REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEURE ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE IBN KHALDOUN - TIARET

MEMOIRE

Présenté à :

FACULTÉ MATHEMATIQUES ET INFORMATIQUE
DÉPARTEMENT D'INFORMATIQUE

Pour l'obtention du diplôme de :

MASTER

Spécialité : Réseaux et Télécommunications

Par :

REGUIEG Sidahmed Lamine

Sur le thème

Etude et Analyse des différentes intrusions réseaux et la détection d'attaque DOS à l'aide des algorithmes d'apprentissage automatique

Soutenu publiquement à Tiaret devant le jury composé de :

Mr. MOSTEFAOUI Kadda	M.A.A Université IBN-KHALDOUN Tiaret	Président
Mr. ALEM Abdelkader	M.A.A Université IBN-KHALDOUN Tiaret	Encadreur
Mr. NASSANE Samir	M.A.A Université IBN-KHALDOUN Tiaret	Examinateur

2019 - 2020

Remerciements

« Louange à Allah qui nous a guidés à ceci. Nous n'aurions pas été guidés, si Allah ne nous avait pas guidés ».

[Sourate 7. Al Araf verset 43]

Je tiens à exprimer mes plus vifs remerciements à ***Monsieur MOSTEFAOUI Kadda*** *pour avoir accepté de présider le jury.*

Ma reconnaissance, et mes sincères remerciements vont à ***ALEM Abdelkader*** *pour m'avoir dirigé tout au long de la réalisation de ce travail. Ses orientations, ses encouragements, sa compréhension, sa disponibilité constante m'ont été d'une précieuse aide.*

Je tiens à remercier également ***Monsieur NASSANE Samir*** *pour avoir accepté d'examiner ce travail et l'enrichir par ses propositions.*

Et enfin, mes sincères remerciements et respects vont aux enseignants qui m'ont enseigné et qui par leurs compétences m'ont soutenu dans la poursuite de mes études.

Dédicaces

J'ai l'honneur de dédier ce modeste travail à mes parents, merci pour les sacrifices que vous avez consentis et les appuis que vous m'avez donnés tout au long de mon cursus et pour la confiance que vous m'avez accordée.

Toute ma gratitude à mes deux frères Aziz et Djallel et à mes trois sœurs Sabrine et Malika, Bissan support quotidien, support émotionnel, support moral, mais avant tout, support inconditionnel de ma vie...

Á mes deux oncles Que Dieu les accueille dans son vaste paradis Ali et Abderrahim, sans oublier bien sûr Nasro et brahim Que Dieu les protège

Á mes camarades et mes amis.

Sidahmed

Résumé

L'Internet des objets (IDO) est l'évolution naturelle de l'utilisation des réseaux, il a pour objectif de rendre le monde réel plus intelligent grâce à la connexion des objets. Ces derniers obtiennent des informations qu'elles transmettent par le réseau. N'importe quel objet autonome qui peut être connecté à Internet et qui peut être utilisé à distance peut être considéré comme un membre de la famille de l'Internet des objets.

De nombreux chercheurs travaillent sur l'Internet des Objets pour fournir une meilleure sécurité, des limitations spécifiques liées aux objets Internet of think (IoT) empêchent l'intégration des solutions de la sécurité traditionnelle dans leur mise en œuvre en raison de leurs ressources limitées telles que la mémoire limitée, le stockage et énergie… les systèmes de détection d'intrusion (IDS) avec les trois catégories principales: anomalie, signature et la détection par spécification ont été un outil populaire pour sécuriser les réseaux IoT.

L'idée principal de ce travail est de proposer un IDS performant en détectant les attaques DOS dans un environnement IoT. Notre approche a montré de bon résultat avec un minimum de fausses alertes et un très bon taux de détection des attaques DOS.

Mots clés : IDS, Iot, DDOS, sécurité, Attaque….

Table des matières

Liste des tableaux

Liste des figures

Liste des abréviations

ACK: Acquittement

DDOS: Distributed denial-of-service

IOT: Internet of Things

6LoPAN: IPv6 over Low -Power Wireless Personal Area Networks

IDS: Intrusion Detection Systems

RFID: Radio-frequency identification

WSN: Wireless sensor network

M2M: Machine to machine

RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks

DIS : Dodag information sollicitation

DIO : Dodag information Object

DAO: Dodag advertisement Object

DODAG: Destination Oriented Directed Acyclic Graph

MQTT: Message Queuing Telemetry Transport

WLAN: Wireless Local Area Network

P2P: Peer-to-Peer

LTE-A: Long Term Evolution—Advanced

Introduction Générale

Introduction générale :

L’internet est devenu une nécessité dans la vie moderne, pour cette raison, les chercheurs ont essayé d'améliorer la vie quotidienne des humains, ou ces derniers n'auront plus besoin de recourir à l'intervention humaine pour fournir des services.

L'internet des objets (IdO), est issue de la convergence des technologies sans fil et des systèmes micro-électromécaniques.

L’IdO en tant qu'une évolution de l'internet actuelle et étant un réseau mondial d'objets interconnectés, elle permet une amélioration considérable de notre mode de vie et la façon dont les objets intelligents dans notre entourage interagissent entre eux et avec leurs utilisateurs.

Ces objets, qui sont considérés comme la plateforme de base de L’IdO basés sur l'utilisation de différents protocoles de communication.

Le terme Internet des objets a été introduit pour la première fois en 1999 par Kevin Ashton.

Cette technologie consiste principalement à connecter des objets avec la technologie RFID (Radio Frequency Identification), une technologie de communication sans fil qui a marqué le début des objets communicants.

Ensuite, de très nombreux protocoles de communication sont apparus tels que Bluetooth, Zigbee, Wi-Fi, Sigfox et LoRa.

Depuis, on assiste à une augmentation importante du nombre d'objets connectés avec des prévisions variables et très impressionnantes selon les différentes sources.

La sécurité de L’IdO reste encore un des problèmes majeurs qui freine l’évolution et le déploiement rapide de cette technologie dû à la multiplication des objets connectés qui deviennent des cibles pour les pirates.

La mise en œuvre de mesures de sécurité est essentielle pour garantir la sécurité des réseaux auxquels sont connectés des dispositifs IdO, ce qui devenu ensuite un objectif pour les chercheurs pour trouver un meilleur mécanisme de sécurité malgré les limitations spécifiques liées aux dispositifs IdO et à la standardisation des technologies de communications.

Parmi les mécanismes développés pour fournir une sécurité optimale dans un environnement IdO, les systèmes de détection d'intrusion (IDS) sont les plus répandus.

Le principal rôle clé d'un système de détection d'intrusion (IDS) est l'analyse et l'interprétation des paquets circulant sur un réseau et détecter toute entrée non autorisée ou toute activité malveillante. Néanmoins, les IDS présentent également certaines faiblesses qui proviennent de leurs qualités : du fait de la grande quantité de données générées. Ils sont très sensibles aux attaques de type DoS, Les IDS souffrent également d'un problème dû à certaines attaques qui peuvent passer inaperçues (faux négatifs) durant la phase d'apprentissage, ou encore de certaines alertes générées, par rapport à des attaques qui n'ont pas eu lieu (faux positif).

Dans ce contexte, notre travail consiste à tester l'efficacité de l'IDS proposé selon sa nature de détection d'intrusion dans un environnement de routage IdO et de proposer un modèle d'un IDS comportementale, et examiner son exactitude de détection qui doit être, enfin, proche de la certitude.

Ce mémoire est constitué de quatre chapitres répartis comme suit :

- Dans Le premier est consacré à la présentation des problèmes de sécurité informatique comme entrée dans le monde attaques et la vulnérabilité …,
- Dans Le deuxième chapitre présente les IDS.
- Ensuite dans le troisième chapitre expose une étude sur l'environnement IdO et les problèmes de sécurité dans L'IdO
- Enfin Le dernier chapitre est consacré à la simulation et l'analyse des résultats obtenues de notre solution proposé.

Chapitre1 : La Sécurité Informatique

Chapitre1 : La Sécurité Informatique

Introduction

En informatique, le terme sécurité recouvre tout ce qui concerne la protection des informations, De nos jours le monde est de plus en plus connecté et son système d'information est accessible de l'extérieur.

Ce chapitre a pour but d'éclaircir les notions fondamentales liées au Sécurité Informatique tels que les définitions, les caractéristiques, les architectures et les domaines d'application.

I - Sécurité Informatique

La sécurité informatique est l'ensemble des moyens mis en œuvre pour minimiser la vulnérabilité d'un système contre des menaces accidentelles ou intentionnelles (Berthomier, E. 2005).

II - Services de la sécurité :

Toujours dans le domaine de l'informatique, le terme sécurité recouvre tout ce qui concerne la protection des informations.

Trois grands concepts ont été définis :

- Les fonctions de sécurité, qui sont déterminées par les actions pouvant compromettre la sécurité d'un établissement ;
- Les mécanismes de sécurité, qui définissent les algorithmes à mettre en œuvre ;
- Les services de sécurité, qui représentent les logiciels et les matériels mettant en œuvre des mécanismes dans le but de mettre à la disposition des utilisateurs les fonctions de sécurité dont ils ont besoin(Pujolle & Salvatori, 2008).

Assurer la sécurité revient alors à assurer les fonctions suivantes :

1 - Confidentialité

La *confidentialité* garantit aux utilisateurs qu'aucune donnée n'a pu être lue et exploitée par un tiers malveillant, les données, les objets et les acteurs de la communication ne peuvent pas être connues d'un tiers non-autorisé.

2 - Authenticité

L'*authentification* consiste à demander à un utilisateur de prouver son identité, L'identité des acteurs de la communication est vérifiée.

3 - Intégrité

L'intégrité assure aux utilisateurs que leurs données n'ont pas été indûment modifiées au cours de la transmission dans le réseau, les données de la communication n'ont pas été altérées.

4 - Non-répudiation

Les acteurs impliqués dans la communication ne peuvent nier y avoir participer, la *non-répudiation* empêche un utilisateur de nier la réalité d'un échange de données.

5 - Disponibilité

Les acteurs de la communication accèdent aux données dans de bonnes conditions. (Cousin, n.d.)

III - Menace sur les réseaux :

1 - Vulnérabilité :

Internet est une mine d'informations pour les entreprises et pour les utilisateurs. En naviguant sur Internet, on peut accéder à des millions de pages Web. A l'aide de moteurs de recherche, on peut obtenir des informations qui sont nécessaires pour le travail, au moment où on a besoin(Cousin, n.d.).

Le Web est une ressource indispensable pour la productivité des entreprises, mais il y a aussi des dangers (les virus, les vers, les cookies…), alors le Web montre une faiblesse.

Pour résoudre ce problème, il faut une discipline où les listes de pages Web à interdire ou à conseiller, mais dans l'évolution très rapide du Web aujourd'hui, comment peut-on faire ? (Cousin, n.d.).

IV - Attaque :

De nos jours la sécurité du réseau informatique est devenue indispensable face aux attaques qui se multiplient rapidement. Pour contrarier ces attaques, les systèmes de sécurité visent à prévenir de ces dernières et à corriger les vulnérabilités exploitées. Il est alors

nécessaire d'établir l'identification des menaces potentielles et de connaître les différents procédés des attaquants afin de sécuriser le réseau. C'est pourquoi nous allons dans un premier temps analyser ce que nous appellerons « l'anatomie d'une attaque », puis dans un second temps, nous caractériserons ces attaques avec ses différents types.

V - Motivation des attaques :

Les motivations des attaques peuvent être de différentes sortes :

- Obtenir un accès au système.
- Voler des informations, tels que des secrets industriels ou des propriétés intellectuelles.
- Glaner des informations personnelles sur un utilisateur.
- S'informer sur l'organisation (entreprise de l'utilisateur, etc.).
- Troubler le bon fonctionnement d'un service.
- Utiliser le système de l'utilisateur comme « rebond » pour une attaque.
- Utiliser les ressources du système de l'utilisateur.

1 - Anatomie d'une attaque :

Fréquemment appelés « les 5 P » dans la littérature, ces cinq verbes anglophones constituent le squelette de toute attaque informatique : Probe, Penetrate, Persist, Propagate, Paralyze.

Observons le détail de chacune de ces étapes(Burgermeister & Krier, 2006):

1-1 - Probe :

Consiste en la collecte d'informations par le biais d'outils comme whois, Arin, DNS lookup. La collecte d'informations sur le système cible peut s'effectuer de plusieurs manières, comme par exemple un scan de ports grâce au programme NAP pour déterminer la version des logiciels utilisés, ou encore un scan de vulnérabilités à l'aide du programme Nessus.

1-2 - Penetrate :

Utilisation des informations récoltées pour pénétrer un réseau. Des techniques comme le brute force ou les attaques par dictionnaires peuvent être utilisées pour outrepasser les protections par mot de passe. Une autre alternative pour s'infiltrer dans un système est d'utiliser des failles applicatives que nous verrons ci-après.

1-3 - Persist :

Création d'un compte avec des droits de super utilisateur pour pouvoir se réinfiltrer ultérieurement. Une autre technique consiste à installer une application de contrôle à distance capable de résister à un reboot (ex : un cheval de Troie).

1-4 - Propagate :

Cette étape consiste à observer ce qui est accessible et disponible sur le réseau local.

1-5 - Paralyze :

Cette étape peut consister en plusieurs actions. Le pirate peut utiliser le serveur pour mener une attaque sur une autre machine, détruire des données ou encore endommager le système d'exploitation dans le but de planter le serveur.

Après ces cinq étapes, le pirate peut éventuellement tenter d'effacer ses traces, bien que cela ne soit rarement utile.

2 - Différents types d'attaques :

De nombreux types d'attaques du réseau ont été identifiés. Ces attaques sont généralement classées en trois principales catégories (Ulmann, 2004) :

- Les attaques dans le but de découvrir des informations.
- Les attaques par intrusions sont menées afin d'exploiter les faiblesses de certaines zones du réseau telles que les services d'authentification.
- Les attaques d'interruption de service (ou déni de service) saturent l'accès à une partie ou à l'intégralité d'un système. Les attaques d'interruption de service distribué (*DDOS : Distributed Denial of Service*) qui consistent à saturer ainsi plusieurs machines ou hôtes, sont encore plus nuisibles.

- Attaques passives : les attaques passives sont la *capture* du contenu d'un message et *l'analyse de trafic*. Elles sont très difficiles à détecter car elles ne causent aucune altération des données. Le but de l'adversaire est d'obtenir une information qui a été transmise figure 1.3 (Rhouma, n.d.) .
- Attaques actives : ces attaques impliquent certaines modifications du flot de données ou la création d'un flot frauduleux ; elles peuvent être subdivisées en 4 catégories : mascarade, rejeu, modification de messages et déni de service.
    - Une mascarade a lieu lorsqu'une entité prétend être une autre entité. Une attaque de ce type inclut habituellement une des autres formes d'attaque active.
    - Le rejeu implique la capture passive de données et leur retransmission ultérieure en vue de produire un effet non autorisé.
    - La modification du messages (man in the middle) signifie que certaines portions d'un message légitime sont altérées ou que les messages sont réorganisés.
    - Dénis de services (Victor MORARU, 2005): d'une manière générale, l'attaque par déni de service (Denial of Service DoS) vise à rendre une application informatique incapable de répondre aux requêtes de ses utilisateurs par saturation de ses ressources. La Figure I.2 montre un exemple de DoS qui s'appelle « ICMPFlood ».

