République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Abderrahmane Mira de Béjaia
Faculté des Sciences Exactes
Département d'Informatique

Mémoire Présenté

Pour l'obtention du Diplôme de Master

En Informatique

Option : Résaux et sécurité

Par : BENAMRAOUI Mohammed

La securité dans un environnement IPv6

Soutenu à l'Université Abderrahmane Mira de Béjaia,
Le 14/09/2023, devant le jury composé de :

D^{r}. ALOUI soraya	Président	à l'UAMB - Bejaia.
D^{r}. YESSAD samira	Examinateur	à l'UAMB - Bejaia
D^{r}.Moktefi Mohand	Encadrant	à l'UAMB - Bejaia.

Année Universitaire 2022 – 2023

Table des matières

Table des figures

Liste des tableaux

Notations

AH : authentification header

ARP : Address Resolution Protocol

BLE : Bluetooth Low Energy

DHCP : Dynamic Host Configuration Pool

DHCPv6 : Dynamic Host Configuration Protocol version 6

DIS : Information Solicitation

DAO : Destination Advertisement Object

Dos : denie of service

DDOS : Distributed Denial-of-Service

DNS : Domain Name Server

DODAGs : Destination Oriented Directed Acyclic Graphs

DTLS : Datagram Transport Layer Security

GUA : Global Unicast Address

IETF : Internet Engineering Task Force

ICMP : Internet Control Message Protocol

ICMPv6 : Internet Control Message Protocol version 6

ID : Identifiant

IEEE : Institute of Electrical and Electronics Engineers

IoT : internet of object

IP : Internet Protocol

ISP : Fournisseur d'Internet

LAN : Local Area Network

LLA : Link-Local Address

MAC : Media Access Control

MLD : Multicast Listener Discovery

MTD : "Moving Target Defense"

MTU : Maximum Transmission Unit

MITM : man in the midle

NA : Neighbor Advertisement

NDP : Neighbor Discovery Protocol

OSPF : Open Shortest Path First

OF : Fonction Objectif

PoS : Proof-of-Stake

P2P : Poste à Poste

RA : Router Advertisement

RFM : Request for Comments

RPL : Routing Protocol for Low-Power and Lossy Networks

RS : Router Solicitation

SASL : (Simple Authentication and Security Layer)

SEND : Secure Neighbor Discovery

SLAAC : StateLess Address Auto Configuration

SSL : Secure Socket Layer

TCP/IP : Transmission Control Protocol / Internet Protocol

TLS : Transport Layer Security

TLV : Type,Lenghth,Value

URL : Uniform Resource Locator

UDP : User Datagram Protocol

VPN : Virtual Private Network

Remerciment et Dédicace

Remerciment

Je remercie ALLAH qui ma donné la santé et la force pour réaliser ce memoire ainsi que mon promoteur Mr Moktefi Mohand d'avoir accepté de m'encadrer, et de me suivre durant toute l'année en assurant le suivi scientifique et technique du présent mémoire. Je le remercie pour sa grande contribution à l'aboutissement de ce travail. sincère reconnaissance et de mon profond respect. mes remerciements vont aussi aux membres du jury pour l'honneur qu'ils m'ont faits en acceptant de juger ce modeste travail. Pour conclure, je remercier ma chères familles et tous ceux qui ont participé de près ou de loin à l'élaboration de ce travail.

Dédicace

je dédie ce mémoire À mes parents qui m'ont soutenu et encouragé durant ces années d'études. Qu'elle trouve ici le témoignage de ma profonde reconnaissance. À mes frères,et sœurs. A rekia, mouad, et ghiles à ma famille et ceux qui ont partagé avec moi tous les moments lors de la réalisation de ce travail. Ils m'ont chaleureusement supporté et encouragé tout au long de mon parcours.

Introduction générale

L'IPv4 manque d'adresses. C'est pourquoi les administrateurs réseau devraient se familiariser avec IPv6. Le protocole IPv6 est venu pour être le successeur de l'IPv4. L'IPv6 possède un espace d'adressage énorme de 128 bits .

Avec le nombre toujours croissant d'appareils mobiles, les fournisseurs de téléphonie mobile ont été à l'avant-garde de la transition vers l'IPv6. Les deux principaux fournisseurs de téléphonie mobile aux États-Unis indiquent que plus de 90(pour cent) de leur trafic passe par IPv6. La pluPartie des principaux FAI (fournisseur d'accès internet) et fournisseurs de contenu tels que YouTube, Facebook ont également fait la transition. De nombreuses entreprises comme Microsoft, Facebook et LinkedIn sont entrain de passer à l'IPv6 uniquement en interne.

Par rapport aux dernières décennies, l'Internet d'aujourd'hui est un peu différent. Avant, Internet est principalement utilisé pour la messagerie électronique, la navigation sur le web et le transfert de fichiers entre ordinateurs. Internet est en passe de devenir un Internet des objets. Les appareils pouvant accéder à Internet ne sont plus seulement des ordinateurs, des tablettes et des smartphones.Demain, les appareils connectés et équipés de capteurs concerneront tous les objets du quotidien, notamment les automobiles, les équipements biomédicaux, l'électroménager, et même les écosystèmes naturels donc l'utlisation de ipv6 est primordiale

Donc Le monde est entraîn de connaître une révolution dans la façon nous communiquons, travaillons, et interagissons avec le monde qui nous entoure. Pour cela on voit que la sécurité des réseaux et des données est devenue une préoccupation cruciale. la technologie (IPv6) est une norme fondamentale qui joue un rôle central dans l'expansion et la continuité de cette révolution numérique.

Pour permettre une connectivité universelle et répondre a la croissance exponentielle des dispositifs connectés à l'Internet ;la transition vers IPv6 s'est imposée.

Cette transition vers IPv6 n'est pas sans susciter des préoccupations en matière de sécurité. Alors que les réseaux du monde entier migrent progressivement vers IPv6, il est impératif de comprendre les défis et les opportunités que cette nouvelle génération de

protocole Internet présente en matière de sécurité

L'objectif de ce mémoire est d'explorer les profondeurs de sécurité associés à l'adoption généralisée d'IPv6. Pour atteindre cet objectif, nous avons organisé le mémoire en 3 chapitres dont le contenu est brièvement décrit dans les points suivants :

Le premier chapitre de ce mémoire se concentre sur les avantages de cette nouvelle version et comment les adresses IPv6 sont représentées, et Comparer ces types .et vas voir comment faire la configuration d'adresse IPv6 monodiffusion (unicast) globale et les adresses réseau IPv6 link-local statiquement et dynamiquement .

Le deuxième chapitre explique les vulnérabilités et les menaces de IPv6 et examine en detail quelques protocoles utilises dans un environnement IPv6, tels que ICMPv6 et la decouverte de voisinage. on vas analyser les failles potentielles de cette technologies, et identifier quelque attaque comme Attaques par d eni de service (DoS) ,Attaque Multicast Listener Discover,Attaques de voisinage .Une compréhension approfondie de ces risques est essentielle pour élaborer des stratégies de sécurité efficaces.

Le troisième chapitre se concentre sur la sécurité dans l'Internet des objets (IoT),qui est un domaine se repose en grande partie sur IPv6 pour permettre la connectivité de milliards d'appareils intelligents,on vas voire les technologie de communication tel que RFID ;lora et les protocole de routage comme Le protocole RPL (Routing Protocol for Low-Power and Lossy Networks) qui joue un r^ole crucial au sein de ces reseaux et les défis de sécurité unique dans ces technologies.

1

Étudier les caractéristiques de l'IPv6

1.1 Introduction

L'invention de IPv6 est venue pour améliorer l'extension de l'espace d'adressage, l'optimisation des tables de routage, et répondre aux besoins croissants de connectivité de notre monde numérique en constante expansion. Il est doté de 128 bits au lieu de 32 bits de IPv4.

Dans ce contexte, ce chapitre vise à fournir une compréhension approfondie des caractéristiques de IPv6 et à vous familiariser avec l'architecture d'adressage étendu mise en œuvre. Il vous expliquera également les différents types d'adresses utilisables dans ce protocole et pourquoi il est conçu de cette manière.

1.2 Définition de IPv6 (Internet Protocol)

IPv6 est une norme de protocole réseau qui définit la dernière version du protocole Internet (IP) qui est largement utilisé pour le routage des données sur Internet. IPv6 a été développé pour résoudre certains des problèmes liés à la version précédente, IPv4 (Internet Protocol version 4), notamment l'épuisement des adresses IPv4.

1.3 Aperçu sur les caractéristiques de IPv6

— Espace d'adressage étendu qui sera suffisant pour plusieur années a venir.
— Un mécanisme pour l'auto-configuration des réseaux d'interface.
— Capacité pour l'encapsulation des données.
— Compatibilité pour coexister et communiquer avec IPv4.

Dans IPv6, on utilise le terme "paquet" au lieu de "datagramme" dans IPv4 et le terme "nœud" [42].

1.4 Syntaxe des adresses IPv6

Le protocole IPv6 est spécifié dans RFC 4291. Les adresses IPv6 ont une structure significativement différente d'IPv4 ; en IPv4, chaque adresse (segment) se composait de 32 bits, tandis qu'une adresse IPv6 comporte 128 bits. Pour assurer la bonne utilisation de telles adresses, celles-ci sont divisées en huit blocs (hextets) de 16 bits ou quatres valeurs hexadécimales séparées par deux points (:) comme illustré dans la Figure 1.1.[32]

Exemple : 2031 :0000 :130F :0000 :0000 :09C0 :876A :130B. Nous verrons dans la partie suivante quelques techniques d'optimisation pour réduire le nombre de chiffres d'IPv6.

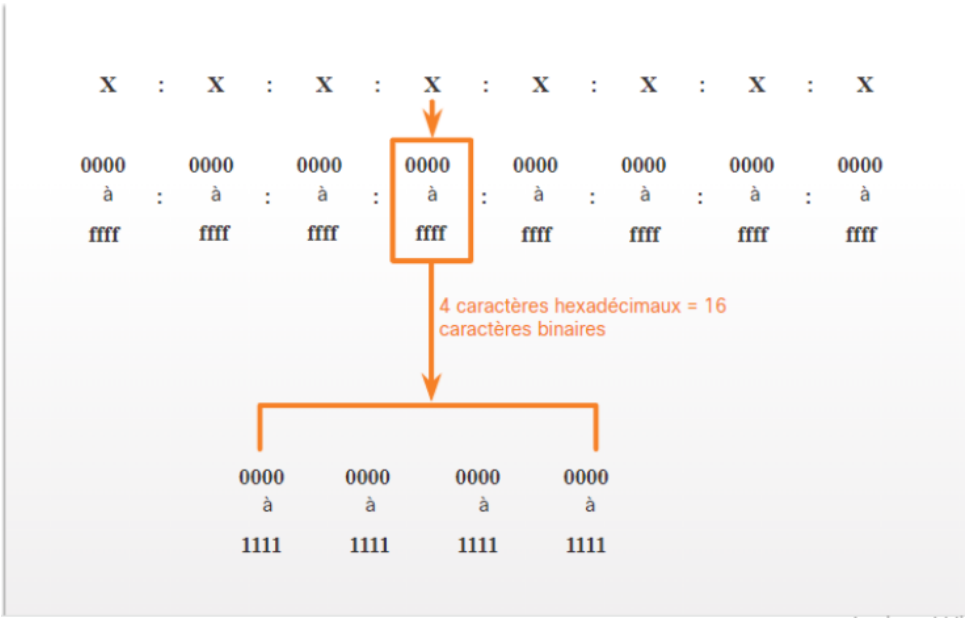

FIGURE 1.1 – Segments ou hextets de 16 bits

1.5 Élimination des zéros d'en-tête

Les zéros figurant dans l'en-tête de chaque bloc peuvent être éliminés. Par exemple, l'adresse "2031 :0000 :130F :0000 :0000 :09C0 :876A :130B" peut être simplifiée en "2031 :0 :130F :0 :0 :9C0 :876A :130B" [32].

1.6 Utilisation d'un double deux-points (: :)

Si l'adresse IPv6 contient des zeros de manière consécutivs,on peut utiliser un double (: :) pour abréger la notation de ces adresses .comme l'exemple précédent on peut éliminer les zéros de 5eme bloc et le 6eme et les remplacer par (: :) on obtient par conséquence : :2031 :0 :130F : :9C0 :876 :130B Avec ce cas les logiciels et les matériels devant rajouter autant de zéros pour obtenir 128bits

Cette technique d'abréviation ne doit jamais être utilisé plus d'une fois dans un segment .[32].

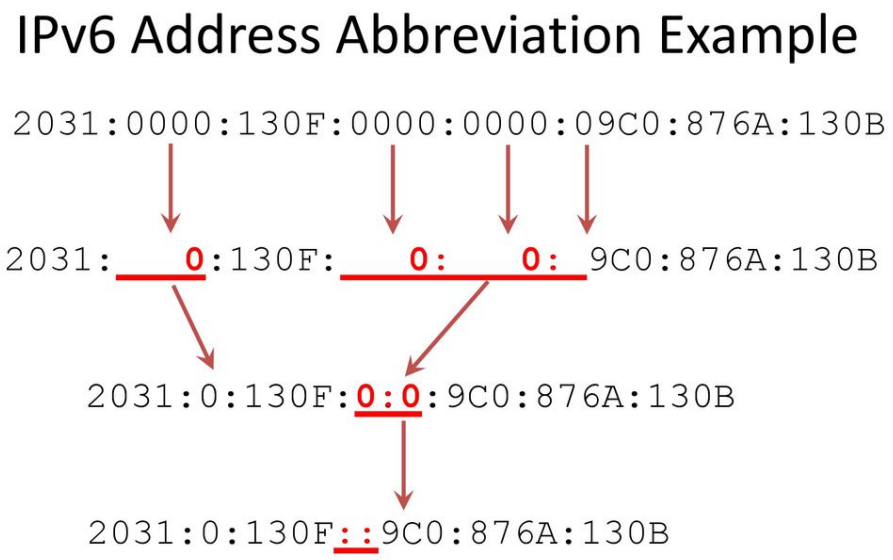

FIGURE 1.2 – Exemple d'abréviation d'une adresse IPv6

1.7 Format d'en-têtes IPv6

Voici la structure d'en-tête d'un paquet IPv6 comme illustré dans la Figure 1.3 :

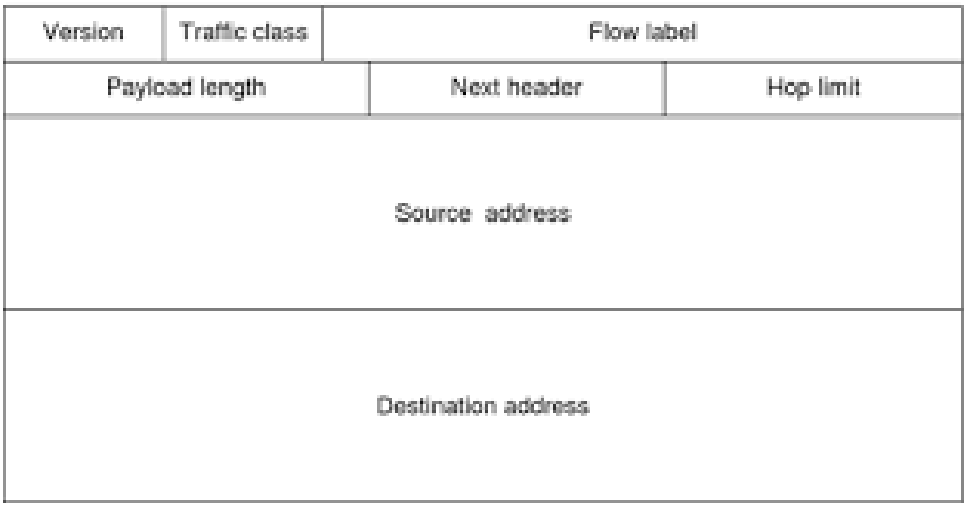

FIGURE 1.3 – Format d'en-tête IPv6 [8]

Examinons maintenant les différents champs :[42]

— Version (4 bits) : Indique la version du protocole, généralement 6 pour IPv6.
— Trafic classe : Utilisé pour la qualité de service (QoS) et la priorisation du trafic.
— Flow label (20 bits) : Utilisé pour l'étiquetage de flux, améliorant ainsi la qualité de service et la gestion du trafic.
— Payload length (16 bits) : Indique la longueur totale du paquet, y compris l'en-tête et les données.
— Next header (8 bits) : Indique le type de l'en-tête suivant (ex. : en-tête TCP, en-tête UDP, etc.).
— Hop limit (8 bits) : Remplace le champ Time to Live (TTL) d'IPv4, indiquant le nombre maximal de sauts (routeurs) que le paquet peut effectuer avant d'être abandonné.
— Adresses source et destination :Les adresses IPv6 de l'émetteur (source) et du destinataire (destination) sont incluses dans chaque paquet IPv6. Ces adresses sont utilisées pour acheminer et livrer le paquet correctement.

1.7.1 En-têtes d'extension (Extension headers)

L'en-tête d'extension (Extension header) est généralement utilisé pour fournir des fonctionnalités supplémentaires ou des informations de contrôle. Plusieurs en-têtes d'extension peuvent être ajoutés dans n'importe quel ordre [42].

1.7.2 L'en-tête « Hop-by-Hop »

L'en-tête « Hop-by-Hop » est un type d'en-tête qui fait partie de la structure modulaire des paquets IPv6 et peut être inséré entre l'en-tête principal IPv6 et d'autres en-têtes d'extension. Son rôle est de fournir des options qui nécessitent une action à chaque routeur traversé par le paquet. Ces options sont traitées par chaque routeur sur le chemin de transmission et ne sont pas ignorées comme indiqué dans la figure 1.4 [42].

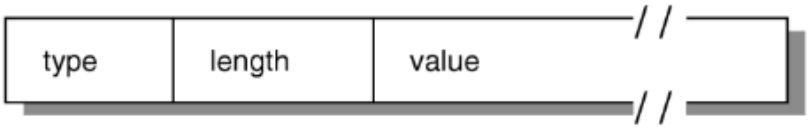

FIGURE 1.4 – Format d'IPv6 (TLV)
[42]

— Type(8bits) :Indique l'en-tête qui suit directement l'en-tête « Hop-by-Hop Options » (ex. : en-tête TCP, en-tête UDP, etc.).
— Length(8bits) :Indique la longueur totale de l'en-tête en unités de 8 octets, y compris les champs de l'en-tête lui-même.
— Value :Ce champ contient les options spécifiques qui nécessitent une action à chaque routeur.
— Traitement :Chaque routeur sur le chemin de transmission examine les options dans l'en-tête « Hop-by-Hop Options » et prend les mesures nécessaires en conséquence. Les options sont traitées dans l'ordre dans lequel elles apparaissent.

Options :

— Les options insérées dans l'en-tête « Hop-by-Hop Options » peuvent inclure diverses informations de contrôle :

Pad1 option :Utilisée pour aligner les options sur des limites d'octets. padN option :Utilisée pour insérer un certain nombre d'octets de bourrage.

