

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Djilali Bounaama Khemis Miliana



Faculté des Sciences et de la Technologie
Département de Technologie

Mémoire du Projet de Fin d'Etudes
Pour l'obtention du diplôme de
Master

En
« Télécommunications »
Option :
« Systèmes des Télécommunications »

Titre :

Implémentation d'un réseau local sans fil à haut
débit

Présenté par

Afif Mohamed Amine & Zergui Fatima Zahra

Soutenu le 10/07/2023 devant le jury

Dr Bounif Aouda

Président

Dr Kaddeche Mourad

Examineur

Dr. Benbekhti Fatiha

Encadreur

Dédicaces 1

Je dédie ce modeste travail :

*A mes parents, mes sœurs, toute ma
famille et mes amis.*

*Et aussi A toute ma promotion de
l'université Djilali Bounaama.*

Mohamed Amine

Dédicaces 2

Je dédie le présent travail à :

*Mes parents qui m'ont toujours
encouragé dans le chemin du savoir ;*

Mon frère et mes sœurs ;

Mon binôme Afif Mohamed amine

Tous mes enseignants dans tous les paliers,

Toute ma promotion,

*A toute personne qui m'a procuré de l'aide
et du courage...*

Fatima Zahra

Remerciements

À Dieu le tout puissant et miséricordieux, nous dédions humblement ce travail en reconnaissance de Sa grâce et de Sa bénédiction.

Nous exprimons également notre profonde gratitude à notre encadreur, Mm. Benbakhti Fatiha, pour sa précieuse conseil, la soutenir et l'encourager tout au long de cette période de recherche.

Nous souhaitons également remercier les membres du jury pour leur intérêt et leur contribution à notre travail, ainsi que toutes les personnes qui ont contribué de près ou de loin à sa réalisation.

Enfin, nous dédions ce travail à nos familles et amis, dont l'amour, le soutien et les encouragements ont été un soutien précieux tout au long de cette aventure.

Que cette humble contribution puisse enrichir le corps de connaissances et apporter une contribution significative à la société.

Résumé

Ce projet vise à étudier la mise en œuvre de réseaux locaux sans fil à haut débit en se concentrant sur des protocoles de routage ad hoc. Il est déterminé que AODV est un protocole plus performant que DSDV et DSR. L'étude se concentre ensuite sur différentes approches pour se défendre contre les attaques dans les réseaux ad hoc, en se concentrant sur les attaques par trou noir, et explore les solutions de sécurité contre de telles attaques. Des mécanismes d'authentification de nœud ont été proposés pour fournir une protection initiale.

Mots clés : Ad hoc, protocole de routage, AODV, DSDV, DSR, BlackHole.

Abstract

This project aims to study the implementation of high-speed wireless LANs focusing on ad hoc routing protocols. It is determined that AODV is a better performing protocol than DSDV and DSR. The study then focuses on different approaches to defend against attacks in ad hoc networks, focusing on black hole attacks, and explores security solutions against such attacks. Node authentication mechanisms have been proposed to provide initial protection.

Keywords: Ad hoc, routing protocol, AODV, DSDV, DSR, BlackHole.

Liste des abréviations

AES:	Advanced Encryption Standard
AIP:	Association Identity
AODV:	Ad hoc on Demand Distance Vector
AP:	Access Point.
ARP:	Address Resolution Protocol
BRAN:	Broad Wireless Access Network
BSSID:	Basic Service Set Identifier.
CCMP:	Counter Mode CBC-MAC Protocol
CDMA:	Code Division Multiple Access
CHAP:	Challenge Handshake Authentication Protocole.
CSMA/CA:	Carrier Sense Multiple Access/Collision Avoidance.
CTS:	Clear To Send.
DCF:	Distributed Coordination Function.
DoS:	Deny of Service.
DS:	Distribution System.
EAP	Extensible Authentication Protocol.
IEEE:	Institute of Electrical and Electronics Engineers.
IV:	Initialization Vector
LAN	Local Area Network
LLC:	Logical Link Control.
LTE:	Long Term Evolution)
MAC:	Media Access Control.
MAN:	Metropolitan Area Network.
MANET:	Mobile Ad hoc NETwork
MIC:	Message Integrity Code.
MITM:	Man In The Middle
MS-CHAP:	Microsoft Challenge Handshake Authentication Protocol.

OFDM: Orthogonal Frequency Division Multiplexing.

OSI: Open Systems Interconnection.

PMD: Physical Medium Dependent

PPP: Point to Point Protocole.

PSK: Pre-Shared Key.

RADIUS: Remote Authentication Dial In User Service.

RC4: Rivest Cipher 4.

RERR: Route Error

RREP: Route Reply

RREQ: Route Request

RRS: Random Routing Scheme

REQ: Request

RF: Radio Frequency.

RTS: Request to Send.

SSID: Service Set Identifier.

Tcp: Transmission Control Protocol.

VPN: Virtual Private Network

TKIP: Temporal Key Integrity Protocol.

WEP: Wired Equivalent Privacy.

WIFI: Wireless Fidelity

Wimax: Worldwide interoperability for Microwave Access

WLAN: Wireless Local Area Network

WMAN: Wireless Metropolitan Area Network

WPAN: Wireless Personal Area Network

WWAN: Wireless Wide Area Network

ZRP: Zone Routing Protocol.

Table des matières

Dédicaces 1	i
Dédicaces 2	ii
Remerciements	iii
Résumé	iv
Abstract	iv
Liste des abréviations	v
Introduction générale	1
Chapitre I	4
Généralités sur les réseaux informatiques	4
I.1. Introduction	5
I.2. Définition de réseau informatique	5
I.3. Modèle OSI	6
I.3.1. Définition	6
I.3.2. Couches du modèle OSI	6
I.4. Modèle TCP/IP	7
I.5. Comparaison entre TCP /IP est OSI	7
I.6. Définition du réseau sans fil	8
I.7. Présentation des différents réseaux sans fil	8
I.7.1. WPAN	9
I.7.2. WLAN	10
I.7.3. WMAN	12
c) WWAN	13
I.7.4. Bande de fréquences	14
I.7.5. Fonctionnement du Wi-Fi	14
a) Avantage du Wi-Fi	15
b) Inconvénients du Wi-Fi	15
c) Architecture du réseaux Wi-Fi	15
- Mode Infrastructure	16
- Mode Ad Hoc	16
I.7.6. Présentation du matériel	17
Cartes Wi-Fi	17
I.8. Normalisation	18
I.9. Couche physique	20
I.9.1. PLCP	20
I.9.2. PMD	20

I.9.3. Technique de modulation.....	20
I.10. La couche liaison de données	21
I.10.1. Couche LLC	21
I.10.2. Couche MAC.....	22
I.11. Trame MAC.....	22
I.11.1. Trame de contrôle.....	23
I.11.2. Duration ID.....	24
I.11.3. Champ adresses	24
I.11.4. Champ FCS.	24
I.11.5. Champ contrôle de séquence	24
I.12. Conclusion.....	25
Chapitre II	26
II.1. Introduction	27
II.2. Aperçu sur WLAN	27
II.3. Politique globale.....	27
II.4. Services de sécurité	28
II.5. Attaques principales d'un réseau Wi-Fi.....	30
II.5.1. C'est quoi une attaque ?	30
II.5.2. Motivation et objectif de l'attaquant.....	30
II.5.3. Différentes attaques d'un réseau Wi-Fi	31
II.5.3.1. Usurpation (spoofing)	31
II.5.3.2. Attaque homme au milieu « MEN-IN-THE-MIDDLE ».....	32
II.5.3.3. Dénî de service (DOS)	33
II.5.3.4. Intrusion	34
II.5.3.5. Attaque de dictionnaire	34
II.5.3.6. Détourner une session existante.....	34
II.5.3.7. Attaque de trou noir « BlackHole »	34
II.5.3.8. Espionage (sniffing).....	35
II.6. Risques liés aux réseaux sans fil	35
II.6.1. Manque de sécurité.....	35
II.6.2. War-Driving.....	35
II.6.3. Risques liés en matière de sécurité.....	36
II.7. Solutions pour sécuriser un réseau Wi-Fi.....	37
II.7.1. Sécurité élémentaire	37
II.7.1.1 Identificateur de réseau	37
II.7.1.2 Mot de passe	37
II.7.1.3 Filtrage d'adresse MAC	38

II.7.1.4	Protection par adresse IP	38
II.7.1.5	Sécurité des points d'accès	38
II.7.2.	Sécurité renforcée.....	39
II.7.3.	Cryptages des données	39
II.7.3.1	Définition	39
II.7.3.2	Etude des protocoles de sécurité liés aux Wi-Fi	41
II.7.3.3	Protocoles de routage dans un réseau sans fil.....	51
II.8.	Conclusion.....	54
Chapitre III		54
Simulation d'un réseau local sans fil		54
III.1.	Introduction	55
III.2.	L'environnement de simulation.....	55
III.2.1.	Présentation du NS-2.....	55
III.2.1.1	Processus de simulation	56
a.	Le langage TCL :	57
b.	NAM :	57
d.	Les avantages et les inconvénients du simulateur NS2 :	58
III.3.	Les critères d'évaluation.....	58
III.3.1.	Taux de transfert des paquets.....	58
III.3.2.	.Temps bout en bout	59
III.3.3.	Pert des paquets (PL).....	59
III.3.4.	Surcharge.....	59
III.3.5.	Lancement de la simulation.....	59
III.4.	. Résultats et discussion.....	60
III.4.1.	Scénario 1	60
III.4.2.	Scénario 2	66
III.5.	Conclusion.....	71

Liste des figures

Chapitre I

Figure I. 1. Diagramme du modèle OSI.....	6
Figure I. 2. Couches de modèle OSI et TCP/IP.....	9
Figure I. 3. Réseau WPAN.....	10
Figure I. 4. Réseau WLAN.....	12
Figure I. 5. Différents réseaux sans fil.....	15
Figure I. 6. Mode infrastructure.....	18
Figure I. 7. Mode AD Hoc.....	19
Figure I. 8. Carte PCMCIA Wi-Fi.....	20
Figure I. 9. Carte réseau PCI.....	21
Figure I. 10. Format général de la trame MAC 802.11.....	26

Chapitre II

Figure II. 1. Sécurité et niveaux de l'architecture OSI [23].....	29
Figure II. 2. Différentes cas de cyberattaque [24].....	30
Figure II. 3. Attaque ARP spoofing [29].....	32
Figure II. 4. Attaque MITM [30].....	33
Figure II. 5. Cryptage symétrique [40].....	40
Figure II. 6. Cryptage asymétrique [40].....	41
Figure II. 7. Le chiffrement WEP [42].....	43

Chapitre III

Figure III. 2. Paramètre de simulation.....	60
Figure III. 3. PDR en fonction de la variation des nombres des nœuds pour AODV, DSDV et DSR.	62
Figure III. 4. délai de retard moyen en fonction du nombre des nœuds.....	63
Figure III. 5. Les pertes perdues de retard moyen en fonction du nombre de nœuds pour AODV, DSDV, DSR.....	65
Figure III. 6. Surcharges par rapport le nombre de nœuds pour AODV, DSDV, DSR.....	66
Figure III. 7. Variation de PDR en fonction du nombre des nœuds pour AODV sans et avec blackhole.	69
Figure III. 8. Variation de paquets perdus en fonction du nombre des nœuds pour AODV sans et avec blackhole.	69
Figure III. 9. Délai en fonction du nombre des nœuds pour AODV sans et avec blackhole.....	70
Figure III. 10. Le cout en fonction du nombre des nœuds pour AODV sans et avec blackhole.....	71

Liste des tableaux

Chapitre I

<i>Tableau I. 1. Bande de fréquences [17]</i>	15
<i>Tableau I. 2. Normalisation 802.11 [9,10]</i>	22
<i>Tableau I. 3. Modulation technique</i>	24
<i>Tableau I. 4. Types et les sous-types de trame de contrôle</i>	27

Chapitre III

<i>Tableau III. 1. Paramètres de simulation du scénario 1</i>	61
<i>Tableau III. 2. Variation de PDR vs le nombre des nœuds pour AODV, DSDV, DSR</i>	61
<i>Tableau III. 3. Délai de retard moyen en fonction du nombre de nœuds pour AODV, DSDV, DSR</i>	63
<i>Tableau III. 4. Les pertes perdues de retard moyen en fonction du nombre de nœuds pour AODV, DSDV, DSR</i>	64
<i>Tableau III. 5. Surcharge par rapport le nombre de nœuds pour AODV, DSDV, DSR</i>	65
<i>Tableau III. 6. Paramètres de simulation du scénario 2</i>	67
<i>Tableau III. 7. Variation des paramètres de performances en fonction du nombre des nœuds pour AODV sans et avec Blackhole</i>	67

Introduction générale

Dans la société d'aujourd'hui, la communication et la technologie jouent un rôle important, ce qui est de bon augure pour le développement des réseaux informatiques. Le succès de ces réseaux dépend en grande partie de la technologie et des moyens de communication utilisés pour les sécuriser.

Actuellement, la transmission numérique et la communication sans fil sont devenues courantes. Les progrès technologiques ont permis d'augmenter les vitesses et les capacités de transfert de données tout en réduisant les coûts. Par conséquent, les réseaux locaux sans fil tels que le WiFi sont de plus en plus utilisés en raison d'avantages tels que la mobilité, la facilité d'installation et la convivialité.

Cependant, il est important de souligner que ces réseaux sans fil sont également utilisés dans les entreprises où des risques de sécurité existent.

Par conséquent, il est essentiel de disposer de mécanismes de sécurité solides pour protéger ces réseaux. Dans ce cas, il est important de prendre en compte les différents objectifs de sécurité et les ressources disponibles pour déterminer le niveau de sécurité approprié. Il est recommandé d'utiliser un protocole de sécurité adapté aux besoins spécifiques de chaque entreprise, tel que WEP, 802.1X, WPA, WPA2 ou WPA3. De plus, la formation des utilisateurs aux bonnes pratiques de sécurité est essentielle pour éviter les pratiques à risque telles que l'utilisation de mots de passe faibles ou le partage d'informations sensibles sur des réseaux non sécurisés. Par conséquent, la sensibilisation à la sécurité et la formation des utilisateurs sont des éléments clés du renforcement de la sécurité WLAN.

En bref, la sécurité WLAN est le problème le plus préoccupant pour les entreprises. Des mesures de sécurité appropriées doivent être en place pour protéger les informations confidentielles et sensibles, utiliser des protocoles de sécurité appropriés et former les utilisateurs aux bonnes pratiques de sécurité. Dans le cadre de l'évolution des réseaux locaux sans fil à haut débit, la sécurité doit être une priorité pour prévenir les cyberattaques et les violations de données. Par conséquent, les entreprises doivent tenir compte de ces problèmes pour sécuriser leurs réseaux sans fil et protéger leurs données sensibles.

Notre projet se compose de trois chapitres qui ont été planifiés de manière précise. Le premier chapitre vise à fournir une définition générale des réseaux, en présentant les concepts clés et les notions de base qui permettent de comprendre les réseaux de manière approfondie.

Dans le deuxième chapitre, nous nous concentrerons sur les attaques principales qui ciblent les réseaux locaux sans fil, en mettant l'accent sur les aspects importants de la sécurité et des mécanismes de sécurité des réseaux Wi-Fi, ainsi que les différentes solutions disponibles pour contrer ces attaques.

Enfin, dans le troisième chapitre, nous procéderons à une comparaison et à une simulation des protocoles AODV et DSR, en évaluant leurs performances respectives et en identifiant les avantages et les inconvénients de chaque protocole.

Nous terminerons par une conclusion générale.

Chapitre I

Généralités sur les réseaux informatiques

I.1. Introduction

Les réseaux ont pour objectif de transférer des données d'une machine terminale à une autre, en utilisant une combinaison de dispositifs matériels et de processus logiciels pour assurer la transmission de données à travers des câbles ou des ondes radio. Ces processus incluent des protocoles et des règles qui permettent de traiter les données de manière efficace et fiable.

La première partie de ce chapitre consiste à présenter plusieurs termes et définitions clés liées à notre travail, qui sont nécessaires pour une compréhension approfondie du sujet. Dans la deuxième partie, nous aborderons les concepts de base des réseaux sans fil, en nous concentrant sur la technologie Wi-Fi.

I.2. Définition de réseau informatique

Un réseau informatique est un ensemble d'ordinateurs et d'autres périphériques connectés entre eux pour échanger des données et des ressources. Les réseaux informatiques peuvent être utilisés pour diverses applications, telles que le partage de fichiers, l'accès à des imprimantes et à des périphériques de stockage, la communication par courrier électronique, la messagerie instantanée et la vidéoconférence.

Les réseaux informatiques peuvent être de différentes tailles, allant d'un simple réseau local (LAN) reliant quelques ordinateurs dans une maison ou un bureau, à des réseaux étendus (WAN) connectant des ordinateurs dans des lieux géographiquement éloignés.

Les réseaux informatiques peuvent également être classés en fonction de leur topologie, qui décrit la manière dont les nœuds du réseau sont connectés entre eux, ou en fonction de leur mode de fonctionnement, tels que les réseaux filaires, sans fil ou basés sur la communication de paquets.

Les réseaux informatiques sont un élément clé des technologies de l'information et de la communication (TIC) et jouent un rôle important dans la plupart des activités modernes, y compris le commerce électronique, la banque en ligne, la télémédecine et la surveillance à distance.

I.3. Modèle OSI

I.3.1. Définition

Le modèle OSI est un modèle de référence pour la communication réseau qui décrit la fonction et l'interaction des différents protocoles de communication nécessaires pour transférer des données entre les différents composants du réseau. [1]

I.3.2. Couches du modèle OSI

Le modèle OSI est un cadre de référence qui décrit la fonctionnalité d'un réseau ou d'un système de télécommunications. Il est composé de sept couches qui décrivent visuellement les différentes étapes d'un système de réseau. Cela est illustré dans la Figure I.1 qui montre comment chaque couche interagit avec les autres pour permettre le transfert de données.

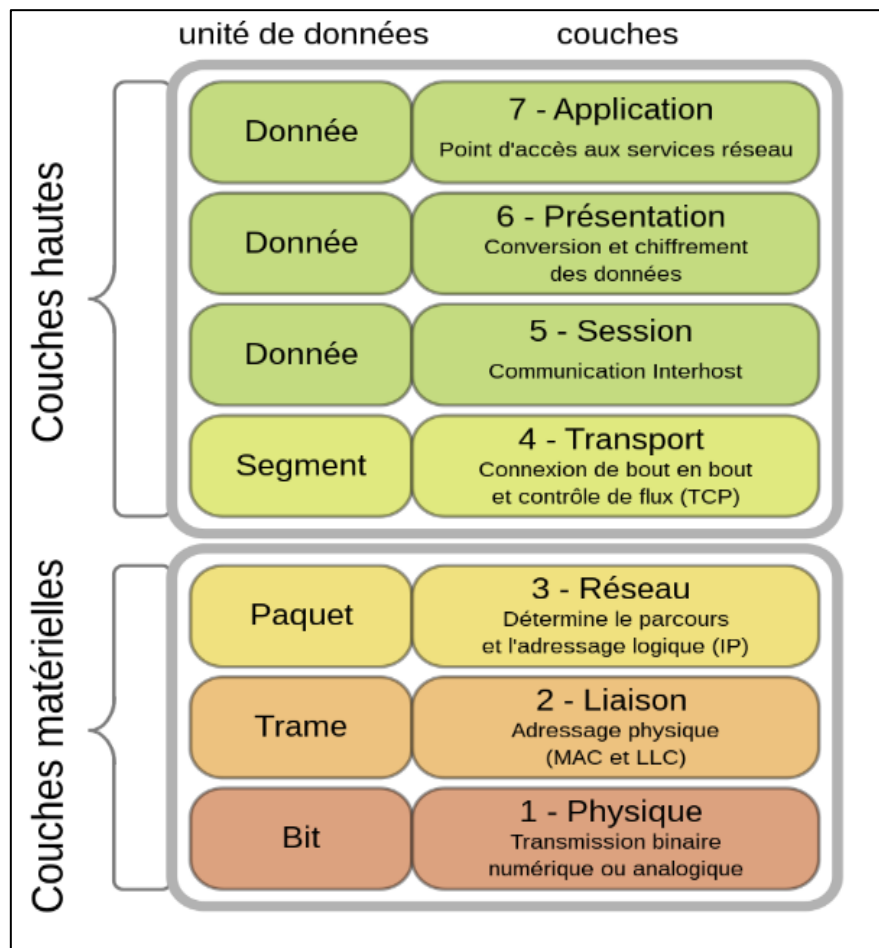


Figure I. 1. Diagramme du modèle OSI [1].

I.4. Modèle TCP/IP

Le modèle TCP/IP est un modèle de communication réseau développé par l'armée américaine dans les années 1970 pour la communication entre ordinateurs distants. Il est progressivement devenu la norme de facto pour l'interconnexion des réseaux.

