REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

UNIVERSITE SAAD DAHLAB – BLIDA

Faculté des Sciences
Département d'Informatique

Mémoire de fin d'étude pour l'obtention
D'un diplôme de Master en informatique
Option : Ingénierie des logiciels

Sujet :

SÉCURITÉ DES RÉSEAUX MAILLÉS SANS FIL : L'authentification basée sur un serveur

Réalisé par :

- LESLOUS MOURAD
- FERGAGUE CHEMS EDDINE

Encadré par :

- DR. NOUALI-TABOUDJEMAT NADIA
- MR. BABAKHOUYA ABDELAZIZ

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

UNIVERSITE SAAD DAHLAB – BLIDA

Faculté des Sciences
Département d'Informatique

Mémoire de fin d'étude pour l'obtention
D'un diplôme de Master en informatique
Option : Ingénierie des logiciels

Sujet :

SÉCURITÉ DES RÉSEAUX MAILLÉS SANS FIL : L'authentification basée sur un serveur

Réalisé par :

- LESLOUS MOURAD
- FERGAGUE CHEMS EDDINE

Encadré par :

- DR. NOUALI-TABOUDJEMAT NADIA
- MR. BABAKHOUYA ABDELAZIZ

Résumé

Depuis quelques années, la recherche dans le domaine des réseaux maillés sans fil (Wireless Mesh Network ou WMN) suscite un grand intérêt auprès de la communauté des chercheurs en réseaux. Ceci est dû aux nombreux avantages que la technologie WMN offre, telles que l'installation facile et peu coûteuse, la connectivité fiable et l'interopérabilité flexible avec d'autres réseaux existants (réseaux Wi-Fi, réseaux WiMax, réseaux cellulaires, réseaux de capteurs, etc.). Cependant, plusieurs problèmes restent encore à résoudre comme la sécurité, la qualité de service (QdS), la gestion des ressources, etc. Ces problèmes persistent pour les WMN, d'autant plus qu'à l'extensibilité du réseau le nombre des utilisateurs va en se multipliant. Il faut donc penser à améliorer les protocoles existants ou à en concevoir de nouveaux.

L'objectif de notre projet est d'étudier certains des problèmes de sécurité rencontrés dans les WMN en termes d'authentification des utilisateurs. Après l'analyse des différentes méthodes d'authentification existantes proposées par le standard 802.11i qui est conçu pour améliorer la sécurité des réseaux 802.11, il apparait que la solution la plus sûre et la plus adaptable est l'utilisation du standard 802.1x pour l'authentification et le contrôle d'accès.

Du fait que notre travail s'inscrit dans un cadre de gestion de catastrophes, l'installation et la mise en œuvre du réseau doit être rapides et flexibles tout en garantissant une large couverture de service, la disponibilité à tout moment avec une procédure d'authentification rapide et fiable, en assurant que seuls les utilisateurs autorisés vont parvenir au réseau.

Mots clés : Réseaux maillés sans fil, sécurité, méthode d'authentification.

Abstract

In the last few years, Wireless Mesh Networks (WMNs) brought a new field of advanced research among network specialized scientists. This is due to the many advantages which WMN technology offers, such as: easy and inexpensive installation, reliable connectivity and flexible interoperability with other existing networks (Wi-Fi, WiMAX, Cellular, Sensors, WPAN networks, etc.). However, several problems still remain to be solved such as security, quality of service (QoS), resources management, etc.

In this document, we study some of the security problems met in the wireless networks and focus on the users' authentication issues. After the examination of the different authentication methods proposed by the 802.11i standard which is designed to improve the security of 802.11 networks, we found that the reliable and adaptable solution for the authentication and access control is the 802.1x standard.

As our solution will be applied to disaster management, the installation and the set up of the network have to be fast and flexible insuring, availability at any time and fast and reliable authentication process so as the only appropriate users could reach the network.

Keywords: Wireless mesh network, security, authentication, RADIUS.

ملخص

في السنوات الأخيرة، البحث في مجال الشبكات اللاسلكية المتشابكة (Wireless Mesh Network أو WMN) أثار اهتماما كبيرا لدى الباحثين في مجال الشبكات. وهذا راجع إلى الإيجابيات العديدة التي توفرها تقنية WMN, مثل سهولة التركيب, قلة التكلفة,الإتصال الموثوق و التوافق مع مختلف الشبكات الموجودة مثل (شبكات Wi-Fi, شبكات WiMax , الشبكات الخلوية, شبكات التحسس, إلخ ...). إلا أنه توجد بعض المشاكل التي يتعين حلها, كالأمن وجودة الخدمة (QoS) وتسيير الموارد, و ما إلى ذلك.هذه المشاكل تبقى قائمة لأن الشبكة قابلة للإمتداد و عدد المستخدمين سوف يتضاعف,ولذلك يجب أن نفكر في تحسين البروتوكولات الموجودة أو تصميم بروتوكولات جديدة.

الهدف من مشروعنا هو دراسة بعض مشاكل الأمن الموجودة في شبكات WMN من حيث المصادقة على المستخدمين. فبعد تحليل مختلف أساليب المصادقة الموجودة والمقترحة من طرف المعيار 802. 11i, يبدو أن الحل الأكثر نجاعة والأكثر تكيفا هو إستخدام المقياس 802.1X للمصادقة ومراقبة الدخول.

بما أن عملنا مرتبط بتسيير الكوارث, فإن تركيب و تشغيل الشبكة يجب أن يكون سريعا و سهلا مع ضمان تغطية شاملة, و وفرة للخدمات في جميع الأوقات مع إجراء مصادقة سريع و موثوق لضمان دخول المستخدمين المناسبين فقط.

كلمات المفتاح : الشبكات اللاسلكية المتشابكة, الأمن, المصادقة , RADIUS.

Remerciements

Nous remercions tout d'abord Dieu pour nous avoir donné le courage et la santé pour accomplir ce travail.

Nos vifs remerciements accompagnés de toute notre gratitude vont ensuite à nos encadreurs Madame Nouali-Taboudjemat Nadia, Maître de recherche classe A et Monsieur Babakhouaya Abdelaziz, attaché de recherche au CERIST, pour avoir accepté de nous encadrer et de nous avoir prodigué de précieux conseils.

Enfin, nous remercions nos familles et nos ami(e)s pour leur aide et leur soutien effectif durant cette année.

Dédicaces

Grace à Dieu voila notre travail terminé et il est temps pour moi de partager ma joie avec tous ceux qui m'ont soutenu et encouragé.

A vous, ma mère et mon père, vous consacriez votre vie à notre éducation et à faire notre bonheur.

A ma sœur Hakima avec sa petite famille.

A mes frères, Riyad, Djaber et Abderrahim ainsi qu'à ma belle sœur Houria.

A toute ma famille et mes amis.

A mon binôme Chemsso et sa famille.

Mourad

Dédicaces

Avant tout, louange à Dieu qui nous à donné la force, le courage, la patience de mener à bien notre travail.

Je dédie ce modeste travail

A tous ceux qui me sont les plus chers : ma mère, mon père, ma sœur Hanane et mon cher petit frère Samy.

A ma grand-mère Zakia,

A toute ma famille,

A mes amies et collègues,

A mon binôme Mourad et sa famille,

Et à tous ceux qui m'ont aidé de prés ou de loin.

CHEMS EDDINE

Table des matières

Liste des figures

Liste des tableaux

Introduction générale

Dans une situation de crise, les personnes intervenantes doivent prendre beaucoup de décisions critiques, quelques fois en se basant inévitablement sur des informations incomplètes ou périmées à cause de la pénurie des moyens de communication. Ainsi, les récents événements tragiques tels que le 11 Septembre, l'ouragan Katrina aux États-Unis et le Tsunami du Japon mais aussi les catastrophes qui ont eu lieu en Algérie[1] ont clairement montré les limites et les lacunes des technologies de communication classiques des premiers intervenants, ce qui complique leurs tâches.

L'utilisation des réseaux maillés sans fil (WMN pour Wireless Mesh Network) dans de telles situations est une solution pratique et efficace, puisqu'ils ne sont pas reliés par une infrastructure fixe, et qu'ils peuvent être implémentés rapidement et fournir la plateforme nécessaire pour la communication. Ainsi, les WMN ont émergé comme un concept promoteur pour répondre aux défis de la prochaine génération des réseaux sans fil tels que le service flexible et l'architecture évolutive et reconfigurable. La connectivité sans fil multi-sauts réduit considérablement le coût de déploiement initial et les coûts des maintenances par la suite. Les WMN supportent avec excellence une large palette d'applications telles que la connectivité backhaul pour l'accès aux réseaux cellulaires métropolitains à haut débit, les réseaux communautaires, les réseaux domestiques, les réseaux intelligents des systèmes de transport, les systèmes de défense et les systèmes de surveillance urbaine.

Toutefois, les WMN ont des caractéristiques spéciales telles que la nature sensible des liaisons radio, l'omniprésence des communications sans fil et le routage multi sauts, ce qui les rend sujet à différentes attaques. Ainsi, l'objectif principal d'une solution de sécurité conçue pour les WMN est de surmonter les risques tels que l'accès non autorisé au réseau, la modification des données et le déni de service.

Il y a encore un fort besoin de solutions efficaces et adaptées pour les exigences de sécurité des WMN dans différents scénarios d'utilisation. L'authentification et l'autorisation font partie des solutions pour protéger les WMN, comme tous les autres réseaux d'ailleurs, en permettant seulement aux utilisateurs autorisés de se connecter, et en empêchant les

[1] Nous travaillons actuellement, en collaboration avec la protection civile.

utilisateurs non désirables de pénétrer le réseau et perturber son fonctionnement normal ou paralyser totalement le service.

Il existe une solution d'authentification simple qui consiste à déployer un serveur dédié qui s'occupe de la tâche d'authentification des utilisateurs réseau. Toutefois, cette solution ne résiste pas face aux attaques de déni de service, où les attaquants isolent le serveur et empêchent les utilisateurs d'y accéder. Ce scénario survient aussi quand le serveur tombe en panne ou s'il perd la connexion. La tâche qui nous est confiée est de trouver une solution robuste qui consiste à déployer une architecture d'authentification permettant d'augmenter à la fois la sécurité du réseau et la disponibilité du service, tout en préservant une performance acceptable.

Dans ce présent mémoire, nous présentons les réseaux maillés sans fil et leur sécurité d'une manière générale, et l'authentification en particulier. Puis nous proposons une architecture robuste et fiable qui garantie la disponibilité du réseau et du service d'authentification. Dans le premier chapitre, nous ferons une introduction des réseaux maillés sans fil, leurs caractéristiques et une comparaison entre les WMN et les réseaux ad hoc. Nous aborderons dans le deuxième chapitre les différents aspects de la sécurité, les attaques existantes et leurs solutions. Dans le troisième chapitre nous analyserons les différentes solutions d'authentification existantes afin de trouver celle qui répond à nos besoins. Enfin, dans le dernier chapitre nous décrirons les différentes étapes d'installation d'un réseau maillés sans fil et nous adapterons sur ce dernier la solution d'authentification choisie. Nous terminons ce chapitre par une analyse critique de la solution et des propositions d'amélioration.

Chapitre 1 : Généralités sur les réseaux maillés sans fil

Introduction

Avec les avancées réalisées dans le domaine des communications sans fil, les réseaux maillés sans fil ou WMN *(Wireless Mesh Network)* constituent une classe émergente [1]. La terminologie *réseau maillé sans fil* est utilisée pour décrire un ensemble de routeurs sans fil fixes communicant en multi-sauts, c'est-à-dire que les communications entre deux nœuds peuvent être supportées par plusieurs nœuds intermédiaires, et qui forment un *backhaul* derrière des points d'accès sans fil qui servent les clients mobiles. Ainsi, les WMN peuvent être organisés et configurés dynamiquement, ce qui apporte beaucoup d'avantages tels que la réduction du prix, la maintenance relativement facile et la fiabilité de la couverture réseau ; ce qui a attiré les Fournisseurs d'accès Internet (Internet Service Provider (ISP)). De plus, ils permettent d'offrir aux utilisateurs une connexion omniprésente n'importe où et à tout moment.

Nous aborderons dans ce premier chapitre les principes des WMN, leurs caractéristiques, et quelques notions techniques nécessaires pour leur fonctionnement. Le groupe de travail au sein de la famille 802.11 qui est en charge de la standardisation des réseaux maillés est le 802.11s [2].

1.1.Définition des WMN

Les WMN sont des réseaux sans fil multi-sauts formés par des routeurs et des clients mesh. Les routeurs mesh sont typiquement stationnaires et n'ont pas de contraintes d'énergie. Cependant, les clients sont mobiles et ont une contrainte forte d'énergie. Les routeurs mesh conçus comme des gateway sont connectés à Internet via une infrastructure quelconque. Une gateway fournit l'accès à Internet pour les utilisateurs finaux et pour les autres réseaux (cellulaires, détecteurs,..). Les WMN sont considérés comme un alternatif moins couteux des WLAN (Wireless Local Area Network), ainsi qu'ils constituent des réseaux dorsaux pour les clients mobiles. Les réseaux sans fil existants tels qu'IEEE 802.11, IEEE 802.15, IEEE 802.16, et IEEE 802.20 sont souvent utilisés pour implémenter les WMN.

L'avantage de ces réseaux est qu'ils peuvent couvrir une zone géographique importante, sans nécessiter de pose de câbles. Par exemple, sur un grand campus, les points d'accès peuvent se mettre sur les toits des différents bâtiments sans que l'architecte du réseau ait à se préoccuper de relier les points d'accès à un système câblé de type Ethernet.

1.2.Le standard 802.11s

Le groupe IEEE 802.11s a été créé en Janvier 2004 pour offrir les fonctionnalités du maillage aux architectures et protocoles de la famille IEEE 802.11. Plus spécifiquement, pour définir les amendements nécessaires au niveau des couches MAC et physique pour la création d'un système de distribution sans fil à base de la technologie IEEE 802.11.

Dans les réseaux WLAN non maillés, les stations doivent s'associer à un point d'accès (AP) afin d'accéder au réseau, et ces stations dépendent de ce point d'accès avec lequel ils se sont associés pour communiquer. Dans un réseau maillé les AP peuvent communiquer entre eux directement sans l'intermédiaire d'un réseau externe.

1.3.Les composantes d'un WMN

Plusieurs dénominations sont présentes dans la littérature, nous préférons de les nommées selon leur significations afin d'éviter l'ambiguïté. Les différentes composantes des WMN sont [1]:

- MR (Mesh Router) : ils forment le backbone du réseau. Ce sont des routeurs sans fils qui ont la capacité de router et de relayer le trafic d'un routeur maillé à un autre jusqu'à la passerelle. Les MR sont généralement fixes et n'ont pas de contraintes de consommation d'énergie.
- MAP (Mesh Access Point) : c'est un MR qui joue parallèlement le rôle d'un point d'accès. Il fournit l'accès au réseau pour les stations ou les clients mobiles.
- Mesh Gateway : un MR qui joue aussi le rôle de passerelle vers d'autres types de réseaux comme Internet. Il est généralement connecté au réseau filaire afin de fournir aux clients une connectivité Internet à tout moment et n'importe où.
- Les Stations : il s'agit du client ou l'utilisateur. Les stations ne participent pas au routage et aux services Mesh. Ils sont mobiles et communiquent entre eux à travers leur station de base. Les stations peuvent être un ordinateur portable, un PDA, etc.

1.4.Architecture du réseau

Les réseaux WMN se composent de deux types de nœuds : les routeurs mesh et les clients mesh. Les routeurs mesh possèdent des fonctionnalités pour supporter le routage dans les WMN. Ils sont aussi dotés de multiples interfaces sans fil pour se connecter aux différentes technologies sans fil, et grâce aux fonctionnalités de passerelle/pont ajoutées, les WMN incorporent les réseaux existants. Le client maillé sans fil a deux rôles : un utilisateur final

et/ou un routeur avec un minimum de fonctionnalité. Ces clients maillés ont une seule interface sans fil [3].

L'architecture des WMN peut être classée en trois groupes principaux se basant sur la fonctionnalité des nœuds.

1.4.1. L'architecture à infrastructure

Ce type de WMN inclut des routeurs mesh qui forment le Backbone de l'infrastructure pour les clients en leur offrant la connectivité. Les routeurs mesh forment le réseau mesh à partir des fonctionnalités de routage, l'auto-configuration, l'auto-prévention et grâce aux fonctionnalités pont/passerelle intégrées dans les routeurs mesh, cette infrastructure fournit une interface pour l'intégration d'autres réseaux sans fil existants ainsi que l'Internet (voir la figure 1).

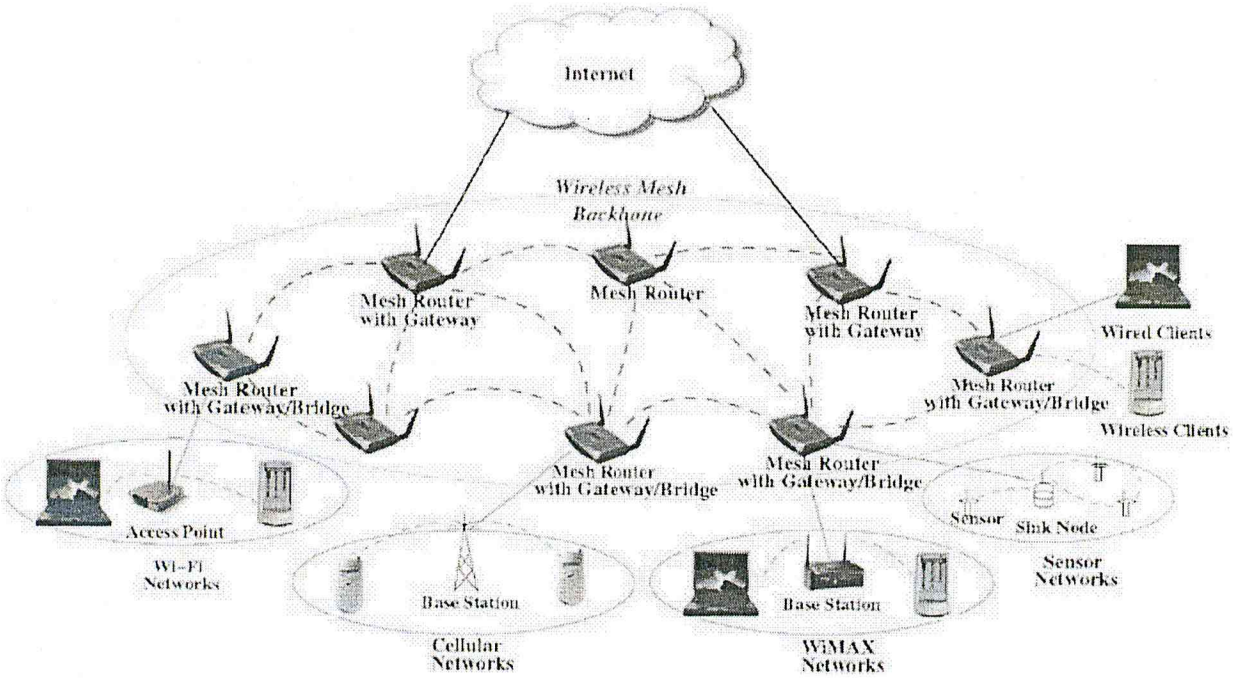

Figure 1: l'Infrastructure / Backbone

L'infrastructure ou le *Backbone* du WMN est le type le plus utilisé, par exemple dans les réseaux des communautés et les réseaux de voisinage. Les routeurs maillés sont placés sur les toits des maisons dans un voisinage et ceux-ci peuvent servir comme des points d'accès pour les utilisateurs dans les maisons et sur les routes. La communication de Backbone peut être établie en utilisant les techniques de communication en incluant les antennes directionnelles (voir la figure 2).

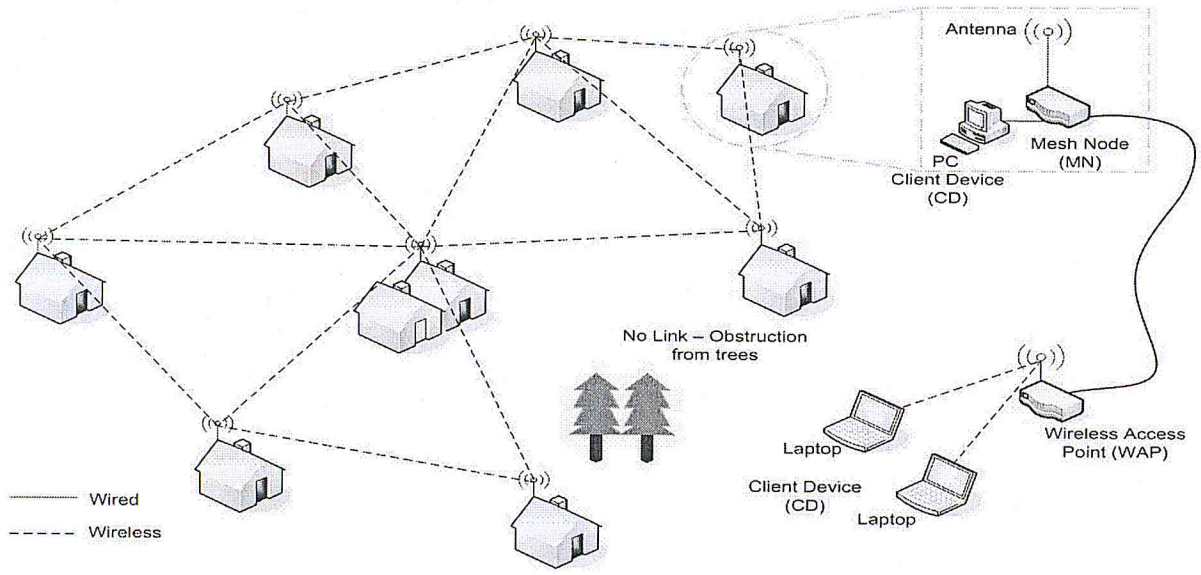

Figure 2: Déploiement de WMN dans la communauté

1.4.2. L'architecture clients

Constituée des nœuds clients seulement. Ceux-ci jouent un double rôle : utilisateur final et routeur. Cette architecture fournit une communication « point à point » à travers tous les nœuds du réseau. Ce type de réseaux est plus similaire aux réseaux conventionnels ad hoc. Cependant, ces nœuds doivent être équipés par des logiciels et matériels supplémentaires pour supporter le routage, voir la figure 3.

