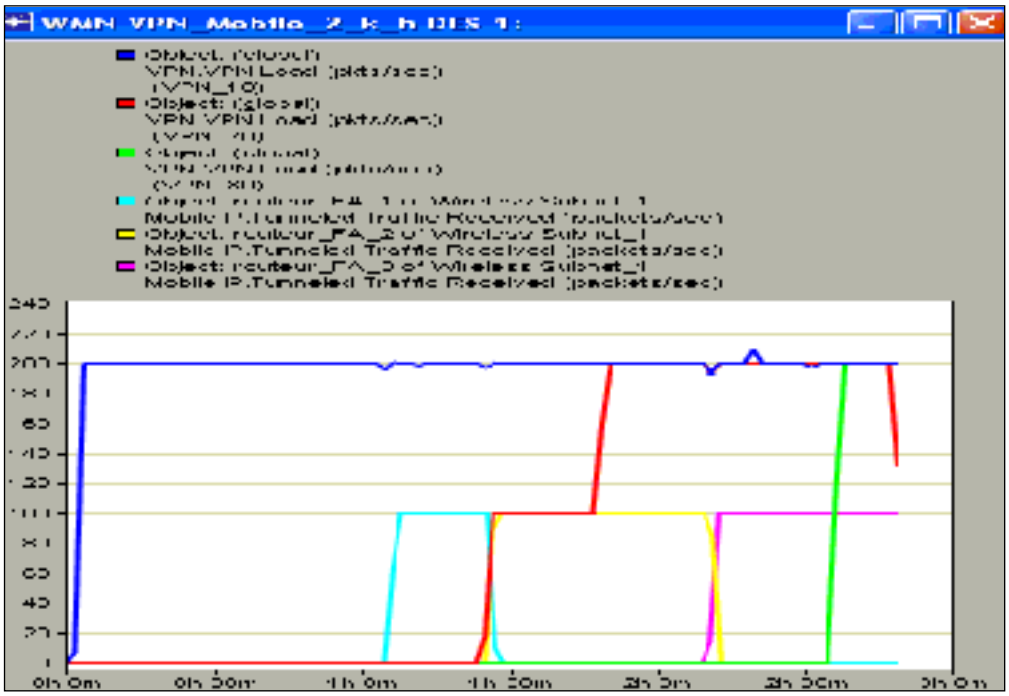

Figure 5.13 Charges de différentes connexions VPN
et les Trafic reçus des FAs via le tunnel d'IP mobile Vs. Le temps

La figure 5.13, représente les graphes de connexions VPN du nœud mobile, et le trafic transmis à MN via le tunnel établi entre HA et FA_1 et entre HA et FA_2. La charge de VPN est exprimée en paquets / seconde et le temps est exprimé en minutes.

Ces graphes montrent que pour l'intervalle [0, 1h04mn], la connexion VPN_10 est établie entre MN et CN. Pour le même intervalle, la figure montre qu'il n'y a aucun trafic qui passe dans les routeurs FA_1, FA_2 et FA_3. Ceci prouve que le nœud mobile est connecté au routeur d'agent d'accueil, et que ses données sont acheminées via ce routeur, en utilisant une connexion VPN_10.

Pour l'intervalle du temps [1h, 1h23mn], le trafic de FA_1 est passé de zéro paquet à 100 paquet/s. Ce qui démontre que le nœud mobile est dans le site 2, et qu'il est connecté à FA_1

Pour le même intervalle le graphe de la figure 5.13 montre que la connexion VPN_10 demeure utilisée pour l'envoi des données vers MN au serveur de l'application voix.

En effet HA et FA_1 ont utilisé le même routeur CE_1 pour sélectionner un PE le proche de leurs localité, selon l'algorithme proposé de Handoff VPN. À son tour CE_1 a choisi PE_1 pour l'acheminement de ses données. Étant donné que celui-ci supporte VRF_10, le VPN_10 a été utilisé pour se connecter au serveur de l'application voix.

Pour l'intervalle [1h40mn, 2h12mn] le trafic de FA_1 passe à zéro et celui de FA_2 passe à 100 paquets/s. Ceci montre que MN s'est connecté au routeur FA_2 (couleur turquoise). D'après le graphe en rouge, une connexion VPN_20, pour l'acheminent des données de MN à CN a été utilisée. Dans ce cas-ci, le MN a utilisé CE_2 pour transmettre ses données, car il est le proche de sa localisation. CE_2 à son tour a sélectionné le PE le proche de lui, qui est PE_2. Étant donné que celui-ci supporte le VRF_20, VPN_20 est utilisé pour la transmission des données de MN.

Pour l'intervalle [2h12mn, 2h34mn] le trafic de FA_3 passe de 0 à 100 paquets/s. La connexion de VPN_20 est utilisée dans cet intervalle. Ceci dit que le PE_2 est choisi, car il est le plus proche de FA_3. Étant donné que celui-ci supporte le VRF_20, le VPN_20 est utilisé pour acheminer les données.

À partir d'un temps égal à 2h34mn la charge de connexion de VPN_30 augmente de 0 à 200 paquets/s, ce qui prouve qu'un nouveau chemin optimal a été sélectionné pour l'acheminement des données de MN. En effet pour cet instant le FA_3 choisit d'acheminer le trafic par CE_3, qui à son tour a sélectionné le PE_3, qui est plus proche de lui. Étant donné que PE_3 supporte le VRF_3, le VPN_3 est utilisé pour l'acheminement les données de FA_3.

5.4.1.2 Résultats et analyses de l'effet des paramètres WLAN

Dans cette partie, quatre scénarios ont été modélisés afin d'illustrer les étapes intermédiaires qui ont permis à la configuration des paramètres WLAN sur le modèle proposé. Ceci a contribué à l'étudier de l'impact des paramètres WLAN sur les performances du modèle SHVM. Cette étude consiste à varier les valeurs de la vitesse du nœud, le data rate et la puissance. Un assignement dynamique du canal a été aussi attribué à tous les nœuds du réseau. Dans cette partie l'étude va se limiter seulement à déterminer le taux de perte de paquets, étant donné que la variation de ces derniers agit seulement sur ce paramètre.

a) Résultat et analyse scénario 1 : effet d'attribution dynamique du canal

Ce scénario consiste à étudier l'effet de l'assignement dynamique du canal sur le modèle proposé. Pour cela le modèle de référence a été repris et une nouvelle configuration concernant l'attribution dynamique du canal a été effectuée sur tous les nœuds du réseau. Le taux de perte de paquet a été déterminé et comparé aux résultats obtenus par le modèle de référence.