TCP/IP est le protocole de communication le plus couramment utilisé sur le Web, à tel point que la plupart des utilisateurs ne s'en rendent même pas compte. La plupart des ordinateurs ont TCP/IP intégré par défaut, il fonctionne donc sans configuration manuelle. Il vous suffit de vous connecter à votre réseau sans fil local pour l'utiliser.

Le modèle TCP/IP est organisé en quatre couches distinctes, chacune ayant une fonction spécifique. Les couches du modèle TCP/IP sont les suivantes :

- Couche liaison de données
- Couche Internet
- Couche Transport
- Couche Application

I.5. Comparaison entre TCP /IP et OSI

La principale différence entre les deux modèles est que TCP/IP est un modèle en couches plus simple, qui comprend quatre couches : couche réseau, couche transport, couche application et couche Liaison de données. Le modèle OSI, quant à lui, comprend sept couches : couche physique, couche liaison de données, couche réseau, couche transport, couche session, couche présentation et couche application [2].

Les avantages du modèle TCP/IP sont sa simplicité et son efficacité pour les réseaux actuels. Il est également plus étroitement intégré à Internet que le modèle OSI. Cependant, le modèle OSI est considéré comme plus complet et permet une meilleure compréhension de la façon dont les différents protocoles de communication interagissent [2].

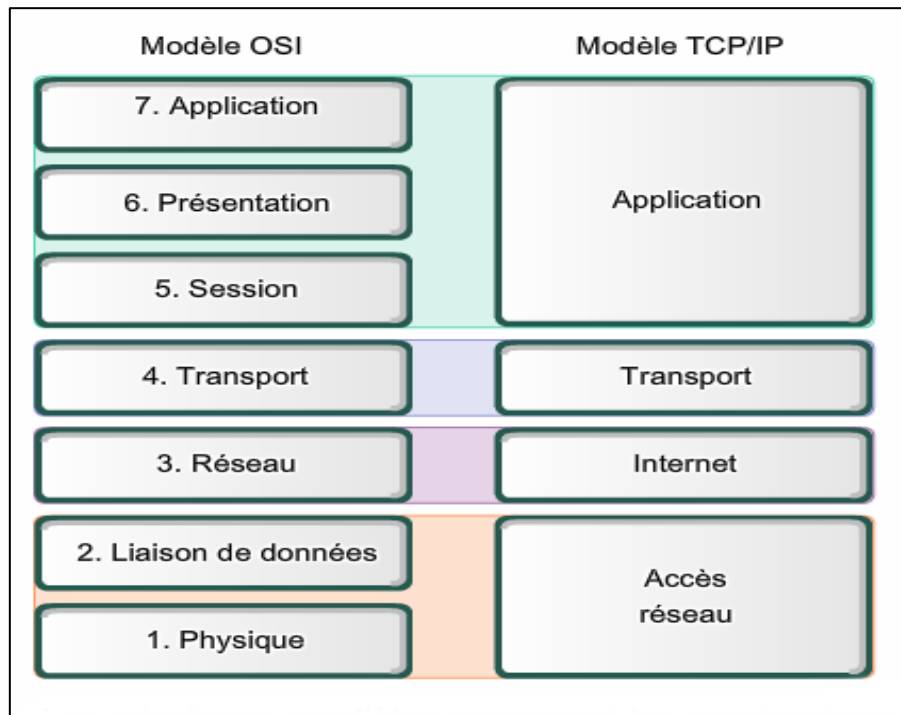


Figure I. 2. Couches de modèle OSI et TCP/IP [2].

I.6. Définition du réseau sans fil

Un réseau sans fil est un système de communication de données qui permet le transfert d'informations entre des dispositifs informatiques sans l'utilisation de câbles physiques. Le réseau sans fil est composé de plusieurs éléments tels que des dispositifs clients (par exemple, ordinateurs portables, smartphones, tablettes), des points d'accès (APs), des antennes, des routeurs, des commutateurs, et des protocoles de communication sans fil tels que Wi-Fi, Bluetooth, NFC, 4G, 5G, etc.

La technologie sans fil utilise des ondes radio pour transmettre des données à travers l'espace. Les dispositifs sans fil communiquent entre eux en émettant et en recevant des signaux radiofréquences qui sont ensuite convertis en données par des circuits électroniques.

Les signaux sans fil peuvent être perturbés par des obstacles physiques tels que des murs ou des interférences électromagnétiques provenant d'autres dispositifs, ce qui peut entraîner des pertes de données et une diminution de la qualité de la connexion.

I.7. Présentation des différents réseaux sans fil

Les informations sont transmises au moyen d'ondes électromagnétiques grâce à cette technologie. Cela signifie que la longueur d'onde et sa fréquence déterminent le type de réseau, et parmi ces réseaux, on peut citer les suivants :

I.7.1. WPAN

Ce type de réseau permet la transmission d'informations et de commandes sur une courte distance d'environ 10 mètres maximum, et il contient peu d'éléments tels que des imprimantes, des lumières et des dispositifs de musique. C'est l'un des éléments de base de la maison intelligente, et ces réseaux s'appuient sur plusieurs technologies.

A. Bluetooth

Le Bluetooth est une norme de communication qui a été mise au point en 1994 par la société suédoise Ericsson. Cette technologie utilise des ondes radio UHF pour permettre à plusieurs périphériques de se connecter et d'échanger des données et des fichiers sur une courte distance, généralement inférieure à 10 mètres.

Le Bluetooth fonctionne sur des fréquences comprises entre 2,4 GHz et 2,483 GHz. Le principal avantage de cette technologie est la possibilité de connecter des appareils sans utiliser de câbles. Depuis sa création, le Bluetooth a été largement adopté dans le monde de la téléphonie mobile et de l'informatique [2]

B. Zigbee

Zigbee est une technologie de communication sans fil utilisée pour les réseaux d'objets connectés à faible consommation d'énergie, tels que les capteurs, les actionneurs et les dispositifs de surveillance. Cette technologie utilise la norme de connectivité IEEE 802.15.4 pour permettre la communication sans fil entre les périphériques.

Elle est conçue pour fonctionner dans des bandes radio sans licence, telles que 2,4 GHz, 900 MHz et 868 MHz, et est capable de gérer des réseaux de taille variable, allant de quelques appareils à plusieurs milliers. Zigbee offre une faible consommation d'énergie, une faible latence et une haute fiabilité de transmission de données, ce qui en fait une technologie populaire pour les applications IoT dans les domaines de la domotique, de la santé, de l'industrie et de l'agriculture intelligente [3].

C. Ir DA

Les liaisons infrarouges (IR) sont un type de technologie de communication sans fil utilisée dans les réseaux. Cette technologie permet aux appareils électroniques de connecter à distance tels que des téléphones portables, des ordinateurs portables, des imprimantes et des scanners. L'avantage de cette technologie est de sécuriser les informations et de transférer en une fraction de seconde. La technologie IR est limitée

car elle est affectée par des facteurs externes tels que la lumière du soleil. Elle nécessite également une communication directe entre les appareils connectés pour assurer l'information.

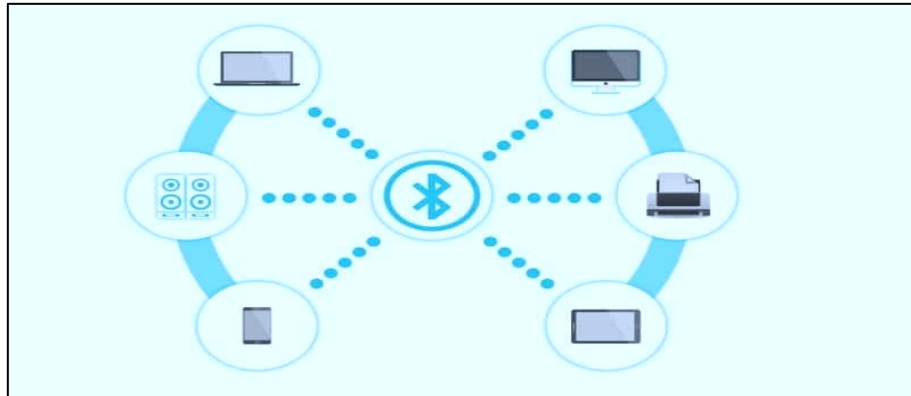


Figure I. 3. Réseau WPAN [4]

I.7.2. WLAN

Un WLAN est un réseau sans fil avec une zone de couverture et un nombre d'appareils connectés plus importants qu'un réseau WPAN. Il est utilisé dans les entreprises, les aéroports et les restaurants, et ses avantages incluent des connexions plus rapides et plus flexibles entre les utilisateurs, et une communication précise et ciblée. Il permet également aux utilisateurs d'accéder à Internet.

Il est basé sur la norme de communication sans fil IEEE 802.11 et utilise des ondes radio pour transmettre des données entre divers appareils connectés. Les réseaux WLAN peuvent être sécurisés à l'aide de protocoles de cryptage tels que WPA2 ou WPA3 pour protéger les données transmises et un débit de 11 à 54 MBS. Il existe plusieurs technologies concurrentes utilisant les bandes de fréquences 2,4 GHz, 5 GHz et 6 GHz. D'autres types de WLAN peuvent fonctionner sur différentes bandes de fréquences [5] :

A. Wi-Fi

Le Wi-Fi est un ensemble de protocoles de communication sans fil régis par l'ensemble de normes IEEE 802.11. Avec la norme Wi-Fi, vous pouvez créer rapidement un réseau local sans fil. En fait, le Wi-Fi peut connecter des ordinateurs portables, des ordinateurs de bureau, des assistants numériques personnels (PDA) pour la communication d'objets, et même des connexions à haut débit avec des périphériques de communication d'appareils (11 Mbit/s en théorie, 6 Mbit/s en pratique). D'autre part, 802.11b a un maximum théorique de 54 Mbps, et 802.11a a

un débit effectif d'environ 25 Mbps ou 802.11g à l'intérieur dans un rayon de dizaines de mètres (généralement 20-50 mètres).

B. Hiper LAN

Hiper LAN est un standard LAN sans fil développé par la division BRAN (Broadband Wireless Access Networks) de l'ETSI. HIPERLAN est spécialisé dans la technologie LAN, sans fil à haut débit et à haut rendement qui répond aux exigences en Europe., HIPERLAN/2 fonctionne dans la bande 5 GHz et les données à quatre chiffres jusqu'à 54 Mbps. Alors que HIPERLAN semble offrir des performances au WLAN 802.11a (WIFI), il est plus efficace en termes d'allocation de ressources radio aux utilisateurs.

Malheureusement, le WIFI est déjà disponible et a été certifié pour un fonctionnement au Royaume-Uni par la RA (Radiocommunication Agency). Pour cette raison et les économies d'échelle, il s'avérera initialement être une option beaucoup moins chère que HIPERLAN. À cette fin, on voit que les dérivés Wifi tels que WiFi5, WiFi6 deviendront les technologies dominantes [6].



Figure I. 4. Réseau WLAN [6].

I.7.3. WMAN

WMAN (Réseau métropolitain sans fil) est un type de réseau sans fil qui couvre une zone géographique plus large que le WLAN mais plus petite qu'un WAN. Les deux technologies les plus couramment utilisées dans WMAN sont WiMax et LTE et WIBRO :

a) WiMax

WiMAX est une technologie de communication sans fil qui fonctionne dans une plage de fréquences de 2 à 66 GHz. Des fréquences plus élevées sont utilisées pour les transmissions en vue directe, qui peuvent atteindre jusqu'à 66 GHz. WiMAX est conçu pour fournir un accès Internet à haut débit et d'autres services de données à la fois aux dispositifs fixes et portables.

Il peut offrir jusqu'à 40 Mbps de capacité par canal sans fil, en fonction de la configuration spécifique utilisée. Pour le service en vue directe, WiMAX utilise une plage de fréquences plus basse de 2 GHz à 11 GHz, et une antenne parabolique fixe est utilisée pour pointer le signal directement vers le récepteur. WiMAX peut être utilisé pour fournir un accès Internet à large bande dans les zones urbaines et rurales, ainsi que pour les réseaux mobiles [7].

b) WIBRO

WiBro (Wireless Broadband) est une technologie de connexion Internet à large bande sans fil développée par l'industrie des télécommunications sud-coréenne. WiBro est le nom du service sud-coréen pour la norme internationale IEEE 802.16e (mobile WiMax). Les stations de base WiBro offriront un débit de données agrégé de 30 à 50 Mbits/s et couvriront un rayon de 1 à 5 km, permettant une utilisation d'internet portable.

La technologie offrira également une qualité de service qui permettra à WiBro de diffuser du contenu vidéo et d'autres données sensibles à la perte de manière fiable. Deux opérateurs télécoms sud-coréens (KT, SKT) ont lancé un service commercial en juin 2006.

Cependant, il semblait être plus performant que le WiMax, mais sa "propriété industrielle coréenne" et sa position sur le spectre électromagnétique (cette bande de fréquence pouvant déjà être utilisée en dehors de la Corée) l'ont empêché de devenir une norme internationale au même titre que le Wi-Fi, par exemple [8].

c) WWAN

WWAN (réseau étendu sans fil) est un type de réseau sans fil qui couvre une zone géographique plus étendue qu'un réseau local sans fil typique (WLAN). Il s'agit d'un type de réseau cellulaire qui utilise des fréquences radio pour connecter des appareils sur une grande zone géographique.

Les réseaux WWAN utilisent des tours cellulaires pour transmettre et recevoir des signaux, ce qui permet aux appareils de se connecter et de communiquer entre eux. Les réseaux WWAN sont généralement exploités par des opérateurs de réseaux mobiles (MNO) ou des fournisseurs de services sans fil.

Les trois principales technologies WWAN sont GSM/UMTS, CDMA, CDMA2000. Il existe plusieurs technologies concurrentes [9] :

- Technologie : AMPS
- Technologie 2G : GSM
- Technologie 3G : UMTS
- Technologie 4G : LTE
- Technologie 5G

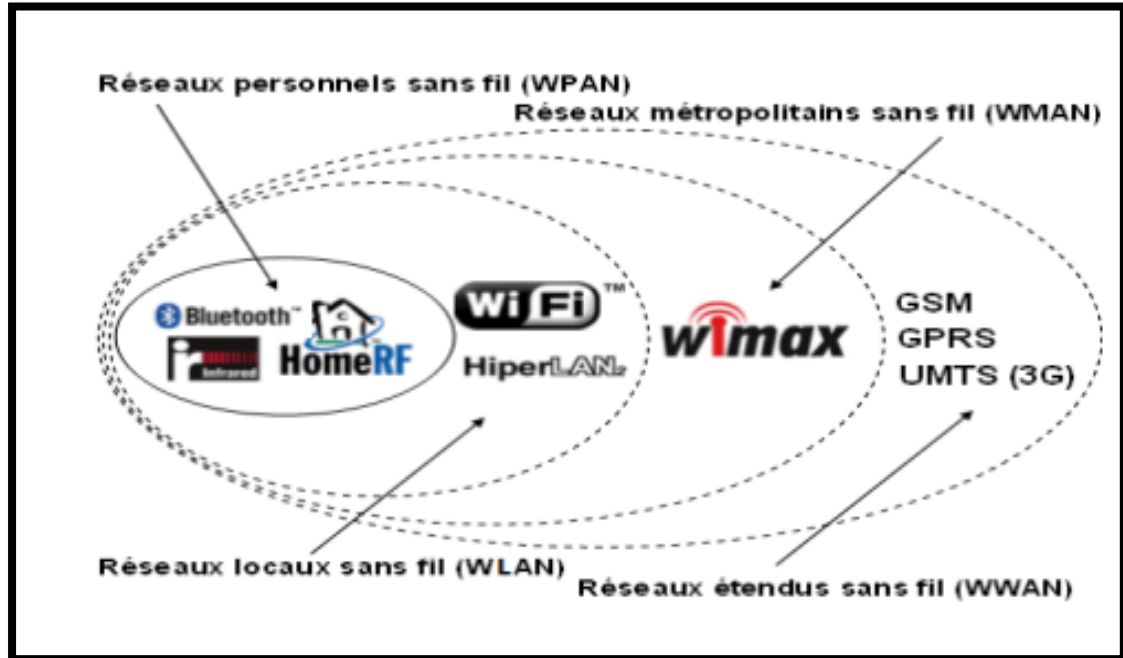


Figure I. 5. Différents réseaux sans fil [10]

I.7.4. Bande de fréquences

Le tableau I.1 illustre les réseaux disponibles au niveau du monde, chaque technologie a des performances comme le débit, la portée et la bande de fréquence.

Tableau I. 1. Bande de fréquences [11]

Réseaux	Technologie	Débit (en réel)	Portée (Km)	Bande de fréquence (GHZ)
WPAN	Bluetooth	1 Mbits/s	5	2,4- 2,4835
	HomeRF	10Mbits/s	50 - 100	2,4 2,4835
	ZigBee	20 – 250 Kbits/s	100	2,4 - 2,4835
WLAN	HiperLAN 1	19 - 20	Max 150	2,4
	HiperLAN 2	54Mbit/s	Max 150	5,4–5,7
	HiperLink	155Mbit/s	150 - 200	17,2 – 17,3
	DECT	2Mbit/s	300	1880 – 1900 MHz
WMAN	WiMax	70Mbit/s	50	1– 66
	HiperAccess	Supérieur à 100Mbit/s	Très courte portée	11–66
WWAN	CDMA 2000	≤ 2 Mbits/s		2
	2G	>50 Kbits/s		900-1900 MHZ
	3G	42Mbit/s		800-2100 MHZ
	4G	100Mbit/s		700-2600 MHZ
	5G			600-52600 MHZ

I.7.5. Fonctionnement du Wi-Fi

Pour simplifier, le fonctionnement d'un réseau Wi-Fi est similaire à celui d'un téléphone portable : les données sont transmises à travers des ondes radio. Pour se connecter au Wi-Fi, un ordinateur doit être équipé d'un adaptateur sans fil qui convertit les données en un signal radio, envoyé par l'antenne à un décodeur appelé routeur. Les informations sont ensuite transmises à internet par une connexion filaire Ethernet.

Les câbles Ethernet permettent de relier l'ordinateur et les périphériques au routeur. Les données en provenance d'internet sont également envoyées au routeur pour être converties en signal radio, puis réceptionnées par l'adaptateur sans fil de l'ordinateur. Pour une bonne qualité de la connexion Wi-Fi, il est important de veiller à ne pas avoir d'autres appareils électroniques émettant des ondes électromagnétiques à proximité [11].

a) Avantage du Wi-Fi

- Facilité d'installation : les réseaux Wi-Fi sont faciles à installer et ne nécessitent pas de câblage complexe comme les réseaux filaires ;
- Mobilité : les utilisateurs peuvent se connecter à Internet depuis n'importe quel endroit dans la zone de couverture du signal Wi-Fi ;
- Flexibilité : les réseaux Wi-Fi peuvent être configurés pour prendre en charge différents types d'appareils électroniques et de nombreux utilisateurs simultanés ;
- Évolutivité : les réseaux Wi-Fi peuvent être facilement étendus en ajoutant des points d'accès supplémentaires pour couvrir une zone plus large ;
- Coût : l'installation d'un réseau Wi-Fi est généralement moins coûteuse que celle d'un réseau filaire [12].

b) Inconvénients du Wi-Fi

- Portée limitée : la portée des signaux Wi-Fi est limitée, ce qui signifie que les utilisateurs doivent être à proximité d'un point d'accès sans fil pour se connecter.
- Intensité du signal : la qualité du signal Wi-Fi peut varier en fonction de l'emplacement du point d'accès, de la distance et de l'obstruction par des objets tels que des murs ;
- Coûts initiaux : bien que les coûts de mise en place d'un réseau Wi-Fi soient généralement moins élevés que ceux d'un réseau filaire, l'installation de points d'accès supplémentaires peut augmenter les coûts ;
- Bande passante partagée : les réseaux Wi-Fi partagent la bande passante entre tous les utilisateurs connectés, ce qui peut entraîner des ralentissements lorsqu'il y a de nombreux utilisateurs simultanés ;
- Disponibilité : certains endroits ne disposent pas d'un réseau Wifi disponible, ce qui peut limiter la connectivité [12].

c) Architecture du réseaux Wi-Fi

Le réseau sans fil, connu sous le nom de Wi-Fi est généralement basé sur une architecture cellulaire similaire à celle utilisée dans la téléphonie mobile. Dans cette architecture, des téléphones mobiles communiquent entre eux via des stations de base.

Dans un réseau Wi-Fi, il y a un ou plusieurs points d'accès (AP) auxquels se connectent un certain nombre de stations de base dotées de cartes Wi-Fi pour échanger

des données. Les points d'accès servent de pont entre les stations du réseau et le réseau extérieur pour unifier le réseau.

Réseau Wi-Fi, qui repose sur une architecture cellulaire similaire à celle des réseaux de téléphonie mobile, est déterminé par la portée de couverture du point d'accès, également appelé cellule. Cette unité unique constitue l'architecture de base du Wi-Fi et s'appelle le BSS. Selon cette architecture, il existe deux topologies : le mode infrastructure et le mode Ad Hoc [13].