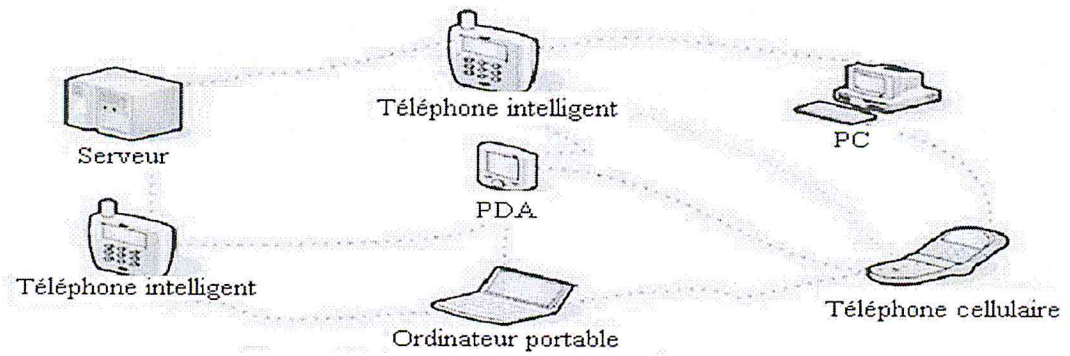

Figure 3: l'Architecture des clients

1.4.3. L'architecture hybride

Cette architecture est une combinaison des deux architectures **infrastructure** et **clients**. Les nœuds clients communiquent entre eux via des routeurs maillés ou encore directement (point à point), voir la figure 4. L'infrastructure WMN permet la connectivité aux différents réseaux tels qu'Internet, Wi-Fi, WiMAX et les réseaux cellulaires. Cette dernière architecture est le modèle préconisé pour la future génération.

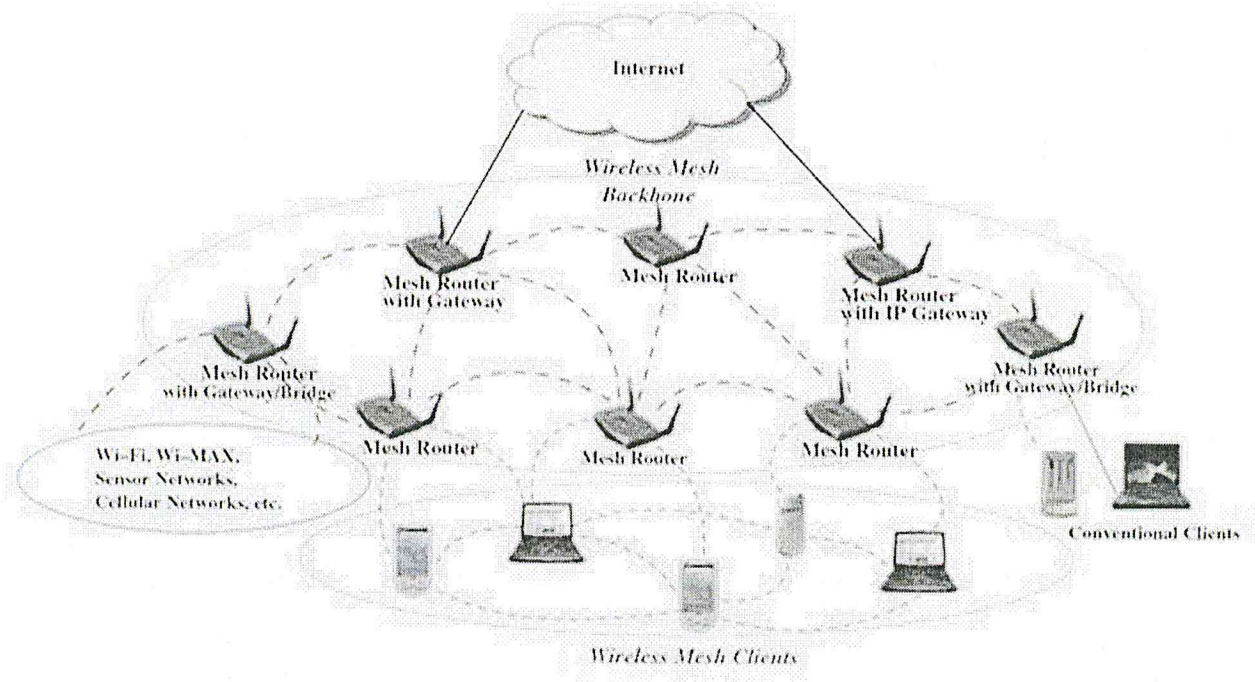

Figure 4: l'Architecture Hybride

1.5.Caractéristiques des WMN

Les WMN ont des caractéristiques spécifiques telles que :

1.5.1. La connexion sans fil multi-sauts

Les WMN permettent d'étendre la couverture d'un réseau sans fil déjà installé sans sacrifier la capacité du canal. Un autre objectif important des WMN est de fournir la connectivité entre les utilisateurs sans avoir une liaison directe entre eux. Pour satisfaire ces besoins, la communication multi-sauts est indispensable.

1.5.2. Le support des réseaux ad hoc

Le support de l'architecture ad hoc améliore la performance des réseaux mesh, telle que la flexibilité, la facilité du déploiement et de la configuration, une tolérance aux pannes et une connectivité maillée.

1.5.3. La mobilité dépend du type de nœuds mesh

Les routeurs mesh ont une mobilité minimale, alors que les clients mesh peuvent être des nœuds stationnaires ou mobiles. Ainsi, la mobilité dans les WMN varie d'un nœud à un autre, ce qui le distingue des réseaux ad hoc.

1.5.4. La diversité d'accès au réseau

Dans les WMN, l'accès à Internet et la communication peer to peer (P2P) sont tous les deux supportés. L'intégration des WMN avec d'autres réseaux sans fil fournit des services aux clients de ces réseaux. Cependant, un réseau ad hoc ne supporte pas ces fonctionnalités.

1.5.5. Les contraintes de consommation d'énergie dépendent du type de nœud

Les routeurs maillés dans les WMN n'ont pas souvent de contraintes strictes sur la consommation d'énergie. Cependant, les clients mesh peuvent exiger des protocoles efficaces pour économiser leurs énergies. Ainsi, le protocole MAC et les protocoles de routage optimisés pour les routeurs mesh peuvent ne pas être satisfaisants pour les clients mesh.

1.5.6. La compatibilité et l'interopérabilité avec les réseaux sans fil existants

Un WMN construit en se basant sur la technologie IEEE 802.11 doit être compatible avec la norme IEEE 802.11 afin de supporter le réseau mesh et les clients Wi-Fi conventionnels. Un tel WMN a besoin d'être aussi interopérable avec d'autres réseaux sans fil tels que le WiMAX, le ZigBee et les systèmes cellulaires.

1.6. Avantages des WMN

Potentiellement, les réseaux maillés permettent de servir une multitude de clients mobiles, opérants sur des structures différentes, sur une surface géographique quasiment illimitée puisque l'ajout d'un nouveau nœud augmente encore cette surface.

De plus, l'insertion donc l'extension du réseau, et la déconnexion d'un nœud est extrêmement facile et ne nécessite pas de reconfiguration manuelle du réseau. Le réseau maillé est en fait une structure s'organisant et se régénérant elle-même. De la même manière, le déploiement et l'installation de l'infrastructure sont peu coûteux puisque les

routeurs Mesh sont généralement installés dans des lieux publics tels que les points hauts de l'éclairage public. D'autre part, le maillage sans fil permet d'éliminer totalement le câblage sauf pour les points d'accès et les stations de bases pour lesquelles l'accès à Internet se fait par le réseau filaire. Les équipements étant basés sur le Wi-Fi sont peu coûteux. [1]

1.7.L'utilisation des WMN

La recherche et le développement sur les WMN sont motivés par plusieurs applications qui démontrent clairement le marché prometteur ; les cas d'usages de ce type de réseau sont : le home networking pour les maisons, les entreprises, les lieux publics, et enfin comme infrastructure temporaire en cas de catastrophe. Ces cas d'usage sont détaillés dans ce qui suit.

1.7.1. Home networking

Les réseaux maillés pour les maisons, permettra de créer à faible coût et avec une facilité de déploiement une excellente couverture sans fil dans toute la maison. La technologie des réseaux maillés permet d'éliminer les zones non couvertes ou les zones avec une qualité de couverture sans fil médiocre dans toute la maison. Ainsi, les nouvelles applications à haut débit comme la transmission et la diffusion de vidéo haute définition (~10Mb/s) seront facilement supportées dans les réseaux domestiques (voir la figure 5).

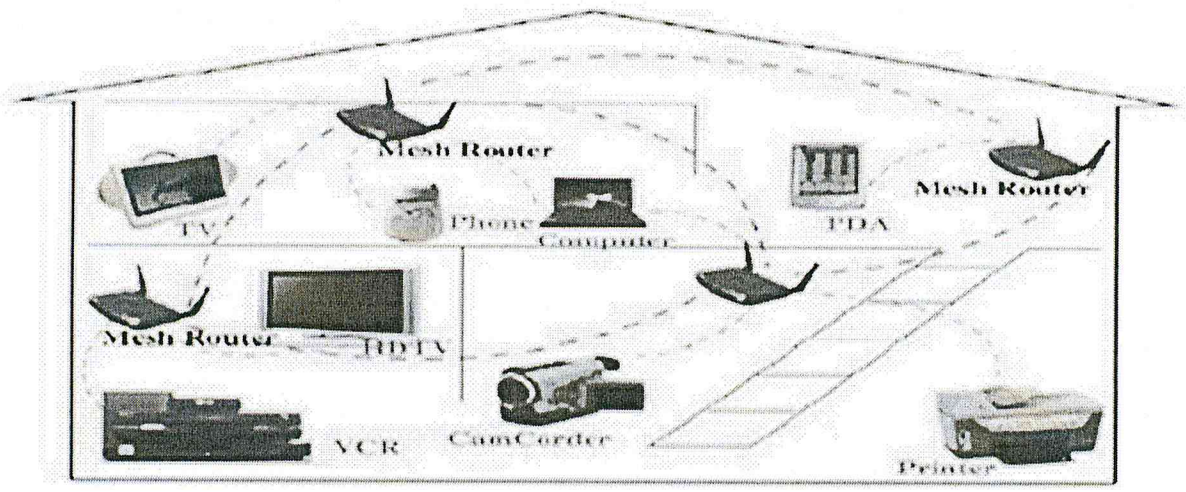

Figure 5: Home networking

1.7.2. Entreprise

La motivation principale derrière l'introduction des réseaux maillés pour fournir de la connectivité dans l'entreprise est d'utiliser des technologies sans fil performantes, fiables, peu coûteuses, et faciles à déployer. Les entreprises peuvent ainsi maîtriser les coûts associés à l'installation du réseau et de réduire le temps nécessaire pour le déploiement (voir la figure 6) la connexion entre les bureaux de multiple bâtiments se fait par des liaisons sans fil.

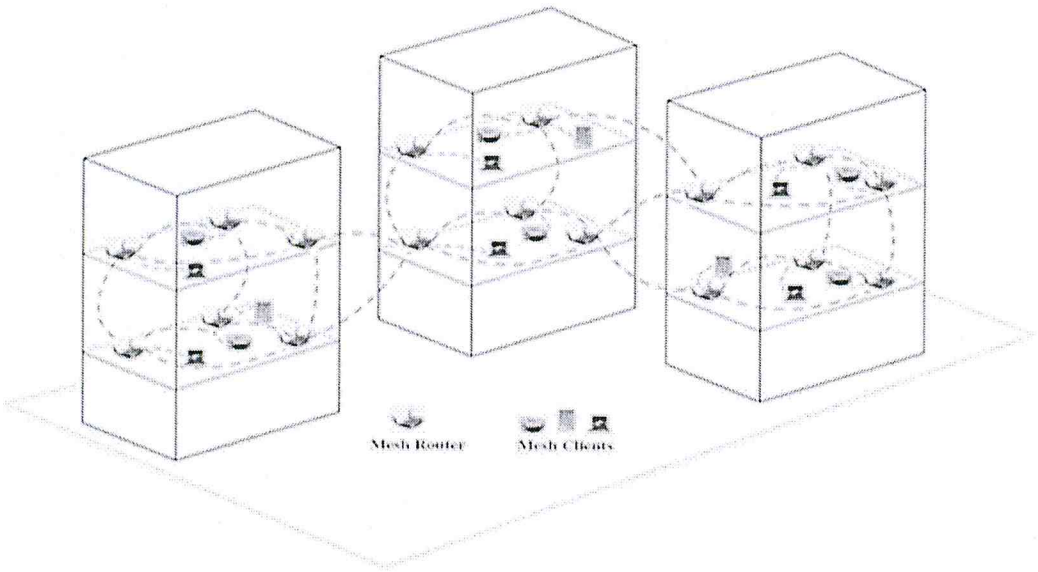

Figure 6: WMN pour les entreprises

1.7.3. Zone public (campus, communauté)

Les réseaux maillés sont aussi candidats pour fournir de la connectivité dans les zones publiques. En plus des avantages cités auparavant liés au coût et à la simplicité de déploiement, les réseaux maillés facilitent l'introduction des services de localisation, qui sont d'une importance majeure pour différentes applications. Sur un autre volet, ils participent à l'émergence des réseaux de communauté.

1.7.4. Réseau temporaire après catastrophe

Les réseaux maillés sont envisageables également pour fournir de la connectivité sans fil pour des secours durant leur intervention par exemple, ou pour fournir une infrastructure temporaire pour l'accès à l'Internet après une catastrophe naturelle. Le réseau peut être utilisé pour la vidéosurveillance à distance, la transmission de la voix et des données d'urgence, etc., (Voir la figure 7).

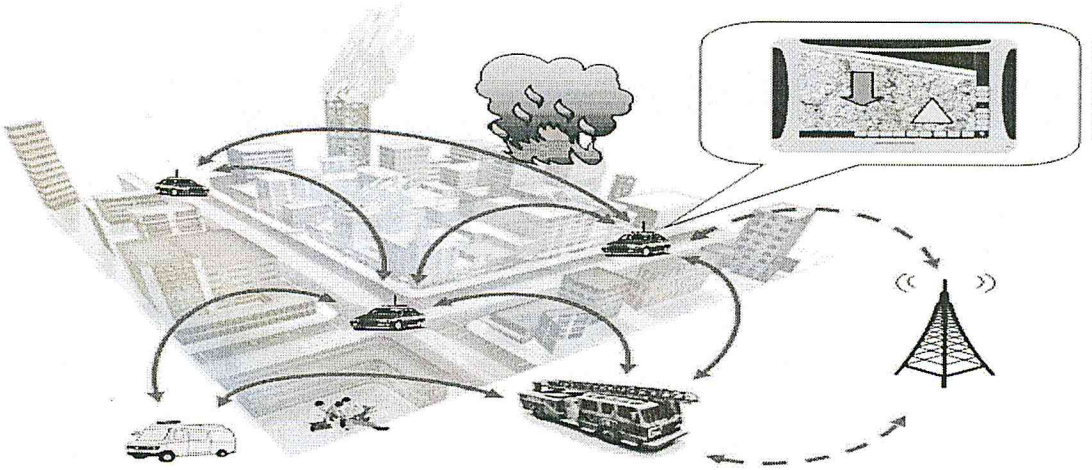

Figure 7: Mise en œuvre d'un réseau maillé après incendie

1.8. Routage interne

Le routage consiste à trouver la route optimale. Il existe un grand nombre de protocoles de routage dédiés aux réseaux sans fils comme **AODV** (*AdHoc On demand Distance VectorRouting*), **OSLR** (*Optimized Link State Routing Protocol*), **DSR** (*Dynamic Source Routing Protocol*), **OSPF** (*Open ShortestPath First*), **BGP** (*Border Gateway Protocol*), et autres. Néanmoins, on peut distinguer deux familles de protocoles de routage dans les réseaux Mesh : les **protocoles réactifs** et **les protocoles proactifs.**

1.8.1. Les protocoles réactifs

Les protocoles de routage réactif créent et maintiennent les routes à la demande. Lorsqu'une route est requise, il y a un lancement d'une procédure de découverte globale de routes, dans le but d'obtenir une information spécifiée et inconnue au préalable.

Aucun échange de paquets de contrôle n'est requis pour construire des tables de routage, on utilise une technique d'inondation et il y a donc une consommation d'une grande quantité de ressources pour découvrir une simple route entre 2 points du réseau.

Dans le cas d'un réseau dense, c'est un protocole très coûteux, mais plus avantageux dans les réseaux fluides pour lesquels l'échange d'information pour maintenir des tables de routage de faible taille à jour est coûteux.

Exemple : Le protocole AODV

L'algorithme de routage AODV (*Ad-hoc On Demand Distance Vector*) est un protocole de routage destiné aux réseaux mobiles. AODV est capable d'effectuer du routage unicast et également multicast. C'est un algorithme « à la demande », cela veut dire qu'il ne construit

des routes entres les nœuds que lorsqu'elles sont demandées par des nœuds sources. Il maintient ces routes aussi longtemps que nécessaire. De plus, AODV construit des arborescences connectant les membres des groupes multicast. Les arbres sont composés des membres des groupes et des nœuds nécessaires d'interconnexion. Ainsi, AODV utilise un numéro de séquence pour assurer la validité des routes, et il construit les routes par l'emploi d'un cycle de requêtes « *route request/ route reply* ».

Lorsqu'un nœud source désire établir une route vers une destination pour laquelle il ne possède pas encore de route, il diffuse un paquet « *route request* » (**RREQ**) sur le réseau. Les nœuds recevant le paquet mettent à jour leurs informations relatives à la source et établissent des pointeurs de retour à destination des sources dans les tables de routage. Un nœud recevant un RREQ émettra un paquet « *route reply* » (**RREP**) s'il est la destination, ou s'il possède une route vers la destination avec un numéro de séquence supérieur ou égal à celui repris dans la RREQ. Dans ce cas, il envoie (unicast) un paquet RREP vers la source. Sinon, il rediffuse la RREQ. Les nœuds conservent chacun une trace des IP sources et des ID de diffusion des RREQ. S'il reçoit une RREQ déjà traité, il l'écarte et ne le transmet pas. Les nœuds établissent des pointeurs de propagation vers la destination tandis que les RREP reviennent vers la source. Une fois que la source a reçu les RREP, elle peut commencer à émettre des paquets vers la destination. Si par la suite la source reçoit une RREP contenant un numéro de séquence supérieur ou le même mais dont le compte de hop est plus petit, elle mettra à jour son information de routage vers cette destination et commencera à utiliser la meilleure route.

Une route est maintenue aussi longtemps qu'elle est active. Une route est considérée active tant que des paquets de données transitent de la source à la destination selon ce chemin. Lorsque la source aura arrêté d'émettre des paquets de données, le lien expirera et sera alors supprimé des tables de routages des nœuds intermédiaires. Si un lien est interrompu alors qu'une route est active, le nœud d'extrémité du lien interrompu émet un paquet « *route erreur* » (**RERR**) vers le nœud source pour l'informer que la destination est désormais inatteignable. Après la réception de RERR, si la source désire toujours la route, elle peut recommencer le processus de découverte de route.

1.8.2. Les protocoles proactifs

Le routage proactif a la même philosophie que les protocoles de routage utilisés dans les réseaux filaires conventionnels. On distingue 2 méthodes : la méthode par états de liens

(**link state routing**) et la méthode par vecteur de distance (**distance vector routing**). Il y a donc une mise à jour périodique des données de routage, diffusée par les différents nœuds de routage du réseau.

Example: OLSR (Optimized Link State Routing Protocol)

OSLR est développé pour les réseaux mobiles ad-hoc. Il fonctionne comme une table de routage, il effectue des échanges d'informations de topologies avec les autres nœuds régulièrement [4]. Chaque nœud choisit un ensemble de ses nœuds voisins en tant que "*relais multipoint*" (**MPR**). Dans le protocole OLSR, seuls les nœuds sélectionnés en tant que MPR sont responsables du contrôle du trafic destiné à la diffusion dans le réseau entier. Les MPR fournissent un mécanisme efficace pour le contrôle de trafic de commande de « *flooding* » en réduisant le nombre de transmissions exigées.

Les nœuds choisis comme MPR, ont également une responsabilité spéciale en déclarant l'information d'état de lien dans le réseau. En effet, la seule condition avec OLSR de fournir les itinéraires de chemin les plus courts à toutes les destinations est que les nœuds de MPR déclarent l'information d'état de lien pour leurs sélecteurs MPR. Les informations supplémentaires disponibles d'état de lien peuvent être utilisées, par exemple, pour la redondance.

Les nœuds qui ont été choisis en tant que relais multipoint par certains nœuds voisins diffusent cette information périodiquement dans leurs messages de contrôle. Un nœud annonce de ce fait au réseau, celui qu'il a la possibilité de rejoindre les nœuds qui l'ont choisi comme MPR. Dans le calcul d'itinéraire, les MPR sont employés pour former l'itinéraire d'un nœud donné vers n'importe quelle destination du réseau. En outre, le protocole emploie les MPR pour faciliter le flooding efficace des messages de contrôle dans le réseau.