1.7.3 Authentification Header (AH)

Defintion :L'en-tête d'authentification (Authentification Header ou AH) est un type d'en-tête d'authentification particulièrement utile dans les scénarios où l'intégrité des données est cruciale en transit.

Son but principal est de garantir que les paquets ne sont ni altérés ni falsifiés pendant leur acheminement sur le réseau. Chaque paquet doit être authentifié et validé en utilisant des mécanismes de signature numérique et des protocoles de hachage tels que MD5 et

SHA1. Le principe est de placer l'en-tête AH entre l'en-tête IPv6 d'origine et le reste du paquet [32].

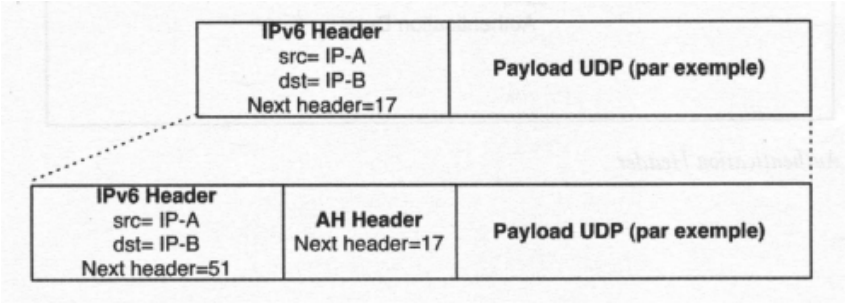

FIGURE 1.5 – AH en mode transport [32]

Format de l'en-tête AH : L'en-tête AH suit le format suivant [42] :

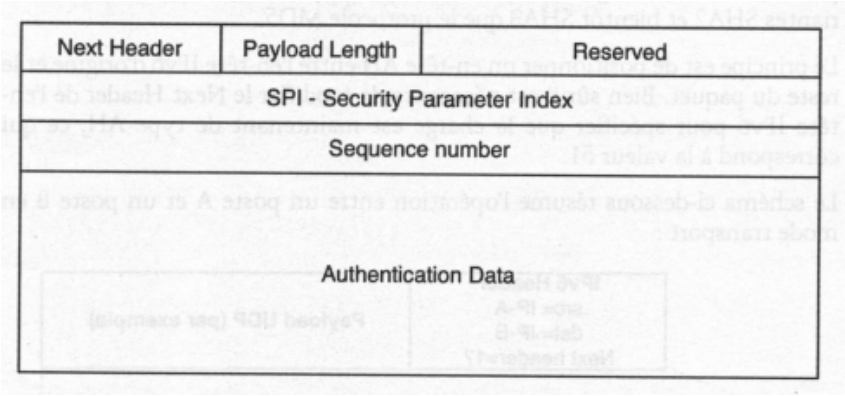

FIGURE 1.6 – Format de l'en-tête AH [32]

— Next header (8 bits) : Indique le type d'en-tête qui suit directement l'en-tête AH (ex. : en-tête TCP, en-tête UDP, etc.).
— Payload length (8 bits) : Indique la longueur totale de la charge utile, y compris l'en-tête AH et les données.
— RESERVED5 (16 bits) : Réservé à des fins futures, doit être mis à zéro.
— Security parameter index (SPI) : Identifie le contexte de sécurité pour la connexion, utilisé pour la correspondance avec les paramètres de sécurité sur le destinataire.
— Sequence number (32 bits) : Numéro de séquence pour prévenir les attaques de rejeu.
— Data : Champ contenant le code d'authentification (ICV) qui garantit l'intégrité des données.

1.7.4 Encapsulating Security Payload (ESP)

Defintion : L'Encapsulating Security Payload (ESP) est une extension header spéciale qui fournit à la fois la confidentialité (chiffrement), l'intégrité et la confidentialité des données en transit.

Il est principalement utilisé dans le contexte des protocoles de sécurité IPsec (IP Security) car toutes les données qui suivent ESP sont cryptées [32]. L'ESP offre un mécanisme de sécurité pour garantir que les données sont protégées contre l'écoute, la modification et la falsification.

Son principe de fonctionnement consiste à insérer un en-tête original IPv6 et le reste du paquet d'origine.

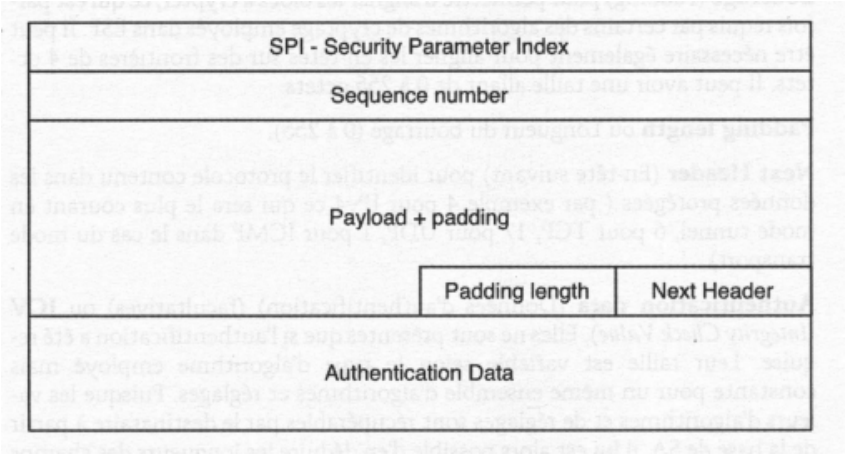

FIGURE 1.7 – Format de l'en-tête ESP [32]

L'ESP est ajouté en tant qu'en-tête d'extension après l'en-tête IPv6 de base. Son format général est illustré dans la Figure 1.7[32] :

- Security parameter index (SPI) : Identifie le contexte de sécurité pour la connexion, utilisé pour la correspondance avec les paramètres de sécurité sur le destinataire.
- Payload data : Champs contenant les données chiffrées et éventuellement les codes d'authentification.
- Sequence number : Numéro de séquence pour prévenir les attaques de rejeu.
- Padding : Padding qui permet d'aligner les blocs à crypter ou les en-têtes sur des frontières de 4 octets. Sa taille est de 0 à 255 octets.
- Padding length : Longueur de bourrage (0 à 255).
- Next header : Header suivant.
- Authentication data (données d'authentification) : ICV (intégrité check value) présentes uniquement si l'authentification est requise.

1.8 Types d'adresses IPv6

1.8.1 Longueur de préfixe IPv6

pour distinguer la partie adresse d'un réseau IPv6,il ont trouver une technique qui permet de préciser ce réseau,et celle qui correspond a l'interface ;c'est le rôle de la longueur préfixé.La longueur préfixe a un seul rôle qui est de préciser combien de bit représentant le préfixe Donc préfixe en IPv6 s'exprime avec la syntaxe suivant [32] :

-Adresse ipv6/longueur de préfixe.

Cette notation appelé CIDR (Classless Inter-Domain Routing), qui consiste en une adresse IPv6 suivie d'un slash (/) et du nombre de bits du préfixe. Par exemple, l'adresse IPv6 "2001 :0db8 :85a3 :0000 :0000 :8a2e :0370 :7334" avec un préfixe de 64 bits serait écrite comme "2001 :0db8 :85a3 : :/64". Le préfixe de 64 bits indique que les 64 premiers bits de l'adresse sont utilisés pour identifier le réseau, tandis que les 64 derniers bits sont utilisés pour identifier l'hôte sur le réseau.

Les préfixes permettant de détermine le type de adresse ; le tableau ci dessus nous montre çà [32] :

Type d'adresse	**Préfixe binaire**	**Notation IPv6**
Non spécifique	000000...00 (128 bits)	: :/128
Loopback	000...1 (128 bits)	: :1/128
Multicast	1111 1111	FF00 : :/8
Unicast local de liaison	1111 1110 10	FE80 : :/10
Unicast local unique	1111 1100 et 1111 1101	FC00 : :/7
Unicast global	Tous les autres	

TABLE 1.1 – Préfixes d'adresse IPv6

Il existe trois grandes catégories d'adresses IPv6 :

1.8.2 Adresse unicast et ces sous types :

Ce type d'adresse identifie une seule interface réseau et est utilisé pour une communication point à point. En d'autres termes, lorsqu'un périphérique souhaite envoyer des données à un autre périphérique spécifique sur le réseau, il utilisera une adresse unicast pour cibler l'interface réseau de ce périphérique çà veut dire que tout paquet ayant pour destination . cette adresses est délivré uniquement a l'interface détentrice de cette adresse ;l'identifient d'interface est la plupart de temps sur 64bits .elle est couramment dérivé de l'adresses MAC d'interface [32] .

n bits	128-n bits
Prefixe des sous-réseaux	Interface ID

La figure montre les différents sous types d'adresses de mono diffusion (unicast) IPv6 :

À l'intérieur des adresses unicast, il existe différents sous-types, comme illustré dans la Figure 1.8 ci dessous.

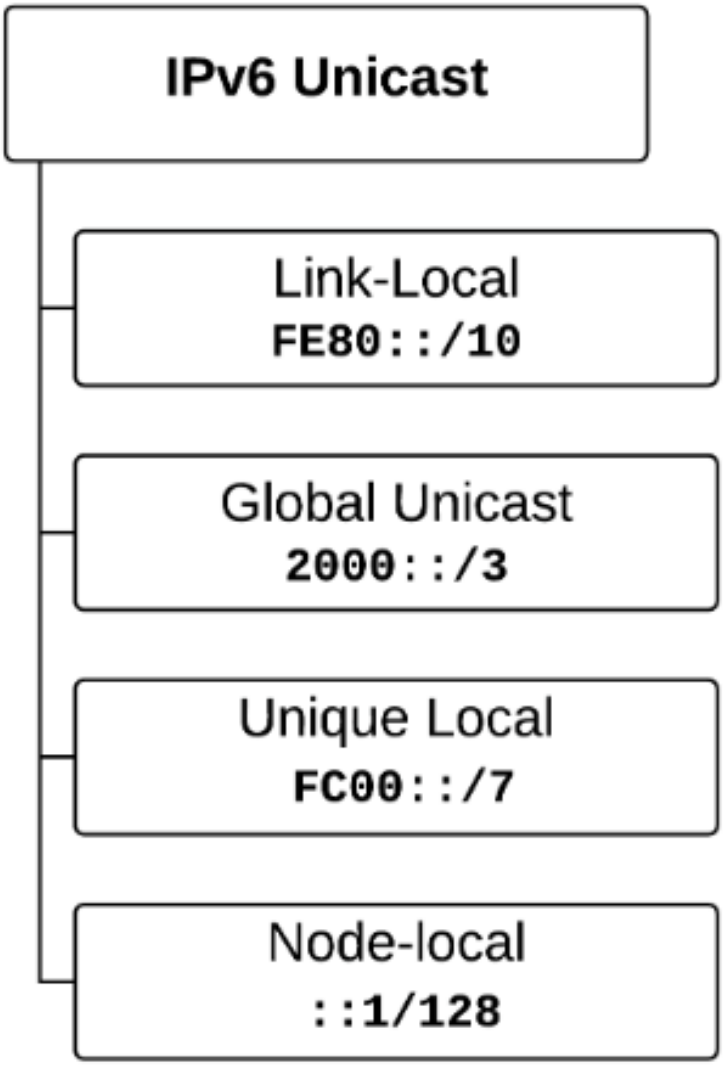

FIGURE 1.8 – Sous-types d'adresses unicast [3]

Note : L'ICANN (Internet Committee for Assigned Names and Numbers), opérateur de l'IANA, attribue des blocs d'adresses IPv6 aux cinq organismes d'enregistrement Internet locaux. Actuellement, seules des adresses de mono diffusion (UNICAST) globale dont les premiers bits sont 001 ou 2000 : :/3 sont attribuées.

Adresse unicast globale (GUA)

Ces adresses sont uniques au monde et routables sur Internet. Configurées de manière statique ou attribuées dynamiquement. Le préfixe de routage globale est la valeur permettant de destiner(router) les paquets depuis internet vers le site

— Plage d'adresse unicast globale : 2000 : :/3

— Remarque : Le préfixe 2001 :0DB8 : :/32 est réservé à des fins de documentation et n'est pas routable sur Internet.

Adresse de liaison locale (LLA)

Defintion :ce type d'adresses ne sont pas routable en dehors du lieu local veut dire que ces adresses n'ont qu'une signification local. les adresses de ce type commence systématiquement par :FE80 : :/10. Ces sont souvent les seul adresses générer par une interface par le mécanisme auto-configuration.

Unicast local unique (ULU)

Defintion :se sont des adresses routable dans un réseau prive mais pas sur internet mais ils sont conçu par une algorithme de tel sorte que des réseau identique ne seront pas exister sur deux sites différent .

Le préfixé réservé pour ce type d'adresses est fc00 : :/7.

LA structure de ce type d'adresses est définît dans RFC 4193 ;veut dire pour générer ces adresses il faut utiliser l'algorithme $\text{pseudo}_a léatoire$.

Les adresses locales uniques (plage de FC00 : :/7 à FDFF : :/7) ne sont pas encore couramment implémentées. Elles peuvent éventuellement être utilisées pour adresser des périphériques connectés à Internet, mais elles n'ont pas encore été largement adoptées.

1.8.3 Adresse GUA (Global Unicast Address) IPv6

Defintion : :Une adresse GUA (Global Unicast Address) est un type d'adresse IPv6 utilisée dans les réseaux IPv6. Les adresses GUA sont destinées à identifier de manière unique des dispositifs, des hôtes ou des nœuds dans un réseau IPv6 global, c'est-à-dire sur Internet

On pourrait identifier plusieurs adresses Global unicast sur les interfaces, soit l'équivalent de nos adresses IPv4 publiques. On les définira plus précisément comme des destinations publiées sur l'Internet. Les routeurs transfèrent le trafic vers ces destinations. Elles sont donc "globalement routables."

Structure du Global Unicast Adresse

Le format des adresses IPv6 Global Unicast est défini dans les RFC 3587 et RFC 3177 et voici la structure[32] :

Bits	Global routing prefix (45 bits)	Subnet ID (16 bits)	Interface ID (64 bits)
001 (3 bits)	Global routine préfixe	Subnet ID	Interface ID

TABLE 1.2 – Structure du Global Unicast Adresse

— Le "global routing prefix" est la partie de l'adresse assignée à un site (c'est-à-dire un ensemble de sous-réseaux et de liens). Ces numéros sont attribués par les RIRs et les ISPs. Il a une longueur par défaut de 48 bits.
— Le "subnet ID" est l'identifiant du sous-réseau dans le site. Il est géré par les administrateurs du site. Il a une longueur de 16 bits portant le masque de sous-réseau à 64 bits. ID de sous réseau est utilisé par une entreprise pour identifier les sous-réseaux au sein de son site. Plus l'ID de sous-réseau est un nombre important, plus il y a de sous-réseaux disponibles.
— L'"Interface ID" identifie l'interface dans le sous-réseau. C'est élément de 64 bits qui est configuré de différentes manières.

Note : De nombreuses organisations reçoivent un préfixe de routage global /32. L'utilisation du préfixe/64 est recommandée pour créer un ID d'interface 64 bits. Cela signifie qu'une organisation avec un préfixe de routage global /32 et un ID de sous-réseau 32 bits aura 4,3 milliards de sous-réseaux.

1.8.4 Les GUA et l'adressage Dynamique de l'IPv6

L'adressage Dynamique d'adresse IPv6 est l'un des concepts clés de la conception d'IPv6 visant à simplifier la configuration des adresses pour les hôtes connectés au réseau. Contrairement à IPv4 où l'attribution des adresses IP nécessite souvent l'utilisation de protocoles de configuration tels que DHCP, IPv6 intègre un mécanisme d'auto-configuration qui permet aux hôtes de configurer automatiquement leurs adresses IPv6 et d'autres paramètres réseau essentiels.

Les messages RS et RA : une hôte obtient son GUA dynamiquement via les messages publicité de routeur (RA) et de sollicitation de routeur (RS) comme illustré dans la Figure 1.9 [13] :

— RA (Router Advertisement) : ce message est envoyé par un routeur IPv6 en réponse de la demande RS envoyée précédemment ; dans le but d'annoncer sa présence dans le réseau. Quand la hôte (interface) reçoit le message RS, elle extrait les

informations de configuration comme l'IPv6 du routeur, les préfixes réseau et les options d'auto-configuration.

— RS (Router Sollicitation) : c'est un message envoyé par une hôte ou un périphérique pour indiquer sa présence dans le lien. Quand un nœud a besoin de faire mise à jour à sa configuration réseau pour se connecter dans le réseau IPv6, il envoie ce type de message au routeur pour lui dire qu'il a besoin de certaines informations nécessaires pour configurer son adresse IPv6 et les autres paramètres réseau. Le message RS est envoyé pour demander les informations de configuration, et RA est envoyé par un routeur pour indiquer sa présence dans le réseau et fournir les informations de configuration.

Donc, l'adressage se fait dynamiquement via des messages ICMPv6 (Internet Control Message Protocol version 6). Les routeurs IPv6 envoient des messages d'annonce de routeur ICMPv6 toutes les 200 secondes à tous les périphériques IPv6 du réseau. Un message d'annonce de routeur est également envoyé en réponse à un hôte qui envoie un message de sollicitation de routeur ICMPv6, qui est une demande de message RA. Les deux messages sont affichés sur la figure.

FIGURE 1.9 – Messages RS et RA ICMPv6

Les méthodes pour les messages RA/RS :

Méthode 1 : SLAAC (Stateless Address Autoconfiguration)

Defintion :

La méthode SLAAC (Stateless Address Autoconfiguration) est utilisée dans IPv6 pour permettre aux nœuds de configurer automatiquement leurs adresses IPv6 sans avoir besoin d'un serveur DHCP (Dynamic Host Configuration Protocol). Avec SLAAC, les adresses IPv6 sont configurées de manière dynamique en utilisant les informations disponibles sur le réseau.

Voici comment fonctionne SLAAC :

1. Préfixe réseau global : Un routeur annonce périodiquement le préfixe réseau global dans les messages RA (Router Advertisement).
2. ID d'interface : en utilisant l'adresse MAC, chaque nœud dérive un identifiant d'interface.
3. Construction de l'adresse IPv6 : la hôte combine le préfixe et l'identifiant pour former l'adresse IPv6 finale.

   Donc en utilisant SLAAC, les nœuds peuvent configurer automatiquement leurs adresses IPv6 sans avoir à compter sur un serveur DHCP centralisé. Cela facilite la mise en place et la gestion des réseaux IPv6, tout en offrant une configuration d'adresse efficace et une connectivité réseau comme illustré dans la Figure 1.10.

