الجمهورية الجزائرية الديمقراطية الشعبية

République Algérienne Démocratique et Populaire

وزارة التعليم العالي والبحث العلمي

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Nº Réf :……

Centre Universitaire
Abdelhafid Boussouf Mila

Institut des Sciences et Technologie **Département de Mathématiques et Informatique**

Mémoire préparé en vue de l'obtention du diplôme de Master

En : Informatique

Spécialité : Sciences et Technologies de l'Information et de la Communication (STIC)

Thème

A solution for managing firewalls in the Internet Of Things

Préparé par : Boulmis Bilal
Lakhal Dounia

Soutenue devant le jury

- **Guettiche Mourad (MCA)**	**C.U.Abdelhafid Boussouf**	**Président**
- **Lalouci Ali (MCA)**	**C.U.Abdelhafid Boussouf**	**Encadreur**
- **Attia Mourad (MAA)**	**C.U.Abdelhafid Boussouf**	**Examinateur**

Année Universitaire : 2020/2021

Remerciement

Avant tout nous remercions "Allah", qui nous a aidés à accomplir ce travail.

Nous adressons nos remerciements à notre encadreur consultant ***Mr.Lalouci Ali*** *et spécial remerciement pour* ***Mr.guettiche mourade*** *qui nous avoir guidés tout au long de ce travail, pour leur compréhension, leur patience, leur compétence, et ses remarques qui nous ont été précieuses.*

Nos chaleureux remerciements aux tout les enseignants du centre universitaire « Abd Elhafid Boussouf -MILA » nous sommes honorés d'étudier et apprendre d'eux.

Dédicaces

A ma mère et mon très cher père paix a son âme, pour leur affection et leur patience qui m'a soutenu et m'encourager, pendant tous les jours de ma vie.

A mon frère ***youcef*** *et mes sœurs* ***chahinez & meriem***

A mes amis ***Amira & zakariya et soumia***

A mes ***collègues de travail*** *qui m'ont beaucoup aidé*

Dounia

Dédicaces

شكرا لوالديَّ الذين تعبوا من أجلي وشكرا لكل من ساعدنا على إتمام هذا العمل من قريب أو من بعيد

فالحمد أولا وآخرا

Bilal Boulmis

Résumé :

La technologie de l'internet des objets apparait et émerge ces dernières années. Elle se caractérise par un nombre gigantesque d'objets mobile et hétérogène connectés, ce qui nécessite des mécanismes efficaces pour les superviser et assurer leur sécurité. Le firewall est l'une des techniques les plus utilisées pour atteindre ces objectifs.

Un firewall est un mécanisme permettant de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types de communications autorisés. Il surveille et contrôle les applications et les flux de données. Cependant, l'installation et la maintenance de ces dernies nécessite un cout très élevé.

L'objectif de ce projet est de maitre en place une solution efficace permettant de réduire le cout d'installation des firewalls dans le système, d'équilibrer les charges entre les différents firewalls installés, et d'assurer le contrôle de flux de donné dans le système.

Tout, en respectant certaines propriétés inhérentes telles que la mobilité et l'hétérogénéité. Notre objectif également est d'avoir une stratégie tolérante aux fautes qui permet d'assurer le bon fonctionnement du système même si certain nombre de firewall tombe en panne.

ABSTRACT

Internet of Things technology is emerging and emerging in recent years. It is characterized by a gigantic number of mobile and heterogeneous objects connected, which requires effective mechanisms to supervise them and ensure their security. The firewall is one of the techniques most used to achieve these goals.

A firewall is a mechanism making it possible to enforce the network security policy, which defines what types of communications are authorized. It monitors and controls applications and data flows. However, the installation and maintenance of these requires a very high cost.

The objective of this project is to master an effective solution allowing to reduce the cost of installing firewalls in the system, to balance the loads between the different firewalls installed, and to ensure the control of data flow in the system. the system.

All while respecting certain inherent properties such as mobility and heterogeneity. Our goal is also to have a fault tolerant strategy that allows the system to function properly even if a number of firewalls fail.

الملخص

تقنية إنترنت الأشياء آخذة الظهور في السنوات الأخيرة. وتتميز بعدد هائل من الأجسام المتحركة وغير المتجانسة المتصلة ، الأمر الذي يتطلب آليات فعالة للإشراف عليها وضمان أمنها. يعد جدار الحماية أحد الأساليب الأكثر استخدامًا لتحقيق هذه الأهداف.

جدار الحماية عبارة عن آلية تتيح فرض سياسة أمان الشبكة ، والتي تحدد أنواع الاتصالات المسموح بها. يراقب ويتحكم في التطبيقات وتدفقات البيانات. ومع ذلك ، فإن تركيبها وصيانتها يتطلب تكلفة عالية للغاية.

الهدف من هذا المشروع هو إتقان حل فعال يسمح بتقليل تكلفة تثبيت جدران الحماية في النظام ، وموازنة بين مختلف جدران الحماية المثبتة ، ولضمان التحكم في تدفق البيانات في النظام.

كل ذلك مع احترام بعض الخصائص مثل التنقل وعدم التجانس. هدفنا أيضًا هو أن يكون لدينا إستراتيجية للتعامل مع الأخطاء تسمح للنظام بالعمل بشكل صحيح حتى في حالة فشل عدد من جدران الحماية.

TABLE DES MATIÈRES

TABLE DES FIGURES

Liste des abréviations

SMTP Simple Mail Transfer Protocol

HTTP Hypertext Transfer Protocol

RFID Radio Frequency Identification

IBM International Business Machines

CIOs Congress of Industrial Organizations

BLE Bluetooth Low Energy

GSM Global Systems for Mobile

M2OCITY Operateur Telérelevé

GRDF Gaz Réseau Distribution France

OSI Open Systems Interconnexion

ACL Access Control List

TCP Transfer Control Protocol

DOS Denial of Service

UDP User Datagram Protocol

ICMP Internet Control Message Protocol

ARP Address Resolution Protocol

MAC Media Access Control

RSA Rivest–Shamir–Adleman

NAT Translation Address Réseau

WPA2 Wi-Fi Protected Access 2

SNPH Strongly NP-Hard

INTRODUCTION GÉNÉRALE

Context :

L'Internet des objets est une extension du monde numérique d'Internet pour inclure des objets Le monde physique, c'est la numérisation et l'interconnexion des choses pour améliorer la base Décisions de gestion, agir à distance, automatiser et faciliter les opérations en général la vie des hommes.
Les appareils IoT génèrent des modèles de comportement de réseau uniques et identifiables. À l'aide de l'apprentissage automatique et de l'IA, IoT Security reconnaît ces comportements et identifie chaque appareil sur le réseau, créant ainsi un inventaire riche et contextuel, maintenu dynamiquement et toujours à jour.
L'Internet des objets (IoT) permet une connectivité mondiale aux appareils intelligents distants. Cette technologie implique la détection, la communication et le traitement des données en temps réel reçues de milliards d'appareils connectés avec une intervention humaine minimale. L'exposition à Internet et les contraintes des appareils IoT, une mémoire généralement limitée, une faible capacité de traitement et des opérations principalement basées sur la batterie les rendent vulnérables à diverses attaques.
Les modèles de sécurités traditionnels pour les applications Internet n'est pas adapté à l'IoT, car il n'est généralement pas en temps réel. Par conséquent, il est important d'avoir des solutions alternatives qui offrent une sécurité significative aux appareils/applications IoT.
La théorie des graphes a connu un regain d'intérêt pour la modélisation de nombreux problèmes en informatique. En effet, un graphe peut modéliser un programme, un algorithme, mais aussi divers types de réseaux. Par exemple, le réseau internet peut être modélisé par un graphe dont les sommets représentent des routeurs ou des ordinateurs, et les arêtes entre deux sommets un lien de communication par exemple (fibre optique), trouver la solution optimale est un problème $NP - complet$.
Nous proposons une nouvelle architecture de sécurité des firewalls adaptée aux applications IoT. elle est basée sur la théorie des graphes et spécialement l'algorithme dominant, l'idée est de trouver une solution efficace permettant de réduire le cout d'installation des firewalls dans le système, d'équilibrer les charges entre les firewalls installés ,et d'assurer le contrôle de flux de donné dans le système et ainsi de donner une stratégies tolérantes aux fautes qui permet d'assurer le bon fonctionnement du système même si certain nombre de firewall tombe en panne.

Problématique :

Est comment minimiser le nombre des firewalls et le cout d'installation des firewalls dans un réseau IoT et protéger le réseaux au même temps ?

Objectif :

Dans notre projet nous avons développé un algorithme qui permet de réduire le nombre des firewalls tout en conservant de la sécurité de notre réseau IoT.

Organisation du mémoire :

Ce mémoire est organisé en trois chapitres comme suit :

- **Le premier chapitre :**Dans ce chapitre, nous présentons les principaux concepts et définitions de l'Internet of Things (IoT) et comment sécurisé ces différents objets en utilisant l'une des solutions existante « les firewalls».

- **Le deuxième chapitre :** Ce chapitre sera décomposé en deux parties, la première nous présentons les principaux concepts de La théorie des graphes et des concepts généraux sur les réseaux.

- **Le troisième chapitre :** Dans ce chapitre, nous présentons les principaux concepts et définitions du smart city.
- **Quatrième chapitre :**Dans ce chapitre, nous allons présenter la partie de la simulation et la partie de la modélisation .

CHAPITRE 1

L'INTERNET DES OBJETS ET LES FIREWALLS

1.1 Introduction

L'Internet des Objets ou en anglais the Internet of Things (IoT) représente aujourd'hui une partie majeure de notre vie quotidienne. Des milliards d'objets intelligents et autonomes, à travers le monde sont connectés et communiquent entre eux.
Ce paradigme révolutionnaire crée une nouvelle dimension qui enlève les frontières entre le monde réel et le monde virtuel. Son succès est dû à l'évolution des équipements matériels et des technologies de communication notamment sans fil.
Les réseaux de capteurs sans fil représentent une pièce maîtresse du succès de l'IoT. Car en utilisant des petits objets qui sont généralement limités en terme de capacité de calcul, de mémorisation et en énergie, des environnements industriels, médicaux, agricoles, et autres peuvent être couverts et gérés automatiquement.
La grande puissance de l'IoT repose sur le fait que ses objets communiquent, analysent, traitent et gèrent des données d'une manière autonome et sans aucune intervention humaine [1].
Les appareils IoT à proprement parler ne sont pas les uniques sources de préoccupation. En effet, connectés à l'Internet des objets, les périphériques réseau et les routeurs peuvent être utilisés pour propager des logiciels pirates ou malveillants. Il est donc nécessaire d'appliquer des mesures de sécurité des systèmes afin de limiter ces risques.
Chaque objet connecté à internet d'une manière plus générale à n'importe quel réseau informatique est susceptible d'être victime d'une attaque d'un pirate informatique.
Dans ce chapitre, nous présentons les principaux concepts et définitions de l'Internet of Things (IoT) et comment sécurisé ces différents objets en utilisant l'une des solutions existante « les firewalls».

1.2 IoT :

1.2.1 Définition de L'internet des objets (IoT) :

L'internet des objets, ou sous son nom anglais Internet Of Things, se définit comme la matérialisation d'internet dans le monde réel. Cela concerne divers objets comme des montres,

des pèse-personnes et même votre brosse à dents qui peut être connectée à votre dentiste comme expliqué sur cette page.

Grâce à l'IOT, tous ces objets connectés peuvent être contrôlés mais aussi suivis à distance. En effet, de plus en plus d'objets que nous utilisons sont connectés à internet. En utilisant une carte sim m2m, ils transmettent des informations à des serveurs dédiés qui sont regroupés en un réseau IOT[1].

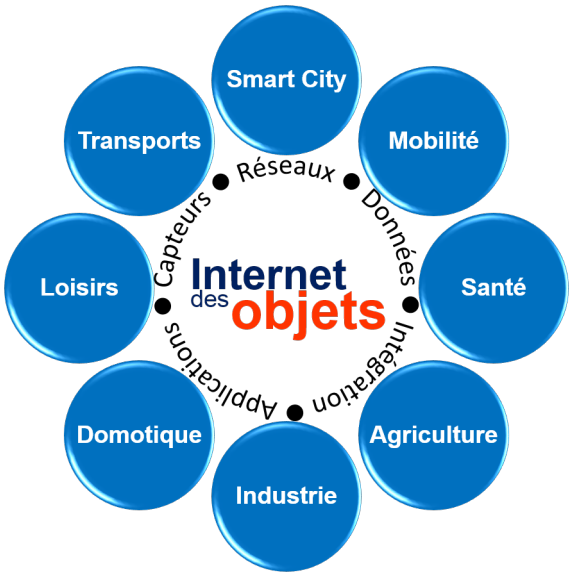


FIGURE 1.1 – le paradigme de l'IoT.

. **D'un point de vue conceptuel :** l'Internet des objets caractérise des objets physiques connectés ayant leur propre identité numérique et capables de communiquer les uns avec les autres. Ce réseau crée en quelque sorte une passerelle entre le monde physique et le monde virtuel.

. **D'un point de vue conceptuel :** l'IoT consiste en l'identification numérique directe et normalisée (adresse IP, protocoles smtp, http...) d'un objet physique grâce à un système de communication sans fil qui peut être une puce RFID, Bluetooth ou Wi-Fi [2].

FIGURE 1.2 – Exemple des objets connectés.

FIGURE 1.3 – Exemple des objets connectés.

1.2.2 le mode fonctionnement de l'IoT

The Internet of things repose sur l'identification des objets afin d'en recueillir les données et que celles-ci soient envoyées sur une plateforme Cloud ou sur une application. Chaque objet dispose ainsi d'une adresse IP et le réseau permet de connecter tous les objets disposant d'une adresse IP.

De ce fait, pour fonctionner le réseau IOT a besoin de la technologie M2M (machine to machine). En effet, c'est cette technologie qui, en utilisant un réseau de télécommunication, et grâce à un mode cellulaire ou au Wifi, connecte les objets à un réseau.

Un objet connecté a donc besoin d'une carte sim m2m. C'est le réseau de télécommunication de cette carte qui permet le transfert des informations. Les opérateurs historiques de téléphonie répondent donc à ce nouveau besoin de plus en plus présent en proposant une offre m2m à ses clients utilisant l'internet de l'objet.

Par ailleurs, toutes les personnes utilisant un même objet connecté comme un aspirateur par exemple ne seront pas chez le même opérateur. Les entreprises proposant les objectes connectés doivent donc utiliser un réseau IOT qui permet de mutualiser les données et qui soit géré par des spécialistes.

Le but des entreprises commercialisant ces objets connectés est de pouvoir recueillir des données brutes dans le but d'améliorer ses services, de mettre à jour le produit ou encore de pouvoir réaliser des diagnostics et effectuer des réparations à distance[1].

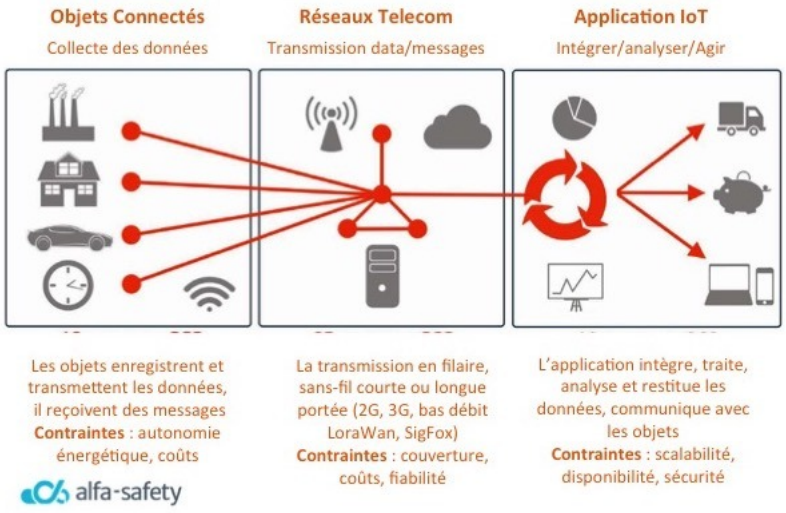


FIGURE 1.4 – Mode de fonctionnement de l'IoT.

1.2.3 Architecture de l'IoT

1.2.3.1 Niveau 1 : Capteurs et actionneurs :

1.2.3.1.1 • Capteur : C'est un dispositif utilisé pour détecter un événement ou une grandeur physique, tels que luminosité, température, humidité du sol, pression, etc. et qui fournit un signal électrique correspondant.

- Les capteurs IoT sont généralement de petite taille, ont un faible coût et consomment moins d'énergie.

- Les signaux produits par un capteur sont traités par un microcontrôleur pour, l'interprétation l'analyse.

1.2.3.1.2 • Actionneur : Une technologique complémentaire aux capteurs, convertit l'énergie électrique en mouvement ou énergie mécanique.

- Les actionneurs permettent de transformer l'énergie reçue en un phénomène physique (déplacement, dégagement de chaleur, émission de lumière . . .).

- Exemple : Haut-parleurs qui convertissent les signaux électriques correspondants en sons Ondes (acoustiques) [3].