Un nœud choisit un MPR parmi ses voisins situé à un « saut ». Par conséquent, le choix de l'itinéraire par MPR évite automatiquement les problèmes liés aux excédents de transfert de paquet de données sur un lien unidirectionnel. OLSR est conçu pour fonctionner indépendamment des autres protocoles.

OLSR hérite du concept de "forwarding" et "relaying" de **HIPERLAN** (un protocole de couche MAC standardisé par l'ETSI). Le protocole est développé au sein de projet

IPANEMA (qui fait partie du programme Euclid) et du projet PRIMA (qui fait partie de programme RNRT).

1.9.Comparaison entre les WMN et les réseaux ad-hoc

En se basant sur ces caractéristiques, les WMN sont généralement considérés comme un type de réseaux ad-hoc. Tandis que les techniques des réseaux ad-hoc sont nécessaires pour les WMN, les capacités supplémentaires de ceux-ci nécessitent des techniques bien conçus et des algorithmes plus sophistiqués. La comparaison ci-dessous entre ces deux réseaux est faite sur plusieurs critères où l'architecture hybride des WMN est considérée parce qu'elle englobe tous les avantages des WMN.

1.9.1. Infrastructure sans fil/Backbone

Les WMN se composent d'un backbone qui assure une large couverture de connectivité robuste. Alors que, la connectivité des réseaux ad hoc dépend des contributions individuelles des utilisateurs qui peuvent ne pas être fiables.

1.9.2. L'intégration

Les WMN supportent l'intégration des différents réseaux existants tels que le Wi-Fi, Internet, les réseaux cellulaires et les réseaux de capteurs en utilisant les fonctionnalités de passerelle/pont des routeurs mesh, ce qui permet aux clients de ces réseaux de bénéficier des services du réseau mesh. Cependant, les réseaux ad hoc ne supportent pas l'intégration d'autres réseaux.

1.9.3. Routage dédié

Dans les réseaux ad-hoc, les clients implémentent les fonctions de routage pour tous les autres nœuds du réseau. Cependant, dans les WMN, ce sont les routeurs mesh qui se chargent de ces fonctions, ce qui signifie que la charge sur les clients est significativement diminuée, avec moins de consommation d'énergie et plus de capacités pour les applications de client.

1.9.4. Multiplicité des interfaces radio

On a vu que les routeurs mesh peuvent être équipés des interfaces radio multiples pour se connecter à différentes technologies sans fil. Le routage des paquets est tenu par les routeurs mesh sur différentes interfaces radio, cela améliore la capacité du réseau. Cependant, les

réseaux ad hoc implémente ces fonctions sur le même canal ce qui entrave la performance du réseau.

1.9.5. La mobilité

Le routage dans les réseaux ad hoc est fourni par les clients [5], ainsi que la topologie et la connectivité du réseau dépendent de l'itinérance de ces utilisateurs. Cela impose des défis supplémentaires pour configurer et déployer des protocoles convenables au routage. Dans les WMN, les routeurs mesh fournissent l'infrastructure et la couverture du réseau, alors, la mobilité des clients est encore supportée, sans sacrifier la performance du réseau.

Conclusion

Les réseaux maillés sans fil sont la technologie de la prochaine décennie, grâce à ses avantages significatifs, cependant ils souffrent de failles de sécurités importantes qui ont besoin d'être prises en compte. Dans le chapitre suivant, nous analysons les menaces et les mécanismes de sécurités possibles dans les WMN.

Chapitre 2 : Sécurité des réseaux maillés sans fil

Introduction

Les réseaux maillés ont émergé comme une technologie clé des réseaux sans fil de la prochaine génération, en montrant un progrès rapide et en inspirant de nombreuses applications. Cependant, les WMN ne sont pas encore prêts au déploiement à grande échelle à cause de deux raisons principales : l'interférence provoquée par la communication sans fil et l'absence de garanties de sécurité. Toute communication sans fil est sujette aux contraintes de retard à causes des interférences des ondes radio. Néanmoins, on croit que les solutions technologiques seraient capables de surmonter ce problème, par exemple, en utilisant des points d'accès multi radio multi canaux [6]. Le manque de garanties de sécurité est un autre facteur qui ralentit le déploiement des WMN. Alors que ces réseaux continuent à se développer et puisque l'accès au mesh est disponible à n'importe quel équipement sans fil, il faut mettre en place des mécanismes qui détermine quel niveau de sécurité est nécessaire, les préventions qui doivent être appliquées, et le niveau de tolérance autorisé dans chaque réseau, tout en garantissant un comportement collaboratif entre les nœuds.

2.1. Les défis de sécurité dans les réseaux maillés sans fil

Les WMN ont des caractéristiques spéciales qui les distinguent des autres technologies réseau. Par conséquent, elles imposent une large gamme de défis de conception et d'implémentation. La mobilité de nœuds, l'environnement sans fil hybride créé par les différentes architectures mesh, la densité des connexions dans ces réseaux et le comportement imprévisible des nœuds sont des facteurs essentiels qui influencent sur la nature des solutions de sécurité.

2.1.1. La mobilité des nœuds

Un point attrayant des WMN commercial est l'itinérance transparente des clients mobiles. Cependant, la mobilité des clients est un défi en elle-même qui pose quelques problèmes de sécurité. Une partie de ce défi réside dans les appareils mobiles qui sont sujets aux vols et peuvent être utilisés ainsi par les attaquants pour accéder au réseau ou interrompre la communication. Ainsi, le fait que les appareils les plus mobiles sont des appareils « clients légers » à énergie limitée et une capacité de stockage faible, pose une difficulté à mettre en place quelques solutions de sécurité (à titre d'exemple, les algorithmes de cryptage qui exigent des ressources spéciales).

2.1.2. L'environnement sans fil hybride

L'environnement sans fil hybride permet un accès en mode multi sauts en combinant une communication peer-to-peer entre les nœuds mobiles, ainsi que la communication des nœuds mobiles à travers une infrastructure sans fil fixe. La facilité d'itinérance transparente fournie par les WMN est un point attrayant. Cependant, il y a un risque de sécurité quand un utilisateur mobile se promène entre les réseaux disparates. Par conséquent, quelques caractéristiques essentielles comme l'itinérance sécurisée, l'authentification et l'autorisation devraient être fortement considérées dans ce type d'environnement.

2.1.3. La charge et la densité des connexions

La densité dans les WMN est un point capital qui doit être pris en considération pendant le développement des solutions de sécurité. Plusieurs facteurs peuvent affecter la charge des liaisons telle que l'architecture du réseau, la densité des nœuds mobiles, le nombre des canaux de transmission utilisés pour chaque nœud mobile, la puissance de signal et la mobilité des nœuds. La compréhension de la relation entre ces facteurs et la capacité des WMN est essentielle pour concevoir des solutions pratiques.

2.1.4. Le comportement égoïste des nœuds

La coopération entre les nœuds dans les WMN est nécessaire pour la communication multi sauts, le traitement collectif des données et les fonctions de sécurité coopératives. Cependant, le déploiement des services mutuels consomme d'énormes ressources, qui sont généralement rares dans les nœuds mobiles. Ainsi, la coopération peut ne pas être garantie, surtout dans les scénarios de réseaux mesh ouverts, parce que chaque utilisateur préférerait maximiser son propre avantage en minimisant sa contribution. La solution de coopération concerne différentes couches du réseau, avec différents buts et façons d'agir, où un nœud égoïste peut se comporter d'une manière malicieuse par :

- La non-adhérence aux spécifications des protocoles.
- L'optimisation d'une fonction particulière qui peut affecter le service.

2.2. Les menaces de sécurité dans les WMN

Les menaces dans les WMN sont principalement causées par la nature des liaisons radio et la communication multi sauts. La principale tâche des solutions de sécurité des WMN est de surmonter les types de menaces suivantes :

- **L'écoute passive et la modification des données** : La nature de l'environnement sans fil peut provoquer l'écoute et la modification des données envoyées par les nœuds. La nature des liaisons sans fil et la présence des nœuds mobiles intermédiaires exigent l'existence d'une solution de sécurité qui garantit la confidentialité et l'intégrité des données transmises.
- **L'accès non autorisé :** L'accès sans autorisation aux réseaux mesh pose un risque sérieux à ces réseaux. Dans les WMN fermés, qui ont une administration centralisée, l'authentification devrait être une exigence pour se connecter au réseau. Cependant, dans les réseaux mesh ouverts sans un contrôle central, des solutions alternatives doivent être mises en place pour permettre l'authentification entre les nœuds mobiles d'une manière distribuée.
- **Le déni de service (DoS) :** Un DoS traditionnel peut survenir pendant la transmission multi sauts par un ou plusieurs nœuds mobiles intermédiaires en supprimant sélectivement des paquets de trafic. Le DoS dans les WMN est généralement provoqué par le mauvais routage d'un ou de plusieurs nœuds mobiles.

2.3. Les attaques dans les WMN

Les attaques réseau peuvent se produire au niveau des trois premières couches du modèle OSI, car elles forment le cœur du réseau. Nous ne prenons pas en considération les attaques de la couche transport et les couches supérieures parce que ces couches sont implémentées en général dans les appareils des utilisateurs terminaux, par conséquent, les attaques sur ces couches sont indépendantes du réseau sous-jacent.

2.3.1. Les attaques de la couche physique

Tous les réseaux sans fil, en incluant les WMN, sont vulnérables aux attaques de brouillage radio de la couche physique. L'attaque de brouillage radio [7] est une attaque potentiellement nuisible qui peut être lancée avec une aisance relative en permettant simplement à un dispositif sans fil de transmettre un signal fort sur le canal pour provoquer une interférence avec le réseau cible. Dans sa forme la plus simple, l'attaquant peut transmettre continuellement le signal de brouillage (brouilleur constant). Alternativement, l'attaquant peut utiliser des stratégies par lesquelles il transmet seulement le signal radio quand il écoute une activité sur le canal et reste silencieux sinon (brouilleur réactif). Cependant, ces types d'attaques de brouillage, où la transmission est un signal arbitraire,

peuvent être considérés comme un bruit sur le canal, et les protocoles MAC tel que BMAC [8] peuvent les surmonter.

2.3.2. Attaques de la couche MAC

2.3.2.1. L'écoute passive clandestine

La nature de diffusion de transmission des réseaux sans fil les rend sujets à l'écoute passive par des attaquants externes qui se trouvent dans le rayon de transmission des nœuds communicants. Les réseaux sans-fil multi sauts tels que les WMN sont sujet aussi à l'écoute interne par les nœuds intermédiaires, où un nœud intermédiaire malicieux peut garder une copie de toutes les données qu'il fait suivre, sans que d'autres nœuds le sachent. Bien que l'écoute passive n'affecte pas la fonctionnalité du réseau directement, elle affecte la confidentialité et l'intégrité des données. Le cryptage des données est généralement employé par l'utilisation des clés fortes pour protéger la confidentialité et l'intégrité des données.

2.3.2.2. L'Attaque de Brouillage de la couche liaison

Les attaques de brouillage de la couche liaison sont plus complexes que les attaques aveugles de la couche physique. Plutôt que de transmettre continuellement des bits au hasard, l'attaquant peut transmettre des en-têtes de trames MAC régulières sur le canal de transmission qui se conforment au protocole MAC utilisé dans le réseau victime [9]. Par conséquent, les nœuds légitimes trouvent toujours le canal occupé et attendent une durée aléatoire pour réécouter le canal de nouveau. Cela provoque un déni de service pour les nœuds légitimes, et permet aussi au nœud brouilleur d'économiser son énergie.

2.3.2.3. L'attaque par l'usurpation de l'adresse MAC

Les adresses MAC sont utilisées depuis longtemps comme un identifiant de la deuxième couche des réseaux LAN filaires et sans fil. Les adresses MAC qui sont globalement uniques étaient souvent utilisés comme un identifiant unique pour attribuer des niveaux variables de privilèges aux utilisateurs réseau. Ceci est particulièrement répandu dans les réseaux Wi-Fi 802.11. Cependant, les protocoles MAC et les cartes réseau actuelles n'assurent aucune protection qui empêcherait un attaquant potentiel de modifier l'adresse MAC source dans ses trames transmises. Au contraire, c'est souvent supporté sous forme de pilote du fabricant, qui rend la tâche facile. La modification de l'adresse MAC dans les trames transmises est appelé *spoofing MAC,* et elle peut être utilisé par les attaquants de différentes manières. Le spoofing MAC permet à l'attaquant d'éviter les systèmes de

détection d'intrusion (IDS) présents dans le réseau. D'ailleurs, les administrateurs réseau d'aujourd'hui utilisent souvent les adresses MAC pour contrôler l'accès au réseau. Un attaquant peut facilement écouter le réseau, déterminer les adresses MAC des appareils légitimes et les utiliser une pour accéder au réseau. L'attaquant peut même injecter un grand nombre de trames fausses dans le réseau afin de consommer les ressources réseau (en particulier, la bande passante et l'énergie) et provoquer un déni de service pour les nœuds légitimes.

2.3.2.4. L'attaque de rejeu

Souvent connue par l'attaque de « l'homme du milieu » [10], L'attaque de rejeu, elle peut être lancée par des nœuds externes ainsi que par des nœuds internes. Un nœud malveillant externe (qui n'appartient pas au WMN) peut capturer la communication entre deux nœuds (A et B) (voir la figure 8). Il peut retransmettre alors ces messages légitimes dans un autre moment pour avoir l'accès aux ressources du réseau. Généralement, l'information d'authentification est retransmise quand l'attaquant trompe un nœud (le nœud B dans la figure 8) pour qu'il croie que l'attaquant est un nœud légitime (le nœud A dans la figure 8). Dans une telle situation, un nœud malveillant interne, qui est un saut intermédiaire entre deux nœuds communicants, peut garder une copie de toutes les données retransmises. Il peut les retransmettre alors à un point d'accès après pour gagner l'accès non autorisé aux ressources du réseau.

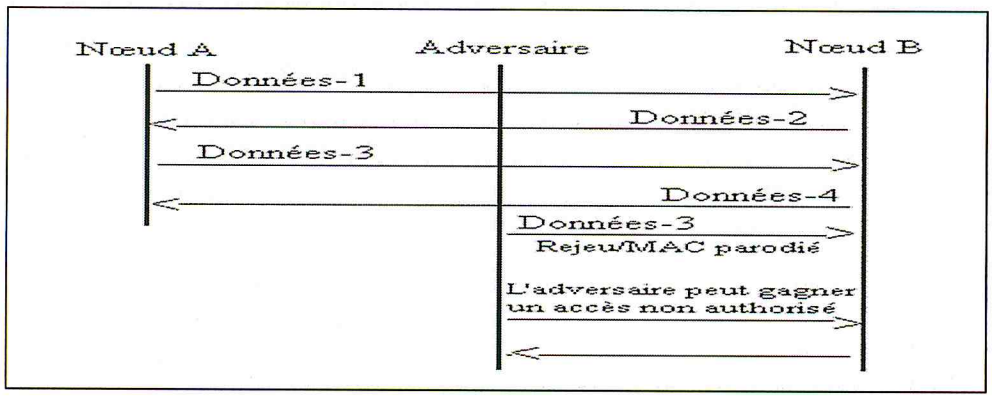

Figure 8: Robustesse contre les attaques de rejeu et de spoofing MAC

2.3.2.5. Les attaques de pré-calcul et de concordance partielle

Dans cette section nous discutons un type différent d'attaques de sécurité. Contrairement aux attaques susmentionnées où les vulnérabilités du protocole MAC sont exploitées, ces attaques exploitent les vulnérabilités des mécanismes de sécurité qui sont utilisés pour

protéger la couche MAC. Les attaques de pré-calcul et de concordance partielle exploitent les primitives cryptographiques qui sont utilisés dans la couche MAC pour protéger la communication. Dans une attaque de pré-calcul ou une attaque TMTO (Time Memory Trade-Off) [11], l'attaquant calcule une grande quantité d'informations (la clé, le texte en clair et le cryptogramme respectif) et enregistre ces information avant de lancer l'attaque. Quand la transmission réelle commence, l'attaquant utilise l'information pré-calculée pour accélérer le processus de la cryptanalyse. Les attaques TMTO sont extrêmement efficaces face à un grand nombre de solutions cryptographiques. D'autre part, dans une attaque de concordance partielle, l'attaquant possède l'accès à certaines paires (cryptogramme, texte en clair), qui diminue la puissance de la clé de chiffrement et améliore les chances de succès des mécanismes de force brute. Les attaques de concordance partielle exploitent le faible déploiement des algorithmes de cryptage. Par exemple, dans la norme IEEE 802.11i pour la sécurité de la couche MAC des réseaux sans fil, les champs d'adresse MAC dans l'en-tête MAC sont utilisés dans le code d'intégrité du message (MIC) [12]. L'en-tête MAC est transmis en clair pendant que le champ MIC est transmis sous forme de texte crypté. La connaissance partielle du texte en clair (l'adresse MAC) et le cryptogramme (MIC) rend IEEE 802.11i vulnérable aux attaques de concordance partielle.

2.3.3. Les attaques de la couche réseau

Les attaques de la couche réseau peuvent être classées en attaques de contrôle et attaques de données, et elles peuvent être de nature active ou passive. Les attaques de contrôle visent généralement la fonctionnalité de routage de la couche réseau. L'objectif de l'attaquant est de bloquer les chemins ou forcer le réseau à choisir des chemins non optimaux. Ainsi, les attaques de données affectent la fonctionnalité d'expédition des paquets. L'objectif de l'attaquant est de provoquer un déni de service aux utilisateurs légitimes en supprimant les paquets ou en injectant des données aléatoires dans le réseau.

2.3.3.1. Les attaques du contrôle

Les attaques de précipitation [13] qui ciblent les protocoles de routage à la demande (par ex. AODV) étaient parmi les premières attaques découvertes sur la troisième couche des réseaux sans fil multi saut. Ces attaques exploitent le mécanisme de découverte de chemin des protocoles de routage à la demande. Dans ces protocoles, le nœud qui a besoin d'un chemin diffuse un message de demande. Les protocoles spécifient une durée spécifique de retard entre la réception du message par un nœud particulier et son expédition pour éviter

la collusion. Le nœud malicieux qui lance l'attaque hâte la retransmission de ce message au nœud prévu avant tout autres nœuds. Par conséquent, le chemin de la source à la destination inclut le nœud malicieux comme intermédiaire, qui peut alors supprimer les paquets de données, ce qui provoque un DoS.

L'attaque de trou de ver a un objectif semblable bien qu'elle utilise une technique différente [14]. Dans une attaque de trou de ver, au moins deux nœuds malicieux établissent un tunnel en utilisant un lien de communication rapide (c'est-à-dire, une connexion filaire ou sans fil à grande vitesse, etc.) (voir la figure 9). Pendant la phase de découverte de chemin en demande des protocoles de routage, les messages de demande de chemin sont envoyés entre les nœuds malicieux en utilisant le tunnel établi. Donc, le premier message de la requête de chemin qui atteint le nœud de destination est celui envoyé par les nœuds malicieux. Par conséquent, ceux-ci sont ajoutés dans le chemin de la source à la destination. À ce moment, ils suppriment tous les paquets, ce qui mène au déni complet de service, ou des paquets sélectivement pour éviter la détection.

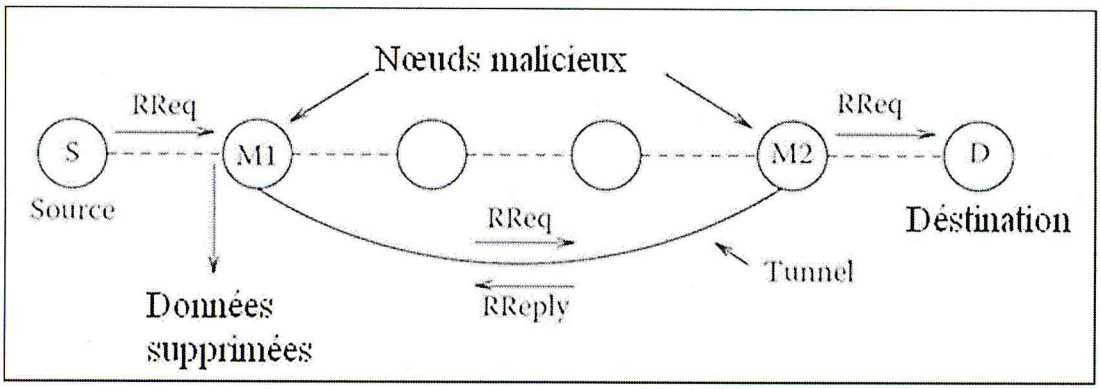

Figure 9: L'attaque de trou de ver

Une attaque de trou noire [15] est une autre attaque qui mène au déni de service dans les réseaux mailles sans fil. Elle exploite aussi le mécanisme de découverte de chemin des protocoles de routage à la demande. Dans cette attaque, le nœud malicieux répond toujours positivement à une demande de chemin bien qu'il puisse ne pas avoir un chemin valide vers la destination. Puisque le nœud malicieux ne vérifie pas ses entrées de routage, il sera toujours le premier à répondre au message de demande de chemin. Donc, presque tout le trafic dans le voisinage du nœud malicieux sera dirigé vers lui, ce dernier peut supprimer tous les paquets, ce qui provoque un déni de service. La figure 10 montre l'effet d'une attaque de trou noire dans le voisinage du nœud malicieux, où tout le trafic est dirigé vers le nœud malicieux.