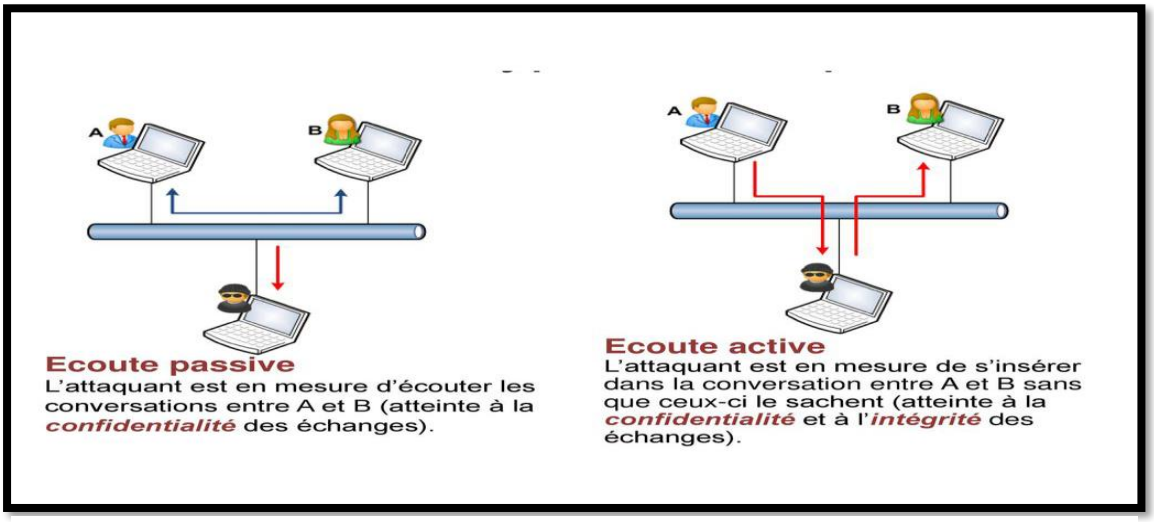


Figure 1: Ecoute passives et Ecoute actives.

3 - Buts des attaques

les attaques sur le système informatique ou réseau peut être largement classé selon leur but comme suit : interruption, interception, modification et fabrication.(Stallings, 2006)

- **Interruption :** vise la **disponibilité** des informations
- **Interception :** vise la **confidentialité** des informations
- **Modification** : vise **l'intégrité** des informations
- **Fabrication :** vise **l'authenticité** des informations

4 - Différentes étapes d'une attaque :

Une attaque est l'exploitation d'une faille d'un système informatique connecté à un réseau. Pour réussir leur exploit, les attaquants tentent d'appliquer un plan d'attaque bien précis pour aboutir à des objectifs distincts.

La plupart des attaques, de la plus simple à la plus complexe fonctionnent suivant le même schéma (Chaouki et al., 2009) :

4-1 - Identification de la cible :

Cette étape est indispensable à toute attaque organisée, elle permet de récolter un maximum de renseignements sur la cible en utilisant des informations publiques et sans engager d'actions hostiles. On peut citer par exemple l'interrogation des serveurs DNS.

4-2 - Scanning :

L'objectif est de compléter les informations réunies sur une cible visée. Il est ainsi possible d'obtenir les adresses IP utilisés, les services accessibles de même qu'un grand nombre d'informations de topologie détaillée.

4-3 - Exploitation :

Cette étape permet à partir des informations recueillies d'exploiter les failles identifiées sur les éléments de la cible, que ce soit au niveau protocolaire, des services et applications ou des systèmes d'exploitation présents sur le réseau.

4-4 - Progression :

Il est temps pour l'attaquant de réaliser son objectif. Le but ultime étant d'obtenir les droits de l'utilisateur root sur un système afin de pouvoir y faire tout ce qu'il souhaite.

VI - Autres attaques réputées :

Attaque par identification des systèmes réseau :

1 - Le balayage de ports : (Llorens et al., 2011)

1. Attaque par balayage ICMP
2. Attaque par balayage TCP
3. Attaque par balayage semi-ouvert TCP

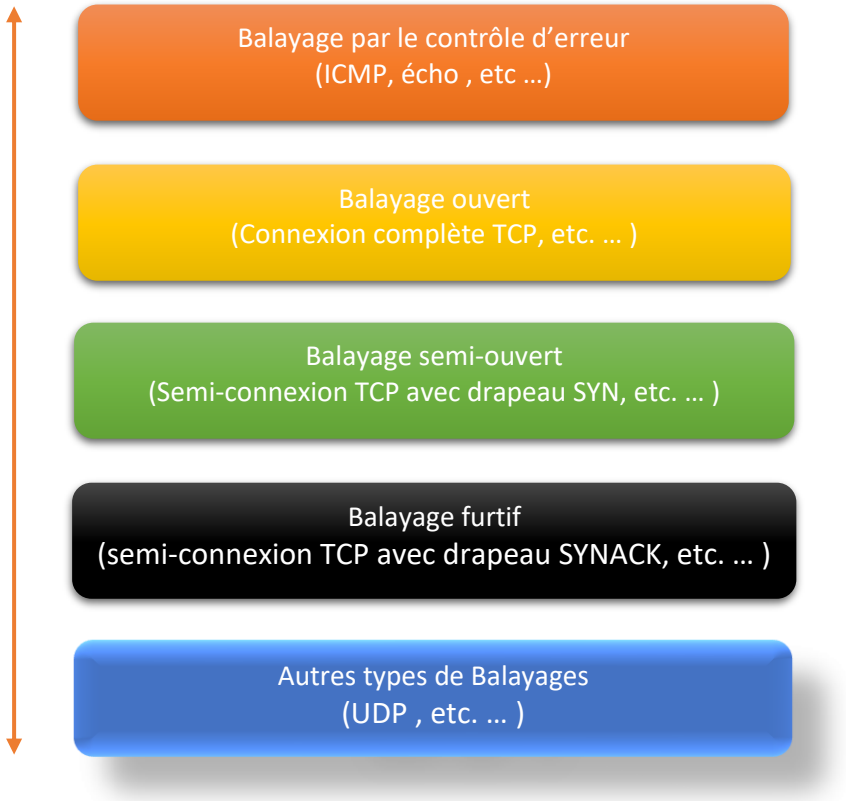


Figure 2 : Les différents types de balayages

VII - Types de logiciels malveillants :

1 - Virus :

Un virus est un logiciel capable de s'installer sur un ordinateur à l'insu de son utilisateur légitime. Le terme virus est réservé aux logiciels qui se comportent ainsi avec un but malveillant, parce qu'il existe des usages légitimes de cette technique dite de code mobile.

En général, pour infecter un système, un virus agit de la façon suivante : il se présente sous la forme de quelques lignes de code en langage machine binaire qui se greffent sur un programme utilisé sur le système cible, afin d'en modifier le comportement. Le virus peut être

tout entier contenu dans ce greffon, ou il peut s'agir d'une simple amorce, dont le rôle va être de télécharger un programme plus important qui sera le vrai virus.

Une fois implanté sur son programme-hôte, le greffon possède aussi en général la capacité de se recopier sur d'autres programmes, ce qui accroît la virulence de l'infection et peut contaminer tout le système ; la désinfection n'en sera que plus laborieuse(Bloch et al., 2013).

2 - Vers :

Un ver *(Worm)* est une variété de virus qui se propage par le réseau. Il se reproduit en s'envoyant à travers un réseau (e-mail, Bluetooth, chat.). Le ver contrairement aux virus, n'a pas besoin de l'interaction humaine pour pouvoir se proliférer.

3 - Cheval de Troie :

Un cheval de Troie *(Trojan horse)* est un logiciel qui se présente sous un jour honnête, utile ou agréable, et qui une fois installé sur un ordinateur y effectue des actions cachées et pernicieuses.

La différence essentielle entre un trojan et un ver réside dans le fait que le ver tente de se multiplier, Ce que ne fait pas le trojan.

4 - Porte dérobée :

Une porte dérobée *(backdoor)* est un logiciel de communication caché, installé par exemple par un virus ou par un cheval de Troie, qui donne à un agresseur extérieur accès à l'ordinateur victime, par le réseau (Berthomier, E. 2005).

5 - Bombe logique :

Une bombe logique est une fonction, cachée dans un programme en apparence honnête, utile ou agréable, qui se déclenchera à retardement, lorsque sera atteinte une certaine date, ou lorsque surviendra un certain événement. Cette fonction produira alors des actions indésirées, voir nuisibles (Berthomier, E. 2005).

Les bombes logiques présentent des caractéristiques similaires aux chevaux de Troie (incapacité de se reproduire et de se propager).

6 - Logiciel espion :

Un logiciel espion, comme son nom l'indique, collecte à l'insu de l'utilisateur légitime des informations au sein du système où il est installé, et les communique à un agent extérieur, par exemple au moyen d'une porte dérobée.

Une variété particulièrement toxique de logiciel espion est le *keylogger* (espion dactylographique), qui enregistre fidèlement tout ce que l'utilisateur tape sur son clavier et le transmet à son honorable correspondant ; il capte ainsi notamment identifiants, mots de passe et codes secrets (Berthomier, E. 2005).

7 - Spam :

Le spam est du courrier électronique non sollicité envoyé à un très grand nombre de personnes sans leur accord préalable.

Les messages électroniques non sollicités contiennent généralement de la publicité.

8 - Spyware :

Un spyware (mouchard) est un programme capable en plus de sa fonction propre de collecter des données sur ses utilisateurs et de les transmettre via Internet. Les spywares sont parfois confondus avec les adwares, ces logiciels dont l'auteur se rémunère par l'affichage de bannières publicitaires mais sans recueillir ni transmettre d'informations. (Berthomier, 2005)

Le but des mouchards est de recueillir le plus d'information possible de l'utilisateur. Ces mouchards sont présents dans de nombreux « freewares » ou « sharewares » et ils s'installent lors des téléchargements à l'insu des utilisateurs.

9 - Cookies :

Les cookies ne représentent pas de menace directe pour votre ordinateur ou les données qui y sont placées. Cependant, ils sont vraiment une menace pour la confidentialité : un cookie permet à un site Web de conserver vos références et de suivre à la trace vos visites du site. C'est pourquoi, si vous préférez garder l'anonymat, vous devriez désactiver les cookies en utilisant les paramètres de sécurité de votre navigateur.

Un cookie est un petit fichier au format texte d'un maximum de 4 Ko, envoyé ("offert", comme un biscuit ?) par le serveur d'un site Web et enregistré sur votre disque dur par votre navigateur, Un cookie n'étant pas exécutable, il ne peut contenir de virus.

VIII - Mécanismes de sécurité :

La sécurité vise à garantir la confidentialité, l'intégrité et la disponibilité des services. Il faut mettre en place des mécanismes pour s'assurer que seules les personnes autorisées ont accès à l'information et que le service est rendu correctement. Parmi ces mécanismes, on peut citer :

1 - Cryptage :

Cryptographie est une science mathématique dans laquelle on fait les études des méthodes permettant de transmettre des données de manière confidentielle.

Afin de protéger un message, on lui applique une transformation qui le rend incompréhensible ; c'est ce qu'on appelle le chiffrement, qui, à partir d'un texte clair, donne un texte chiffré ou cryptogramme. Inversement, le déchiffrement est l'action qui permet de reconstruire le texte en clair à partir du texte chiffré. Dans la cryptographie moderne, les transformations en question sont des fonctions mathématiques, appelées algorithmes cryptographiques, qui dépendent d'un paramètre appelé clef.

Dans les réseaux, pour contrer les vols d'informations dans la voie de transmission, on utilise les techniques de cryptographie pour chiffrer et déchiffrer les messages transmis. Il existe à l'heure actuelle deux grands principes de cryptage : le cryptage symétrique basé sur l'utilisation d'une clef privée et le cryptage asymétrique qui repose sur un codage à deux clefs, une privée et l'autre publique.

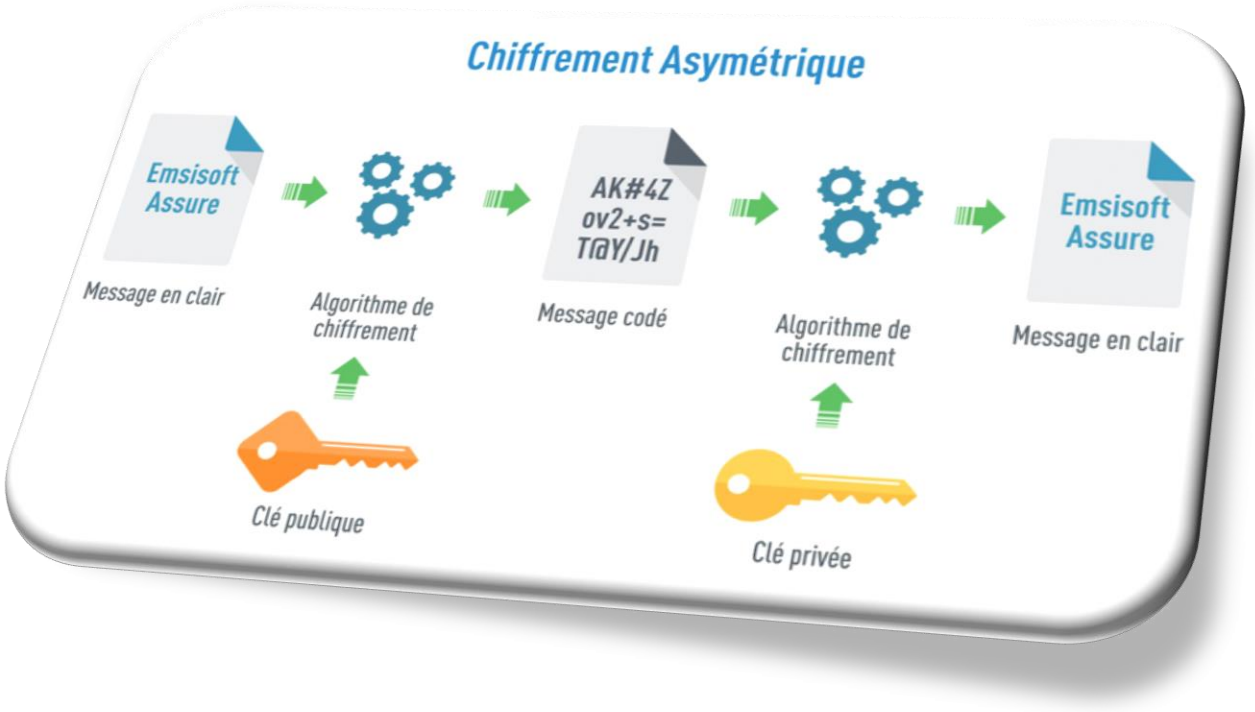


Figure 3 : Chiffrement

2 - Pare-feu :

Un pare-feu (firewall) est une solution matérielle ou logicielle mise en place au sein de l'infrastructure du réseau afin de filtrer l'accès à des ressources réseau définies. Il ne laisse entrer que les utilisateurs autorisés, disposant d'une clef ou d'un badge, et crée une couche protectrice entre le réseau et le monde extérieur. Il est doté de filtres intégrés qui peuvent empêcher des documents non autorisés ou potentiellement dangereux d'accéder au système. Il enregistre également les tentatives d'intrusions dans un journal transmis aux administrateurs du réseau. Il permet également de contrôler l'accès aux applications et d'empêcher le détournement d'usage (Berthomier, E. 2005).