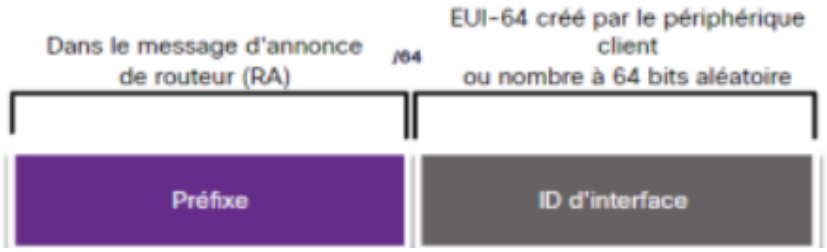

FIGURE 1.10 – SLAAC

Méthode 2 : Protocole DHCPv6

Defintion : Le protocole DHCPv6, spécifié dans RFC3315, fournit un mécanisme pour l'allocation d'adresse IPv6 et les informations de configuration aux nœuds IPv6. "Options de préfixe IPv6 pour DHCPv6" (RFC3633) spécifie un mécanisme pour la délégation automatique des préfixes IPv6 et des options qui s'y rapportent. Tout comme DHCPv4 (RFC2131), les serveurs DHCPv6 détiennent les informations d'autorité relatives à leurs opérations, incluant, mais sans s'y limiter, les informations prêtes pour les adresses IPv6 et les préfixes délégué [15]

L'auto-configuration d'adresse IPv6 est un domaine important à explorer pour comprendre comment IPv6 simplifie la configuration réseau et facilite le déploiement de nouveaux périphériques sur un réseau.

DHCPv6 Stateless Mode

Dans ce mode, DHCPv6 fournit des informations supplémentaires aux hôtes, telles que les paramètres de DNS, de serveur de temps, etc., et laisse la génération d'adresse à la méthode SLAAC.

DHCPv6 Stateful Mode

Ce mode vise à attribuer des adresses IPv6 spécifiques aux hôtes et à gérer de manière centralisée la configuration réseau.

Avantages de l'auto-configuration d'adresse IPv6

— Simplicité : Réduit les erreurs humaines et simplifie la gestion, car les hôtes utilisent l'adressage dynamique.
— Réactivité : Les hôtes peuvent configurer rapidement de nouvelles adresses en cas de changement de réseau ou de panne d'un routeur.
— Extensibilité : Fonctionne efficacement dans des environnements réseau de grande taille sans nécessiter de serveurs de configuration centralisés.
— Sécurité : L'utilisation de l'adresse MAC dans le processus de génération d'adresse aide à assurer l'unicité des adresses.

Stateless Auto Configuration

Ici, il n'y a plus de serveur DHCP, c'est le routeur qui fournit les informations nécessaires telles que le préfixe et la longueur du préfixe, mais aucune option supplémentaire n'est proposée.

1.8.5 IPv6 LLA (Link-Local Address)

Génération des adresses link local

Un périphérique peut obtenir un LLA de deux façons} :

— Statique : le périphérique a été configuré manuellement.
— Dynamique : en utilisant des valeurs générées aléatoirement ou en utilisant la méthode Extended Unique Identifier (EUI), la hôte génère son propre ID d'interface, qui utilise l'adresse MAC du client.

LLA dynamique

À partir d'un préfixe FE80 : :/10 et de l'id d'interface et en exécutant la méthode EUI-64, on obtient une adresse link-local d'une manière dynamique.

1.8.6 IPv6 Unique Local Unicast

Les Adresses locales uniques sont des adresses unicast pouvant être routées uniquement au sein d'un LAN : elles ont la même fonction que les adresses IP privées de l'IPv4. La plage de ces adresses est : FC00 : :/7.

Structure des adresses locale unique

champ	préfixe	L	ID globale	Subnet	Interface
bits	7	1	40	16	64

FIGURE 1.11 – Structure local unicast

1.8.7 Adresses multicast IPv6

Ce type d'adresse identifie un groupe d'interfaces et est utilisé pour une communication de un-à-plusieurs. Les périphériques peuvent s'abonner à un groupe multicast et recevoir les données envoyées à ce groupe. Chaque paquet envoyé à des adresses de ce type est traité par l'ensemble des interfaces (hôtes) appartenant à ce groupe de diffusion.

Structure d'adresse multicast

La structure d'adresse multicast est la suivante :[5]

8 bits	4 bits	4 bits	112 bits
1111 1111	Drapeaux	Porté (scope)	Group ID

Les premiers 8 bits identifient l'adresse comme étant une adresse de type multidiffusion. On identifiera le champ scope qui indique la portée du groupe :

— 1 - Interface-Local scope.
— 2 - Link-Local scope.
— 3 - Admin-Local scope.
— 4 - Site-Local scope.
— 5 - Organization-Local scope.
— 6 - Global scope.

Des contraintes particulières s'appliquent aux adresses multicast telles que :

— L'adresse multicast ne peut jamais être utilisée comme adresse source.
— Les routeurs ne doivent pas propager leur adresse multicast au-delà de leur portée.

Parmi les adresses multicast prédéfinies, on peut citer :

— FF01 : :2 pour tous les routeurs de l'interface.
— FF05 : :2 pour tous les routeurs de site (all nodes).
— FF02 : :2 pour tous les routeurs de lien.

Type d'adresse multicast

Il existe deux types d'adresses de IPv6 multicast :

— Multicast Assigné : Existe en deux types :

1. Multicast de tous les nœuds - FF02 : :1. La multidiffusion qui a remplacé la diffusion en IPv6, tous les équipements (routeurs, commutateurs, ordinateurs personnels, ordinateurs portables) compatibles IPv6 qui répondent à ce type de multidiffusion.
2. Multicast de tous les routeurs - FF02 : :2. Multicast qu'ils utilisent pour communiquer entre routeurs IPv6, c'est-à-dire ceux qui ont été configurés avec la commande `ipv6 unicast-routing`.

— Multicast de nœud demandé : Fonctionnellement similaire à la multidiffusion de tous les nœuds, il était principalement utilisé avec le protocole NDP (Neighbor Discovery Protocol) acheminé par ICMPv6 pour remplacer le protocole ARP dans IPv6. Ils sont créés en combinant le préfixe FF02 :0 :0 :0 :0 :FF00 : :/104 et les 24 bits moins significatifs de l'adresse unicast globale.

1.8.8 Adresses anycast

Cette adresse IPv6 identifie un groupe de plusieurs interfaces réseau, mais les paquets envoyés à cette adresse sont routés vers l'interface la plus proche du groupe, déterminée par les protocoles de routage. Cela permet de fournir des services redondants, où plusieurs hôtes peuvent offrir le même service, mais seul l'un d'entre eux est choisi pour répondre à une demande. L'avantage est que les paquets sont routés vers l'hôte le plus proche, ce qui réduit le temps de transit et améliore les performances globales du réseau.

1.9 Adresses spécifiques

— **Loopback (adresse de bouclage)** : 0 :0 :0 :0 :0 :0 :0 :0 :1 ou :1/128. Elle est utilisée par une interface pour s'envoyer des paquets. C'est un peu l'équivalent de 127.0.0.1 en IPv4.

— **Adresse non spécifiée (unspecified address)** : cette adresse en 0 :0 :0 :0 :0 :0 :0 :0 ou : :/128 indique tout simplement l'absence d'adresse IPv6 sur une interface. Elle ne doit jamais être utilisée sur une interface ou comme adresse de destination. Par contre elle peut être utilisée comme adresse source, par exemple lors d'une requête DHCP [32].

1.10 La méthode EUI64

Defintion : :L'IEEE a défini l'identifiant unique étendu (EUI), ou format EUI-64 modifié. EUI-64 signifie « identifiant unique étendu ». C'est une façon de former les

adresses IPv6 de type unicast,

cette technique se base sur l'adresse MAC de la carte réseau. Ce processus utilise l'adresse MAC Ethernet à 48 bits d'un client et insère 16 autres bits au milieu de cette adresse MAC pour créer un ID d'interface de 64 bits. Ce mécanisme permet à un hôte de s'attribuer à lui-même une adresse IPv6 et se fait en trois étapes comme illustré dans la Figure 1.12.

— **Étape 1** : on prend le préfixe de l'adresse IPv6 et l'adresse MAC de la carte réseau. On les combine en ajoutant FFFE au milieu de l'adresse MAC.

— **Étape 2** : on effectue une modification sur le septième bit du troisième octet sur lequel on va lui faire une inversion pour modifier sa valeur en décimale. Ce qui fait passer le septième bit du troisième octet de « 0 » à « 1 ».

— **Étape 3** : on écrit l'adresse IPv6 finale en enlevant les « 0 » inutiles.

Un ID d'interface EUI-64 comprend trois parties essentielles :

— Identifiant unique d'entité (OUI) : il est codé sur 24 bits provenant de l'adresse MAC du client.

— La valeur de 16 bits FFFE intégrée (au format hexadécimal).

— ID de périphérique de 24 bits de l'adresse MAC du client.

Le processus EUI-64 est présenté à la figure ci-dessus [2].

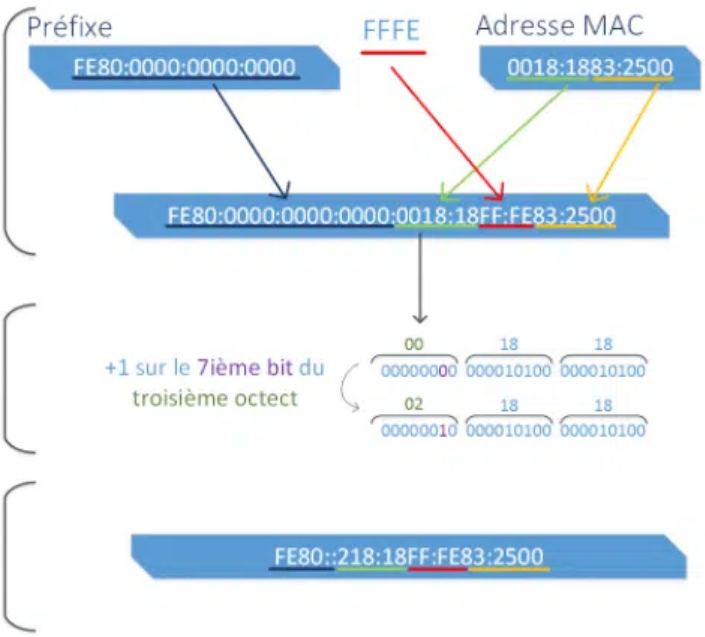

FIGURE 1.12 – Le processus EUI-64. [1]

La machine pendant la période de l'auto-configuration ne reçoit que les 64 premiers bits de l'adresse IPv6 et il lui reste d'obtenir les 64 derniers bits pour constituer une adresse complète. Pour atteindre ce but, il existe deux techniques : soit la génération de

l'adresse selon le format EUI-64, basée sur l'adresse MAC de l'interface Ethernet utilisée, soit la génération « aléatoire » des 64 derniers bits de l'adresse. Pour éviter que les adresses se multiplient à cause de la génération aléatoire, le périphérique procédera à une vérification.

1.11 DNS dans IPv6

Avec l'utilisation de 128 bits pour les adresses IPv6, il est devenu impossible d'identifier un nœud dans un autre réseau. Pour cela, le rôle du DNS est fondamental dans ce cas. Voici un aperçu des points clés liés aux DNS dans le contexte d'IPv6 [42].

- **Enregistrement AAAA** : les enregistrements AAAA sont utilisés pour associer un nom de domaine à une adresse IPv6 spécifique qui sont stockés dans les serveurs DNS. Ils offrent la possibilité aux navigateurs de trouver les adresses IPv6 correspondantes aux noms de domaine plutôt qu'en mémorisant des adresses numériques complexes.
- **Configuration des serveurs DNS** : Les fournisseurs d'internet (ISP) et les administrateurs réseau doivent configurer leurs serveurs DNS pour prendre en charge les enregistrements AAAA.

1.12 Conclusion

- Les adresses IPv6 ont une longueur de 128 bits et sont notées sous forme de chaînes de valeurs hexadécimales.
- Un périphérique obtient une (GUA,LLA) dynamiquement via des messages ICMPv6 RA (Router Advertisement) et RS (Router Solicitation), ou statiquement.
- IPv6 a été conçu en pensant au sous-réseau. Le champ ID de sous-réseau est la zone située entre le préfixe de routage global et l'ID d'interface.
- La méthode EUI-64 forme des adresses IPv6 de type unicast.

2

Vulnérabilités et attaques dans l'environnement IPv6

2.1 Introduction

Depuis l'adoption de la nouvelle technologie du protocole internet(IP) ipv6,celle qui a bien rapporter de révolutionnaire fonctionnalités et une meilleure extensibilité ,mais tous ça vas pas venir bien évidement sans nouvelles vulnérabilités et menaces potentielles on va traiter dans ce chapitre les menaces principales et les attaques potentielles et vulnérabilités existante dans un environnement ipv6.

2.2 Les protocoles de IPv6

2.2.1 ICMPv6

definition :ICMP veut dire internet contrôle message protocole. Son rôle est donc bien de véhiculer non pas des données utilisateur mais des information permettant de gérer la communication entre les défirent composants d'une réseau (poste,routeurs,imprimant,switche..) [32].

Les messages ICMPv6 sont essentiels pour le bon fonctionnement du protocole IPv6

et sont utilisés pour diverses fonctions de contrôle et de gestion du réseau.

Types de messages ICMPv6

Messages d'écho (Écho Messages) : connu sous le nom de «ping»,sont utiliser pour tester la connectivité entre 2 nœuds ipv6. Messages de redirigement (Redirect Messages) :ce types de message icmpv6 sont utiliser pour déclarer a une hôte qu'il doit utiliser un autre routeur pour satisfaire sont objectif d'atteindre un destination spécifique. Messages de routage (Routing Messages) :sont des message qui ont un rôle bien spécifique de mettre à jour les tables de routage et de maintenir une connectivité optimale au sein du réseau.

Format général de icmpv6

Son format général est le suivant [32] :

Type : sur un octet

Code : sur un octet

Checksum (somme de contrôle) : sur deux octet

Message body(corps du message) : de taille variable selon le message

La taille d'un packet icmpv6 ne doit jamais dépasser la taille minimale du MTU(maximum transmision unite)

2.2.2 Le protocole Neighbor Discovery(ND)

Defintion : Ce Protocole de voisinage son rôle primordiale est l'échange d'information entre les nœuds et les hôtes ipv6 dans le bute de découvrir les adresses (ip) des voisins,résoudre les adresses MAC (Media Access Control),et bien sure mettre a jour les tables de voisins. Ce protocole utilisé pour étudier la topologie local et identifier les adresses IP et les prefixes des routeurs

Le mécanisme Neighbor Discovery Protocol (NDP) fournit en IPv6 un certain nombre de fonctionnalités indispensables au bon fonctionnement du protocole IPv6.La plus connue est la fonctionnalité de résolution d'adresse qui correspond à ce qu'est ARP en IPv4 [19]

Touts ces fonctionnalité essentielle dans la communication sont le but de l'attaquant pour compromettre la sécurité de réseau.

Le ND est basé sur les messages :

on peut destinguer cinq types d'ICMPv6 selon [12] :

— Type 134 : Router Advertisement (RA)
— Type 133 : Router Solicitation (RS)
— Type 135 : Neighbor Solicitation (NS)
— Type 136 : Neighbor Advertisement (NA)
— Type 137 : Redirect

Les tâches et des possibilités du NDP

le protocole NDP peut :[9]

— Détecter le routeur et le préfixe réseau.
— Déterminer les paramètres importants pour la transmission des paquets.
— Résolution de l'adresse IP dans l'adresse MAC : il permet d'identifier les adresses MAC (Media Access Control) correspondant aux adresses IPv6 des autres nœuds du réseau local.
— Détecter l'inaccessibilité d'un voisin : permet à chaque nœud de réseau de détecter les autres hôtes qui sont présents dans le lien ; pour faciliter la connexion entre eux, les nœuds envoient périodiquement des messages Neighbor Advertisement pour déclarer leur disponibilité.
— Détecter les adresses dupliquées.
— Auto configuration d'adresses et Détection de duplication d'adresse.

2.3 Attaques par déni de service (DoS)

2.3.1 Définition

Les attaques par déni de service (DoS), appelées aussi attaques de saturation, sont des attaques informatiques visant à rendre un service, un site web ou un réseau indisponible pour les utilisateurs légitimes. L'objectif principal de ces attaques est de submerger les ressources du système cible, telles que la bande passante du réseau, la puissance de traitement du serveur ou les connexions disponibles, afin d'empêcher leur bon fonctionnement.[10]

2.3.2 Méthode d'attaque (DoS) dans IPv6

La méthode de fonctionnement d'une attaque par déni de service (DoS) dans le contexte d'IPv6 est similaire à celle des attaques DoS dans IPv4 :

1. Reconnaissance de la cible : L'attaquant identifie la cible IPv6 qu'il souhaite rendre indisponible. Cela peut être une adresse IP spécifique, un sous-réseau ou un service hébergé sur un réseau IPv6.

2. Choix de la méthode d'attaque : L'attaquant sélectionne une méthode spécifique d'attaque DoS adaptée à IPv6. Les méthodes couramment utilisées incluent l'inondation de paquets, l'amplification du trafic, l'épuisement des ressources, les attaques de fragmentation, etc.
3. Préparation de l'attaque : L'attaquant prépare les outils et les ressources nécessaires pour lancer l'attaque DoS. Cela peut impliquer la configuration de logiciels malveillants, l'utilisation de botnets ou d'autres moyens pour générer un trafic massif ou exploiter des vulnérabilités spécifiques à IPv6.
4. Lancement de l'attaque : L'attaquant envoie un volume élevé de paquets ou de demandes malveillantes vers la cible IPv6. Cela peut inclure l'envoi de paquets d'inondation, l'exploitation de vulnérabilités spécifiques à IPv6, l'utilisation de techniques d'amplification, etc. L'objectif est de submerger les ressources du système cible et de rendre le service indisponible.
5. Impact sur la cible : Lorsque le système cible IPv6 est submergé de trafic malveillant, ses ressources peuvent être épuisées, entraînant une indisponibilité du service pour les utilisateurs légitimes. Les ressources telles que la bande passante, la mémoire, le processeur ou les connexions réseau peuvent être saturées, ce qui affecte la capacité du système à répondre aux demandes légitimes.
6. Durée de l'attaque : La durée de l'attaque DoS peut varier, allant de quelques minutes à plusieurs heures, voire plus longtemps. Elle dépend de la capacité de l'attaquant à maintenir l'attaque et des mesures de protection mises en place par la cible.

2.3.3 exemples d'attaques DoS courantes :

Les attaques de saturation de la bande passante : le principe de ce mode d'attaque est que L'attaquant envoie une quantité massive de paquets IPv6 vers la cible,qui dépassent la capacité de sa bande passant,dans le but d'épuiser cette dernière.

Attaque d'amplification :ce type d'attaque exploite généralement le protocole icmpv6 pour renvoyait des demandes conçues a des hôtes tiers qui renvoient des réponses volumineuses à la cible.