1.2.3.2 Niveau 2 : Passerelle :

Une passerelle (gateway) est une combinaison de composants matériels et logiciels utilisés pour connecter un réseau à un autre.
• Les gateways permettent de relier les capteurs ou les noeuds de capteurs avec le monde extérieur.
• Les gateways sont donc utilisées pour la communication de données en collectant les mesures effectuées par les noeuds de capteurs et en les transmettant à l'infrastructure Internet.
• La gateway peut faire des traitements locaux sur les données avant de les relayer au Cloud

[3].

1.2.3.3 Niveau3 : Cloud computing :

Le niveau 3 est un choix technologique (optionnel) qui permet d'alléger la charge du travail vers le Cloud et de faire des traitements locaux (on the Edge).
• Trois solutions techniques sont possibles pour l'implémentation du 3ème niveau :
– **Fog Computing :** permet un calcul décentralisé en traitant les données IoT au niveau des nœuds locaux –Fog avant de relayer l'information vers le cloud.
– **Edge Computing :** le traitement des données IoT se fait à l'extrémité du réseau (Gateways ou des nœuds intermédiaires entre objets et gateways).
– **Mist Computing :** le traitement des données se fait localement dans les nœuds capteur[3].

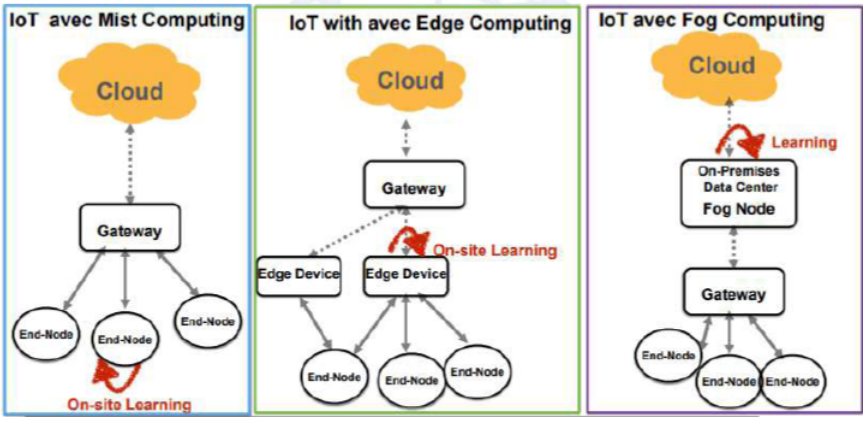


FIGURE 1.5 – Cloud Via Fog via Edge[3].

1.2.3.4 Niveau4 : Plateformes IoT :

Une plateforme d'IoT est un ensemble de services permettant de collecter, stocker, corréler, analyser et exploiter les données [3].

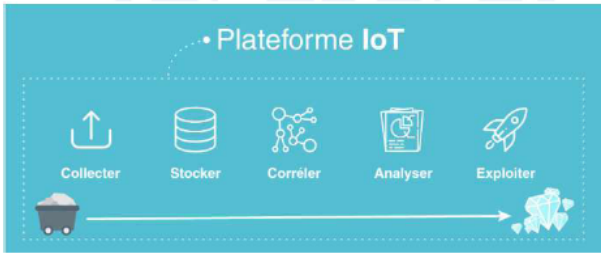


FIGURE 1.6 – Plateforme IoT[3].

1.2.4 Les Protocoles de fonctionnement de l'IoT

Le modèle OSI (Open Systems Interconnexion) fournit une carte des différentes couches qui envoient et reçoivent des données. Chaque protocole IoT de l'architecture du système

IoT permet une communication d'appareil à appareil, d'appareil à passerelle, de passerelle à centre de données ou de passerelle à Cloud, ainsi qu'une communication entre centres de données [4].

-Au niveau de la couche de liaison, le standard IEEE 802.15.4 est plus adapté que l'Ethernet aux environnements industriels difficiles.
-Au niveau réseau, le standard 6loWPan a réussi a adapter le protocole IPV6 aux communication sans fil entre nœud a très faible consommation.
-Au niveau routage, l'IETF a publié en 2011 le standard RPL.
-Au niveau de la couche application le protocole CoAP qui tente d'adapter http, beaucoup trop gourmand aux contraintes des communications entre nœuds à faible Consommation [5].

1.2.5 Les technologies de l'IoT :

1.2.6 Les technologies de courte portée :

1.2.7 le Protocol NFC :

Les protocoles **Near Field Communication (NFC)** sont fondés sur la technologie d'identification par radio fréquence RFID (Radio frequency identification).
Les objets équipés d'une puce électronique RFID possèdent une « étiquette » et sont automa-

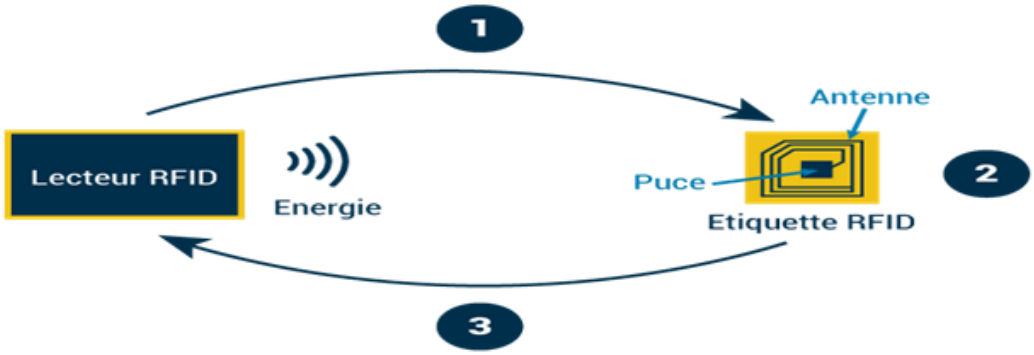


FIGURE 1.7 – Présente la technologie RFID.

tiquement identifiés par radio fréquence lorsqu'ils se trouvent à proximité d'un équipement appelé interrogateur. Le protocole NFC est un standard de communication radiofréquence sans contact à très courte distance, de l'ordre de quelques centimètres, permettant une communication simple entre deux équipements électroniques.
Il est par exemple utilisé dans de nombreuses entreprises pour les badges d'accès aux locaux, ou comme support d'un abonnement à un réseau de transport en commun.

1.2.8 Bluetooth :

Inventé en 1994 par la société suédoise Ericsson, le protocole Bluetooth est un standard de transfert de données sans fil. Il utilise une faible bande passante, ce qui ne lui permet de transférer que peu de données à de courtes distances, mais est également très peu énergivore.

FIGURE 1.8 – Exemple badge d'accès aux locaux.

Inclus à l'immense majorité des téléphones mobiles, afin de réaliser une communication entre deux téléphones, ou entre un téléphone et un objet connecté de nature différente, il possède désormais de nombreuses applications : oreillette de discussion téléphonique sans fil, montre intelligente, moniteur de fréquence cardiaque, enceinte portative de diffusion de musique, station météo, thermostat, etc.
Ce protocole est également utilisé sur des capteurs statiques appelés beamers pour mesurer des flux, par exemple des clients dans un magasin.

1.2.9 Zigbee :

Zigbee est un protocole de communication radio développé spécifiquement pour les applications de domotique. D'une portée moyenne de 10 mètres, il utilise une faible bande passante et est idéal pour le transfert de données en faible volume.
Peu énergivore et conçu pour des échanges de données à bas débit, le dispositif Zigbee convient aux appareils alimentés par une pile ou une batterie, et en particulier aux capteurs. Il est conçu pour fonctionner en réseau maillé : chaque nœud reçoit, envoie et relaie des données. Il est par exemple utilisé par certains détecteurs de fumée.

1.2.10 Les technologies de moyenne portée :

1.2.11 ZWave :

Le Z-Wave est un protocole de communication sans fil principalement dédié à la domotique. Il permet de transmettre des données sur des distances allant de 30 mètres en intérieur à 100 mètres en plein air. Il fonctionne en réseau maillé, chaque appareil connecté pouvant relayer les informations émises par ses voisins, ce qui lui permet d'élargir sa portée.
Le protocole Z-Wave a été développé pour des usages peu énergivores nécessitant un faible débit de données. Tout comme le protocole Zigbee, l'utilisation de Z-Wave ne nécessite que très peu de puissance et les appareils peuvent donc communiquer pendant plusieurs années avec une simple pile.

1.2.12 Wi-Fi :

Le Wi-Fi désigne un ensemble de protocoles de communications sans fil, permettant des connexions à haut débit sur des distances de 20 à 100 mètres. Il s'agit d'un réseau local sans fil très énergivore, qui ne convient que pour les appareils branchés sur secteur ou dont l'alimentation électrique peut être aisée et fréquente.
Il permet de transférer rapidement beaucoup de données. Il existe différentes normes Wi-Fi correspondant à une portée et un débit variables.

1.2.13 Bluetooth Low Energy :

Aussi connue sous l'appellation Wibree, la technologie Bluetooth Low Energy (BLE) est un protocole de réseau personnel sans fil à très basse consommation. Comme la technologie Bluetooth originelle, le BLE ne permet de transférer qu'une quantité limitée de donnée à une distance moyenne de 60 mètres.
La différence entre les dispositifs Bluetooth et BLE se situe au niveau de la consommation électrique nécessaire à la communication, qui est dix fois moindre pour BLE.

1.3 Les technologies de longue portée :

1.3.1 Réseaux cellulaires mobiles :

Fournis par les opérateurs de télécommunication, les réseaux cellulaires mobiles, basés sur la technologie GSM, permettent de transférer une quantité importante de données à une longue portée. Ils nécessitent l'installation d'une carte SIM dans l'appareil à connecter, afin d'identifier celui-ci sur le réseau de communication.
Succédant aux premières générations des standards pour la téléphonie mobile, qui ont progressivement permis d'accroître le débit de communication, la quatrième génération (4G) permet une communication mobile à très haut débit.

1.3.2 Réseaux radio bas-débit :

1.3.2.1 Sigfox :

Est un réseau de communication radio sans fil à bas débit et à basse fréquence, d'une portée moyenne de 10 kilomètres en milieu urbain et de 30 à 50 kilomètres en milieu rural. Il est également une technologie créée par l'entreprise du même nom. Ce réseau convient à des appareils à basse consommation, dotés ainsi d'une grande autonomie qui transfèrent une faible quantité de données.

1.3.2.2 LoRa :

Est un protocole de communication radio à très basse consommation, qui permet de transmettre des données en petite quantité, à des distances de 2 à 5 kilomètres en ville et jusqu'à 45 kilomètres en milieu urbain. À l'instar de Sigfox, il s'agit d'un dispositif qui convient

particulièrement aux équipements peu énergivores n'émettant que périodiquement, notamment les capteurs.

1.3.2.3 Réseaux propriétaires :

Certains grands groupes industriels, dotés de moyens financiers conséquents, préfèrent installer leur propre réseau de communication. Le déploiement de ces réseaux dits privés ou propriétaires est particulièrement intéressants en cas de déploiement à très grande échelle d'appareils communicants.
C'est ainsi que m2ocity, filiale de Veolia Eau et d'Orange, a choisi d'installer son propre réseau de communication pour connecter les compteurs d'eau intelligents et réaliser des opérations de télé-relevé, de même que Suez.
Le système de comptage évolué à destination des clients résidentiels de gaz naturel de GRDF se fonde également sur un protocole radio à longue portée spécifique et propriétaire : une bande de fréquence radio réservée (169 MHz) est utilisée pour assurer la communication des données entre les compteurs et les concentrateurs de données, eux-mêmes chargés de transmettre au système d'information central les informations qu'ils ont collectées[5].

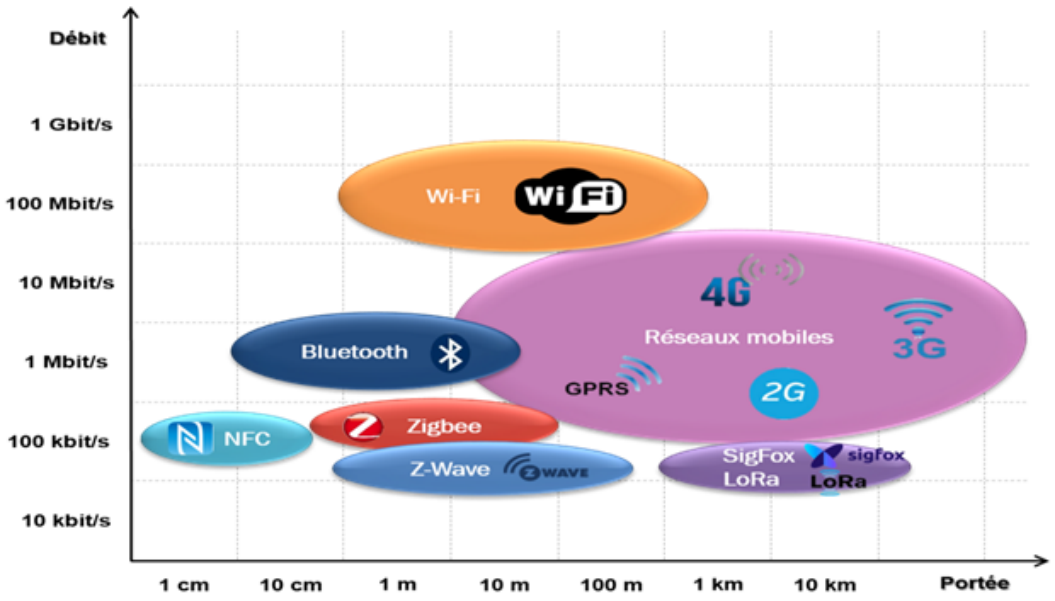


FIGURE 1.9 – Différents technologies de l'IoT.

1.3.3 Domaines d'applications de L'IoT :

Le marché des objets connectés est promis à une grande croissance dans les années à venir car il a une valeur immense dans les différents domaines d'objets connectés pour les professionnels. Cependant, seules quelques applications sont actuellement déployées [2].
L'utilisation de l'IDO permettra le développement de plusieurs applications intelligentes qui toucheront essentiellement ceux qu'on citera dans ce qui suit, nous citrons brièvement des exemples d'applications de l'IDO [3].

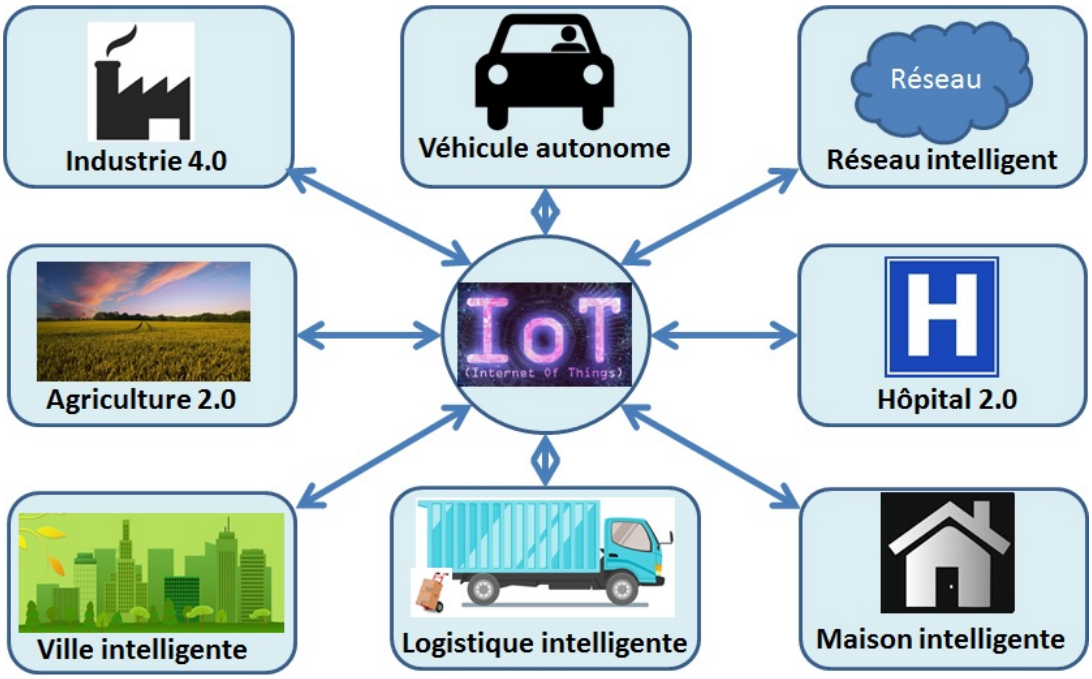


FIGURE 1.10 – Domaines d'applications de L'IoT.

1.3.3.1 Transports intelligents :

Les cartes touristiques peuvent être équipées par des balises à base de la technologie NFC2, et permettre au Smartphone de récupérer via le web les informations qui peuvent intéresser les touristes (hôtels, restaurants, évènements) [23].

FIGURE 1.11 – Transports intelligents[23].

1.3.3.2 Domotique || Smart Home :

L'IdO permet l'accès à un monde ambiant, ou les objets domestiques collaborent entre eux pour améliorer l'habitat humain. Ce concept permet de gérer tous les équipements (tâches ménagères, verrouillage des portes / fenêtres, vidéo surveillance, etc.) en-site ou à distance

via un réseau de communication[24].