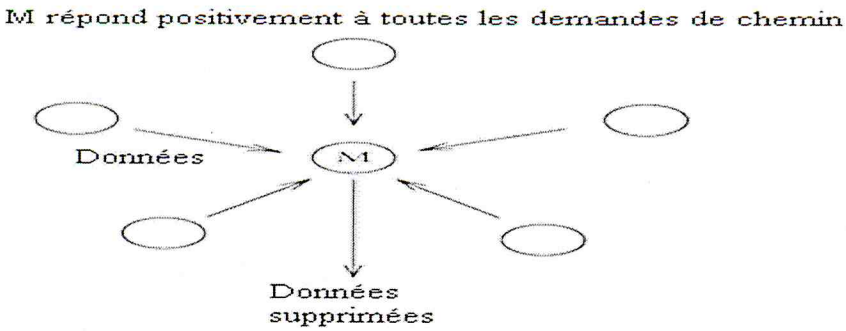

Figure 10: Attaque de trou noire

En plus des attaques susmentionnées, les réseaux maillés sans fil sont susceptibles aussi aux attaques de partage du réseau et aux attaques de boucle de routage. Dans une attaque de partage du réseau, les nœuds malicieux fonctionnent ensemble pour perturber les tables de routage de façon que le réseau soit divisé en partitions non-interconnectées, ce qui provoque un déni de service pour une certaine partie de réseau. Les attaques de boucle de routage affectent la capacité de circulation des paquets dans le réseau où les paquets continuent à circuler dans la boucle jusqu'à ce qu'ils atteignent le nombre de saut maximal, à ce stage les paquets sont tout simplement supprimés.

2.3.3.2. Les attaques de données

Les attaques de données sont lancées essentiellement par les nœuds égoïstes et malicieux et causent la dégradation de performance ou le déni de service. L'attaque de données la plus simple est l'écoute passive. Le comportement égoïste des nœuds participant dans le réseau est un point de sécurité importante parce que les nœuds dans les WMN dépendent l'un de l'autre pour la livrer les données. Les nœuds intermédiaires égoïstes peuvent ne pas livrer des paquets conformément au protocole. Ils peuvent supprimer tous les paquets de données, ayant pour résultat le déni complet de service, ou il peut supprimer des paquets de données sélectivement ou au hasard. Il est difficile de distinguer entre le comportement égoïste d'une part, et l'échec de liaison ou la congestion du réseau d'autre part.

2.4. Les mécanismes de sécurité des WMN

Les mécanismes de sécurité peuvent être classés en deux grandes catégories : la prévention d'intrusion et la détection d'intrusion.

2.4.1. Les mécanismes de sécurité de la couche MAC

2.4.1.1. Mécanismes de prévention d'intrusion

Plusieurs solutions de sécurité ont été proposées [16, 17] pour les réseaux sans fil multi-sauts qui sont applicables aux réseaux maillés sans fil avec une modification légère. Ces solutions de sécurité fournissent les services d'authentification, de confidentialité et d'intégrité de données pour la couche MAC. La plupart des solutions de sécurité utilisent des primitifs cryptographiques. Une solution de sécurité basée sur le chiffrement par flux a été proposée [16] pour fournir les services de confidentialité de données, l'intégrité de données et l'authentification. L'objectif d'utiliser le cryptage par flux est de permettre un traitement en ligne des données. Deux clés de sécurité secrètes, la clé d'authentification secrète (SAK) et la clé de session secrète (SSK), sont utilisées pour l'authentification du supplicant(utilisateur/client) et l'authentificateur. SAK est échangé entre le supplicant et l'authentificateur après l'authentification réciproque initiale du serveur d'authentification, alors que le SSK est utilisé pour une session de communication donnée entre les deux nœuds. Le SAK et la paire SSK sont utilisés dans la communication des nœuds pour produire le vecteur de permutation (PV), qui est utilisé pour le cryptage et le décodage de données. Dans le mode le plus fort de sécurité, les données sont aussi impliquées dans la génération de PV. La synchronisation du vecteur de permutation généré entre l'expéditeur et le récepteur des données a pour résultat l'authentification d'origine de chaque Unité de Données du Protocol MAC (MPDU).

IEEE 802.11i a été ratifié en juin de 2004 comme la norme de sécurité de la couche MAC des réseaux sans fil. La norme est basée sur les primitives cryptographiques et elle fournit les services de confidentialité de données, d'intégrité de données et l'authentification.

Une des exigences de sécurité importantes des réseaux sans fil multi sauts comme les WMN est la confiance entre les nœuds communicants. Les mécanismes basés sur la cryptographie conventionnels sont généralement non applicables pour les réseaux multi-sauts comme les WMN. Par conséquent, un certain nombre de protocoles d'authentification et de collaboration distribuée en voisinage ont été proposée par les chercheurs pour ce but [18, 19, 20]. Une solution basée sur le seuil de cryptographie a été proposée [20] pour la distribution de la paire de clés (clé publique, clé privée) et l'authentification des nœuds en se basant sur la clé privée. Dans le schéma proposé, tous les nœuds possèdent la clé

publique, tandis que chaque nœud a une partie de la clé privée. Le partage du seuil secret (k, n) est utilisé pour produire la clé privée. Un nœud déclarant « k » à partir de « n » parties de la clé privée peut construire la clé privée complète, et moins que k parties de la clé secrète ne peuvent pas construire la clé privée complète. Basé sur ce mécanisme, chaque fois qu'un nœud a besoin de rafraîchir sa clé privée, a besoin des k voisins pour lui envoyer leur partie secrète afin de reconstruire la clé privée complète, et aucun nœud ne peut construire la clé privée en se basant seulement sur ses propres informations. Le processus de génération de la clé privée est montré dans la figure 11, où le nœud demandeur diffuse le message de demande avec sa propre partie de la clé privée pour la vérification. Les nœuds voisins répondent au message de demande en lui envoyant leur propre partie de la clé secrète. Le nœud demandeur est capable de produire la clé privée complète lors de la réception des k parties de cette clé. En utilisant ce mécanisme, un nœud ne peut pas produire la clé privée à moins que sa propre partie de la clé privée soit vérifiée par les k nœuds voisins. Pareillement, la clé privée du nœud malicieux n'est pas rafraîchie par ces voisins. Donc, le partage de seuil secret permet une forte solution d'authentification et de gestion de clés.

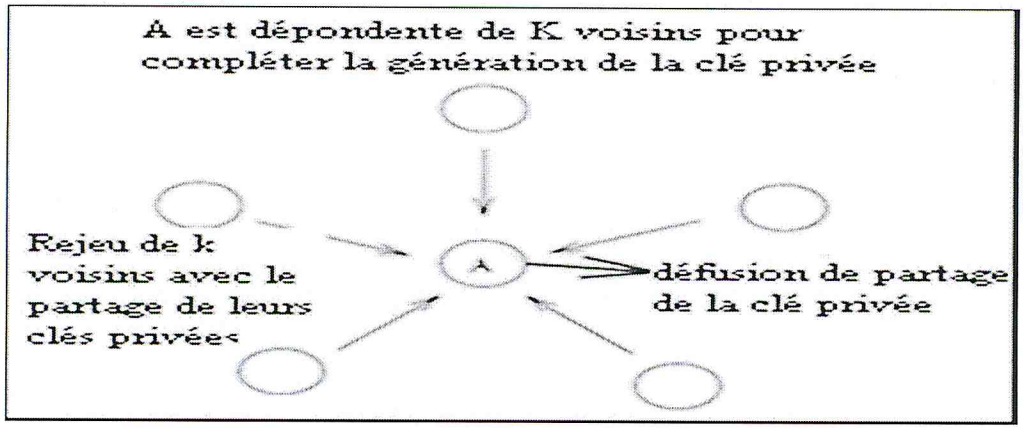

Figure 11: Collaboration des voisins pour générer la clé dans un réseau maillé

2.4.1.2. Mécanismes de détection d'intrusion

Un nombre très réduit de systèmes de détection d'intrusion de la couche MAC des réseaux sans fil a été proposés. Lim et autres [21] ont proposé un système de détection d'intrusion couplé avec la réponse automatisée active pour protéger les points d'accès sans fil. Les auteurs ont proposé de déployer des appareils de détection spécifiques près des points d'accès sans fil, la détection est faite au niveau de la couche MAC. Ils proposent des messages RTS/CTS (Ready To Send/Clear To Send) de la liste noire des adresses MAC

comme une métrique de détection. Pour répondre à l'intrusion, les auteurs proposent l'utilisation de la tactique de l'intrus en générant et transmettant des paquets mal formés à l'intrus.

L'un des travaux améliorés dans ce contexte est de Liu et autres [22]. Les auteurs ont proposé l'approche de la théorie de jeu pour sélectionner une stratégie de détection d'intrusion optimale pour un instant donné à partir d'un ensemble de faibles mécanismes de détection d'intrusion déployés. L'idée fondamentale c'est que plusieurs techniques de détection d'intrusion sont très bonnes pour découvrir certains types d'attaques, mais ne fonctionnent pas de façon optimale dans les autres cas. La combinaison de ces stratégies et l'utilisation d'une stratégie optimale dans un scénario donné peuvent augmenter l'exactitude du système de détection.

2.4.2. Les mécanismes de sécurité de la couche réseau

2.4.2.1. *Mécanismes de prévention d'intrusion*

Plusieurs techniques de prévention d'Intrusion ont été proposées pour protéger les protocoles de routage des réseaux sans fil multi-sauts. Par exemple, SRP [23] est utilisé pour sécuriser le processus de découverte du chemin, et protéger la fonctionnalité de routage des attaques qui exploitent le protocole de routage lui-même. Les messages de *Route Request* et *Route Response* sont protégés par le code d'authentification de message pour authentifier le nœud expéditeur. Les adresses IP des nœuds intermédiaires sont aussi ajoutées au message de *Route Request* pour prévenir les attaques du trou noir et de trou de ver.

Les mécanismes de prévention d'intrusion sont essentiellement utilisés pour établir une confiance entre les nœuds participant et fournir la confidentialité et l'intégrité des messages de contrôle.

2.4.2.2. *Mécanismes de détection d'intrusion*

Plusieurs techniques de détection d'intrusion de la couche réseau ont été proposées pour les réseaux filaires et sans fil. Par exemple, Yang et autres [24] ont proposé une solution de sécurité pour la couche 3 des réseaux ad hoc mobiles auto-organisés. C'est l'une des solutions qui garantissent l'auto-guérison et l'auto-organisation des réseaux. La solution est basée sur la collaboration distribuée des voisins et la validation mutuelle d'information. Le schéma est basé sur le partage d'un seuil secret négocié auparavant, qui est utilisé pour

rafraîchir le jeton des nœuds. Les auteurs ont proposé un schéma basé sur un jeton de crédit. Ce jeton expire après une durée donné. Le temps d'expiration symbolique du nœud dépend du crédit du nœud. Le crédit des nœuds qui se comportent bien est accumulé avec le temps. Donc, le temps d'expiration symbolique de ces nœuds est plus long et linéairement augmenté à chaque fois que le nœud rafraîchit son jeton. Le jeton du nœud malicieux ou égoïste est révoqué par la collaboration des voisins qui l'empêchent de participer au réseau. La métrique de détection qui fait la différence entre les nœuds qui se comportent bien et les nœuds malicieux est basée sur les protocoles de routage, et consiste à calculer le nombre de sauts, le rapport de livraison des paquets, etc.

Conclusion

Les attaques réseaux sont fréquentes et leur détection et prévention deviennent de plus en plus nécessaires et difficiles à la fois, ce qui pousse les chercheurs à concevoir des systèmes d'authentification des utilisateurs qui empêchent les nœuds non autorisés à accéder au réseau.

Dans le prochain chapitre, nous discuterons l'authentification d'une manière générale et quelques solutions proposées pour ce sujet. Nous ferons une comparaison entre ces solutions, et enfin, nous en choisirons une pour l'analyser et la déployer sur un réseau maillé sans fil.

Chapitre 3 :
L'authentification dans les réseaux maillés sans fil

Introduction

La sécurité est un grand souci dans les réseaux mesh, où le déploiement d'un système sécurisé et robuste est considéré comme l'un des défis majeurs qui entravent les WMN et influencent sur leur utilisation. Ainsi, l'authentification est une mesure de prévention incontournable dans les WMN, en permettant seulement aux utilisateurs autorisés d'utiliser les services du réseau, et en empêchant les autres de pénétrer le réseau et interrompre le fonctionnement normal ou consommer les ressources.

Ce chapitre présente les concepts d'authentification d'une manière générale. Nous commençons par la définition du terme « Authentification » et ses avantages. Puis nous analysons quelques solutions existantes tout en faisant une comparaison entre elles. Enfin, en se basant sur le résultat de cette comparaison, nous déduisons la solution d'authentification la plus robuste et la plus adéquate pour les WMN.

3.1.Définition de l'authentification

Selon le dictionnaire; le mot « Authentification » signifie quelque chose qui n'est pas fausse, ou une imitation usurpée, mais une chose acceptée comme vraie ou réelle.

L'authentification se compose de deux parties: la première consiste à fournir une preuve de l'authenticité de l'information transmise ou enregistrée, et la seconde consiste à vérifier la preuve de l'authenticité de l'information reçue ou enregistrée. L'authentification est l'un des mécanismes fondamentaux de sécurité.

3.2. Avantages de l'authentification

L'authentification empêche les utilisateurs non autorisés d'accéder aux ressources protégées du réseau, telles que les serveurs, les applications d'entreprise et les bases de données. Sans authentification, un pirate informatique pourrait accéder facilement au réseau LAN en connectant un portable à un port Ethernet tout simplement, ou s'associant à un point d'accès du réseau sans fil du parking de la compagnie. Si on permet à des pirates informatiques d'accéder au réseau, ils chercheront n'importe quelle façon d'exploiter les vulnérabilités de sécurité.

Le déploiement d'un contrôle d'accès est un grand pas vers la sécurisation d'un réseau informatique. Cependant, le contrôle d'accès n'est pas une formule magique pour garantir la

sécurité du réseau, alors, on doit l'utiliser avec d'autres méthodes, tel que le cryptage des paquets de données, la détection d'intrusion et la prévention du déni de service.

3.3.Spécificités dans les réseaux maillés sans fil

Les réseaux maillés sans fil ont des caractéristiques spéciales qui les distinguent des autres réseaux et quelques fois même des réseaux ad hoc. L'authentification dans les WMN doit fournir un processus d'accès réseau sécurisé, rapide et performant tout en respectant les exigences de sécurité imposées et bénéficier des avantages que ces caractéristiques peuvent offrir. Les caractéristiques des WMN qui influencent sur le processus d'authentification sont:

- **La mobilité des nœuds :** C'est un avantage et inconvénient à la fois, car la mobilité augmente la flexibilité du réseau, et en même temps lorsque le nœud se ré-authentifie au cours de son itinérance, il alourdit le réseau. Les WMN peuvent bénéficier de la stabilité relative des routeurs mesh par rapport aux nœuds des réseaux ad hoc pour diminuer le nombre des messages échangés et économiser l'énergie consommée.
- **La bande passante limitée :** La contrainte de la bande passante exige un processus d'authentification qui ne surcharge pas le canal de transmission par ces messages. Alors, l'authentification dans les WMN ne doit pas être très lourde.
- **Le comportement égoïste des nœuds :** le comportement égoïste des nœuds est un problème majeur dans les réseaux multi sauts en général, et des WMN en particulier, car un nœud intermédiaire peut capturer les données de l'authentification et les utiliser pour un accès illégal au réseau, ou peut ne pas les délivrer pour qu'aucun utilisateur ne puisse s'authentifier, ce qui provoque un déni de service.

3.4. Les différentes solutions d'authentification

Il y a trois catégories principales d'authentification:

- **L'authentification des clients :** Un client du réseau fournit les informations de son identité à une entité d'authentification, celle-ci vérifie si l'identité actuellement correspond à ce client. La différence qui réside dans le terme « client » entre un utilisateur humain et une machine n'est pas très claire dans certaines situations. Prenons l'exemple de client d'un opérateur de téléphonie mobile, il utilise à chaque fois les mêmes informations personnelles enregistrées dans sa carte SIM pour s'authentifier, ce qui rend difficile de distinguer entre l'utilisateur et sa carte SIM du

point de vue authentification.

- **L'authentification des messages :** C'est la deuxième catégorie de l'authentification. Bien que l'authentification des clients assure la légitimité des différentes parties communicantes, l'authentification des messages assure que les messages reçus du point X sont réellement venus du point X, et que ces messages ne sont pas modifiés sur le chemin entre les deux points, en d'autres termes, ce type d'authentification assure l'intégrité des messages.
- **L'authentification mutuelle :** Elle englobe les deux catégories d'authentification précédentes, où chaque nœud s'authentifie à l'autre nœud et signe les messages envoyés à celui-ci.

Ce qui nous intéresse dans ce présent travail est l'authentification des utilisateurs. Il existe plusieurs solutions pour ce faire, nous énumérons les plus connues dans la technologie IEEE 802.11 qui est utilisée dans les réseaux maillés :

3.4.1. La solution WEP

Le WEP (Wired Equivalent Privacy) est la première solution de sécurité intégrée dans le standard 802.11. WEP est un protocole élaborée en 1999 dans le but d'offrir aux réseaux sans fil un moyen d'authentification, de confidentialité et de contrôle d'intégrité. Son principe se base sur un système à clé symétrique, la même clé étant utilisée pour chiffrer et déchiffrer les données. Cette clé de 40 ou 104 bits est partagée par tous les clients du réseau et par le point d'accès. Le mécanisme de chiffrement et de contrôle d'intégrité du WEP se base sur l'algorithme RC4 (Ron's Code 4) conçu en 1987 par Ronald Rivest, un algorithme 10 fois plus rapide que le DES, réalise le chiffrement des données en mode flux (chiffrement par bit ou par octet à la fois).

Deux techniques d'authentification sont associées au WEP : Soit par un système ouvert, où tout client demandant l'authentification sera authentifié, cette technique est utilisé si la facilité de l'utilisation est prioritaire, ou encore là où la sécurité n'est pas cruciale pour un administrateur réseau. La deuxième technique utilise une clé partagée entre les utilisateurs et le point d'accès, cette clé est utilisée pour l'authentification et pour le cryptage symétrique à l'aide de l'algorithme RC4.

Quelques inconvénients du WEP :

- Le WEP présente de nombreuses failles de sécurité, notamment sur la gestion de clés, car le WEP n'introduit pas un mécanisme de gestion de clés, et l'administrateur sera obligé de générer, stocker, distribuer et sécuriser les clés.
- Le principe d'authentification avec WEP est que le point d'accès envoie un challenge de 128 octets en clair et que l'utilisateur doit lui renvoyer chiffré. Si la réponse de l'utilisateur est correcte, alors le point d'accès considère que la station possède la clé WEP. L'attaque peut être réalisée en interceptant le message en clair et la réponse cryptée et déduit la clé de l'authentification.
- Le contrôle d'intégrité souffre aussi de sérieuses failles dues à l'utilisation de l'algorithme CRC32 choisi pour cette tâche. Cet algorithme est fréquemment utilisé pour la détection d'erreurs mais n'a jamais été considéré cryptographiquement sûr pour du contrôle d'intégrité à cause de sa linéarité.

3.4.2. La solution WPA PSK

WPA PSK permet de mettre en œuvre une infrastructure sécurisée basée sur le WPA (Wireless Protected Access) sans mettre en œuvre un serveur d'authentification. Le WPA PSK repose sur l'utilisation d'une clé partagée, appelées *PSK* pour *Pre-shared Key*, renseignée dans le point d'accès ainsi que dans les postes clients. Contrairement au WEP, il n'est pas nécessaire de saisir une clé de longueur prédéfinie. En effet, le WPA PSK permet de saisir une « *passphrase* » (*phrase secrète*), traduite en *PSK* par un algorithme de hachage.

Quelques inconvénients du WPA personnel :

- Si le mot de passe qui est choisi est trop court, un pirate peut lancer une attaque hors ligne pour le retrouver.
- La clé est partagée, tous les utilisateurs peuvent espionner le trafic des autres utilisateurs.

3.4.3. La solution IEEE 802.1X

Introduit en 2001, le standard 802.1x fournit un contrôle d'accès réseau basé sur le port. Un port désigne une entité supervisant le trafic échangé entre un visiteur (le client) et le réseau de communication auquel il désire accéder. Un port non authentifié bloque tous les paquets qui ne transportent pas les informations d'authentification jusqu'à valider son identité. Le standard 802.1X utilise un serveur qui réalise la procédure de l'authentification avec la borne sans fil et valide la demande d'accès (voir la figure 12).

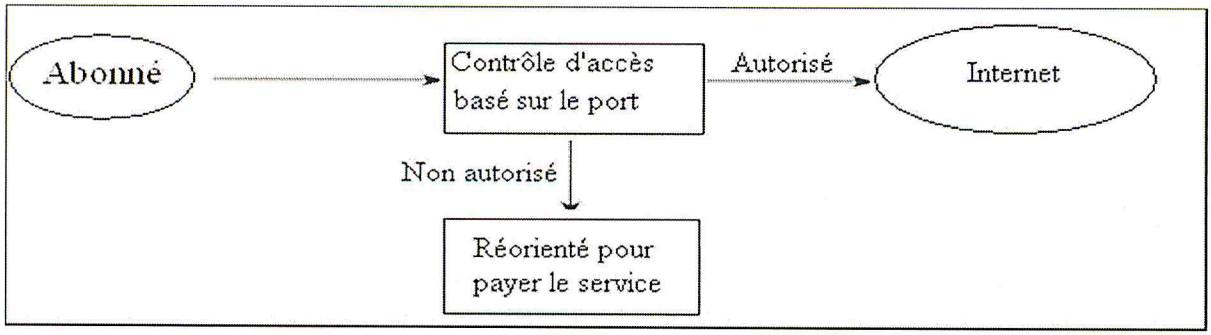

Figure 12: Le contrôle d'accès basé sur le port

Le standard IEEE 802.1X est intégré dans le standard Wi-Fi 802.11i sous le nom WPA Entreprise, bien que 802.1X existe avant 802.11i et il est utilisé dans plusieurs autres solutions de sécurité.