2.3.4 Quelle est la différence entre une attaque DoS et une attaque par déni de service distribué (DDoS) ?

La principale différence entre une attaque par déni de service distribué (DDoS) et une attaque DoS réside dans l'origine de l'attaque. Une attaque DDoS est lancée de

façon orchestrée depuis de multiples emplacements et par plusieurs systèmes en même temps, tandis qu'une attaque DoS est isolée par nature. En général, une attaque DDoS est considérée comme plus sophistiquée et représente une menace bien plus grave pour les entreprises du fait de l'utilisation de plusieurs terminaux basés en divers endroits, ce qui complique son identification, son suivi et sa neutralisation. Le plus souvent, les cybercriminels utilisent un botnet ou réseau de robots (un ensemble d'ordinateurs ou de terminaux compromis supervisés par un canal de commande et contrôle (CC))pour exécuter ce type d'attaque synchronisée [6]

Mais on peut limiter le risque de ce type d'attaque en appliquant régulièrement des exercices de simulation de gestion d'incident et des tests d'intrusion pour améliorer les capacités de prévention grâce à l'identification des points faibles de l'architecture réseau.

2.4 Attaque par Scanning d'adresses IPv6 :

L'identification de la cible est une partie essentielle dans l'attaque, c'est pourquoi l'attaquant commence généralement par le scanning.

2.4.1 Définition :

L'attaque par Scanning d'adresses IPv6 est une méthode sophistiquée utilisée par les experts en sécurité informatique pour effectuer une reconnaissance détaillée et exhaustive d'un réseau IPv6 spécifique. Cette technique vise à identifier et à analyser de manière systématique les adresses IPv6 actives au sein d'un réseau donné.

2.4.2 La méthode de fonctionnement :

Voici une description de la méthode qui peut être employée par l'attaquant :

— Collecte d'informations : Pour bien comprendre la topologie du réseau à attaquer, cette étape est cruciale. Pour cela, l'attaquant commence généralement par collecter des informations sur les adresses IPv6, les préfixes, les protocoles de découverte de voisinage utilisés, et les adresses multicast.

— Génération d'adresses IPv6 : À partir des informations collectées, l'attaquant commence à générer des adresses IPv6 potentielles à scanner en utilisant des règles et des schémas spécifiques, ou en utilisant les préfixes annoncés.

— Scanning des adresses IPv6 : Après la génération d'adresses IPv6, l'attaquant cible envoie des requêtes à ces adresses pour tester la correspondance des hôtes (s'ils sont actifs). Pour atteindre ce but, il existe différentes techniques de scanning pouvant

être utilisées, telles que le ping ICMPv6, les requêtes de protocoles spécifiques (comme HTTP, FTP, DNS, etc.).

— Analyse des réponses : Afin de déterminer les services ouverts, les versions de logiciels, les vulnérabilités potentielles, l'attaquant peut utiliser des outils d'analyse de paquets pour extraire et traiter les informations obtenues lors du scanning.

— Cartographie du réseau : Pour mieux comprendre la structure du réseau à attaquer, l'attaquant utilise les informations recueillies pour établir une cartographie détaillée du réseau IPv6, y compris les adresses actives, les relations de voisinage, les services exposés, les points d'entrée potentiels, les vulnérabilités.

2.5 Attaques specifique a IPv6 :

2.5.1 Attaque Multicast Listener Discovery MLD :

Definition :Le MLD est l'équivalent du protocole Internet Group Management Protocol (IGMP) utilisé dans IPv4 pour la gestion du trafic multicast. Ce type d'attaque de l'ipv6 vise à perturber le bon fonctionnement de mécanisme MLD.

Dans ce type d'attaque l'intrusive vas essayer de [50] :

Envoyer massivement des messages MLD Membership Query sur le réseau. Ces requêtes sont normalement utilisées pour découvrir quels hôtes sont intéressés par la réception de trafic multicast spécifique. L'attaque d'inondation MLD peut submerger le réseau de requêtes MLD qui vas causer que les hôtes légitimes d'accéder aux flux multicast légitimes ou en provoquant des interruptions de service pour les utilisateurs.

2.5.2 Attaques de Tunneling :

definition :le tunneling est une technique qui permet d'acheminer des données à travers des réseaux, en les encapsulant dans un format spécifique pour assurer leur confidentialité, leur intégrité et/ou leur acheminement efficace.

Le protocole ipv6 a été conçu pour pouvoir fonctionner dans un environnement hétérogène où IPv4 coexiste.les mécanismes de tunneling donne la possibilité de transformer le paquet ipv6 a travers le ipv4. Ce type d'attaque se produit dans ipv6 quand un attaquant exploite les mécanismes de tunneling d'IPv6 pour contourner les mesures de sécurité mises en place sur un réseau.voici comment on peut faire une attque de tunneling [50] :

Teredo :est un mécanisme de tunneling qui permet à des hôtes IPv6 de communiquer avec des hôtes IPv4 via NAT.cela peut être utilisé pour contourner du trafic malveillant à travers un pare-feu ou un routeur NAT.

ISATAP :c'est un mécanisme qui permet de coexister avec l'ipv4 dont les paquets ipv6 sont transformé dans des paquets icmpv4.

2.5.3 Attaques de voisinage (Neighbor Discovery) :

C'est une attaque sur les protocoles de découverte de voisinage comme Neighbor Discovery Protocol (NDP), ou sur les messages ICMPv6, qui peut exploiter des vulnérabilités spécifiques de ces protocoles de réseau pour mener des attaques.

utilisation dans des attaques courantes :

Ce type d'attaque se base sur l'exploitation des messages envoyés entre les dispositifs (RS, RA, NS, NA) pour les contrôler et prendre la connexion en charge, et peut lancer une attaque DoS ou MITM (Homme du Milieu). Voici comment mener une attaque de voisins :[39]

- Attaques d'usurpation Spoofing : Le principe de cette attaque est quand un nœud (attaquant) dans le lien envoie des messages de découverte de voisins (NDP) tels que des messages Neighbor Solicitation (demande de voisin) ou Neighbor Advertisement (annonce de voisin) falsifiés sur le réseau dans le but de :
  - Falsification de l'identité du nœud émetteur : tromper les nœuds voisins du réseau IPv6 à traiter ce dernier comme une hôte légitime alors qu'ils interagissent en réalité avec l'attaquant ; en manipulant les adresses MAC (Media Access Control) ou les adresses IPv6.
  - Falsification de l'adresse IP de destination : afin d'intercepter ou de manipuler les communications entre les nœuds du réseau. L'attaquant va modifier les adresses de destination pour diriger le trafic vers des destinations illégitimes.
- Attaques de déni de service (DoS) : Ce type d'attaque vise à submerger la bande passante des nœuds cibles avec un trafic excessif de messages de découverte de voisins invalides ou falsifiés. Quand la capacité de traitement des nœuds est saturée, les hôtes ne répondent pas aux demandes nécessaires, ce qui entraîne une perturbation dans la communication et une dégradation des performances du réseau.[12]
- Attaques d'épuisement de la table de voisinage : Les protocoles de routage doivent maintenir dans une table la liste des routes qu'ils sont chargés de distribuer. La taille de cette table est limitée par la mémoire de l'équipement. Chaque nœud IPv6 dispose d'une table de routage qui enregistre les adresses IPv6 et les adresses MAC de ses voisins. Dans ce cas, l'attaquant vise à envoyer un nombre important de messages de découverte de voisins falsifiés, ce qui entraîne des erreurs de routage et des pertes de paquets à cause du nombre important de messages non supportés

par la table de voisinage.

— Attaques de rejeu (replay) ou Homme du Milieu : L'attaquant essaie de capturer des messages de découverte de voisins échangés entre les nœuds légitimes, puis ensuite il essaie de les réutiliser pour mener des attaques en faisant croire que celui qui envoie ces messages est un nœud légitime pour tromper les nœuds cibles. Cela peut conduire à des comportements indésirables comme l'envoi de données corrompues qui compromettent l'intégrité des communications.[12]

— Attaques de détection et de suivi : Ce type d'attaque consiste à surveiller les communications échangées et les messages de découverte de voisins afin d'obtenir des informations telles que les adresses IP, les adresses MAC, les identifiants de nœud, etc., qui peuvent être utilisées pour identifier les vulnérabilités du réseau et donc assurer la réussite de l'attaque.

— Attaques de détournement de voisins : L'attaquant avec cette méthode essaie d'usurper l'identité d'un nœud voisin légitime pour détourner les communications à son avantage. Ce nœud falsifie les messages de découverte de voisin pour annoncer qu'il est le nœud de destination légitime. En conséquence, le trafic qui était initialement destiné à un nœud spécifique est redirigé vers l'attaquant.

Secure Neighbor Discovery (SeND) : SeND a été développé pour renforcer la sécurité de Neighbor Discovery en fournissant des mécanismes de protection contre ces types d'attaques, notamment la cryptographie comme RSA [39]

2.5.4 Les attaques par fragmentation

Définition d'une fragmentation

La fragmentation est une technique qui permet de diviser un paquet IPv6 en petits fragments, faciles à envoyer dans des liaisons ou des réseaux ayant des limitations de taille maximale de transmission [39].

Attaque de fragmentation

Une attaque de fragmentation dans IPv6 est une technique utilisée par des pirates informatiques ou des attaquants, dans laquelle ils exploitent les techniques de fragmentation de paquets échangés dans le protocole IPv6 dans le but de compromettre un réseau ou de perturber son fonctionnement normal. Dans une attaque de ce type, l'attaquant tente d'envoyer des fragments mal formés ou assemblés de manière incorrecte [20].

Méthodes d'exploitation d'attaques par fragmentation

- **Attaque de ré-assemblage inachevé :** Les attaquants pourraient fragmenter un paquet de manière à ce que le ré-assemblage ne puisse pas être fait correctement, ce qui produira un comportement inattendu dans le réseau attaqué.
- **Bypass de filtrage :** Les pare-feu et les IDS peuvent avoir du mal à analyser les paquets fragmentés. Les attaquants peuvent exploiter cette faiblesse en fragmentant leurs attaques pour contourner les mécanismes de sécurité et atteindre la cible sans être détectés.
- **Manipulation de la taille des fragments :** Dans ce type d'attaque, l'attaquant peut fragmenter un paquet de manière à ce qu'une partie importante de l'en-tête soit placée dans un fragment particulier, ce qui pourrait entraîner une mauvaise interprétation par les dispositifs de sécurité

2.6 Les vulnérabilités d'IPv6

Les caractéristiques de sécurité d'IPv6 ont été mentionnées dans RFC 2401, RFC 2402 et RFC 2406, mais nous allons décrire les vulnérabilités d'IPv6 dans cette partie.

2.6.1 Large espace d'adressage

L'espace d'adressage d'IPv6 est extrêmement vaste, ce qui offre des avantages en termes d'adressage, mais peut aussi créer des difficultés en termes de gestion d'un tel volume d'adresses. Par exemple, une mauvaise gestion des adresses pourrait permettre à des dispositifs non autorisés de gagner l'accès à travers des adresses IP valides et compromettre la sécurité du réseau. Les attaquants peuvent cibler les vulnérabilités de l'espace d'adressage pour effectuer des attaques sur le réseau. Voici quelques méthodes d'attaque possibles liées à l'espace d'adressage étendu d'IPv6 [20] :

- Scans d'adresses : en raison de la vaste plage d'adresses, les attaquants peuvent explorer cette vulnérabilité pour effectuer un scan afin d'identifier les hôtes actifs et vulnérables sur le réseau.
- Utilisation malveillante de l'auto-configuration : la technologie IPv6 permet aux dispositifs de configurer leur adresse sans avoir besoin d'un serveur DHCP. Les attaquants pourraient exploiter ce processus pour générer de nouvelles adresses IP et accéder au réseau de manière indésirable.
- Attaque de l'Internet des objets (IoT) : les attaquants peuvent explorer l'expansion de l'espace d'adressage pour trouver des objets connectés et vulnérables.

2.6.2 Suivi l'identite de utlilisateur dans L'IPv6

Cette vulnérabilité est liée au suivi de l'identité de l'utilisateur dans un environnement IPv6, ce qui signifie la capacité des nœuds malveillants à collecter des informations sur l'activité d'un utilisateur et à suivre sa présence. Cette situation peut mettre en danger la vie privée et la sécurité de l'utilisateur. Dans IPv6, l'appareil connecté au réseau se voit attribuer une adresse IP unique de manière statique. La longueur accrue des adresses IPv6 permet la création d'un plus grand nombre d'adresses, ce qui peut faciliter la mise en place de mécanismes de suivi. Un utilisateur obtient un préfixe de 64 bits, et après avoir été connecté par la découverte de routeur, il est possible de tracer l'identité du trafic d'un nœud spécifique [20].

Implications sur la vie privée et la sécurité

Le suivi de l'identité peut avoir des conséquences significatives sur la vie privée et la sécurité de l'utilisateur, telles que l'utilisation des informations collectées à des fins nuisibles, la surveillance illégale, le vol d'identité et le piratage. Cette vulnérabilité peut également affecter la liberté et l'anonymat des utilisateurs dans le réseau.

2.6.3 Auto-configuration et adresse temporaire

Les dispositifs dans un environnement IPv6 génèrent des adresses IP de manière automatique sans avoir besoin d'un serveur DHCP (Dynamic Host Configuration Protocol), en utilisant le mécanisme SLAAC basé sur les préfixes annoncés par les routeurs du réseau. Cela peut entraîner certains risques liés à l'auto-configuration :

- Accès non autorisé : en raison de l'auto-configuration, les dispositifs non autorisés peuvent obtenir une adresse IP valide et accéder au réseau.
- Adresses temporaires : grâce à l'auto-configuration, les dispositifs peuvent générer des adresses temporaires afin de préserver la confidentialité de l'adresse permanente. Cependant, cela peut être exploité pour compliquer la surveillance et la traçabilité des activités des utilisateurs.
- Inondation d'annonces : les annonces de routeurs sont nécessaires pour que l'auto-configuration fonctionne. Cependant, les attaquants peuvent exploiter ce mécanisme pour envoyer de fausses annonces de routeurs, provoquant ainsi des perturbations dans l'attribution correcte des adresses IP et potentiellement des dysfonctionnements dans le réseau.

2.7 Conclusion

Dans ce chapitre, nous avons examiné en détail quelques protocoles utilisés dans un environnement IPv6, tels que ICMPv6 et la découverte de voisinage, et comment ils peuvent être exploités pour mener des attaques. Nous avons également examiné en détail quelques vulnérabilités et les attaques courantes dans l'environnement IPv6, susceptibles de compromettre la disponibilité, l'intégrité et la confidentialité des réseaux, ainsi que la manière dont ces attaques peuvent avoir lieu.

3

Sécurité d'Internet des objets sous Ipv6

3.1 Introduction

L'Internet des Objets (IoT) a révolutionné la façon dont nous interagissons avec le monde qui nous entoure. Des capteurs intelligents intégrés dans nos maisons aux appareils connectés dans l'industrie, en passant par les véhicules autonomes, l'IoT promet de rendre notre vie plus pratique, efficace et interconnectée que jamais. Cependant, derrière cette révolution technologique se cache un défi majeur : la sécurité

3.2 definition d'Internet des objets IoT

L'internet des Objets (iot) est un paradigme technologique et conceptuel qui repose sur l'interconnexion d'entités physiques ou virtuelles au sein d'un environnement global, via des protocoles de communication standardisés, afin de permettre l'acquisition, le partage et l'analyse de données de manière automatique et autonome. Il englobe une variété d'objets, tels que des capteurs, des dispositifs électroniques, des systèmes embarqués et autres entités connectées, qui sont habilités à collaborer et à interagir les uns avec les autres ainsi qu'avec des systèmes informatiques à travers les réseaux informatiques et Internet. Internet of things (IOT) rend les objets simples des objets intelligents capables de transférer des données sur un réseau sans interaction humaine[26]

L'Iot repose sur des technologies de communication sans fil, de traitement des données en temps réel, d'apprentissage automatique et d'intelligence artificielle, permettant ainsi aux objets de collecter, de transmettre, de stocker et d'analyser des données provenant de leur environnement, afin de fournir des informations exploitables pour des applications diverses. Ce concept trouve des applications dans de nombreux secteurs, tels que l'industrie 4.0, la surveillance environnementale, la santé connectée, la logistique, l'agriculture de précision, et bien d'autres encore. En somme, l'Internet des Objets constitue une convergence entre les mondes physique et numérique, ouvrant la voie à des systèmes autonomes et intelligents capables de prendre des décisions en temps réel en se basant sur les données collectées et analysées à travers des réseaux de communication interconnectés.

3.3 Pourquoi utilise l'internet des objets (iot)

Tout d'abord l'IoT et sa technologie améliorent tous les aspects de notre quotidien. Par exemple, elle supprime une partie de notre effort manuel au niveau des machines en exécutant les taches à un temps donné ou selon une condition précise, réduit les coûts et rend la vie plus confortable. On peut citer les machines à café automatiques, des voitures autonomes, des bracelets qui détectent et signalent les maladies parmi les applications possibles grâce à l'internet des objets .

3.4 L'architecture IoT

On ne peut pas étudier la sécurité dans l'IoT sans comprendre son architecture. Ci-dessous, nous décrivons les six couches de l'IoT comme illustré dans la Figure 3.1 :

3.4.1 La couche de codage

La couche de codage est la base de l'IoT, fournissant une identification (ID) aux objets d'intérêt [27].

3.4.2 La couche perception

La couche perception de l'IoT donne un sens physique à chaque objet. Elle se compose de capteurs de données sous différentes formes, tels que les étiquettes RFID, les capteurs infrarouges (IR) et d'autres réseaux de capteurs capables de détecter la température, l'humidité, la vitesse et la localisation des objets. Cette couche recueille des informations utiles des objets via les capteurs qui leur sont associés, puis convertit ces informations en

signaux numériques qui sont ensuite transmis à la couche réseau pour d'autres traitements [47].

3.4.3 La couche réseau

La couche réseau a pour objectif de recevoir les informations sous forme de signaux numériques de la couche de perception, puis de les transmettre vers les systèmes de traitement via différents supports de transmission tels que le WiFi, le Bluetooth, le WiMaX, Zigbee, GSM [47].

3.4.4 La couche Middleware

Également appelée la couche de traitement, elle stocke, analyse et traite une énorme quantité de données en provenance des capteurs. Elle utilise différentes technologies telles que les bases de données, le cloud computing et les modules de traitement de données massives (big data processing) [27].

3.4.5 La couche Application

Cette couche a pour but de fournir des services spécifiques aux utilisateurs grâce à des applications intelligentes de haut niveau de l'IoT. Elle est essentielle au développement d'un réseau IoT à grande échelle, car elle encourage l'expansion de l'IoT en offrant des applications adaptées à divers besoins [47].

3.4.6 La couche Business

Les applications et les services fournis par l'IoT sont gérés dans cette couche [47].