- Mode Infrastructure

Il s'agit d'un réseau sans fil qui contient des points d'accès entre les éléments de ce réseau. Au moins un point d'accès doit être présent sur le réseau, qui est le lien entre les périphériques du réseau. Tous les messages et les informations échangés passent également par lui pour être transférés au destinataire final. Les points d'accès sont considérés comme la passerelle d'entrée vers les réseaux filaires, et il est possible d'étendre la portée du réseau en ajoutant « BSS » plusieurs points d'accès [14].

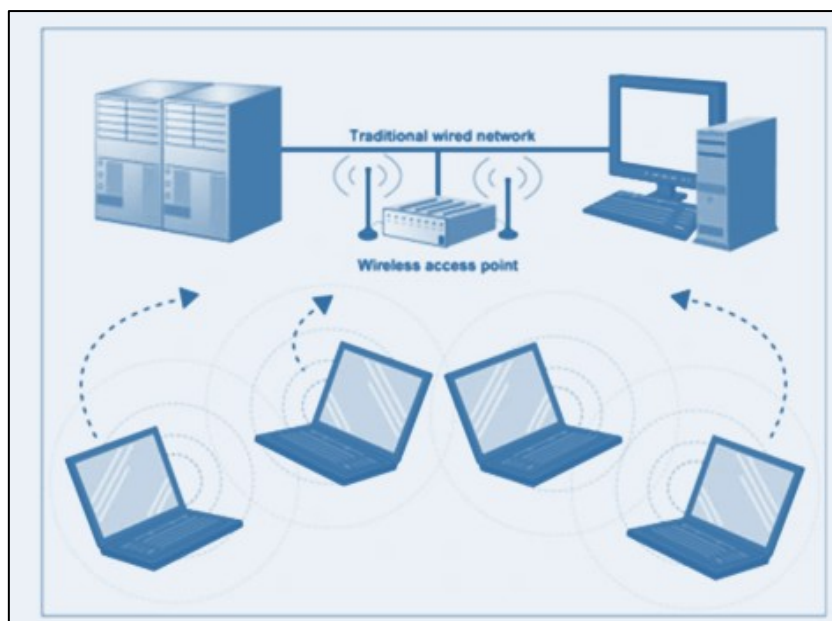


Figure I. 6. Mode infrastructure [14].

- Mode Ad Hoc

C'est une partie intégrante du réseau WLAN et elle est souvent utilisée pour des durées courtes. Son rôle principal est généralement le transfert de fichiers. Les avantages de ce réseau incluent l'absence de points d'accès, ce qui permet aux stations de se connecter sans assistance externe, réduisant ainsi le temps nécessaire pour les mettre en place [15].

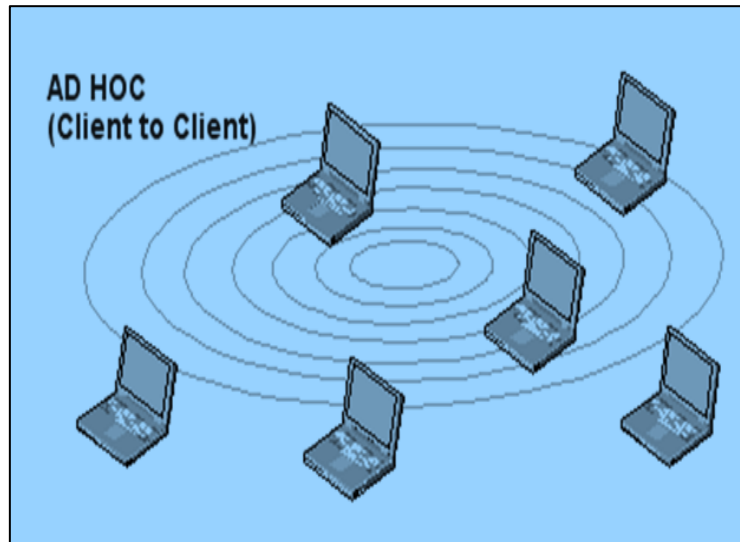


Figure I. 7. Mode AD Hoc [15].

I.7.6. Présentation du matériel

Cartes Wi-Fi

Les cartes Wi-Fi les plus couramment utilisées sont les cartes de stations mobiles. Pour les ordinateurs portables, les cartes au format PCMCIA sont les plus couramment utilisées, tandis que pour les organisateurs, le format de la carte varie en fonction du type de PDA (Personale Digital Assistant) utilisé.



Figure I. 8. Carte PCMCIA Wi-Fi [16]

Pour les stations fixes de bureau, différents modèles de cartes sont disponibles. À l'origine, les machines fixes n'avaient pas d'interfaces PCMCIA, contrairement aux portables, qui n'avaient que des interfaces USB ou PCI, et les machines relativement anciennes avaient même ISA. Par conséquent, les cartes Wi-Fi pour stations fixes utilisent ces types de ports.



Figure I. 9.Carte réseau PCI [16].

I.8. Normalisation

Le tableau ci-dessous (Tableau I.2) montre les normes internationales qui existent dans le réseau et la description de leur technologie.

Tableau I. 2. Normalisation 802.11 [16]

Nom de la norme	Technologie	Description
802.11a	Wifi5	Permet un débit théorique de 54 Mbps et un débit réel de 30 Mbps. Elle spécifie 8 canaux radio dans la bande de fréquence des 5 GHz.
802.11b	Wifi	Propose un débit théorique de 11 Mbps (6 Mbps réel) avec une portée allant jusqu'à 300 mètres dans un environnement dégagé.
802.11c	Pontage 802.11vers 802.1d	C'est une modification de la norme 802.11 (niveau liaison de données).
802.11d	Internationalisation	Permet une utilisation internationale des réseaux locaux 802.11 en échangeant des informations sur les plages de fréquence et les puissances autorisées dans le pays d'origine du matériel.
802.11 e	Amélioration de laqualité de service	Offre des possibilités en matière de qualité de service pour permettre une meilleure transmission de la voix et de la vidéo.
802.11f	Itinérance(romain)	Recommandation pour une meilleure interopérabilité des produits avec le protocole Interaccès Point Romain Protocol permettant une itinérance transparente lors d'un déplacement.
802.11g	Wifi 2	Offre un haut débit (54 Mbps théorique, 30 Mbps réel) sur la bande de fréquence de 2.4 GHz avec une compatibilité ascendante avec la norme 802.11b
802.11h		Harmonisation de 802.11a avec le standard européen
802.11i		Améliore la sécurité des transmissions en s'appuyant sur l' AES
802.11IR		Norme dépassée techniquement qui utilisait des signaux infrarouges.
802.11j		La norme 802.11j est à la réglementation japonaise ce que le 802.11h est à la réglementation européenne

I.9. Couche physique

La couche physique (PHY) du standard IEEE 802.11 spécifie les caractéristiques électriques, mécaniques, fonctionnelles et procédurales des interfaces physiques pour les réseaux locaux sans fil (WLAN) également connus sous le nom de Wi-Fi. La couche PHY est responsable de la transmission et de la réception des signaux sans fil sur le support de transmission, tels que les ondes radio, elle est constituée de deux sous couches : PMD et PLCP [16].

I.9.1. PLCP

La sous-couche de procédure de convergence de couche physique (PLCP) joue un rôle crucial dans la norme 802.11 pour les réseaux locaux sans fil (WLAN). Elle prépare les trames 802.11 pour la transmission et dirige la sous-couche dépendante du support physique (PMD) pour transmettre des signaux, changer de canal radio, recevoir des signaux et plus encore.

La PLCP prend chaque trame 802.11 qu'une station souhaite transmettre et forme une unité de données de protocole PLCP (PPDU), qui comprend des champs tels que le signal, identifiant le débit de données de la trame 802.11.[16]

I.9.2. PMD

La sous-couche de dépendance du support physique (PMD) est responsable de la définition des détails de la transmission et de la réception des bits individuels sur un support physique. Elle contribue à définir la couche physique des protocoles de réseau informatique et englobe le chronométrage des bits, le codage de signal, l'interaction avec le support physique et les propriétés du câble, de la fibre optique ou du fil lui-même [16].

I.9.3. Technique de modulation

Pour transmettre de la donnée dans le réseau sans fil le tableau suivant (tableau I.3) montre les techniques de modulation plus utilisées.

Tableau I. 3. Modulation techniqueI.10. Couche liaison de données

Technique	Débit	Bande
FHSS	1-2 Mbit/s	900 MHz, 2,4 GHz, 5 GHz
DSSS	11 Mbit/s	2,4 GHz
DSSS/HR	22Mbit/s	2,4 GHz, 5 GHz
OFDM	54Mibt/s	2,4 GHz, 5 GHz
MIMO-OFDM	600Mbit/s	2,4 GHz, 5 GHz

I.10. La couche liaison de données

La couche liaison de données est la deuxième couche du modèle OSI pour un ensemble de protocoles de télécommunication. Elle assure le transfert des données sur les liaisons physiques du réseau, en codant, décodant et organisant les bits de données dans des trames avant de les transporter sous forme de paquets entre deux nœuds adjacents du réseau.

La couche liaison de données fournit également les moyens fonctionnels et procéduraux pour le transfert de données entre des entités d'un réseau et, dans certains cas, les moyens de détecter et potentiellement corriger les erreurs qui peuvent survenir au niveau de la couche physique Il se compose de deux couches [17] :

I.10.1. Couche LLC

La couche LLC 802.11 est la sous-couche supérieure de la couche liaison de données dans le modèle de référence IEEE 802 des réseaux informatiques. La sous-couche LLC agit comme une interface entre la sous-couche MAC (Media Access Control) et la couche réseau.

La fonction principale de la sous-couche LLC est de multiplexer les protocoles sur la couche MAC lors de la transmission et de démultiplexer les protocoles lors de la réception. La sous-couche LLC fournit un contrôle de flux hop-to-hop et de correction d'erreur et permet une communication multipoint sur les réseaux informatiques.

La sous-couche LLC fournit des mécanismes de multiplexage qui permettent à plusieurs protocoles réseau (tels que IP, IPX et DECnet) de coexister au sein d'un réseau multipoint et d'être transportés sur le même support réseau. La sous-couche LLC joue un rôle crucial dans l'assurance d'un fonctionnement efficace et fiable des réseaux informatiques [17]

I.10.2. Couche MAC

La couche MAC (contrôle d'accès au support) 802.11 est une sous-couche de la couche liaison de données spécifique aux réseaux locaux sans fil (WLAN) et définie par la norme IEEE 802.11. La fonction principale de la couche MAC 802.11 est de coordonner l'accès à l'interface aérienne partagée afin que le point d'accès (AP) et les stations Wi-Fi à portée puissent communiquer efficacement.

Elle couvre trois domaines fonctionnels : la livraison fiable de données, le contrôle d'accès et la sécurité. Elle est responsable de l'encapsulation des trames et de la description des formats de trame. La couche MAC 802.11 définit également les adresses de réseau, qui sont des identifiants uniques de 48 bits (6 octets) connus sous le nom d'adresse MAC. La couche MAC 802.11 joue un rôle crucial dans l'assurance d'un fonctionnement efficace et fiable des réseaux WLAN [18].

I.11. Trame MAC

La trame MAC 802.11, utilisée pour gérer l'accès au canal de communication partagé dans un réseau sans fil 802.11. Elle est essentielle pour la transmission des données sans fil entre les appareils connectés au réseau. La trame MAC 802.11 encapsule les données à transmettre et ajoute les informations nécessaires pour les acheminer de manière fiable et efficace vers leur destination.

La trame est constituée de plusieurs champs qui remplissent des fonctions spécifiques. Le champ de contrôle, le champ de durée, le champ d'adresse, le champ de séquence, le champ de données contient les données à transmettre.

Enfin, le champ de vérification de redondance. En somme, la trame MAC 802.11 est un élément crucial du fonctionnement des réseaux sans fil et permet d'assurer une communication fiable et efficace entre les appareils connectés. Structure générale d'une trame MAC est présentée dans la figure ci-dessous [19] :

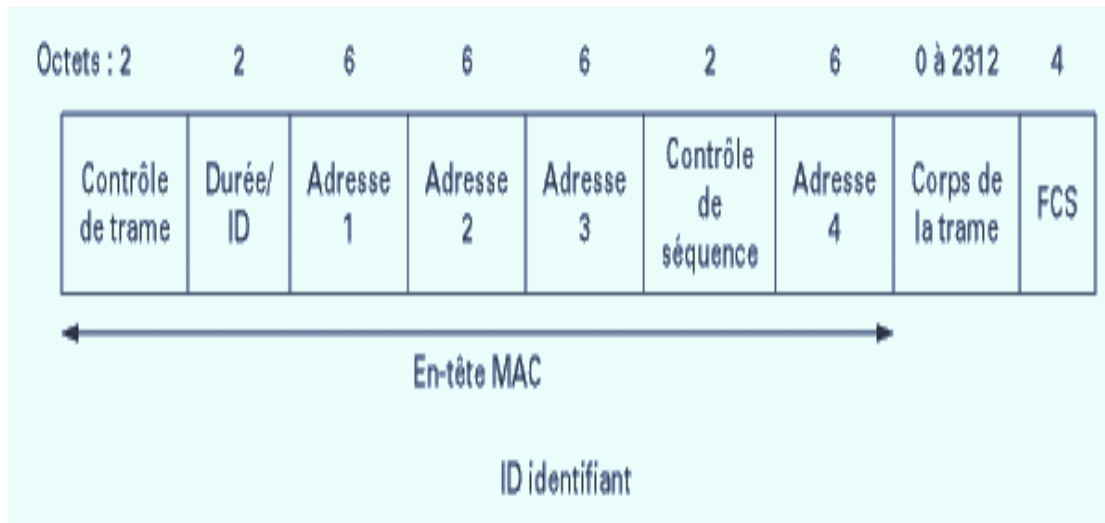


Figure I. 10. Format général de la trame MAC 802.11[19]

Toutefois, selon le type de trame, certains champs peuvent être absents, notamment les champs adressent 1, adresse 2, adresse 3, adresse 4 et le corps de la trame, et le champ de données peut avoir une taille maximale de 2312 octets champ FCS, qui sert à détecter les erreurs de transmission et à garantir l'intégrité des données reçues, a une taille fixe de 6 octets. La taille maximale d'une trame est de 2347 octets.

I.11.1. Trame de contrôle

- Version de protocole : ce champ contient 2 bits qui pourront être utilisés pour reconnaître des versions standard 802.11
- Contrôle les types et les sous-types de trame
- Contrôle l'échange d'informations entre le client sans fil et les points d'accès
- Contrôle les collisions entre les clients en incluant une période de temps, ce qui garantit que les données ne sont pas envoyées en même temps par les utilisateurs
- Renvoyer les informations non reçues.

Ce tableau ci-dessous (tableau I.4) illustre les types et les sous types de chaque trame :

Tableau I. 4. Types et les sous-types de trame de contrôle

Type	Sous-type
Control	CTS, ACK, RTS, PS-POLL,
gestion	Balise, ATIM, Des association,
Donne	CF-ACK, CF-poll-Function null,

I.11.2. Duration ID

Le champ "Duration ID" est un sous-champ du champ de contrôle de trame de la trame MAC 802.11. Il contient un nombre de bits qui indique la durée d'accès au canal requise pour la transmission de la trame. Cette durée comprend à la fois le temps de transmission de la trame elle-même et le temps d'attente avant la transmission. En utilisant ces informations, les périphériques sans fil peuvent synchroniser leurs transmissions pour éviter les collisions et maximiser l'utilisation du canal de communication.

A deux sens différents suivant le type de trames utilisées. Pour les trames de contrôle en mode d'économie d'énergie, il correspond à l'identifiant de la station, ou AID (Association Identity), qui transmet la trame. Pour toutes les autres trames, ce champ correspond à la valeur de durée de vie qui est utilisée lors du calcul du NAV[19].

I.11.3. Champ adresses

Ces champs correspondent à des adresses MAC de stations sources, de stations de destination ou de BSSID.

I.11.4. Champ FCS.**I.11.5. Champ contrôle de séquence**

Le champ de séquence de la trame MAC 802.11 est composé de deux sous-champs distincts, à savoir le numéro de séquence et le numéro de fragment. Les trames Wi-Fi peuvent être de différents types, notamment les trames de contrôle qui contiennent les informations de supervision nécessaires au bon fonctionnement du réseau, les trames de gestion qui sont utilisées par l'administrateur du réseau, et les trames de données qui transportent les informations des utilisateurs [20].

I.12. Conclusion

Ces dernières années, les réseaux sans fil ont connu une croissance rapide grâce à leurs multiples avantages, tels que la mobilité et la fiabilité, ainsi que la disponibilité de terminaux peu coûteux et performants tels que les ordinateurs portables, les assistants personnels (PDA) et les téléphones mobiles.

En offrant une connectivité performante et économique, le Wi-Fi a réussi à surpasser ses concurrents et est devenu le moyen dominant pour fournir une architecture de réseaux locaux sans fil .

Dans le prochain chapitre, nous nous concentrerons sur les attaques qui touchent le réseau sans fil et précisément la standard Wi-Fi, en explorant les spécifications techniques de la sécurité qui ont permis à cette technologie de devenir largement utilisée.

Chapitre II

Sécurité d'un réseau
local sans fil

II.1. Introduction

Les réseaux locaux sans fil sont devenus omniprésents dans notre vie quotidienne, et il est de plus en plus important de comprendre comment les sécuriser efficacement. Voici une brève introduction aux développements récents en matière de sécurité des réseaux locaux sans fil.

Avec la popularité croissante des technologies sans fil telles que le Wi-Fi et le Bluetooth, la sécurité des réseaux sans fil est devenue une préoccupation majeure. Les réseaux sans fil sont vulnérables aux attaques malveillantes en raison de leur ouverture et de leur accessibilité.

Les attaquants peuvent facilement intercepter les données transmises sur des réseaux sans fil non sécurisés, ainsi que mener des attaques telles que des attaques par déni de service, des attaques de l'homme du milieu et le piratage de clés de sécurité.

Bien que le Wi-Fi soit largement utilisé et apprécié, il comporte des vulnérabilités qui le rendent moins sécurisé et fiable. Ainsi, dans ce chapitre, nous allons étudier en détail les protocoles et mécanismes de sécurité afin de proposer des solutions améliorant la qualité de service du réseau tout en minimisant les risques de sécurité.

II.2. Aperçu sur WLAN

Les réseaux WLAN gagnent en popularité dans les entreprises, les établissements d'enseignement et les foyers, offrant aux utilisateurs une plus grande flexibilité et mobilité. Les technologies WLAN courantes incluent Wi-Fi, Bluetooth et Zigbee. Les réseaux locaux se caractérisent par de faibles coûts d'installation. Les coûts de câblage jouent un rôle important dans les installations de réseau.

Avec la croissance explosive des ordinateurs portables et des assistants numériques personnels, les réseaux locaux intègrent la technologie sans fil. Cette technologie réduit le coût d'installation du réseau et répond aux nouveaux besoins des utilisateurs en termes de nomadisme. Une autre caractéristique du réseau local est la facilité de mise en œuvre et de configuration [21]. Cependant, la sécurité du réseau WLAN est une préoccupation majeure et des mesures de sécurité appropriées doivent être prises pour protéger les données transmises.

II.3. Politique globale

La sécurité au niveau Wi-Fi est essentielle pour protéger les réseaux sans fil contre les attaques malveillantes. La stratégie de sécurité globale d'un réseau Wi-Fi doit inclure des mesures telles que l'utilisation de protocoles de cryptage forts, la gestion de

clés sécurisées, l'authentification des utilisateurs et la mise en œuvre de mesures pour prévenir les attaques par déni. Des politiques de sécurité spécifiques pour les utilisateurs doivent être en place, et des procédures de surveillance et de détection des attaques doivent être en place. La sensibilisation des utilisateurs à la sécurité des réseaux sans fil est également importante [22].

II.4. Services de sécurité

La cybersécurité est l'ensemble des mesures techniques, organisationnelles, juridiques et humaines nécessaires et mises en œuvre pour maintenir, rétablir et assurer cette sécurité. La sécurité du réseau comprend généralement la sécurité des systèmes informatiques sur lesquels repose le réseau.

La sécurité des réseaux peut être évaluée par rapport à de nombreux critères de sécurité. En général, il existe cinq principaux critères de sécurité [22] :

- **Chiffrements des données** : Le chiffrement des données brouille les données afin que seuls les utilisateurs autorisés puissent les déchiffrer et les lire. Le cryptage protège les informations sensibles en empêchant tout accès non autorisé.
- **Authentification** : a comme objectif d'assurer l'identité du communicateur. Elle permet de confirmer que la personne qui se connecte est en règle. L'authentification peut être simple ou mutuelle, elle consiste le plus souvent à comparer les données de l'utilisateur connecté à des informations stockées sur des sites web sécurisés mais susceptibles d'être piratés [23].
- **Contrôle d'intégrité des messages** : garantit que les données reçues sont exactement celles qui ont été émises par l'émetteur autorisé et se préserver des pertes d'informations.
- **Non répudiation** : Il fournit une preuve au destinataire/expéditeur pour empêcher le d'envoyer le message.
- **Le contrôle d'accès** : a la capacité de bloquer l'accès aux ressources dans des conditions définies et par des utilisateurs spécifiques.