Résultats de pertes de paquets

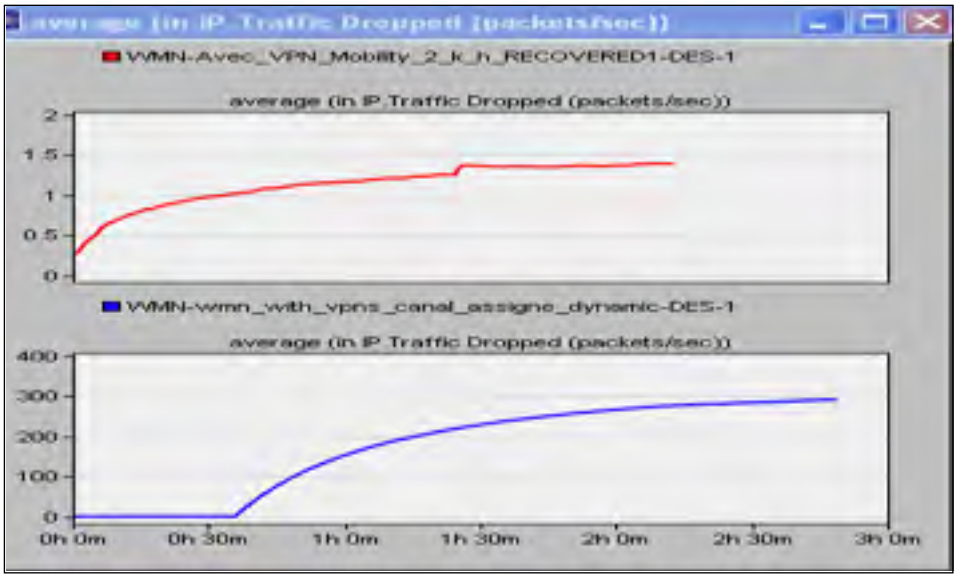

Figure 5.14 Taux de perte de paquets pour un assignement du canal

Le graphe en bleu de la figure 5.14 représente la perte de paquets lorsque le canal est attribué d'une façon dynamique dans le réseau. On constate que le taux de perte paquets est très élevé, il atteint 300 paquets par seconde.

Le graphe rouge représente le taux de perte de paquets pour assignement non dynamique des canaux dans le réseau. La configuration de l'assignement du canal est représentée dans le tableau 5.4.

Dans l'assignement dynamique du canal pour les stations locales mobiles, chaque nœud a la possibilité de trouver le meilleur canal pour transmettre des données. L'utilisation de cette méthode a engendré de l'interférence entre le client mobile et les autres stations locales, lors de son déplacement d'un site à un autre. Dans un tel cas, deux nœuds peuvent opérer sur le même canal. Ce qui peut causer des interférences.

Dans la norme 802.11/ g, un transmetteur opérant sur une fréquence 2,4 GHz a 3 canaux sans chevauchement (canal1, canal 6 et canal 11). De ce fait, pour éviter l'interférence des canaux, on a équipé chaque ensemble de quatre nœuds mobiles, de même BSS, avec l'un des trois canaux.

Les résultats obtenus ont enregistré une nette amélioration comme le montre le graphe rouge de la figure 5.13 où une diminution importante de perte de paquets sur le réseau global a été observée.

b) Résultats et Analyse du Scénario 2 : effet de la puissance

Dans cette partie le scénario de référence a été repris et une augmentation de la puissance sur les interfaces supportant la mobilité IP a été effectuée. Le paramètre de taux de perte de paquet a été déterminé. Celui-ci a permis déterminer les performances du modèle en termes de qualité de service. Le tableau 5.5 illustre différentes valeurs attribuées aux interfaces des nœuds supportant la mobilité IP.

Tableau 5.5 Variation de la puissance

Nœud	**Puissance de transmission (W)**			
	Valeurs initiales	**Augment 1**	**Augment 2**	**Augment 3**
HA	0.02	0.06	0.1	0.2
FA_1	0.009	0.06	0.1	0.2
FA_2	0.009	0.06	0.1	0.2
FA_3	0.05	0.06	0.1	0.2
Nœud mobile	0.1	0.1	0.1	0.1

Résultat de perte de paquet

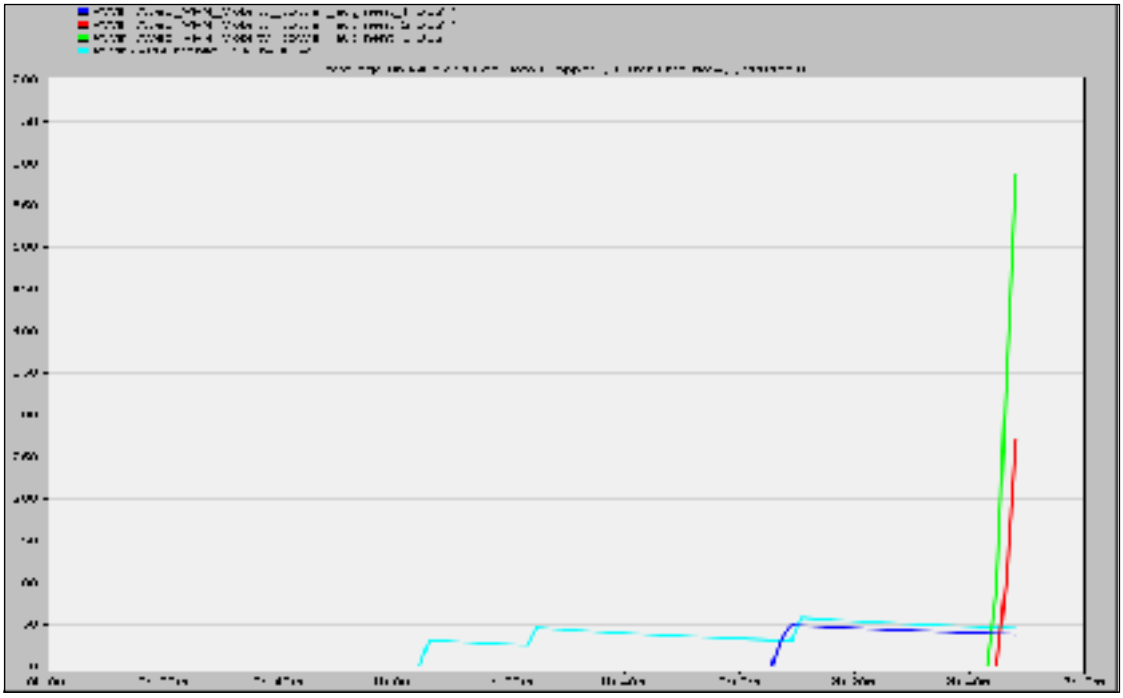

Figure 5.15 Taux de perte de paquet pour la variation de la puissance

Le graphe de la figure 5.15 montre que dans le cas de l'augmentation de la puissance, le taux de perte de paquets diminue pour la première augmentation, mais à partir d'une certaine valeur qui correspond augment_2 (tableau 5.5), le ratio de paquets perdus augmente et demeure stable pour les autre valeurs de la puissance. Le graphe de la figure 5.16 illustre la variation de la valeur de la puissance avec la variation du ratio de pertes de paquets.