FIGURE 1.12 – Services de la domotique[24].

1.3.3.3 Réseaux électriques intelligents || Smart Grid

Un réseau électrique intelligent est un réseau amélioré grâce à l'intégration des énergies renouvelables et des TIC en garantissant la communication bidirectionnelle entre les différents acteurs du réseau et en temps réel. Il vise à garantir la disponibilité, l'efficacité, le coût réduit et la sécurité de l'énergie fournie[23].

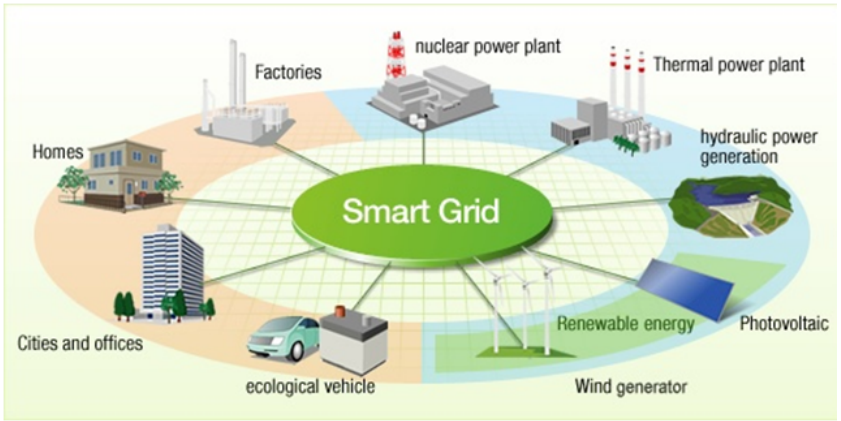


FIGURE 1.13 – Services du Smart Grid[23].

1.3.4 L'industrie :

Le problème des pièces non homologues résultant de l'utilisation des pièces qui ne répondent pas aux exigences (Suspected Unapproved Parts) particulièrement dans le secteur

de l'aéronautique peut être résolu à l'aide de l'IdO en marquant chaque pièce avec des tags contenant des identifiants et permettant la récupération automatique des informations relatives à la pièce [24].

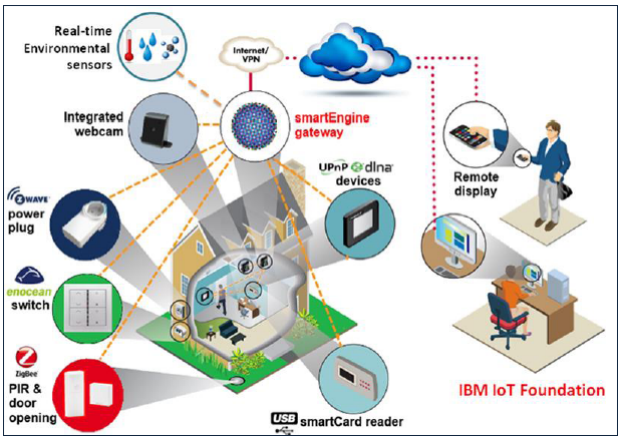


FIGURE 1.14 – IoT dans l'industrie[24].

1.3.4.1 L'internet des objets dans le domaine de la santé :

Le secteur de la santé a connu un très grand nombre d'applications permettant à un patient et à son docteur de recevoir des informations, parfois même en temps réels, qu'il aurait été impossible de connaître avant l'apparition d'IoT.

Par exemple, (Porteuse Digital Health) qui est le premier médicament connecté sur le marché grâce à un capteur directement intégré dans l'être humain qui permet après ça le suivi des patients à distance.

Il existe Plusieurs autres dispositifs sont disponibles, fixé autour du poignet et permettent également de suivre l'activité physique quotidienne du patient, mesurer le taux de sucre, compter le nombre de pas, les kms parcourus, le nombre de calories brûlées. . . ,Le dispositif lui envoie une alerte dans les cas anormaux.

Récemment, Goldman Sachs a publié une étude qui prouve que l'Internet des Objets pourrait faire économiser des milliards de dollars au service de santé américain[25] .

1.3.5 Les défis de l'internet des objets :

Les défis de l'émergence de l'IoT sont nombreux. Ils sont à la fois techniques et sociaux. Ces défis doivent être surmontés afin de garantir l'adoption et la diffusion de l'IoT, Nous présentons quelque défis dans les points suivantes :

- **Disponibilité et fiabilité :** La méthode de collecte et de transmission des informations influence fortement la qualité des données fournies.

- **Interopérabilité :**l'hétérogénéité et la diversité des environnements logiciels et matériels des objets.

- **Sécurité et confidentialité :** nécessité de sécuriser et cloisonner les données échangées.

- **Evolutivité et passage à l'échelle (Scalabilité) :** trouver des solutions flexibles pour le passage à l'échelle dans un scénario d'objets dispersés et nombreux.

- **Politique réglementaire :** la réglementation n'est pas adaptée pour des applications IoT spécifiques.

- **Propriété intellectuelle :** Une compréhension commune des droits de propriété entre les parties prenantes devrait être clairement définie pour libérer tout le potentiel de l'IoT.

La question demeure ouverte, par exemple dans les dispositifs médicaux implantés dans le corps d'un patient, la question du droit sur la donnée générée, le patient ou le fabricant de l'appareil[6].

1.4 les Firewalls :

1.4.1 Définition des firewalls

Un pare-feu ou Firewall en anglais est parfois appelé coupe-feu, garde-barrière où barrière de sécurité. En informatique l'usage du terme «pare-feu» est métaphorique : il évoque une porte empêchant les flammes d'Internet d'entrer chez soi et/ou de « contaminer » un réseau informatique .
C'est un logiciel ou un matériél qui vérifie les informations provenant d'Internet ou d'un réseau,puis les empêche d'accéder à l'ordinateur ou les y autorise, selon la configuration qui lui a été donné. Il gère les flux entrants et les flux sortans [26].

1.5 Les différents types de filtrages

1.5.1 Le filtrage simple de paquet (Stateless)

1.5.1.1 Le principe

C'est la méthode de filtrage la plus simple, elle opère au niveau de la couche réseau et transport du modèle Osi. La plupart des routeurs d'aujourd'hui permettent d'effectuer du

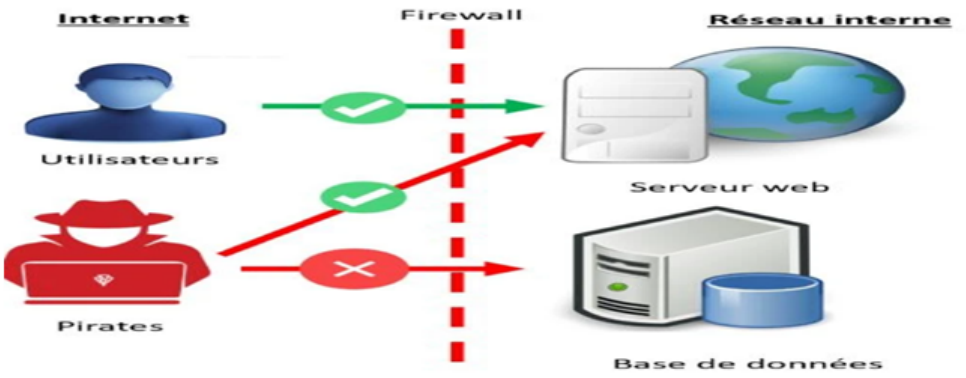


FIGURE 1.15 – présente un firewall

filtrage simple de paquet. Cela consiste à accorder ou refuser le passage de paquet d'un réseau à un autre en se basant sur :

- L'adresse IP Source/Destination.
- Le numéro de port Source/Destination.
- Et bien sûr le protocole de niveau 3 ou 4.

Cela nécessite de configurer le Firewall ou le routeur par des règles de filtrages, généralement appelées des ACL (Access Control Lists).

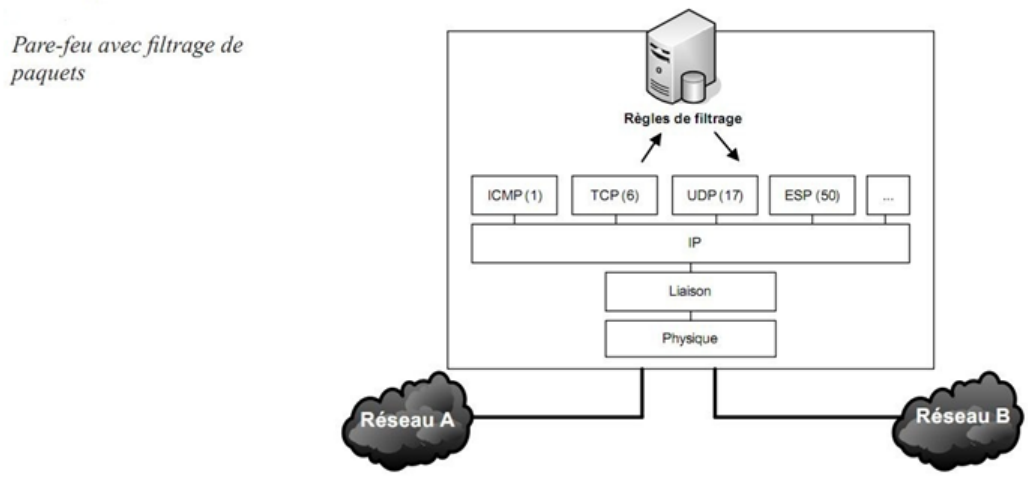


FIGURE 1.16 – présente firewall avec filtrage de paquet

1.5.1.2 Les limites

Le premier problème vient du fait que l'administrateur réseau est rapidement contraint à autoriser un trop grand nombre d'accès, pour que le Firewall offre une réelle protection. Par exemple, pour autoriser les connexions à Internet à partir du réseau privé, l'administrateur devra accepter toutes les connexions Tcp provenant de l'Internet avec un port supérieur à 1024. Ce qui laisse beaucoup de choix à un éventuel pirate.

Il est à noter que de définir des ACL sur des routeurs haut de gamme – c'est à dire, supportant un débit important – n'est pas sans répercussion sur le débit lui-même. Enfin, ce type de filtrage ne résiste pas à certaines attaques de type IP Spoofing / IP Flooding, la mutilation de paquet, ou encore certaines attaques de type DoS. Ceci est vrai sauf dans le cadre des routeurs fonctionnant en mode distribué.
Ceci permettant de gérer les Acl directement sur les interfaces sans remonter à la carte de traitement central. Les performances impactées par les Acl sont alors quasi nulles.

1.5.2 Le filtrage de paquet avec état (Stateful)

1.5.2.1 Le principe

L'amélioration par rapport au filtrage simple, est la conservation de la trace des sessions et des connexions dans des tables d'états internes au Firewall. Le Firewall prend alors ses décisions en fonction des états de connexions, et peut réagir dans le cas de situations protocolaires anormales. Ce filtrage permet aussi de se protéger face à certains types d'attaques DoS.
Dans l'exemple précédent sur les connexions Internet, on va autoriser l'établissement des connexions à la demande, ce qui signifie que l'on aura plus besoin de garder tous les ports supérieurs à 1024 ouverts. Pour les protocoles UDP et ICMP, il n'y a pas de mode connecté. La solution consiste à autoriser pendant un certain délai les réponses légitimes aux paquets envoyés. Les paquets Icmp sont normalement bloqués par le Firewall, qui doit en garder les traces. Cependant, il n'est pas nécessaire de bloquer les paquets Icmp de type 3 (destination inaccessible) et 4 (ralentissement de la source) qui ne sont pas utilisables par un attaquant. On peut donc choisir de les laisser passer, suite à l'échec d'une connexion Tcp ou après l'envoi d'un paquet Udp.
Pour le protocole Ftp (et les protocoles fonctionnant de la même façon), c'est plus délicat

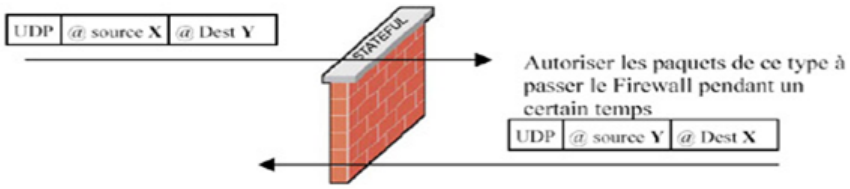


FIGURE 1.17 – filtrage de paquet avec état (Stateful)

puisqu'il va falloir gérer l'état de deux connexions. En effet, le protocole Ftp, gère un canal de contrôle établi par le client, et un canal de données établi par le serveur. Le Firewall devra donc laisser passer le flux de données établi par le serveur.
Ce qui implique que le Firewall connaisse le protocole Ftp, et tous les protocoles fonctionnant sur le même principe. Cette technique est connue sous le nom de filtrage dynamique (Stateful Inspection) et a été inventée par Checkpoint. Mais cette technique est maintenant gérée par d'autres fabricants.

1.5.2.2 Les limites

Tout d'abord, il convient de s'assurer que les deux techniques sont bien implémentées par les Firewalls, car certains constructeurs ne l'implémentent pas toujours correctement.

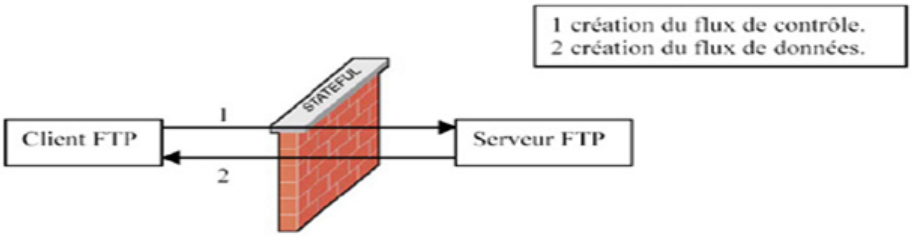


FIGURE 1.18 – filtrage de paquet avec état (Stateful)

Ensuite une fois que l'accès à un service a été autorisé, il n'y a aucun contrôle effectué sur les requêtes et réponses des clients et serveurs. Un serveur Http pourra donc être attaqué impunément (Comme quoi il leur en arrive des choses aux serveurs WEB !). Enfin les protocoles maisons utilisant plusieurs flux de données ne passeront pas, puisque le système de filtrage dynamique n'aura pas connaissance du protocole.

1.5.3 Le filtrage applicatif (ou pare-feu de type proxy ou proxying applicatif)

1.5.3.1 Le principe

Le filtrage applicatif est comme son nom l'indique réalisé au niveau de la couche Application. Pour cela, il faut bien sûr pouvoir extraire les données du protocole de niveau 7 pour les étudier. Les requêtes sont traitées par des processus dédiés, par exemple une requête de type Http sera filtrée par un processus proxy Http.
Le pare-feu rejettera toutes les requêtes qui ne sont pas conformes aux spécifications du protocole. Cela implique que le pare-feu proxy connaisse toutes les règles protocolaires des protocoles qu'il doit filtrer.

Pare-feu passerelle de niveau applicatif

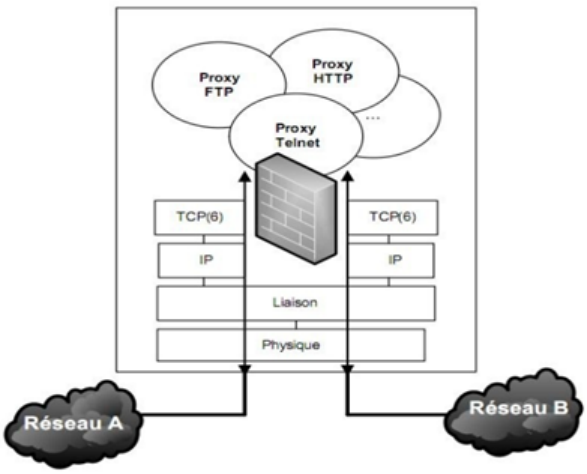


FIGURE 1.19 – présente firewall avec filtrage applicatif

1.5.3.2 Les limites

Le premier problème qui se pose est la finesse du filtrage réalisé par le proxy. Il est extrêmement difficile de pouvoir réaliser un filtrage qui ne laisse rien passer, vu le nombre de protocoles de niveau 7. En outre le fait de devoir connaître les règles protocolaires de chaque protocole filtré pose des problèmes d'adaptabilité à de nouveaux protocoles ou des protocoles maisons.
Mais il est indéniable que le filtrage applicatif apporte plus de sécurité que le filtrage de paquet avec état, mais cela se paie en performance. Ce qui exclut l'utilisation d'une technologie 100 proxy pour les réseaux à gros trafic au jour d'aujourd'hui. Néanmoins d'ici quelques années, le problème technologique sera sans doute résolu.

1.5.4 Que choisir

Tout d'abord, il faut nuancer la supériorité du filtrage applicatif par rapport à la technologie Stateful. En effet les proxys doivent être paramétrés suffisamment finement pour limiter le champ d'action des attaquants, ce qui nécessite une très bonne connaissance des protocoles autorisés à traverser le firewall. Ensuite un proxy est plus susceptible de présenter une faille de sécurité permettant à un pirate d'en prendre le contrôle, et de lui donner un accès sans restriction à tout le système d'information.
Idéalement, il faut protéger le proxy par un Firewall de type Stateful Inspection. Il vaut mieux éviter d'installer les deux types de filtrage sur le même Firewall, car la compromission de l'un entraîne la compromission de l'autre. Enfin cette technique permet également de se protéger contre l'ARP spoofing.