Le pare-feu permet à laisser passer tout ou partie des paquets qu'ils sont autorisés, et à bloquer et journaliser les échanges qui sont interdits.

La Figure ci-dessous schématise le fonctionnement d'un pare-feu.

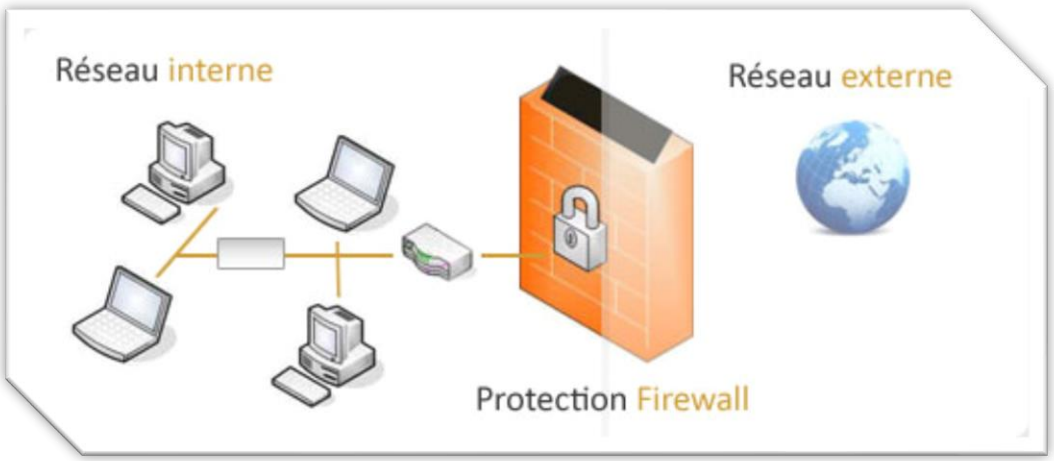


Figure 4 : Pare-feu

Le pare-feu est un IDS, mais il détecte seulement les attaques de l'extérieur. Pour Intranet, les pares-feux sont nécessaires, mais pas suffisants, pour commencer à implémenter une politique de sécurité.

Certains pares-feux laissent uniquement passer le courrier électronique. De cette manière, ils interdisent toute autre attaque qu'une attaque basée sur le service de courrier. D'autres pare-feu, moins strictes, bloquent uniquement les services reconnus comme étant des services dangereux. Généralement, les pares-feux sont configurés pour protéger contre les accès non authentifiés du réseau externe.

3 - Antivirus :

Un antivirus est un logiciel qui protège une machine contre les virus. Les antivirus se fondent sur des fichiers de signatures et comparent alors les signatures génétiques du virus aux codes à vérifier. Certains programmes appliquent également la méthode heuristique tendant à découvrir un code malveillant par son comportement.

Les antivirus peuvent scanner le contenu d'un disque dur, mais également la mémoire de l'ordinateur. Pour les plus modernes, ils agissent en amont de la machine en scrutant les échanges de fichiers avec l'extérieur, aussi bien en flux montant que descendant. Ainsi, les courriers sont examinés, mais aussi les fichiers copiés sur ou à partir de supports amovibles tels que cédéroms, disquettes, connexions réseau, ...

Aujourd'hui, il y a beaucoup d'antivirus comme Norton Antivirus, McAfee Antivirus, Kaspersky Antivirus...

4 - VPN :

Les réseaux privés virtuels (VPN : Virtual Privat Network) permettent à l'utilisateur de créer un chemin virtuel sécurisé entre une source et une destination. Avec le développement d'Internet, il est intéressant de permettre ce processus de transfert de données sécurisé et fiable. Grâce à un principe de tunnel (tunneling) dont chaque extrémité est identifiée, les données transitent après avoir été chiffrées.

Un des grands intérêts des VPN est de réaliser des réseaux privés à moindre coût. En chiffrant les données, tout se passe exactement comme si la connexion se faisait en dehors d'I internet. Il faut par contre tenir compte de la toile, dans le sens où aucune qualité de service (QoS) n'est garantie.

Le principe du VPN est basé sur la technique du tunneling. Cela consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Ensuite la source chiffre les données et les achemine en empruntant ce chemin virtuel.

Les données à transmettre peuvent appartenir à un protocole différent d'IP. Dans ce cas le protocole de tunneling encapsule les données en rajoutant un entête. Permettant le routage des trames dans le tunnel. Le tunneling est l'ensemble des processus d'encapsulation, de transmission et de dés encapsulation .(Desgeorge, 2000)

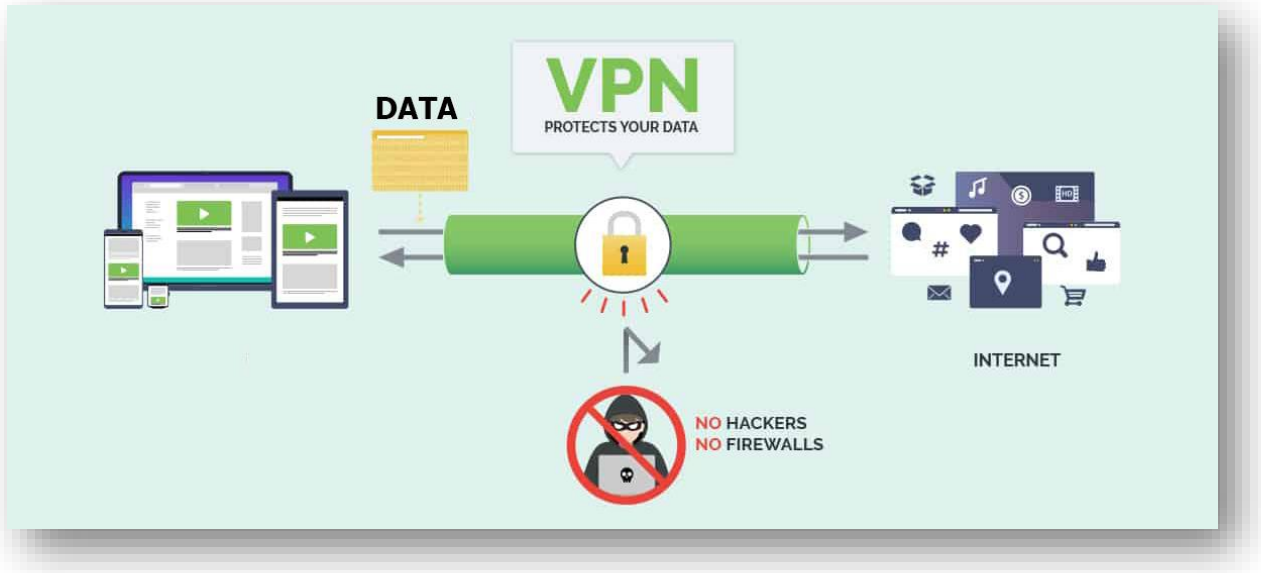


Figure 5 : VPN.

Conclusion

Dans ce chapitre nous avons vu comment un attaquant peut compromettre un système informatique en suivant une stratégie bien définie. Pour remédier à ces problèmes, des solutions de sécurité efficaces sont mises en œuvre par les administrateurs. Dans une optique d'optimisation de cette sécurisation, les systèmes de détection d'intrusions présentent un bon moyen de garantir cette sécurité des réseaux. C'est pourquoi nous entamerons dans le chapitre suivant l'étude des différents systèmes de détection d'intrusions et leur fonctionnement, ainsi que nous discutons aussi ses deux approches comportementales et par scénario.

Chapitre 2 : les systèmes de détection d'intrusion (IDS)

Chapitre 2 : les systèmes de détection d'intrusion (IDS)

Introduction :

L'informatique évolue, les systèmes et les réseaux informatiques deviennent de plus en plus complexes et les risques des failles augmentent donc la sécurité devienne de plus en plus difficile, car les délais laissés aux administrateurs sont souvent très courts.

Les attaques distribuées seront toujours redoutables si la plupart des machines ne sont pas protégées. Afin de détecter les attaques que peut subir un système, il est nécessaire d'avoir un logiciel spécialisé dont le rôle serait de surveiller les données qui transitent sur ce système, et qui serait capable de réagir si des données semblant suspectes.

Plus communément appelé IDS, les IDS conviennent parfaitement pour réaliser cette tâche.

Ce chapitre a pour but d'éclaircir les notions fondamentales liées au IDS, par la suite, nous présentons une classification des IDS selon deux approches, comportementale et par scénario, on va parler sur la préparation des IDS, comment on le faire ?

I - Définition d'un système de détection d'intrusions :

La détection d'intrusion est le processus de la surveillance des événements qui se produisent dans un ordinateur ou dans un réseau et de les analysent pour des signes d'intrusions, qui sont définis comme des tentatives qui compromettent la confidentialité, l'intégrité ou la disponibilité ou bien qui dépassent les conditions de la sécurité d'un ordinateur ou un réseau(Arvidson & Carlbark, 2003).

IDS signifie Intrusion Détection System. Il s'agit d'un équipement permettant de surveiller l'activité d'un réseau ou d'un hôte donné, afin de détecter toute tentative d'intrusion et éventuellement de réagir à cette tentative(Baudoin & Karle, 2004).

IDS est un appareil ou une application qui alerte l'administrateur en cas de faille de sécurité, de violation de règles ou d'autres problèmes susceptibles de compromettre son réseau informatique (Lerman et al., 2011).

IDS est un périphérique ou processus actif qui analyse l'activité du système et du réseau pour détecter toute entrée non autorisée et / ou toute activité malveillante. La manière dont un IDS détecte des anomalies peut beaucoup varier ; cependant, l'objectif principal de tout IDS est de prendre sur le fait les auteurs avant qu'ils ne puissent vraiment endommager vos ressources(Lerman et al., 2011).

Les IDS analysent les configurations des systèmes et leurs vulnérabilités, ainsi, ils vérifient l'intégrité des fichiers. Ils peuvent reconnaitre des schémas d'attaque classiques. Pour ce faire, ils analysent les comportements anormaux et suivent les violations de règles par les utilisateurs.

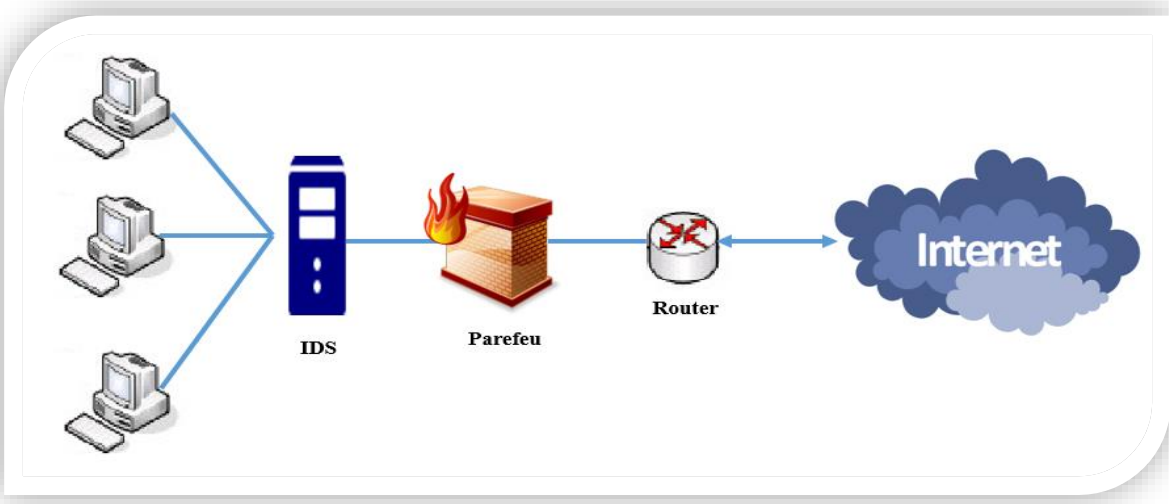


Figure 6 : Système de détection d'intrusions

Ses fonctions principales peuvent être résumées dans les points suivants :

- Journaliser l'événement source d'information et vision des menaces courantes.
- Comparer les données collectées avec des données de référence qui correspondent à des opérations interdites ou autorisées.
- Avertir un système avec un message (Exemple : appel SNMP[1]).

[1] Simple Network Management Protocol (abrégé SNMP), en français « protocole simple de gestion de réseau », est un protocole de communication qui permet aux administrateurs réseau de gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes réseaux et matériels à

- Avertir un humain avec un message (Courrier électronique, SMS, interface web …).
- Amorcer certaines actions sur un réseau ou hôte (Exemple : mettre fin à une connexion réseau, ralentir le débit des connexions …).
- Appliquer des mesures correctives en cas de détection d'une intrusion (Hodo et al., 2017).

II - Architecture Intrusion Détection System :

Plusieurs schémas ont été proposés pour décrire les composants d'un système de détection d'intrusions. Parmi eux, nous avons retenu celui issu des travaux d'Intrusions Détection exchange formatWorking Group (IDWG) de l'Internet Engineering Task Force (IETF) comme base de départ, car il résulte d'un large consensus parmi les intervenants du domaine (Debar et al., 2004).

L'objectif des travaux du groupe IDWG est la définition d'un standard de communication entre certains composants d'un système de détection d'intrusions. La figure (7) illustre ce modèle et permet d'introduire un certain nombre de concepts :

distance. SNMP est utilisé pour administrer les équipements et/ou surveiller le comportement des équipements.