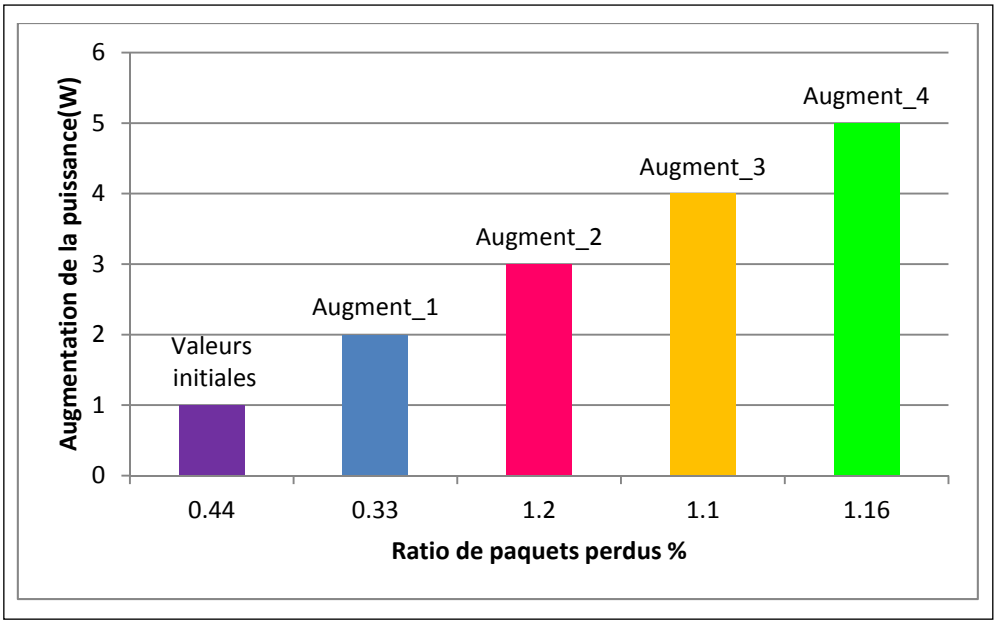

Figure 5.16 Ratio de perte de paquets pour différentes valeurs de la puissance

En effet, l'augmentation de la puissance, peut améliorer les performances du réseau en diminuant le taux de perte de paquet, ce qui contribue à assurer un seamless handoff. Cependant, Cela peut avoir d'autres effets négatifs, comme une grande consommation d'énergie, et la création de l'interférence dans le réseau. Pour bien gérer l'utilisation de la puissance, un ajustement de la puissance a été effectué sur chaque nœud de telle manière à ce qu'il n'interfère pas avec les nœuds voisins. Cela a été réalisé en attribuant aux nœuds du réseau des valeurs de puissances différentes, selon leurs besoins nécessaires en termes de consommation d'énergie. Notons que la consommation d'énergie varie avec la nature du nœud maillé. Ainsi les routeurs maillés et APs ont une mobilité minimale et leurs contraintes en consommation d'énergie sont réduites par rapport aux nœuds mobiles.

c) Résultats et Analyse du scénario 3 : effet de la vitesse

Dans cette partie, l'étude consiste à déterminer le taux de perte de paquets, ainsi que la charge de VPN, étant donné que l'augmentation de la vitesse agit sur ces paramètres. Pour cela, une augmentation de la vitesse a été effectuée sur la trajectoire du nœud mobile MN, afin de permettre d'évaluer les limites du modèle SHVM en termes de performances QoS.

1) Résultat de perte de paquets

Figure 5.17 Taux de perte de paquet avec variation de la vitesse Vs le temps

La figure 5.17 représente les graphes de Paquets perdus pour différentes valeurs de la vitesse. Les résultats obtenus montrent que la perte des paquets augmente au fur à mesure que la vitesse augmente. Celle-ci atteint son seuil pour une valeur de la vitesse égale à 30k/h. Le graphe de la figure 5.18 illustre cette valeur seuil qui correspond un ratio de pertes da paquets de 5.6% qui une valeur supérieure à la norme requise pour les applications à temps réel (tableau 5 .1).

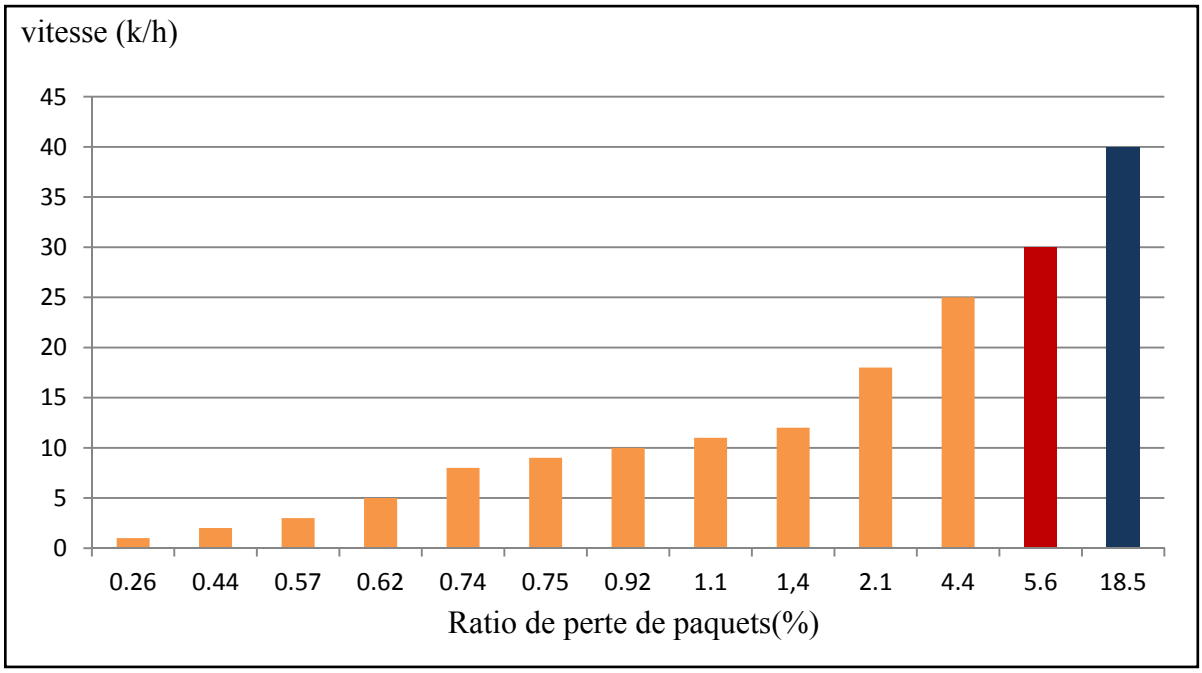

Figure 5.18 Ratio de perte de paquets pour différents vitesses

En effet, la mobilité à grande vitesse cause une rupture des chemins de routage(Chen et al.), par conséquent, on obtient des informations de localisation imprécise correspondant aux nœuds voisins et ceux de destination, ce qui engendre une perte de paquets. Les problèmes de perte de connexion et les problèmes de perte de paquets causés par une vitesse élevée réduisent le débit du réseau. Dans notre modèle la valeur de 2 k/h de la vitesse moyenne a été utilisée pour la trajectoire du client mobile, celle-ci s'est avéré adéquate pour les performances du réseau en tenant compte des résultats obtenus dans la section 5.4.1.1.