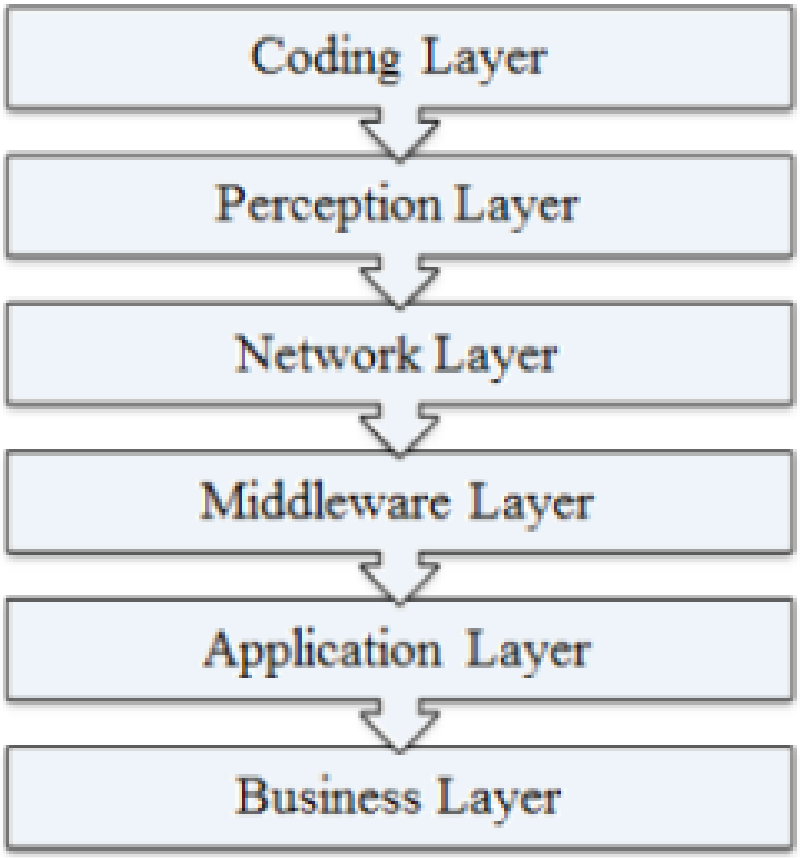

FIGURE 3.1 – Les couches de l'IoT [27]

3.5 Domaines d'Applications

L'Internet des Objets (IoT) touche pratiquement tous les domaines de notre vie quotidienne, offrant des solutions novatrices et des améliorations significatives. Voici quelques exemples de domaines d'application de l'IoT [23] :

- **Les villes :** L'IoT permet une meilleure gestion des réseaux d'infrastructure urbaine tels que l'eau, l'électricité, le gaz, etc. Il permet un contrôle continu en temps réel et précis. Des capteurs peuvent être utilisés pour améliorer la gestion des parkings, surveiller le trafic urbain, réduire les embouteillages et les émissions de CO2.
- **Le transport :** L'IoT joue un rôle essentiel dans le domaine des véhicules intelligents, contribuant à la sécurité routière et à l'aide à la conduite. Cela implique la communication entre véhicules, ainsi qu'entre les véhicules et l'infrastructure routière.
- **La santé :** L'IoT permet le contrôle et le suivi des signes cliniques, facilitant la télésurveillance des patients à domicile. Il offre des solutions pour l'autonomie des

personnes à mobilité réduite.

— **L'industrie :** L'IoT offre une traçabilité totale des produits, depuis la chaîne de production jusqu'à la chaîne logistique et de distribution. Il supervise également les conditions d'approvisionnement.

— **L'agriculture :** Dans ce domaine, des réseaux de capteurs interconnectés à l'IoT sont utilisés pour surveiller l'environnement des cultures. Cela permet une meilleure prise de décision en agriculture, notamment pour optimiser l'irrigation et planifier les travaux agricoles. Ces réseaux peuvent également être utilisés pour lutter contre la pollution de l'air, du sol et de l'eau, améliorant ainsi la qualité globale de l'environnement.

3.6 C'est quoi IoT sous IPv6 ?

L'Internet Engineering Task Force (IETF), qui a créé l'IPv4, a décidé de ne pas utiliser l'IPv5 parce qu'il ne serait éventuellement jamais suffisant en termes d'espace d'adressage. IPv6 est la dernière version du protocole Internet. Les dispositifs qui utilisent Internet sont reconnus par leur adresse IP unique.

Les caractéristiques d'un environnement IoT sont définies comme suit [23] :

— L'IoT est un environnement non maîtrisé en raison de la mobilité des objets interconnectés et de la moins grande possibilité d'y accéder physiquement.

— L'hétérogénéité : un environnement IoT peut comporter une variété de dispositifs, de protocoles, de technologies et de plates-formes qui composent l'écosystème.

— La scalabilité : grâce à l'espace d'adressage étendu, la quantité d'objets qui peuvent être interconnectés est énorme.

— Les ressources limitées en matière d'énergie, de capacité de calcul et d'espace de stockage.

3.7 Intégration de IPv6 dans l'Internet des Objets

L'intégration de l'IPv6 (Internet Protocol version 6) dans l'Internet des objets (IoT) est cruciale pour la croissance et le développement de cet écosystème. IPv6 représente l'évolution par rapport à son prédécesseur, IPv4, en offrant un espace d'adressage considérablement plus vaste, répondant ainsi aux besoins fondamentaux de connecter un grand nombre d'objets et de dispositifs. Cette évolution élimine les contraintes liées au partage d'adresses et les problèmes de translation d'adresses réseau (NAT).

L'utilisation d'IPv6 dans l'Internet des objets présente de nombreux avantages et mécanismes, notamment l'authentification et l'intégrité des données. IPv6 favorise également

la scalabilité, un aspect essentiel pour l'IoT en constante expansion.

Les avantages de l'utilisation d'IPv6 par rapport à IPv4 dans l'IoT sont [21] :

- **Mobilité :** I :ipv6 dans iot offre la capacité de rester connecter de manière transparent quand il se déplace ente différent réseau par exemple donner la possibilité a un téléphone mobile de se connecter même dans le cas du mouvement et pour ce ipv6 utilise les fonctionnalité de (automatic IP configuration et extended headers).ca veut dire que les appareils iot peuvent maintenir leur adresses ipv6 globalement routable même dans le cas de passer d'une point d'accès a une autre cette fonctionalite offre la disponibilité et la connectivité des appareille même dans le déplacement.

  grâce à l'espace d'adressage étendu et à la structure hiérarchique de son adressage l'ipv6 facilite la mobilité ;les routeurs et les reseau sont conçu pour acheminer correctement le trafic vers l'appareille en utilisant cette adresse ipv6.cela vas offrire la capacité aux dispositifs IoT de maintenir des sessions actives sans interruption notable. On déduit que la mobilité est cruciale pour la gestion de flottes de véhicules, la surveillance en temps réel d'actifs mobiles, la télémétrie des objets en mouvement et les applications de suivi de la localisation.
- **Auto-configuration :** LAuto-configuration se réfère a la capacité des dispositifs de configurer automatiquement leurs adresses IP et d'autres paramètres réseau sans nécessiter d'intervention manuelle ou un serveur DHCP en utilisant d'autre méthode automatisé et efficace. En utilisant le mécanismes tels que le Protocole d'auto-configuration sans état (SLAAC) les dispositifs d'internet des objets obtient des adresses ipv6 et d'autre information réseau L'Auto-configuration simplifie la gestion des dispositifs iot .en éliminant la nécessité de configurer manuellement chaque appareil.afin économiser le temps et des efforts et facilite le process ajoute d'autre dispositif au réseau.
- **Adressage étendu :** Par rapport a l'ipv4 ; l'ipv6 offre la capacité d'utiliser des adresses IP beaucoup plus longues et uniques avec 128 bits il peut répondre au demandes agressive au niveau mondiale et offrir une quantité astronomiquement plus grande de combinaisons possibles.
- **Connectivité directe :** ipv6 permet a chaque dispositifs d'avoir son propre adresse ip unique peut être utilisé pour identification et la communication direct. Grâce a l'espace d'adressage étendu et la possibilité d'attribuer des adresses publiques uniques à chaque dispositif connecté.Ipv6 offre aux dispositifs de iot la capacité de faire des communication entre eux sans mécanismes complexe de traduction d'adresses. La connectivité directe présente plusieurs avantages pour

l'IoT : -Simplicité de communication :communication direct entre iot dispositifs -Amélioration de sécurité : La communication directe permet de contourner les éventuelles vulnérabilités introduites par la translation d'adresses. -Meilleur évolutivité :chaque dispositifs a un adresse ipv6 unique ce qui simplifie la gestion des réseaux à grande échelle.

— **Sécurité renforcée :** Ipv6 vient avec la fonctionnalité de sécurité IPsec qui donne la possibilité de crypter et d'authentifier les communications entre les dispositifs IoT.ceci peut protège contre les attaques potentielles. Dans le contexte d'internet des objet le contexte de sécurité est crucial ;o un grande nombre de dispositifs interconnecté échangent des information sensible pour cela été l'intégration de IPsec (IP security) ;un protocole qui offre une couche supplémentaire de protection pour les données en transit.

Les principales fonctions de sécurité

— **Cryptage :** Lorsque des tiers interceptent des paquets de données transférés entre les dispositifs interconnectés, ils ne peuvent pas déchiffrer les informations contenues à l'intérieur grâce au chiffrement des données. Cela protège les données sensibles contre les interceptions et les violations de la confidentialité.

— **Authentification :** IPsec fournit des mécanismes d'authentification pour s'assurer que les dispositifs communiquent avec des pairs légitimes. Dans le contexte de l'IoT, où les dispositifs interconnectés échangent une variété de données, cette authentification est essentielle pour garantir que les informations importantes sont traitées en toute sécurité.

— **Gestion de la qualité de service (QoS) :** Pour garantir les performances des applications sensibles telles que la télémédecine ou les systèmes de contrôle industriels, IPv6 offre des options spéciales pour la gestion de la qualité de service. La QoS est un aspect crucial de l'Internet des objets, permettant :

  — **Réduction de la latence :** Pour minimiser la latence, c'est-à-dire le temps de retard entre l'envoi et la réception des données, afin d'offrir une expérience plus fluide pour les applications nécessitant une communication en temps réel, telles que les jeux en ligne.

  — **Priorisation des données :** En permettant la priorisation des données en fonction de leurs besoins, afin de garantir une expérience fluide et réactive pour l'utilisateur.

  — **Adaptabilité dynamique :** L'ajustement des conditions du réseau en fonction de la charge du réseau et des besoins changeants des applications.

  — **Préparation pour l'avenir :** IPv6 offre une solution à long terme pour

répondre à tous les besoins d'adressage croissants.

Après avoir examiné tous ces avantages de l'utilisation du protocole IPv6 dans l'IoT, il est clair que le déploiement de cette technologie n'est pas seulement justifié, mais il est également indispensable pour soutenir la croissance continue de l'IoT et garantir son succès futur. La durabilité est un facteur clé dans cet écosystème en expansion.

3.8 L'internet des Objets : vulnérabilités et menaces

3.8.1 Authentification et/ou autorisation insuffisantes :

L'accès aux ressources d'un objet doit être interdit aux entités non authentifiées ou non autorisées. Ce type de vulnérabilité est classé comme **SÉVÈRE** concernant l'impact sur les données et sur l'appareil lui-même (la perte ou la compromission des données, et même la prise de contrôle de l'équipement et/ou des comptes d'utilisateurs). L'attaquant peut aussi profiter de l'absence d'un contrôle d'accès granulaire et de la faiblesse des identifiants. Elle est classée comme **MOYENNE** en termes d'exploitabilité et **FACILE** en termes de détectabilité [24].

Risques et vulnérabilités de cette faille :

- **Accès non autorisé :** Les utilisateurs qui n'ont pas le droit d'accéder à des informations sensibles peuvent obtenir l'accès et compromettre la confidentialité et la sécurité des informations.
- **Modification non autorisée :** Un attaquant peut modifier les données d'un appareil et causer des dysfonctionnements, des erreurs de contrôle ou des interruptions dans les opérations.
- **Attaques d'élévation de privilèges :** Un attaquant peut utiliser une autorisation insuffisante pour élever sans autorisation dans le réseau et compromettre le réseau.
- **Destruction de données :** Un utilisateur non légitime peut supprimer des données importantes en exploitant des autorisations insuffisantes.

Pour résoudre le problème de l'authentification et/ou de l'autorisation insuffisantes dans l'Internet des Objets (IoT), il faut essayer de mettre en place une gestion centralisée des identités et des accès pour tous les dispositifs IoT. Utilisez des systèmes de gestion d'identités pour attribuer des autorisations spécifiques à chaque dispositif en fonction de ses rôles et responsabilités.

3.8.2 Attaques ciblant les interfaces web non sécurisées :

Un acteur interne ou externe peut exploiter la faiblesse des identifiants et/ou l'énumération des comptes des utilisateurs. Cette vulnérabilité est classée comme **FACILE**, ce qui signifie que les attaques de ce type peuvent être découvertes simplement en examinant manuellement l'interface ou en utilisant des outils de tests automatisés qui peuvent de plus détecter d'autres attaques telles que le cross-site scripting (XSS). L'impact d'une interface web non sécurisée peut conduire à la corruption, la perte des données ou la prise de contrôle de l'appareil. C'est la raison pour laquelle ce type de vulnérabilité est classé comme **SÉVÈRE** en termes d'impact [24].

Risques et vulnérabilité de cette faille :

- **Injection de code :** Un attaquant peut injecter un code de type JavaScript ou SQL dans les champs de formulaire. Cela peut entraîner l'exécution de ce code indésirable, la divulgation de données sensibles ou la prise de contrôle du dispositif.
- **Accès non autorisé.**
- **Attaque DoS (Déni de service) :**
- **Attaque de force brute.**

Cependant, on peut utiliser le protocole SSL/TLS pour chiffrer toutes les communications entre les dispositifs IoT et les interfaces web. Ou encore, utiliser des certificats SSL/TLS valides émis par une autorité de certification de confiance pour garantir l'authenticité des interfaces web IoT. Il est également recommandé d'utiliser des méthodes d'authentification solides, telles que l'authentification multifactorielle (MFA) pour les utilisateurs.

3.8.3 Absence de chiffrement de la couche de transport :

L'écoute ou la falsification des données peuvent être facilement exécutées par un attaquant dans le cas où des données non chiffrées sont envoyées sur le réseau. L'absence de chiffrement du trafic sur le réseau local est souvent liée au fait que ce trafic n'est pas visible depuis l'extérieur. Cependant, dans un réseau local mal configuré, cela peut ne pas être le cas, ce qui peut entraîner la fuite de données ou leur perte. Plusieurs propositions pour le chiffrement de bout en bout utilisent soit DTLS soit des mécanismes cryptographiques demandant une faible capacité de calcul [48].

Risques et vulnérabilités de cette faille :

- **Interception de trafic :** Un attaquant peut écouter le trafic et intercepter le flux de données transféré, exposant ainsi les informations sensibles à un accès non autorisé.

— **Vol de données :** Les données sensibles, telles que les mots de passe, les informations de carte de crédit ou les données de santé, peuvent être volées.

— **Attaque de l'homme du milieu.**

Afin d'éviter ces risques, il est recommandé d'utiliser des protocoles de communication qui intègrent nativement la sécurité, tels que SFTP (Secure File Transfer Protocol) pour le transfert de fichiers, SSH (Secure Shell) pour l'accès distant sécurisé.

3.8.4 Software / Firmware non sécurisé :

Le software (logiciel) ou le firmware (microprogramme) d'un dispositif IoT est responsable de son fonctionnement. Le firmware peut contenir des vulnérabilités exploitables par des attaquants lorsque le software est développé sans prendre en compte les meilleures pratiques de sécurité. L'exploitabilité de ce genre de vulnérabilité est **DIFFICILE**, elle a un impact considéré comme **SÉVÈRE**, pouvant conduire à la compromission des données de l'utilisateur et même permettre la prise de contrôle de l'appareil [24].

Risques et vulnérabilité de cette faille :

— **Défauts de conception :** Un attaquant peut contourner les mécanismes de sécurité lorsque le software est non sécurisé.

— **Mauvaise gestion des identifiants :** Quand un software stocke les mots de passe ou des clés de manière non sécurisée, cela les expose à un accès non autorisé.

Afin de réduire le danger de cette faille, il faut intégrer la sécurité dès le début du développement des logiciels (security by design). Cela inclut des revues de code, des tests de sécurité et une évaluation des risques. En plus, choisissez des protocoles de communication sécurisés tels que HTTPS, MQTT avec TLS/SSL, CoAP avec DTLS.

3.8.5 Collecte d'informations personnelles via l'équipement :

Selon une étude réalisée par HP [25], un nombre dépasse de 90 (pour cent) des appareils collectent au moins une information personnelle via l'équipement, le Cloud, ou l'application mobile. Ces informations peuvent être un nom d'utilisateur, son adresse, sa date de naissance, des informations de santé, et même des numéros de carte bancaire [24].

Donc les dispositifs de l'IoT sont conçus afin d'échanger une variété de données ; mais quand ces appareils collectent des informations personnelles comme la localisation et des habitudes d'utilisation, des préférences personnelles ou même des informations de santé, cela peut exposer les utilisateurs à des risques majeurs tels que :

— **Usurpation d'identité :** Si un attaquant obtient des informations sur un utilisateur, il peut potentiellement usurper son identité et mener des attaques de phishing.

— **Divulgation non autorisée :** En cas de violation de sécurité, les données personnelles collectées par les dispositifs IoT comme les coordonnées bancaires ou les données médicales peuvent être divulguées involontairement.
— **Surveillance :** L'utilisation d'informations personnelles collectées pourrait permettre de donner des informations détaillées sur les utilisateurs pour mener une surveillance constante.

Afin d'éviter cela, il faut utiliser des mécanismes de gestion des identifiants robustes pour sécuriser l'accès aux objets IoT et aux données collectées. Les mots de passe doivent être forts et uniques. De plus, les vulnérabilités de type XSS et les identifiants faibles doivent être corrigées.

3.8.6 Vulnérabilités de type XSS et des identifiants faibles :

60 (pour cent) des interfaces d'utilisateur présentent toutes des vulnérabilités, notamment des vulnérabilités de type XSS et des identifiants faibles. La vulnérabilité de type cross-site scripting (XSS) se produit lorsque un attaquant insère du code, généralement de JavaScript, dans un service en ligne pour être exécuté par le navigateur. Cela peut permettre aux attaquants de voler des données, de pirater des sessions utilisateur et d'exécuter des actions non autorisées au nom de l'utilisateur. Dans un environnement IoT, un dispositif IoT domestique contrôlé via une application mobile pourrait être vulnérable à une attaque XSS si les données entrées par l'utilisateur ne sont pas correctement filtrées ou échappées. Un attaquant pourrait alors exploiter cette faille pour accéder aux dispositifs, voler des données sensibles ou prendre le contrôle des dispositifs [24].

L'usage d'identifiants faibles, tels que les noms d'utilisateur et les mots de passe peu complexes, est une vulnérabilité très sensible dans l'IoT. Les dispositifs livrés avec de telles combinaisons d'identifiants faibles peuvent permettre aux attaquants de prendre le contrôle ou de compromettre les réseaux.