Bien qu'un système d'authentification 802.1X bloque les utilisateurs non autorisés d'accéder au réseau, il supporte aussi:

- **La localisation des utilisateurs :** Une application peut traquer facilement un utilisateur mobile en gardant la trace de son réauthentification à des points d'accès différents. Les informations de localisation peuvent servir à une large variété d'applications. Par exemple, un hôpital peut utiliser cette information pour localiser les médecins et les infirmiers en utilisant des équipements sans fil.
- **Les mécanismes de facturation et de comptabilité:** l'authentification basée sur le port, lorsqu'elle est combinée avec les mécanismes de facturation et de comptabilité, permet aux fournisseurs d'accès Internet (ISP) d'appliquer un accès à Internet basé sur l'horaire. Si l'utilisateur n'est pas autorisé, il peut être dirigé à payer pour le service via une carte de crédit, et puis lui donner un certificat (nom d'utilisateur et mot de passe) que l'abonné peut utiliser lorsqu'il se connecte au système. L'authentification basée sur le port incite les utilisateurs à entrer leur nom d'utilisateur et mot de passe, que le système utilise pour les authentifier. Si le certificat correspond à ce qui est enregistré dans la base de données du système, il sera autorisé à accéder au côté protégé du réseau, qui est l'Internet.
- **L'accès au réseau personnalisé :** En se basant sur la permission affectée au moment de l'authentification, le système peut définir les ressources qu'un utilisateur spécifique est autorisé à utiliser [25].

3.5. Comparaison entre les différentes solutions d'authentification

Solution d'authentification	Robustesse aux attaques	Accès au réseau personnalisé	Rapidité de traitement	Surveillance et suivi des utilisateurs	Authentification mutuelle	Négociation du protocole de sécurité
WEP	Faible (RC4 pour le chiffrement des données, et CRC32 pour l'intégrité des données).	Non (Une clé d'authentification partagée).	Rapide (authentification au niveau du point d'accès).	Non.	Non (Avec WEP, la station mobile n'authentifie pas le point d'accès. Elle ne peut donc pas vérifier si elle s'accorde avec le vrai point d'accès dans le réseau WLAN).	Non.
WPA PSK	Assez fort.	Non (Une clé d'authentification partagée).	Rapide (authentification au niveau du point d'accès).	Non.	Non.	Non.
IEEE 802.1X	Fort.	Oui (l'attribution de différents niveaux d'autorisation à différents utilisateurs).	Selon la charge du serveur (interrogation de serveur d'authentification) .	Oui (En gardant l'historique des utilisateurs mobiles au cours de leur itinérance).	Oui (Grace aux certificats SSL).	Oui (L'utilisateur choisit une méthode d'authentification parmi une liste proposée par le serveur).

Tableau 1: Comparaison entre les différentes solutions d'authentification

D'après la comparaison ci-dessus qui se base sur différents critères, on déduit que la solution WEP est rapide mais obsolète, car des failles de sécurité potentielles lui sont associées. Toute fois l'accès personnalisé au réseau, c.-à-d. l'attribution de différents niveaux de privilèges et le suivi des utilisateurs réseau, est un point essentiel pour partager le réseau en différentes zones (VLAN) selon la confidentialité des données et assurer la sécurité à long terme. Ce point là est pris en considération par la solution d'authentification 802.1X alors que les solutions WEP et WPA PSK n'en tiennent pas compte. Malgré la puissance relative du cryptage de la solution WPA PSK par rapport au WEP, elle ne donne pas la main au client pour choisir un protocole d'authentification selon ses ressources et priorités. En plus, la solution d'authentification 802.1X est actuellement ce qu'il y a de plus sûr en termes de sécurité, elle convient aux WMN grâce à sa flexibilité en termes de gestion des utilisateurs et leurs droits d'accès [26].

3.6.La solution d'authentification choisie pour les WMN

Suite à l'étude précédente, nous avons donc opté pour l'authentification basée sur le port 802.1X.

En plus de la norme IEEE 802.1X, il y a des protocoles et des standards qui sont nécessaires pour former un système d'authentification complet. Ces standards sont élaborés par différents organismes tels que l'IEEE et l'IETF. L'IEEE a conçu le protocole EAPOL, tandis que l'IETF a fournit les RFC de EAP, EAP-Methods et RADIUS. Radius est un protocole qui répond au modèle AAA. Ces initiales résument les trois fonctions du protocole :

- A = Authentication : authentifier l'identité du client ;
- A = Authorization : accorder des droits au client ;
- A = Accounting : enregistrer les données de comptabilité de l'usage du réseau par le client.

Un système d'authentification 802.1X se déroule en 3phases :

3.6.1 Mise en accord sur la politique de sécurité

La première phase permet aux deux parties communicantes de s'accorder sur la politique de sécurité à utiliser. Un point d'accès diffuse dans ses trames *beacon* ou *Probe Response*

(suivant un message Probe Request du client) des éléments d'information, ou IE (Information Element), afin de notifier au client 802.1x les indications suivantes :

- Les méthodes d'authentification supportées (EAP/MD5, EAP/TLS, EAP/PEAP, ….),
- Le protocole de sécurité pour le chiffrement du trafic vers une seule destination (unicast) (CCMP, TKIP, etc.)
- Le protocole de sécurité pour le chiffrement du trafic en diffusion (multicast) (CCMP, TKIP, etc.)

Le schéma de la figure 13 illustre la phase 1 :

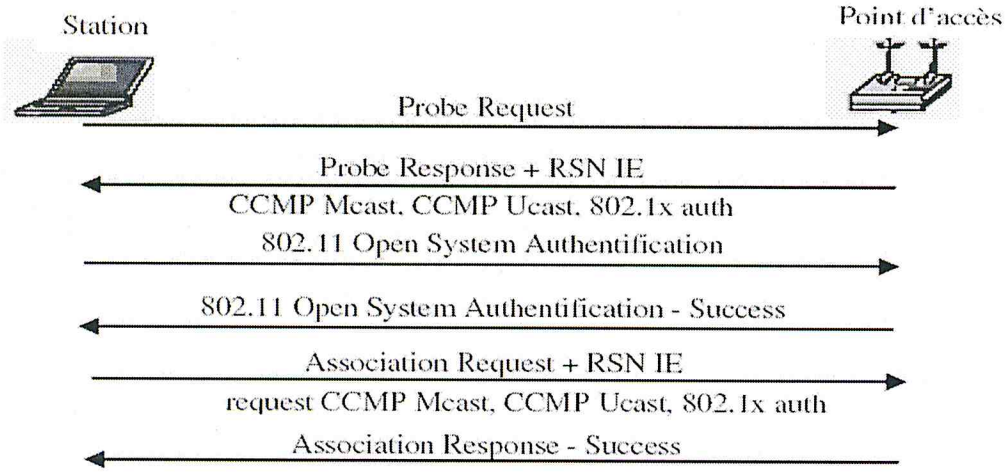

Figure 13: La mise en accord sur la politique de sécurité [27]

3.6.2 Authentification 802.1X

La structure d'IEEE 802.1X :

Le 802.1X utilise un modèle qui s'appuie sur trois entités fonctionnelles :

1. **Le client (supplicant) :** c'est un poste de travail (terminal informatique) demandant un accès au réseau.
2. **L'authentificateur (authenticator) :** c'est l'unité qui contrôle et fournit la connexion au réseau, dans les réseaux sans fil, le point d'accès joue le rôle d'authentificateur.
3. **Le serveur d'authentification (AS) :** il réalise la procédure d'authentification avec l'authentificateur et valide la demande d'accès. Le serveur d'authentification peut être soit un serveur RADIUS dédié ou un simple processus fonctionnant sur le point d'accès.

Comme l'illustre la figure 14, la station et l'authentificateur ont un PAE (Port access entity) qui traite les protocoles et les algorithmes d'authentifications. Le PAE authentificateur contrôle le statut autorisé/non-autorisé de son *Port Contrôlé* dépendamment des résultats du processus d'authentification. Avant que le client ne soit authentifié, l'authentificateur utilise le port non contrôlé pour communiquer avec le PAE client et bloquer tout le trafic à l'exception des messages IEEE 802.1X.

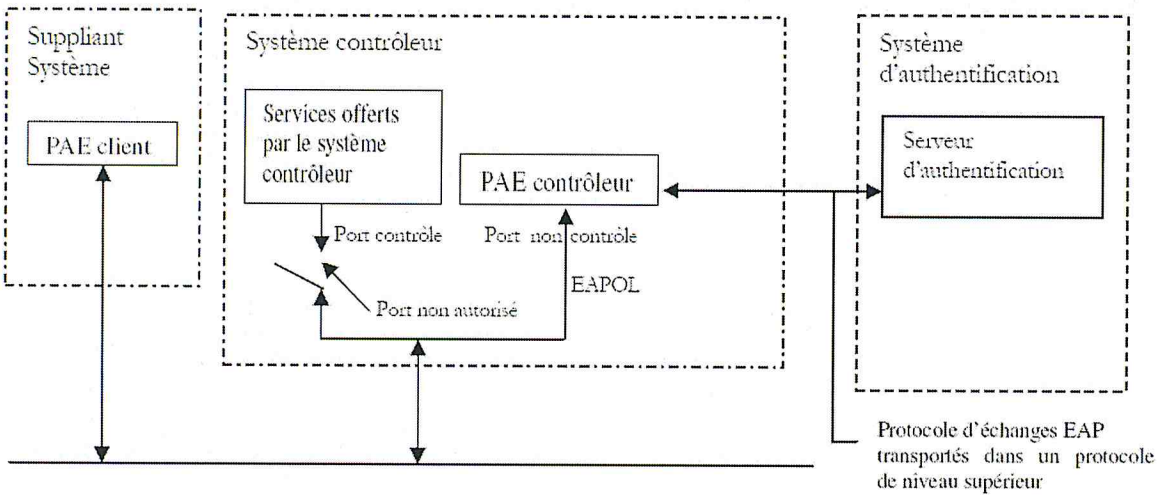

Figure 14: Architecture d'authentification 802.1X [28]

Le standard IEEE 802.1X emploie le protocole EAP qui réalise une enveloppe générique pour de multiples méthodes d'authentifications telles que MD5, TLS, TTLS, PEAP et MS-CHAPv2 (voir la figure 15).

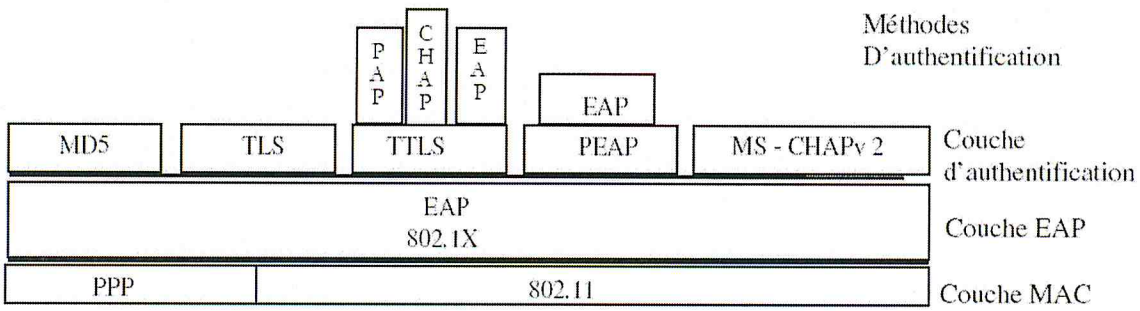

Figure 15: la pile EAP

EAP

EAP (Extensible Authentication Protocol) est un protocole originalement développé pour PPP (Point-to-Point Protocol) comme alternative aux méthodes d'authentification basées sur le mot de passe. Contrairement à ces prédécesseurs, EAP ne définit pas de méthode

d'authentification particulière, mais il définit un moyen de transport général pour les échanges d'authentification. Il repose sur le paradigme de communication challenge-response [29].

Les messages EAP sont eux mêmes encapsulés, le protocole EAP Over LAN (EAPoL) transporte les paquets EAP entre la station et le point d'accès en faisant appel aux messages suivants [29 ,30]:

- EAPoL-Start : permet au client de prévenir l'authentificateur qu'il souhaite se connecter.
- EAPoL-Packet : ce sont ces paquets qui encapsulent les paquets EAP.
- EAPoL-Key : permet l'échange de clé de cryptage.
- EAPoL-Logoff : permet au client de demander la fermeture de sa session.

Le serveur d'authentification et le point d'accès, qui partagent un secret, communiquent en utilisant le protocole RADUIS ; les messages EAP sont transportés comme des attributs par le protocole RADUIS qui contient un mécanisme pour vérifier l'authenticité et l'intégrité des paquets échangés.

Le format d'un paquet RADUIS est illustré par la figure 16; le champ *Authenticator* contient un résumé HMAC-MD5 du paquet, calculé avec le secret partagé. HMAC-MD5 (Hash-based Message Authentication Code – Message Digest Code 5) est méthode de vérification de l'intégrité des messages en utilisant la fonction de hachage MD5.

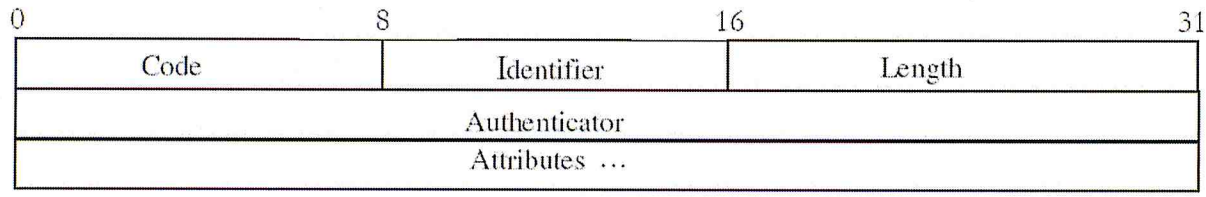

Figure 16: Format d'un paquet RADIUS

L'insertion d'une station mobile dans un environnement 802.1X se déroule de la manière suivante (voir la figure 17) :

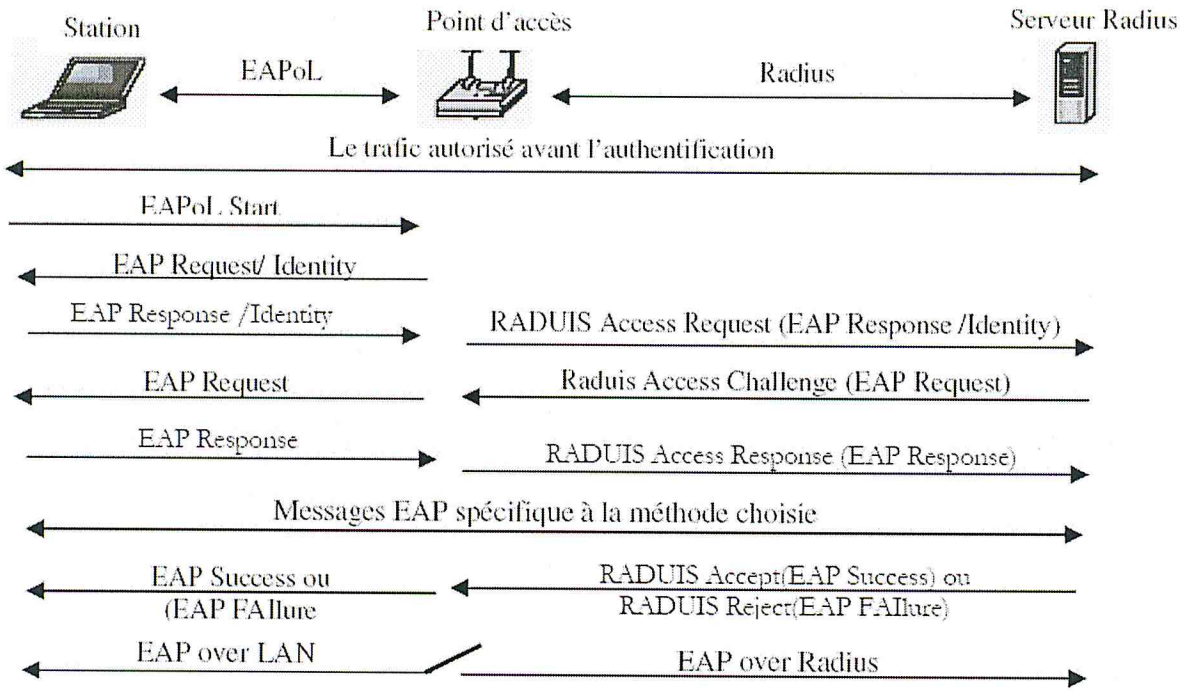

Figure 17: Echange des messages 802.1x et EAP [30]

Après la phase d'association avec le point d'accès, le client envoie le message EAPoL-Start au point d'accès pour initialiser le processus d'authentification. Le point d'accès, envoie à l'utilisateur une requête d'identité EAP-Request/Identity. La station mobile produit en retour une réponse EAP-Response/Identity. Cette réponse comporte l'identité du client et les méthodes d'authentification supportées.

Le point d'accès transmet au serveur d'authentification le message EAP Response/Identity encapsulé dans une requête RADIUS. À partir de ce moment, les échanges dépendent de la méthode d'authentification choisie afin de générer une clé maîtresse (Pairwise Master Key – PMK) si elle est génératrice de clés.

Durant l'échange des messages EAP (requêtes et réponses) entre le serveur d'authentification et la station mobile, le point d'accès agit comme un simple relais passif.

Le serveur d'authentification prend la décision d'accepter ou de refuser l'accès au réseau, et on aura 3 cas:

- Si l'authentification est réussie, RADUIS envoie le message EAP-Success à la station mobile pour indiquer le succès de la procédure d'authentification. Le *port contrôlé* passe alors à l'état autorisé.

- Si l'authentification a échoué le message EAP-Failure sera envoyé, dans ce cas le port reste dans l'état non autorisé.
- Si l'authentification est réussie et la station mobile veut se déconnecter du point d'accès courant, elle lui envoie un paquet EAPoL-Logoff, le port contrôlé passe alors à l'état non autorisé.

3.6.3 Hiérarchie et distribution des clés

La sécurité des transmissions repose essentiellement sur des clés secrètes. Chaque clé a une durée de vie limitée et de nombreuses clés sont utilisées et organisées dans une hiérarchie. Après une authentification réussie, des clés temporaires (de sessions) sont créées et régulièrement mises à jour jusqu'à la fermeture de la connexion. La génération et l'échange des clés utilisent deux Handshakes:

- Le 4-Way Handshake pour la dérivation de la PTK (Pairwise Transient Key) et de la GTK (Group Transient Key),
- Le Group Key Handshake pour le renouvellement de la GTK.

Avec un protocole dit *4-way Handshake* (négociation en quatre passes), le client et la borne sans fil calculent une clé appelée *Pairwise Transient Key* (PTK). Pour ce faire, ils utilisent une formule (hachage) qui inclut la PMK (Pairwise Master Key) (qu'ils connaissent tous les deux), leur adresse MAC et des nombres aléatoires échangés pendant le 4-way handshake. À ce stade, la communication est toujours portée par le protocole EAP dans des requêtes EAPoL-Key. La PTK est différente pour chaque poste connecté à la borne.

La dérivation de la PMK dépend de la méthode d'authentification choisie :

- Si la PSK (Pre-Shared Key) est utilisée, PMK = PSK. La PSK est générée à partir de la phrase secrète (composée de 8 à 63 caractères) ou directement à partir d'une chaîne de 256 bits, cette méthode est adaptée pour les particuliers n'ayant pas de serveur d'authentification,
- Si un serveur d'authentification est utilisé, la PMK est dérivée de la MK issue de l'authentification 802.1X [27].

La PMK en elle même n'est jamais utilisée pour le chiffrement ou le contrôle d'intégrité. Néanmoins, elle est utilisée pour la génération des clés de chiffrement temporaires, pour le trafic d'une machine, il s'agit de la PTK (Pairwise Transient Key).

La taille de la PTK dépend du protocole de chiffrement choisi : 512 bits pour TKIP et 384 bits pour CCMP.

La PTK consiste en plusieurs clés temporelles dédiées (la figure 18):

- **KCK** (Key Confirmation Key – 128 bits) : Clé pour authentifier les messages (MIC) Durant le 4-Way Handshake et le Group Key Handshake,
- **KEK** (Key Encryption Key – 128 bits) : Clé pour la confidentialité des données durant le 4- Way Handshake et le Group Key Handshake,
- **TK** (Temporary Key – 128 bits) : Clé pour le chiffrement des données (utilisé pour le calcul des données d'intégrité dans le protocole CCMP)
- **TMK** (Temporary MIC Key – 2x64 bits) : Clé pour l'authentification des données (utilisée seulement par Michael dans TKIP). Une clé dédiée est utilisée pour chaque sens de communication.