Il peut y avoir des conditions spécifiques pour chacun de ces services, comme le montre la figure II.1 :

	Niveau						
	1	2	3	4	5	6	7
Confidentialité avec connexion sans connexion d'un champ particulier	oui	oui oui	oui oui	oui oui	oui oui	oui oui oui	oui oui oui
Authentification			oui	oui			oui
Intégrité avec reprise sans reprise d'un champ particulier			oui	oui oui			oui oui oui
Non-répudiation							oui
Controle d'accès			oui	oui			

Figure II. 1.Sécurité et niveaux de l'architecture OSI [23]

Cette méthode résulte de l'étude des exigences de l'expéditeur et du destinataire lors de l'utilisation des cinq services de sécurité présentés précédemment :

- 1) Seul le destinataire doit recevoir le message.
- 2) Le destinataire doit recevoir le message.
- 3) L'expéditeur du message doit être identifié avec certitude.
- 4) Le message transmis et le message reçu doivent être identiques.
- 5) La réception du message ne peut être contestée par le destinataire.
- 6) La transmission du message ne peut être contestée par l'expéditeur.
- 7) L'expéditeur ne peut accéder à certaines ressources que s'il y est autorisé.

II.5. Attaques principales d'un réseau Wi-Fi

II.5.1. C'est quoi une attaque ?

Une attaque est l'utilisation d'une faille d'un système informatique, tel qu'un système ou un logiciel d'exploitation, à des fins inconnues de l'exploitant du système. Tout ordinateur relié à un réseau d'information est susceptible d'être attaqué [24].

Afin de mettre en place des mesures préventives pour arrêter ces attaques, il est essentiel de comprendre les principaux types d'attaques.

- Une station d'espionnage doit être utilisée pour attaquer un réseau, qu'elle se trouve à l'intérieur ou à l'extérieur de la région de service, à condition qu'elle dispose d'une antenne directionnelle. Qu'elle se trouve à l'intérieur ou à l'extérieur de la région de service, tant qu'elle dispose d'une antenne directionnelle, la figure II.2, ci-dessous illustre les principales attaques dans le monde [24] :

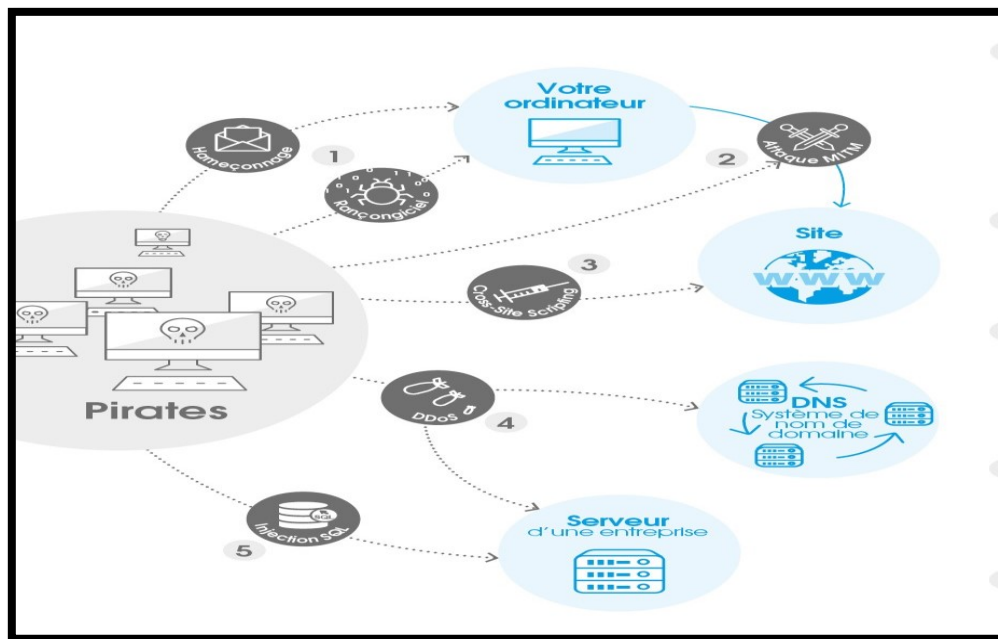


Figure II. 2. Différentes cas de cyberattaque [24]

II.5.2. Motivation et objectif de l'attaquant

Les attaquants, parfois appelés "hackers", peuvent avoir des motivations diverses.

- L'attrait interdite, le besoin d'argent et le désir d'argent (par exemple, abuser du système financier).
- La célébrité, ou le désir de faire du mal aux autres (pour impressionner des amis, détruire des données, empêcher le système de fonctionner).

- Les pirates informatiques peuvent être des travailleurs malhonnêtes, des journalistes véreux, des rivaux (espions de l'industrie), des agents de la police ou des agences de renseignement gouvernementales, des terroristes ou simplement des criminels solitaires [25 ;26].

Souvent, un attaquant veut prendre le contrôle d'une machine afin de mener à bien l'activité qu'il souhaite. Il existe plusieurs approches pour y parvenir :

- Obtenir des informations pertinentes pour une attaque.
- Profiter des failles du système.
- Perturber violemment le système.

II.5.3. Différentes attaques d'un réseau Wi-Fi

II.5.3.1. Usurpation (spoofing)

a) Description du fonctionnement

- Le protocole ARP est utilisé pour effectuer la conversion des adresses IP (32 bits dans IPv4) en adresses MAC (42 bits).
- Comme les paquets ARP sont envoyés d'un système à l'autre, chaque système du réseau local maintient une base de données locale des correspondances entre l'adresse IP et l'adresse MAC [27].

b) Principe d'attaque ARP spoofing

- Le système pirate notifie au système cible, au moyen de paquets ARP, qu'il est la passerelle à laquelle appartient l'adresse IP de la nouvelle adresse MAC.
- Tout le trafic du système cible est dirigé vers le système pirate.
- La machine malveillante peut alors écouter passivement, modifier et rediriger la communication vers sa destination prévue [28].
- La figure II.3 illustre les étapes de déroulement de l'attaque [29] :

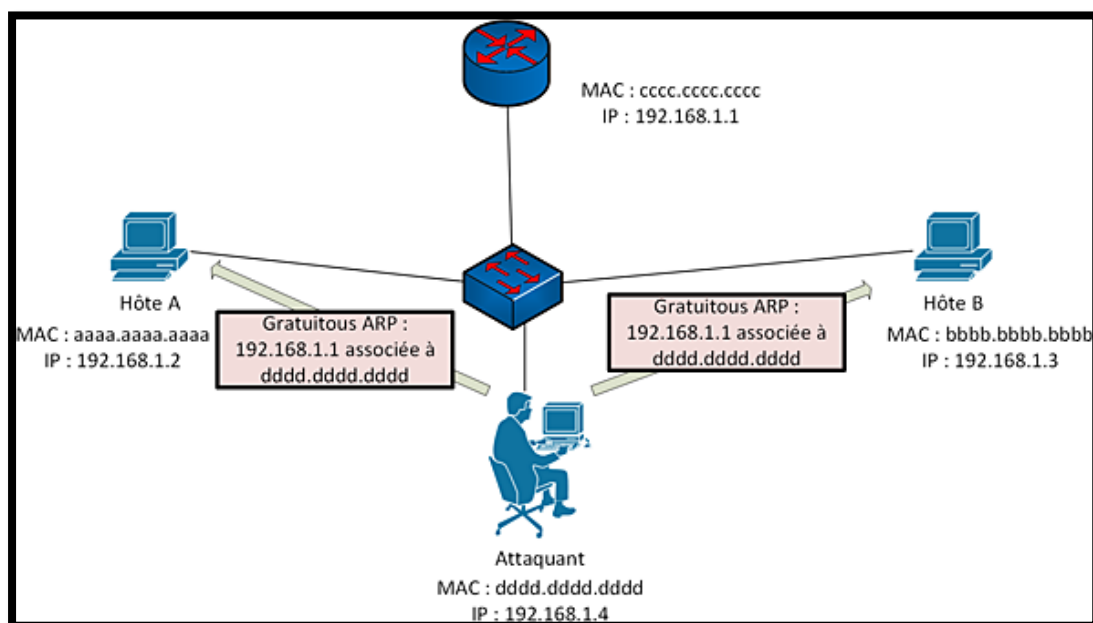


Figure II. 3. Attaque ARP spoofing [29]

c) Outil de défaite : Il faut utiliser les VLANs pour diviser le réseau afin de se prémunir contre ce type d'attaque.

II.5.3.2. Attaque homme au milieu « MEN-IN-THE-MIDDLE »

Le trafic vers le port SSL (HTTPS sur le port 443 TCP) est détourné de manière transparente vers le poste de travail de l'attaquant, qui agit comme un serveur HTTPS (HyperText Transfer Protocol Secure sockets), dans le cadre d'une attaque contre le cryptage SSL.

a) Fonctionnement de l'attaque

Une attaque de type "Man-in-the-Middle" dans un réseau Wi-Fi consiste à installer un point d'accès frauduleux à proximité d'autres points d'accès légitimes. Lorsqu'une station tente de se connecter au réseau, elle fournit involontairement au point d'accès frauduleux les informations nécessaires à la connexion.

Ces informations peuvent alors être utilisées par une station pirate qui intercepte le trafic en écoutant les échanges entre les stations et les points d'accès légitimes [30]. Pour ce faire, la station pirate récupère l'adresse MAC d'une station légitime et de son point d'accès, et s'intercale entre les deux pour capturer les informations confidentielles qui y circulent.

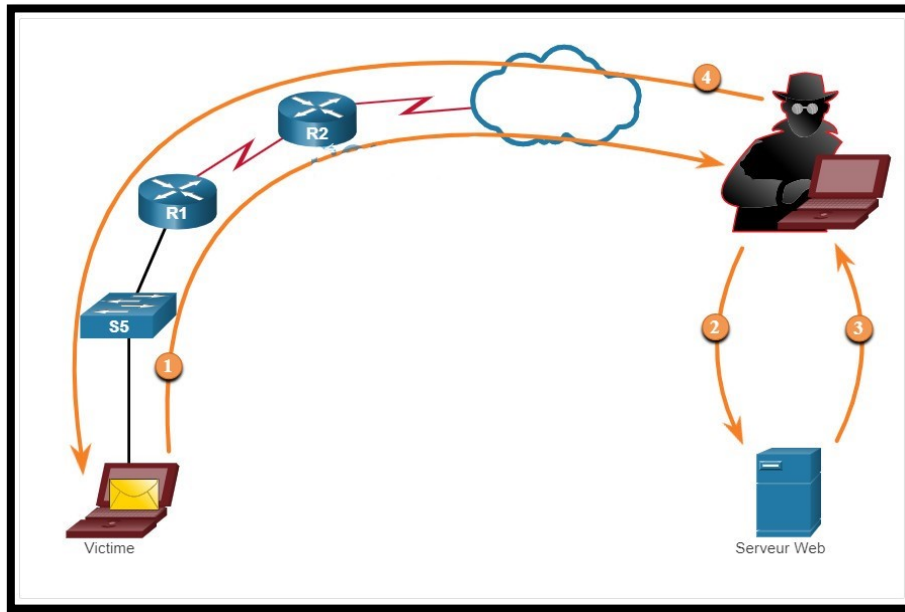


Figure II. 4. Attaque MITM [30]

- b) **Outil de défense :** Afin de contrer ce type d'attaque, l'utilisation d'un VPN avec le protocole de chiffrement IP-sec est recommandée.

II.5.3.3. Déni de service (DOS)

Le déni de service (DOS) est une attaque qui consiste à perturber le réseau en le saturant de messages, qu'ils soient valides ou non, et qui affectent la disponibilité des ressources du réseau. Cette attaque peut être menée de différentes manières, notamment au niveau des couches 1 et 2 du modèle OSI.

❖ Attaques par interférence radio au niveau de la couche physique : exploitez la sensibilité des ondes radio aux interférences et utilisez de puissants émetteurs radio pour interférer avec toutes les communications dans un réseau Wi-Fi.

❖ Les attaques de dés authentification au niveau de la couche MAC exploitent une faille dans la norme 802.11, qui ne fournit pas de sécurité pour les trames de gestion. Les pirates peuvent se faire passer pour un point d'accès (AP) et utiliser des trames de dés authentification pour déconnecter des utilisateurs spécifiques du réseau, ou envoyer un flux continu de ces trames à toutes les stations connectées au point d'accès pour empêcher l'utilisation du réseau. Des mécanismes de sécurité sont nécessaires pour prévenir et combattre ces attaques et maintenir la disponibilité des ressources du réseau [30].

II.5.3.4. Intrusion

L'intrusion dans un réseau Wi-Fi désigne le processus de pénétration dans le système informatique du réseau en question, permettant ainsi de consulter ou de modifier des données sensibles telles que des bases de données, des fichiers ou des e-mails, et de bénéficier d'un accès à Internet. En l'absence de mesures de sécurité efficaces, l'intrusion est facilitée par la simple association à l'un des points d'accès du réseau [31].

II.5.3.5. Attaque de dictionnaire

Pour le premier type d'intrusion, l'attaquant doit réussir à tromper le système d'authentification. Pour cela, il doit soit retrouver le mot de passe en clair lors de son échange, soit attaquer l'algorithme de chiffrement lors de son chiffrement. Une autre méthode consiste à utiliser une attaque par dictionnaire, où l'attaquant essaie des millions de mots de passe jusqu'à ce qu'il trouve le bon. Cette méthode peut être effectuée en ligne ou hors ligne [32].

- **Lors d'une attaque en ligne**, l'attaquant essaie successivement chaque mot de passe jusqu'à ce qu'il trouve le bon.
- **Lors d'une attaque hors ligne**, l'attaquant enregistre la boîte de dialogue d'authentification réussie, qui contient le défi et la réponse de l'utilisateur. Il utilise ensuite le même défi et le même algorithme pour tester des millions de mots de passe jusqu'à ce qu'il trouve la même réponse que l'utilisateur [32].

II.5.3.6. Détourner une session existante

Il est possible de modifier l'adresse MAC des adaptateurs Wi-Fi, ce qui peut permettre à un attaquant de détourner facilement des sessions en écoutant le trafic sur le réseau jusqu'à l'arrivée d'un utilisateur légitime. Une fois que cet utilisateur s'est identifié, le pirate peut observer son adresse MAC et configurer son propre adaptateur Wi-Fi pour imiter cette adresse. Cette technique est appelée "spoofing d'adresse MAC"[33].

II.5.3.7. Attaque de trou noir « BlackHole »

Une attaque par trou noir est une attaque active conçue pour empêcher certains messages reçus par les nœuds de routage. Les suppressions de paquets peuvent être modifiées à partir d'une manière qui n'augmente pas la suspicion d'attaques de nœuds. Il a plus de

variantes ou pas trop similaire, mais avec des objectifs différents. Parmi ces variantes on peut citer :

- **Loupe de routage** : permet aux nœuds de créer des boucles dans le réseau.
- **Trou gris** : seuls les paquets routés sont autorisés à transférer et transmettre des données.
- **Extorsion** : permet à un nœud attaquant d'isoler un autre nœud. Les nœuds le font en envoyant des messages d'erreur (par exemple, des erreurs de routage).

II.5.3.8. Espionnage (sniffing)

L'écoute clandestine, également connue sous le nom de reniflement, est l'une des attaques les plus courantes contre la confidentialité des données sur les réseaux sans fil. Cette attaque consiste à intercepter les transmissions radio de tous les utilisateurs du réseau, permettant à l'attaquant de récupérer toute information transmise.

Pour mener à bien cette attaque, le pirate n'a besoin que d'un adaptateur Wi-Fi capable de lire toutes les données circulant sur le réseau sans fil, même celles qui ne lui étaient pas destinées. Les attaquants peuvent alors utiliser des logiciels d'analyse de réseau tels que "Wire-Shark" ou "Ki-Smet" pour examiner les données collectées et obtenir des informations sensibles.

II.6. Risques liés aux réseaux sans fil

II.6.1. Manque de sécurité

Les ondes radio ont une forte capacité inhérente à parcourir de longues distances dans toutes les directions, ce qui rend difficile la limitation de leur portée. De plus, la propagation des ondes radio doit être considérée en trois dimensions, car elles peuvent aussi se propager d'une couche à l'autre, mais avec une plus grande atténuation. Cette propagation incontrôlée des ondes radio permet aux personnes non autorisées d'écouter facilement sur les réseaux sans fil. De plus, il est possible d'installer un réseau sans fil dans une entreprise à l'insu du service informatique. Tout ce qu'un employé doit faire est de connecter le point d'accès à une prise réseau, et tout le trafic réseau est accessible à portée du point d'accès, exposant le réseau à des risques de sécurité [34].

II.6.2. War-Driving

Depuis sa création, la technologie Ethernet sans fil a suscité l'intérêt des pirates, qui emploient de nouvelles formes de piratage comme le wardriving (ou

war-xing). La pratique, originaire des États-Unis, consiste à localiser des réseaux sans fil publics ou privés et à tenter de les infiltrer à l'aide d'un ordinateur portable équipé d'une carte réseau PCMCIA 802.11b. Les pirates ont parcouru les quartiers dans leurs voitures, recherchant les fréquences du réseau. Cette technique peut être améliorée en utilisant des antennes directionnelles et un puissant logiciel de détection. Des logiciels spécialisés peuvent même tirer parti des dispositifs de géolocalisation tels que le GPS pour créer des cartes précises. Les cartes ainsi créées peuvent mettre en évidence des réseaux sans fil non sécurisés, qui fournissent parfois un accès à Internet. De nombreux sites ont été créés pour profiter de ces informations [35].

II.6.3. Risques liés en matière de sécurité

Les risques associés aux réseaux sans fil mal sécurisés peuvent être très préjudiciables aux utilisateurs et aux propriétaires de ces réseaux.

- Les attaquants peuvent utiliser des techniques d'interception de données pour espionner les transmissions des utilisateurs du réseau sans fil, leur permettant d'accéder à des informations sensibles telles que des mots de passe ou des informations de carte de crédit.
- Le détournement de **connexion** est une autre technique utilisée par les attaquants pour accéder à un réseau local ou à Internet. Les attaquants peuvent utiliser des outils de piratage pour intercepter le trafic Web et rediriger le trafic vers des sites Web malveillants, où ils peuvent voler des informations sensibles ou installer des logiciels malveillants sur les ordinateurs des utilisateurs.
- L'interférence de transmission est la transmission de signaux radio de telle sorte qu'ils interfèrent, ce qui peut rendre les réseaux sans fil inutilisables. Les attaquants peuvent utiliser cette technique pour empêcher les utilisateurs légitimes d'accéder à un réseau sans fil, ce qui peut perturber les opérations quotidiennes.

Enfin, le déni de service est une autre forme d'attaque qui peut rendre un réseau inutilisable en envoyant des commandes factices et en saturant les ressources du réseau. Les attaquants peuvent utiliser cette technique pour empêcher les utilisateurs légitimes d'accéder à un réseau sans fil, ce qui peut perturber les opérations quotidiennes. C'est pourquoi les réseaux sans fil doivent être correctement sécurisés

en utilisant des protocoles de sécurité tels que WPA2, en changeant régulièrement les mots de passe et en utilisant des pare-feux pour empêcher tout accès non autorisé. En prenant des mesures de sécurité appropriées, les utilisateurs et les propriétaires de réseaux sans fil peuvent réduire considérablement les risques de sécurité et protéger leurs informations sensibles contre les attaques potentielles [35].

II.7. Solutions pour sécuriser un réseau Wi-Fi

II.7.1. Sécurité élémentaire

La sécurité de base du réseau Wi-Fi est essentielle pour protéger les données et la propriété privée en ligne. En mettant en œuvre un accord de sécurité fiable, en sélectionnant des mots de passe complexes et en maintenant les conditions finales de l'équipement, vous pouvez réduire le risque d'attaque et d'invasion. La sécurité du réseau Wi-Fi est une étape importante pour assurer la sécurité des cheminées numériques et conserver des informations personnelles.

Ces technologies peuvent être utilisées de manière complémentaire comme suit :

II.7.1.1 Identificateur de réseau

Le SSID (Set Identifier Service) est le nom du réseau sans fil configuré sur le point d'accès. Il permet au poste client de choisir le point d'accès qu'il espère détecter plusieurs réseaux sans fil dans un environnement direct.

Pour nous connecter au point d'accès, nous devons comprendre l'identifiant réseau (SSID). Par conséquent, il peut être recommandé de modifier SSID et d'interdire la publicité sur le réseau sans fil. Cependant, vous devez savoir que vous pouvez facilement trouver cet identifiant grâce à une écoute simple. Par conséquent, basé sur la restriction de l'accès au réseau sans fil est le fantasme sur SSID [36].

II.7.1.2 Mot de passe

Il existe plusieurs méthodes d'authentification, mais les mots de passe sont les plus courants. Selon l'organisation SANS (SysAdmin, Audit, Network, Security) de 165 000 professionnels de la sécurité, les mots de passe faibles sont la deuxième vulnérabilité système la plus courante après le manque de mises à jour régulières. Par conséquent, il est essentiel de choisir des mots de passe forts qui rendent difficile le décryptage par des outils automatisés et empêchent les devinettes par des individus malveillants.