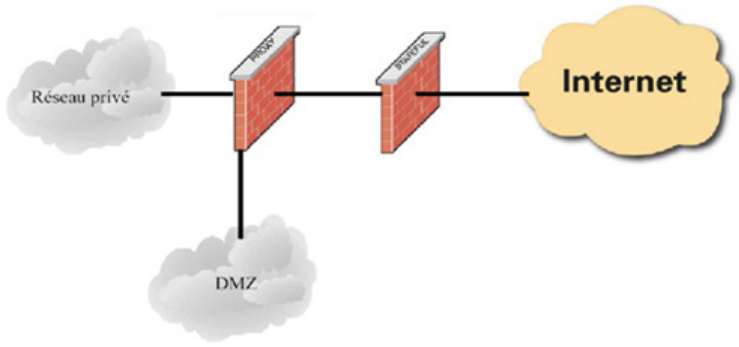


FIGURE 1.20 – présente firewall avec filtrage applicatif

1.6 Les différents types de Firewall

1.6.1 Les Firewall Bridge

Ces derniers sont relativement répandus. Ils agissent comme de vrais câbles réseau avec la fonction de filtrage en plus, d'où leur appellation de firewall. Leurs interfaces ne possèdent pas d'adresse Ip, et ne font que transférer les paquets d'une interface a une autre en leur appliquant les règles prédéfinies. Cette absence est particulièrement utile, car cela signifie

que le firewall est indétectable pour un hacker lambda. En effet, quand une requête ARP est émise sur le câble réseau, le firewall ne répondra jamais. Ses adresses Mac ne circuleront jamais sur le réseau, et comme il ne fait que « transmettre » les paquets, il sera totalement invisible sur le réseau. Cela rend impossible toute attaque dirigée directement contre le firewall, étant donné qu'aucun paquet ne sera traité par ce dernier comme étant sa propre destination. Donc, la seule façon de le contourner est de passer outre ses règles de drop. Toute attaque devra donc « faire » avec ses règles, et essayer de les contourner.
Dans la plupart des cas, ces derniers ont une interface de configuration séparée. Un câble vient se brancher sur une troisième interface, série ou même Ethernet, et qui ne doit être utilisée que ponctuellement et dans un environnement sécurisé de préférence.
Ces firewalls se trouvent typiquement sur les switchs[9].

Avantages	Inconvénients
Impossible de l'éviter (les paquets passeront par ses interfaces)Peu coûteux	Possibilité de le contourner (il suffit de passer outre ses règles) Configuration souvent contraignante Les fonctionnalités présentes sont très basiques (filtrage sur adresse IP, port, le plus souvent en Stateless)

FIGURE 1.21 – Avantages et inconvénients d'un Firewall Bridge

1.6.2 Les Firewalls matériels

Ils se trouvent souvent sur des routeurs achetés dans le commerce par de grands constructeurs comme Cisco ou Nortel. Intégrés directement dans la machine, ils font office de « boite noire », et ont une intégration parfaite avec le matériel. Leur configuration est souvent relativement ardue, mais leur avantage est que leur interaction avec les autres fonctionnalités du routeur est simplifiée de par leur présence sur le même équipement réseau. Souvent relativement peu flexibles en terme de configuration, ils sont aussi peu vulnérables aux attaques, car présent dans la « boite noire » qu'est le routeur. De plus, étant souvent très liés au matériel, l'accès à leur code est assez difficile, et le constructeur a eu toute latitude pour produire des systèmes de codes « signés » afin d'authentifier le logiciel (système RSA ou assimilés). Ce système n'est implanté que dans les firewalls haut de gamme, car cela évite un remplacement du logiciel par un autre non produit par le fabricant, ou toute modification de ce dernier, rendant ainsi le firewall très sûr. Son administration est souvent plus aisée que les firewall bridges, les grandes marques de routeurs utilisant cet argument comme argument de vente. Leur niveau de sécurité est de plus très bon, sauf découverte de faille éventuelle comme tout firewall. Néanmoins, il faut savoir que l'on est totalement dépendant du constructeur du matériel pour cette mise à jour, ce qui peut être, dans certains cas, assez contraignant. Enfin, seules les spécificités prévues par le constructeur du matériel sont implémentées. Cette dépendance induit que si une possibilité nous intéresse sur un firewall d'une autre marque, son utilisation est impossible. Il faut donc bien déterminer à l'avance ses besoin et choisir le constructeur du routeur avec soin[9].

1.6.3 Les Firewalls logiciels

Présents à la fois dans les serveurs et les routeurs « faits maison », on peut les classer en plusieurs catégories :

Avantages	Inconvénients
Intégré au matériel réseau Administration relativement simple Bon niveau de sécurité	Dépendant du constructeur pour les mises à jour Souvent peu flexible

FIGURE 1.22 – Avantages et inconvénients d'un Firewall matériel

1.6.3.1 Les Firewalls personnels

Ils sont assez souvent commerciaux et ont pour but de sécuriser un ordinateur particulier, et non pas un groupe d'ordinateurs.
Souvent payants, ils peuvent être contraignants et quelque fois très peu sécurisés. En effet, ils s'orientent plus vers la simplicité d'utilisation plutôt que vers l'exhaustivité, afin de rester accessible à l'utilisateur final.

Avantages	Inconvénients
Sécurité en bout de chaîne (Poste Client) Personnalisable assez facilement	Facilement contournable Difficiles à départager de par leur nombre énorme

FIGURE 1.23 – Avantages et inconvénients d'un Firewall personnel

1.6.4 Les Firewalls plus « Sérieux »

Tournant généralement sous linux, car cet OS offre une sécurité réseau plus élevée et un contrôle plus adéquat, ils ont généralement pour but d'avoir le même comportement que les firewalls matériels des routeurs, à ceci prêt qu'ils sont configurables à la main.
Le plus courant est IP tables (anciennement IP chains), qui utilise directement le noyau linux. Toute fonctionnalité des firewalls de routeurs est potentiellement réalisable sur une telle plateforme.
Ces firewalls logiciels ont néanmoins une grande faille : ils n'utilisent pas la couche bas ré-

Avantages	Inconvénients
Personnalisables Niveau de sécurité très bon	Nécessite une administration système supplémentaire

FIGURE 1.24 – Avantages et inconvénients d'un Firewall plus sérieux

seau. Il suffit donc de passer outre le noyau en ce qui concerne la récupération de ces paquets, en utilisant une librairie spéciale, pour récupérer les paquets qui auraient été normalement « droppés » par le Firewall.
Néanmoins, cette faille induit de s'introduire sur l'ordinateur en question pour y faire des modifications. . . chose qui induit déjà une intrusion dans le réseau, ou une prise de contrôle physique de l'ordinateur, ce qui est déjà Synonyme d'inefficacité de la part du firewall.

1.7 DMZ « Zone Démilitarisée »

1.7.1 Notion de cloisonnement

Les systèmes pare-feu permettent de définir des règles d'accès entre deux réseaux. Néanmoins, dans la pratique, les entreprises ont généralement plusieurs sous-réseaux avec des politiques de sécurité différentes. C'est la raison pour laquelle il est nécessaire de mettre en place des architectures de systèmes pare-feux permettant d'isoler les différents réseaux de l'entreprise : on parle ainsi de « cloisonnement des réseaux » (le terme isolation est parfois également utilisé).

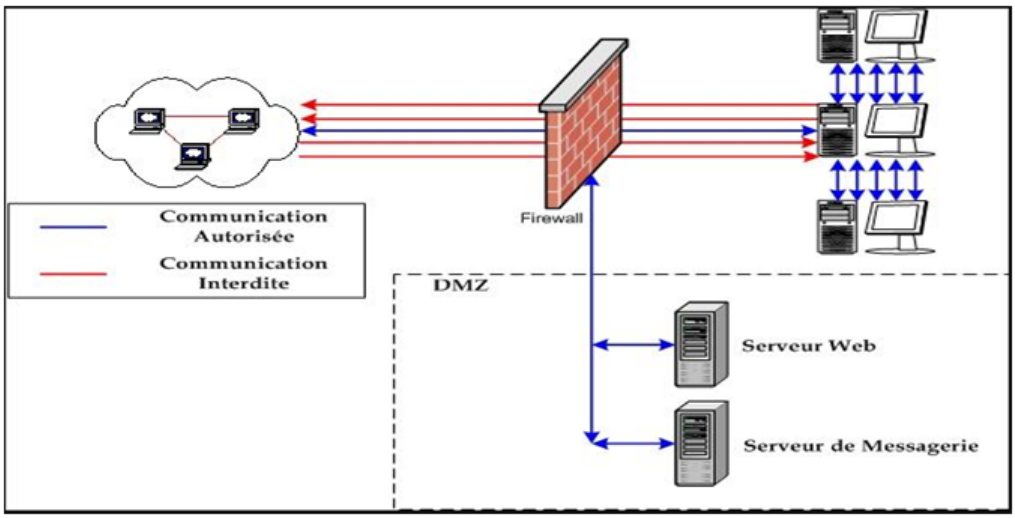


FIGURE 1.25 – Architecture DMZ

Lorsque certaines machines du réseau interne ont besoin d'être accessibles de l'extérieur (serveur web, un serveur de messagerie, un serveur FTP public, etc.), il est souvent nécessaire de créer une nouvelle interface vers un réseau à part, accessible aussi bien du réseau interne que de l'extérieur, sans pour autant risquer de compromettre la sécurité de l'entreprise.
On parle ainsi de « zone démilitarisé » (notée DMZ pour DeMilitarized Zone) pour désigner cette zone isolée hébergeant des applications mises à disposition du public. La DMZ fait ainsi office de « zone tampon » entre le réseau à protéger et le réseau hostile. La figure ci-dessous montre la position d'une DMZ au sein d'un réseau. Les serveurs situés dans la DMZ sont appelés « bastions » en raison de leur position d'avant poste dans le réseau de l'entreprise.
La politique de sécurité mise en œuvre sur la DMZ est généralement la suivante :

- Trafic du réseau externe vers la DMZ autorisé.
- Trafic du réseau externe vers le réseau interne interdit.
- Trafic du réseau interne vers la DMZ autorisé.
- Trafic du réseau interne vers le réseau externe autorisé.
- Trafic de la DMZ vers le réseau interne interdit.
- Trafic de la DMZ vers le réseau externe interdit.

La DMZ possède donc un niveau de sécurité intermédiaire, mais son niveau de sécurisation n'est pas suffisant pour y stocker des données critiques pour l'entreprise. Il est à noter qu'il est possible de mettre en place des DMZ en interne afin de cloisonner le réseau interne selon différents niveaux de protection et ainsi éviter les intrusions venant de l'intérieur[4].

1.8 but d'un Firewall

1.8.1 Se protéger de malveillances "externes"

- des curieux qui génèrent du trafic, qui font plus de peur que de mal, mais qui, quelques fois, finissent par coûter cher.

- les vandales, ceux qui veulent embêter pour embêter, (saturation de liaisons, saturation de CPU, corruptions de données, mascarade d'identité, etc).

- les "espionnages", (problèmes de confidentialité de l'information –> cf Sniffer).

1.8.2 Avoir un point de passage obligé permettant

- de bien vérifier si les règles de sécurité telles que spécifiées dans la politique sécurité d'établissement sont réellement celles qui sont appliquées.

- de contrôler le trafic entre le réseau interne et externe (locations des Liaison Louées) pour éviter des abus (téléchargement intempestif).

- d'auditer/tracer de façon "centrale" ce trafic, aider à prévoir les évolutions du réseau (statistiques possibles).

- éventuellement d'avoir une vue de la consommation Internet des différents utilisateurs/services.

1.8.3 les adresses IP

Un firewall permet, en utilisant la conversion d'adresse NAT, d'utiliser des adresses IP privées qui ne seront ni connues ni routées vers internet pour étendre le domaine d'adressage interne.

FIGURE 1.26 – présente la conversion adresse NAT

1.8.4 8 Les Étapes de sécurisation des réseaux et des routeurs :

Les appareils IoT à proprement parler ne sont pas les uniques sources de préoccupation. En effet, connectés à l'Internet des objets, les périphériques réseau et les routeurs peuvent

être utilisés pour propager des logiciels pirates ou malveillants. Il est donc nécessaire d'appliquer des mesures de sécurité des systèmes afin de limiter ces risques [11] :

- **Mappez et surveillez tous les périphériques connectés** (paramètres, mots de passe, versions de micrologiciel, correctifs récents. . .). Cette mesure permet d'identifier les objets intelligents que vous devez remplacer ou mettre à jour.

- **Segmentez le réseau!** La segmentation du réseau empêche la propagation des attaques en isolant les périphériques problématiques qui ne peuvent pas être immédiatement mis hors ligne en cas d'attaque.

- **Veillez à la sécurité du réseau** en configurant les routeurs avec un VLAN (réseau local virtuel) ou une DMZ (zone démilitarisée). Ces mécanismes de segmentation et d'isolation ajoutent une couche supplémentaire de sécurité aux réseaux connectés.

- **Respectez les bonnes pratiques de cybersécurité** à savoir l'activation du pare-feu du routeur, la désactivation de WPS (Wi-Fi Protected Setup) et l'activation du protocole de sécurité WPA2, l'utilisation d'un mot de passe fort pour l'accès Wi-Fi. . .

- **Désactivez les services inutiles** afin d'éviter les problèmes de sécurité[11].

1.9 Conclusion :

Nous allons présenter dans ce chapitre, une vision générale de l'IoT, la définition, les technologies utilisées et les domaines d'application, les méthodes approuvées pour protéger des attaques extérieures , et Pour sécuriser efficacement l'ensemble de ces objets intelligents, il faut donc mettre en place un plan de sécurité , le firewall est un composant réseau qui permet non seulement de concentrer l'administration de la sécurité en des points d'accès limités au réseau mais aussi de créer un périmètre de sécurité.

CHAPITRE 2

LA THÉORIE DES GRAPHES ET TOPOLOGIES DES RÉSEAUX

2.1 Introduction :

La théorie des graphes est un très vaste domaine, en évolution constante. Cette théorie permet de représenter un ensemble complexe d'objets en exprimant les relations entre les éléments.
Les graphes (et par conséquent la théorie des graphes) sont utilisés dans de nombreux domaines. On peut citer quelques exemples :
(Les réseaux de transport,Les réseau de l'information ,Les Circuits électroniques).
Ce chapitre sera décomposé en deux parties, la première nous présentons les principaux concepts de La théorie des graphes et les type des graphs (oriente ,non oriente ...) et paramètre de graphe dominant. Dans la deuxième partie nous allons des concepts généraux sur les réseaux, à savoir leurs classifications,Topologies des réseaux. .

2.2 Bref sur l'historique des graphes

Tout le monde s'accorde à considérer que la théorie des graphes est née en 1736 avec la communication d'Euler (1707-1783) dans laquelle il proposait une solution au célèbre problème des sept ponts de Königsberg. Le problème posé était le suivant. Deux îles A et D sur la rivière Prege de la Königsberg étaient reliées entre elles ainsi qu'aux rivages B et C à l'aide de sept ponts (désignés par des lettres minuscules) comme le montre la figure[14]

Le problème posé consistait à partir d'une terre quelconque A, B, C, ou D, à traverser chacun des ponts une fois et une seule et à revenir à son point de départ (sans traverser la rivière à la nage!). Euler représenta cette situation à l'aide d'un dessin où les sommets représentent les terres et les arêtes, les ponts comme le montre la figure

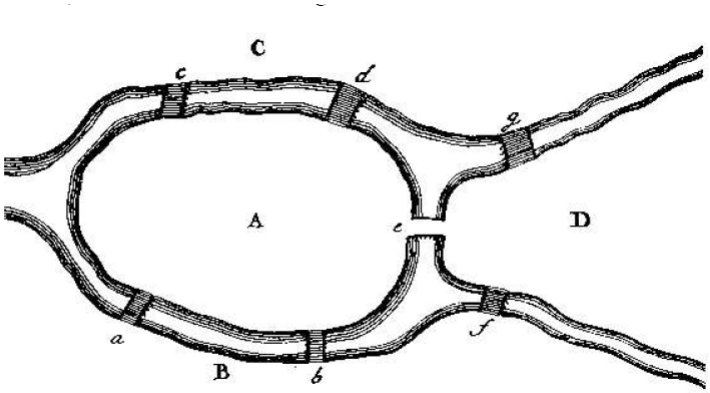


FIGURE 2.1 – la rivière Pregel et l'île de Kneiphof.