3.9 La sécurité des dispositifs IoT

La protection de la technologie IoT concerne en premier lieu la sécurité des données, des communications et des infrastructures réseaux. Cette protection est nécessaire pour contrer les attaques classiques et futures sur l'intégrité, l'authenticité et la confidentialité des données, ainsi que les attaques sur les infrastructures réseaux et leurs fonctionnalités.

3.9.1 Les Technologies de communication dans IoT

Radio Frequency Identification (RFID)

Un système d'identification par radiofréquence (RFID) est un système de communication sans fil dans lequel la liaison radio entre la station de base et les transpondeurs est fournie par les ondes rétro-diffusées modulées. RFID est utilisé pour une grande variété d'applications allant de l'accès familier au bâtiment, au contrôle des cartes de proximité pour le suivi de la chaîne d'approvisionnement, à la collecte de péages, à l'accès au stationnement des véhicules, au contrôle des stocks de détail, à l'accès aux remontées mécaniques, au suivi des livres de bibliothèque, à la prévention du vol, aux systèmes d'immobilisation des véhicules et à l'identification et au suivi du matériel roulant ferroviaire [27].

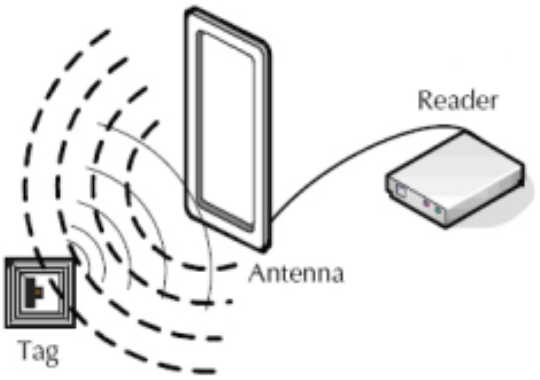

FIGURE 3.2 – Scénario de RFID [27]

On peut distinguer 4 types de fréquences selon le type d'application :

1. Low frequency (135 KHz)
2. High Frequency (13.56 MHz)
3. Ultra-High Frequency (862 MHz - 928 MHz)
4. Microwave Frequency (2.4 GHz, 5.8 GHz)

LoRa

Defintion : LoRa est la nouvelle technologie de communication Réseau étendu de faible puissance (LPWAN). Il s'agit d'un schéma de transmission sans fil ultra longue distance basé sur la technologie à spectre étalé.

LoRa est principalement utilisé dans l'Internet des objets. La longue portée représente un avantage essentiel de LoRa, avec une distance de communication pouvant atteindre

jusqu'à 15 kilomètres. Les caractéristiques de LoRa comprennent une sensibilité de -148 dBm, une faible consommation d'énergie de travail, de nombreux nœuds de réseau, une forte capacité anti-interférence et un coût abordable [27].

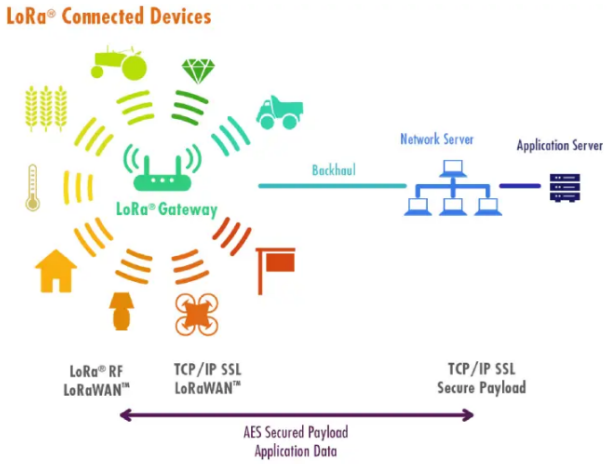

FIGURE 3.3 – LoRa dans un environnement IoT [4]

Bluetooth

Bluetooth est la technologie de communication sans fil à courte portée utilisée pour gérer les connexions entre les appareils sans nécessiter de mot de passe. La technologie Bluetooth utilise des ondes radio UHF (ultra haute fréquence) entre 2.400 et 2.485 GHz, avec une portée maximale d'environ 164 pieds entre deux appareils [31].

Les normes de Bluetooth incluent IEEE 802.15.3, qui vise à proposer du haut débit (20 Mbit/s) avec la technologie Bluetooth, et IEEE 802.15.4, qui vise des applications Bluetooth à bas débit .

Technologies de réseau

— **Wi-Fi :**

Le réseau IEEE 802.11 est une spécification du réseau local sans fil (WLAN). En mode basse bande, IEEE 802.11 (b, g, n) transmet des données à des débits de 11 Mbps à 54 Mbps sur des distances allant jusqu'à 32 mètres à l'intérieur et 95 mètres à l'extérieur. La norme IEEE 802.11n utilise le double du spectre radio par rapport à 802.11a ou 802.11g. Cependant, IEEE 802.11a, avec des données de transmission jusqu'à Gbps, peut dépasser la portée de deux fois celle de b et g. Le Wi-Fi à basse bande transmet dans la bande ISM 2,4 GHz, tandis que le Wi-Fi à haute bande transmet dans la bande 5 GHz [16].

— **Zigbee :**

Defintion : Zigbee est conçu pour les réseaux de l'Internet des Objets (IoT) et pour connecter et contrôler une variété d'appareils domestiques et industriels. Il consomme peu d'énergie et peut prendre en charge de grands réseaux de dispositifs.

Zigbee utilise une topologie maillée, ce qui signifie que les nœuds peuvent agir comme des routeurs. Zigbee est basé sur les spécifications 802.15.4 et comprend des normes telles que Zigbee Pro et Zigbee RF4CE [44].

— **BLE (Bluetooth Low Energy) :**

Defintion :qui signifie "Bluetooth Low Energy", est une technologie de communication sans fil conçue pour fournir une connectivité à faible consommation d'énergie entre des appareils IoT [44] .

BLE utilise la méthode maître et esclave comme illustré dans la Figure 3.4, où un seul nœud est un maître et les autres nœuds sont des esclaves. Il utilise la méthode TDMA pour économiser de l'énergie et offre une grande capacité de transmission, allant de 20 à 200 Mbps [46].

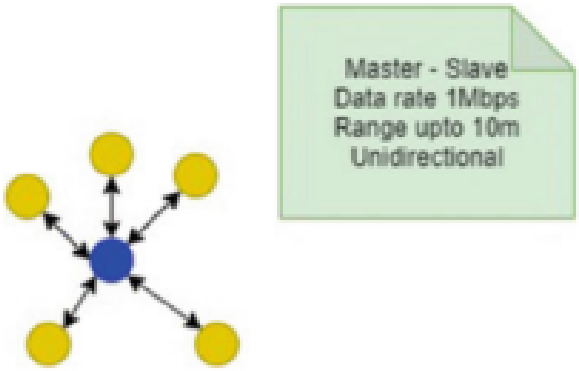

FIGURE 3.4 – Caractéristique de BLE

Le tableau suivant présente une comparaison des caractéristiques des technologies de communication IoT :

Réseau	Bande passante	Distance	Énergie	Coût
Bluetooth	0.27 mégabit/s	100 mètres	Basse	Bas
Wi-Fi	54 mégabit/s	50 mètres	Moyenne	Bas
4G	50 mégabit/s	1 kilomètre	Haute	Haute
5G	10 Gigabit/s	100 mètres	Haute	Haute
Zigbee	250 kbit/s	100 mètres	Basse	Bas
LoRa	50 kbit/s	1 kilomètre	Basse	Moyenne
BLE	Faible à moyen débit	Courte portée	Basse	Bas/Moyenne
RFID	Faible débit	Courte portée	Basse	Bas

TABLE 3.1 – Caractéristiques des technologies de communication IoT

3.9.2 Les Protocoles de l'IoT

De nombreux protocoles peuvent être utilisés pour interconnecter les objets entre eux, parmi lesquels nous mentionnons :

La Couche Application

— **MQTT :**

Defintion : signifie "Message Queuing Telemetry Transport", est un protocole de communication léger basé sur le modèle de publication/abonnement (publish/subscribe) et sur TCP.

Il est largement utilisé dans les applications IoT (Internet des Objets) et M2M (Machine-to-Machine) pour bien transformer les données dans des espaces où la bande passante et les ressources sont limitées [18].

— **DDS :** afin de faciliter la communication en temps réel et la distribution de données entre des systèmes distribués. "Data Distribution Service", est venu avec un ensemble de normes et de spécifications. Il est utilisé dans les systèmes embarqués, les systèmes de contrôle industriels, les systèmes de défense et les systèmes autonomes nécessitant une communication fiable, rapide et prévisible [44].

— **CoAP :**

Defintion : (Constrained Application Protocol) est un protocole apatride développé par l'IETF pour remplacer HTTP dans les périphériques limités en ressources.

Il a été développé pour assurer la fiabilité des communications dans des environnements à faible bande passante entre des capteurs ou des actionneurs. Il fonctionne dans la couche application [24].

Exemple d'utilisation du protocole CoAP :

Il existe des mises en œuvre de la domotique qui incluent plusieurs services comme la sécurité et la mesure de la température ambiante de la maison qui fonctionnent avec l'aide de CoAP. Au sein d'un réseau domestique, différents appareils IoT sont connectés et la communication est établie entre eux à l'aide du protocole CoAP.

La Couche Réseau

— **LoRaWan :**

Défintion : LoRaWan (« Long Range Wide-area network ») est un protocole de communication par radio à bas débit et à longue portée.

LoRaWan permet à des dispositifs intelligents à faibles ressources de communiquer entre eux en utilisant la technologie LoRa, voire d'être connectés à Internet via des passerelles. L'architecture de base d'un réseau LoRaWan repose sur une topologie en étoile, dans laquelle les passerelles transmettent les messages entre les dispositifs et un serveur central souvent connecté à Internet [14].

La Couche Perception

— **Protocole IEEE 802.15.4e :** Pour offrir des améliorations dans la fiabilité, l'efficacité et la flexibilité dans l'IoT, le protocole IEEE 802.15.4e est utilisé. Il propose des caractéristiques telles que la synchronisation pour assurer la continuité de la connexion dans le réseau, réduisant ainsi les interférences et les collisions, et améliorant l'efficacité du réseau. Il inclut également la formation de réseau pour établir une structure de communication cohérente, fiable et sécurisée entre les appareils connectés [46].

— **Z-wave :**

Défintion :est un protocole de communication sans fil destiné à être utilisé dans des smart homes ou des petits commerces. Il a une portée de 30 mètres et utilise CSMA/CA pour la communication ainsi que des messages ACK [46].

A cause de la complexité des communications des nouvelles techniques de sécurité sont inventées.

3.9.3 Protocoles de sécurité d'IoT

IPsec :

Défintion :est un ensemble de protocoles conçus pour assurer la sécurité des communications IP en ajoutant une couche de protection dans le protocole réseau. Son rôle essentiel est de sécuriser les connexions entre les dispositifs IoT et les réseaux, ainsi que les communications entre réseaux distants.

Le mécanisme IPsec introduit deux extensions d'en-tête [46] :

— l'en-tête AH (authentification header) : est conçu pour assurer l'intégrité et l'authentification des données IP sans chiffrement des paquets. Il comprend des champs tels que Next header, Payload length, Spi (security parameter index), Séquence number, Authentification data, et ICV (integrity check value).

— l'en-tête ESP : a pour rôle d'assurer la confidentialité, l'intégrité et l'authentification des paquets IP. Il comprend des champs tels que Spi, Séquence number, Payload data, Padding, Pad length, et Next header.

Pour le mode transport, les en-têtes AH et ESP sont insérés entre l'en-tête IP et la charge utile du paquet IP d'origine. Dans l'environnement IPv6, ces en-têtes apparaissent après les extensions hop by hop, destination, routing et fragment.

Parfois, ESP et AH sont utilisées conjointement pour fournir à la fois le chiffrement et l'authentification/intégrité, offrant ainsi une sécurité complète pour les communications [46].

Comment IPsec fonctionne dans le contexte de l'IoT sous IPv6 :

— Authentification et intégrité : à l'aide de mécanismes de signature numérique, IPsec assure l'authentification et l'intégrité des paquets, ce qui signifie que les paquets proviennent d'une source légitime.

— Chiffrement : IPsec garantit que même si les paquets sont interceptés, leur contenu reste confidentiel et ne peut pas être déchiffré sans la clé appropriée.

— Modes de fonctionnement : avec le mode transport, IPsec protège seulement les données du paquet. Cependant, le mode tunnel crypte tout le paquet IP, y compris l'en-tête. Le mode tunnel est couramment utilisé pour les communications entre réseaux.

Le protocole SSL/TLS :

Défintion :SSL (Secure Socket Layer) et TLS (Transport Layer Security) sont des protocoles cryptographiques populaires utilisés pour sécuriser les communica-

tions Web.

Ils utilisent une paire de clés pour authentifier les identités et crypter les informations envoyées sur Internet.[22]

Le protocole TLS/DTLS :

Défintion :(Transport Layer Security) et DTLS (Datagram Transport Layer Security) sont des protocoles de sécurité utilisés pour chiffrer et sécuriser les communications sur Internet et d'autres réseaux, en assurant la confidentialité, l'intégrité et l'authenticité des données.[46]

Le protocole SASL :

Défintion :(Simple Authentication and Security Layer) est un framework d'authentification et de sécurité

SASL utilisé pour sécuriser les échanges d'informations entre des entités au sein d'un réseau IoT.[46]

Le protocole Thread :

Défintion :

est un protocole de communication sans fil optimisé pour l'IoT, caractérisé par sa faible consommation d'énergie, la sécurité intégrée et la prise en charge native d'IPv6. Il vise à fournir une solution robuste pour la connectivité des appareils intelligents dans les maisons intelligentes et d'autres applications IoT similaires. Il est basé sur des techniques éprouvées telles que 802.15.4, 6LoWPAN et UDP.[46]

Le modèle de communication :

Il existe deux types de communications :[45]

1. Communication publication/abonnement : où les utilisateurs peuvent s'abonner à un contenu précis.
2. Communication requête/réponse : Dans cette communication, un utilisateur peut acquérir des données avec des messages de requêtes personnalisés.

Finalement, le choix du protocole de sécurité dépend des besoins spécifiques de l'application IoT, de la topologie du réseau et des types de données en jeu. Chaque protocole a son rôle dans la sécurité de l'environnement contre les menaces potentielles. TLS et DTLS sont largement utilisés pour sécuriser les communications,

Radius et Kerberos pour l'authentification solide, Thread pour la gestion centralisée des clés. La sécurité ne dépend pas uniquement du protocole utilisé, mais aussi de la façon dont il est implémenté et configuré.

3.9.4 La notion de l'identité et identité partielle

Un attaquant ayant physiquement accès à un objet connecté est en mesure de recueillir beaucoup de ses informations sensibles. S'il réussissait par exemple à récupérer ses clés de chiffrement, il pourrait accéder à tout le trafic entrant et sortant de l'objet, et il pourrait aussi injecter du code malveillant destiné à d'autres objets du réseau. Chaque objet connecté apparaît ainsi comme un point critique dans l'architecture de l'IoT [49]

Les notions d'identité de sécurité qui devraient être garanties afin de sécuriser un objet connecté : [24]

L'identité :

Défintion : La notion d'identité présente une partie très importante dans la sécurité des objets connectés (IoT) fonctionnant sous IPv6, afin de garantir l'identité des objets connectés dans un environnement IoT sous IPv6 pour établir la confiance et maintenir la sécurité.

Pour créer un réseau IoT sécurisé et fiable, des mécanismes d'authentification solides, une gestion sécurisée des clés et des certificats auront lieu, ainsi que des politiques de contrôle d'accès basées sur l'identité, contribueront à créer. Les objets intelligents sont considérés comme des entités indépendantes, capables d'agir au nom d'un utilisateur.

Il existe plusieurs définitions dans la littérature, concernant principalement l'identité et l'identité partielle des objets intelligents. L'identité permet d'une part de distinguer les différents objets à l'intérieur du réseau, et d'autre part de vérifier leur origine. Dans toute architecture de gestion d'identité, l'établissement d'un environnement de confiance nécessite l'unicité des identités afin de pouvoir les authentifier. Les ressources contraintes des objets imposent cependant des extensions à la gestion traditionnelle d'identité [34]

Les aspects de l'identité à prendre en compte :

— **Authentification forte :** L'authentification forte se base sur la clé publique qui donne la possibilité de vérifier l'identité d'un objet et d'établir des connexions sécurisées et prouver son identité de manière fiable.

— **Attribut d'identité :** Dans le but de différencier les objets les uns des autres

et à éviter la falsification, les objets connectés doivent posséder des attributs d'identité uniques et fiables.

— **Gestion des clés :** Les dispositifs IoT utilisent des protocoles comme le protocole de gestion de clés IKEv2 (Internet Key Exchange version 2) pour gérer leurs clés de manière sécurisée.

— **Gestion des certificats :** La génération, la distribution, la révocation et la rotation appropriées des certificats utilisés pour l'authentification doivent être gérées de manière sécurisée.

— **Mise à jour sécurisée de l'identité :** Si des mises à jour de l'identité des objets connectés sont nécessaires, assurez-vous de les implémenter de manière sécurisée pour éviter les attaques de falsification ou de remplacement.

L'identité partielle :

Est créée, principalement pour des raisons d'anonymat, elle peut également être utilisée pour authentifier des objets. Une identité partielle contient un sous-ensemble d'attributs ou de données d'une identité globale ; ainsi le pseudonyme peut être considéré comme une identité partielle. Ces attributs peuvent être choisis soit par l'utilisateur, soit par le fournisseur d'identité. L'attribution d'une identité globale (ou l'identité en général) ou d'une identité partielle dépend de la situation et du contexte [24].

Le concept de l'identité partielle est venu pour minimiser la quantité d'informations personnelles ou d'attributs d'identité divulgués par un objet connecté lorsqu'il interagit avec d'autres dispositifs ou systèmes IoT qui communiquent entre eux ou avec des serveurs dans un environnement IPv6.

Et voici comment l'identité partielle pourrait être appliquée aux objets IoT sous IPv6 :

— **Échange minimal d'information :** Quand une communication entre deux dispositifs IoT a lieu, ils pourraient s'échanger uniquement les informations essentielles nécessaires à l'interaction en cours, sans avoir besoin de divulguer toutes les informations.

— **Chiffrement de données :** Les informations échangées doivent être incompréhensibles pour toute personne ou objet non autorisé. Pour cela, les objets IoT pourraient chiffrer les données échangées.

— **Minimisation de métadonnées :** Il faut minimiser les informations transmises pour éviter de révéler des informations supplémentaires qui pourraient être utilisées pour identifier les objets ou suivre leurs activités.