II.7.1.3 Filtrage d'adresse MAC

Chaque adaptateur réseau a sa propre adresse physique. Ces points d'accès sont généralement autorisés à permettre la liste d'accès aux droits (appelée ACL) dans l'interface de configuration, qui est basée sur l'adresse MAC de l'appareil autorisé à se connecter au réseau sans fil. Ces mesures de prévention restrictives peuvent restreindre l'accès au réseau à de nombreux ordinateurs. En retour, cela ne peut pas résoudre le problème des secrets de communication. Veuillez noter que certains adaptateurs permettent de modifier son adresse, alors faisant semblant d'être d'autres adaptateurs dans d'autres positions [37].

II.7.1.4 Protection par adresse IP

En allouant les adresses IP fixes aux stations de radio bénéficiant de connexions sans fil, le risque d'invasion externe est beaucoup plus faible. Par conséquent, il est nécessaire d'arrêter la fonction DHCP au niveau du serveur connecté à la borne WiFi.

II.7.1.5 Sécurité des points d'accès

Modifier les paramètres par défaut des points d'accès constitue une démarche cruciale pour assurer la sécurité d'un réseau sans fil. Les étapes à suivre incluent [38] :

- Remplacer les mots de passe par défaut (en particulier pour les comptes administrateurs) par des mots de passe robustes.
- Ajuster les paramètres par défaut (tels que l'adressage privé en utilisant DHCP ou l'adresse de l'interface).
- Désactiver les services non utilisés (SNMP, Telnet, etc.).
- Réguler la puissance d'émission du point d'accès selon les besoins.

Il est également important de mettre à jour le micrologiciel (firmware) de la station de base dès qu'une mise à jour est disponible. Des tests approfondis sont nécessaires pour garantir la compatibilité avec l'infrastructure existante après la mise à niveau. Renommer le SSID par défaut est largement recommandé et il vaut mieux ne pas choisir un SSID attractif [38].

II.7.2. Sécurité renforcée

Les méthodes suivantes peuvent être appliquées pour améliorer la sécurité du réseau :

- Introduction du VPN, le VPN utilise un protocole de tunnellation pour crypter les données de l'entreprise et permet aux utilisateurs de se connecter au réseau en toute sécurité.
- Pare-feu Un pare-feu surveille le trafic interne et externe pour protéger un réseau informatique des attaques Internet et filtrer les paquets de données échangés avec le réseau. Il peut être configuré comme si le point d'accès dispose d'une connexion Internet et peut être un serveur IPSEC pour le client sans fil [39].
- En utilisant un serveur RADIUS, vous pouvez améliorer votre authentification, ce qui vous permet de gérer plus efficacement les comptes utilisateurs, les autorisations et leurs droits d'accès associés.

Bref, il est recommandé de mettre en place un VPN, un pare-feu, et d'améliorer l'authentification avec un serveur RADIUS pour sécuriser efficacement votre réseau.

II.7.3. Cryptages des données

II.7.3.1 Définition

Le cryptage est une technique utilisée pour garder les informations confidentielles et s'assurer qu'elles sont accessibles par un seul destinataire authentifié. Il est principalement basé sur l'arithmétique, convertissant les lettres du message en nombres puis calculant les nombres afin qu'ils soient incompréhensibles et puissent être déchiffrés par le destinataire. Le chiffrement consiste à brouiller le message pour le garder privé, tandis que le déchiffrement nécessite une clé de déchiffrement. Il y'a deux types de chiffrement : symétrique et asymétrique.

- a) **La cryptographie symétrique :** également appelée cryptographie conventionnelle ou cryptographie à clé privée, utilise une clé unique pour chiffrer et déchiffrer les messages. Les algorithmes de chiffrement les plus couramment utilisés sont DES (Data Encryption Standard), Triple DES et AES. Cependant, la distribution de clés sur un grand réseau présente un défi important car elle nécessite le partage d'une clé unique avec chaque participant [40]

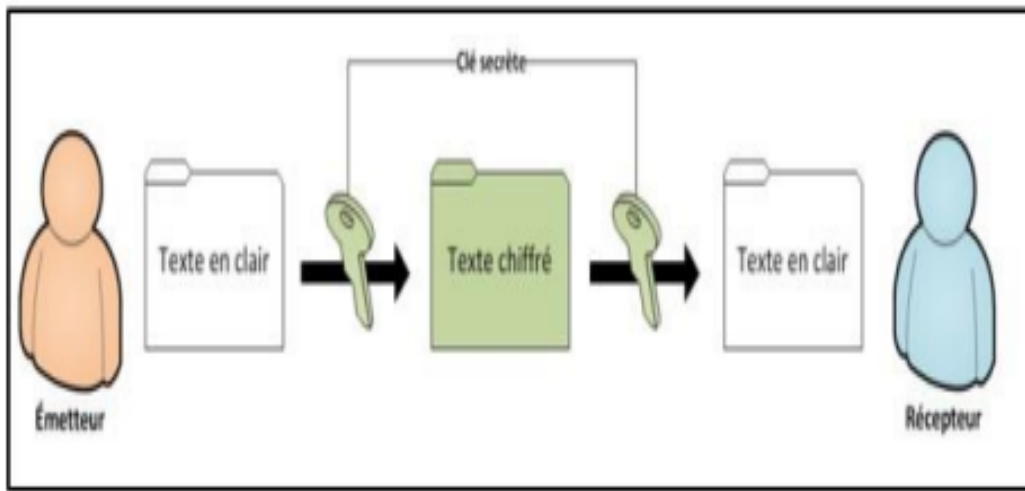


Figure II. 5. Cryptage symétrique [40].

b) Le cryptage asymétrique : à clé publique utilise deux clés différentes pour chaque utilisateur. L'une est une clé privée que seul le propriétaire connaît, et l'autre est une clé publique à laquelle tout le monde peut accéder. Un message chiffré avec une clé publique ne peut être déchiffré qu'avec la clé privée correspondante, car les clés publique et privée sont mathématiquement liées par l'algorithme de chiffrement. En effet, ces deux clés sont générées en même temps. Ainsi, une clé est utilisée pour le chiffrement et l'autre pour le déchiffrement. Le principal avantage de la cryptographie à clé publique est qu'elle résout le problème de l'envoi de clés privées sur des réseaux non sécurisés. Il est plus lent que la plupart des cryptographies à clé privée, mais il est recommandé pour plusieurs raisons :

- Meilleure évolutivité pour les systèmes comptant des millions d'utilisateurs.
- Les messages peuvent être signés, garantissant l'authentification et la non-répudiation.

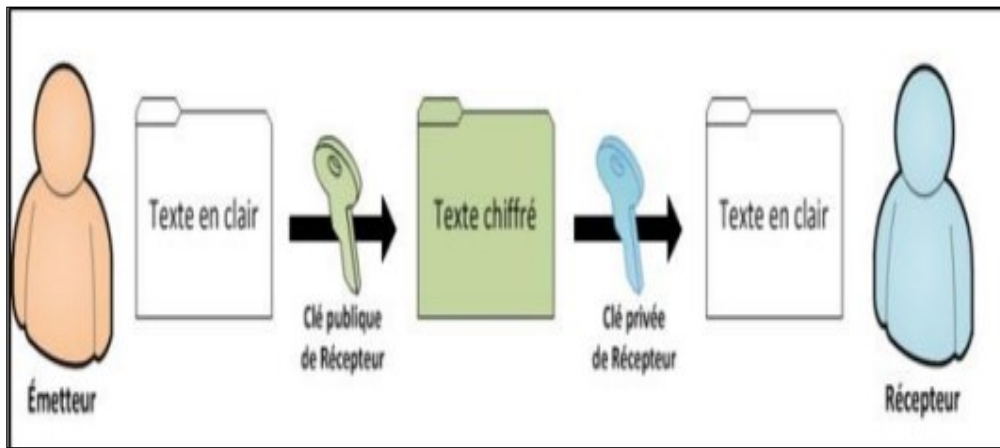


Figure II. 6. Cryptage asymétrique [40]

II.7.3.2 Etude des protocoles de sécurité liés aux Wi-Fi

Des protocoles sont en cours d'évaluation pour améliorer la sécurité des réseaux Wi-Fi.

Ces évaluations ont pour but de :

- Assurer la confidentialité des données échangées au sein du réseau.
- Activez l'authentification client pour vous assurer que seuls les utilisateurs autorisés peuvent accéder à votre réseau.
- Assurer l'intégrité des données en s'assurant que les données échangées n'ont pas été altérées en transit sur le réseau.

II.7.3.2.1 Protocole WEP (Wired Equivalent Privacy)

A. Qu'est-ce que le WEP ?

Le protocole WEP fait partie de la norme internationale IEEE 802.11, ratifiée en septembre 1999. Il s'agissait du premier mécanisme de cryptage mis en œuvre dans les réseaux sans fil pour sécuriser les communications radio. Le protocole WEP utilise une clé partagée (K) entre les parties communicantes pour protéger les corps des trames de données transmises. Le principe du protocole WEP repose sur l'utilisation de l'algorithme de chiffrement en mode flux RC4. À l'aide d'une clé pré-partagée (PSK) longue de 40 à 104 bits (une version améliorée de WEP) et d'un vecteur d'initialisation (IV) de 24 bits envoyés non chiffré avec chaque paquet, WEP crée un flux de clé (Ks) pour générer un flux de clés, une séquence pseudo-aléatoire d'octets[41].

B. Présentation de l'algorithme RC4 et PSK [42]

❖ **RC4 :**

RC4 est un algorithme de chiffrement de flux symétrique qui utilise le mode OFB (output feedback). Cette méthode est très rapide, environ dix fois plus rapide que DES. De plus, les boîtiers S utilisés dans RC4 s'adaptent à l'exécution. Cela signifie que les mêmes bits ne renvoient pas toujours le même résultat, ce qui rend RC4 très efficace. RC4 est un algorithme de génération de bits pseudo-aléatoire. Cela vous permet d'obtenir de la clé privée une séquence binaire aléatoire et unique de la même longueur que le texte en clair. Ensuite, une opération XOR au niveau du bit est effectuée pour obtenir la forme chiffrée. Le destinataire peut récupérer le message en clair en effectuant une opération XOR entre la séquence chiffrée reçue et la séquence aléatoire d'origine [42].

- ❖ **Une clé pré-partagée (PSK – Pre-shared key) :** Il s'agit d'une clé secrète partagée qui doit être préalablement échangée entre les deux parties à l'aide d'un canal sécurisé avant d'être utilisée. La Figure 2.8 montre le mécanisme total de chiffrement

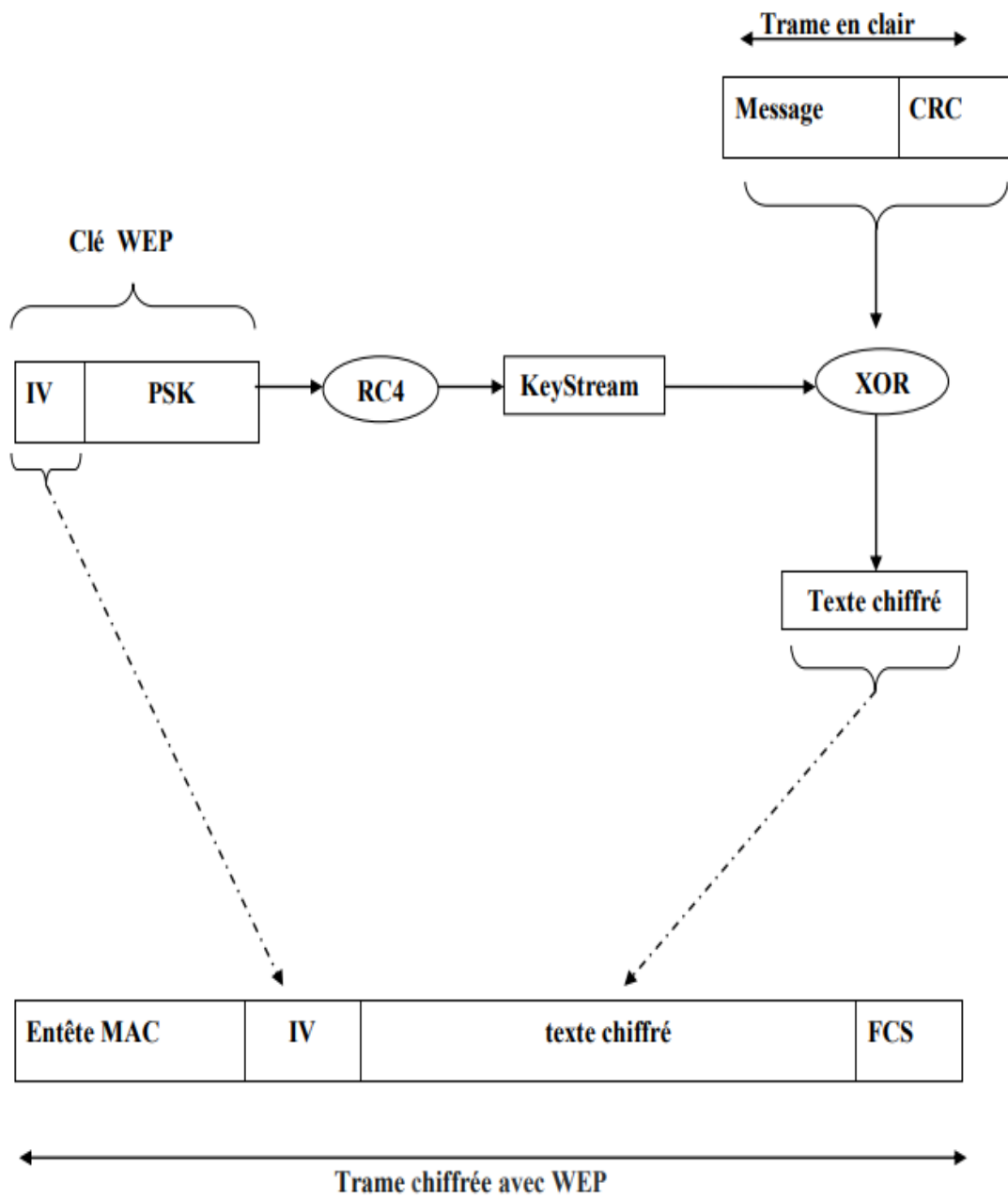


Figure II.7. Le chiffrement WEP [42].

c) Failles du WEP

Les principaux inconvénients du WEP sont :

- Les contrôles d'intégrité et les algorithmes d'authentification sont très faciles à contourner.
- Le protocole utilise un vecteur d'initialisation (IV) 24 bits trop court, permettant aux attaquants d'obtenir des clés WEP en analysant le trafic réseau.
- Le protocole WEP utilise l'algorithme de chiffrement RC4, ce qui le rend vulnérable aux attaques d'analyse statistique.
- Les clés WEP sont souvent partagées entre les utilisateurs et ne sont pas mises à jour régulièrement, ce qui rend les réseaux vulnérables aux attaques par force brute.

C. Protocole WPA (Wi-Fi Protected Access)

WPA (Wi-Fi Protected Access) a été proposé en octobre 2002 en réponse à des vulnérabilités découvertes dans le protocole WEP. Il s'agit d'une version "allégée" du protocole 802.11i qui utilise un protocole d'authentification et un algorithme de chiffrement fort appelé TKIP (Temporary Key Integrity Protocol). Les fonctionnalités de WPA sont les suivantes. [42]

- **Authentification:** WPA peut fonctionner avec un serveur d'authentification 802.1X (généralement un serveur RADIUS) qui distribue des clés uniques à chaque utilisateur. Il propose également un mode moins sécurisé appelé PSK, qui repose sur un secret partagé par tous les utilisateurs.
- **Gestion des clés:** WPA utilise le protocole TKIP pour surmonter les faiblesses du WEP en changeant périodiquement la clé de cryptage.
- **Intégrité des messages:** WPA utilise des codes de vérification d'intégrité (MIC) au lieu de CRC pour garantir l'intégrité des messages échangés sur le réseau.
- **Protocole TKIP :** WPA améliore la sécurité grâce à la génération de clés aléatoires et à la possibilité de modifier les clés de chiffrement plusieurs fois par seconde. Contrairement au WEP, le WPA augmente la sécurité en autorisant une clé unique pour chaque station connectée au réseau sans fil. Les clés WPA sont automatiquement générées et distribuées par les points d'accès (AP) si le réseau est compatible. De plus, des validateurs de données sont utilisés pour vérifier l'intégrité

des informations reçues et s'assurer qu'elles n'ont pas été altérées. Les avantages de TKIP par rapport aux clés WEP sont :

- Vecteur d'initialisation 48 bits (IV) au lieu de 24 bits pour WEP.
- Génération et distribution de clés : WPA génère et distribue périodiquement des clés de chiffrement à chaque client, en utilisant une nouvelle clé à chaque trame, éliminant ainsi le besoin d'utiliser la même clé WEP pendant des semaines ou des mois.[42]
- Code d'intégrité de message : WPA utilise un code de contrôle d'intégrité (MIC) à 8 octets pour vérifier l'intégrité de la trame, tandis que WEP utilise une valeur de contrôle d'intégrité (ICV) à 4 octets.

➤ **Architectures WPA :**

Le WPA peut fonctionner selon deux modes :

- 🚦 **WPA Enterprise** : le mode Enterprise nécessite l'utilisation d'un serveur d'authentification tel qu'un serveur RADIUS et une infrastructure d'authentification 802.1x basée sur des contrôleurs de réseau (points d'accès). Cela nécessite un ordinateur serveur dédié et est quelque peu coûteux. [42]
- 🚦 **WPA Personnel** : Le mode personnel permet de mettre en place une infrastructure sécurisée basée sur WPA-PSK (Pre-Shared Key) sans passer par un serveur d'authentification. Le WPA personnel utilise une clé commune appelée PSK qui est déployée sur tous les appareils (points d'accès et postes de travail clients). Contrairement au WEP, il n'est pas nécessaire d'entrer une longueur de clé prédéfinie. WPA vous permet d'entrer une phrase de passe qui est convertie en PSK par un algorithme de hachage. La première version de WPA ne prenait en charge que les réseaux en mode infrastructure. Cela signifie que les réseaux sans fil peer-to-peer (mode ad-hoc) ne peuvent pas être protégés.

➤ **Fonctionnement de WPA :**

Étant donné que WPA utilise un vecteur d'initialisation (IV) de 48 bits, il est plus avancé que WEP et le recyclage IV est beaucoup plus lent. De plus, WPA offre des méthodes de connectivité plus sophistiquées utilisant des configurations avancées telles que les clés pré-partagées et l'authentification LDAR et RADIUS. Une clé WPA est créée lorsque l'utilisateur se connecte au réseau. WPA génère périodiquement de nouvelles clés pour chaque utilisateur en combinaison avec la longueur du numéro IV, ce qui rend le piratage beaucoup plus difficile. Pour garantir l'intégrité des paquets, WPA ajoute un code de vérification d'intégrité (ICV) de 4 octets à chaque paquet envoyé. Cependant, un attaquant pourrait intercepter la transmission, modifier le contenu, recalculer l'ICV et renvoyer le paquet sans que personne ne s'en aperçoive. WPA résout ce problème en utilisant un message d'intégrité de 8 octets qui rejoint la charge utile chiffrée et alimente le calcul ICV, éliminant les opportunités suivantes de falsification de paquets. Cela peut réduire considérablement l'usurpation d'adresse IP source.

➤ **Les failles de WPA.**

Le WPA présente quelques faiblesses, notamment une sensibilité aux attaques de type déni de service. Si un attaquant envoie au moins deux paquets chaque seconde en utilisant une clé de chiffrement incorrecte, le point d'accès sans fil peut tuer toutes les connexions utilisateur pendant une minute afin d'éviter les accès non autorisés. Cela peut entraîner le blocage de tout le réseau sans fil.

En outre, le WPA présente certains défauts en matière de sécurité :

- L'absence d'un SSID sécurisé, qui est une chaîne de caractères alphanumériques utilisée pour identifier un réseau sans fil.
- La nécessité d'une déconnexion rapide et sécurisée.
- La nécessité de dé-authentification et dé-association sécurisées.
- L'utilisation d'un meilleur protocole de chiffrement, tel que l'AES (Advanced Encryption Standard).

Ces lacunes ont conduit à l'évolution du WPA vers le WPA2, qui utilise l'AES pour le chiffrement et introduit des améliorations dans les autres aspects de la sécurité. Le WPA2 est considéré comme plus robuste et plus sûr que le WPA.

D. Protocole WPA2 /802.11i

WPA présente certaines faiblesses, notamment la vulnérabilité aux attaques par déni de service. Si un attaquant envoie plus d'un paquet par seconde avec la mauvaise clé de cryptage, le point d'accès sans fil peut suspendre toutes les connexions des utilisateurs pendant une minute pour empêcher tout accès non autorisé. Cela peut bloquer l'ensemble du réseau sans fil.