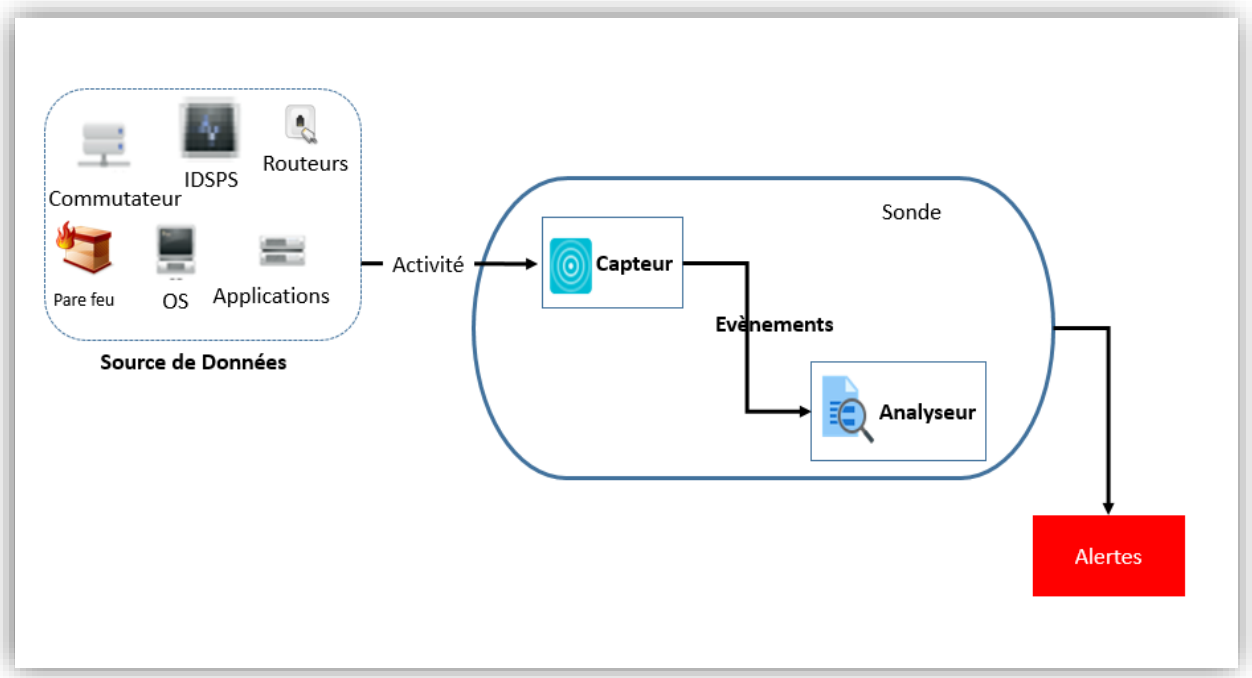


Figure 7 : Modèle générique de la détection d'intrusions proposé par l'IDWG

L'architecture IDWG d'un système de détection d'intrusions contient des capteurs qui envoient des événements à un analyseur. Les capteurs couplés avec un analyseur forment une sonde, cette dernière envoie des alertes vers un manager qui la notifie à un opérateur humain. Les différents éléments de cette architecture sont :

- **Source de données :** dispositif générant de l'information sur les activités des entités du système d'information.
- **Capteur :** génère des événements en filtrant et formatant les données brutes provenant d'une source de données.
- **Evénement :** message formaté et renvoyé par un capteur. C'est l'unité élémentaire utilisée pour représenter une étape d'un scénario d'attaques connu.
- **Analyseur :** c'est un outil logiciel qui met en œuvre l'approche choisie pour la détection (comportementale ou par scénarios), il génère des alertes lorsqu'il détecte une intrusion.
- **Sonde :** un ou des capteurs couplés avec un analyseur.
- **Alerte :** message formaté émis par un analyseur s'il trouve des activités intrusives dans une source de données.

Dans ce modèle qui représente le processus complet de la détection ainsi que l'acheminement des données au sein d'un IDS. L'administrateur configure les différents composants (capteur(s), analyseurs(s)) selon une politique de sécurité bien définie. Les capteurs accèdent aux données brutes, les filtrent et les formatent pour ne renvoyer que les événements intéressants à un analyseur. Les analyseurs utilisent ces événements pour décider de la présence ou non d'une intrusion et envoient dans le cas échéant une alerte au manager, qui notifie l'opérateur humain, une réaction éventuelle peut être menée automatiquement par le manager ou manuellement par l'opérateur.(Michel, 2003)

III - Classification des systèmes de détections d'intrusion :

La classification adoptée selon différents critères qui ne sont pas forcément mutuellement exclusifs n'est pas hiérarchique , elle présente tour à tour et au même niveau les catégories caractérisant chaque IDS, et utilise les critères suivants (figure 8) : (Michel, 2003)

- La méthode de détection utilisée.
- Le comportement après détection
- La source des données à analyser.
- La fréquence de l'analyse.

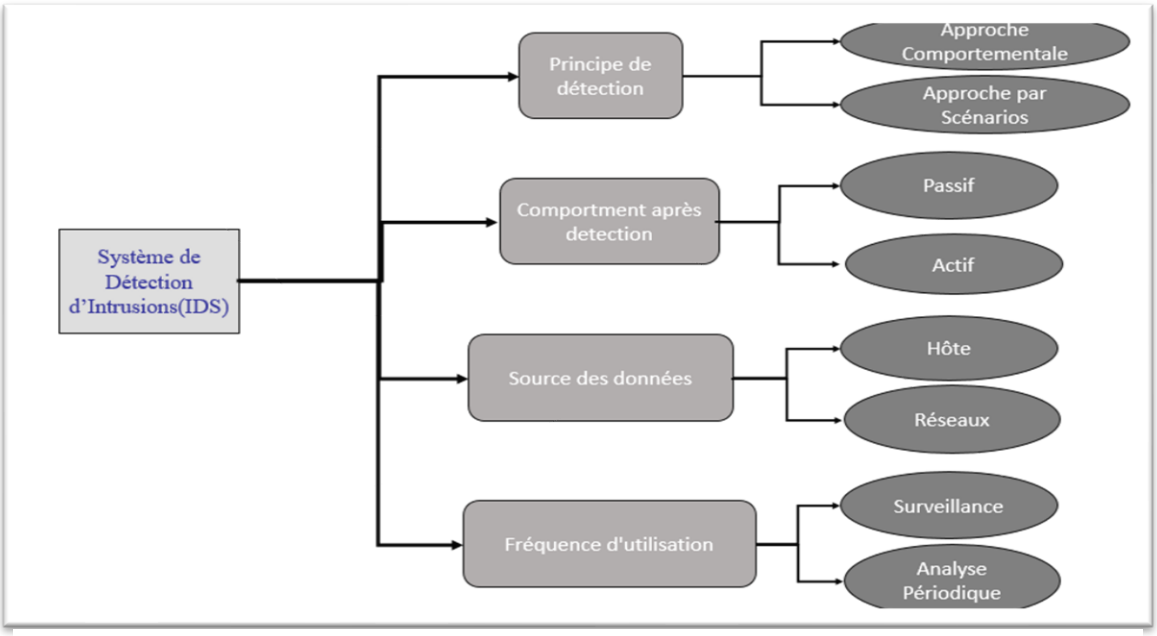


Figure 8: Taxonomie des systèmes de détection d'intrusions

IV - Les méthodes d'analyses des systèmes de détections d'intrusion

Deux techniques de détection d'intrusion sont généralement mises en œuvre par les IDS courants. La Méthode de détection décrit les caractéristiques de l'analyseur, lorsque le système de détection d'intrusion utilise des informations sur le comportement normal des systèmes qu'il surveille, on qualifie de comportement (détection par comportement). Lorsque le système de détection d'intrusion utilise des informations sur les attaques, on qualifie (détection par signature).

1 - Détection par signature (scénario)

La détection par signature considère comme normal tout ce qui n'est pas hostile, et elle adopte la politique suivante : «si ce n'est pas dangereux, alors c'est normal ». Donc, il est impératif de disposer d'une base de toutes les attaques connues.

Dans la détection par signature (aussi appelée détection de mauvaise utilisation), l'IDS analyse l'information recueillie et la compare avec une base de données de signatures (motifs définis, caractéristiques explicites) d'attaques connues (i.e., qui ont déjà été documentées), et toute activité correspondante est considérée comme une attaque (avec différents niveaux de sévérité).(Dagorn, 2006)

Cette méthode est très efficace pour détecter des attaques sans produire un grand nombre

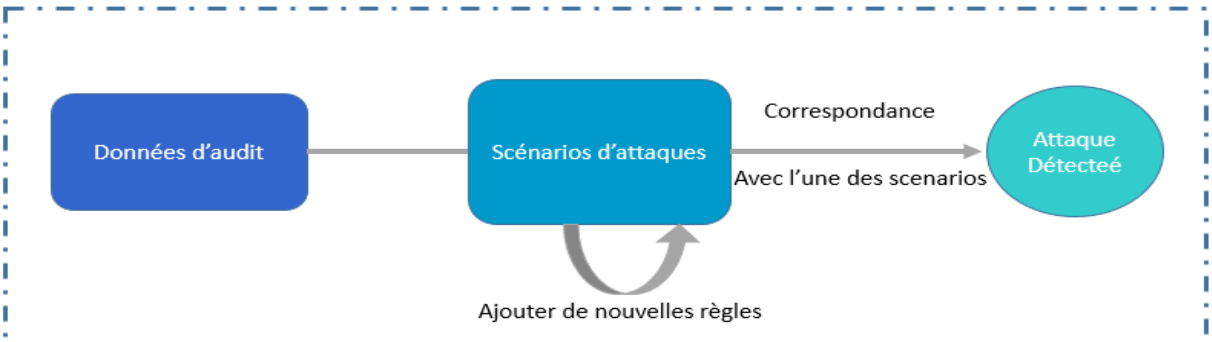


Figure 9 Fonctionnement d'un IDS par l'approche basée connaissance

de fausses alarmes. Elle peut rapidement et sûrement diagnostiquer l'utilisation d'un outil spécifique ou une technique d'attaque. Ceci peut aider les responsables de la sécurité à donner la priorité aux mesures correctives. Cependant, elle peut seulement détecter les attaques connues, dont les signatures sont introduites dans le système, donc le système de détection doit être constamment mis à jour avec les signatures des nouvelles attaques. De plus, beaucoup de systèmes adoptant cette approche sont conçus pour employer un nombre limité de signatures qui peuvent être définies, ce qui les empêchent de détecter les variantes de ces attaques.

2 - Détection par comportement

La détection par comportement consiste à considérer comme hostile tout ce qui n'est pas normal, au sens où on cherchera plutôt à bien définir ce qui est un comportement normal sur le système pour pouvoir y opposer toute déviation, que l'on considérera comme étant une attaque : « si ce n'est pas normal, alors c'est dangereux ».

L'idée principale est de modéliser durant une période d'apprentissage le comportement "normal" d'un système/programme en définissant une ligne de conduite (dite profil), et de considérer ensuite (en phase de détection) comme suspect tout comportement inhabituel (les déviations significatives par rapport au modèle de comportement "normal"). Les modèles de détection comportementale incluent fréquemment des modèles statistiques. La détection par comportement revient donc à repérer tout ce qui sort du cadre de la normalité.(Ahmed, 2014)

La détection comportementale est la capacité à détecter le comportement peu commun. Elle a ainsi la capacité de détecter les symptômes des attaques connues et inconnues sans la connaissance spécifique des détails. De plus, cette approche permet de produire l'information utile pour la définition des signatures pour les systèmes de détection d'intrusions à base de signatures. Cependant, cette approche produit un grand nombre de fausses alarmes dues aux comportements imprévisibles des utilisateurs du réseau. Elle exige souvent l'historique à long terme des événements enregistrés afin de caractériser les modèles normaux de comportement.

Les systèmes basés sur cette approche doivent être dotés d'une certaine intelligence pour raison d'apprentissage automatique de la normalité. Il existe plusieurs méthodes de détection d'intrusion utilisées pour implémenter cette approche. Voici quelques principales méthodes

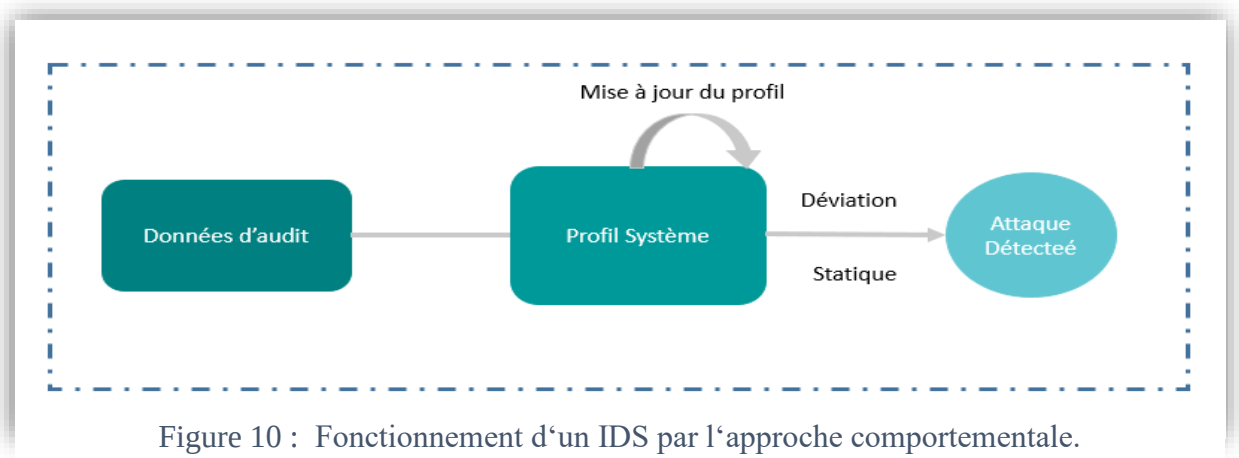


Figure 10 : Fonctionnement d'un IDS par l'approche comportementale.

utilisées : la méthode statistique, le système expert, etc. pour plus d'information dirigez-vous dans(Llorens et al., 2011) .

V - Comportement après détection :

Nous pouvons également faire une distinction entre les IDS en se basant sur le type de réaction lorsqu'une attaque est détectée :

1-1 - Passive :

Généralement, la plupart des systèmes de détection d'intrusions n'apportent qu'une réponse passive à l'intrusion ; c'est à dire lorsqu'une attaque est détectée, ils génèrent une alarme et notifient l'administrateur système par e-mail, message dans une console, voire même par beeper ou SMS. C'est alors l'opérateur qui devra prendre les mesures qui s'imposent.

1-2 - Active :

Des systèmes de détection d'intrusions peuvent, en plus de la notification à l'opérateur, prendre automatiquement des mesures pour stopper l'attaque en cours. Par exemple, ils peuvent couper les connexions suspectes ou même, pour une attaque externe, reconfigurer le pare-feu pour qu'il refuse tout ce qui vient du site incriminé. Toutefois, il apparait que ce type de fonctionnalité automatique est potentiellement dangereux car il peut mener à des dénis de service provoqués par l'IDS. Un attaquant déterminé peut, par exemple, tromper l'IDS en usurpant des adresses du réseau local qui seront alors considérées comme la source de l'attaque par l'IDS. Il est préférable de proposer une réaction facultative à un opérateur humain (qui prend la décision finale).(Michel, 2003)

1-3 - Source des données à analyser

Parmi les caractéristiques essentielles des systèmes de détection d'intrusions, les sources de données à analyser constituent la matière première du processus de détection. Ces données proviennent soit de logs (journaux) générés par le système d'exploitation, soit de logs des applications, soit d'informations provenant du réseau, soit encore d'alertes générées par d'autres IDS.(Michel, 2003)

1-4 - Fréquence de l'analyse.