La sécurité des dispositifs IoT dans un environnement IPv6 est cruciale à cause

de la sensibilité des données échangées dans le réseau. IPv6 offre plusieurs avantages en termes de capacité d'adressage et de connectivité, mais d'autres défis de sécurité doivent être considérés pour assurer le bon comportement de l'environnement. Voici les points à considérer pour améliorer la sécurité :

— **Adressage IPv6 sécurisé :** IPv6 permet aux dispositifs d'être directement accessibles via l'internet. Il faut s'assurer que les dispositifs IoT utilisent des adresses IPv6 correctement configurées et évitent d'exposer des adresses inutilement.
— **Protection contre les attaques DDOS :** Avec l'espace d'adressage étendu offert par IPv6, les attaques par déni de service distribué (DDoS) peuvent devenir encore plus puissantes. Il est donc important de mettre en place des mécanismes de protection et de détection.
— **Chiffrement et authentification :** Pour chiffrer les données en transit et garantir l'authenticité des dispositifs communicants, il faut utiliser des protocoles tels que IPsec (Internet Protocol Security).
— **Gestion des adresses publiques :** Utilisez des pare-feux et des règles de filtrage pour contrôler l'accès aux dispositifs IoT qui utilisent des adresses IPv6 publiques.
— **Mise à jour sécurisée :** Il faut assurer que les dispositifs IoT peuvent avoir accès à des mises à jour sécurisées de manière irrégulière.
— **Sensibilisation à la sécurité :** Il faut éduquer les utilisateurs finaux, les administrateurs et les développeurs sur les bonnes pratiques de sécurité.
— **Tests de sécurité réguliers :** Des tests sont primordiaux pour identifier les vulnérabilités spécifiques à IPv6.

3.9.5 Systèmes de Sécurité dans IoT

L'outil SENTINEL

est un système permettant d'identifier dynamiquement les objets connectés présents et de sécuriser les communications.

Il utilise des mécanismes d'apprentissage pour classifier les différents objets, puis identifie leurs vulnérabilités. Il segmente ensuite le réseau local en définissant des classes, proposées en fonction du risque de compromission des objets, imposant des restrictions de communication en interne mais également vers l'extérieur[38].

Le concept de "Moving Target Defense" (MTD)

Défintion : MTD est une technologie qui vise à compliquer les attaques en modifiant constamment les caractéristiques du système ciblé.

Son idée est que le MTD crée un environnement informatique en constante évolution, ce qui rend plus difficile pour les attaquants de prévoir les vulnérabilités du système et de planifier des attaques efficaces[30].

L'architecture de Confiance nulle

est un mécanisme qui se base sur le principe que plutôt que de faire confiance aux dispositifs uniquement parce qu'ils sont dans le réseau, les architectures Zéro Confiance imposent des vérifications constantes et l'authentification, même pour les dispositifs internes. Cependant, si l'on déploie ce concept, il faut vérifier à chaque fois l'identité des dispositifs, ce qui peut introduire des problèmes au niveau des ressources et de la consommation d'énergie.[7]

L'utilisation de SVELTE

SVELTE est un IDS (système de détection d'intrusion) permettant de surveiller les échanges utilisant les protocoles IPv6 et 6LoWPAN, qui sont déployés dans le monde de l'IoT, permettant notamment d'accéder à l'objet depuis n'importe où sur Internet. La particularité et l'intérêt de cet outil résident notamment dans son faible coût, permettant de l'inclure dans les différents objets.[43]

3.10 Les services de sécurité dans un environnement IoT

La sécurité informatique vise généralement cinq principaux services [11] :

Intégrité

Vérifier l'intégrité des données consiste à déterminer si les données, ressources, traitements ou services n'ont pas été altérés durant la communication de manière fortuite ou intentionnelle.

Non répudiation

Elle consiste en l'assurance qu'une action sur la donnée réalisée au nom d'un utilisateur (après authentification) ne saurait être répudiée par ce dernier. À

l'instar de la confidentialité et de l'intégrité, la non-répudiation fait appel à des mécanismes de chiffrement.

Confidentialité

La confidentialité consiste à rendre l'information discrète ou inintelligible à d'autres personnes que les seuls acteurs de la transaction.

Disponibilité

La disponibilité garantit que les utilisateurs autorisés d'un système ont un accès rapide et ininterrompu aux informations contenues dans ce système, ainsi qu'au réseau. Il est important de déployer des protections contre les interruptions de tous les systèmes qui doivent fonctionner en continu. Les différentes options incluent la redondance matérielle, la bascule, les sauvegardes de routine dans un espace géographiquement séparé.

L'approche AAA

L'approche AAA vise à mettre en place un contrôle d'accès complet et solide dans le réseau IoT.

Authentification

L'authentification s'appuie sur la gestion d'identité d'un nœud qui est crucial. Quand un nœud rejoint un réseau, l'authentification est réalisée via un serveur d'authentification avec un protocole d'accès tel que PANA . Les dispositifs et les utilisateurs doivent prouver leur identité de manière fiable.

Autorisation

L'autorisation implique de définir des politiques de contrôle d'accès qui précisent quelles actions et quelles données un dispositif ou un utilisateur peut manipuler. Les mécanismes tels que DCAF (Delegated CoAP Authentication and Authorization Framework) ou OAUTH 2.0 vont permettre de contrôler l'accès des dispositifs aux ressources associées aux objets connectés [24].

Comptabilité (Accounting)

Afin de garder une trace des accès et des actions effectuées, et d'aider à identifier les comportements anormaux ou suspects, la comptabilité sert à surveiller les activités des utilisateurs.

3.11 Sécurité dans le Protocole RPL

Les protocoles de routages pour les réseaux filaires classiques (OSPF, IS-IS) et pour les réseaux ad-hoc (AODV, OSLR) ne conviennent pas aux spécifications de réseaux avec pertes et à faible puissance appelés réseaux LLN qui permettent à de nombreux équipements embarqués comme des sondes ou des capteurs de pouvoir communiquer entre eux dans un environnement IoT.

Donc, un protocole de routage appelé RPL a été spécialement conçu par l'IETF pour répondre aux contraintes spécifiques qu'impose ce type de réseaux. Néanmoins, ce protocole reste exposé à de nombreuses attaques de sécurité.

3.11.1 Description du protocole RPL

Défintion : Le protocole RPL est un protocole de routage à vecteur de distance utilisant IPv6, spécialement conçu par l'IETF pour répondre aux besoins des réseaux LLN. **Description :**

RPL consiste en un ou plusieurs DODAGs (Destination Oriented Directed Acyclic Graphs), c'est-à-dire des graphes acycliques orientés dirigés vers une destination qui est la racine du réseau. Ces graphes sont dirigés de façon à éviter les boucles parce que chaque nœud dans le DODAG a un rang (distance de la racine), et ce rang doit diminuer en remontant dans le graphe vers la racine. RPL assure la QoS dans la couche réseau à partir d'une fonction objectif qui permet d'optimiser la topologie en fonction d'une contrainte/métrique comme la préservation de l'énergie, le chemin le plus court ou la qualité des liens [40].

3.11.2 Identifiants RPL et procédure de construction de la Topologie DODAG

Défintion : Un DODAG est une structure de données en forme de graphe acyclique dirigé, où chaque nœud représente un dispositif ou un capteur du réseau, et les liens entre les nœuds indiquent la communication possible entre eux. La particularité d'un DODAG est qu'il est dirigé vers une destination spécifique, souvent appelée "racine" du DODAG. Le DODAG est généralement utilisé pour optimiser le routage des données vers cette destination.

Un réseau RPL est identifié par quatre champs :

— Fonction Objectif (OF) : définit comment les nœuds RPL sélectionnent et optimisent les itinéraires au sein d'une instance RPL.

— Rank (range) : c'est le rang d'un nœud définit la position individuelle du nœud

à d'autres nœuds à l'égard d'une racine DODAG. Le classement strictement augmente dans la direction vers le bas et diminue strictement vers le haut. La façon exacte de calculer le rang se dépend de la fonction objectif (OF).

— RPL Instance ID : Les DODAG ayant le même RPL Instance ID partagent la même fonction Objectif.

— Instance RPL : Une instance RPL est un ensemble d'un ou plusieurs DODAG qui partagent un RPL Instance ID.

Les messages de contrôle ICMPv6 qui sont responsables de la construction et de la maintenance des DODAGs :

1. DODAG Information Solicitation (DIS).
2. DODAG Information Object (DIO).
3. Destination Advertisement Object (DAO).

Quand un nœud veut rejoindre un réseau, il envoie un message DIS pour solliciter en réponse un message DIO qui contient des informations sur le DODAG comme le numéro de version et l'identifiant du DODAG, l'identifiant de l'instance et l'OF utilisée. (Un nœud peut également attendre de recevoir un message DIO diffusé périodiquement par ses voisins). Après avoir reçu un message DIO, le nœud calcule son rang en utilisant l'OF spécifiée. Le rang d'un nœud correspond à son emplacement dans le graphe par rapport à la racine. La valeur du rang augmente toujours en descendant dans le graphe. C'est donc la racine qui a le rang le plus petit dans le graphe.

Pour établir les routes descendantes, un nœud doit envoyer un message DAO à son parent contenant le préfixe des nœuds situés dans son sous-DODAG. Lorsque le message se propage vers la racine, les préfixes sont agrégés et les routes descendantes sont alors disponibles pour les parents [37].

3.11.3 Réparation d'anomalies

Dans les cas de la détection des boucles dans le graphe DODAG, le RPL applique une fonctionnalité appelée validation du chemin de données, dont il envoie des informations de contrôle transportées dans les paquets de données via des flags placés dans l'en-tête d'extension IPv6 Hop-By-Hop :

— Le flag 'O' indique la direction attendue du paquet, soit vers le haut si ce flag = 1, soit vers le bas si le flag 'O' = 0.

— Le flag 'R' indique si une erreur de rang a été détectée. Ce flag est mis à 1 lorsqu'un nœud observe une incohérence entre la direction supposée du paquet indiquée par le flag 'O' et le rang du nœud qui vient de le transférer. Le flag

'R' est utilisé pour réparer ce type d'anomalie appelée incohérence DODAG [37].

Mécanismes de réparation

On a deux mécanismes :

— Réparation locale : La réparation locale consiste à trouver un chemin alternatif pour router les paquets. Par exemple, lorsque la communication avec le parent préféré est rompue, un nœud peut choisir un autre parent pour transférer ses paquets.

— Réparation globale : Consiste à la reconstruction complète du graphe en incrémentant le numéro de version du DODAG.

3.11.4 Modes de sécurité

RPL prend en charge trois modes de sécurité [33] :

— Non sécurisé : Dans lequel les messages ICMPv6 de base comme DIS (Sollicitation d'informations DODAG), DIO (objet information DODAG), DAO (objet annonce DODAG) utilisés pour la configuration de la topologie ne portent pas de sections de sécurité, reposant sur les protocoles de couche inférieure pour sécuriser les cadres.

— Pré-installé : Pour garantir la confidentialité, l'intégrité et l'authenticité des messages, un nœud censé rejoindre le réseau possède une clé pré-installée.

— Authentifié : Qui s'apparente au mode précédent, il est basé sur la pré-installation d'une clé, étant uniquement autorisé à devenir un hôte. Pour être promu routeur, il doit obtenir une deuxième clé d'une autorité de clé, ce qui peut authentifier que le demandeur est autorisé à être un routeur avant de lui fournir la deuxième clé.

3.11.5 Catégories d'attaques de RPL

Je vais essayer d'établir une taxonomie des attaques de routage contre le protocole RPL comme illustré dans la Figure 3.5 [36] :

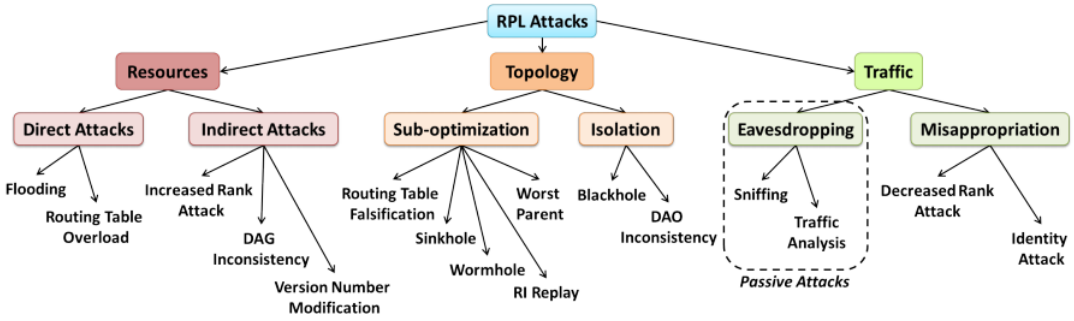

Figure 2: Taxonomy of attacks against RPL networks

FIGURE 3.5 – Taxonomie d'attaque sur les réseaux RPL [36].

Première catégorie

Ce type d'attaque concerne l'épuisement des ressources du réseau, ce qui signifie que le but du nœud malveillant est de surcharger la consommation d'énergie, de la mémoire et/ou de la puissance, ce qui impacte la disponibilité du nœud. Cette catégorie peut être subdivisée en deux sous-catégories :

— Attaques directes : dans lesquelles le nœud malveillant génère directement la surcharge perturbant le réseau.

— Attaques indirectes : dans lesquelles le nœud malveillant provoque les autres nœuds pour leur faire générer de la surcharge.

Deuxième catégorie

Regroupe les attaques visant la topologie DODAG du réseau RPL. Le but de ces attaques est de perturber le fonctionnement normal du réseau, alors elles visent à provoquer l'isolement d'un ou de plusieurs nœuds du DODAG. Cette catégorie peut également être subdivisée en deux sous-catégories :

— La sous-optimisation : qui signifie que le réseau convergera vers une forme non optimale, induisant de mauvaises performances.

— L'isolation : d'un nœud ou d'un sous-ensemble de nœuds, les coupant du reste du réseau.

Troisième catégorie

Couvre les attaques contre le trafic du réseau. Ces attaques visent à faire en sorte qu'un nœud malveillant s'introduise à l'intérieur du réseau, sans faire aucun changement dans le fonctionnement de ce dernier, ce qui va entraîner une fuite d'informations en écoutant le trafic ou en se faisant passer pour des nœuds

légitimes. Cette catégorie se subdivise à nouveau en deux sous-catégories :
— L'écoute (passive) : des informations qui sont transmises par le réseau.
— Le détournement : d'un nœud ou d'un ensemble de nœuds, notamment pour altérer les informations légitimes échangées.

3.11.6 Exemples d'attaques de routage

On peut définir plusieurs exemples d'attaques de chaque catégorie définie ci-dessous selon [36] :

Identity Attack

Cette attaque se produit typiquement lorsque un nœud malveillant se prétend être un nœud légitime. Dans les réseaux RPL, le nœud racine joue un rôle primordial dans la construction du graphe DODAG. Cela signifie qu'elle construit toute la topologie en envoyant des messages de routage. Un attaquant, lorsqu'il s'identifie comme un nœud racine, peut avoir le contrôle sur toute la topologie.

Flooding Attack

Ce type d'attaque consiste à générer une grande quantité de trafic dans le réseau jusqu'à ce que les nœuds ne soient plus disponibles, c'est-à-dire submerger la bande passante du réseau. Plus spécifiquement, le protocole de routage nécessite que les nœuds voisins d'un même réseau échangent des messages HELLO pour indiquer leur présence et leur disponibilité, découvrir des routes et mettre à jour les tables de routage. Le nœud malveillant envoie un nombre énorme de paquets HELLO à différents nœuds pour se présenter comme voisin, afin qu'ils lui transmettent leurs données.

Version Number Attack

Le but de ces types d'attaques est d'augmenter le champ du numéro de version à l'intérieur des messages DIO et de les transmettre à ses voisins. En conséquence, une nouvelle construction DODAG est forcée, ce qui cause la perte de paquets de données, l'encombrement du réseau et l'épuisement des ressources des nœuds en raison de la surcharge du message de contrôle.

Wormhole Attack

Les attaques de type wormhole reposent sur l'utilisation de deux nœuds RPL malveillants (A et B) dans la topologie DODAG interconnectée via un réseau privé.

La figure ci-dessous explique un exemple de scénario :

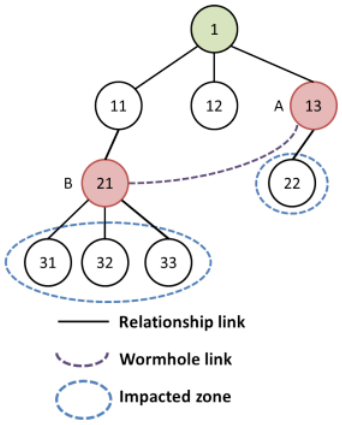

FIGURE 3.6 – Wormhole Attack [36].

Dans cet exemple, tout paquet reçu par le nœud 13 sera transféré vers le nœud 21 à travers le wormhole link. Le nœud 21 peut fonctionner de la même manière que le nœud 13. Ce type d'attaque déforme le routage dans les réseaux RPL, dans lesquels si l'attaquant peut transférer les informations de routage vers une autre partie du réseau, alors des nœuds qui sont distants estimeront être proches, ce qui causera une création non optimisée.[36]

Worst Parent Attack

Ce type d'attaque consiste à choisir systématiquement le père le plus mauvais dans la topologie DODAG selon la fonction objectif. Son objectif est que le routage des nœuds finaux ne soit pas optimisé, ce qui causera une mauvaise performance.

Blackhole Attack

Ce type d'attaque est très dangereux car il consiste à arrêter la transformation totale des paquets supposés être transférés. Si l'attaquant est situé dans une position critique dans la topologie, il peut isoler de nombreux nœuds.

c

Decreased Rank Attack

Dans la topologie DODAG, la racine a le rang le plus bas. La racine a la capacité de gérer le plus grand nombre de nœuds. Ce type d'attaque consiste à faire de la publicité pour un rang inférieur afin que les nœuds légitimes se connectent au DODAG via l'attaquant. Cela peut bien sûr servir de base à des attaques de type "blackhole".

3.11.7 Gestion de Risques

La gestion de risques permet d'identifier, évaluer et traiter les risques auxquels sont confrontés les réseaux et les systèmes d'information. On peut aussi le définir comme donné dans l'équation suivante :

$$\mathcal{R} = \sum_{a \in A} P(a) \times E(a) \times C(a)$$

Prenons une attaque, notée a. Le risque total du réseau se définit comme la somme sur toutes les attaques possibles de chaque niveau de risque. Le niveau de risque $R(a)$ dépend de la potentialité $P(a)$ de l'attaque, de l'exposition $E(a)$ du réseau RPL et des conséquences $C(a)$ de l'attaque sur le réseau si elle réussit. La gestion de risques consiste à surveiller, hiérarchiser et contrôler les risques. Par exemple, si on observe une forte potentialité $P(a)$, c'est-à-dire une attaque en cours, on peut activer un mécanisme de sécurité en prenant en compte son coût afin de réduire l'exposition $E(a)$ et maintenir le niveau de risque $R(a)$ à une valeur raisonnable [37].