- De plus, WPA présente des failles de sécurité.
- Absence de SSID sécurisés (chaînes alphanumériques utilisées pour identifier les réseaux sans fil).
- Besoin d'une séparation rapide et sûre.
- La nécessité d'une dés-authentification et d'une dissociation sécurisée.
- Utilisation de meilleurs protocoles de cryptage tels que AES (Advanced Encryption Standard).

En raison de ces lacunes, WPA a évolué en WPA2. WPA2 utilise AES pour le cryptage et introduit d'autres améliorations de sécurité. WPA2 est considéré comme plus robuste et sécurisé que WPA.

➤ Qu'est-ce que l'AES et CCMP ?

L'AES (Advanced Encryption Standard) est un algorithme de chiffrement largement utilisé pour sécuriser les données contre les regards indiscrets. L'AES comprend trois chiffrements par bloc, chacun ayant un nombre différent de combinaisons de clés possibles [42] :

- AES-128 : longueur de clé de 128 bits = $3,4 \times 10^{38}$ combinaisons possibles
- AES-192 : longueur de clé de 192 bits = $6,2 \times 10^{57}$ combinaisons possibles
- AES-256 : longueur de clé de 256 bits = $1,1 \times 10^{77}$ combinaisons possibles

En ce qui concerne la sécurité des réseaux sans fil, le protocole de chiffrement CCMP (Counter Mode CBC-MAC Protocol) est utilisé comme standard de chiffrement pour la norme IEEE 802.11i. CCMP est basé sur l'AES, mais évite que chaque message utilise le même bloc d'initialisation, ce qui renforce la sécurité du chiffrement. Ainsi, l'option de sécurité WPA2-AES-CCMP offre une protection efficace pour les réseaux sans fil [42].

➤ **Présentation WPA2**

Le WPA2 (Wi-Fi Protected Access 2) est la version améliorée de WPA. Comme son prédécesseur, il assure le chiffrement et l'intégrité des données pour les réseaux sans fil. Cependant, le WPA2 offre de nouvelles fonctionnalités de sécurité telles que le "Key Caching" et la « Pré-Authentification » [42].

➤ **Key Caching**

Le "Key Caching" est une fonctionnalité importante du WPA2 qui permet à un utilisateur de conserver la clé PMK (Pairwise Master Key) du protocole WPA, une fois qu'une authentification a été effectuée avec succès avec un point d'accès spécifique. Cette fonctionnalité est très utile pour les utilisateurs mobiles, car elle leur permet de ne s'authentifier qu'une seule fois avec un point d'accès spécifique, même s'ils se déplacent entre plusieurs points d'accès dans le même réseau sans fil [42]

Lorsqu'un utilisateur s'authentifie avec succès auprès d'un point d'accès, le PMKID (Pairwise Master Key Identifier) est généré. Le PMKID est un hachage unique de la clé PMK, de l'adresse MAC du point d'accès et du client mobile, ainsi qu'une chaîne de caractères. Grâce à ce PMKID, l'utilisateur peut réutiliser la clé PMK lors de ses prochaines transactions avec le même point d'accès, sans avoir besoin de s'authentifier à nouveau.

Le PMKID est utilisé pour identifier de manière unique la clé PMK et permet une reconnaissance plus rapide et plus efficace lors de la connexion ultérieure de l'utilisateur avec le même point d'accès. Cependant, il est important de noter que le PMKID n'est pas une clé de sécurité en soi, mais plutôt un identifiant de la clé PMK.

Il convient également de noter que la sécurité de la clé PMK dépend de sa complexité. Il est donc conseillé d'utiliser des clés PMK longues et complexes pour garantir une sécurité optimale. En général, le "Key Caching" est une fonctionnalité très utile pour les utilisateurs mobiles et offre une expérience utilisateur plus fluide et plus pratique lors de la connexion à des réseaux sans fil sécurisés.

➤ **Pré-Authentification**

Cette fonctionnalité est réalisée en redirigeant les trames d'authentification envoyées par le client au point d'accès actuel vers le futur point d'accès via le réseau filaire. La fonctionnalité de "Pré-Authentification" du WPA2 permet aux utilisateurs mobiles de s'authentifier avec un autre point d'accès sur lequel ils pourraient se connecter dans le

futur. Cependant, pour bénéficier pleinement des avantages du WPA2, les entreprises doivent disposer d'un équipement spécifique, tel qu'une puce cryptographique dédiée pour effectuer les calculs requis par l'AES, ce qui peut entraîner des coûts supplémentaires.

➤ **Faibles du WPA2 :**

Malgré les avantages du protocole WPA2, il présente également quelques inconvénients. L'un des principaux problèmes est la vulnérabilité aux attaques de réinstallation de clé (KRACK). Cette attaque exploite une faiblesse dans WPA2 qui permet aux attaquants de créer un réseau clone et de forcer la victime à s'y connecter. Les hackers peuvent ainsi déchiffrer un petit paquet de données agrégées pour craquer la clé de chiffrement.

Cependant, il est important de noter que cette vulnérabilité peut être corrigée par des mises à jour de sécurité et de nombreux fabricants ont publié des correctifs pour leurs dispositifs. Malgré cette faiblesse, WPA2 est toujours considéré comme étant plus sécurisé que les protocoles précédents, tels que WEP ou WPA.

En résumé, bien que WPA2 présente des inconvénients tels que la vulnérabilité aux attaques de réinstallation de clé, il reste considéré comme le protocole de sécurité le plus sûr pour les réseaux sans fil. Les correctifs sont disponibles pour les dispositifs vulnérables, et il est important de les installer pour maintenir la sécurité de votre réseau sans fil.

F. Protocole WPA3

Le protocole WPA3 offre des protocoles de sécurité de pointe pour les réseaux sans fil. Il est basé sur le succès et l'adoption généralisée de la sécurité Wi-Fi et intègre de nouvelles fonctionnalités pour simplifier la sécurité Wi-Fi, proposer une authentification plus robuste, offrir une force cryptographique accrue pour les marchés de données hautement sensibles et maintenir la résilience des réseaux critiques [42].

Tous les réseaux WPA3 utilisent les dernières méthodes de sécurité, interdisent les anciens protocoles obsolètes et exigent l'utilisation de cadres de gestion protégés (PMF).

Étant donné que les réseaux Wi-Fi diffèrent en termes d'objectif d'utilisation et de besoins de sécurité, WPA3 inclut des fonctionnalités supplémentaires spécifiques pour les réseaux personnels et d'entreprise. Les utilisateurs de WPA3-Personal bénéficient d'une protection accrue contre les tentatives de deviner le mot de passe, tandis que les utilisateurs de WPA3-Enterprise peuvent désormais profiter de protocoles de sécurité de niveau supérieur pour les réseaux de données sensibles.

En somme, le protocole WPA3 représente une avancée significative en matière de sécurité pour les réseaux sans fil. Les fonctionnalités supplémentaires spécifiques pour les réseaux personnels et d'entreprise renforcent encore la sécurité et la robustesse de ce protocole de sécurité

➤ **Architectures WPA 3 :**

🚦 **Le protocole WPA3-Personnel** : améliore considérablement la sécurité des utilisateurs individuels grâce à une authentification renforcée basée sur un mot de passe, même lorsque les utilisateurs choisissent des mots de passe qui ne répondent pas aux recommandations générales de complexité. SAE est un protocole d'authentification qui permet aux utilisateurs de se connecter à des réseaux sans fil à l'aide d'un mot de passe partagé sans nécessiter de point d'accès. Les utilisateurs peuvent également utiliser des mots de passe faciles à retenir, ce qui facilite et accélère la connexion aux réseaux sans fil. Cette fonctionnalité utilise une technologie de cryptage de bout en bout pour garantir la protection de vos données même si un attaquant compromet votre mot de passe. En résumé, le protocole WPA3-Personal améliore la sécurité des utilisateurs individuels tout en maintenant la facilité d'utilisation et la confidentialité en transit. Le mode d'authentification de message haché HMAC-SHA256 avec une dérivation et une confirmation de clé d'au moins 256 bits est utilisé pour améliorer la sécurité de la connexion. De plus, une protection robuste des trames de gestion est assurée par un code d'authentification de message basé sur le protocole d'intégrité de diffusion/multidiffusion BIP-CMAC128 avec un cryptage minimal de 128 bits.

🚦 **Le protocole WPA3-Enterprise** : offre aux entreprises un niveau de protection plus élevé en utilisant des méthodes d'authentification plus fortes et un cryptage plus fort. Les entreprises peuvent choisir entre différentes méthodes d'authentification EAP pour garantir les connexions aux utilisateurs authentifiés. Les données sont protégées par un cryptage authentifié AES-CCMP d'au moins 128 bits, de sorte que les personnes non autorisées ne peuvent pas lire les données. Dans l'ensemble, le protocole WPA3 Enterprise offre aux entreprises une meilleure sécurité en utilisant

des méthodes d'authentification plus fortes, un cryptage plus fort et une protection renforcée du cadre administratif. Il vise à garantir que les données sont protégées contre les attaques et les intrusions, ce qui en fait l'option de sécurité sans fil optimale pour les entreprises.

✚ **Le mode optionnel de WPA3-Enterprise** avec une sécurité de niveau minimum de 192 bits est conçu pour mieux protéger les données sensibles en utilisant des protocoles de sécurité plus forts et des outils cryptographiques plus avancés. Ce mode garantit l'utilisation de la bonne combinaison d'outils cryptographiques pour assurer la sécurité des données sensibles.

Le mode de sécurité 192 bits défini par WPA3-Enterprise est conçu pour offrir une base de sécurité cohérente dans un réseau sans fil WPA3. Il utilise des protocoles de sécurité plus forts que le mode standard de WPA3-Enterprise, ce qui le rend plus adapté aux environnements où la sécurité des données est une priorité absolue.

Les outils cryptographiques utilisés dans le mode de sécurité 192 bits comprennent des algorithmes de chiffrement plus avancés et des clés plus longues, ce qui rend les données encore plus difficiles à déchiffrer pour les personnes non autorisées. Le mode de sécurité 192 bits est conçu pour protéger les données sensibles telles que les informations financières, les données personnelles et les secrets commerciaux.

En somme, le mode optionnel de WPA3-Enterprise avec une sécurité de niveau minimum de 192 bits offre une protection supplémentaire pour les données sensibles en utilisant des protocoles de sécurité plus forts et des outils cryptographiques plus avancés. Il est conçu pour offrir une base de sécurité cohérente dans un réseau WPA3 et pour protéger les données sensibles contre les attaques et les intrusions.

II.7.3.3 Protocoles de routage dans un réseau sans fil

Le routage est la fonctionnalité qui permet d'acheminer les flux de données à partir des nœuds sources vers les nœuds destinations, via des routes prédéfinies ou découvertes à la demande. Il peut être unicast, multicast ou broadcast, selon le nombre de nœuds impliqués dans la communication. Il existe deux types principaux de routage : le routage proactif, qui établit des routes à l'avance en échangeant des tables de routage, et le routage réactif, qui recherche des routes à la demande. Il existe également un type de routage hybride qui combine les deux approches.

II.7.3.3.1 Routage proactif

Les protocoles proactifs sont basés sur des algorithmes d'état de liaison et de vecteur de distance et maintiennent à jour les tables de routage grâce à des échanges réguliers de paquets de contrôle. Il existe deux types de paquets de contrôle, l'un est envoyé localement pour découvrir les voisins et l'autre est diffusé sur tout le réseau pour communiquer l'état du voisin. Les nœuds mettent à jour leurs tables de routage en recevant ces paquets et construisent de nouvelles routes basées sur les informations de topologie transportées par les paquets de contrôle. Les protocoles proactifs offrent une disponibilité de routage instantanée en cas de besoin. Les principaux protocoles actifs sont OLSR et DSDV.

➤ **DSDV** : Le protocole de routage DSDV est amélioré sur la base de l'algorithme Bellman-Ford distribué. Chaque station mobile maintient une table de routage contenant toutes les destinations possibles, le nombre de sauts nécessaires pour les atteindre et les numéros de séquence pour éviter les boucles de routage. DSDV élimine les boucles de routage et le problème du "compte à l'infini", mais est lent car il attend une mise à jour de la prochaine destination pour mettre à jour la table de distance. DSDV utilise des mises à jour périodiques et basées sur des événements, ce qui peut entraîner un contrôle excessif de la communication.

➤ **OLSR** : Le protocole OLSR (Optimized Link State Routing) est une adaptation du protocole à état de lien pour les réseaux ad hoc mobiles distribués sans entité centrale. Contrairement aux protocoles à état de liens classiques, OLSR utilise la technologie de relais multipoint (MPR) pour minimiser le nombre de messages échangés dans le réseau. Les étapes du processus de construction de route dans OLSR incluent la détection des voisins, l'élection MPR, l'annonce MPR et l'annonce des voisins, ainsi que le calcul de la table de routage chaque fois que la topologie ou les voisins changent.

II.7.3.3.2 Routage réactif

Contrairement aux protocoles actifs, qui mettent constamment à jour les tables de routage, les protocoles de routage passif évitent les inondations gourmandes en ressources. Une approche réactive consiste à lancer le processus de recherche d'itinéraire uniquement lorsque cela est nécessaire. Lorsqu'un nœud demande à relayer ses données vers une destination inconnue, le mécanisme de découverte de route est

déclenché et le nœud émetteur diffuse la demande de route dans son rayon de propagation. Les paquets voyagent à travers différents nœuds mobiles vers leurs destinations et reviennent dans l'autre sens. Le nœud source choisit alors la route la plus courte et la stocke dans son cache pour une utilisation future. Cependant, le délai nécessaire pour acheminer les paquets vers leur destination est plus important par rapport aux protocoles proactifs. Les principaux schémas réactionnels sont AODV et DSR.

➤ **AODV** : Le protocole de routage AODV est spécifique aux réseaux mobiles ad hoc et minimise le nombre de diffusions de messages en créant le chemin à la demande. Les messages utilisés pour l'établissement et le maintien des routes sont Route Request (RREQ), Route Reply (RREP), Hello message et Route Error (RERR). Une entrée de la table de routage contient l'adresse du nœud destination, l'adresse du nœud suivant, la distance en nombre de nœuds, le numéro de séquence destination, la durée de vie de la route et la liste des voisins utilisant cette route.

➤ **DSR** : Le protocole de routage DSR) est particulièrement adapté aux réseaux ad hoc mobiles multi-sauts. Il se base sur la technique de "routage source", qui consiste à ce que la source des données détermine elle-même la séquence de nœuds à travers lesquels les paquets seront transmis. En cas d'absence de route vers une destination, la source envoie un Route_Request qui est renvoyé par chaque nœud intermédiaire avec l'ajout de son identificateur ID. Lorsque le Route_Request parvient à la destination, celle-ci établit la route complète de la source vers la destination et retourne un Route_Reply contenant la route sélectionnée. Si un lien est défaillant, un message Route_Error est envoyé à la source pour qu'elle remplace la route brisée.

➤ **Protocoles hybrides**

Enfin les réseaux de capteurs peuvent emprunter les protocoles ad hoc hybrides comme ZRP (Zone Routing Protocol).

Les protocoles hybrides tirent parti des avantages des protocoles proactifs et réactifs. Ainsi, on distingue deux zones :

- IARP dans laquelle le routage est proactif
- IERP dans laquelle le routage est réactif

On a donc un routage à deux niveaux avec l'utilisation de zones qui permet d'optimiser la diffusion des paquets *route requis*. Le comportement pro-actif est limité au voisinage d'un nœud ainsi les informations de topologie ne sont transmises qu'aux voisins.

II.8. Conclusion

Dans notre fin de chapitre, lors de sa création, le protocole WEP avait pour but de fournir une solution de confidentialité équivalente au réseau filaire en s'appuyant sur l'algorithme de chiffrement RC4. Cependant, la simplicité d'utilisation a été privilégiée au détriment de la sécurité, ce qui a conduit à de nombreuses failles de sécurité. En conséquence, l'utilisation de WEP est à proscrire en entreprise et à utiliser avec parcimonie en environnement domestique.

Le développement exponentiel de l'Internet a bouleversé la sécurité des réseaux. Au fil des années, de nombreuses failles ont été découvertes dans le protocole WEP, ce qui a conduit à son remplacement progressif par des solutions plus performantes telles que le 802.1x, WPA, WPA2 et WPA3. Cependant, il est important de noter que chaque protocole a ses propres faiblesses.

En fin de compte, la sécurité des réseaux sans fil est un enjeu critique pour les entreprises et les particuliers, et il est important de prendre des mesures pour protéger les données sensibles. Les protocoles de sécurité sans fil ne doivent pas être considérés comme une solution unique, mais plutôt comme une combinaison de mesures pour renforcer la sécurité des réseaux sans fil. La mise en place de politiques de sécurité robustes, la formation des utilisateurs et la mise à jour régulière des logiciels de sécurité sont autant de mesures clés pour garantir la sécurité des réseaux sans fil.

Chapitre III

Simulation d'un
réseau local fil

III.1. Introduction

Les réseaux sans fil ont connu une croissance importante ces dernières années en raison de la prolifération des appareils mobiles et de la demande croissante de connectivité. Dans ces réseaux, la technologie Wi-Fi est largement utilisée pour fournir une connectivité Internet dans des zones géographiques spécifiques.

Un réseau Wi-Fi ad hoc est un réseau sans fil décentralisé et auto-organisé. Dans ce type de réseau, chaque nœud peut communiquer directement avec d'autres nœuds à sa portée. Lorsque deux nœuds hors de portée veulent communiquer, ils utilisent d'autres nœuds intermédiaires pour relayer leurs paquets. Ce modèle de communication multi-sauts nécessite l'utilisation de protocoles de routage pour découvrir et maintenir les chemins entre chaque source et destination.

Ce chapitre dans la première partie se concentre sur l'analyse des performances des protocoles de routage ad hoc, tels que AODV, DSDV, et DSR. Nous décrivons ensuite une méthode de simulation de ces trois protocoles selon les trois scénarios à l'aide du logiciel NS-2, qui permet le calcul de différents critères d'évaluation. Enfin, nous interprétons et évaluons les résultats obtenus lors de ces simulations.

III.2. L'environnement de simulation

Nous avons choisi deux niveaux de simulation :

- **Le premier niveau** : logiciel NS-2.
- **Le deuxième niveau** : est l'utilisation d'un hyperviseur (VMware Workstation 8)

III.2.1. Présentation du NS-2

Le simulateur réseau (NS-2) est un outil de simulation à événements discrets. Il permet la simulation des réseaux IP filaires et sans fil. Il a débuté en 1989, on l'a amélioré au fil des versions. Depuis 1995, le NS est soutenu par la contribution de DARPA (Defense Advanced Research Project Agency). En 1996, la version 2 de ns a été introduite avec, bien sûr, des améliorations architecturales. En 1997, le ns-2 a été étendu pour soutenir les réseaux sans fil. De nos jours, le NS-2 est l'outil de simulation le plus utilisée pour les réseaux typiques ainsi que pour l'attribution des ressources. NS-2 est un outil de simulation de réseaux de données. Il est bâti autour d'un langage de programmation appelé Tcl dont il est une extension. Du point de vue de l'utilisateur, la

mise en œuvre de ce simulateur se fait via une étape de programmation qui décrit la topologie du réseau et le comportement de ses composants, puis vient l'étape de simulation proprement dite et enfin l'interprétation des résultats. Cette dernière étape peut être prise en charge par un outil annexe, appelé Nam qui permet une visualisation et une analyse des éléments simulés. NS2 est en réalité un programme relativement complexe écrit en C++ et interfacé via Tcl. Pour modifier le comportement d'objets existants, il est donc nécessaire de modifier le code C++ qui en réalise l'implantation. Il existe dans le NS-2 une extension, NAM (Network Animator) qui permet la visualisation de la topologie du réseau et peut afficher les flux de paquets et des files d'attente [43].

- Le simulateur de réseau comprend une interface de programmation en Tcl et un noyau écrit en C++ qui inclut la plupart des protocoles réseaux couramment utilisés.
- ✚ **Au niveau de la couche application** : le simulateur prend en charge plusieurs types de trafic tels que le trafic parreto, ON/OFF, CBR, FTP, telnet, etc.
- ✚ **Au niveau de la couche transport** : le simulateur prend en charge les protocoles TCP et UDP.
- ✚ **Au niveau de la couche réseau** : le simulateur prend en charge le routage dans les réseaux ad-hoc (AODV, DSR, DSDV, TORA, AMODV), le routage dans les réseaux filaires (Link state, Distance vector), les réseaux multicast, IntServ, DiffServ, etc.
- ✚ **Au niveau de la couche MAC** : le simulateur prend en charge plusieurs protocoles tels que CSMA, CDMA, 802.X, Token ring, MPLS, liens satellite, etc.

III.2.1.1 Processus de simulation

Le simulateur NS-2 utilise un fichier de scénario Tcl comme entrée pour décrire le réseau à simuler. Le scénario est une séquence de commandes Tcl qui sont fournies au simulateur de réseau. En utilisant le scénario, le simulateur produit des résultats d'analyse des performances réseau dans deux fichiers distincts : un fichier trace (.tr) et un fichier NAM (.nam).