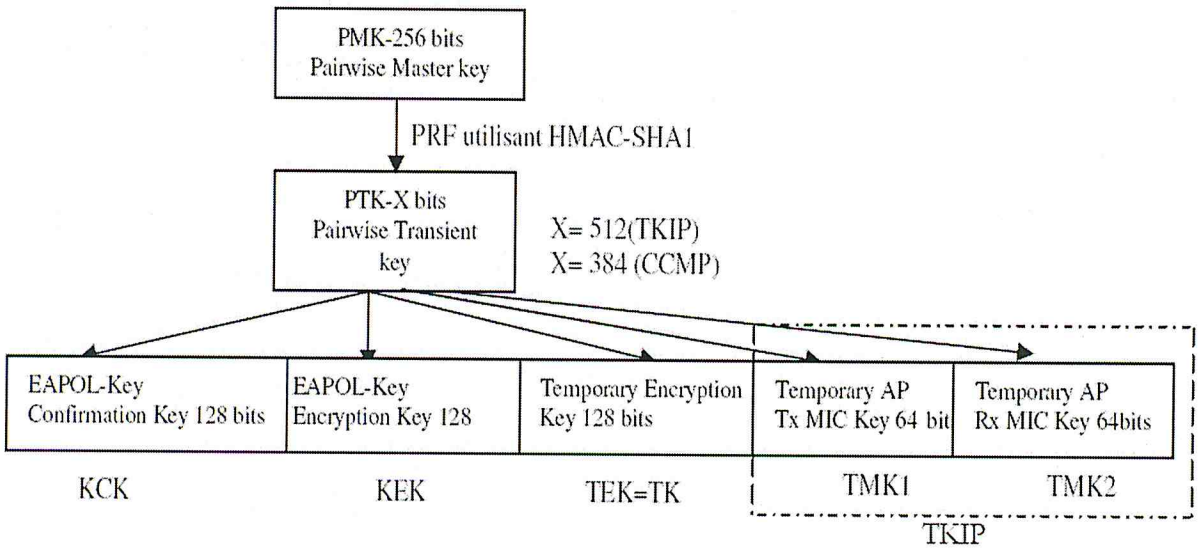

Figure 18: Hiérarchie de clé Pairwise [27]

Le 4-way handshake :

Le 4-Way Handshake, initié par le point d'accès, permet de:

- Confirmer la connaissance de la PMK par le client,
- Dériver une nouvelle PTK,
- Installer les clés de chiffrement et d'intégrité,
- Chiffrer le transport de la GTK,
- Confirmer la suite de chiffrement choisie.

Le Group Key Handshake est seulement nécessaire en cas de dé-association d'un client ou lors du renouvellement de la GTK suite à une demande client.

Conclusion

Dans ce chapitre, nous avons étudié le problème d'authentification dans les réseaux maillés, et les solutions d'authentification existantes, et nous avons opté pour la solution IEEE 802.1X car elle est la plus adéquate pour les réseaux maillés sans fil du point de vue sécurité et flexibilité de gestion des utilisateurs et leurs droits d'accès. Puis, nous avons discuté l'architecture de cette solution et les différents standards et protocoles associés ainsi que les phases de déroulement d'un tel processus.

Dans le prochain chapitre, nous aborderons la mise en œuvre d'un réseau maillés et nous appliquerons notre solution d'authentification tout en expliquant les différentes étapes d'installation et de configuration. Enfin, nous analyserons la solution et nous ferons des tests afin de déduire l'intérêt d'une telle solution et ses éventuels points faibles.

Chapitre 4: Déploiement et tests

Introduction

La solution d'authentification IEEE 802.1X et son modèles AAA offrent plusieurs avantages, car la gestion des utilisateurs réseaux et des droits d'accès deviennent plus souples et plus robustes.

Dans ce chapitre, nous abordons la partie implémentation, où nous commençons par le déploiement d'un réseau maillé sans fil. Ce réseau sera lié au réseau LAN du CERIST par quelques passerelles (gateways). Puis, nous mettons en œuvre la solution d'authentification basée sur un serveur RADIUS. Ensuite, nous présenterons une proposition de solution d'authentification répartie plus adaptée aux réseaux maillés.

4.1.L'architecture adoptée

Nous avons mis en place des routeurs pour construire le backbone du réseau maillé, et des points d'accès pour lier les utilisateurs au réseau (voir la figure 19).

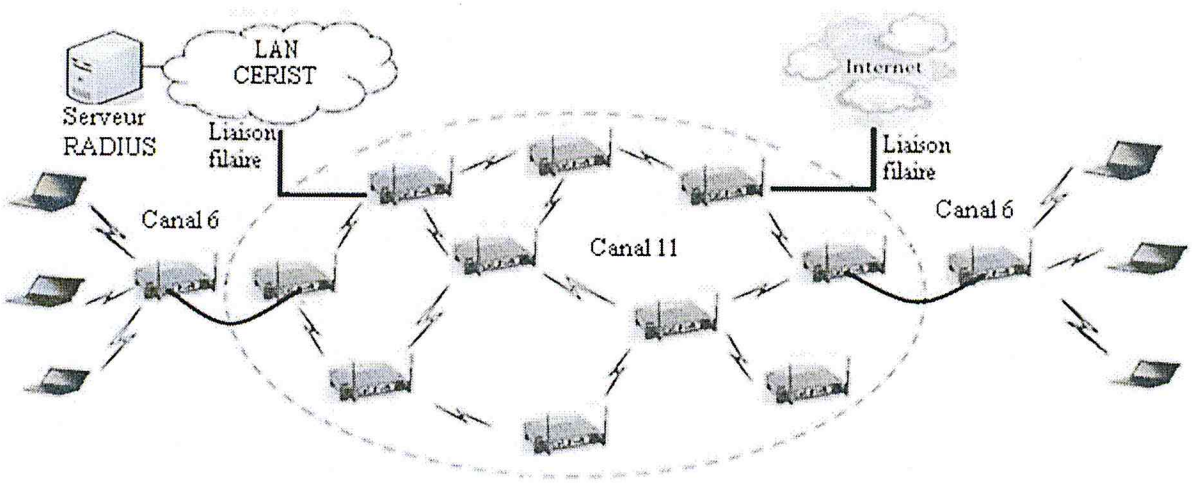

Figure 19: L'architecture du réseau

Le schéma précédent, que nous avons déployé, prend en considération :

- La disponibilité du service Internet par l'utilisation des passerelles.
- La sécurité physique du serveur RADIUS placé au sein du réseau LAN du CERIST.
- Le choix des canaux de transmission différents pour les réseaux adjacents afin d'éviter les interférences.
- L'utilisation de NAT (Network Address Translation) pour minimiser le nombre

des adresses publiques utilisées.

- L'utilisation de routeurs Linksys pour connecter les clients au réseau mesh, car ce type de routeurs ne contient qu'une seule interface sans fil.
- L'utilisation du protocole OLSR pour connecter les routeurs mesh, car il est le plus utilisé des protocoles de routage dans les réseaux maillés, en plus, il supporte l'ajout dynamique d'autres réseaux sans modifier manuellement la table de routage de chaque routeur [31].

4.2.Installation du réseau mesh

4.2.1. Matériels et logiciels nécessaires

4.2.1.1. Matériels

Nous avons utilisé des routeurs sans fils tels que Linksys WRT54G (à partir de la version 4.0) ou Linksys WRT54GL (version 1.0 ou 1.1). Les routeurs Linksys WRT54GL sont actuellement parmi les routeurs les plus populaires pour déployer les réseaux mesh. Un ordinateur est nécessaire pour mettre en œuvre le serveur RADIUS, et quelques laptops dotés des interfaces Wi-Fi pour tester le fonctionnement du réseau.

4.2.1.2. Logiciels

Nous avons utilisé la version 2.4 du firmware DD-WRT (téléchargeable depuis http://www.dd-wrt.com/dd-wrtv2/downloads.php Sélectionner *stable* --> *dd-wrt.v23 SP2* --> *standard* → *dd-wrt.v23_wrt54g.bin*), car elle supporte le protocole OLSR, qui s'occupe de la fonctionnalité de routage dans le réseau maillé.

4.2.2. Planification du réseau maillé

Les réseaux maillés sans fil ont besoin d'être bien planifiés. La configuration et la gestion du réseau est facile lorsque le réseau est petit. Cependant, les réseaux sont flexibles et évolutifs et s'ils ne sont pas planifiés dès le départ, la gestion devient très difficile.

4.2.2.1. Choix de la topologie réseau

Le choix de la topologie est crucial pour la performance du réseau. Alors, nous proposons d'utiliser plusieurs gateways Internet pour augmenter la disponibilité du service.

4.2.2.2. Allocation des canaux de transmission

L'allocation du canal de transmission est une tâche simple, lorsque les nœuds sont sur le même canal ils peuvent communiquer. Nous avons choisit, par exemple, le canal 11 pour le réseau mesh dorsal, et les canaux 1 et 6 pour les clients afin de diminuer l'interférence entre les différents réseaux. Nous attribuons des canaux différents à des réseaux adjacents (Voir la figure 20).

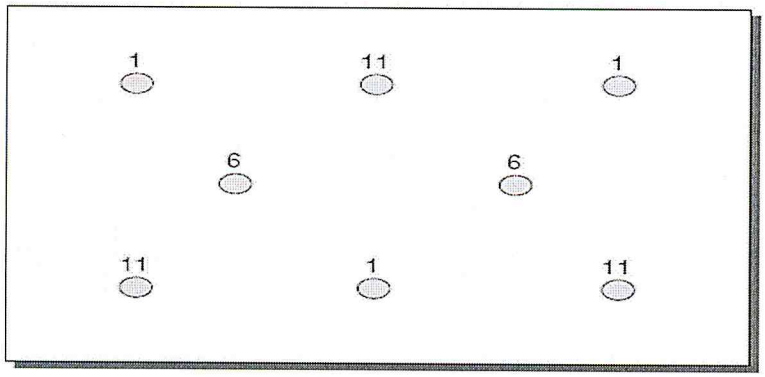

Figure 20: Allocation des canaux de transmission

4.2.2.3. Plan d'adressage

Les adresses sont attribuées selon le RFC 1918 [32] qui décrit les plages d'adressage privées. Le schéma d'adressage assure que chaque ordinateur ou nœud sur le réseau possède une adresse unique. Selon le RFC 1918, les sous plages d'adressage privées sont:

- 10.0.0.0 - 10.255.255.255 (10/8)
- 172.16.0.0 - 172.31.255.255 (172.16/12)
- 192.168.0.0 - 192.168.255.255 (192.168/16)

Une fois le sous réseau choisi, nous proposons une méthode d'affectation des adresses IP et la suivons rigoureusement. Un exemple de méthode d'affectation des adresses IP est montré dans la table 2, et un exemple d'utilisation de cette méthode est montré dans la figure 21.

Type	Sans fil	Ethernet
Nœud mesh	10.1.1.X	10.2.X.1
Point d'accès	10.2.X.Y	10.2.X.Y
Utilisateur	10.2.X.Y	10.2.X.Y

Tableau 2: Méthode d'attribution des adresses IP

Remarque :

Le nombre X est statique, mais le nombre Y est attribué dynamiquement aux points d'accès et aux clients par un serveur DHCP au niveau du routeur mesh associé.

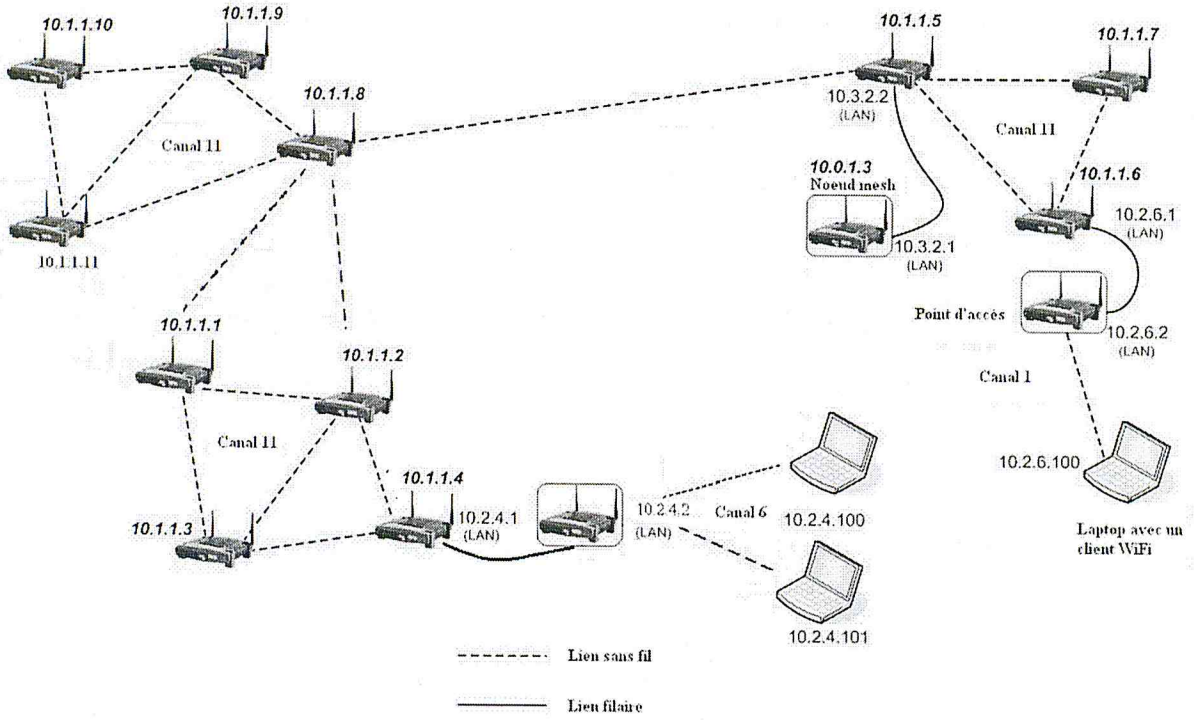

Figure 21: Plan d'adressage du réseau

4.2.3. Préparation des routeurs mesh

Lors de l'ouverture du boitier on trouve les composants suivants (voir la figure 22).

Figure 22: Composants d'un routeur Lynksys WRT54GL

Les étapes suivantes sont nécessaires pour préparer le nœud mesh :

- Mise à niveau du firmware pour tous les nœuds mesh et les points d'accès.

- Configuration :
  - des adresses IP sans fil,
  - du protocole OLSR,
  - de la sécurité des communications sans fil en utilisant 802.1X pour les clients et WEP pour les routeurs mesh,
  - Et du serveur DHCP.

4.2.3.1. Mise à niveau du firmware

Cette étape nous permet d'installer le firmeware choisi et qui répond à notre besoin.

1. Télécharger le firmware DD-WRT.
2. Connecter au routeur par câble LAN.
3. S'assurer que la machine a obtenu une adresse IP dynamique.
4. Aller à *Administration* → *Upgrade* et parcourir vers le firmware téléchargé et appuyer sur *Upgrade*.

4.2.3.2. Configuration des routeurs

1. Sélectionner *Ad hoc* dans *Wireless Mode*, et créer un réseau mesh (SSID) sous n'importe quel nom (*MESH* dans notre cas), l'essentiel que tous les nœuds mesh se connectent au même réseau. Dans *Network configuration*, cocher *Unbrigded* pour les routeurs mesh et *Bridged* pour les points d'accès (voir la figure 23).

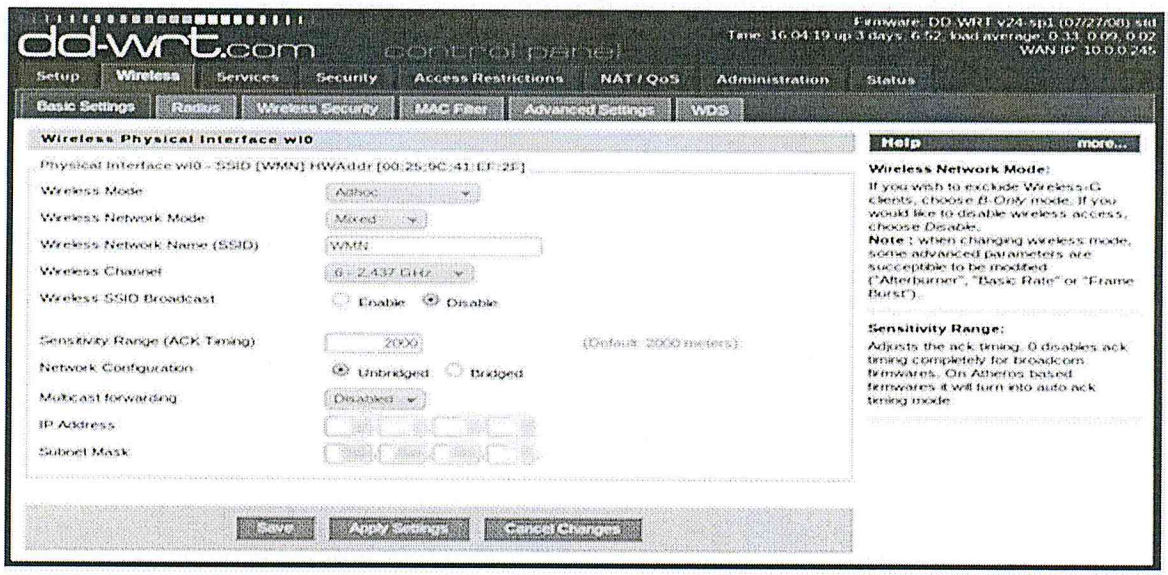

Figure 23: Configuration du réseau mesh

2. Affecter une adresse manuelle à l'interface LAN selon le plan d'adressage choisi dans l'étape précédente, et laisser l'adresse WAN dynamique.
3. Choisir OLSR comme *Operating mode,* et affecter un sous réseau pour les messages HNA de la forme : 10.2.X.0 255.255.255.0, ou 0.0.0.0 0.0.0.0 (Chemin par défaut) pour les gateways.
4. Appliquer le protocole de sécurité WEP pour la communication entre les nœuds mesh (La sécurité des communications Ad Hoc est un point faible de ce type de réseaux par ce qu'elle utilise le protocole WEP, mais des recherches sont lancées pour trouver des méthodes plus fiables) (voir la figure 24).

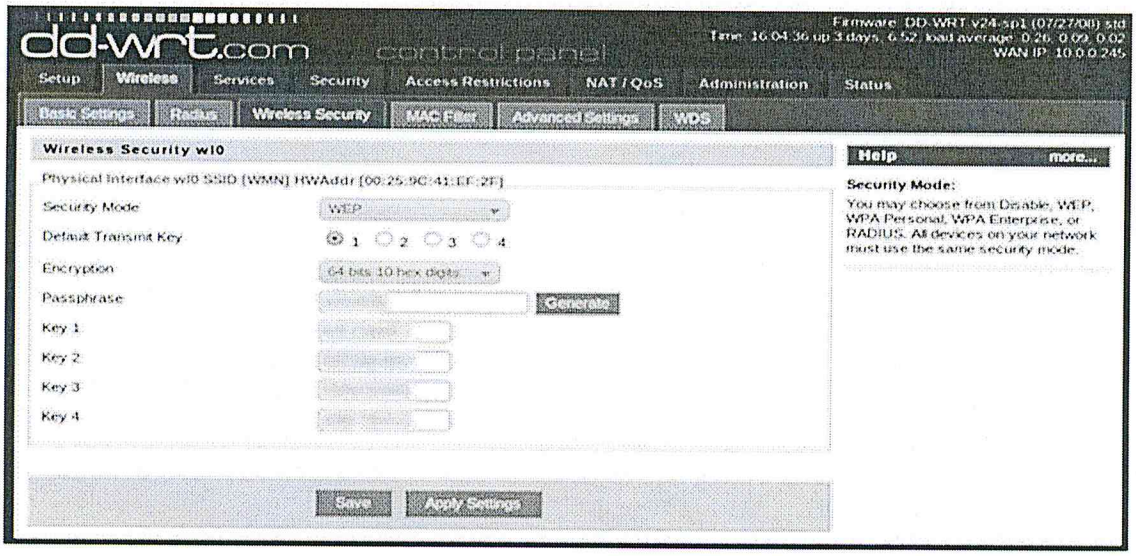

Figure 24: Configuration du protocole WEP

5. Ajuster les points d'accès pour utiliser un serveur RADIUS distant afin d'authentifier les utilisateurs.
6. Activer un serveur DHCP au niveau de chaque nœud mesh pour affecter des adresses dynamiques aux points d'accès et aux utilisateurs associés.
7. Injecter la commande suivante au niveau des gateway pour faire le NAT et donc le réseau mesh pourra se connecter à Internet :
   iptables -t nat -A POSTROUTING -o vlan1 -j MASQUERADE
8. Lier les ports WAN des gateways à internet et les ports WAN des points d'accès aux ports LAN des routeurs mesh par des câbles RG45.

4.3.Déploiement de la solution IEEE 802.1X

L'acteur principal dans une telle solution est le serveur RADIUS, il doit donc avoir l'autorité qui contrôle l'accès au réseau. Nous avons installé le logiciel open source FreeRadius.

4.3.1. Configuration du serveur FreeRadius

La configuration du serveur FreeRadius est faite par la modification des 4 fichiers principaux: radiusd.conf, eap.conf, client.conf et users. Dans notre distribution Linux (Ubuntu 10.10), seuls les fichiers clients.conf et users vont être modifiés car la configuration originale des autres fichiers est adéquate pour notre contexte.

4.3.1.1. Le fichier radiusd.conf

Ce fichier de configuration regroupe l'ensemble des paramètres nécessaires pour décrire le type de fonctions souhaitées. Il existe un très grand nombre d'options et de modules. Nous ne les décrirons pas exhaustivement, mais nous verrons les plus intéressants que nous replacerons dans notre contexte. Le fichier radiusd.conf est composé de plusieurs parties :

- Paramètres du service Radiusd.
- Section de déclaration des modules.
- Section Instantiate.
- Section Authorize.
- Section Authenticate.
- Section Pre-Acct.
- Section Post-Auth.
- Section Pre-Proxy.
- Section Post-Proxy.

Ce qui nous intéresse ici ce sont les sections Autorise et Authenticate qui doivent être de la forme:

```
authorize {
chap
eap
files
}
```

```
authenticate {
Auth-Type CHAP {
chap
}
eap
}
```

Ces deux sections peuvent être séparées dans un fichier à part (dans notre version le fichier est *repertoire_de_configuration/sites-available/default*).