Une autre caractéristique des systèmes de détection d'intrusions est leur fréquence d'utilisation, dans ce cas nous distinguons deux (2) types :

- **IDS online (continue) :**

Ce sont des IDS qui font leur analyse des fichiers d'audit ou des paquets réseau de manière continue ou en permanence afin de détecter une attaque au moment de sa production, c'est une détection en temps réel. Ce type d'IDS consomme un taux élevé de ressources systèmes car il faut analyser à la volée tout ce qui se passe sur le système et ce qu'il le rend non préférable en cas de ressources précieuses telle que les serveurs de messagerie par exemple.

- **IDS offline (périodique) :**

Ce type d'IDS fait l'analyse dans des durées périodiques afin de détecter des traces d'attaques au but de modéliser des signatures d'attaques pour la base du système, l'avantage de ce type est qu'il ne consomme pas beaucoup de ressources système. Cela peut être suffisant dans des contextes peu sensibles (nous ferons alors une analyse journalière, par exemple). L'inconvénient majeur de ce type est sa détection tardive des attaques ce qui risque de provoquer des dégâts dangereux.(Michel, 2003).

VI - Types des IDS

Suivant l'emplacement de l'IDS dans l'architecture du réseau informatique à surveiller, nous distinguons trois types d'IDS :

1 - IDS réseau

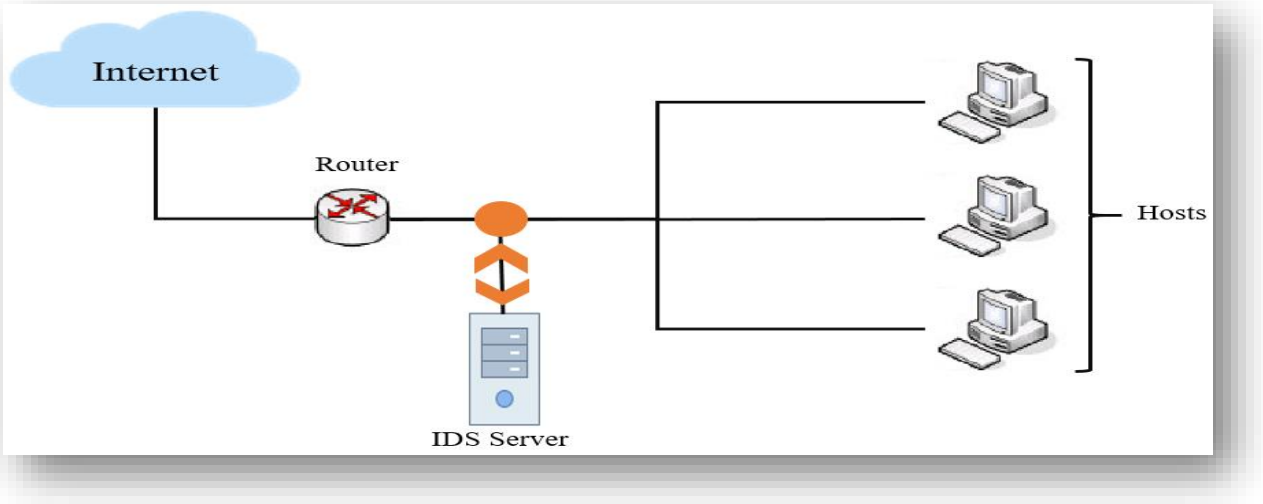


Figure 11 Exemple d'une architecture d'un NIDS

L'IDS réseau (Network IDS ou NIDS) est situé sur un réseau isolé et ne voit qu'une copie du trafic, c'est-à-dire des paquets qui circulent sur le réseau. Et en cas de détection d'une menace, le NIDS peut lever des alertes et ordonner les actions pour le blocage d'un flux. En termes d'architecture, le NIDS est situé sur un réseau isolé et analyse une copie du trafic du réseau à surveiller, entre ses points d'entrées et les terminaux du réseau. A noter qu'il est entièrement passif et n'est pas capable de dialoguer avec le réseau surveillé.

Il est fréquent de trouver plusieurs IDS sur les différentes parties du réseau. Nous trouvons souvent une architecture composée d'une sonde placée à l'extérieur du réseau afin d'étudier les tentatives d'attaques et d'une sonde en interne pour analyser les requêtes ayant traversé le pare-feu (AMAND & NSIRI, 2011).

1-1 - Avantages de NIDS :

- Les capteurs peuvent être bien
- Sécurisés puisqu'ils se contentent d'observer le trafic.
- Détecter plus facilement les scans grâce aux signatures.
- Filtrage de trafic.
- Assurer la sécurité contre les attaques puisqu'il est invisible.

1-2 - Inconvénients de NIDS :

- La probabilité de faux négatifs (attaques non détectées) est élevée et il est difficile de contrôler le réseau entier.
- Ils doivent principalement fonctionner de manière cryptée d'où une complication de l'analyse des paquets.
- A l'opposé des IDS basés sur l'hôte, ils ne voient pas les impacts d'une attaque.(Belkhatmi Keltouma, 2016)

2 - IDS hôte

Il y a ensuite les IDS hôte (Host IDS ou HIDS) ou IDS système. Les HIDS (Host Intrusion Détection System), surveillent l'état de la sécurité des hôtes selon différents critères :

- Activité de la machine (comme par exemple le nombre et listes de processus, le nombre d'utilisateurs, ressources consommées, etc.).
- Le second critère de surveillance est l'activité de l'utilisateur sur la machine : horaires et durée des connexions, commandes utilisées, programmes activés, etc.

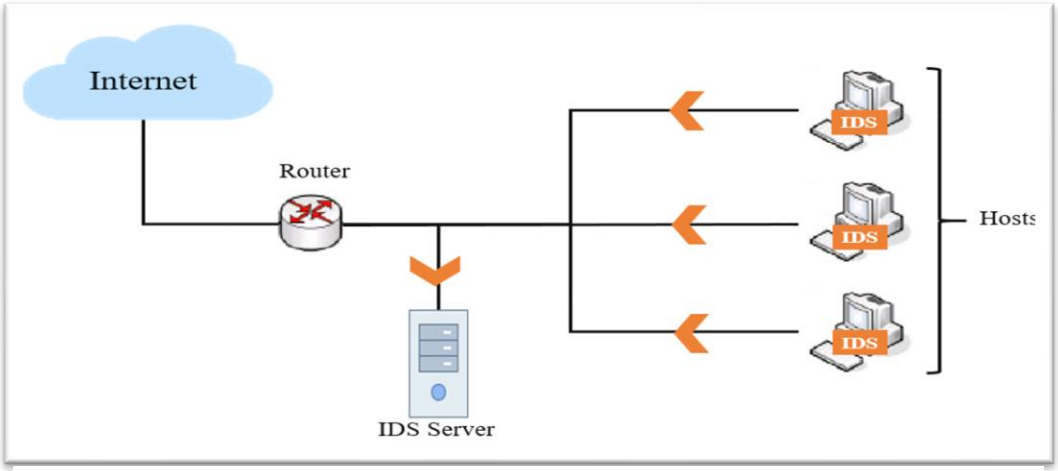


Figure 12 : Exemple d'une architecture d'un HIDS

Évidemment le HIDS analyse toute activité potentielle liée à l'activité d'un ver, d'un virus ou cheval de Troie. En termes d'architecture, les HIDS sont, généralement, placés sur des machines sensibles, susceptibles de subir des attaques et possédantes des données sensibles pour l'entreprise. Les serveurs web et applicatifs, peuvent notamment être protèges par un

HIDS. Le HIDS master récupère les informations remontées par une machine sur laquelle un client HIDS est installé. Ensuite, le HIDS master va analyser ces informations sur le fonctionnement et l'état des machines afin de détecter les menaces (AMAND & NSIRI, 2011).

2-1 - Avantages de HIDS :

- Découvrir plus facilement un Cheval de Troie puisque les informations et les possibilités sont très étendues.
- Détecter des attaques impossibles à détecter avec des IDS réseau puisque le trafic est souvent crypté.
- Observer les activités sur l'hôte avec précision.

2-2 - Inconvénients de HIDS :

- Ils ont moins de facilité à détecter les scans.
- Ils sont plus vulnérables aux attaques de type Dos.
- Ils consomment beaucoup de ressources CPU (Belkhatmi Keltouma, 2016).

3 - IDS hybride

Les IDS hybrides sont, généralement, utilisés dans un environnement décentralisé, ils permettent de réunir les informations de diverses sondes placées sur le réseau, et agissent comme NIDS et/ou HIDS suivant leurs emplacements. Leur appellation « hybride » provient du fait qu'ils sont capables de réunir aussi bien des informations provenant d'un système HIDS qu'un NIDS. Toutes ces sondes HIDS et NIDS remontent alors les alertes à une machine qui va centraliser le tout, et agréger/lier les informations d'origines multiples. Ainsi, nous comprenons que les IDS hybrides sont basés sur une architecture distribuée, où chaque composant unifie son format d'envoi (par exemple IDMEF2). Cela permet de communiquer et d'extraire des alertes plus pertinentes (AMAND & NSIRI, 2011).

3-1 - Avantages d'IDS hybride :

- Moins de faux positifs.
- Meilleure corrélation (la corrélation permet de générer de nouvelles alertes à partir de celles existantes).
- possibilité de réaction sur les analyseurs (Belkhatmi Keltouma, 2016)

3-2 - Inconvénients d'IDS hybride :

- taux élevé de faux positifs (Belkhatmi Keltouma, 2016).

VII - Mesures d'évaluations (performances) des systèmes de détection d'intrusions :

La matrice de confusion est utilisée pour visualiser, pour chaque classe de modèle, les vraies classifications et les classifications prédites.

		Prédiction de la classe	
		Classe négative (normal)	**Classe positive (attaque)**
Classe actuelle	**Classe négative (normal)**	**Vrai négative (VN)**	**Faux positif (FP)**
	Classe positive (attaque)	**Faux négative (FN)**	**Vrai positif (VP)**

Tableau 1 : Matrice de confusion.

Les vrais négatifs ainsi que les vrais positifs correspondent à un fonctionnement correct de la technique de data mining, ce qui signifie que la technique de data mining a prédit avec succès respectivement le comportement normal et les attaques. Les faux négatifs sont des attaques incorrectement prédites comme des comportements normaux.

Les métriques traditionnelles de classification comprennent le taux d'exactitude, le taux de fausse alerte et le taux d'erreur de la classification, elles sont définies comme suit :

1 - Le taux d'exactitude (TE) :

Montre à quel point le système est exacte, c'est le nombre de type bien classé sur le nombre de type de tout le corpus.

$$\boldsymbol{Exactitude} = \frac{VP + VN}{VP + VN + FP + FN}$$

.

2 - Le taux de fausse alerte (TFA) :

Ce critère mesure le taux de fausses alertes générées par un IDS dans un environnement donné et pendant une durée donnée. C'est le nombre des alertes généré comme attaque sur le nombre des types classés comme normal existants dans le corpus.

$$\boldsymbol{FAR} = \frac{FP}{VP + FP}$$

3 - Le taux de détection (DR : Détection Rate) :

Mesure le taux des attaques détectées par un IDS dans un environnement donné et pendant une durée donnée. C'est le nombre des attaques détecté sur le nombre des attaques existants dans le corpus.

$$\boldsymbol{DR} = \frac{VN}{VP + FN}$$

Dans (Porras & Valdes, 1998) , il est défini trois critères pour évaluer l'efficacité des systèmes de détection d'intrusion :

- **L'exactitude (*accuracy*)** : on parle de l'exactitude quand le système de détection d'intrusion déclare comme malicieux une activité légale. Ce critère correspond au faux positif.
- **La performance (*performance*)** : la performance du système de détection d'intrusion est le taux de traitement des évènements. Si ce taux est faible, la détection en temps réel est donc impossible
- **La complétude (*completeness*)** : on parle de la complétude quand le système de détection d'intrusion ne rate pas la détection d'une attaque. Ce critère est le plus difficile, parce qu'il est impossible d'avoir une connaissance globale sur les attaques. Ce critère correspond au faux négatif.
- Debar dans (Llorens et al., 2011) a rajouté également ces critères suivants[i] :
- **La tolérance aux fautes (*Fault tolerance*)** : le système de détection d'intrusions doit lui-même résisté aux attaques, particulièrement au déni de service. Ceci est important, parce que plusieurs systèmes de détection d'intrusion s'exécutent sur des matériels ou logiciels connus comme vulnérables aux attaques.

- **La réaction à temps (*Timeliness*) :** le système de détection d'intrusion doit s'exécuter et propager les résultats de l'analyse le plus tôt possible, pour permettre à l'officier de sécurité de réagir avant que de graves dommages n'aient lieu.
- **Rapidité :** Un système de détection d'intrusions doit exécuter et propager son analyse d'une manière prompte pour permettre une réaction rapide dans le cas d'existence d'une attaque pour permettre à l'agent de sécurité de réagir.

VIII - Les limites d'un IDS :

Parmi les faiblesses des IDS on trouve :(Yann Berthier & Baptiste, 2004)

- Nombreux faux positifs.
- Configuration complexe et longue.
  - Nombreux faux positifs après configuration.
- Pas de connaissance de la plate-forme.
  - De ses vulnérabilités.
  - Du contexte métier.
- Les attaques applicatives sont difficilement détectables.
  - Injection SQL.
  - Exploitation de CGI mal conçus.
- Des évènements difficilement détectables.
  - Scans lents / distribués
  - Canaux cachés / tunnels.
- Pollution des IDS.
  - Consommation des ressources d'IDS.
  - Perte de paquets.
  - Déni de service contre IDS / opérateur.
  - Une attaque réelle peut passer inaperçue.
- Attaque contre IDS lui-même.
- Ils ne peuvent pas compenser les trous de sécurité dans les protocoles réseaux.
- Ils ne peuvent pas compenser des manques significatifs dans votre stratégie de sécurité, votre politique de sécurité ou votre architecture de sécurité.

Conclusion :

Ce chapitre nous a permis de constater que les IDS sont de plus en plus fiables, d'où le fait qu'ils soient souvent intégrés dans les solutions modernes de sécurité. Les avantages qu'ils présentent par rapport aux autres outils de sécurité les favorisent. Il nous a également permis de comprendre que ces derniers sont indispensables aux entreprises afin d'assurer leur sécurité informatique.

Le cha

Chapitre 3 : L'Internet des objets (IdO)

Chapitre 3 : L'Internet des objets (IDO)

Introduction :

L'internet des objets ou IdO (en anglais (the) Internet of Things ou IoT) est l'interconnexion entre l'Internet et des objets, des lieux et des environnements physiques. L'appellation désigne un nombre croissant d'objets connectés à l'Internet permettant ainsi une communication entre nos biens dits physiques et leurs existences numériques. Ces formes de connexions permettent de rassembler de nouvelles masses de données sur le réseau et donc, de nouvelles connaissances et formes de savoirs.

Dans ce chapitre on va expliquer ce qu'est l'IoT, Nous présentons dans un premier temps son fonctionnement, les domaines d'application d'IoT et leur communication, comment sécurisé nos appareils intelligents.