- Fichier trace (.tr)
- Fichier NAM (.nam)

a. Le langage TCL :

TCL est un langage de programmation interprété, multi-plateforme et extensible, conçu pour passer des commandes à des programmes interactifs. Il s'interface facilement avec le langage C et est économe en mémoire vive. Les utilisateurs peuvent écrire des procédures pour créer des commandes plus puissantes que celles fournies par l'ensemble préconstruit. TCL est utilisé pour la création de scripts pour automatiser des tâches répétitives et est également utilisé comme langage de script pour les outils de simulation tels que NS-2. TCL est flexible et puissant, et peut être utilisé pour une variété de tâches, y compris la création d'applications, la gestion de systèmes et la simulation de réseaux.

b. NAM :

NAM est un outil de visualisation utilisé pour représenter la topologie d'un réseau créé avec NS-2 et afficher les résultats temporels d'une trace d'exécution de NS-2. Il peut représenter des paquets TCP ou UDP, la rupture d'un lien entre nœuds et les paquets rejetés d'une file d'attente pleine. Les chercheurs appellent souvent NAM directement depuis les scripts TCL pour NS-2 pour visualiser directement les résultats de simulation. En résumé, NAM est un outil de visualisation qui permet aux utilisateurs de voir la topologie d'un réseau et les résultats de la simulation en temps réel.

c. Fichier awk

Paramètre : Le fichier doit être analysé avec le fichier de trace pour générer les résultats analysés. **Fonctionnement :** Le fichier peut prendre en charge la génération des indicateurs de performance (les métriques) suivants [43] :

- Débit
- Délai minimum
- Délai maximum
- Délai moyen
- Paquets de données transmis
- Les paquets de données reçues avec succès par leurs destinations respectives
- Le taux de livraison de paquets de données
- Énergie moyenne utilisée
- Pourcentage moyen de l'énergie consommée
- Statistiques des paquets perdus.

d. Les avantages et les inconvénients du simulateur NS2 :

Avantage :

Le simulateur NS-2 présente plusieurs avantages, notamment :

- Il est capable de simuler plusieurs couches de protocoles.
- Il est un outil complètement libre qui peut être utilisé sur plusieurs plateformes.
- Il permet aux utilisateurs d'ajouter des composants à la demande pour personnaliser les simulations.
- Il est développé en utilisant une approche orientée objet, offrant une grande flexibilité aux développeurs.
- De nombreux protocoles sont disponibles pour NS-2 grâce à sa popularité.

Inconvénients

Cependant, NS-2 présente également quelques inconvénients, notamment :

- La modélisation dans NS-2 est une tâche complexe car il n'y a pas d'interface graphique, ce qui peut rendre la création de scénarios de simulation difficile.
- L'utilisation de NS-2 nécessite un haut niveau de technicité et une connaissance approfondie des protocoles et des paramètres de simulation, ce qui peut être difficile pour les utilisateurs débutants.

III.3. Les critères d'évaluation

III.3.1. Taux de transfert des paquets

Taux de livraison des paquets Le taux de livraison des paquets représenté par PDR est le rapport entre le nombre de paquets reçus avec succès par la destination et le nombre de paquets transmis par la source. Cela nous permet de vérifier si les extensions du protocole ont un effet sur la réussite de la transmission des paquets.

$$PDR = \frac{\sum \text{nombre de paquets recus par la destination}}{\sum \text{nombre de paquets envoyes par tous les noeuds source}} \times 10 \quad (3.1)$$

III.3.2. .Temps bout en bout

Le retard d'un paquet est le temps qu'il faut pour atteindre la destination, et le retard moyen est calculé comme la moyenne du retard de chaque paquet transmis. Il est classé RAL pour la latence d'acquisition de route ou la latence de bout en bout.

$$EDD = \frac{1}{n} \sum (Tri - Tsi) \times 100[\text{ms}] \quad (3.2)$$

III.3.3. Pert des paquets (PL)

Le paramètre PL (perte de paquets) est la différence entre le nombre total de paquets envoyés et le nombre de paquets reçus.

$$PL = \text{nombre total des paquets envoyés} - \text{nombre total paquet reçus} \quad (3.3)$$

Des valeurs de perte de paquets plus faibles offrent les meilleures performances. Paramètres PL.

III.3.4. Surcharge

La surcharge du réseau (network overhead) correspond au trafic généré par les messages de contrôle et de routage, par rapport au trafic utile des données

$$\text{Surcharge} = (\text{Trafic de contrôle}) / (\text{Trafic total}) \quad (3.4)$$

Les valeurs NRL plus élevées offrent des performances supérieures, mais elles réduisent la consommation de bande passante.

III.3.5. Lancement de la simulation

Nous avons simulé les protocoles AODV, DSDV et DSR. On revient sur les métriques de performances pour évaluer ces derniers. Ensuite, le scénario que nous avons défini est mis en œuvre, suivi des paramètres d'évaluation.

Nous commençons notre simulation par les étapes suivantes :

- Nous choisissons les protocoles AODV, DSDV et DSR pour le script de simulation.
- Nous utilisons une plage de simulation de 1800×1000 .

- Nous configurons les paramètres du réseau, y compris le nombre de nœuds, le temps de simulation, la vitesse des nœuds, le débit moyen de données envoyées et la taille du paquet.

```

3
4 # Define options
5 set val(chan)      Channel/WirelessChannel    ;# channel type
6 set val(prop)      Propagation/TwoRayGround   ;# radio-propagation model
7 set val(netif)      Phy/WirelessPhy          ;# network interface type
8 set val(mac)        Mac/802_11               ;# MAC type
9 set val(ifq)        Queue/DropTail/PriQueue   ;# interface queue type
10 set val(ll)        LL                        ;# link layer type
11 set val(ant)        Antenna/OmniAntenna      ;# antenna model
12 set val(ifqlen)     50                      ;# max packet in ifq
13 set val(nn)         60                      ;# number of mobilenodes
14 set val(rp)         DSR                      ;# routing protocol
15 set val(x)          1800                    ;# X dimension of topography
16 set val(y)          1000                    ;# Y dimension of topography
17 set val(stop)       150                     ;# time of simulation end
18 if { $val(rp) == "DSR" } {

```

Figure III. 1. Paramètre de simulation.

Afin de l'interpréter d'une manière claire et facile et de tirer des conclusions, nous lançons le calcul et affichons le résultat, qui sera utilisé dans un autre simulateur pour illustrer comme des graphes et des tableaux.

III.4. . Résultats et discussion

Nous avons choisi de simuler trois protocoles de routage dans ce travail, deux protocoles proactifs (DSDV et DSR) et un protocole réactif (AODV). Les paramètres d'évaluation suivants ont été examinés : débit, latence, taux de livraison de paquets, perte de paquets et charge de routage normalisée.

En outre, nous avons aussi simulé le protocole réactif AODV sans et avec l'implémentation de l'attaque de trou noir (BlackHole) dans un réseau fixe, nous avons choisi les paramètres suivants : over Head, drop et le délai.

III.4.1. Scénario 1

Selon les métriques ou les indicateurs de performance que nous avons choisis, dans ce scénario, le nombre des nœuds connectés au réseau pour les trois protocoles

étudiés (AODV, DSDV et DSR) varie constamment entre 10,25 et 60. Les paramètres du réseau choisis pour ce scénario sont présentés dans *le tableau 3.1* ci-dessous.

Tableau III. 1.Paramètres de simulation du scénario 1

<i>Paramètres</i>	
<i>Nombre de nœuds</i>	<i>10, 25, 60</i>
<i>Temps de simulation (s)</i>	<i>150</i>
<i>Temps de pause</i>	<i>0</i>
<i>Mode Wifi</i>	<i>Ad hoc</i>
<i>Protocole mac</i>	<i>Mac/802_11</i>
<i>Protocole de routage</i>	<i>AODV, DSDV, DSR</i>
<i>La zone de simulation</i>	<i>1800×1000</i>
<i>Vitesse de nœud (m/s)</i>	<i>20</i>
<i>Taille de packets (bits)</i>	<i>1500</i>
<i>Nombre de source</i>	<i>01</i>
<i>Type de canal</i>	<i>Channel/Wireless Channel</i>

Le taux de transmission (PDR) est la première mesure à prendre en compte. Les résultats de la simulation sont présentés dans le tableau III.2. Ce dernier montre la variation du débit de transmission des paquets en fonction du nombre de nœuds pour les trois protocoles étudiés : AODV, DSDV, DSR.

Tableau III. 2.Variation de PDR vs ? le nombre des nœuds pour AODV, DSDV, DSR.

Nombre de nœuds Protocole		10	25	60
PDR (%)	AODV	99.13	99.13	99.15
	DSR	99.07	96.09	80,05

	DSDV	49.94	67.99	61.99
--	-------------	-------	-------	-------

Les résultats obtenus sont présentés sur la Figure III.2, qui représente le débit de transfert de paquets (PDR). Pour les trois protocoles étudiés, nous avons compté le nombre de paquets abandonnés selon les nœuds connectés.

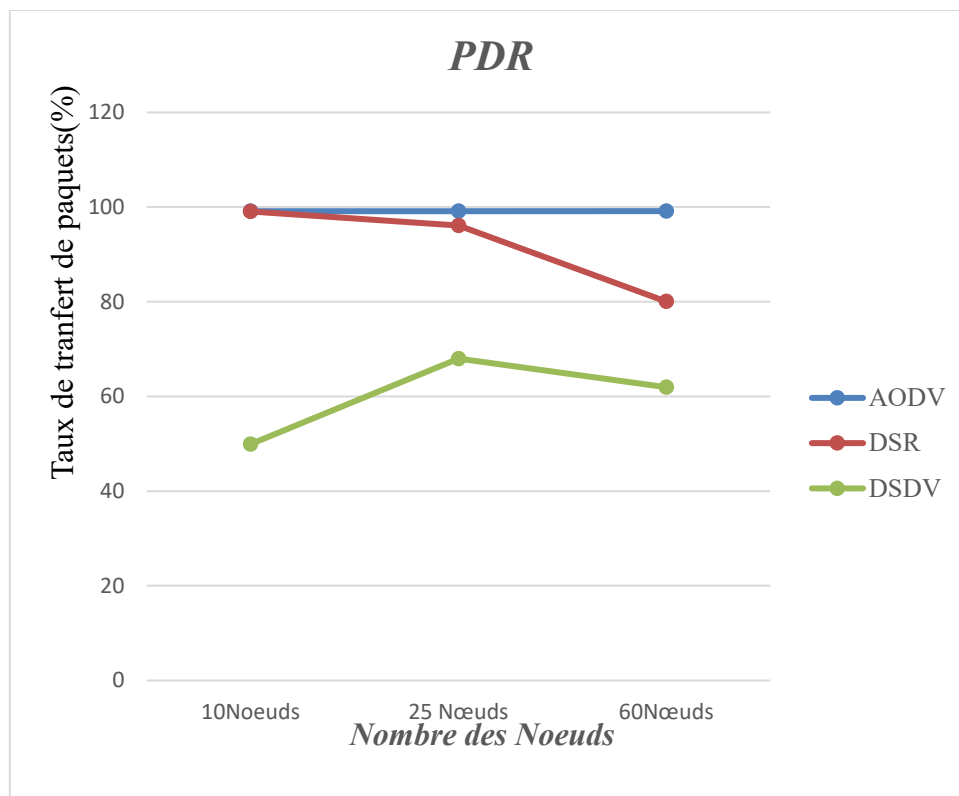


Figure III. 2.PDR en fonction de la variation des nombres des nœuds pour AODV, DSDV et DSR.

Dans la figure III.2, nous pouvons voir que les protocoles DSR et AODV ont présenté le plus haut taux de réussite de livraison de paquets (PDR). De plus, notre étude a révélé que ces deux protocoles offrent un débit de transmission de paquets plus élevé que le protocole DSDV.

Un autre critère que nous avons examiné est le délai de retard moyen, qui mesure le temps nécessaire pour transmettre les données de bout en bout. Les résultats de cette métrique sont présentés dans le tableau III.3, où nous avons comparé la variation du délai de retard moyen de bout en bout (EED) pour les trois protocoles de routage étudiés : AODV, DSDV et DSR.

Tableau III. 3. Délai de retard moyen en fonction du nombre de nœuds pour AODV, DSDV, DSR.

Nombre de nœuds Protocole		10	25	60
EDD (ms)	AODV	810	276	118.33
	DSDV	1040	352	213.33
	DSR	730	260	106.66

Les résultats obtenus sont illustrés dans la figure III.3. Cette figure représente le délai de retard moyen de bout en bout (EED), en variant le nombre de nœuds mobiles du réseau, puis nous avons tracé ce délai de retard moyen qui est mesuré en ms en fonction du nombre de nœuds pour les trois protocoles étudiés.

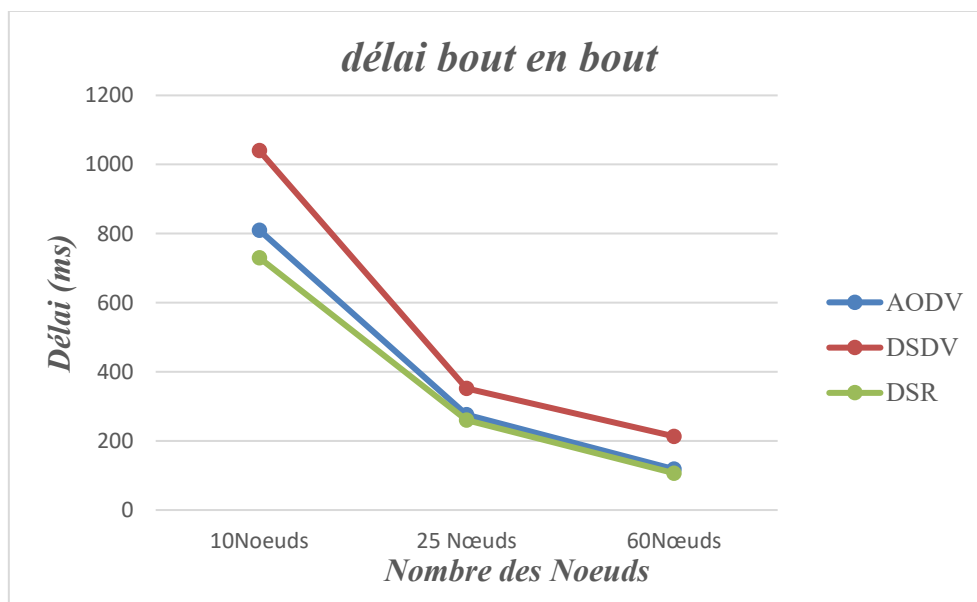


Figure III. 3. délai de retard moyen en fonction du nombre des nœuds.

Les simulations de deux protocoles de routage ont produit des résultats montrant que, comparativement au protocole DSDV, les protocoles AODV et DSR entraînent un retard plus important dans les trois topologies de réseau étudiées. Bien que les délais mesurés par les protocoles AODV et DSR augmentent avec le nombre de nœuds, l'EED calculé par le protocole DSDV reste stable. En fin de compte, le protocole DSDV est considéré comme le meilleur des trois protocoles étudiés, car il favorise le chemin le plus court et fournit les valeurs les plus optimales.

Le troisième critère étudié s'appelle la perte de paquets (PL). Toutes les valeurs obtenues de simulation pour les protocoles AODV, DSDV et DSR sont présentées dans le tableau III.4, illustre la variation de la perte de paquets en fonction du nombre de nœuds mobiles dans le réseau.

Tableau III. 4. Les pertes perdues de retard moyen en fonction du nombre de nœuds pour AODV, DSDV, DSR.

Nombre de nœuds Protocole		10	25	60
PL	AODV	34	34	113
	DSDV	21	21	21
	DSR	30	41	34

Nous avons calculé le nombre de paquets abandonnés dans *la figure III.4* en fonction des nœuds connectés pour les trois protocoles étudiés.

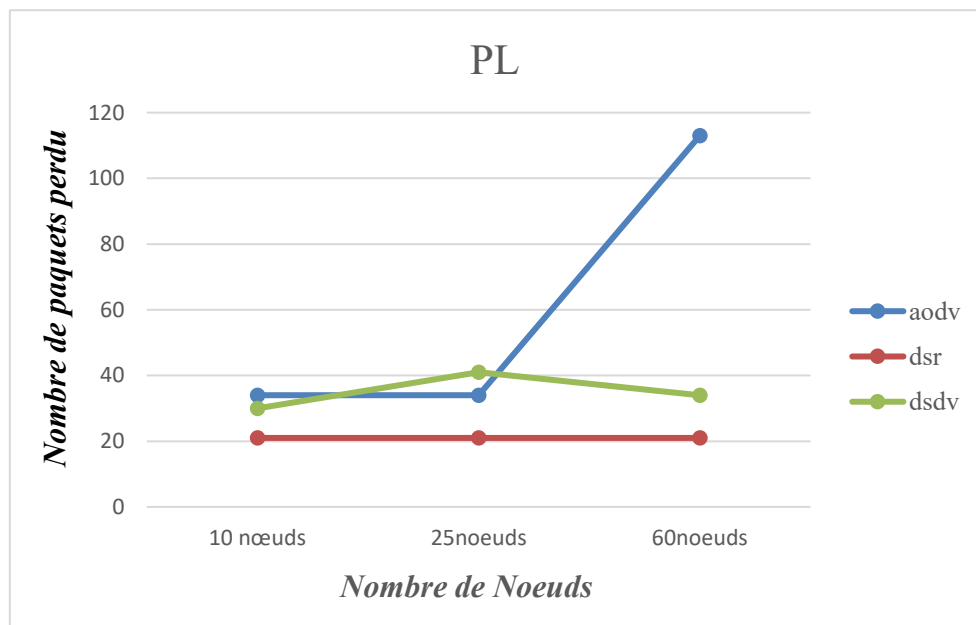


Figure III. 4. Les pertes perdues de retard moyen en fonction du nombre de nœuds pour AODV, DSDV, DSR.

La Figure III.4 montre que la valeur PL de DSR est inférieure à celle des deux autres protocoles AODV et DSDV, et que la perte est également inférieure à AODV. Par conséquent, DSR est plus efficace que les autres protocoles car il abandonne les paquets.

La dernière métrique étudiée est la surcharge de réseau, les résultats de simulation obtenus sont donnés dans le tableau suivant (*Tableau III.5*).

Tableau III. 5. Surcharge par rapport le nombre de nœuds pour AODV, DSDV, DSR.

Nombre de nœuds	10	25	60
-----------------	----	----	----

	Protocole			
Surcharge	AODV	233	886	4605
	DSDV	0	0	0
	DSR	0	0	0

La charge d'acheminement normalisée (NRL) est représentée sur la Figure III.

5. Pour les trois protocoles étudiés AODV, DSDV et DSR, nous traçons la variation de surcharge de réseau normalisée en fonction du numéro de nœud.

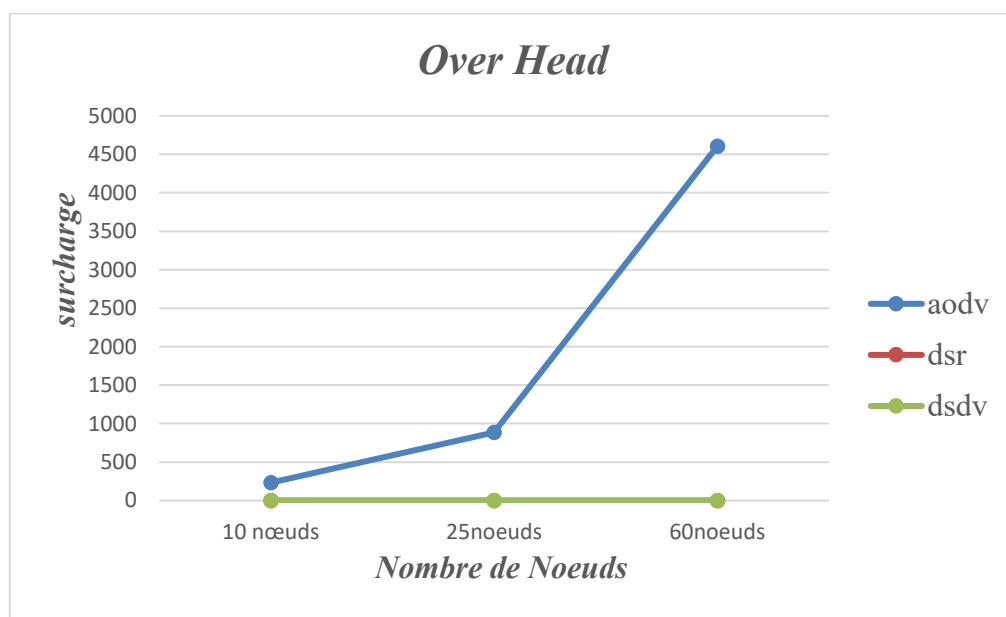


Figure III. 5. Surcharges par rapport le nombre de nœuds pour AODV, DSDV, DSR.