4.3.1.2. Le fichier eap.conf

Le fichier eap.conf est inclus dans radiusd.conf au moyen d'une instruction INCLUDE. On y trouve le module eap qui a pour fonction d'implémenter les couches EAP. Ce module eap est lui-même constitué de sous-modules qui correspondent chacun à un protocole (couche EAP-Method). Le format général est le suivant :

```
eap {
options de configuration.
Protocole-eap1 {
configuration du protocole1.
.....
}
protocole-eap2 {
configuration du protocole2
....
}
}
```

Parmi les options de configuration, on trouve le config-item default_eap_type. Il contient le protocole par défaut proposé par le serveur dans l'étape de négociation de protocole.

La section eap doit contenir : default_eap_type = peap.

Le module peap peut être configuré ainsi :

```
peap {
default_eap_type = mschapv2
copy_request_to_tunnel = no
use_tunneled_reply = no
```

```
}
mschapv2 {
}
```

4.3.1.3. Le fichier client.conf

Ce fichier a pour fonction de définir les secrets partagés avec chaque équipement réseau. Cela revient à déclarer quels matériels (NAS) peuvent soumettre des requêtes au serveur FreeRadius. Tout autre matériel sera refusé et le message suivant sera émis dans le fichier de journalisation : *Ignoring request from unknown client adresse-ip-du-NAS*

Pour chaque NAS, la syntaxe est la suivante :

```
client adresse-ip {
secret = le-secret-partagé
shortname = nom
}
```

Tel que :

- *adresse-ip* est l'adresse IP du commutateur ou de la borne sans fil.
- *le-secret-partagé* est le secret partagé entre le serveur et cet équipement. On peut définir un secret différent pour chaque équipement. Il faudra enregistrer le même secret dans l'équipement.
- *nom* est un alias que l'on donne à cet équipement. Il peut être choisi librement et n'est pas forcément égal au nom DNS de l'équipement. Il est important de donner un nom différent pour chaque équipement car ils apparaîtront dans les journaux de FreeRadius pour indiquer à partir d'où un poste a réussi à s'authentifier.

Dans notre cas nous ajoutons une entrée par gateway car les points d'accès ne sont pas visibles par le serveur RADIUS à cause des services NAT, et seules les adresses des gateway sont visibles. Voici une entrée pour le gateway qui porte l'adresse sans fil 10.1.1.5 et l'adresses WAN 10.0.0.245 :

```
client 10.0.0.245/16{
secret = **********
shortname = R5
}
```

4.3.1.4. La base users

Le fichier *users* est la base de données locale. Elle est utilisée soit comme base d'autorisations, soit comme base d'authentification ou les deux à la fois. Il s'agit d'un simple fichier texte.

Ce fichier est constitué d'une liste d'entrées, chacune correspondant à un utilisateur ou à une machine. Le format de ces entrées est :

identifiant <config-items>,<check-item>,....<check-item>
reply-item,
reply-item,
.....
reply-item
Dans notre cas il suffit d'ajuter un client comme suit:
"mourad" User-Password = "**********"
"chemsso" User-Password = "********"

4.3.1.5. Implémentation du module SQL sur un serveur FreeRadius :

Pour pouvoir intégrer une base de donnée MySQL et la configurer de façon à ce que le serveur FreeRadius l'utilise pour authentifier et autoriser les clients et les points d'accès, les packages suivants doivent être installés :

libdbd-mysql-perl (4.016-1)
libhtml-template-perl (2.9-1)
mysql-client-5.1 (5.1.49-1ubuntu8.1)
mysql-client-core-5.1 (5.1.49-1ubuntu8.1)
mysql-server (5.1.49-1ubuntu8.1)
mysql-server-5.1 (5.1.49-1ubuntu8.1)
mysql-server-core-5.1 (5.1.49-1ubuntu8.1)

Une fois ces packages installés, on passe à la phase de configuration. On enlève les commentaires de la ligne *$include sql.conf* dans le fichier *radiusd.conf*. Puis, on modifie dans le fichier *sql.conf* l'adresse IP, le login, le mot de passe et le nom de la base de données SQL.

Le fichier doit être similaire à celui-ci :

sql {

```
database = "mysql"
driver = "rlm_sql_${database}"
server = "localhost"
login = "radius"
password = "radpass"
radius_db = "radius"
readclients = yes
.....}
```

On prend le fichier qui se trouve dans le chemin /etc/raddb/sites-enabled/default. On modifie la section *authorize* et *accounting,* on enlève les commentaires de la line sql.

Le fichier doit être similaire à ça:

```
authorize {
        preprocess
        chap
        mschap
        suffix
        eap
        sql
        pap
}
accounting {
        detail
        sql
}
```

Dans le package télécharger: freeradius-server-2.x.x on accède au dossier /raddb/sql/mysql/ où on trouve les deux fichiers: **schema.sql** et **nas.sql**. Si ces deux fichiers ne sont pas disponible dans le package téléchargé, il y on a pleinement sur Internet, il suffit de les télécharger.

Une fois que ces fichiers sont sur le disque dur, on ouvre un terminal et on accède au mode MySQL par la commande : *mysql -u login -ppassword*, et on crée une base de données nommé par exemple *radius* à l'aide de la commande : *create database radius ;*

Remarque :

Le nom choisi pour la base de données doit être similaire à celui introduit dans le fichier sql.conf.

On quitte le mode mysql et on injecte les deux commandes suivantes :

mysql --user=root --password=<le lien où se trouve le fichier schema.sql sur le disque dur>
mysql --user=root --password=<le lien où se trouve le fichier nas.sql sur le disque dur>
A partir de cette liste ce qui nous intéresse c'est les deux tables nas et radcheck, nas joue le rôle du fichier clients.conf où on ajoute les clients RADIUS (point d'accès), et radcheck joue le rôle du fichier *users* où on ajoute les utilisateurs.
Les point d'accès sont ajoutés à la table *nas* par la commande « *insert into nas (nasname, shortname, secret) values ('@IP-du-NAS', Password, 'secret-partager');* »

nasname est l'adresse IP du point d'accès.

shortname est par default Password.

secret est le secret partagé entre le point d'accès et le serveur radius.

Puis, on ajoute les utilisateurs à l'aide de la commande « *insert into radcheck (username, attribute, op, value) values ('username', 'Cleartext-Password', ':=' , 'password');* ».

4.3.2. Configuration des points d'accès

Étant donnée la diversité des équipements réseau présents sur le marché, il n'est pas possible de donner des exemples pour tout ce qui existe. Pour configurer les bornes Linksys WRT54GL avec le firmware DD-WRT le mode *WPA2 Entreprise* est choisi comme mode de sécurité et *TKIP* comme algorithme de WPA, et l'adresse IP du serveur RADIUS le secret partagé sont ensuite saisis, les autres champs ne sont pas modifiés (voir la figure 25).

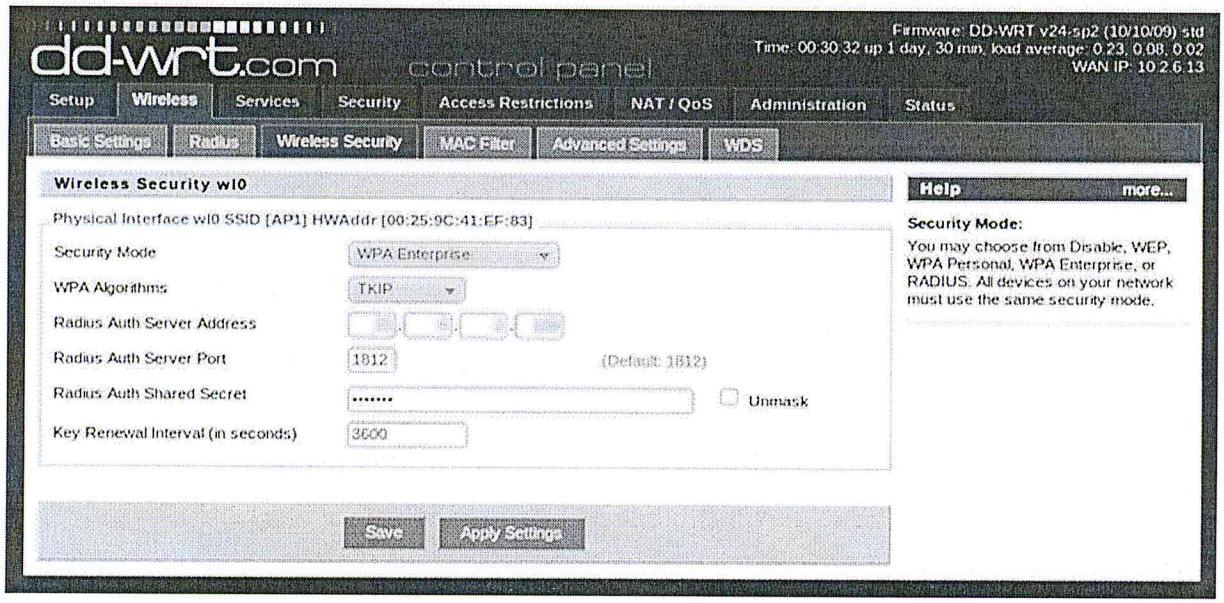

Figure 25: Configuration des bornes Lynksys avec le firmware DD-WRT

4.3.3. Configuration des supplicants

4.3.3.1. Client d'authentification natif de Windows:

Afin d'intégrer un équipement client dans un système d'authentification basé sur le port 802.1X, le client doit avoir un logiciel client 802.1X et une sorte de connexion réseau, comme Wi-Fi ou Ethernet. Le logiciel client 802.1X doit supporter le type d'EAP-Method utilisé. A titre d'exemple, Windows XP et Vista supportent par défaut 802.1X, le choix des EAP-Methods est limité à EAP-TLS et EAP-PEAP. Si on veut ajouter d'autres EAP-Methods, on a probablement besoin d'installer des logiciels additionnels ou utiliser des supplicant différents.

Pour configurer le client Windows, les étapes suivantes sont nécessaires :

1. Ouvrir la fenêtre « Connexions Réseau ».
2. Sélectionner la connexion sans fil à utiliser, ça correspond à une carte sans fil installée sur le périphérique client.
3. Sous « Gestion du réseau », sélectionné « Modifier les paramètres de cette connexion ».
4. Sélectionner l'onglet "Réseaux sans fil".
5. Sélectionner le réseau sans fil qu'on veut configurer pour 802.1X, et cliquer sur le bouton « Propriétés ». la liste des réseaux listés dans la fenêtre correspondante à des réseaux sans fil spécifiques. La configuration 802.1X sera appliquée seulement sur le réseau sans fil qu'on a choisi (voir la figure 26).

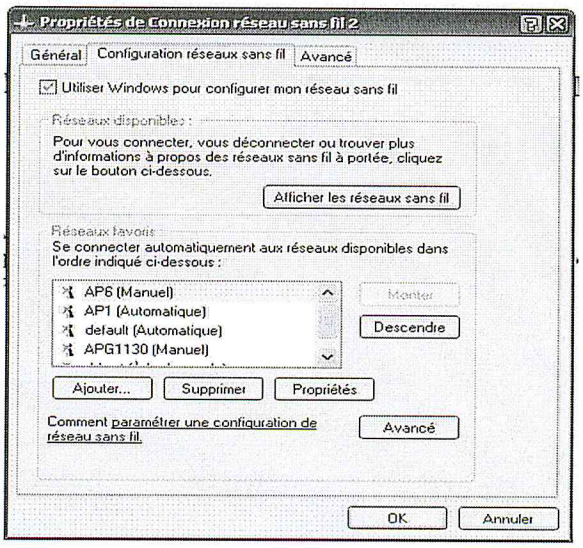

Figure 26: Chois de réseau

6. Sélectionner l'onglet « Authentification » (voir la figure 27).
7. Cocher la case « Activer l'authentification IEEE 802.1X pour ce réseau ».
8. Sélectionner le type EAP (EAP Méthod) qu'on veut implémenter, comme PEAP.
9. Cliquer sur le bouton « Propriétés » pour configurer le type EAP choisi.
10. Cliquer « OK ».

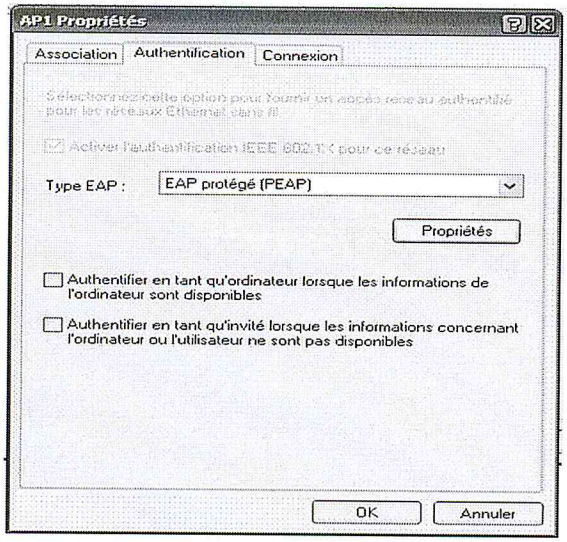

Figure 27: Choix d'EAP-Method

4.3.3.2. wpa_supplicant sous Windows

Ce supplicant est le plus adapté sous Windows pour notre cas grâce à sa légèreté et stabilité. En plus, il supporte plusieurs méthodes d'authentification. Pour s'authentifier avec se supplicant les étapes suivantes sont nécessaires :

- Dans l'anglet *manage networks,* ajouter l'interface sans fil préférée, puis ajouter le nouveau réseau (voir la figure 28).

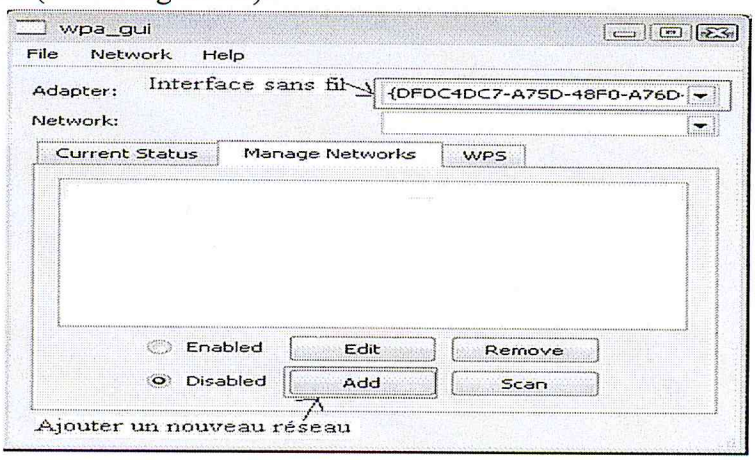

Figure 28: Ajout d'un nouveau réseau on utilisant wpa_supplicant

- Une fenêtre s'ouvrira à que l'utilisateur pour saisir ses informations d'authentification (voir la figure 29).

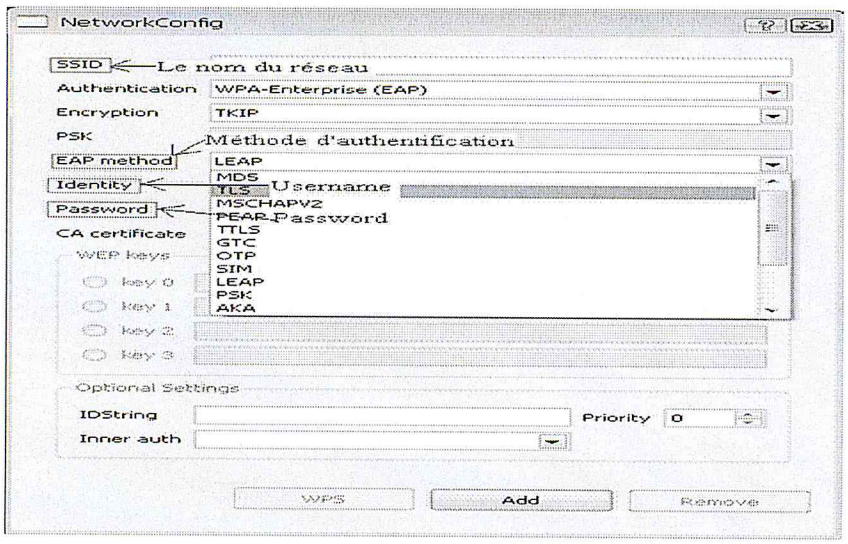

Figure 29: Saisir les informations d'utilisateur

- Une fois les informations sont bien saisies, on enregistre les informations d'authentification à propos de ce réseau.

4.3.3.3. wpa_supplicant sous Linux:

Wpa_supplicant est une implémentation open source de supplicant IEEE 802.11i (WPA2) pour linux, BSD, et Microsoft Windows. Il supporte presque toutes les EAP-Metods. La configuration de client wpa-supplicant est relativement simple ; on ouvre la fenêtre de gestion des réseaux, on clique sur le réseau concerné, sous l'onglet « Wireless Security » on choisit l'EAP-Method et on saisit le login et le mot de passe (voir la figure 30).

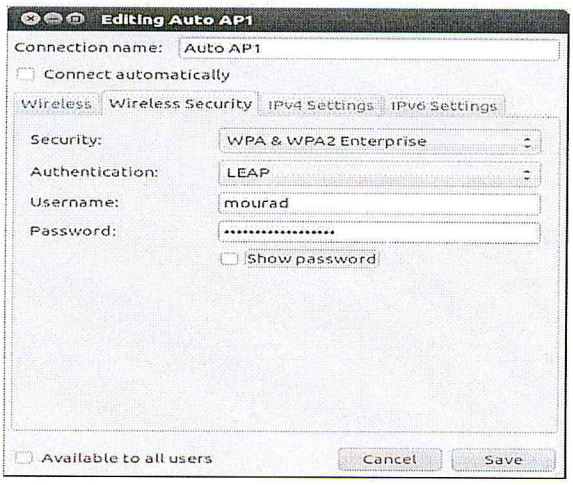

Figure 30: Configuration de wpa-supplicant sous Linux Ubuntu

4.4.Scénario d'application

Les utilisateurs peuvent accéder au réseau par différents matériels, il suffit que le matériel possède une carte réseau sans fil qui supporte l'authentification 802.1x et un supplicant.

4.4.1. L'ajout des utilisateurs et des points d'accès

A la réception d'un utilisateur, un compte lui est créé au niveau de la base de données que le serveur va interroger. Nous avons développé une application PHP qui sert à la gestion des utilisateurs. Cette application interroge la base de données MySQL pour gérer les utilisateurs intervenant et minimiser le temps d'écrire des requêtes SQL en ligne de commande (voir la figure 31).

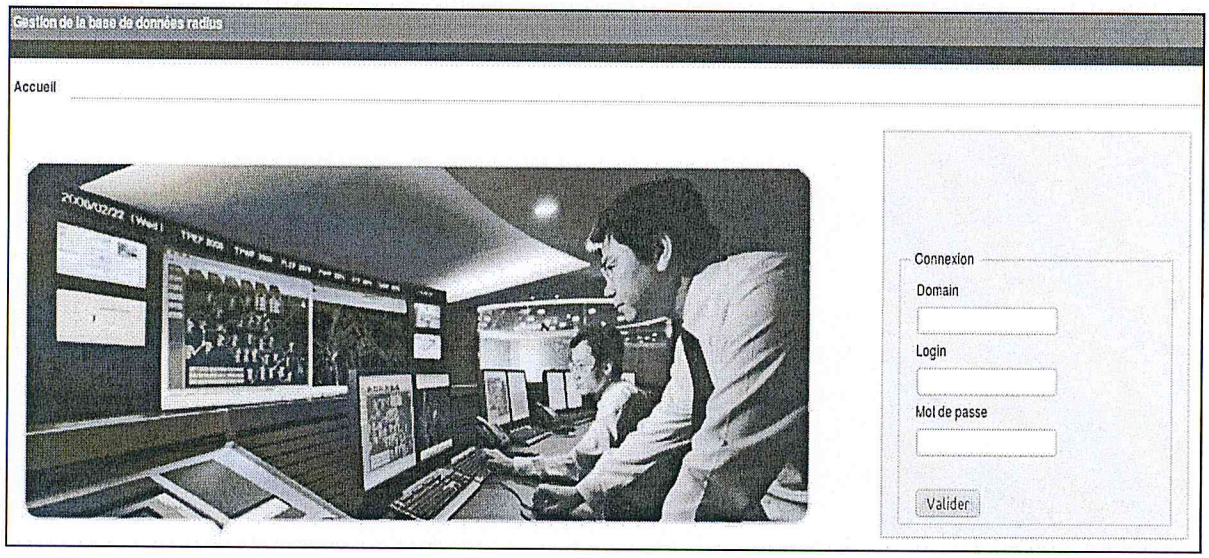

Figure 31:L'interface de gestion de la base de données FreeRADIUS

4.4.2. L'authentification

Après la création du compte, l'utilisateur peut accéder au réseau à l'aide des informations de son propre compte. Alors, si l'utilisateur utilise un système Windows, il peut s'authentifier en utilisant le gestionnaire par défaut des réseaux sans fil, de plus il peut installer l'un des supplicants 802.1x tels que (XSupplicant, wpa_supplicant, etc..). Sous windows XP il est préférable d'installer l'un des supplicants afin d'éviter les erreurs.

Pour le test, nous avons utilisé le supplicant *wpa_supplicant*. Nous essayons de nous authentifier au réseau AP1 (voir la figure 32), le supplicant envoie les requêtes d'authentification au serveur pour vérifier son identité.