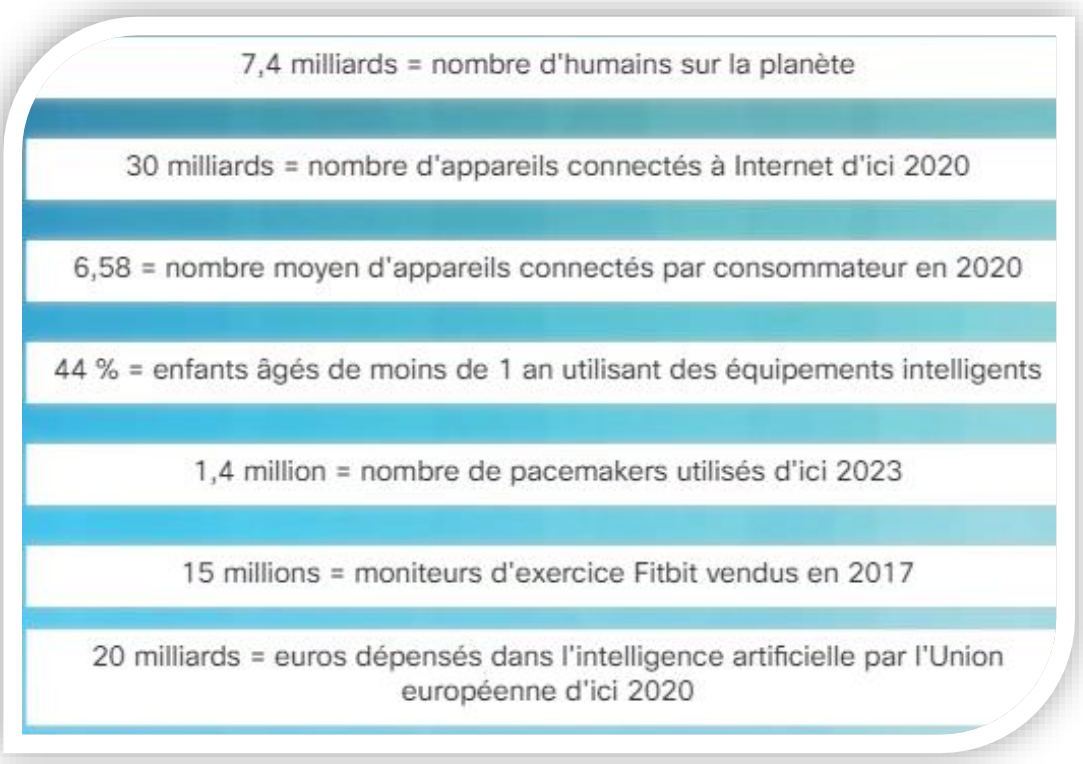


Figure 13 : la distribution des appareils intelligents et une étude sur les personnes connectées

I - Définition :

L'Internet des objets (IoT) désigne l'interconnexion de millions d'appareils et de capteurs intelligents connectés à Internet. Ces capteurs et ces appareils connectés collectent et partagent des données qui seront utilisées et analysées par plusieurs organismes, dont des entreprises, des villes, des gouvernements, des hôpitaux et des particuliers.

Il faut savoir que **:** '' L'Internet des Objets est un réseau de réseaux qui permet, via des systèmes d'identification électronique normalisés et unifiés, et des dispositifs mobiles sans fil, d'identifier directement et sans ambiguïté des entités numériques et des objets physiques et ainsi de pouvoir récupérer, stocker, transférer et traiter, sans discontinuité entre les mondes physiques et virtuels, les données s'y rattachant (Benghozi et al., 2009)'.

II - Technologies de l'IoT

L'IoT permet l'interconnexion des différents Objets intelligents via l'Internet. Ainsi, pour son fonctionnement, plusieurs systèmes technologiques sont nécessaires. "L'IoT désigne diverses solutions techniques (RFID, TCP/IP, technologies mobiles, etc.) qui permettent d'identifier des Objets, capter, stocker, traiter, et transférer des données dans les environnements physiques " (Al-Fuqaha et al., 2015). En effet, bien qu'il existe plusieurs technologies utilisées dans le fonctionnement de l'IoT, nous mettons l'accent seulement sur quelques-unes qui sont, selon Han et Zhanghang, les technologies clés de l'IoT. Ces technologies sont les suivantes :

RFID, WSN et M2M, et elles sont définies ci-dessous :

- RFID : est une technologie sans fil qui est utilisée pour l'identification des Objets(Vasseur et al., 2011), elle englobe toutes les technologies qui utilisent des ondes radio pour identifier automatiquement des Objets ou des personnes. C'est une technologie qui permet de mémoriser et de récupérer des informations à distance grâce à une étiquette qui émet des ondes radio. Il s'agit d'une méthode utilisée pour transférer les données des étiquettes à des Objets, ou pour identifier ces Objets à distance. L'étiquette contient des informations stockées électroniquement pouvant être lues à distance (Al-Fuqaha et al., 2015).

- WSN : est un ensemble de nœuds qui communiquent sans fil et qui sont organisées en un réseau coopératif. Chaque nœud possède une capacité de traitement et peut contenir différents types de mémoires, un émetteur-récepteur RF et une source d'alimentation. Il peut aussi tenir compte des divers capteurs et actionneurs (Palattella et al., 2012) Comme son nom l'indique, le WSN constitue un réseau de capteurs sans fil qui peut être une technologie nécessaire au fonctionnement de l'IoT.

- M2M : est l'association des technologies de l'information et de la communication avec des Objets intelligents dans le but de donner à ces derniers les moyens d'interagir sans intervention humaine avec le système d'information d'une organisation ou d'une entreprise (Al-Fuqaha et al., 2015)

III - Domaines D'applications :

Dans nos jours l'importance de l'internet des objets augmente jour par jour, les chercheurs estiment : ‘’que 3 millions de nouveaux terminaux se connecter à l'Internet chaque mois, dans les 4 prochaine année ce chiffre devrait atteindre les 30 milliards appareils connectées dans le monde entier ‘’.

L'utilisation de IOT 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 IOT(Al-Fuqaha et al., 2015).

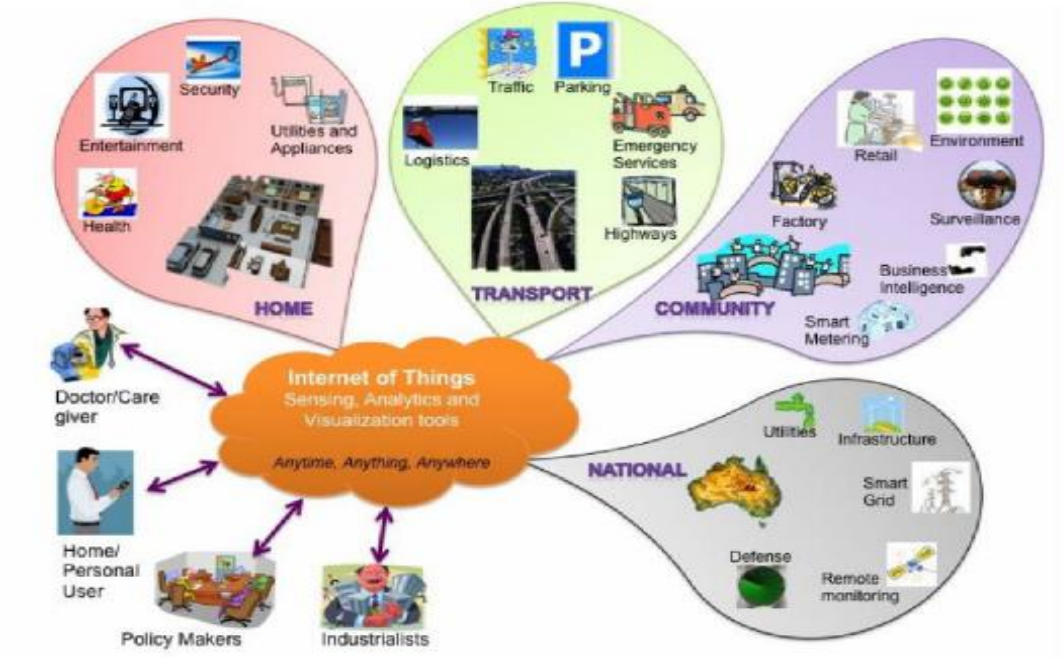


Figure 14 : Les domaines de l'internet des Objets

1 - L'internet des objets dans le domaine des sportifs :

De nombreux objets connectés comme des montres ou des bracelets connectés vous permettrons pendant la journée de calculer le nombre de pas effectuée, la distance par courue, votre temps d'activités, les calories brulées, ainsi pendant la nuit en calculant vos heures de sommeil. Pour les passionnés de High-tech, c'est un grand marché qui s'ouvre à eux ! De la montre connectée au téléviseur connecté en passant par les appareils photos, les montre, les drones, les lunettes (Google glass)(Al-Fuqaha et al., 2015)..

2 - L'agriculture :

L'objectif principal de l'agriculture intelligente rendre fort la capacité des systèmes Agricole permis ces systèmes la prévention des risques météo où la maîtresse de l'irrigation la contribution de la sécurité alimentaire grâce à la collecte et l'analyse des données(Al-Fuqaha et al., 2015).

3 - Domotique :

La domotique ou maison connectée, c'est la manipulation de l'internet des objets dans une maison.

Les grandes entreprises telles que Nest, Netatom ont déployées des écosystèmes communiquant qui permettent de centraliser le contrôle de différents systèmes de votre maison.

Le principe de la domotique est de faire en sorte qu'une maison devienne intelligente indépendante et qu'elle réfléchisse par elle-même(Al-Fuqaha et al., 2015).

4 - La Santé :

Plusieurs applications dans l*e domaine de la santé* utilisent déjà l'internet des objets, machine a rayon X et imagerie, Porteuse Digital Health, Compteur D'énergie etc.

Plus que 60% des hôpitaux mondiale utilise déjà internet des objets, le secteur de la santé a connu pas mal d'applications permettant la liaison d'un patient et à son docteur de récupérer des informations sur la maladie.

Les Objets connotées sont utilisés à la surveillance des établissement médicaux, les opérations chirurgicales, les services de géolocalisation(Al-Fuqaha et al., 2015).

5 - L'internet des objets dans le domaine de L'automobile

Le marché des transports a déjà anticipé l'arrivée des objets connectés. Parmi les enjeux les plus fréquents que ce domaine fait naitre on retrouve la réduction des accidents et des embouteillages, le partage de voitures, le développement des offres de VTC et de TAX ou encore la gestion des flots automobile(Al-Fuqaha et al., 2015)..

6 - L'internet des objets dans le domaine de la sécurité

Pour le cabinet en stratégie, ces entreprises vont rapidement se positionner comme des alliés des personnes qui résident dans leur domicile. En fournissant des données relatives à la consommation d'énergie aux foyers, ces groupes vont apparaitre comme des arguments contre le facteur EDF pour les fournisseurs d'énergie la précision sera difficile à tenir car ils seront probablement contraints d'accompagner leurs clients dans une baisse de leurs facteurs énergétique(Al-Fuqaha et al., 2015).

7 - L'internet des objets dans le domaine de l'industrie

Le déploiement de L'IoT dans l'industrie sera certainement un grand support pour le développement de l'économie et le secteur des services, puisque L'IDO permettra d'assurer un suivi total des produits, de la chaine de production, jusqu'à la chaine logistique et de distribution en supervisant les conditions d'approvisionnements. Cette traçabilité de bout en bout facilitera la lutte contre la contrefaçon, la fraude et les crimes économiques transfrontaliers.

Certains éditeurs tels que SAP et CISCO montrant d'ores et déjà comment certaines zones industrielles comme le port d'Hambourg ont pu être équipés en puces et autres objets connectés. L'internet couvre un énorme nombre d'industries et utilise des cas qui s'étendent d'un seul dispositif contraint aux déploiements croisés de technologies intégrées de systèmes Cloud connectés en temps réel(Al-Fuqaha et al., 2015).

IV - Architecture de l'IoT :

L'Internet de Objets demande un modèle de référence qui permettrait de décrire la manière avec laquelle ces systèmes, ces réseaux et ces applications interagissent entre eux. En effet, un tel modèle aurait les avantages de :

- **Simplifier** :la compréhension de systèmes complexes découpés en parties plus compréhensibles
- **Clarifier** : en fournissant des informations supplémentaires identifiant les niveaux de l'IoT et fournissant une terminologie commune
- **Identifier** : où des types spécifiques de traitement sont optimisés dans les différentes parties du système
- **Standardiser** : pour créer les conditions d'une interopérabilité entre des produits IoT de différents fabriquant
- **Organiser** : rend l'IoT plus accessible et moins conceptuel

Nous présentons maintenant les différentes architectures qui ont été proposées par certains chercheurs **:**

1 - Architectures à trois et cinq couches :

L'architecture la plus élémentaire est une architecture à trois couches [3–5], Elle a été introduite aux premiers stades de la recherche dans ce domaine. Il comporte trois couches, à savoir les couches perception, réseau et application.

- La couche de perception est la couche physique, qui possède des capteurs pour détecter et recueillir des informations sur l'environnement. Il détecte certains paramètres physiques ou identifie d'autres objets intelligents dans l'environnement.

- La couche réseau est responsable de la connexion à d'autres objets intelligents, périphériques réseau et serveurs. Ses fonctionnalités sont également utilisées pour transmettre et traiter les données des capteurs.
- La couche application est chargée de fournir des services spécifiques à l'application à l'utilisateur. Il définit diverses applications dans lesquelles l'Internet des objets peut être déployé, par exemple, les maisons intelligentes, les villes intelligentes et la santé intelligente.(Sethi & Sarangi, 2017)

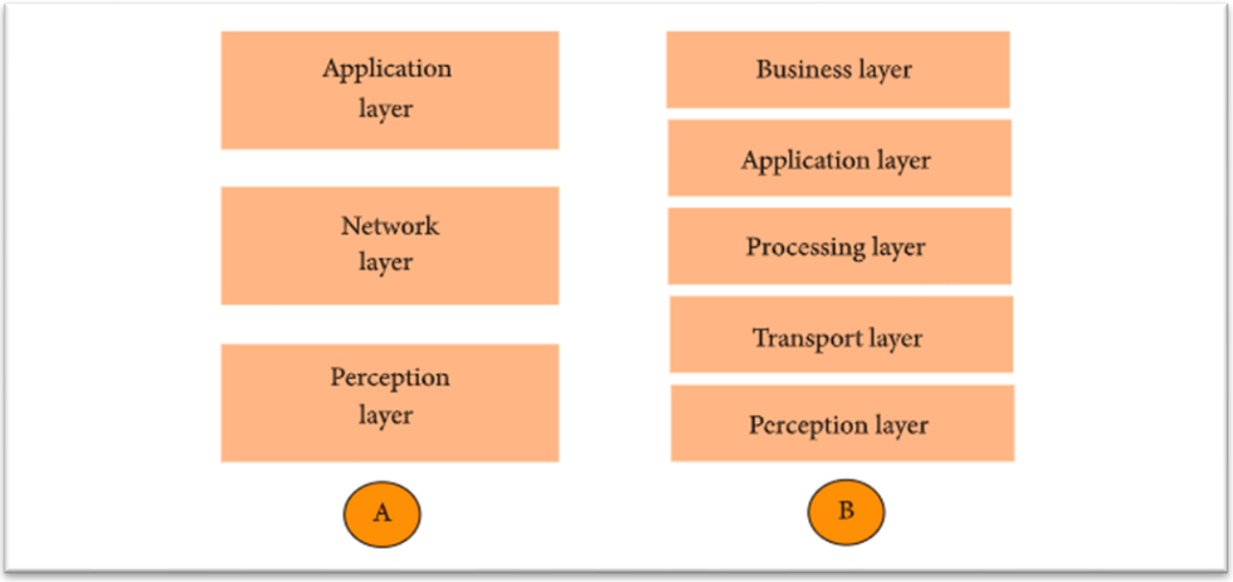


Figure 15 : Architecture de l'IoT (A : trois couches) (B : cinq couches)

En ce qui concerne l'architecture à trois couches, elle définit l'idée principale de l'Internet des objets, mais elle n'est pas suffisante pour la recherche sur l'IoT car la recherche se concentre souvent sur des aspects plus fins de l'Internet des objets.