2) Résultats de la Charge VPN

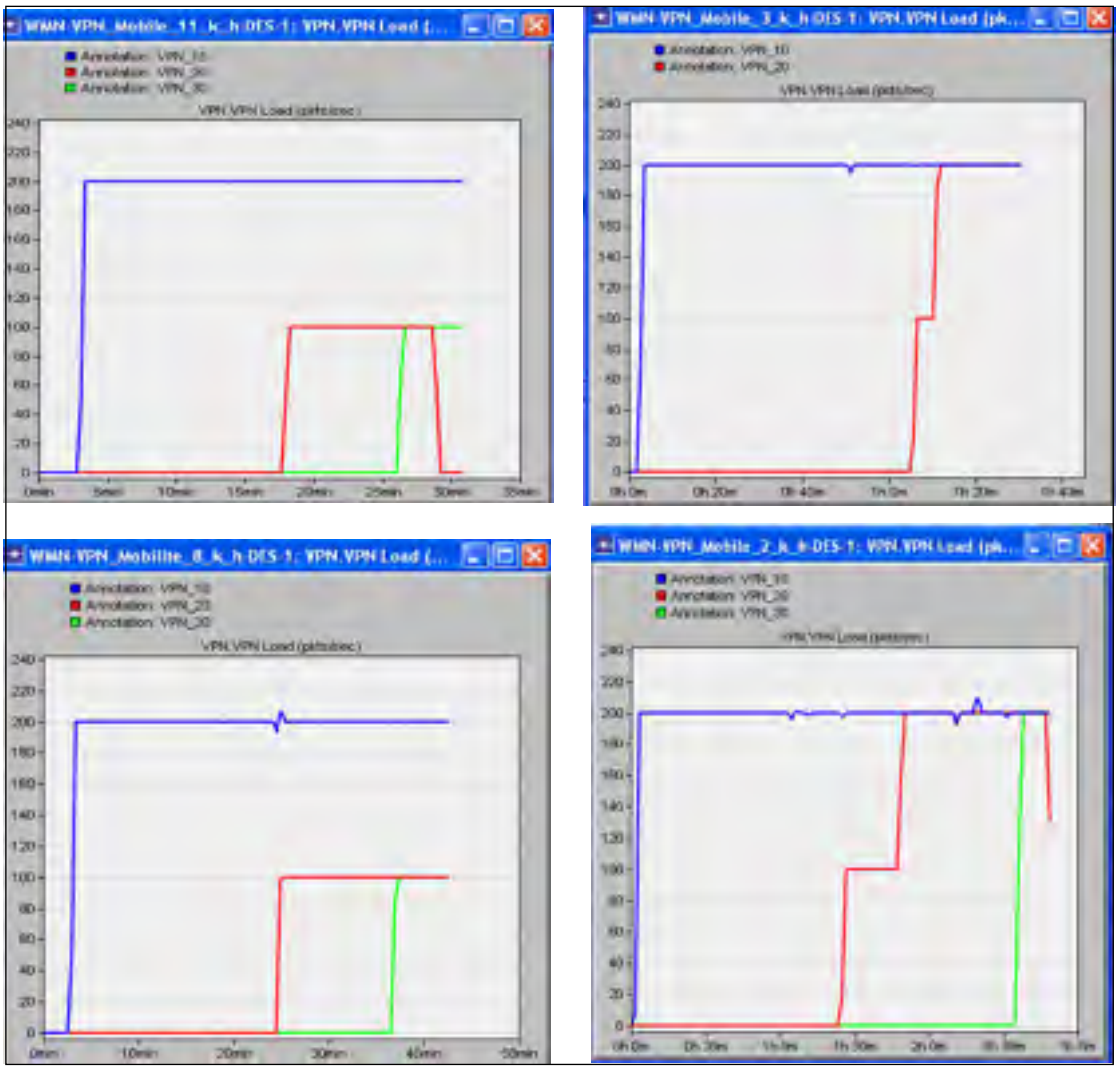

Figure 5.19 Charges de connexion VPN avec variation de la vitesse Vs le temps

Les graphes de la figure 5.19 montrent, les différentes charges de connexions VPN que MN a établi, en fonction de vitesse de son déplacement. Ces graphes montrent que MN établit une nouvelle connexion VPN avant qu'il soit déconnecté de son ancien VPN. Ceci répond à notre objectif, celui d'offrir une connexion VPN continue. Rappelons que ceci est possible grâce à l'utilisation de la conception de CE basé sur les VRFs qui consiste à configurer les CE_i sur plusieurs VPN et de les répartir d'une façon à assurer la continuité de la connexion réseau.

Nous remarquons aussi que la charge de VPN_20 et VPN_30 changent avec la variation de la vitesse. Pour de petites vitesses, la charge de VPN est de l'ordre de 200 paquets/ seconde pour les trois VPN. En effet le fait que le CN ne soit pas mobile, ceci va lui permettre d'utiliser le même PE qui lui est connecté, ceci dit qu'il va supporter le VPN_10 pour l'envoi et la réception de ses données. Donc la charge pour VPN serait 200 paquets /seconde durant toute la simulation.

Par contre, les charges de VPN_20 et VPN_30 dépendent de la vitesse avec laquelle se déplace MN. En effet, pour les grandes vitesses, la charge de VPN_20 et VPN_30 est de l'ordre de 100 paquets/s. Ceci est dû au fait que seule, la transmission des données est effectuée via les VPN_20 et VPN_30 pour MN. En ce qui concerne la réception des donnés, celles-ci sont acheminées par la connexion VPN_10 établie entre HA et CN. Rappelons que la mobilité à grande vitesse cause une interruption de chemins de routage (Chen et al.), ce qui engendre les problèmes de perte de connexion. De ce fait, les PEs ne seront pas en mesure de déterminer la position de MN, car ils ignorent sa nouvelle adresse, mais puisqu'ils connaissent son adresse du réseau d'accueil, ils vont l'utiliser pour envoyer les données à MN via VPN_10. HA intercepte ces données, les encapsule, et les envoie à FA via un tunnel préétabli. FA à son tour, les envoie à MN après décapsulation.

d) Résultats et Analyses du Scénario 4 : effet de data rate

Dans cette partie, le scénario de référence est repris avec des valeurs différentes de débit du transfert. En effet une augmentation des valeurs de débit de transfert des données est attribuée aux routeurs HA, FA_1, FA_2, FA_3 et au nœud mobile sur les interfaces supportant la mobilité IP. Cette augmentation vise à déterminer le taux de perte de paquets dans le but d'évaluer les limites du modèle en termes de performances QoS.

Tableau 5.6 Variation du débit de transfert (*Data Rate*)

Nœud	**taux initial (Mbps)**	**Variation du Taux des données (Mbps)**		
HA	1	6	18	24
FA_1	1	6	18	24
FA_2	1	6	18	24
FA_3	1	6	18	24
Nœud mobile	1	6	18	24

Résultats de perte de paquets

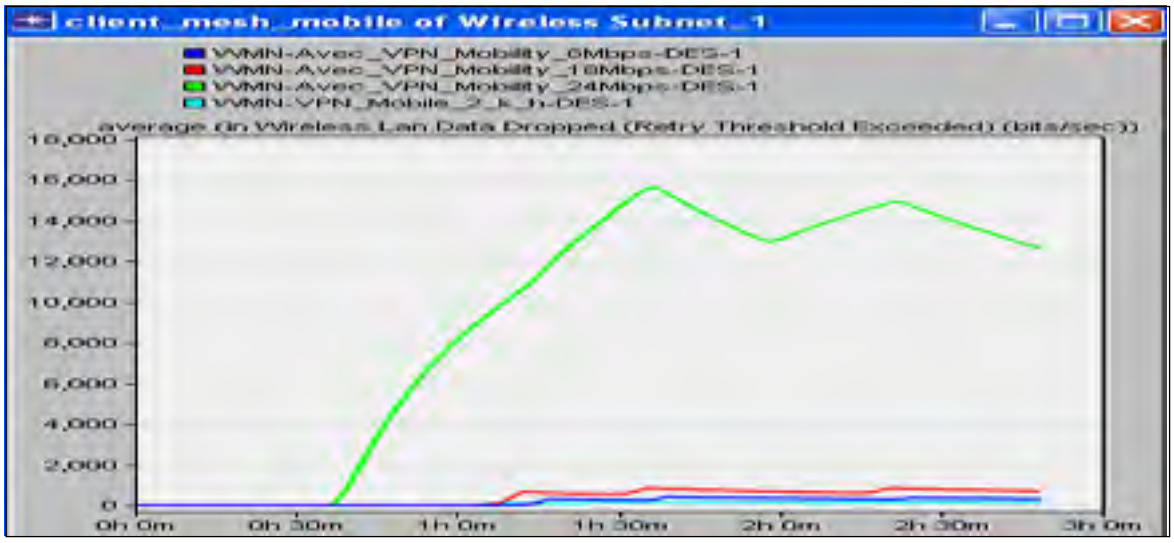

Figure 5.20 Perte de paquets pour différentes valeurs de Data rate

Les résultats obtenus, des graphes de la figure 5.20, montrent que le lien de capacité égale à 24 Mbps a enregistré la plus grande valeur de taux de paquets perdus, et le lien de 1 Mbps a enregistré la plus petite valeur. En effet, sur le graphe de la figure 5.21 on constate que pour un lien 24 Mbps le ratio de perte de paquet atteint 12% qui est une valeur intolérable par la norme exigé pour les applications à temps réel (tableau 5.1).