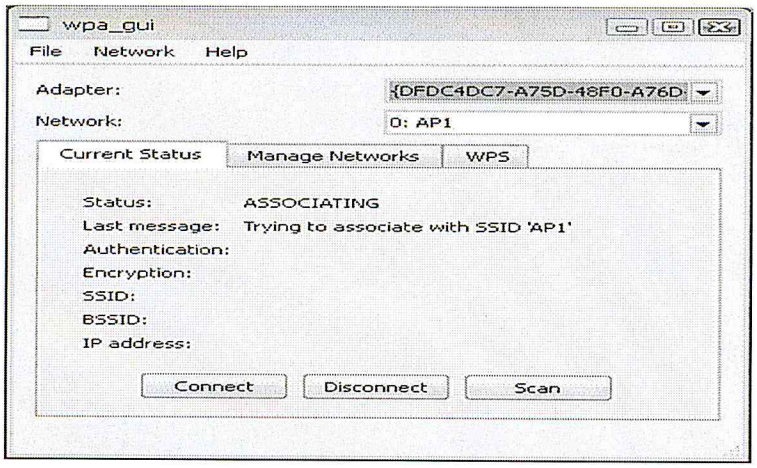

Figure 32: Le supplicant essaie d'accéder au réseau

Après que le serveur valide l'identité du client, il envoie le paquet *Access-Accept* au NAS pour lui permettre l'accès au réseau (voir la figure 33).

```
++[sql] returns ok
++[expiration] returns noop
++[logintime] returns noop
[pap] Found existing Auth-Type, not changing it.
++[pap] returns noop
Found Auth-Type = EAP
++ entering group authenticate (...)
[eap] Request found, released from the list
[eap] EAP/leap
[eap] processing type leap
  rlm_eap_leap: Stage 6
[eap] Freeing handler
++[eap] returns handled
Sending Access-Accept of id 11 to 10.0.0.245 port 2050
        Cisco-AVPair += "leap:session-key=\232\020D\370F\246\343Zx+\255\325\303\300 \027\216\020C\252\022\2202`\363w\352cVZ(L\
344"
        EAP-Message = 0x020400271101001188fb923213a9faf115e53b06fca3fc6341909b0d1ec7611326d6f68616d6564
        Message-Authenticator = 0x00000000000000000000000000000000
        User-Name = "mohamed"
Finished request 25.
Going to the next request
Waking up in 4.9 seconds.
Cleaning up request 25 ID 11 with timestamp +326
Ready to process requests.
```

Figure 33: Le serveur Radius valide l'identité de l'utilisateur

Une fois que le NAS reçoit le paquet *Access-Accept*, il permet à l'utilisateur d'accéder au réseau (voir la figure 34).

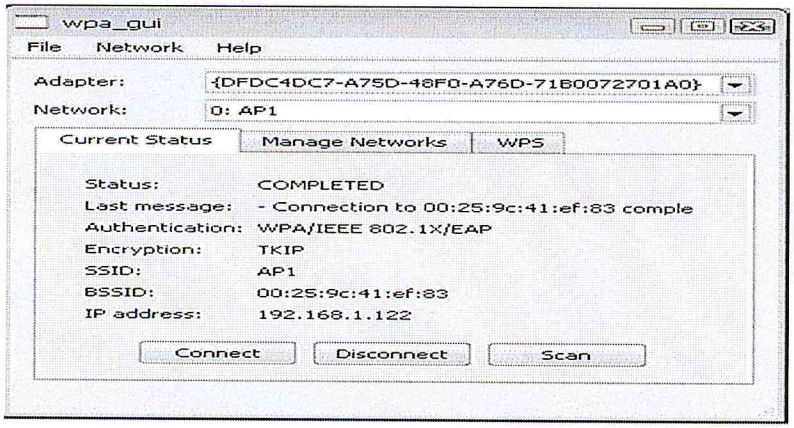

Figure 34: Connexion à AP1 réussie

Alors dans le cas où l'utilisateur utilise Windows et veut installer le supplicant proposé, il le fait et obtient son accès total au réseau en environ 2mn. Ce temps dépend de la version de Windows utilisé et de la performance de la carte réseau sans fil parce qu'avec les avancements technologiques, de nouveaux supplicants sont intégrés dans le système ce qui peut rendre l'accès plus rapide.

Dans le cas où l'utilisateur utilise un système Linux, l'authentification est très facile. Après avoir configuré la connexion au niveau du supplicant avec les informations de l'utilisateur, il suffit de cliquer sur connecter.

Les insuffisances de la solution centralisée

La solution mise en œuvre ci-dessus, nous a servi de moyen d'expérimentation de ce que nous avons étudié sur les réseaux maillés et l'authentification basée sur un serveur Radius. Cependant comme toute solution centralisée, elle possède des faiblesses bien connues principalement :

- la vulnérabilité et la non tolérance aux pannes du serveur (problème de fiabilité et disponibilité),
- la vulnérabilité face aux attaques de déni de service (problème de fiabilité et disponibilité),
- la surcharge potentielle du serveur et la difficulté de passage à l'échelle (chute de performance),

Ceci nous amène à la proposition de la solution décrite ci-après par laquelle nous tentons de répondre à ces inconvénients.

4.5.Solution répartie proposée

Nous avons implémenté la solution centralisée dans le but de tester la possibilité de mise en œuvre et l'utilisation pratique de l'environnement matériel et logiciel nécessaire pour ce type de solution. En effet, la possibilité qu'un serveur d'authentification ou un lien de communication tombe en panne n'est jamais à écarter. Rappelons que tous les impératifs principaux doivent être considérés : la sécurité, la disponibilité et les performances.

4.5.1. Architecture de la solution

Nous proposons de déployer une solution répartie qui se base sur plusieurs serveurs (RADIUS + SGBD) : un serveur joue le rôle du maître, et les autres serveurs jouent le rôle des esclaves. Le serveur maître est responsable des ajouts et modifications des clients et points d'accès. Il met à jour les données de tous les autres serveurs esclaves périodiquement. La période est définie selon les besoins d'utilisation et selon la charge du réseau et du serveur maître lui-même (voir la figure 35).

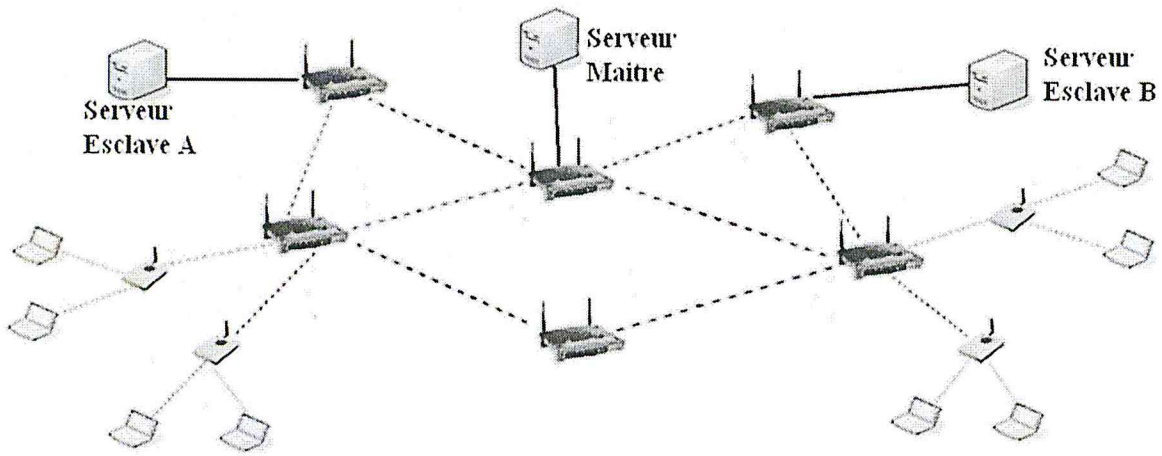

Figure 35: L'architecture répartie proposée

Toutes les bases de données seront synchronisées à l'aide d'un script ou en utilisant une application externe. Pour le SGBD MySQL, l'application open source *mysqldump* est capable de faire un backup de la base de données du maître sur les serveurs d'authentification esclaves. Ainsi, le backup peut être complet (de toute la base de données) ou incrémental (seuls les champs modifiés à partir d'un moment donné) Le backup incrémental est plus rapide et consomme moins de ressources, cependant, le backup complet est incontournable dans certaines situations.

D'une part, notre solution se base sur le concept de *fail-over*, qui signifie la capacité d'un serveur de prendre le rôle d'un autre serveur automatiquement lorsque ce dernier n'est plus fonctionnel. Cela permet d'assurer la disponibilité et la fiabilité qui sont nécessaires dans notre contexte (cas de crise).

D'autre part, pour éviter la surcharge d'un serveur donné, nous proposons de répartir la tâche d'authentification entre les différents serveurs. Chaque serveur esclave est considéré comme un serveur principal pour le groupe des utilisateurs qui passe par les points d'accès qui lui sont associés, et il est considéré comme secondaire pour les groupes d'utilisateurs qui n'arrivent pas à s'authentifié auprès de leurs serveurs principaux (en cas de panne). Par exemple, s'il y a deux serveurs d'authentification A et B (voir la figure 35), on saisie dans la moitie des points d'accès l'adresse IP du serveur A comme un serveur principal, et l'adresse IP du serveur B comme un serveur secondaire, et l'inverse pour l'autre moitie des points d'accès.

Notre système réparti est basé donc sur deux types de serveurs:

- **Serveur Maître :** Responsable de l'ajout et la modification des utilisateurs et des points d'accès d'une part, et de la synchronisation des bases de données esclaves d'autre part. Le serveur maître peut authentifier les utilisateurs ; cependant, il vaut mieux ne pas lui affecter la tâche d'authentification car il pourra être chargé. Dans le réseau, il n'y a donc qu'un seul serveur maître.
- **Serveur esclave :** Son rôle est d'authentifier une partie des utilisateurs. De plus, il peut prendre le rôle de serveur maître en cas de non disponibilité (panne, ou autre) du serveur maître actuel, ou il peut authentifier les utilisateurs d'un autre serveur si ce dernier ne peut assurer cette fonction. Dans le réseau, on peut avoir plusieurs serveurs esclaves.

Initialement, le serveur maître est choisi manuellement, il choisit un successeur parmi les serveurs esclaves (le premier qui répond à une requête diffusée). En cas de crash de serveur maître, ce serveur esclave devient le nouveau serveur maître, ce dernier choisit à son tour son successeur, et ainsi de suite. Donc, le basculement du serveur maître se fait automatiquement.

Si l'administrateur veut modifier les informations d'un utilisateur ou d'un point d'accès, il doit le faire au niveau du serveur maître, et celui-ci est chargé de mettre à jour les autres bases de données. Si un utilisateur veut s'authentifier, il envoie sa requête au serveur esclave auquel le point d'accès qui lui est associé (serveur principal) est rattaché. Au cas où la connexion avec ce dernier échoue, le point d'accès envoie la requête à un serveur secondaire.

4.5.2. Avantage de la solution répartie

- Un meilleur temps de réponse, car le serveur d'authentification esclave sera plus proche et moins chargé.
- Une meilleure disponibilité du service d'authentification grâce au concept de backup.
- Une meilleure robustesse du système face à quelques attaques telles que le DoS et une meilleure tolérance aux pannes.

4.5.3. Quelques inconvénients de la solution répartie

- Le coût relativement élevée par rapport à la solution centralisée, mais nous pensons que la situation le mérite pour réduire l'impact des catastrophes.
- La complexité de configuration et de maintenance, ce qui influe sur le temps de déploiement du réseau. Ce problème peut être réduit par la pré-configuration des serveurs d'authentification.
- La surcharge de calcul induite par les backups, mais ce problème peut être résolu par l'optimisation de la durée entre les backups par rapport à la quantité de données mises à jour dans le serveur maître, et par des backups incrémentaux, c.-à-d. ne mettre à jours que les champs modifiées dans la base de données maître ou bien par la virtualisation des serveurs.

Conclusion

Dans un environnement sans fil, l'authentification IEEE 802.1X semble être la plus sûre parmi ce qui existe comme solutions actuellement. Cependant, nous avons trouvé que le schéma centralisé n'est pas convenable pour les WMN, et la gestion sécurisée des clés devient difficile. Les WMN peuvent être gérés par plusieurs fournisseurs, et l'authentification doit être faite pendant l'itinérance des nœuds mobiles à travers différents domaines administratifs, et la tendance du serveur et des liens sans fil à tomber en panne est

un souci majeur. Donc, le déploiement d'une architecture répartie devient nécessaire, car elle répond mieux aux besoins de disponibilité de service. Cependant, cette solution a besoin d'amélioration pour résoudre le problème de la complexité de configuration et aussi d'une analyse et une évaluation afin de tester si cette solution répond efficacement à ce qui suit :

- **La mobilité des nœuds :** lorsque le nœud se ré-authentifie au cours de son itinérance, il alourdit le réseau.
- **La bande passante limitée :** La contrainte de la bande passante exige un processus d'authentification qui ne surcharge pas le canal de transmission par ces messages.
- **Le comportement égoïste des nœuds :** le comportement égoïste des nœuds est un problème majeur dans les réseaux multi sauts en général, et des WMN en particulier, car un nœud intermédiaire peut capturer les données de l'authentification et les utiliser pour un accès illégal au réseau.

Conclusion générale

Suite aux nombreux avantages offerts par les réseaux maillés sans fil, il est devenu nécessaire de recourir à des techniques et approches plus efficaces pour assurer la sécurité et la confidentialité des utilisateurs accédant au réseau.

La sécurité dans un réseau maillé dépend de l'architecture adoptée et de la méthode d'authentification et de chiffrement des données. Nous avons étudié dans ce mémoire les réseaux maillées sans fil, leurs caractéristiques et avantages, et nous avons analysé le problème de sécurité de ce type de réseaux tout en citant les différentes menaces et leurs solutions. Puis, nous avons analysé les différentes solutions d'authentification existantes pour les réseaux sans fil et les WMN en particulier. La solution d'authentification adéquate pour les WMN doit donc respecter les limitations et les contraintes des réseaux maillés. Nous avons opté pour déployer la solution IEEE 802.1X car elle offre une large gamme de caractéristiques de sécurité et de gestion des utilisateurs.

Néanmoins, l'architecture centralisée qui se base sur un seul serveur d'authentification ne répond pas bien aux besoins d'une situation concrète et surtout en cas de crise. Par conséquent, nous avons proposé une architecture d'authentification répartie basée sur plusieurs serveurs de type RADIUS dotés de bases de données répliquées et synchronisées, ce qui permet d'assurer la disponibilité du service d'authentification qui est primordial dans le cas d'une catastrophe. Notre solution adopte le concept de *fail-over*, où les serveurs esclaves s'occupent automatiquement de la tâche d'authentification si un serveur s'arrête soudainement. Ainsi, nous avons proposé deux méthodes de synchronisation des bases de données, la première consiste à faire un backup complet de la base de données maître dans toutes les bases de données esclaves, la deuxième consiste à ne faire un backup que pour les données modifiées à partir d'un certain repère temporel, c'est ce qu'on appelle un *backup incrémental.*

Les recherches ont découvert de nombreuses failles de sécurité dans la méthode d'authentification 802.1X en termes d'algorithmes de cryptages. Cependant, notre travail n'a pas traité ce sujet car notre but est d'analyser le problème d'authentification du point de vue architecture pour répondre aux cas des catastrophes. Ces vulnérabilités sont à étudier en

perspective à ce travail en même temps que les améliorations qui pouvaient être considérées pour l'architecture proposée, notamment, en termes de choix de certains paramètres tels que la périodicité des synchronisations des données, le nombre de serveurs à déployer, etc.

Nous souhaitons renforcer cette contribution en intégrant une approche répartie plus robuste et plus performante qui consiste à mette en place une architecture peer to peer entre les serveurs, améliorer la négociation et optimiser le transfert des données entre eux, ou même développer un protocole en entier qui gère cette tâche.

Bibliographie

[1] Akyildiz IF, Wang X. et Wang W.: Wireless mesh networks, a survey, *Journal of Computer Networks*, 2005.

[2] G. R. Hiertz, S. Max, Y. Zang, T. Junge et D. Denteneer: IEEE 802.11s MAC fundamentals, IEEE MASS 2007 – The Fourth IEEE International Conference on Mobile Ad-hoc and Sensor Systems.

[3] L. Chen, "Wireless Mesh Networks (WMNs)", *Technical Report* UIUCDCS-R-2006-2874, Dept. of Computer Science, UIUC, 2006.

[4] Anne BENOIT: Réseaux sans fil, note de cours (Algorithme des réseaux et des télécommunications), ENS LYON, M1, 2006.

[5] Chlamtac I, Conti M et Liu J: Mobile ad hoc networking, imperatives and challenges, Journal of Elsevier, 2003.

[6] M. Kodialametet et T. Nandagopal: Characterizing the Capacity Region in Multi-Radio Multi-Channel Wireless Mesh Networks, MobiCom, 2004.

[7] W. Xu, W. Trappe, Y. Zhang, et T. Wood: The feasibility of launching and detecting jamming attacks in wireless networks, ACM MOBIHOC 2005.

[8] J. Pollastre, J. Hill, et D. Culler: Versatile low power media access for wireless sensor networks, In Proceedings of ACM Sensys, 2004.

[9] Y. Law, L. Hoesel, J. Doumen, P. Hartel et P. Havinga: Energy-efficient link-layer jamming attacks against wireless sensor network MAC protocols, In *Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks* (SASN 2005).

[10] Maxime Gicquiaud: Man in the Middle, Global security Subinfo international University, 2011.

[11] Mark Stamp: Once Upon a Time-Memory Tradeoff, 2003.

[12] Stuart J. Kerry, Al Petrick: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE 2007.

[13] Yih-Chun Hu, Adrian Perrig, et David B. Johnson: Rushing attacks and defense in wireless ad hoc network routing protocols, In Proceedings of the 2003 ACM Workshop on Wireless Security (WiSe 2003).

[14] Yih-Chun Hu, Adrian Perrig et David B. Johnson: Packet leashes, A defense against wormhole attacks in wireless ad hoc networks, In Proceedings of IEEE INFOCOM 2003, Avril 2003.

[15] M. Al-Shurman, S. Yoo et S. Park: Black hole attack in mobile ad hoc networks, In Proceedings of the 42nd Annual Southeast Regional Conference, Huntsville, Alabama, April 2004.

[16] Hamdy S. Soliman et Mohammed Omari: Application of synchronous dynamic encryption system in mobile wireless domains, In Proceedings of the 1st ACM International Workshop on Quality of Service and Security in Wireless and Mobile Networks, October 2005.

[17] Kui Ren, Wenjing Lou, et Yanchao Zhang : LEDS, Providing location-aware end-to-end data security in wireless sensor networks, In Proceedings of IEEE International Conference on Computer Communication (INFOCOM '06), April 2006.

[18] S.L. Keohetet et E. Lupu : Towards flexible credential verification in mobile ad-hoc networks, In Proceedings of the 2nd ACM International Workshop on Principles of Mobile Computing, POMC '02. Toulouse, France, October 2002.

[19] J. Kong, P. Zerfos, H. Luo, S. Lu et L. Zhang : Providing robust and ubiquitous security support for MANET (pp. 251–260), In Proceedings of IEEE ICNP, 2001.

[20] D. Hongmei, A. Mukherjee et D.P. Agrawal : Threshold and identity-based key management and authentication for wireless ad hoc networks, In Proceedings of International Conference on Information Technology: Coding and Computing (ITCC 2004), pp. 107–111, Vol. 1, April 2004.

[21] Y.-X. Lim, T.S. Yer, J. Levine, et H.L. Owen : Wireless intrusion detection and response, Information assurance workshop 2003. IEEE Systems, Man and Cybernetics Society, pp. 68–75, June 2003.

[22] Y. Liu, H. Man et C. Comaniciu : A game theoretic approach to efficient mixed strategies for intrusion detection, In IEEE International Conference on Communications (ICC), 2006.

[23] P. Papadimitratos et Z. Haas: Secure routing for mobile ad hoc networks, In SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), January 2002.

[24] Hao Yang, J. Shu, Xiaoqiao Meng, et Songwu Lu. : SCAN, Self-organized network-layer security in mobile ad hoc networks, IEEE Journal on Selected Areas in Communications, Volume 24, Issue 2, pp. 261–273, February 2006.

[25] J. Vollbrecht et D. Spence : RFC 2903, 2000.

[26] Aruesh Mishra et William A. Arbaugh : An initial Security Analysis of the IEEE 802.1X Standard, UMIACS-TR-2002-10,2002.

[27] Guillaume Lehembre : Sécurité Wi-Fi – WEP, WPA et WPA2, Dossier n°1, 2006.

[28] Jyh-Cheng Chen, Ming-Chia Jiang et Yi-Wen Liu, wireless LAN Security and IEEE 802.11i, NATIONAL TSING HUA UNIVERSITY, IEEE Wireless Communication, 2004.

[29] Arunesh Mishra, William A. Arbaugh: An Initial Security Analysis of IEEE 802.1X Standard, UMIACS-TR-2002-10, University of Maryland, 2002.

[30] Mohamad Badra : Le transport et la sécurisation des échanges sur les réseaux sans fil, thèse de doctorat. L'Ecole Nationale Supérieure des Télécommunications, 2004

[31] Mr.Sikander Singh, Mr. Sukhwinder Singh Sran et Dr. Tirlok Chand : Performance Comparison of AODV, OLSR and OFLSR in Wireless Mesh Networks, 2008. Proceedings of 2nd National Conference on Challenges & Opportunities in Information Technology (COIT-2008) RIMT-IET, Mandi Gobindgarh. March 29, 2008.

[32] Y. Rekhter, B. Moskowitz et D. Karrenberg : Request for Comments 1918 : Address Allocation for Private Internets.