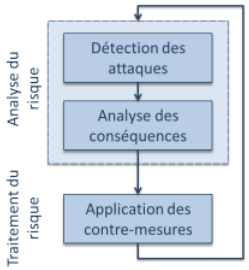

FIGURE 3.8 – Schématisation du processus de gestion de risques.[37]

L'analyse du risque se définit comme la quantification de la potentialité de l'attaque ainsi que ses conséquences. Le traitement du risque consiste, quant à lui, en la sélection et l'application des mécanismes de sécurité requis afin de réduire le niveau de risque à une valeur acceptable comme illustré dans la Figure 3.8.

3.12 Proposition d'utilisation de la technologie blockchain pour renforcer la sécurité dans le protocole RPL

3.12.1 La technologie blockchain

Fondamentalement, la blockchain est une liste croissante des enregistrements (appelés blocs) qui sont connectés les uns aux autres à l'aide de la cryptographie. En d'autres

termes, une blockchain est un ensemble partagé, décentralisé, un registre de base de données immuable qui stocke des séries d'enregistrements de données horodatées et de transaction dans une série de blocs connectés par hachage. Noter que la blockchain est basée sur une topologie peer-to-peer (P2P) et gérée par des participants identifiés par une paire de clés (clé privée-clé publique) dans le réseau. Les nouveaux enregistrements de données (blocs) sont ajoutés à la blockchain via un processus appelé exploitation minière. Une fois que les données de transaction sont enregistrées dans un bloc, elles ne peuvent pas être altérées sans modification de tous les blocs précédents [28].

3.12.2 Mécanismes de consensus

Un mécanisme de consensus est utilisé dans les nœuds du réseau RPL pour enregistrer des informations cruciales liées à la sécurité, telles que les clés de chiffrement, les routes de routage et les transactions de sécurité à la blockchain. Un mécanisme de consensus peut être adapté pour satisfaire les contraintes des nœuds à faible consommation d'énergie du réseau RPL en évitant des mécanismes de consensus énergivores tels que la preuve de travail (PoW) utilisée dans Bitcoin, et en utilisant des alternatives légères comme la preuve d'enjeu (PoS) ou des variantes adaptées aux réseaux IoT. [41]

Proof-of-Stake (PoS)

Le PoS est un algorithme de consensus distribué conçu pour lutter contre les faiblesses de PoW. Le PoS ne nécessite pas beaucoup de puissance de calcul ni de consommation d'énergie massive ou de matériel informatique puissant. Les blockchains PoS sont économes en énergie et sont notamment utilisées dans le cadre des crypto-monnaies [35].

3.12.3 Le rôle du blockchain dans la sécurité de réseau RPL

L'utilisation de la technologie blockchain pour renforcer la sécurité dans le protocole RPL implique la création d'un registre décentralisé, immuable et sécurisé qui enregistre les transactions et les événements liés à la sécurité dans le réseau.

La blockchain peut être utilisée pour :

1. Validation de route de routage : Le protocole RPL est utilisé pour établir des routes de routage entre les nœuds d'un réseau IoT à faible consommation d'énergie LLN. La sécurité des routes de routage est cruciale. Pour garantir la sécurité, à chaque fois qu'une nouvelle route de routage est établie entre les nœuds, elle peut être enregistrée de manière sécurisée sur la blockchain. Les nœuds du réseau peuvent consulter la blockchain pour vérifier la validité des routes qu'ils utilisent en comparant les informations enregistrées sur la blockchain avec les informations de routage actuelles.

2. Création d'identité numérique : Chaque nœud dans la topologie DODAG peut avoir une identité numérique qui sera enregistrée dans la blockchain. Cela signifie que l'ensemble du réseau aurait accès à une liste vérifiable d'identités de nœuds. Cela permettrait de vérifier l'authenticité des nœuds lorsqu'ils rejoignent le réseau, renforçant ainsi la sécurité et protégeant contre l'usurpation d'identité.
3. Enregistrement des clés de chiffrement : Les clés de chiffrement peuvent être usurpées pendant leur distribution aux nœuds. Pour résoudre ce problème, on peut utiliser la blockchain pour stocker de manière sécurisée les clés de chiffrement nécessaires. Quand un nœud souhaite établir une communication sécurisée avec un autre nœud, il peut demander l'accès en présentant son identité numérique.
4. Révocation de clés compromises : Lorsqu'un nœud est compromis, ses clés de chiffrement peuvent être utilisées à des fins malveillantes. Pour répondre à cette menace, le réseau doit être capable de révoquer les clés de chiffrement. Une révocation de ses clés peut être générée et enregistrée sur la blockchain. Les autres nœuds peuvent alors vérifier la blockchain avant d'accepter des communications ou des transactions provenant du nœud compromis.
5. Vérification de l'intégrité des données : Les nœuds du DODAG peuvent assurer l'intégrité des données en comparant les données qu'ils reçoivent avec les enregistrements de la blockchain. Si les données ont été altérées en transit, cette altération peut être détectée. À chaque saut, le message peut être validé en utilisant la blockchain. Les nœuds peuvent vérifier si le message a été modifié ou altéré en comparant le contenu du message avec une empreinte ou une signature enregistrée sur la blockchain. Les nœuds peuvent également utiliser des clés de chiffrement enregistrées sur la blockchain pour chiffrer et déchiffrer les données à chaque saut.

Dans un réseau RPL, les données sont souvent transmises d'un nœud à un autre à travers plusieurs sauts, ce qui crée des opportunités pour des attaques. À chaque saut, le message peut être validé en utilisant la blockchain. Les nœuds peuvent vérifier si le message a été modifié ou altéré en comparant le contenu du message avec une empreinte ou une signature enregistrée sur la blockchain. Les nœuds peuvent également utiliser des clés de chiffrement enregistrées sur la blockchain pour chiffrer et déchiffrer les données à chaque saut.

Conclusion

la sécurité dans les environnements IoT est une préoccupation croissante en raison de l'utilisation rapide de ces systèmes dans notre vie quotidienne.Le protocole RPL (Routing

Protocol for Low-Power and Lossy Networks) joue un rôle crucial en tant que protocole de routage au sein de ces réseaux, mais il présente des vulnérabilités potentielles qui nécessitent une attention particulière.

Conclusion générale

la transition vers IPv6 est inévitable et incontournable,et la securité dans environnement ipv6 est complexe donc on doit nous preparer pour collaborer et mettre en œuvre des stratégies de sécurité robustes dans cet environnement et développer des contre-mesures efficaces, notamment dans le contexte en évolution rapide de l'IoT.

Au fil de ce mémoire, nous avons plongé au cœur d'IPv6, un protocole de communication réseau révolutionnaire. Dans cette exploration approfondie, nous avons parcouru un voyage à travers les caractéristiques fondamentales d'IPv6, ces éléments clés ,et ses mécanismes de configuration à la diversité des adresses IPv6. Ces informations ont une importance cruciale dans un monde de plus en plus connecté, où IPv6 se dresse comme un acteur incontournable pour répondre aux besoins croissants en adresses, en sécurité et en efficacité des réseaux.

De plus, nous avons abordé diverses vulnérabilités et deffirents attaques courantes qui ciblent les réseaux IPv6. Ces dernier peuvent potentiellement compromettre la disponibilité, l'intégrité et la confidentialité des réseaux.et on a vue l'importance cruciale de la sécurité dans l'environnement IPv6. il est essentiel de comprendre les vulnérabilités potentielles et les attaques qui peuvent survenir par ce que ce protocole représente l'avenir des réseaux.

nous avons plongé dans le monde en constante expansion de l'IoT, où les objets connectés interagissent de manière transparente avec notre vie quotidienne. Le protocole RPL, en tant que pilier fondamental des réseaux IoT à faible consommation d'énergie, est essential dans la connectivité et la communication de ces dispositifs. mais Les vulnérabilités potentielles du protocole RPL nécessitent une attention particulière pour prévenir les failles de sécurité

En somme, ce mémoire nous a permis de plonger dans le monde d'IPv6, de comprendre ses avantages et ces dafauts, tout en maitant attention a l'importance vitale de la sécurité pour garantir le succès continu de ce protocole. il est impératif de rester vigilant face aux défis de sécurité qui se présentent.

Bibliographie

[1] *:https ://www.google.com/search ?sca$_e$sv = 564185751rlz = 1C1SQJL$_f$rDZ952DZ952sxsrf = AB5stBiMR1155TmEMGcHr0imqdPC4WVWTQ : 1694370356622q = ipv6 + adresse + abr*

[2] *https ://formip.com/unicast-ipv6-eui64/ : acceder 20/02/2023* (acceder 20/02/2023).

[3] *https ://cisco.goffinet.org/ccna/ipv6/adresses-ipv6-unicast/* (acceder 20/08/2023).

[4] *https ://www.mokolora.com/fr/what-is-lora-iot/* (acceder 20/08/2023).

[5] *https ://cisco.goffinet.org/ccna/ipv6/adresses-ipv6-multicast/* (acceder 20/08/2023).

[6] *https ://www.crowdstrike.fr/cybersecurity-101/denial-of-service-dos-attacks/* (acceder 20/08/2023).

[7] *https ://www.microsoft.com/fr-ca/security/business/security-101* (acceder 20/08/2023).

[8] *:https ://docs.oracle.com/cd/E19957-01/820-2982/ipv6-ref-2/index.html* (acceder 2/08/2023).

[9] *https ://www.ionos.fr/digitalguide/serveur/know-how/quest-ce-que-le-neighbor-discovery-protocol-ndp/* (acceder le 20/08/2023).

[10] *https ://www.futura-sciences.com/tech/definitions/internet-deni-service-2433/* (accéder le 08/2023).

[11] Abbassi, Y., and Benlahmer, H. Un aperçu sur la sécurité de l'internet des objets (iot). In *Colloque sur les Objets et systèmes Connectés-COC'2021* (2021).

[12] Al-Ani, A., Al-Ani, A. K., Laghari, S. A., Manickam, S., Lai, K. W., and Hasikin, K. Ndpsec : Neighbor discovery protocol security mechanism. *IEEE Access 10* (2022), 83650–83663.

[13] Alin, G., and Nurlybayev, T. Ccna7 cisco networking course : Practical assignment. *Southeast Europe Journal of Soft Computing 10*, 1 (2021), 49–54.

[14] Augustin, A., Yi, J., Clausen, T., and Townsley, W. M. A study of lora : Long range & low power networks for the internet of things. *Sensors 16*, 9 (2016), 1466.

[15] Brzozowski, J., Cable, C., and Zeng, S. Leasequery pour dhcpv6.

[16] Challal, Y. *Sécurité de l'Internet des Objets : vers une approche cognitive et systémique*. PhD thesis, Université de Technologie de Compiègne, 2012.

[17] Challoo, R., Oladeinde, A., Yilmazer, N., Ozcelik, S., and Challoo, L. An overview and assessment of wireless technologies and co-existence of zigbee, bluetooth and wi-fi devices. *Procedia Computer Science 12* (2012), 386–391.

[18] Chen, Y., and Kunz, T. Performance evaluation of iot protocols under a constrained wireless access network. In *2016 International Conference on Selected Topics in Mobile & Wireless Networking (MoWNeT)* (2016), IEEE, pp. 1–7.

[19] Cheneau, T., and Combes, J.-M. Une attaque par rejeu sur le protocole send. In *SAR-SSI'08 : 3e Conférence sur la Sécurité des Architectures Réseaux et des Systèmes d'Information* (2008), pp. 289–300.

[20] Dawood, H. Ipv6 security vulnerabilities. *International Journal of Information Security Science 1*, 4 (2012), 100–105.

[21] Deering, S., and Hinden, R. Internet protocol, version 6 (ipv6) specification. Tech. rep., 2017.

[22] D'Orazio, C. J., and Choo, K.-K. R. A technique to circumvent ssl/tls validations on ios devices. *Future Generation Computer Systems 74* (2017), 366–374.

[23] E. Vasilomanolakis, J. Daubert, M. L. V. G. A. W. e. P. K. *On the Security and Privacy of Internet of Things Architectures and Systems »,*. PhD thesis, International Workshop on Secure Internet of Things, Vienna, Austria, 2015.

[24] El Jaouhari, S., Bouabdallah, A., and Bonnin, J.-M. La sécurité des objects connectés. *MISC : multi-system & internet security cookbook*, 88 (2016), 54–59.

[25] Enterprise, H. P. Internet of things research study : 2015 report. *Online : http ://www8. hp. com/h20195 2* (2015).

[26] Fagroud, F. Z., Elfilali, S., Toumi, H., et al. Iot et cloud computing : état de l'art. In *Colloque sur les Objets et systèmes Connectés* (2019).

[27] Farooq, M. U., Waseem, M., Mazhar, S., Khairi, A., and Kamal, T. A review on internet of things (iot). *International journal of computer applications 113*, 1 (2015), 1–7.

[28] Firouzi, F., Chakrabarty, K., and Nassif, S. *Intelligent internet of things : From device to fog and cloud*. Springer, 2020.

[29] Gont, F., Cooper, A., Thaler, D., and Liu, W. Deprecating eui-64 based ipv6 addresses. *draft-gont-6man-deprecate-eui64-based-addresses-00, Internet Engineering Task Force* (2013).

[30] Jajodia, S., Ghosh, A. K., Subrahmanian, V., Swarup, V., Wang, C., and Wang, X. S. *Moving Target Defense II : Application of Game Theory and Adversarial Modeling*, vol. 100. Springer, 2012.

[31] Jakobsson, M., and Wetzel, S. Security weaknesses in bluetooth. In *Cryptographers' Track at the RSA Conference* (2001), Springer, pp. 176–191.

[32] jaun paul ARCHIER. *ipv6 principes et mise en œuvre*. ENI, 2012.

[33] Kim, H.-S., Ko, J., Culler, D. E., and Paek, J. Challenging the ipv6 routing protocol for low-power and lossy networks (rpl) : A survey. *IEEE Communications Surveys & Tutorials 19*, 4 (2017), 2502–2525.

[34] Luecking, M., Fries, C., Lamberti, R., and Stork, W. Decentralized identity and trust management framework for internet of things. In *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (2020), IEEE, pp. 1–9.

[35] Lutta, P., Sedky, M., Hassan, M., Jayawickrama, U., and Bastaki, B. B. The complexity of internet of things forensics : A state-of-the-art review. *Forensic Science International : Digital Investigation 38* (2021), 301210.

[36] Mayzaud, A., Badonnel, R., and Chrisment, I. A taxonomy of attacks in rpl-based internet of things. *International Journal of Network Security 18*, 3 (2016), 459–473.

[37] Mayzaud, A., Sehgal, A., Badonnel, R., and Chrisment, I. Gestion de risques appliquée aux réseaux rpl. In *9ème Conférence sur la Sécurité des Architectures Réseaux et des Systèmes d'Information* (2014).

[38] Miettinen, M., Marchal, S., Hafeez, I., Asokan, N., Sadeghi, A.-R., and Tarkoma, S. Iot sentinel : Automated device-type identification for security enforcement in iot. In *2017 IEEE 37th international conference on distributed computing systems (ICDCS)* (2017), IEEE, pp. 2177–2184.

[39] Najjar, F., Bsoul, Q., and Al-Refai, H. An analysis of neighbor discovery protocol attacks. *Computers 12*, 6 (2023), 125.

[40] Nassar, J., Gouvy, N., and Mitton, N. Fonction objectif pour un rpl adapté aux smart grids. In *ALGOTEL 2017-19èmes Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications* (2017), p. 4.

[41] Petit, J. *Surcoût de l'authentification et du consensus dans la sécurité des réseaux sans fil véhiculaires*. PhD thesis, Université Paul Sabatier-Toulouse III, 2011.

[42] Racherla, S., Daniel, J., et al. *IPv6 Introduction and Configuration.* IBM Redbooks, 2012.

[43] Raza, S., Wallgren, L., and Voigt, T. Svelte : Real-time intrusion detection in the internet of things. *Ad hoc networks 11*, 8 (2013), 2661–2674.

[44] Ryan, M. Bluetooth : With low energy comes low security. In *7th USENIX Workshop on Offensive Technologies (WOOT 13)* (2013).

[45] Saadaoui, F. Z., Maizate, A., and Ouzzif, M. État d'art sur les protocoles en temps réel pour l'internet des objets sous le réseau ndn. In *Colloque sur les Objets et systèmes Connectés* (2019).

[46] Saxena, S., and Pradhan, A. K. *Internet of Things : Security and Privacy in Cyberspace.* Springer Nature, 2022.

[47] Sethi, P., Sarangi, S. R., et al. Internet of things : architectures, protocols, and applications. *Journal of electrical and computer engineering 2017* (2017).

[48] Shemaili, M. B., Yeun, C. Y., Mubarak, K., and Zemerly, M. J. A new lightweight hybrid cryptographic algorithm for the internet of things. In *2012 International Conference for Internet Technology and Secured Transactions* (2012), IEEE, pp. 87–92.

[49] Skarmeta, A., Hernández-Ramos, J. L., and Bernabe, J. B. A required security and privacy framework for smart objects. In *2015 ITU Kaleidoscope : Trust in the Information Society (K-2015)* (2015), IEEE, pp. 1–7.

[50] Ullrich, J., Krombholz, K., Hobel, H., Dabrowski, A., and Weippl, E. {IPv6} security : Attacks and countermeasures in a nutshell. In *8th USENIX Workshop on Offensive Technologies (WOOT 14)* (2014).

Résumé

FRANCAIS

les caractéristiques fondamentales d'IPv6, y compris son extension d'espace d'adressage, ses mécanismes d'auto-configuration, sa compatibilité avec IPv4, sa syntaxe d'adresse, ses en-têtes et types d'adresses,joue un rôle crucial dans la connectivité du monde numérique en évolution constante.

les enjeux de sécurité liés à IPv6 sont très nombreux a cause des ces foncttionalité unique donc il faut prendre les mesures nécessaires pour protéger les réseaux contre les menaces potentielles.

Internet des objet est une technologie révolutionnaire ;mais préoccupations et les vulnérabilités liées à cette technologie sont énorme il est essentiel de mettre en place des mesures de sécurité adéquates pour protéger les appareils IoT et les réseaux qui les connectent. Le protocole RPL est un outil précieux pour la communication dans l'IoT, mais il nécessite également une attention particulière en matière de sécurité pour éviter les failles potentielles./ **mots clé : IPv6 ;RPL ;internet des objets ;menaces,attaque.**

ENGLISH

The fundamental characteristics of IPv6, including its expanded address space, auto-configuration mechanisms, compatibility with IPv4, address syntax, headers, and address types, play a crucial role in the connectivity of the constantly evolving digital world.

The security challenges related to IPv6 are numerous due to its unique features, so it is necessary to take the necessary measures to protect networks against potential threats.

The Internet of Things is a revolutionary technology, but concerns and vulnerabilities associated with this technology are substantial. It is essential to implement adequate security measures to protect IoT devices and the networks that connect them. The RPL protocol is a valuable tool for communication in IoT, but it also requires special attention to security to avoid potential vulnerabilities./ **keywords : IPv6 ;RPL ;internet des objets ;menaces,attaque :**