C'est pourquoi, nous avons beaucoup plus d'architectures en couches proposées dans la littérature. L'une est l'architecture à cinq couches, qui comprend en outre les couches de traitement et d'entreprise [3–6]. Les cinq couches sont les couches perception, transport, traitement, application et métier). Le rôle des couches de perception et d'application est le même que celui de l'architecture à trois couches.

- La couche de transport transfère les données du capteur de la couche de perception à la couche de traitement et vice versa via des réseaux tels que sans fil, 3G, LAN, Bluetooth, RFID et NFC.
- La couche de traitement est également connue sous le nom de couche *middleware*. Il stocke, analyse et traite d'énormes quantités de données provenant de la couche transport. Il peut gérer et fournir un ensemble diversifié de services aux couches inférieures. Il utilise de nombreuses technologies telles que les bases de données, le cloud comptine et les modules de traitement des mégadonnées.
- La couche métier gère l'ensemble du système IoT, y compris les applications, les modèles commerciaux et de profit et la confidentialité des utilisateurs. La couche métier sort du cadre de cet article. Par conséquent, nous n'en discutons pas plus avant(Sethi & Sarangi, 2017).

2 - Architectures basées sur le cloud et le brouillard (cloud and fog) :

Certaines architectures de systèmes, le traitement des données est effectué de manière centralisée à grande échelle par des ordinateurs en nuage. Une telle architecture centrée sur le cloud maintient le cloud au centre, Le cloud comptine bénéficie de la primauté car il offre une grande flexibilité et évolutivité. Il propose des services tels que l'infrastructure principale, la plate-forme, les logiciels et le stockage. Les développeurs peuvent fournir leurs outils de stockage, leurs outils logiciels, leurs outils d'exploration de données et d'apprentissage automatique ainsi que leurs outils de visualisation via le cloud.

Dernièrement, il y a une évolution vers une autre architecture de système, à savoir le calcul de brouillard, où les capteurs et les passerelles de réseau font une partie du traitement et de l'analyse des données. Une architecture de brouillard présente une approche en couches, comme le montre la figure 2, qui insère des couches de surveillance, de prétraitement, de stockage et de sécurité entre les couches physiques et de transport. La couche de surveillance surveille l'alimentation, les ressources, les réponses et les services. La couche de prétraitement effectue le filtrage, le traitement et l'analyse des données des capteurs. La couche de stockage temporaire fournit des fonctionnalités de stockage telles que la réplication, la distribution et le stockage des données. Enfin, la couche de sécurité effectue le chiffrement / déchiffrement et garantit l'intégrité et la confidentialité des données. La surveillance et le prétraitement se font en bordure du réseau avant d'envoyer des données vers le cloud(Sethi & Sarangi, 2017).

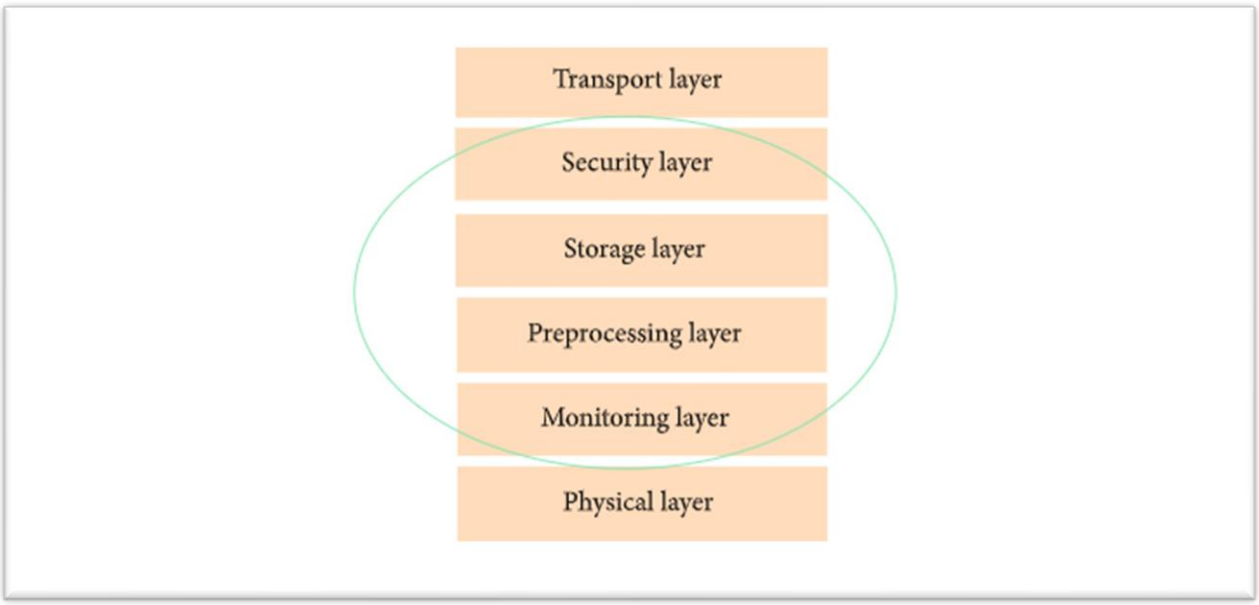


Figure 16 : Architecture de brouillard d'une passerelle IoT intelligente

.

V - Les Protocoles de communication de l'internet Des Objets :

Un protocole de communication est responsable de :'' définir la politique et les règles et les procédures de communication des couche physique et la liaison du modèle OSI ,garce a ces protocoles on peut établir une connexion d'un objet à un réseau sans fil ou filaire qui permettre la transmission et la réception des données depuis l'internet à travers passerelle , Il existe de nombreuses options de passerelle, certaines aussi simples qu'un périphérique mobile (smart phone) co-localisé avec le point de terminaison IoT et communiquant via un RF protocole tel que Bluetooth-LE, ZigBee ou Wi-Fi.(Sennoun, n.d.) ''.

Quand on parle de la connexion d'un objet cela évoque les communications sans fils et les technologies telles que le WIFI, le Bluetooth, il existe pas mal de supports et dizaines de protocoles avec des caractéristique différentes (portée, débit etc.).

Avant que d'essayer d'adapter tous les protocoles IoT aux modèles d'architecture existants tels que le modèle OSI, ils ont divisé les protocoles en couches suivantes :

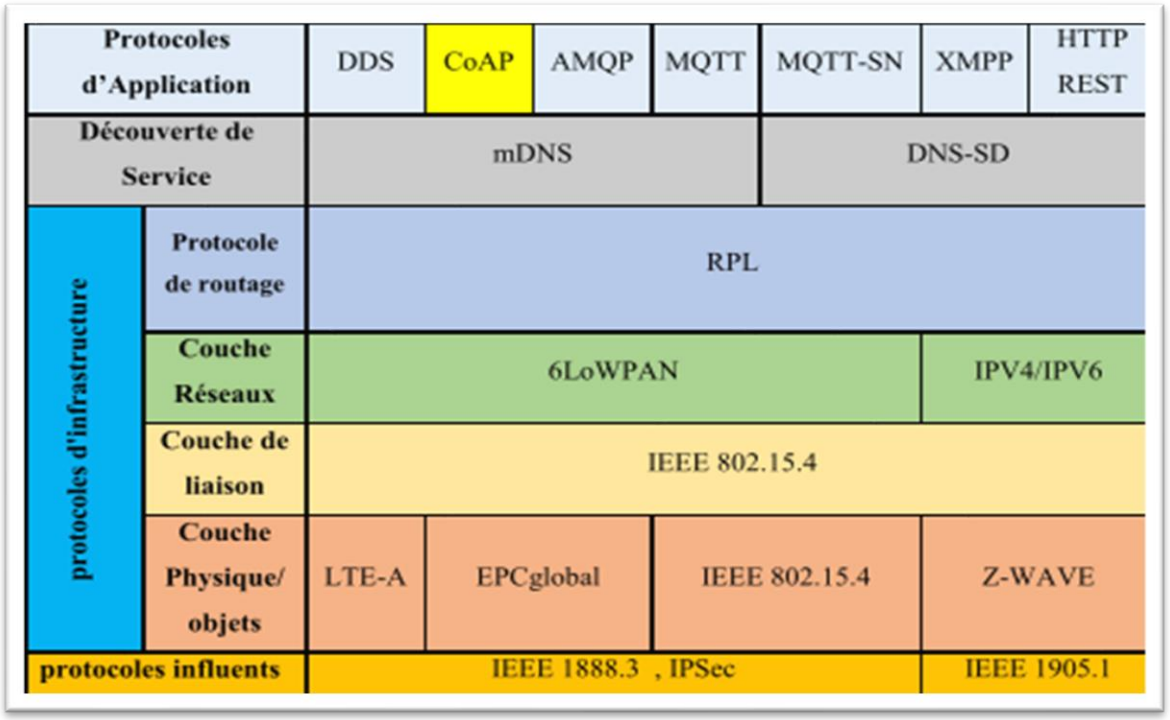


Figure 17 : Protocoles de communication de l'internet Des Objets

VI - Protocoles d'infrastructure :

1 - Routing Protocol for Low Power and Lossy Networks (RPL):

L'Internet Engineering Task Force (IETF) a découvert l'importance de créer un nouveau groupe de travail pour trouver une solution de routage IPv6 pour les réseaux d'objets intelligents IP, le nouveau groupe appelé *ROLL (Routing Over Low power and Lossy).*

Le groupe de travail de routage IETF sur des liaisons à faible puissance et avec perte *(ROLL)* a normalisé un protocole de routage indépendant des liaisons basé sur IPv6 pour les nœuds à ressources limitées appelés RPL, RPL a été créé pour prendre en charge les exigences de routage minimales grâce à la création d'une topologie robuste sur les liaisons avec perte.

Ce protocole de routage est responsable de : '' prend en charge des modèles de trafic simples et complexes tels que multipoint à point, point à multipoint et point à point(Vasseur et al., 2011) ''.

1-1 - 6LoWPAN :

Pour pouvoir parler de protocole *6LoWPAN* nous devons savoir qu'est-ce qu'un WPAN ?

Les réseaux personnels sans fil de faible puissance *(WPAN)* sur lesquels de nombreuses communications IoT peuvent s'appuyer ont certaines caractéristiques spéciales différentes des anciennes technologies de couche liaison comme la taille limitée des paquets (par exemple, 127 octets maximum pour IEEE 802.15.4), diverses longueurs d'adresse et une faible bande passante, Il était donc nécessaire de créer une couche d'adaptation qui adapte les paquets IPv6 aux spécifications IEEE 802.15.4.

Ce protocole a pour rôle de : '' Le groupe de travail IETF 6LoWPAN a développé une telle norme en 2007,6LoWPAN est la spécification des services de mappage requis par IPv6 sur des WPAN à faible puissance pour maintenir un réseau IPv6. (Palattella et al., 2012)- (Ko et al., 2011)''.

1-2 - IEEE 802.15.4 :

Le protocole IEEE 802.15.4 a été créé pour spécifier une sous-couche pour le contrôle d'accès moyen (MAC) et une couche physique (PHY) pour les réseaux privés sans fil à faible débit (LR-WPAN) (Association, 2011).

IEEE 802.15.4 a pour objectif de : '' prend en charge trois bandes de canaux de fréquence et utilise une méthode à spectre étalé en séquence directe (DSSS). Sur la base des canaux de fréquence utilisés, la couche physique transmet et reçoit des données sur trois débits de données : 250 kbps à 2,4 GHz, 40 kbps à 915 MHz et 20 kbps à 868 MHz. Des fréquences plus élevées et des bandes plus larges offrent un débit élevé et une faible latence tandis que les fréquences plus basses offrent une meilleure sensibilité et couvrent de plus grandes distances. Pour réduire les collisions potentielles, IEEE 802.15.4 MAC utilise le protocole CSMA / CA(Al-Fuqaha et al., 2015) ''.

1-3 - EPCglobal :

Plusieurs informaticiens ont pris le souci de clarifier ce terme afin de mieux le comprendre : '' Le code de produit électronique (EPC) est un numéro d'identification unique qui est stocké sur une étiquette RFID et est utilisé essentiellement dans la gestion de la chaîne d'approvisionnement pour identifier les articles. EPCglobal, en tant qu'organisation originale

responsable du développement d'EPC, gère la technologie et les normes EPC et RFID. L'architecture sous-jacente utilise des technologies RFID basées sur Internet ainsi que des étiquettes et lecteurs RFID bon marché pour partager des informations sur les produits (Jones & Chung, 2016). ‘‘.

Cette architecture est : ’‘ reconnue comme une technique prometteuse pour l'avenir de l'IoT en raison de son ouverture, de son évolutivité, de son interopérabilité et de sa fiabilité au-delà de sa prise en charge des principales exigences de l'IoT telles que les ID d'objets et la découverte de services (Minoli, 2013)’‘.

1-4 - LTE-A (Long Term Evolution—Advanced):

Au niveau de la couche physique : ’‘ le LTE-A utilise l'accès multiple par répartition en fréquence orthogonale (OFDMA) par lequel la bande passante du canal est partitionnée en bandes plus petites appelées blocs de ressources physiques (PRB).

Le LTE-A utilise également une technique à spectre étalé à porteuses multiples (CC) qui permet d'avoir jusqu'à cinq bandes de 20 MHz. L'architecture du réseau LTE-A repose sur deux parties essentielles. Le premier est le Coré Network (CN) qui contrôle les appareils mobiles et traite les flux de paquets IP.

L'autre partie est le réseau d'accès radio (RAN) qui gère les communications sans fil et l'accès radio et établit les protocoles du plan utilisateur et du plan de contrôle. Le RAN se compose principalement de stations de base (également appelées NodeB évoluées) qui sont connectées les unes aux autres par l'interface X2.