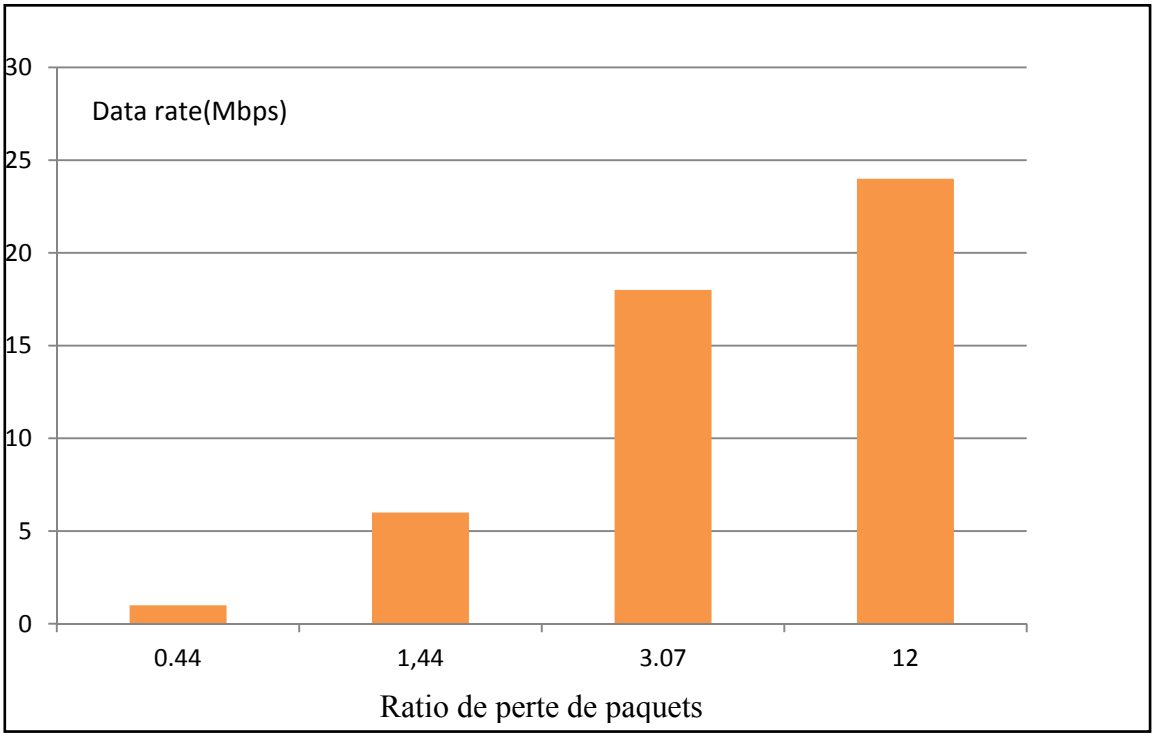

Figure 5.21 Ratio de perte de paquets pour différentes valeurs de data rate

Dans la technologie 802.11g, qui constitue notre modèle, la portée diminue avec l'augmentation de taux de transfert, ce qui rend la transmission et la communication moins performantes quand le nœud mobile se déplace en s'éloignant de la portée.

D'après (Yip, Tan et Chuah, 2011) la capacité des liens à haut débit est fortement dégradée par les liens de taux plus faibles quand les liens sont en compétition d'un même canal. D'après ces auteurs, ceci est peut être attribué au mécanisme de (CSMA / CA) spécifié dans les normes 802.11. En effet le (CSMA / CA) assure l'accès au média pour tous les nœuds du réseau à long terme. Par conséquent, un lien de faible taux peut occuper le canal plus longtemps qu'un lien de haut débit, ce qui engendre une répartition inéquitable du temps total de transmission des nœuds en compétition et dégrade le débit global du réseau. Par conséquent, il faut minimiser la charge du réseau et utiliser un seul débit. Ceci a été réalisé dans notre modèle en configurant tous les routeurs HA et FA à 1 Mbps, et les nœuds mobiles qui peuvent rentrer en compétition du canal à 5.5 Mbps.

5.5 Conclusion

Ce chapitre a permis de mettre en évidence notre étude qui concerne le seamless handoff pour VPN sur les réseaux Maillés sans fil (SHVM).

En effet les résultats obtenus montrent que le délai de handoff a enregistré une valeur minimale, ce qui répond à la norme exigée pour assurer un seamless handoff pour une application à temps réel. Ceci est le résultat de l'application de la conception du multi-chemin. Rappelons que celui-ci avait pour objectif de trouver le meilleur chemin pour se connecter rapidement à un PE. Par conséquent, ceci a permis à MN d'établir rapidement une connexion VPN avec CN. Ce qui a contribué à réduire le délai de handoff de la couche réseau et a permis d'éviter de perdre un grand taux de paquets lors de handoff.

La deuxième conception de CE basé sur les VRFs a aidé le nœud mobile de garder sa connexion VPN lors de handoff. En effet les routeurs CEs supportant plusieurs VPNs offrent à MN la possibilité de garder sa connexion VPN lors de son déplacement d'un site à autre. En gardant sa connexion VPN avec le CN, le MN n'a pas eu besoin de se ré-authentifier pour un autre accès VPN, ce qui a contribué de diminuer le délai d'authentification, par conséquent le délai de la couche de liaison. Le placement adéquat de CEs sur l'aire du réseau a facilité à MN de trouver et de s'associer au bon AP rapidement lors de son déplacement. Cette approche a permis de réaliser un bon délai handoff de couche de liaison et à diminuer le taux de pertes de paquets.

La dernière conception utilisée, est celle liée à l'utilisation de VPN, celle-ci a collaboré à réduire le délai d'attribution d'adresse IP, par conséquent le délai de handoff de la couche réseau.

Le délai de bout en bout et la gigue ont été aussi déterminés, ces derniers ont enregistré des valeurs très inférieures aux normes requises pour assurer les performances du réseau pour une application voix, et ce malgré l'utilisation de la mobilité IP lors de la transmission des

données. En effet, l'un des inconvénients de la mobilité IPv4 est le routage triangulaire qui engendre un délai dans l'acheminement des données, mais l'application de l'approche de chemin optimal a permis de diminuer le délai de bout en bout et celui de la gigue.

Les résultats des scénarios de l'influence des paramètres WLAN, ont permis de mettre en évidence le choix des paramètres utilisés dans le scénario de référence pour réduire l'impact des perturbations sur le modèle. En effet la répartition des canaux a aidé à minimiser les interférences et de maximiser la capacité du réseau en réduisant le nombre des paquets perdus.