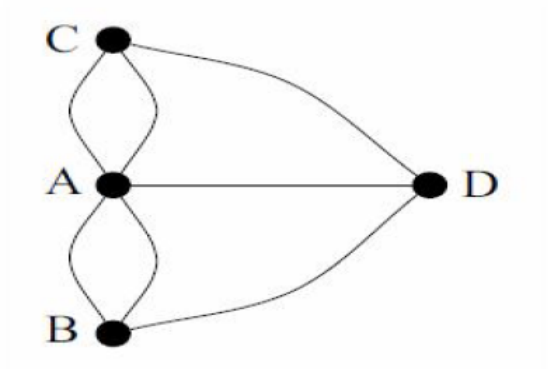


FIGURE 2.2 – Graphe associé au problème des ponts de Königsberg.

FIGURE 2.3 – Modélisation de problème de Königsberg.

2.3 Définition de la théorie du graphe

La théorie des graphes est l'un des outils privilégies de modélisation et de résolution de problèmes dans un grand nombre de domaines allant de la science fondamentale aux applications technologiques concrètes.
Un graphe permet de représenter simplement la structure, les connexions, les cheminements possibles d'un ensemble complexe, comprenant un grand nombre de situations, en expri-

mant les relations, les dépendances entre ses éléments (réseau de communication, réseaux ferroviaire ou routier, arbre généalogique, diagramme de succession de tâches en gestion de projet, etc).
En plus de son expression purement mathématique, le graphe est aussi une structure de données puissante dans l'informatique.[14]

2.3.1 Définition du graphe

Un graphe permet de décrire un ensemble d'objets et leurs relations, c'est à dire les liens entre les objets.

- Les objets sont appelés les noeuds, ou encore les sommets du graphe.
- Un lien entre deux objets est appelé une arête.

Un graphe *G* est un couple (*X*,*U*) :

- ❖ $X = \{ x_1, x_2, x_3, \dots, x_n \}$ est l'ensemble des sommets
- ❖ $U = \{ u_1, u_2, u_3, \dots, u_m \}$ l'ensemble des arcs.

Il existe deux types de graphes : les graphes orientes et les graphes non orientes :

2.3.1.1 Graphe Orienté et Graphe Non Orienté :

- Dans un graphe **non orienté**, la paire de sommets ($x1, x2$) représente une arête (n'est pas orientée. Autrement dit, ($x1, x2$) et ($x2, x1$) représentent la même arête).
- Dans un graphe **orienté**, la paire de sommets ($x1, x2$) représente un arc .(arête orientée. Autrement dit, ($x1, x2$) et ($x2, x1$) représentent deux arcs différents).

2.3.2 Représentations d'un graphe :

Un certain nombre de représentations existent pour décrire un graphe, On distingue principalement la représentation par :

- Matrice d'adjacence sommets – sommets.
- Matrice d'incidence sommets-arcs (ou sommets-arêtes dans le cas non orienté).
- istes d'adjacence.

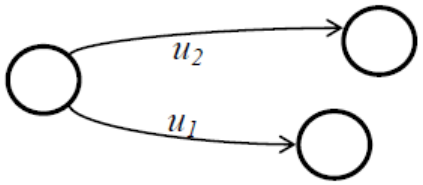
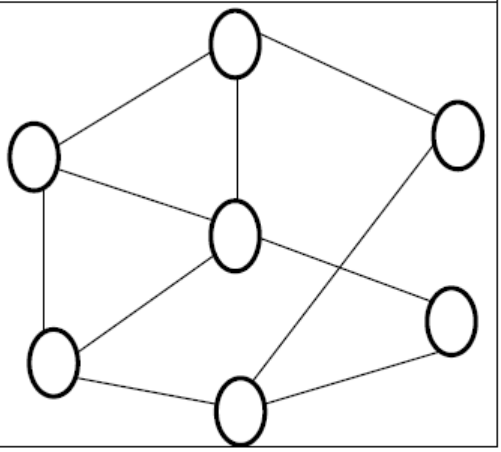
Représentation Mathématique	Représentation Graphique
• $X = \{ x_1, x_2, x_3 \}$ • $U = \{ u_1, u_2 \}$ où $u_1 = (x_1, x_2), u_2 = (x_1, x_3)$	
• $X = \{ a, b, c, d, f, g \}$ • $U = \{ u_1, u_2, u_3, u_4, u_5, u_6, u_7, u_8, u_9, u_{10} \}$ où $u_1 = (a, b), u_2 = (a, f),$ $u_3 = (a, g), u_4 = (b, c),$ $u_5 = (b, g), u_6 = (c, e),$ $u_7 = (d, e), u_8 = (d, g),$ $u_9 = (e, f), u_{10} = (f, g)$	

FIGURE 2.4 – Exemples d'un graphe.

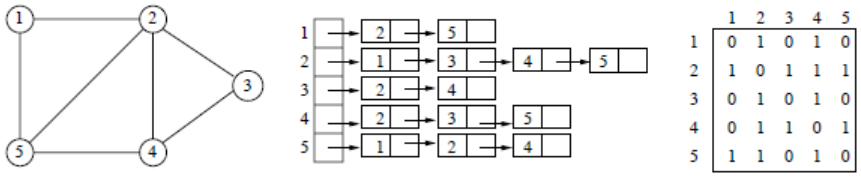


FIGURE 2.5 – Représentation d'un graphe par listes et matrice d'adjacence.

2.3.3 Degré d'un sommet :

Le degré d'un sommet u d'un graphe non-orienté est le nombre d'arêtes incidentes a ce sommet. Dans un graphe orienté, on désigne par demi-degré extérieur de $u2V$ le nombre d'arcs qui quittent le sommet u, par demi- degré intérieur le nombre d'arcs qui arrivent dans le sommet u.

2.3.4 Définitions principales :

2.3.4.1 Adjacence

Deux sommets sont adjacents (ou voisins) s'ils sont reliés par une arête.
Deux arcs sont adjacents s'ils ont au moins une extrémité commune.

2.3.4.2 Le sommet isolé :

Le sommet est un sommet dont le degré est égal à 0. $d(x3) = 0$ alors le sommet $x3$ est un sommet isolé.

FIGURE 2.6 – sommets 1 et 2 sont adjacents.

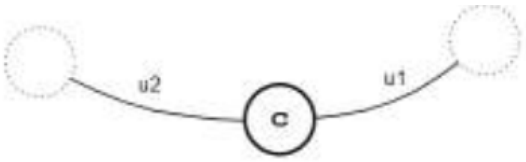


FIGURE 2.7 – Les deux arcs $u1$ et $u2$ sont adjacents.

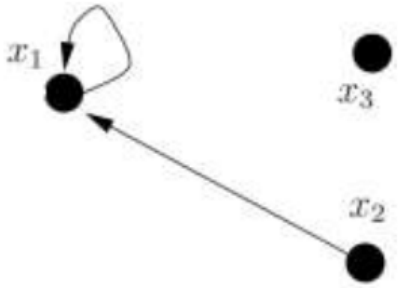


FIGURE 2.8 – Le sommet $x3$ est un sommet isolé.

2.3.4.3 Degré d'un Graphe :

Le degré d'un graphe est le degré maximum de tous ses sommets.

2.3.4.4 L'ordre d'un Graphe :

L'ordre d'un graphe est le nombre de sommets de ce graphe.

2.4 Paramètre de graphe :

Comme mentionné ci-dessus, les paramètres des graphes sont très utiles dans la caractérisation des graphes et résolution des problèmes. Généralement, un problème réel correspond à un paramètre dans le graphe modélisant un tel. Un paramètre de graphe est un invariant qui dépend uniquement sur la structure abstraite du graphe (par exemple le nombre de nœuds ou d'arêtes) et pas sur la représentation graphique (par exemple, dessin graphique). La détermination d'un paramètre de graphe conduit au regroupement ou à la décomposition du graphe nœuds qui facilite l'analyse du graphe. Par exemple, trouver le dominant set permet de regrouper les nœuds définis en dominants et dominés. Par conséquent, les dominantes peuvent être utilisées pour transmettre à tous les autres nœuds d'une communication réseau. La détection et la suppression des nœuds critiques permettent de décomposer le graphique

en petits composants. En tant que tel, la complexité du problème peut être considérablement en traiter chaque composant séparément. Cependant, comme nous l'avons déjà vu, les paramètres de graphes sont très utiles dans les problèmes résolution, mais leur détermination n'est pas toujours une tâche facile, et leur les problèmes d'optimisation sont généralement difficiles à résoudre. Détermination du maximum indépendant set et minimum dominant set sont des exemples d'un tel fait. Pour mieux comprendre, avant de passer en revue les paramètres les plus intéressants, nous introduisons d'abord les différentes classes de complexité des problèmes[16].

2.4.1 Complexité computationnelle

La complexité de calcul est estimée en fonction des ressources nécessaires, principalement en termes de temps (nombre d'opérations) nécessaire à l'algorithme utilisé pour résoudre le problème. Ce temps est appelé la complexité de l'algorithme.

Maintenant, nous fournissons les classes de complexité les plus connues.

2.4.1.1 Classe polynomiale déterministe (P)

Classe polynomiale déterministe (P) : Un problème est dit de classe P, si pour lequel on connaît un algorithme solution de complexité majoré par un polynôme d'ordre t dont la base x est une constante calculée en termes d'entrées du problème tel que le ordre n ou taille m du graphe $G = (E; V)$. La complexité d'un tel algorithme est notée $O(xt)$, et les meilleures complexités algorithmiques des problèmes P sont : $O(logx)$, $O(x)$ ou $O(x2)$.

2.4.1.2 Temps polynomial non déterministe (NP) :

pour lequel les solutions algorithmiques les plus connues sont de complexités telles que $O(2x), O(xx) ou O(x!)$, c'est-à-dire qu'il a une complexité élevée, mais l'optimalité d'un solution peut être vérifiée en un temps polynomial. Par exemple, on peut vérifier en temps polynomial si un circuit donné visite une fois chacun des nœuds du graphe (circuit hamiltonien) mais nous n'avons pas d'algorithme en temps polynomial pour déterminer un tel cycle. Le $NP - problme$ le plus difficile, pour lequel on n'espère pas beaucoup obtenir un algorithme polynomial, est appelé problème $NP - complet$, sauf celui si $NP = P$ qui constitue le problème ouvert le plus important en informatique théorique.
Pratiquement, nous disons qu'un problème NP est un problème NP-complet lorsque nous l'avons réduit avec succès à un problème $NP - complet$ bien connu. Lecteurs intéressés, pour plus de détails sur la théorie de la complexité[16]..

2.4.1.3 Classe NP-difficile

Si la vérification polynomiale de la propriété de solution n'est pas vérifiée alors le problème est dit NP-difficile.
Remarque : En raison de la difficulté des problèmes NP-complets et NP-difficiles, nous devrions définir des limites et fournir des solutions d'approximation avec une complexité moindre, à la place de déterminer la solution exacte dans un délai inacceptable.

Ci-après, nous présentons quelques-uns des paramètres graphiques les plus importants utilisés pour résoudre problèmes de la vie réelle[14].

2.4.2 Paramètres graphiques et applications

2.4.3 Définition d'un ensemble stable

Un stable appelé aussi ensemble indépendant est un ensemble de sommets deux à deux non adjacents (un sous-graphe sans arête)[14].

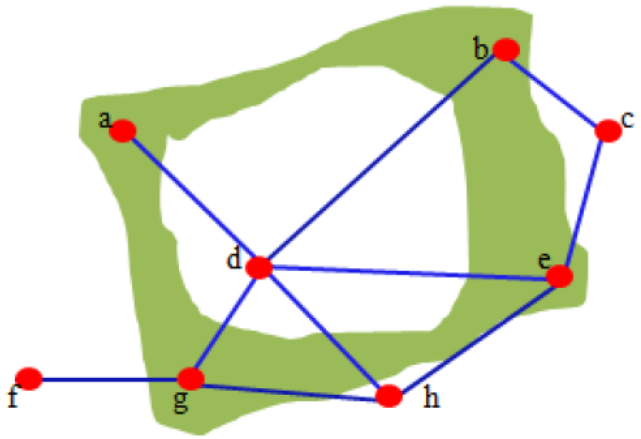


FIGURE 2.9 – L'ensemble stable a, b, e, g.

2.4.4 Ensemble dominant :

Un ensemble dominant d'un graphe $G = (S, A)$ est un sous-ensemble D de l'ensemble S des sommets tel que tout sommet qui n'appartient pas à D possède au moins une arête commune avec un sommet de D. Le problème d'ensemble dominant est de déterminer, en fonction de G et d'un entier naturel k, si G possède un ensemble dominant d'au plus k sommets. Ce problème est $NP - complet$ [3][15].

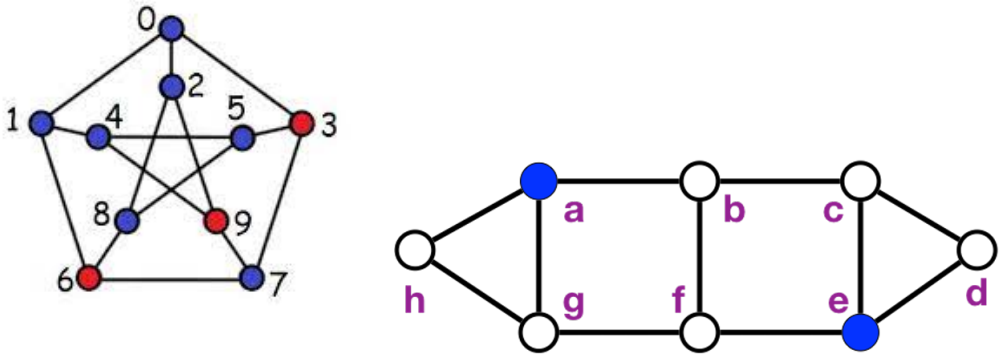


FIGURE 2.10 – Les ensembles dominants (a ,b) (3,9,6).

2.4.5 Définition d'une clique

Dans la théorie des graphes, une clique est un ensemble de sommets deux-à-deux adjacents.

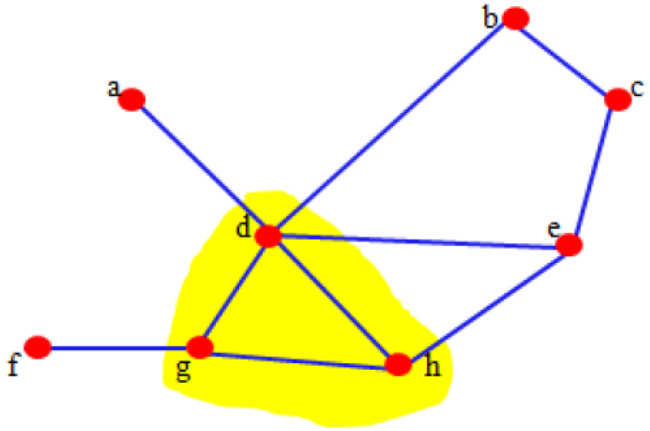


FIGURE 2.11 – La clique d, g, h.

Le graphe G admet 2 cliques d'ordre 3 définies par les ensemble de sommets $d, g, hetd, e, h$.

2.4.6 Coloration des sommets d'un graphe

La coloration des sommets d'un graphe consiste en une affectation de couleurs à tous les sommets du graphe de telle sorte que deux sommets adjacents ne soient pas porteurs de la même couleur.

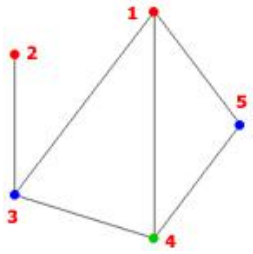


FIGURE 2.12 – La coloration d'un graphe.

2.4.7 Ensemble de sommets de rétroaction :

L'ensemble de sommets de rétroaction est l'ensemble des nœuds dont la suppression rend le graphe en question sans cycle. La rétroaction minimale le problème de sommet consiste à trouver un sommet de retour de cardinalité minimale, noté c, et il est bien connu pour être $NP - Hard$. La pertinence de ce problème se pose dans plusieurs domaines, tels que la suppression des blocages dans un système des processeurs et le placement des convertisseurs dans les réseaux optiques[15].

2.4.8 Nœud et liens critiques

les nœuds et liens critiques représentent l'ensemble des nœuds ou liens importants dans le graphique. En effet, dont la suppression minimise ou maximise, selon le cas, une métrique au sein d'un réseau tel que minimise la connectivité par paires , ou maximise le chemin le plus court entre une paire de nœuds . Les nœuds et liens critiques jouent un rôle essentiel pour maintenir la fiabilité et d'améliorer la sécurité du réseau, ce qui leur permet d'être les acteurs clés des réseaux de communication, sociaux et de transport. Le lecteur est référencé pour une étude complète sur les nœuds critiques et leurs applications.

2.4.9 Communautés

une communauté est souvent définie comme un groupe de membres du réseau avec des liens plus forts avec les membres au sein du groupe qu'avec les membres à l'extérieur du groupe, ce qui induit une organisation des nœuds en clusters. Cela permet la détection de communauté pour être un outil très efficace dans les réseaux complexes analyse, dans laquelle il permet de résoudre efficacement de nombreux problèmes tels que diffusion de l'information et recommandation. Communautés de détection est un problème très difficile pour lequel nous avons de nombreuses approches telles que la hiérarchie clustering , partitionnement de graphes et algorithmes de division tels que Algorithme de *GirvanetNewman* .