Comme le montre la Figure III.5, DSR et DSDV en tant que protocoles proactifs, génèrent moins d'over-Head et plus que la valeur de charge de routage donnée par le protocole AODV, malgré l'augmentation du nombre de nœuds, et ce sont ces valeurs qui produisent les meilleurs résultats. Ce protocole crée et maintient les routes à la demande tant que la source en a besoin.

III.4.2. Scénario 2

On a choisi de simuler le protocole AODV qui varie constamment entre 10,20 et 30 nœuds selon des métriques de performances suivant : le drop, over Head et le délai (Delay), sans et avec l'implémentation de l'attaque du blackhole.

Tableau III. 6.Paramètres de simulation du scénario 2

<i>Paramètres</i>	
<i>Nombre de nœuds</i>	<i>10,20,30</i>
<i>Temps de simulation (s)</i>	<i>180</i>
<i>Temps de pause</i>	<i>0</i>
<i>Mode réseau</i>	<i>Fix</i>
<i>Protocole mac</i>	<i>Mac/802_11</i>
<i>Protocole de routage</i>	<i>AODV</i>
<i>La zone de simulation</i>	<i>2000.06×1014.25</i>
<i>Attaque utilisé</i>	<i>2 blackhole</i>
<i>Type de canal</i>	<i>Channel/Wireless Channel</i>

Dans ce scénario, nous avons étudié les paramètres de performances qui sont déjà cité. Dans le tableau III.7, nous présentons ces paramètres en fonction de la variation de nombre des nœuds pour un protocole AODV.

Après l'illustration des résultats obtenus et avec l'aide de VMware on a implémenté l'attaque blackhole dans le protocole AODV (AODV+BLACKHOLE) dans la variation des nombres de nœuds, nous présentons aussi les métriques de performances, le tableau suivant (*tableau III.7*).

Le tableau ci-dessous résume tout le travail simulé :

Tableau III. 7.Variation des paramètres de performances en fonction du nombre des nœuds pour AODV sans et avec Blackhole

PDR		
	<i>AODV</i>	<i>AODV+BLACKHOLE</i>
<i>10 Nœuds</i>	<i>100</i>	<i>0.041</i>
<i>20 Nœuds</i>	<i>99.97</i>	<i>0.048</i>
<i>30 Nœuds</i>	<i>99.98</i>	<i>8.84</i>
DROP		
<i>10 Nœuds</i>	<i>0</i>	<i>2403</i>
<i>20 Nœuds</i>	<i>0</i>	<i>6143</i>
<i>30 Nœuds</i>	<i>1</i>	<i>6706</i>
DELAI		
<i>10 Nœuds</i>	<i>0.014</i>	<i>0</i>
<i>20 Nœuds</i>	<i>0.013</i>	<i>0.025</i>
<i>30 Nœuds</i>	<i>0.08</i>	<i>0.0091</i>
OVER HEAD		
<i>10 Nœuds</i>	<i>294</i>	<i>362</i>
<i>20 Nœuds</i>	<i>323</i>	<i>1966</i>
<i>30 Nœuds</i>	<i>886</i>	<i>6888</i>

Alors la première métrique qu'on a obtenue avant et après l'implémentation d'attaque Blackhole dans le protocole AODV. D'après *la Figure III.6*, nous pouvons voir les résultats obtenus.

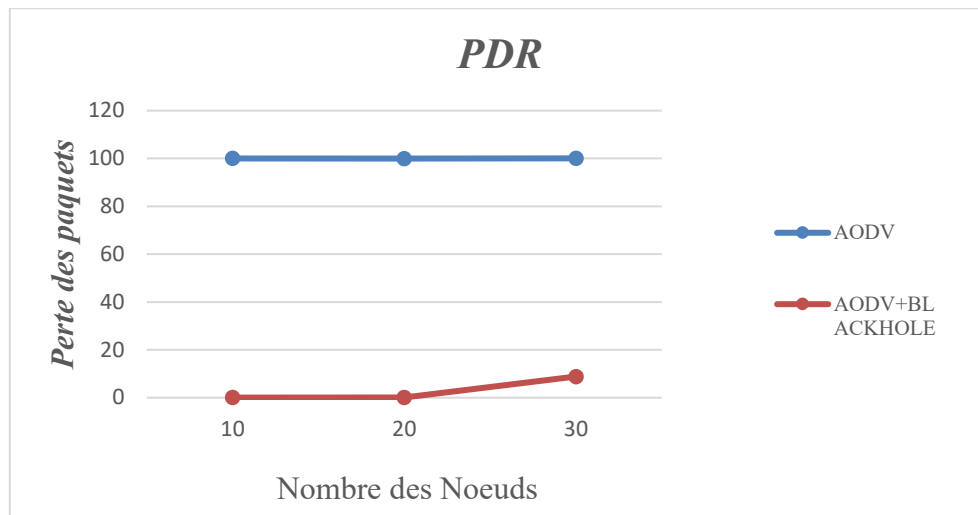


Figure III. 6. Variation de PDR en fonction du nombre des nœuds pour AODV sans et avec blackhole.

D'après *La Figure III.6*, nous constatons que le protocole étudié (AODV) présente un PDR plus élevé, donc nous remarquons que l'AODV seulement reste avec des valeurs accrues, mais après l'implémentation du BlackHoule, cette dernière va supprimer les paquets envoyés vers le nœud destinataire cela indique les valeurs qui sont décroissantes du PDR d'un AODV+BlackHole.

La deuxième métrique étudiée est le drop, les résultats obtenus sont illustrés dans la figure suivante (Figure III.7). Cette figure représente le drop, en variant le nombre de nœuds du réseau, nous avons tracé ce drop dans les deux cas étudiés en fonction de nombre de nœuds.

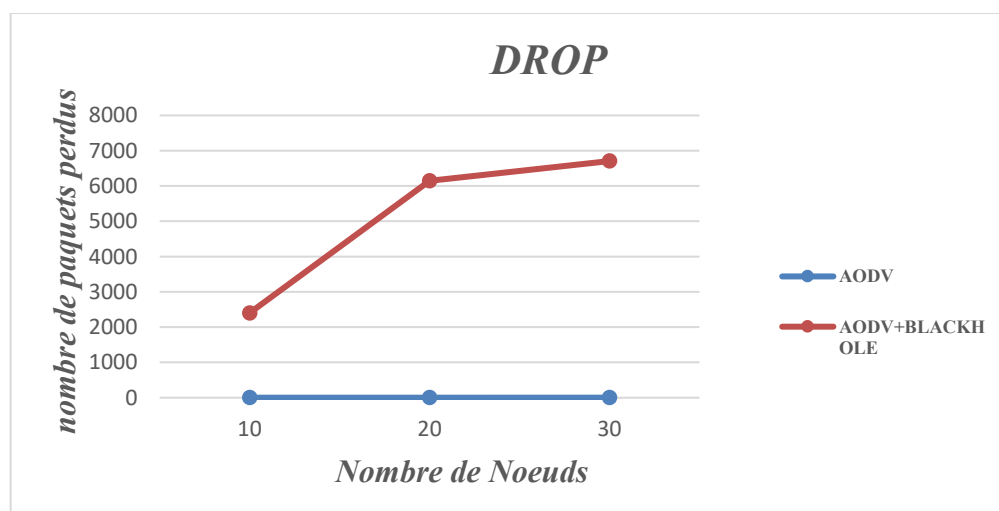


Figure III. 7. Variation de paquets perdus en fonction du nombre des nœuds pour AODV sans et avec blackhole.

D'après la Figure III.7, nous apercevons que la valeur de paquet perdu par le protocole AODV est presque nulle jusqu'à ce que la valeur devienne 1 dans l'utilisation des 30 nœuds, et ce sont ces valeurs qui présentent les meilleurs résultats. Au contraire, nous remarquons un drop élevé dans l'implémentation du BlackHoule qui indique des problèmes de performance dans le réseau.

La troisième métrique étudiée est le délai (Delay). Les résultats obtenus sont illustrés dans la figure suivante (**Figure III.8**). Cette figure représente le délai de retard moyen, d'AODV et AODV+BlackHole en variant le nombre de nœuds du réseau, nous avons tracé ce délai de retard moyen qui est mesuré en ms en fonction de nombre de nœuds.

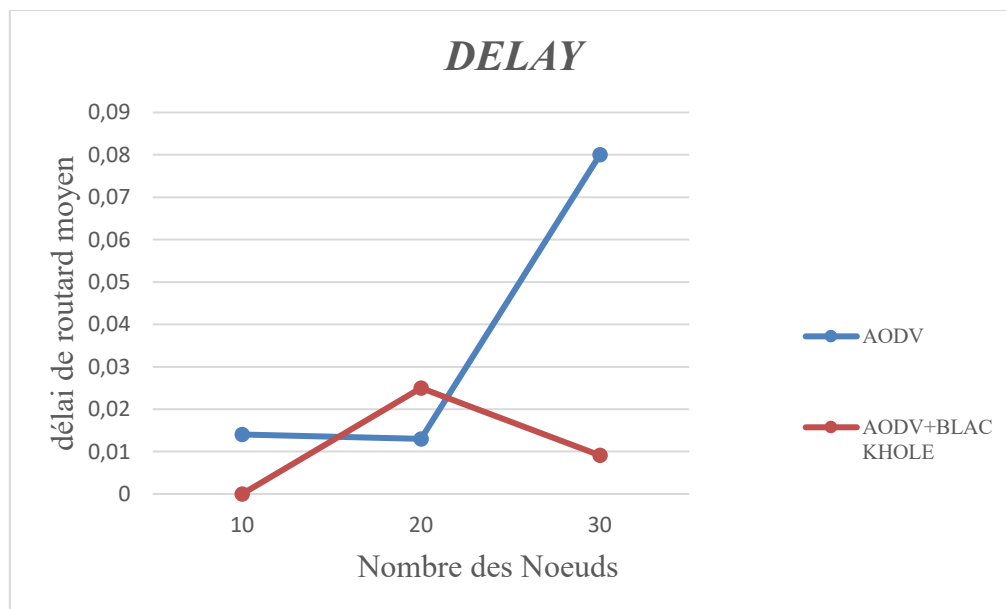


Figure III. 8.Délai en fonction du nombre des nœuds pour AODV sans et avec blackhole.

D'après la **Figure III.8**, nous remarquons que le délai de retard, représenté dans le cas d'un AODV +BlackHole reste court alors que la procédure de découverte de route doit également être répétée pour chaque paquet perdu contrairement que l'AODV.

La dernière métrique étudiée est Over Head, nous avons tracé les résultats obtenus de couts en fonction de nombre de nœuds. La **Figure III.9** ci-dessous montre et illustre le travail simulé.

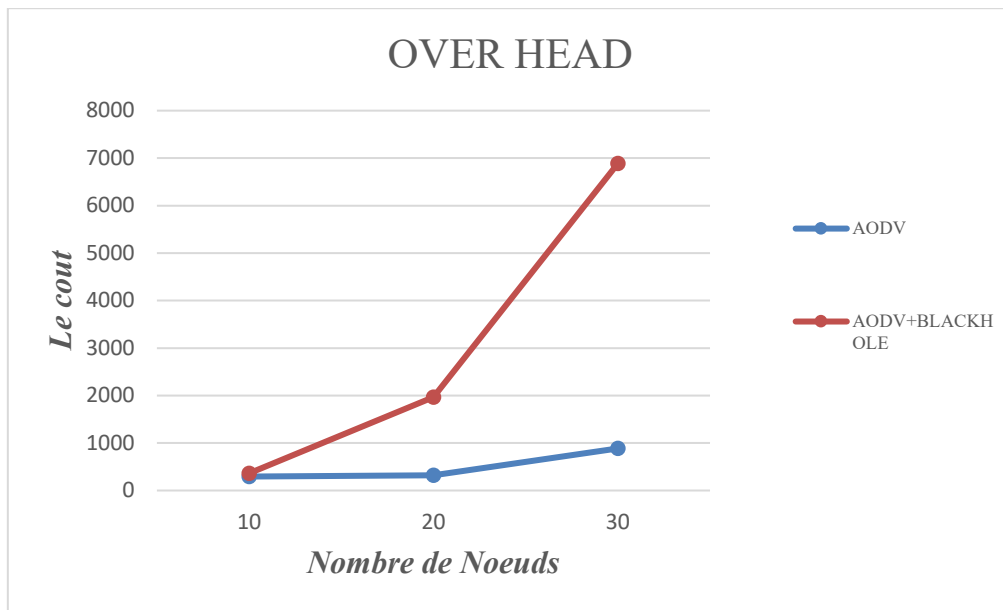


Figure III. 9. Le cout en fonction du nombre des nœuds pour AODV sans et avec blackhole.

D'après la figure III.9, nous constatons que le cas qui présente un Over Head le plus élevé est l'AODV+BlackHole, il est généré significativement par chaque nœud. Ce dernier donne une instabilité globale de routage introduite par l'attaque qui augmente le trafic de contrôle.

III.5. Conclusion

Dans ce chapitre, nous avons élaboré deux différents scénarios, l'un pour comparer les performances des différents protocoles qui sont AODV, DSDV et le DSR, et l'autre est l'attaque Blackhole qui trouble le fonctionnement des protocoles de routage réactif plus précisément le protocole de routage AODV. Nous avons réalisé des simulations pour étudier l'impact de cette attaque.

Conclusion

Générale

Les réseaux ad hoc semblent promis à un bel avenir dans les prochaines années car ils permettent l'information existe de manière distribuée. Cependant, les problèmes de sécurité dans réseaux ad hoc ont une influence déterminante sur leur avenir, les données transmises peuvent être sensible et souvent facile à intercepter ou à manipuler.

Deux aspects sont d'une importance primordiale : la sécurité des données transmises, en particulier sécurité du routage éphémère vulnérable aux attaques multiples

Ce projet vise à rechercher et à mettre en œuvre les protocoles de routage AODV, DSDV et DSR pour les réseaux locaux sans fil à haut débit. Nous comparons les performances de ces protocoles en termes de latence de bout en bout, de débit, de surcharge et de perte de paquets. Le protocole AODV s'est avéré être le plus performant en raison de sa capacité à s'adapter rapidement aux changements de topologie du réseau.

Nous avons également mis en place une attaque de type "trou noir"(BlackHole) sur le protocole AODV pour analyser son impact sur les performances du protocole. Cette attaque entraîne une dégradation significative des performances en termes de débit et de perte de paquets. En raison du manque de mécanismes de sécurité, AODV s'est montré vulnérable à de telles attaques.

A terme, il sera intéressant de mettre en place des mécanismes de sécurité tels que les signatures numériques ou le cryptage pour augmenter la robustesse de l'AODV face aux attaques. Nous pouvons également étendre ces recherches à d'autres protocoles de routage éphémère et à d'autres types d'attaques.

Nous avons basé dans ce projet sur la simulation des protocoles AODV, DSDV et DSR avec le simulateur NS-2, et le VMware pour l'implémentation de l'attaque BlackHole sur le protocole AODV.

En bref, ce projet permet de mieux comprendre le fonctionnement des protocoles de routage dans les réseaux ad hoc et leur vulnérabilité aux attaques, et ouvre des perspectives intéressantes pour améliorer leur sécurité.

Bibliographie

- [1] Keith Shaw, Network World (adaptation Jean Elyan) "Les 7 couches du modèle OSI", le 26/10/2020.
- [2] Nicolas SERY, "modèle OSI et TCP/IP ", Linux - notebook, Novembre 10, 2014
- [3] La Rédaction JDN, "WLAN (Wireless Local Area Network) : définition" et Dictionnaire de l'IoT Bluetooth, Zigbee : définition et fonctionnement", le 02 novembre 2020 .
- [4] Les réseaux informatiques, Site Web créé avec WordPress.com.
- [5] Mohamed Bouaouiouach. "Quels sont les types de réseaux .Internet et leurs définitions" article scientifique, le 20 mai 2021.
- [6] Glossary, HIPERLAN, "HighPERformance Radio Local Area Network".
- [7] WIMAX, "broadband wireless technology", Tutorials Point, 2018.
- [8] Christopher Quente, "Brand Driven Mobile Marketing: 5 Theses for Today and Tomorrow", Christopher Quente, Handbook of Research on Mobile Marketing Management, en 2010, Pages: 16.
- [9] MATTHEW LYNCH, article " What is a Wireless Wide Area Network (WWAN)?", publié le 19 Mars, 2023.
- [10] Abdtar44, " Réseau Sans Fil". Un quiz, le 22 mars, 2022.
- [11] K. MOHAMED. "Etude planification et dimensionnement d'un réseau d'accès WIFI". Mémoire fin d'étude, 2004/2005.
- [12] Yodhan Gowda, "10 Advantages and Disadvantages of Wifi & Wireless Networks".
- [13] WIFI AND SECURITY, "Remplacer le disque dur d'un PC, Transmission par onde WIFI", Le 01 novembre 2006.
- [14] Federal Agencies. "Information Security: Steps to Secure Wireless Networks", le 3 Avril, 2017.
- [15] Alan Freedman and Irma Morrison. "Definition, mobile ad hoc network", "The Computer Language Company Inc , article, 2002.
- [16] Eric Sandler, Article "802.11b Physical Layer Revealed", 29 September, 2021.
- [17] ISSAD Lamia, "Chapitre 7 Exploration 1-Couche liaison de données", pages 1-37.
- [18]. JAONA ANDRIAMPARANY HERIALALAINA et RAFENOHERY LOVA NORENA, "Mise En Place D'un Réseau Sans Fils Sécurisé Dans Une Entreprise", 2005.
- [19] CISCO CCNA3 COURSE , "Fonctionnement LAN sans fil Structure de trame 802.11".

- [20] Xerandy, Wireless Networks," IEEE 802.11 Wireless LAN Standard : MAC",Le 15 Février 2018.
- [21] BOUAZIZ, SIHEM et ZIANI, RAZIKA, Mémoire de fin d'étude"securise une reseaux eifien implementant le protocol d'authentification 802.1x sure le server RADIUS".
- [22] Jordan ASSOULINE, « CISCO – Sécurité Préparation à la certification CCNA 210-260 »,2021
- [23] Comment sécuriser les systèmes d’authentification, de gestion de sessions et de contrôle d’accès de vos applications web ?,Le 5 Octobre 2021, vaadata.com/blog/fr.
- [24] C. Duret N.Gaillar. « Les attaques internet et les moyens de s’en protéger ». 2002.
- [25] Guy Pujolle, « Les Réseaux », Edition Eyrolles, 75240 Paris Cedex 05, France, 2008, pp 867-932.
- [26] Anthony Freda.Article « WEP, WPA ou WPA2 — Quel est le meilleur protocole de sécurité Wi-Fi ? ». Le 14 Février 2022 .
- [27] Net Spot Essential for WiFi security. « Protocoles de sécurité du réseau sans fil: WEP,WPa, WPA2, et WPA3 ».
- [28] Elie MABO, « La sécurité des systèmes informatiques (Théorie) », support de cours, 2010.
- [29] GÉRON, Aurélien. « WiFi Professionnel-3e édition- : La norme 802.11, le déploiement, la sécurité ». Dunod, 2009.
- [30] ZIDANI, Ferroudja. Thèse de doctorat. « Solution d’authentification et de gestion de clés pour le standard 802.11 i des réseaux WiFi ». 2018.
- [31] Jess Logane, « Computer Technology and the Law (LEI 238), Widener University,2019/2020.
- [32] Cedrick KADIMA KALALA, « Mise en place sur le point d'accès d'un réseau wifi » Institut supérieur d'informatique programmation et d'analyse (ISIPA) RDC - Graduat 2010.
- [33] Nadia ADRAR, « Les technologies sans fil Le Wi-Fi et la Sécurité », Université Abderrahmane Mira - Licence Académique en Informatique LMD 2009.
- [34]Xavier Lasserre,Thomas Klein et SebF. « Réseau Privé VirtuelVpn ».
- [37] THINHINANE, Ammariet DJAMILA, Attab. Thèse de doctorat « Etude et application des outils de sécurité d’un réseau Wi-Fi ». 2015. Université Mouloud Mammeri.
- [38] SERET, Dominique, MEHAOUA, Ahmed, et DORTA, Neilze. « Réseaux et télécommunications » . support de cours, Université René Descartes–Paris, 2006.

- [39] NICOPOLITIDIS, Petros, OBAIDAT, Mohammed S., PAPADIMITRIOU, Georgios I., et al. Wireless networks. John Wiley& Sons, 2003.
- [40] <https://web.maths.unsw.edu.au/~lafaye/CCM/wifi/wifi-wpa2.html>
- [41] J.BISIMWA Ngabo « Exploitation des failles de sécurité et étude des méthodes de protection du réseau wifi de micro finance. Cas de la COOPEC Nyawera » Université Biosadec - Licence 2015.
- [42] WIFI Alliance,« discover-wi-fi security » consulté le 26 mai 2022, www.wi-fi.org
- [43] Tahar Chaouch Amel- Benmoumene Abdellah Mahfoudh. « Analyse par simulation des performances d'un réseau de capteurs sans fil (WSN) ». Master En Télécommunications- Université Djilali Bounaama Khemis Miliana- 2015/2016.