Les simulations de la variation du débit de transfert (data rate) effectuée sur le modèle ont entrainé une augmentation de pertes de données avec l'augmentation du débit. Ceci est dû à l'utilisation du mécanisme (CSMA / CA) spécifié dans les normes 802.11, qui a engendré une répartition inéquitable du temps total de transmission des nœuds en compétition dans le réseau. Par conséquent, il faut minimiser la charge du réseau et utiliser un seul débit. Ceci a été réalisé dans notre modèle en configurant tous les routeurs HA et FA à 1 Mbps, et les nœuds mobiles qui peuvent rentrer en compétition du canal à 5.5 Mbps.

La perte de paquets a été constatée dans le cas de l'augmentation de la vitesse. En effet, quand celle-ci est si élevée elle cause une rupture de lien, ce qui fait diminuer le débit du réseau. La valeur de 0.5 m/s de la vitesse moyenne utilisée dans notre modèle, pour la trajectoire du client mobile s'est avérée adéquate pour les performances du réseau.

D'autre part dans le cas de l'augmentation de la puissance, une amélioration des performances a été constatée, bien que cela puisse avoir d'autres effets négatifs si la puissance dépasse une certaine limite de capacité. Cet état de figure peut causer une grande consommation d'énergie, comme il peut créer des interférences dans le réseau. Une solution possible est d'ajuster la puissance de chaque nœud de manière à ce qu'il n'interfère pas avec les nœuds voisins. Cela a été réalisé sur notre modèle en attribuant aux routeurs d'agent

d'accueil, d'agents visités et le nœud mobile des puissances différentes, et cela selon leurs besoins nécessaires en termes de consommation d'énergie.

Finalement, le modèle proposé répond aux critères exigés, en termes de délai, de pertes de paquets, et de la gigue pour améliorer les performances des réseaux sans fil. SHVM non seulement a assuré un handoff VPN pour WMN, mais aussi a contribué à résoudre le problème de routage triangulaire engendré par l'utilisation du tunnel IPv4, celui-ci peut être assimilé à une connexion VPN entre les FAs et HA, qui contribue à l'acheminement des données d'une façon sécuritaire.

les paramètres réseau utilisés pour configurer le réseau ont permis une bonne exploitation de la technologie MPLS-VPN sur le réseau WMN, celle-ci a amélioré les performances du réseau WMN et ce malgré l'introduction de la mobilité qui est une contrainte de performance dans les réseaux maillés en particulier et dans les réseaux sans fil en général. Ceci prouve qu'avec une bonne optimisation des paramètres réseau conduit à une exploitation efficace des capacités de celui-ci

En conclusion, les résultats obtenus des simulations effectuées sur le simulateur OPNET ont montré l'efficacité de l'algorithme pour l'amélioration de la performance de la QoS dans les réseaux WMNs. Notons que ces résultats concordent avec les objectifs tracés au début de l'étude, à savoir réduire le délai de handoff, ainsi que de minimiser le taux de perte de paquets, dans le but d'assurer un seamless handoff.

CONCLUSION

Le réseau maillé sans fil est une technologie attrayante en raison de ses nombreux avantages. Cependant celle-ci présente des contraintes liées à la sécurité. Les VPNs sont parmi les mécanismes employés pour répondre aux exigences de WMNs en termes de sécurité. Le VPN est une technologie très fiable et sécuritaire. Son utilisation avec d'autres technologies comme le MPLS apporte de la sécurité et de la performance aux réseaux.

Dans ce mémoire, la technologie MPLS VPN a été choisie pour être implémentée sur le réseau maillé sans fil. Dans cette étude le modèle proposé, SHVM est supposé sécurisé. À cet effet, notre intérêt s'est focalisé sur l'étude de handoff VPN sur les réseaux maillés sans fil lors de la mobilité du nœud inter domaine. Cette étude a pour objectif de réduire le délai de handoff et minimiser le taux de perte de paquets dans le but d'assurer un handoff rapide et transparent. Pour cela un algorithme a été proposé. Cet algorithme est basé sur trois conceptions. La première conception consiste à utiliser le principe de multi chemins pour optimiser le chemin du nœud mobile. La deuxième conception consiste à placer et à configurer les CEs d'une façon à permettre au nœud de garder la connexion VPN lors de son déplacement d'un site VPN à autre. La troisième est une application de caractéristique de VPN qui permet de diminuer le délai d'attribution d'adresse. Pour valider notre approche celle-ci a été modélisée et simulée sur le simulateur OPNET 16 avec une application voix.

Les résultats obtenus, de pertes de paquet et de délai de handoff ont répondu aux normes requises pour réaliser un handoff pour les applications à temps réel. En effet l'application de la conception du chemin optimal a contribué à réduire le délai de handoff de la couche réseau et a permis d'éviter de perdre un grand taux de paquets lors de handoff.

La deuxième conception de CE basé sur les VRFs, donne au nœud mobile la possibilité de garder sa connexion VPN lors de handoff, ceci a permis de diminuer le délai d'authentification, par conséquent le délai de la couche de liaison. Le placement adéquat de

CEs sur l'aire du réseau a réalisé petit délai de handoff de couche de liaison et a diminué le taux de pertes de paquets.

La dernière conception est celle liée à l'utilisation de VPN, celle-ci a contribué pour la réduction du délai d'attribution d'adresse IP. Par conséquent la réduction de délai de handoff de la couche réseau.

Le délai de bout en bout et la gigue ont été aussi déterminés, ces derniers ont enregistré des valeurs très inférieures aux normes requises pour assurer les performances du réseau pour une application voix, malgré l'utilisation de la mobilité IP lors de la transmission des données. Tout au contraire, notre approche a contribué à tirer profit de l'utilisation de la mobilité IP indirecte. En effet, en utilisant la mobilité IPv4, un tunnel est établi entre HA et FA pour l'acheminement des données de HA à MN, ce qui pouvait engendrer un délai transmission des données et surcharge dans le réseau, à cause de l'encapsulation et décapsulation des données transmis et à l'augmentation de la distance entre HA et MN. Toutefois, avec l'application de notre approche, ces contraintes ont été évitées, ce qui a permis l'utilisation du tunnel pour l'acheminement de données d'une façon sécuritaire entre HA et FA et sans l'ajout de délai de bout au bout.

L'étude de l'influence de la vitesse, la puissance, le data rate et la répartition des canaux sur l'approche SHVM ont été aussi étudiés, les résultats montrent que la vitesse élevée engendre une perte de paquet. En effet quand la vitesse est si élevée elle cause une rupture de connexion, ce qui engendre une perte de paquets dans le réseau.

Les simulations de la variation du débit de transfert (data rate) effectuées sur le modèle proposé ont entrainé une augmentation de pertes de données avec l'augmentation du débit. Ceci est dû à l'utilisation du mécanisme (CSMA / CA) spécifié dans les normes 802.11.Par conséquent, la charge du réseau doit être minimisé et un seul débit doit être utilisé dans le réseau. Ceci a été réalisé sur modèle SHVM en configurant tous les routeurs HA et FA à 1 Mbps, et les nœuds mobiles qui peuvent rentrer en compétition du canal à 5.5 Mbps.