2.4.10 Remarque :

A noter que dans les graphes pondérés, on prend en compte les poids des nœuds ou coûts de bords dans le calcul de la valeur optimale du paramètre. En tant que tel, le l'ensemble indépendant maximum et l'ensemble dominant minimum deviennent le poids maximum ensemble indépendant et ensemble dominant de poids minimum, respectivement.
Nous avons vu précédemment que presque tous les problèmes d'optimisations des paramètres des graphes déterminants sont $NP-complets$ même pour les graphes non pondérés. Dans un tel dernier cas, les problèmes associés sont dits fortement $NP-difficiles(SNPH)$.
Ci-après, nous fournissons la complexité de calcul des paramètres susmentionnés problèmes d'optimisation, pour différentes classes de graphes, pour mettre en évidence les défis et les difficultés liées à de tels problèmes même pour des classes de graphes spécifiques restreintes[16].

Parameters	Planar	Perfect	Bipartite	Chordal	Split	Interval	Trees
Independence number	SNPC[53]	P [45, 84]	P	P	P	P	P
Matching number	P [62]	P	P [34]	P [37]	P	P [4]	P
Domination number	SNPC [54]	SNPC [36]	SNPC [13]	SNPC [17]	SNPC [13]	P [17]	P [29]
Feedback vertex set	SNPC [100]	P	P [112]	P [35]	P	P [91]	trees are without cycles
Chromatic number	SNPC[52]	P [57]	2	P	P	P	2
Clique number	P [54]	P [57]	2	P	P	P	2

FIGURE 2.13 – Graph parameters reviewing for different graph classes.

On peut déduire la valeur de certains paramètres en fonction des relations existantes entre les différents paramètres du graphique (par exemple, le nombre minimal d'ensembles de sommets peut être obtenu directement à partir du nombre d'indépendance en utilisant la relation : $(G) = n - (G)$). Cependant, certaines relations ne sont valables que pour un graphe particulier classes, telles que le nombre de clique (G) qui peut être déduit de Chromatic

nombre $x(G)$, uniquement pour les graphes parfaits, en utilisant la relation $(G) = x(G)$.

Une telle déduction n'est pas correcte dans les graphes planaires, pour lesquels le nombre chromatique le problème reste NP-complet et le problème du nombre de cliques est polynomial résoluble . Pour plus de détails sur les relations des paramètres du graphe.

2.5 Qu'est-ce qu'un réseau

Un réseau est un ensemble d'entités (objets, personnes, . . . etc.) inter-connectées les unes avec les autres par des liaisons qui permettent la circulation d'un flux entre les entités[123] :

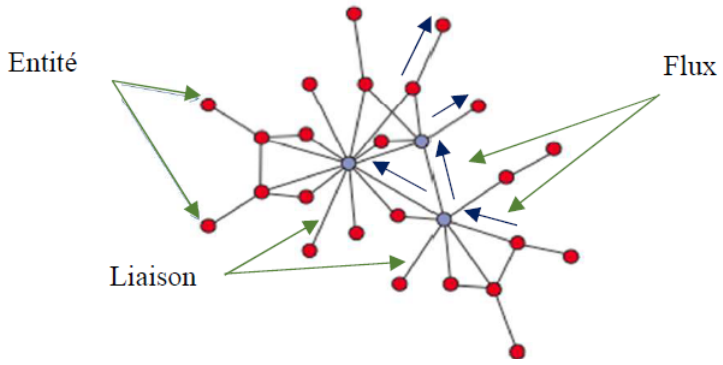


FIGURE 2.14 – Représentation formelle d'un réseau sous forme de graphe.

Les réseaux sont représentés formellement par ce qu'on appelle un graphe constitué d'un ensemble de noeuds, les entités dans notre cas, reliés par des arrêtes, qui sont les liaisons entre les entités dans notre cas.
Les graphes sont une structure de données très efficace pour représenter et manipuler toute sorte de réseau, et toute étude théorique d'un réseau ou d'un phénomène qui se procure au sein d'un réseau est avant tout une étude sur les graphes. Exemple : la recherche du meilleur chemin à emprunter par un paquet de données pour atteindre un serveur le plus rapidement possible n'est que la recherche du plus court chemine sur le graphe représentant le réseau en question. Aussi, dans un réseau informatique, la recherche du routeur par lequel passe le plus grand flux de données ce n'est que la recherche du noeud central du graphe représentant le réseau[123].

2.6 Différents types de réseaux

Plusieurs critères peuvent être considérés dans la classification des réseaux. Selon le type de liens entre les entités, on a des réseaux filaires et des réseaux sans fils. Selon le type d'entité, on a :

2.6.1 Réseau de transport :

c'est un ensemble d'infrastructures (stations, aéroports, etc.) interconnectées par des lignes de transport (routes, voies aériennes, etc.) permettant de transporter des personnes et

des biens entre plusieurs zones géographiques.

FIGURE 2.15 – Réseau de transport aérien de l'Amérique du nord.

2.6.2 Réseau électrique :

c'est un ensemble d'équipements électriques (ex. centrales électriques, pylônes électriques, composantes électroniques, etc.) interconnectées par des câbles permettant d'acheminer l'énergie électrique.

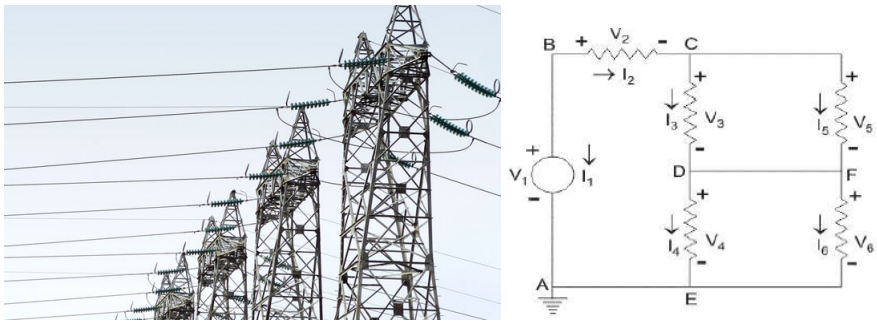


FIGURE 2.16 – Un réseau électrique.

2.6.3 Réseau social :

c'est un ensemble d'identités sociales (individus ou organisations) reliées entre elles par des liens créés lors d'interactions sociales. Le Réseau social en ligne est un réseau social sur internet. Un réseau social permet de circuler tout type d'entités (information, idée, maladie, etc.) qui peut transiter d'une personne à une autre.

2.6.4 Réseau informatique :

un ensemble d'ordinateurs reliés entre eux par des liaisons filaires ou sans fil, et échangeant des informations sous forme de données numériques.

FIGURE 2.17 – Réseau social d'une famille et les réseaux sociaux en ligne.

FIGURE 2.18 – Le réseau informatique ou le réseau de données.

En général, là où il y a un ensemble d'objets avec une interaction entre eux on peut parler de réseau. Dans ce module on s'intéresse aux réseaux informatiques.

2.7 Classification des réseaux

Plusieurs paramètres peuvent être considérés dans la classification des réseaux, et le paramètre le plus répandu est la « taille du réseau ». Selon leurs tailles, on a quatre types de réseaux : PAN, LAN, MAN, WAN.

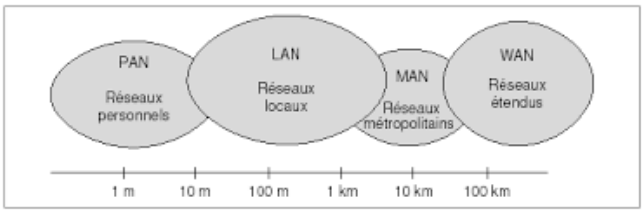


FIGURE 2.19 – Les types de réseau.

2.8 Topologies des réseaux

Pour pouvoir utiliser un réseau, il ne suffit pas de brancher le matériel aléatoirement. Il faut définir, en plus du type de réseau, une méthode d'accès entre les ordinateurs ce qui permettra de connaître la manière dont les informations sont échangées.
Il existe deux types de topologies : topologie physique et topologie logique [15].

2.8.1 La topologie physique :

elle définit la disposition du matériel physique du réseau,On distingue généralement les topologies suivantes : Topologie en bus, Topologie en étoile, Topologie en anneau, Topologie en arbre, Topologie en maillée.

2.8.1.1 Topologie en bus :

Une topologie en bus est l'organisation la plus simple d'un réseau. En effet, dans une topologie en bus tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câble, généralement coaxial. Le mot « bus » désigne la ligne physique qui relie les machines du réseau.

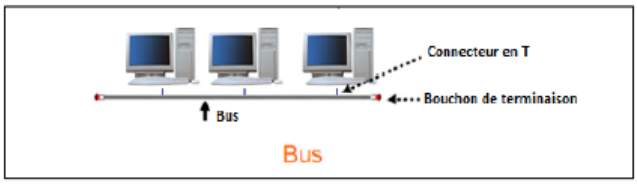


FIGURE 2.20 – Topologie en bus.

2.8.1.2 Topologie en étoile :

Dans une topologie en étoile, les ordinateurs du réseau sont reliés à un système matériel central appelé concentrateur (en anglais hub, littéralement moyen de roue). Il s'agit d'une boîte comprenant un certain nombre de jonctions auxquelles il est possible de raccorder les câbles réseau en provenance des ordinateurs. Celui-ci a pour rôle d'assurer la communication entre les différentes jonctions[15].

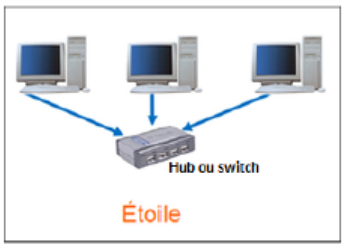


FIGURE 2.21 – Topologie en étoile.

2.8.1.3 Topologie en anneau :

Dans un réseau possédant une topologie en anneau, les ordinateurs sont situés sur une boucle et communiquent chacun à leur tour.

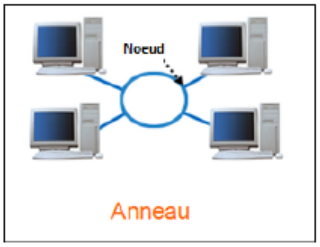


FIGURE 2.22 – Topologie en anneau.

2.8.2 Topologie logique :

Une topologie logique est une structure logique d'une topologie physique. Elle définit comment la communication se passe. Il en existe deux principales Ethernet, Token Ring.

2.9 Conclusion

Dans ce chapitre nous avons donné une brève introduction sur les concepts de base de la théorie des graphes et qui seront utile pour représenter des réseaux .

CHAPITRE 3

SMART CITY

3.1 Introduction

Pour d'atteindre notre objectif on appliquant l'algorithme de domination sur le système, on va proposer un environnement «Smart building » considérer les building comme des nœud contient les firewalls et les arcs c'est le lien entre eux.
Dans ce chapitre, nous allons présenter une vue générale et les composant des smart city .

3.2 Smart city

3.2.1 Définition

Une ville intelligente (en anglais smart city) est une ville utilisant les technologies de l'information et de la communication (TIC) pour améliorer la qualité des services urbains ou réduire leurs coûts. D'autres termes ont été utilisés pour des concepts similaires : ville connectée, cyberville, ville numérique, communautés électroniques.
Une ville intelligente est une zone urbaine qui utilise différents capteurs électroniques de collecte de données pour fournir des informations permettant de gérer efficacement les ressources et les actifs. Cela comprend les données collectées auprès des citoyens, des dispositifs mécaniques, des actifs, traitées et analysées pour surveiller et gérer les systèmes de circulation et de transport, les centrales électriques, les réseaux d'approvisionnement en eau, la gestion des déchets, les systèmes d'information, les écoles, les bibliothèques et les hôpitaux [12].

3.2.2 Les composants essentiels de la smart city

La Smart City, ou ville intelligente, consiste précisément à optimiser les coûts pour garantir un meilleur bien-être aux habitants de la ville.
Les smart city reposent sur le principe d'interconnexion des données et sont hautement dépendantes de la technologie.
Voici 6 classes de technologies indispensables à la Smart City auxquelles nous devons continuer à former toujours plus de talents pour avoir une chance de voir nos projets de Smart

City aboutir et se multiplier [13].

3.2.3 Les technologies d'information et de communication (TIC)

Les technologies de l'information et de la communication construisent un pont entre les citoyens et le gouvernement de sorte à ce que les citoyens puissent communiquer avec le gouvernement et que celui-ci puisse construire une ville selon les souhaits de la volonté générale.
Ces technologies aident les gouvernements à analyser la structure de la demande pour créer un pool de ressources et être en mesure d'adresser ces demandes.
La communication permet donc à la communauté de créer une intelligence collective pouvant être déployée pour l'optimisation des ressources.

3.2.4 Internet of Things (IoT)

L'IoT est à la base de la structure d'une ville intelligente pour interconnecter tous les dispositifs entre eux. Chaque appareil faisant partie d'une smart city requiert d'être connecté à tous les autres afin de permettre une communication permanente pour pouvoir prendre des décisions sans intervention humaine, et garantir ainsi la gestion des ressources de la population d'une métropole.
L'IoT fournit ici un modèle parfait pour permettre la communication des appareils entre eux et fournir des solutions intelligentes aux problèmes quotidiens d'une ville.

3.2.5 Les capteurs

Les capteurs sont des composants omniprésents dans le paysage urbain. Ces derniers sont par ailleurs cruciaux dans n'importe quel système de contrôle intelligent. Un process s'améliore avant tout sur la base de son environnement.
Les capteurs permettent de convertir les paramètres physiques en signaux électroniques pour les rendre interprétables aussi bien par les humains que par des systèmes autonomes : lumière, pression, température, humidité, moisissure, et de

nombreux autres paramètres peuvent désormais être mesurés par nos capteurs pour nous permettre d'avoir une meilleure connaissance de nos environnements et adapter chaque décision en fonction des différents signaux[14].

3.2.6 L'intelligence artificielle (IA)

La quantité massive de données nécessite l'utilisation de l'intelligence artificielle pour permettre des interactions machine-to-machine.
L'AI permet par exemple de déterminer dans quelles situations les hausses de consommations énergétiques se produisent afin d'améliorer la gestion d'un réseau de distribution. Elle joue également un rôle dans la régulation intelligente du trafic.

3.2.7 l'implémentation de l'environnement

Dans ce chapitre nous avons proposé un environnement qui est un groupe de bâtiments intelligents ´´*smartbuilding*ˇ à fin d'appliquer notre algorithme sur cet ensemble.
Les smart buildings sont des bâtiments durables à haute efficacité énergétique qui, de par leur conception, leurs installations et leurs équipements connectés, sont gérés de manière efficiente et offrent une multitude de services à leurs occupants [14].

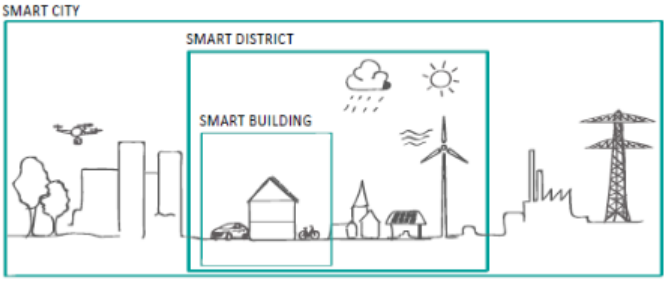


FIGURE 3.1 – Hiérarchisation -smart building– Smart district – Smart city

Les smart buildings sont des bâtiments durables à haute efficacité énergétique qui, de par leur conception, leurs installations et leurs équipements connectés, sont gérés de manière efficiente et offrent une multitude de services à leurs occupants.
Dans ces bâtiments, l'occupant est littéralement au centre des préoccupations : les installations communiquent entre elles, avec les occupants, mais aussi avec l'environnement du bâtiment. Elles assurent ainsi la gestion du confort intérieur (contrôle de la température, de l'éclairage, etc.), de la performance énergétique (optimisation de la gestion du chauffage, du refroidissement, etc.), de la mobilité (réservation de places de parking, gestion de la charge des véhicules électriques, etc.).
Ces installations permettent également un suivi du bâtiment tout au long de sa vie (suivi de l'entretien du système de ventilation, de la chaudière, etc.).
Mais pour ce faire, les constructions et leurs installations doivent pouvoir communiquer avec de multiples équipements et environnements, propres ou non au bâtiment [14].

3.2.7.1 Vers des bâtiments prêts au service (R2S)

Face au défi de communication des smart buildings, un concept de bâtiment 'prêt au service' (Ready to Service – R2S) apparaît, notamment en France. L'objectif de ce concept est de garantir la capacité des bâtiments, quelle que soit leur typologie (résidentiel, tertiaire, industriel, etc.), à communiquer sans limitation technologique. Ce concept est notamment parti du constat que, dans bien des cas, les écosystèmes et matériels communicants intégrés au bâtiment bénéficient de protocoles de communication propres non interopérables.
Un exemple type de cette non-interopérabilité est l'impossibilité d'utiliser les données issues des capteurs de gestion des systèmes de protection solaire. Très souvent, ces données sont inexploitables par d'autres systèmes nécessitant la même information, comme c'est par exemple le cas de la gestion de l'éclairage artificiel en fonction de l'apport d'éclairage naturel.
Pour permettre cette connectivité tout en protégeant l'échange de données, une architecture à trois niveaux (matériel, infrastructure 'réseau' et services est utilisée :

- niveau des équipements (également dénommés écosystèmes), tels que capteurs, actionneurs et contrôleurs des systèmes intégrés au bâtiment : ceux-ci doivent pouvoir communiquer avec la couche 'réseau' du bâtiment (niveau 2).

- niveau de l'infrastructure 'réseau' : c'est par cette couche que communiquent tous les équipements ; elle met en relation les équipements et les services.

- niveau des services : il s'agit de la couche applicative de stockage et de traitement des données. Les données du bâtiment y circulent généralement dans le Cloud. Leur disponibilité doit permettre l'émergence des services aux utilisateurs tant à l'intérieur qu'à l'extérieur du bâtiment.

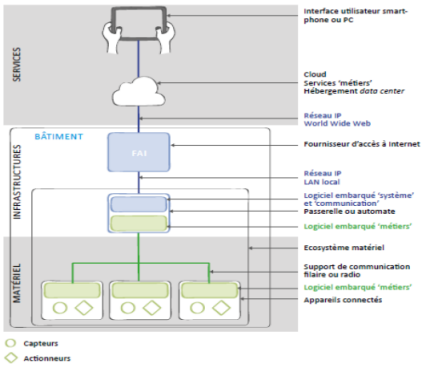


FIGURE 3.2 – Architecture d'un bâtiment prêt au service (R2S)

3.2.7.2 De nouveaux usages et services

Les bâtiments sont désormais considérés, non plus comme une simple enveloppe protectrice, mais comme un réel fournisseur de services (Building as a Service – BaaS).
Les applications et services possibles sont innombrables : maintenance des installations techniques et alarme, gestion de la sécurité et du confort des personnes, maintien des personnes âgées à domicile, gestion des places de parking, optimisation des consommations énergétiques et limitation des puissances, etc. De son côté, la Smart Building Alliance (SBA) distingue six familles de services.
Le rôle des différents acteurs, dont ceux du secteur de la construction en général et des entrepreneurs en particulier, reste cependant à définir. L'essor des smart buildings implique l'installation de produits compatibles qui peuvent nécessiter d'adapter les méthodes de travail existantes, mais également de mettre en place des processus neufs Par exemple, les vitrages dynamiques réagissant à leur environnement et aux demandes de l'occupant nécessiteront toujours d'être installés avec leur menuiserie dans les bâtiments comme n'importe quelle autre menuiserie. Des éléments comme l'information des clients, L'éventuelle compatibilité avec d'autres systèmes du bâtiment, les aspects de raccordement, voire de maintenance constituent de nouveaux éléments qu'il convient de prendre en compte.
Un facteur central dans l'essor des bâtiments intelligents est celui des modèles d'entreprise qui y seront associés et qui offriront une justification économique à leur développement.

FIGURE 3.3 – familles de services selon la smart Buildinn Alliance

3.3 Conclusion

Dans ce chapitre,nous allons présenter une vue générale et les composant des smart citys.Ensuite, dont le chapiter suivant on va décrivons notre environnement de travail.

CHAPITRE 4

SIMULATION ET LA MODÉLISATION

4.1 Introduction

Dans certaines situations on va appliquer des algorithmes d'optimisation, l'objectif vise à déterminer la solution la plus avantageuse peut correspondre à la valeur la plus élevée, et d'un moins cout.
Dans ce chapitre, nous allons présenter la partie de la simulation et la modélisation qui consiste à mettre en place une solution qui permet de réduire le cout d'installation des firewalls dans un environnement IoT.
Pour d'atteindre notre objectif on appliquant l'algorithme de domination sur le système, on va proposer un environnement «Smart building » considérer les building comme des nœud contient les firewalls et les arcs c'est le lien entre eux.
Afin de tester notre algorithme on va faire une simulation qui est une technique de modélisation du monde réel, les outils qu'on va utiliser c'est le Netbeans comme environnement de développement, et langage de programmation java.

4.2 Principe généraux de la simulation

Etymologiquement, le terme "simulation" est dérivé du mot latin ´*SIMULARE*ˇ qui veut dire : copier, feindre, faire paraître comme réelle une chose qui ne l'est point. Ainsi, la simulation peut être définie comme suit [16] :

4.2.1 C'est quoi la simulation ?

La simulation est l'expérimentation sur un modèle. C'est une procédure de recherche scientifique qui consiste à réaliser une reproduction artificielle (modèle) du phénomène que l'on désire étudier, à observer le comportement de cette reproduction lorsque l'on fait varier expérimentalement les actions que l'on peut exercer sur celle-ci, et à en induire ce qui se passerait dans la réalité sous l'influence d'actions analogues [16].

On peut donc dire que simuler le fonctionnement d'un système c'est imiter son fonctionnement au cours du temps en manipulant un modèle. Ceci est équivalent à la génération d'un historique des changements d'état du système, et à l'observation de cet historique pour

faire des déductions sur les caractéristiques de fonctionnement du système. C'est donc une méthodologie essentiellement pratique qui permet de modéliser aussi bien des systèmes conceptuels (qu'on veut concevoir) que des systèmes existants déjà. Elle peut être utilisée pour [16] :

- Décrire et analyser la dynamique d'un système.

- Aider à la conception d'un système réel.

4.2.2 Pourquoi simuler ?

Généralement, la simulation assure :
-Une évaluation des performances du system.
-Un contrôle ou une optimisation du système : estimer l'influence des facteurs les plus significatifs pour garantir les performances exigées du système.
-Une comparaison des scenarios : comparer différentes conceptions, stratégies, politiques et règles de fonctionnement.

4.3 Smart building pour la simulation

La "smart building" pour la simulation et pour la modélisation :

FIGURE 4.1 – Smart city(Exmple)[21]

4.3.0.1 La modélisation du Smart building

La modélisation du smart building par graphs :

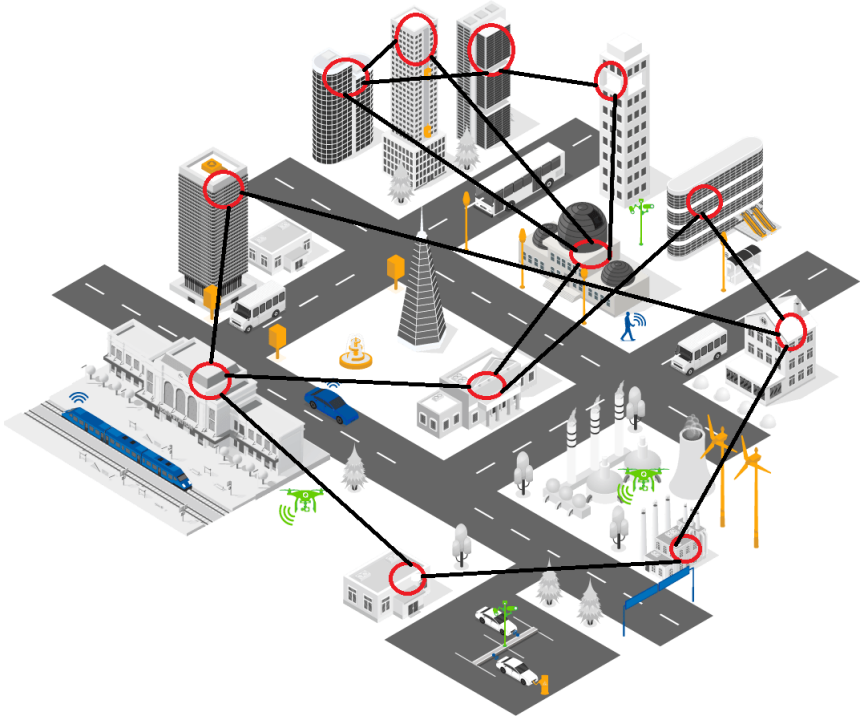


FIGURE 4.2 – La modélisation Smart building[21]

Smart city − − − − − −− >>graphs $G(x,u)$ tel que : chaque sommet représente un bâtiment ou une maison. chaque arc représente la relation entre les sommet (câble, wifi,. . . . .). donc le résulta un graphe $G(x,u)/(x = sommt, u = arc)$.

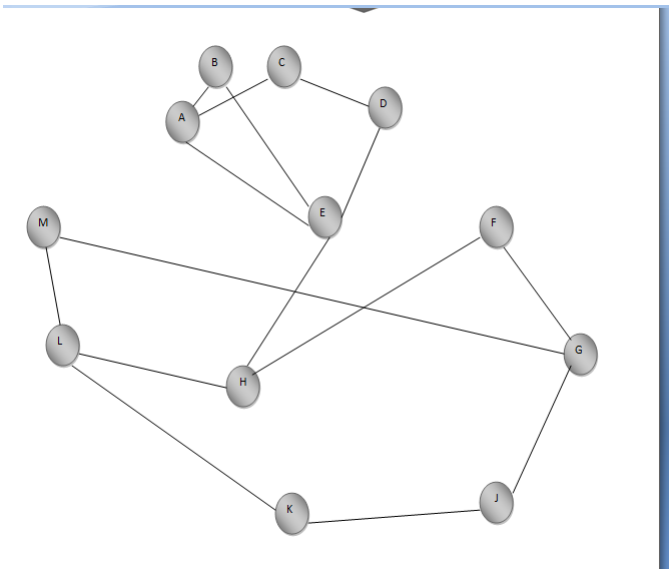


FIGURE 4.3 – Graphs $G(X,U)$

4.4 Algorithm pour la simulation

Il existe plusieur algorithme pour la resolution de ce probleme, Nous avons développé un algorithme qui permet de minimiser le nombre de firewall dans un environnement IoT utilisant l'algorithme de domination. L'approche proposée avait pour objectif de :

- Réduire le nombre des firewall dans un réseau IoT donc réduire la complexité.

- Garantir la sécurité de réseau contre les attaques.

```
Algorithme

Débuts :
Si <graphes (G, v) == non orientés> alors

1-Classer les sommet par ordre croissant ;

2-List L()=TOUTS LES SOMMET GRAPHS(G,V) ;

3-chosé sommet= x ;    // x par l'ordre des sommet .

4-L'() liste =vide H()liste=vide ;

5-Ajouter les voisent du sommet x dans L'()+Ajouter sommet x dans H().

   If( L'()==L())alors{

    Afficher (H()); }

Else{

Allez étape 3 ;}

Fin
```

FIGURE 4.4 – Algorithm Ensemble dominant pour la simulation

4.4.1 l'algorithme Ensemble dominant

On $graphsG(x, u)$:
tel que :$xA, B, C, D, E, F, G, H, J, K, L, M$ et $uu1(A - B), u2(A - C)$, ... graphs $G(x, u)$ non oriente−− >donc :

- Etaps 1 : Classer les sommet par ordre croissant.

SOMMRT	E	A	L	G	H	D	F	B	J	K	M	C
DEGRE	3	3	3	3	3	2	2	2	2	2	2	2

FIGURE 4.5 – Etpa 1

- Etap 2 :List $L(A, B, C, D, E, F, G, H, J, K, L, M)$;

- Etap 3 :Sommet $X = E$ et $L'A, B, D, H$ et HE

- $L'()$!=$L()$ donc aller etap 3 : Sommet $X = L$,$L'(A, B, D, H), M, K$

- $L'()$!=$L()$ donc aller etap 3 : Sommet $X = G$,$L'(A, B, D, H), (M, K), F, J$

- $L'()$!=$L()$ donc aller etap 3 : Sommet $X = C$,$L'(A, B, D, H), (M, K), (F, J)$

DONC l'ensemble dominant graphs $G(x, u)$ sont (E, L, G, C)

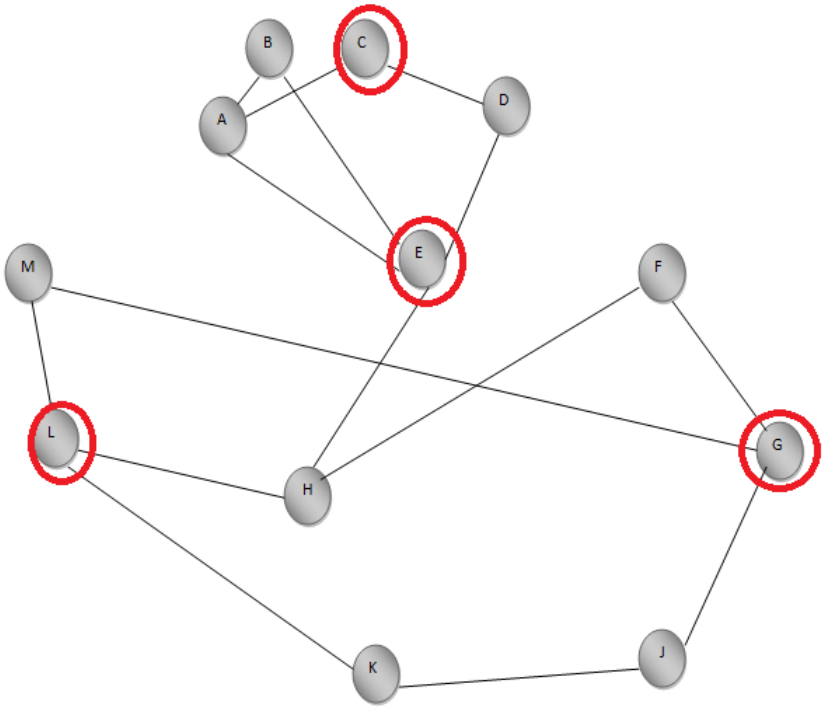


FIGURE 4.6 – l'ensemble dominant (E, L, G, C)

4.4.1.1 La représentation du l'algorithme

La représentation graphique sur le simulateur :

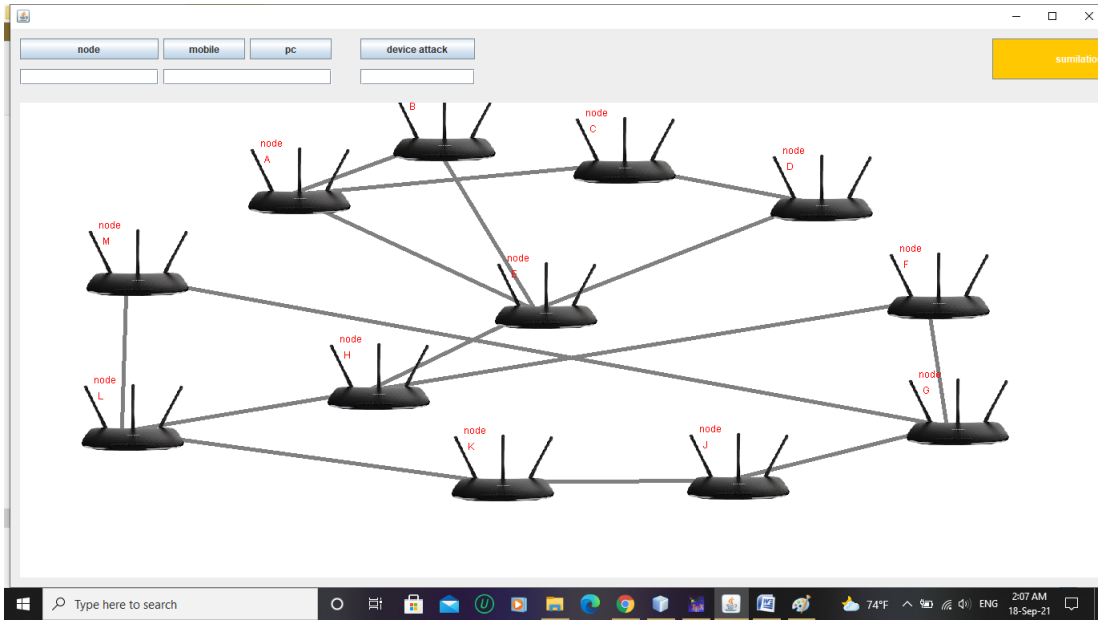


FIGURE 4.7 – Application sur simulateur

4.4.1.2 L'application du l'algorithme

L'application du l'algorithme domian sur le simulateur :

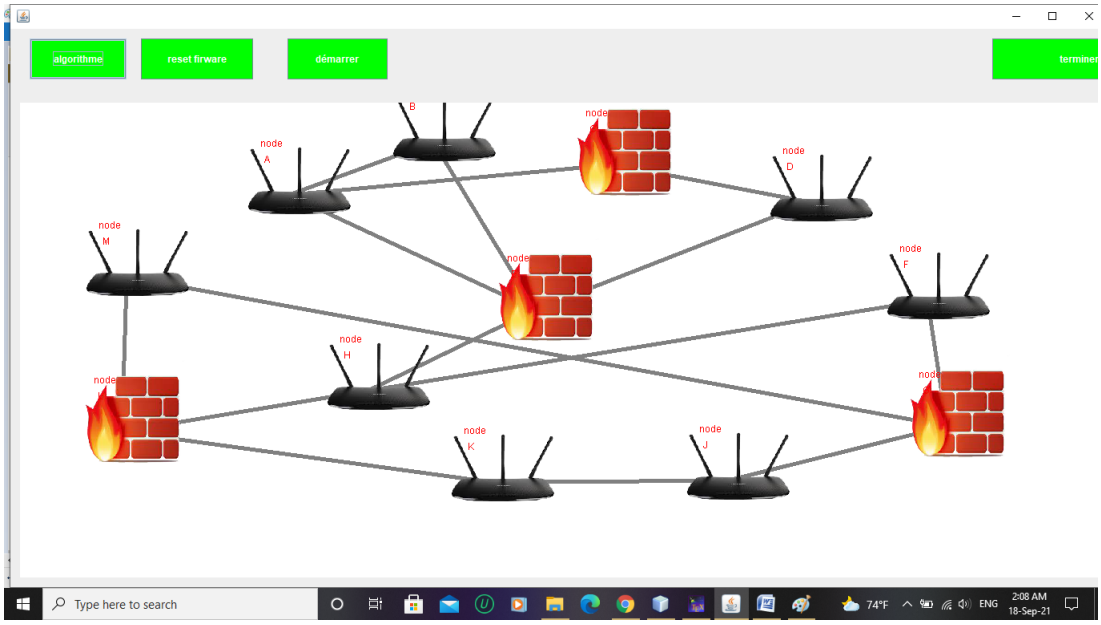


FIGURE 4.8 – l'ensemble dominant sur la simulateur

4.4.1.3 Attaque hacker

Les attaques représentent les moyens d'exploiter une vulnérabilité. Ils s'appuient sur divers types de faiblesses telles que les faiblesses des protocoles, faiblesses d'authentification, faiblesses d'implémentation ou bogues et les Mauvaises configurations.