D’autre part dans le cas de l’augmentation de la puissance, une amélioration de performance a été enregistrée pour notre modèle, mais à certaines valeurs de la puissance, des effets négatifs sur le paramètre de perte paquets. En effet l’augmentation de la puissance peut causer une grande consommation d’énergie, comme elle peut créer des interférences dans le réseau. Pour pallier à ce problème, la puissance de chaque nœud doit être ajustée de manière à ce qu'il n'interfère pas avec les nœuds voisins. Cela a été réalisé sur notre modèle SHVM en attribuant aux routeurs d’agent d’accueil, d’agents visités et le nœud mobile des puissances différentes, selon leurs besoins nécessaires en termes de consommation d’énergie.

En conclusion, les résultats obtenus des simulations effectuées sur OPNET ont montré l’efficacité de l’algorithme pour l’amélioration de la performance de la QoS dans les réseaux WMNs. Notons que ces résultats concordent avec les objectifs tracés au début de l’étude, à savoir réduire le délai de handoff, ainsi que de minimiser le taux de perte de paquets, dans le but d’assurer un seamless handoff.

RECOMMANDATIONS

Parmi les solutions proposées pour sécuriser les réseaux maillés sans fil nous citons la technique de tunneling IPSec dans MPLS-VPN proposée par (Muogilim, Loo et Comley, 2011) pour fournir une haute sécurité dans les réseaux maillés sans fil, mais les résultats obtenus montrent que VPN-IPsec introduit un coût de signalisation de routage dans le processus de sécurisation des données, car celui-ci utilise considérablement les ressources du réseau en transmettant moins de charges. Ceci peut affecter les performances des réseaux WMN dont les ressources de CPU posent des contraintes de sécurité (Siddiqui et Hong). En outre les auteurs (Yin, Zhang et Li, 2009) trouvent que le protocole IPSec est difficile à déployer et moins sécurisant sur les réseaux mobiles, ces derniers proposent d'utiliser SSL comme solution alternative, en raison de son faible cout et sa configuration facile. À cet effet, une étude de l'utilisation conjointe de SSL et les VPN pour sécuriser les réseaux maillés sans fil est suggérée.

.

Lors de déploiement des VPNs sur les réseaux maillés sans fil, le protocole IP dynamique a été utilisé à cause que les VPNs ne supportent pas les protocoles Manet. Toutefois, le protocole dynamique Manet AODV pour VPN sans fil a été abordé par(Natarajan, Muthiah et Nachiappan, 2010), ces derniers l'ont suggéré pour préserver de la bande passante dans le réseau. Par conséquent, le protocole dynamique Manet AODV peut être proposé comme protocole de routage des VPNs sur WMN, pour réduire le délai de la couche de liaison d'un nœud mobile.

Bien que les résultats de la gigue et de délai de bout en bout du modèle SHVM, fussent satisfaisants, d'autres applications de mobilité IP peuvent être suggérées, afin de permettre au nœud mobile d'avoir un lien direct avec CN. Ces solutions sont basées sur le protocole de mobilité IPv6 et le protocole NEMO. Elles permettent d'avoir de la connexion transparente à l'hôte mobile et au site mobile qui se déplacent d'un site VPN vers un autre site VPN (Byun et Lee, 2008). L'application de ces protocoles sur SHVM peut être recommandée, pour éliminer les effets négatifs du routage triangulaire.

LISTE DE RÉFÉRENCES BIBLIOGRAPHIQUES

A. Jaha, Fathi Ben Shawna et Majdi Ashibani. 2008. « Proper Virtual Private Network (VPN) Solution ».

ang, Namhi K, Luigi L o Iacono, Christoph R uland et Younghan Kim. 2006. « Efficient Application of IPsec VPNs in Wireless Networks ».

Belghoul, Farouk. 2005. « Mécanismes de Gestion de Mobilité Généralisée dans un Système Hétérogène Fixe/Mobile ». Télécom ParisTech.

Bontozoglou, A., Yang Kun, K. Guild et M. P. Farrera. 2012. « An experimental framework for vertical hand-over to guarantee session continuity in heterogeneous wireless environments ». In *Globecom Workshops (GC Wkshps), 2012 IEEE*. (3-7 Dec. 2012), p. 1004-1009.

Byun, Haesun, et Meejeong Lee. 2008. « Network Architecture and Protocols for BGP/MPLS Based Mobile VPN ». In *Information Networking. Towards Ubiquitous Networking and Services*. p. 244-254. Springer.

Chen-Han, Lin, Yang Jen-Shun et Wu Ko-Ching. 2005. « Mobile intelligent agent technologies to support VoIP seamless mobility ». In *Advanced Information Networking and Applications, 2005. AINA 2005. 19th International Conference on*. (28-30 March 2005) Vol. 2, p. 177-180 vol.2.

Chen, Yuh Shyan, Ching Hsueh Cheng, Chih Shun Hsu et Ge Ming Chiu. 2009. « Network Mobility Protocol for Vehicular Ad Hoc Networks ». In *Wireless Communications and Networking Conference, 2009 WCNC 2009 IEEE*. (5-8 April 2009), p. 1-6.

Davie, Bruce S., et Adrian Farrel. 2008 *Virtual Private Networks MPLS: Next Steps* Morgan Kaufmann.

Davies, Joseph, et Elliot Lewis. 2004. *Deploying Virtual Private Networks with Microsoft Windows Server 2003.*

Davy, Stéphane. 2010. « Performance des réseaux maillés multiradio sur banc de test ». Thèse (M Ing). Montréal, École de technologie supérieure.

Deal, Richard. 2008. *The Complete Cisco VPN Configuration Guide*. Coll. « Cisco Press. © 2006. Books24x7 ».

Dhaini, Ahmad R, Pin Han Ho et Xiaohong Jiang. 2010. « WiMAX-VPON: A Framework of Layer-2 VPNs for Next-Generation Access Networks ».

Dhaini, A R, Ho Pin-Han et Jiang Xiaohong. 2010. « Performance Analysis of QoS-Aware Layer-2 VPNs over Fiber-Wireless (FiWi) Networks ». In *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*. (6-10 Dec 2010), p. 1-6.

Dingguo, Yu, Chen Nan et Tan Chengxiang. 2009. « Design and Implementation of Mobile Security Access System (MSAS) Based on SSL VPN ». In *Education Technology and Computer Science, 2009. ETCS '09. First International Workshop on*. (7-8 March 2009) Vol. 3, p. 152-155.

(D. Johnson, 2004), J. Arkko. 2004. Mobility Support in IPv6 . www.ietf.org/rfc/rfc3775.txt . Consulté le 15 Juillet 2013.

Eronen, P. 2006. IKEv2 Mobility and Multihoming Protocol (MOBIKE) . www.ietf.org/rfc/rfc4555.txt . Consulté le 01 Aout 2013.

Evers, F., et J. Seitz. 2006. « A VPN-driven Infrastructure for Vertical Handovers ». In *Sarnoff Symposium, 2006 IEEE*. (27-28 March 2006), p. 1-4.

Ghein, Luc De. *MPLS VPN MPLS Fundamentals: A Comprehensive Introduction to MPLS Theory and Practice*.

Gupta, Meeta. 2003. *Introduction to VPNs Building a Virtual Private Network*

Heusse, Martin. 2009. « Vers une utilisation efficace du canal radio ». Université Joseph Fourier.

Hossain, Ekram, et Kin Leung. 2008. *Wireless Mesh Networks Architectures and Protocols*.

Hu, Lili, Zhizhong Ding et Huijing Shi. 2012. « An Improved GPSR Routing Strategy in VANET ». *2012 International Conference on Wireless Communications, Networking and Mobile Computing (Wicom)*.