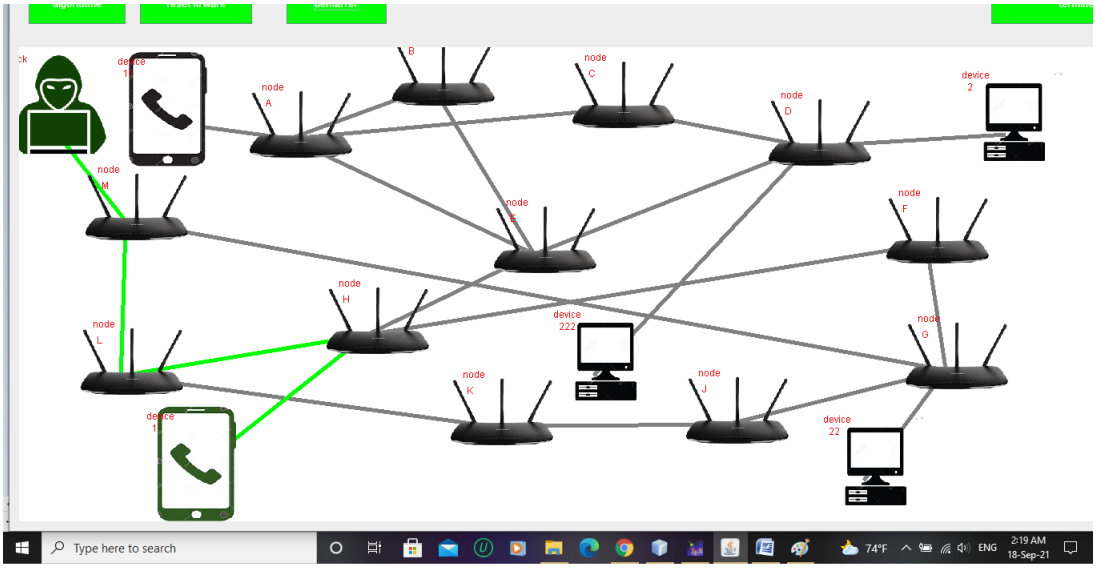


FIGURE 4.9 – Attaque haker

4.4.1.4 Objectifs de la sécurité

La sécurité vise à assurer plusieurs propriétés :

- **La confidentialité :** C'est la propriété qui garantie que les informations transmises ne sont compréhensibles que par les entités autorisées.

- **l'authentification :**L C'est la propriété qui consiste à vérifier l'identité d'un utilisateur avant de lui donner l'acccès à une ressource.

- **L'intégrité :** C'est la propriété qui consiste à vérifier si les informations n'ont pas été modifiées durant la transmission.

- **La disponibilité :** c'est la propriété qui permet de garntir l'accès aux données.

Pour des raisons de sécurité, on utilise l'algorithme dominain pour placer des pare-feu sur les nœuds et éviter les attaques.
L'application de l'algorithme dominant, permet de trouver la solution optimale d'un réseau complexe avec un nombre minimum des firewalls pour bloquer les attaques de l'extérieur.

Les appareils doivent être connectés dans la même zone afin de pouvoir communiquer entre eux.

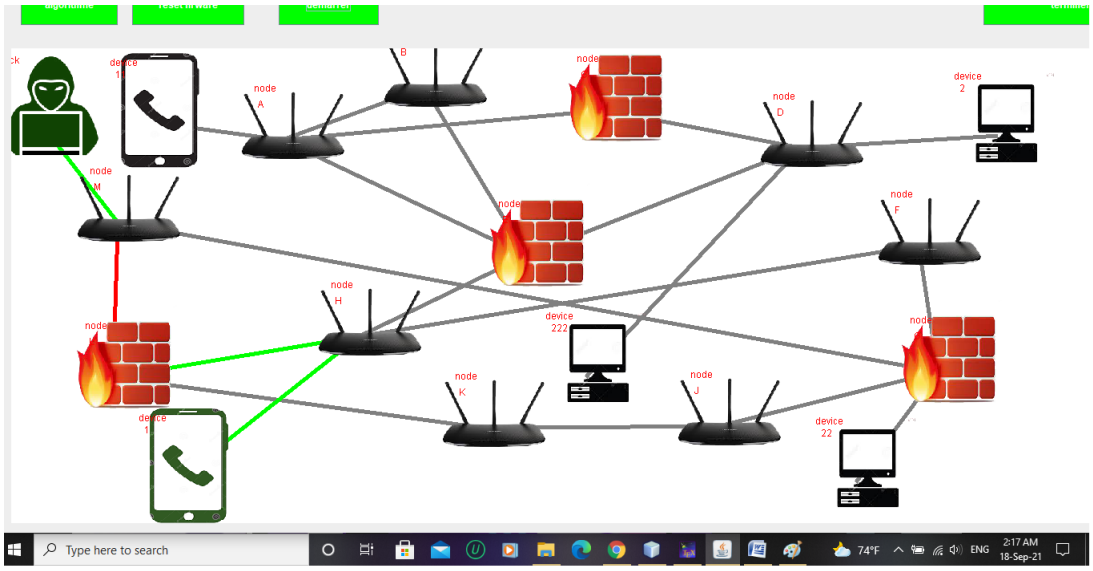


FIGURE 4.10 – Empêcher les attaques de pirates

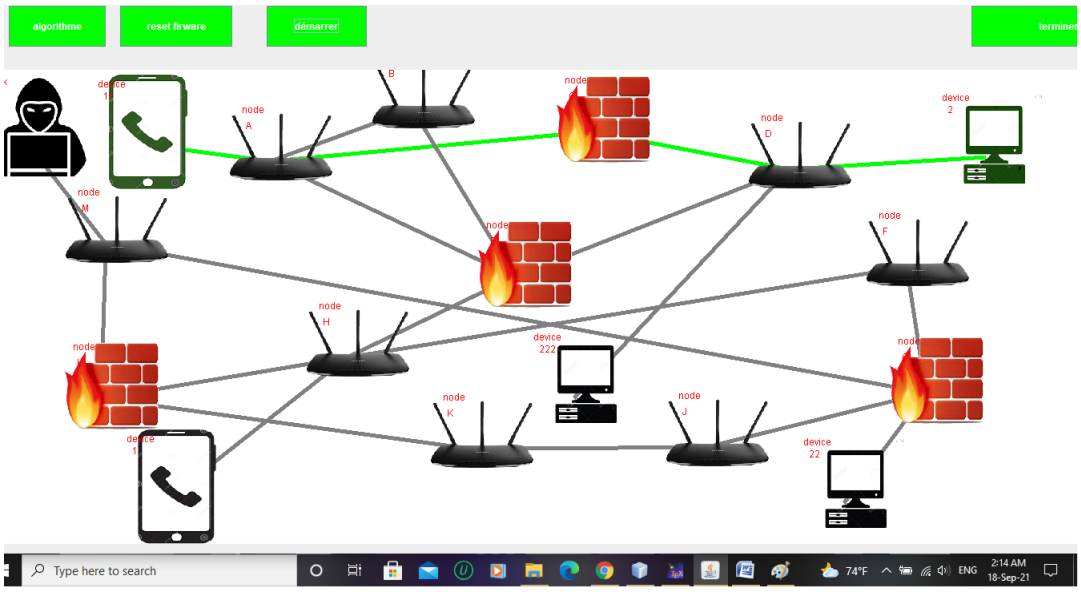


FIGURE 4.11 – téléphone et pc connectés dans la même zoner

4.5 Outils de travail

4.5.1 L'environnement de développement

NetBeans est un environnement de développement intégré (EDI), placé en open source par Sun en juin 2000 sous licence CDDL (Common Development and Distribution License) et GPLv2. En plus de Java, NetBeans permet la prise en charge native de divers langages tels le C, le C++, le JavaScript, le XML, le Groovy, le PHP et le HTML, ou d'autres (dont Python et Ruby) par l'ajout de greffons. Il offre toutes les facilités d'un IDE moderne (éditeur avec coloration syntaxique, projets multi-langage, refactoring, éditeur graphique d'interfaces et de pages Web).

Compilé en Java, NetBeans est disponible sous Windows, Linux, Solaris (sur x86 et SPARC), Mac OS X ou sous une version indépendante des systèmes d'exploitation (requérant une machine virtuelle Java). Un environnement Java Development Kit JDK est requis pour les développements en Java.

NetBeans constitue par ailleurs une plateforme qui permet le développement d'applications spécifiques (bibliothèque Swing (Java)). L'IDE NetBeans s'appuie sur cette plate forme.

L'IDE Netbeans s'enrichit à l'aide de greffons.
NetBeans comprend les fonctions générales suivantes :

- configuration et gestion de l'interface graphique des utilisateurs,

- support de différents langages de programmation,

- traitement du code source (édition, navigation, formatage, inspection..),

- fonctions d'import/export depuis et vers d'autres IDE, tels qu'Eclipse ou JBuilder.

4.6 Les langages de programmations

4.6.1 JDK

Le Java Development Kit (JDK) désigne un ensemble de bibliothèques logicielles de base du langage de programmation Java, ainsi que les outils avec lesquels le code Java peut être compilé, transformé en bytecode destiné à la machine virtuelle Java.

Il existe plusieurs éditions de JDK, selon la plate-forme Java2 considérée (et bien évidemment la version de Java ciblée) :

JSE pour la Java 2 Standard Edition également désignée J2SE ;
JEE, sigle de Java Enterprise Edition également désignée J2EE ;
JME 'Micro Edition', destinée au marché mobiles .

À chacune de ces plateformes correspond une base commune de Development Kits, plus des bibliothèques additionnelles spécifiques selon la plate-forme Java que le JDK cible, mais le terme de JDK est appliqué indistinctement à n'importe laquelle de ces plates-formes.

4.6.2 Le langage java

Java est un langage de programmation orienté objet créé par James Gosling et Patrick Naughton de Sun Microsystems. Le langage Java a été introduit par la société SUN en 1995. Il possède de nombreuses caractéristiques parmi lesquelles on peut citer :

- JAVA fonctionne comme une machine virtuelle (Indépendant de toute plateforme).

- JAVA est simple (pas de pointeur).

- JAVA autorise le multitâche (multithreading).
- JAVA peut être utilisé sur INTERNET.
- JAVA contient une très riche bibliothèque de classes(Packages) qui permettent de :
  - Créer des interfaces graphiques.
  - Utiliser les données multimédia.
  - Communiquer à travers les réseaux. . . etc.

4.7 Conclusion

Dans ce chapitre, nous avons présenté une vue sur la simulation. Nous avons aussi présenté les différents outils et langages de programmation utilisés pour le développement de notre application. Enfin, nous avons a ajouté quelques interfaces pour illustrer le fonctionnement de notre application Tout en expliquant le déroulement des scénarios de simulation.

CONCLUSION GÉNÉRALE

Dans ce projet, Nous avons abordé le problème d'optimisation réseau dans un environnement IoT. Les objets sont connectés avec la technologie de l'information et de la communication, nous avons présenté les différentes technologies de l'IoT et la méthode utilisée pour protéger ces objets connectés nous nous sommes concentrés sur les firewalls, la théorie des graphes nécessaires pour l'analyse des réseaux complexes, ainsi nous avons donné un résumé sur les problèmes d'optimisation et leurs méthodes de résolution.
Dans notre projet nous avons proposé une solution du problème posé qui est de développer un système qui permet d'optimiser la complexité des graphes contre les attaques.
Nous avons développé un algorithme qui permet de minimiser le nombre des firewalls dans un environnement IoT et assurer la performance de sécurité contre les attaques.
Notre projet est mis en œuvre comme suit : Nous avons d'abord découverts nœuds dans le réseau et appliqué le lien entre ces nœuds, deuxièmement la simulation, nous avons implémenté notre algorithme et blocage des attaques. Réaliser la simulation ce fait par langage Java qui contient des packages facilite le déroulement de travaille.
L'application de notre algorithme, permet de faire la simulation des graphes dans un réseau complexe et trouver la solution optimale avec le nombre minimum des firewalls pour bloquer les attaques de l'extérieur. Le choix de nœud à protéger est assuré par l'application de l'algorithme de domination. Et avec ca, l'application reste incomplète, nous mentionne ces lacunes dans les perspectives.
Notre solution reste évolutive comme projet de future avec l'inclusion des adresses Ip et les paramètres de sécurité.

Perspective

Le travail que nous avons présenté dans ce projet peut être étendus et développé dans le futur.

Nous avons fait la première étape, qui est de mettre en place une stratégie pour déterminer l’ensemble dominant à pour but de réduire le nombre des dispositifs de protection dans un domaine IoT.

L'un des points les plus importants que nous n'avons pas pu aborder dans ce projet est :

- ✓ La configuration et le routage des objets connectés.
- ✓ Mètre en place une stratégie de sécurité pour protégé le réseau.

BIBLIOGRAPHIE

[1] https ://www.djvuzone.org/reseau-iot-de-quoi-sagit/.

[2] https ://www.futura-sciences.com

[3] PRIDA Track 1 (T1) Les fondamentaux de l'IoT 24/08/2020.

[4] https ://azure.microsoft.com/fr-fr/overview/internet-of-things-iot/iot-technology-protocols/ .

[5] les technologies de IoT https ://www.smartgrids-cre.fr/encyclopedie/linternet-des-objets-au-coeur-des-smart-grids/definitions-autour-des-objets-connectes .

[6] Ecole Nationale des Ponts et Chaussées – Thèse Professionnelle Mastère Spécialisé® Ingénierie et Management des Smart Cities Pierre Kassaa 2019.

[7] https ://www.forcepoint.com/fr/cyber-edu/firewall

[8] https ://www.forcepoint.com/fr/cyber-edu/firewall2021.

[9] https ://www.frameip.com/firewall/2021.

[10] Etude et conception d'un firewall Projet de fin d'étude pour l'obtention du diplôme de Master en Réseaux et Télécommunications UNIVERSITÉ SAAD DAHLEB DE BLIDA.

[11] http ://wapiti.enic.fr/commun/ens/peda/options/ST/RIO/pub/exposes.

[12] https ://easypartner.fr/blog/6-technologies-indispensables-a-la-smart-city

[13] https ://www.itaia.fr/internet-des-objets/.

[14] Théorie des Graphes.A.merabet – centre universitaire de Mila – 2020.

[15] Mémoire de Fin de cycle.Option : Administration et Sécurity Réseaux.Simulation d'un pare-feu d'entreprise Cas de SONATRACH de Béjaïa.Promotion 2015/2016.

[16] LALOU Mohammed.Mémoire de Fin d'études Master Filière : Informatique Option : Systèmes informatique.Reconnaissance des motifs dans des graphes EMF.

[17] Etude et réalisation d'une application réseau à base de noeuds critiques.Année universitaire : 2015/2016.

[18] Guettiche Mourad.Thèmel a Détection Des Noeuds Critiques Dans Les Graphes De Puissance (Power Graphs).

[19] https ://web.maths.unsw.edu.au/ lafaye/CCM/initiation/topologi.html.

[20] Decomposition and Domination of Some Graphs Fairouz Beggas.HAL.

[21] https ://www.entelec.eu/fr/solutions/smart-city.

[22] SmartCard Alliance, “Smart Cards and Biometrics,” available to :Consulté le : wwww.smartcardalliance.org , Mars 2011.

[23] «IOT, or InterOperability Testing, in the Age of Cloud, Things DevOps,» 29 Janvier 2015. [En ligne]. Available :http ://labs.sogeti.com/iot-or-interoperability-testing-in-the-age-of-cloud-things-devops/. [Accès le 07 Juillet 2018].

[24] https ://wikimemoires.net/2019/09/domaines-d-applications-de-l-iot/.

[25] https ://www.commentcamarche.net/faq/22304-le-pare-feu-ou-firewall.