Hui, Wang, Huang Quan, Xia Yong, Wu Yichuan et Yuan Yingang. 2007. « A Network-Based Local Mobility Management Scheme for Wireless Mesh Networks ». In *Wireless Communications and Networking Conference, 2007.WCNC 2007. IEEE*. (11-15 March 2007), p. 3792-3797.

Hui, Zhang, Qin Yajuan, Zhang Hongke et Guan Jianfeng. 2006. « Study on host and station mobility in BGP/MPLS VPN ». In *Wireless, Mobile and Multimedia Networks, 2006 IET International Conference on*. (6-9 Nov. 2006), p. 1-3.

Jaha, A. A., F. Ben Shatwan et M. Ashibani. 2008. « Proper Virtual Private Network (VPN) Solution ». *Ngmast 2008: Second International Conference on Next Generation Mobile Applications, Services, and Technologies, Proceedings*, p. 309-314.

Kadlec, J., R. Kuchta et R. Vrba. 2009. « Performance Tests of the Dynamics of the Wireless Networks ». In *Networks, 2009. ICN '09. Eighth International Conference on*. (1-6 March 2009), p. 112-115.

Kosta, Y.P, Upena D Dalal et Rakesh Kumar Jha. 2010 «Security Comparison of Wired and Wireless Network with Firewall and Virtual Private Network (VPN) ».

Leung, Kin K. Hossain Ekram. 2007. « Wireless mesh networks architectures, protocols, services and applications ». < http://dx.doi.org/10.1007/978-0-387-68839-8 >.

Lijun, Dong, Kang Xiaojun et Song Jun. 2010. « A WTLS-based virtual private network for wireless intrusion prevention ». In *Computer Application and System Modeling (ICCASM), 2010 International Conference on*. (22-24 Oct. 2010) Vol. 3, p. V3-467-V3-471.

Lin, Chen-Han, Jen-Shun Yang et Ko-Ching Wu. 2005. « Mobile intelligent agent technologies to support VoIP seamless mobility ». In *Advanced Information Networking and Applications, 2005. AINA 2005. 19th International Conference on*. Vol. 2, p. 177-180. IEEE.

Liu, Zong-Hua, Jyh-Cheng Chen et Tuan-Che Chen. 2009. « Design and Analysis of SIP-Based Mobile VPN for Real-Time Applications ».

Misra, Sudip, et Isaac Subhas Chandra Misra. 2009. « Guide to Wireless Mesh Networks ».

Munasinghe, K. S., et S. A. Shahrestani. 2004. « Evaluation of an IPSec VPN over a Wireless Infrastructure ».

Munasinghe, Kumudu S., et Seyed A. Shahrestani. 2005. « Wireless VPNs: An Evaluation of QoS Metrics and Measures ».

Muogilim, Okechukwu E., Kok-Keong Loo et Richard Comley. 2011. « Wireless mesh network security: A traffic engineering management approach ». *Journal of Network and Computer Applications,* vol. 34, n^{o} 2, p. 478-491.

Namhi, Kang, L L Iacono, C Rulan et Kim Younghan. 2006. « Efficient application of IPsec VPNs in wireless networks ». In *Wireless Pervasive Computing, 2006 1st International Symposium on*. (16-18 Jan 2006), p. 5 pp.

Natarajan, Mahalakshmi Chidambara, Ramaswamy Muthiah et Alamelu Nachiappan. 2010. « Performance investigation of virtual private networks with different bandwidth allocations ». *IJCSI International Journal of Computer Science Issues*.

Oya, T., H. Kamiyama, J. Miyoshi, Y. Kitamikado et Y. Ichikawa. 2010. « Evaluation of the route optimization architecture for MOBIKE-based mobile communication systems ».In *Network Operations and Management Symposium Workshops (NOMS Wksps), 2010 IEEE/IFIP*. (19-23 April 2010), p. 55-58.

Park, Shihyon, Bradley Matthews, Danny D'Amours et Jr. William J. McIver. 2010. « Characterizing the Impacts of VPN Security Models on Streaming Video ».

Perkins. 2002. « IP Mobility Support for IPv4 ». In *IP Mobility Support for IPv4*. www.ietf.org/rfc/rfc3344.txt Consulté le 28 Juillet 2013.

Pujolle, Guy. 2007. *Management, Control and Evolution of IP Networks*

Rongsheng, Huang, Zhang Chi et Fang Yuguang. 2007. « A Mobility Management Scheme for Wireless Mesh Networks ». In *Global Telecommunications Conference, 2007. GLOBECOM '07. IEEE*. (26-30 Nov. 2007), p. 5092-5096.

Shihyon, Park, B Matthews, D D'Amours et W. J McIver. 2010. « Characterizing the Impacts of VPN Security Models on Streaming Video ». In *Communication Networks and Services Research Conference (CNSR), 2010 Eighth Annual*. (11-14 May 2010), p. 152-159.

Siddiqui, Muhammad Shoaib, et Choong Seon Hong. 2007. « Security Issues in Wireless Mesh Networks ». *MUE: 2007 International Conference on Multimedia and Ubiquitous Engineering, Proceedings*, p. 717-722.

Sook-Chin, Yip, Tan Su-Wei et Chuah Teong-Chee. 2011. « Capacity Based Data Rate-Aware Channel Assigment in multi-rate wireless mesh networks ». In *Networks (ICON), 2011 17th IEEE International Conference on*. (14-16 Dec. 2011), p. 77-82.

Srivatsa, A. M., et Xie Jiang. 2008. « A Performance Study of Mobile Handoff Delay in IEEE 802.11-Based Wireless Mesh Networks ». In *Communications, 2008. ICC '08. IEEE International Conference on*. (19-23 May 2008), p. 2485-2489.

Wu, J. L., et Y. P. Zhang. 2010. « A Layered MPLS Network Architecture ». *2010 6th International Conference on Wireless Communications Networking and Mobile Computing (Wicom)*.

Yin, Zhiyu, Linwei Zhang et Wenna Li. 2009. « Study on Security Strategy of Wireless Mobile Office System ». In *Education Technology and Computer Science, 2009 ETCS '09 First International Workshop on*. (7-8 March 2009) Vol. 2, p. 495-498.

Yip, Sook-Chin, Su-Wei Tan et Teong-Chee Chuah. 2011. « Capacity Based Data Rate-Aware Channel Assigment in Multi-Rate Wireless Mesh Networks ».

YOUNES, Nadine. 2009. « La qualité de service multimédia sur les réseaux ad hoc sans fil à multi sauts ».

Yu, Dingguo, Nan Chen et Chengxiang Tan. 2009. « Design and Implementation of Mobile Security Access System (MSAS) Based on SSL VPN ».

Zhang, Hui, Yajuan Qin, Hongke Zhang et Jianfeng Guan. 2006. « Study on Host and Station Mobility in BGPIMPLS VPN ».

Zhang, yan, Jun Zheng et Huglin Hu. 2009 *Security in wireless mesh networks.*

Zhenxia, Zhang, et A. Boukerche. 2008. « A Novel Mobility Management Scheme for IEEE 802.11-Based Wireless Mesh Networks ». In *Parallel Processing - Workshops, 2008. ICPP-W '08. International Conference on*. (8-12 Sept. 2008), p. 73-78.

Zong-Hua, Liu, Chen Jyh-Cheng et Chen Tuan-Che. 2009. « Design and analysis of SIP-based mobile VPN for real-time applications ». *Wireless Communications, IEEE Transactions on,* vol. 8, n^{o} 11, p. 5650-5661.