Le RAN et le CN sont connectés via l'interface S1. Les appareils mobiles ou MTC peuvent se connecter aux stations de base directement ou via la passerelle MTC (MTCG). Ils peuvent également avoir une communication directe avec d'autres appareils MTC(Al-Fuqaha et al., 2015)’‘.

1-5 - Z-Wave :

Z-Wave en tant que protocole de communication sans fil à faible puissance pour les réseaux domotiques (HAN) a été largement utilisé dans les applications de contrôle à distance dans les maisons intelligentes ainsi que dans les domaines commerciaux de petite taille .

Il a été développé par ZenSys (actuellement Sigma Designs) et a ensuite été utilisé et amélioré par Z-Wave Alliance(Gomez & Paradells, 2010).

Ce protocole permet de : '' couvre environ 30 mètres de communication point à point et est spécifié pour les applications qui nécessitent une transmission de données minuscule comme le contrôle de la lumière, le contrôle des appareils électroménagers, l'énergie intelligente et le CVC, le contrôle d'accès, le contrôle des soins de santé portable et la détection d'incendie.

Z-Wave fonctionne dans les bandes ISM (environ 900 MHz) et permet un taux de transmission de 40 kbps. Les versions récentes prennent également en charge jusqu'à 200 kbps. Sa couche MAC bénéficie d'un mécanisme anti-collision. Une transmission fiable est possible dans ce protocole par des messages ACK optionnels. Dans son architecture, il y a des nœuds contrôleurs et esclaves.

Les contrôleurs gèrent les esclaves en leur envoyant des commandes. À des fins de routage, un contrôleur conserve une table de toute la topologie du réseau. Le routage dans ce protocole est effectué par la méthode de routage source dans laquelle un contrôleur soumet le chemin à l'intérieur d'un paquet(Al-Fuqaha et al., 2015)''.

VII - La sécurité et la protection de la vie privée (privacy)

Le niveau d'acceptation des nouvelles technologies et services offert par l'IOT au niveau de la société est fortement lié au degré de fiabilité des informations et de protection des données privées des utilisateurs. Bien que plusieurs projets aient été lancés dans le but de trouver des solutions adéquates pour la protection de la privacy et d'assurer une protection rigoureuse aux utilisateurs finaux à la confidentialité, la privacy et la gestion de la confiance (Y.ait mouhoub, 2015)

VIII - Vulnérabilités et menaces dans l'internet des Objets

A cause de la forte intégration de l'IOT, les objets du quotidien deviennent des risques potentiels d'attaque sur la sécurité, l'ubiquité de L'IoT amplifiera les menaces classiques de la sécurité qui pèsent sur les données et les réseaux, de plus l'apparition de nouvelles menaces qui toucheront directement à l'intégrité des objets eux-mêmes, les infrastructures et processus et la privacy des personnes (Y.ait mouhoub, 2015).

1 - Menaces sur les données et les réseaux

Le manque de surveillance et de protection physique des objets communicants peut en gendres des attaques potentielles portées sur le matérielle telles que le vol, la corruption ou la contrefaçon de ces derniers pour récupération des données qui sont stockées sur ces dispositifs ou pour interrompre le bon fonctionnement des réseaux ou les systèmes complexes les hébergent.

De plus, les transmissions sans fil sont réputées par leur forte vulnérabilité aux attaques de l'écoute passive et de déni de service. Les solutions cryptographiques existantes aujourd'hui ne sont pas adéquates pour tenir faces à ces problèmes cités à cause de la limitation de ressources des objets communicants, de ce fait, l'adaptation de ces dernières ou la conception de nouveaux modèles est une nécessité afin d'assurer les services de sécurité (Y.ait mouhoub, 2015)

2 - Menaces sur la vie privée

De nombreux objets seront intégrés, portés ou même bien installés dans les lieux privés des personnes, ces objets présentent une potentielle menace pour la vie privée (privacy) de leurs utilisateurs. En effet, ces appareils électriques non seulement sont traçables, mais peuvent filmer, écouter ou même enregistrer leurs rythmes cardiaque ou respiratoire ainsi que la température du corps ou sa cinématique dans le but d'un malicieux (Y.ait mouhoub, 2015).

3 - Menaces sur les systèmes et l'environnement physique des objets

Des objets malicieux connectés à un réseau ou intégrés dans un système complexe peuvent causer un dysfonctionnement quelconque, un déni de service ou autres types d'attaques à l'intégrité des données et les informations sensibles du système, ou pire encore prendre le contrôle du système en causant des importants (Y.ait mouhoub, 2015).

IX - Attaques dans l'IoT

L'IoT est vulnérable à un nombre considérable d'attaques. Il existe diverses attaques sur des schémas d'authentification d'utilisateurs distants tels que le dictionnaire, men-in-the middle, le texte en clair, la carte à puce perdue, la modification, le déni de service (DOS), la divulgation de clé de session, l'emprunt d'identité, etc. Ces attaques peuvent être gênantes pour un utilisateur légitime lors de l'accès à un système dans un but spécifique. Une attaque de dictionnaire tente de deviner des mots de passe communs basés sur le dictionnaire. Une attaque

men-in-the-middle est implémentée pour reconnaitre l'information. Une attaque en clair est utilisée lorsque le texte chiffré est volé. Une attaque perdue de carte à puce est introduite lorsqu'une carte à puce est perdue, puis un attaquant peut appliquer des procédures pour acquérir l'information. Une attaque de modification est implémenté pour modifier les informations ; en d'autres termes, l'attaquant modifie les informations puis retransmet les données à nouveau (Limbasiya & Doshi, 2017). Ces attaques sont présentées dans le tableau 2

Nom de l'attaque	But et résultat de l'attaque	Menace	Active ou Passive
DoS	-Saturer un serveur ou bloquer le trafic. -rendre un service non disponible.	Intégrité. Disponibilité. Confidentialité.	Active
Man-in-the-Middle	- Intercepter les communications entre deux Parties contrôler la conversation. - ´écouter, modifier ou supprimer des données.	Intégrité. Confidentialité	Active
L'usurpation d'identité	- vol d'identité. - réaliser des actions frauduleuses. - prendre délibérément l'identité d'une autre personne Vivante.	Confidentialité Authentification.	Active
Footing	- épuiser la mémoire et l'énergie des nœuds - Saturer le réseau	Disponibilité.	Active
Les attaques de cartes à puce	- pouvoir accéder aux informations et aux secrets contenus dans la carte (code PIN, Clé(s) secrète(s) cryptographie(s), etc.…).	Physiques Logicielles	Active
Wardriving	- Utilisé pour pouvoir accéder à internet au nom D'une autre personne. - Parcourir tous les lieux où le Wifi est déployée afin De découvrir toutes les bornes Wifi existantes noter L'adresse géographique.	Confidentialité.	Passive
Sniffing	- Capturer les trames circulent local et afficher leur contenus (entêtes des paquets sur un réseau protocoles, id des user, MDP non crypté, etc.).	-confidentialité.	Passive

Tableau 2 : Type d'attaques dans l'IoT

X - DDOS (Distributed denial-of-service):

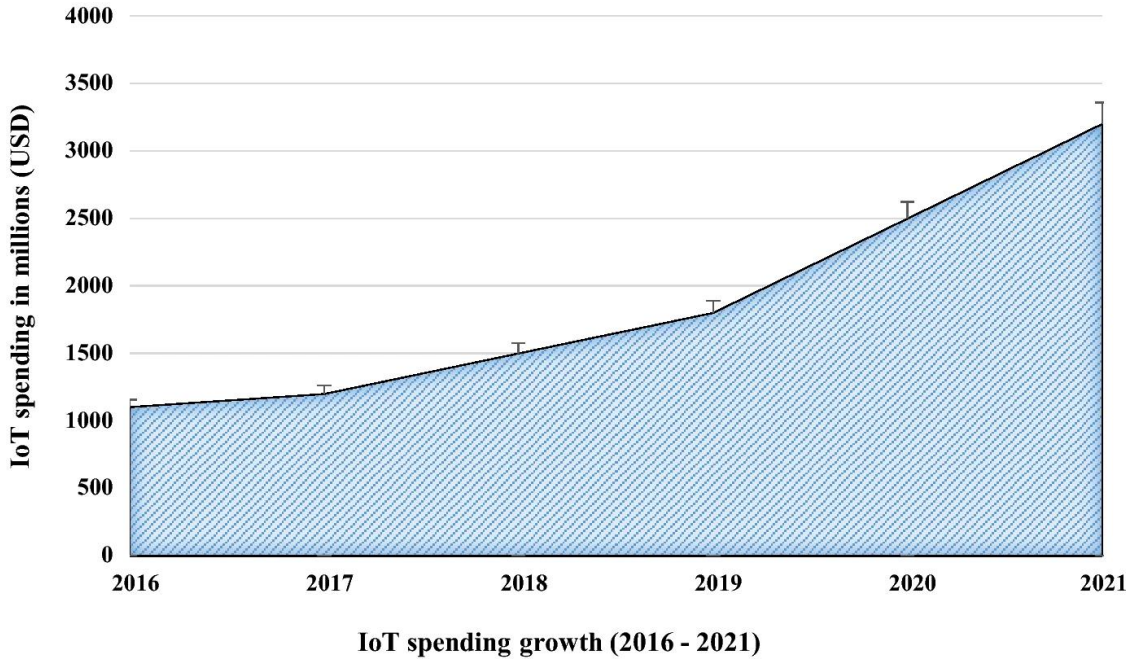
Il est nécessaire de prendre en compte l'évolution des systèmes de piratage et le danger qui nous menace à cause de ces attaques. DDOS est une tentative de rendre une ressource indisponible pour ses utilisateurs prévus en surcharge (*by overloading*).

Pendant l'attaque, le serveur n'est jamais accessible, les bases de données ne sont jamais consultées et les données ne sont jamais supprimées.

Le déni de service (*Denial of Service Distributed : DDoS)* est **:** « l'attaque qui bloque pour un utilisateur, l'accès à sa machine ou qui retarde le temps de réponse et le rend inaccessible. Il peut survenir à la suite d'une attaque programmée lorsqu'une personne malveillante surcharge intentionnellement une ressource, un système ou accidentellement lorsqu'un utilisateur légitime, par inadvertance, déclenche une procédure inappropriée qui rend une ressource inaccessible et non disponible. Dans les deux cas l'administrateur d'une entreprise se doit de prendre les mesures nécessaires pour protéger ses machines (Trabelsi & Ly, 2005) ».

L'augmentation énorme du nombre d'appareils connectés à Internet (*IoT*) ces dernières années contribue à offrir de nouvelles opportunités aux attaquants.

La figure suivante représente les dépenses de sécurité de l'industrie pour la sécurité de l'IoT en millions (dollars américains) et prévisions futures.



1 - Qu'est-ce qu'un Botnet ? :

Avant de parler des attaques DDoS nous devons expliquer qu'est-ce qu'un botnet. Tout d'abord, il faut savoir faire la différence entre un *botnet* traditionnel et un *botnet* IoT.

Un botnet (*bot network*) normal est un réseau d'ordinateur personnel avec des logiciels malveillants et contrôlés à distance par un pirate, ils fonctionnent principalement sous Windows.

Si nous comparons d'un botnet IoT **:** « Les botnets IoT ressemblent toujours étroitement aux botnets traditionnels, en ce sens qu'ils ont deux composants principaux. L'un est le serveur de commande et de contrôle (C&C) où un acteur de la menace envoie des commandes et contrôle le botnet. Et les seconds sont les bots ou zombies qui sont des appareils piratés ou infectés individuellement qui font partie d'un plus grand réseau de bots infectés de manière similaire. Ces bots peuvent être constitués d'autres composants communs, comme un scanner pour d'autres appareils vulnérables, un tueur de logiciels malveillants concurrents, un attaquant qui exécute des DDoS et, pour certains, une charge utile d'extraction de crypto-monnaie.(*Into the Battlefield: A Security Guide to IoT Botnets*, n.d.)».

Le réseau de rebots (*botnet*) IoT précisément DDos est utilisé principalement pour envoyer du spam par le responsable de l'attaque appelé *Master MindIntruder* (organisateur de l'attaque) et lancer des attaques DDoS à travers un nouvel acteur appelé *Client Attack Commander* via des carneaux IRC (*Internet Relay Chat*) qui saturent le serveur de la cible et consomment sa bande passante (*Consumer Bandwith*) et aussi rendre le temps de réponse lent (*Consumer Network Processing Power*).

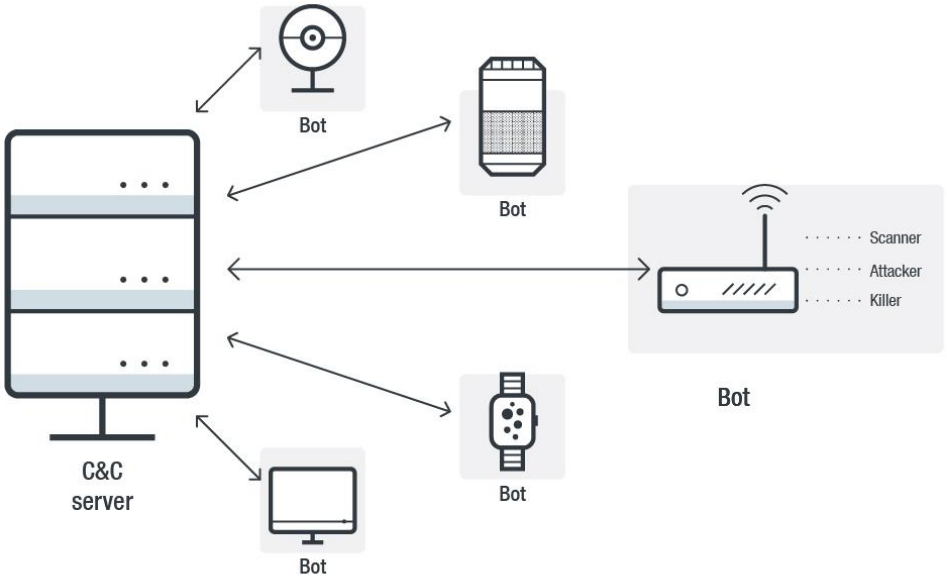


Figure 18 : Cible d'un botnet

2 - Motivation Des Attaques DDoS :

Le coût des attaques informatiques a augmenté de 4,9 millions de dollars à 7,5 millions de dollars, selon la commission de sécurité américaine, entre 2017 et 2018. Parmi les différents motifs des attaques DDos, nous citons :

2-1 - Financement

Les attaques DDoS touchent gravement de nombreux services bancaires et financiers, ce qui mène à paralyser l'accès aux services bancaires mobiles et en ligne.

2-2 - Demande de rançon

Tout en lançant des attaques DDoS contre, les entreprises par exemple, afin d'intimider et convaincre les victimes de payer une rançon demandée.

2-3 - Raisons politique

Les attaques DDoS à motivation politique sont les plus fréquentes et ont pour but de perturber le processus et le débat politique.

3 - DDoS et la 5G :

L'introduction de la 5G étendra considérablement les attaques DDoS, des chercheurs informaticiens déclarent que **127** nouveaux appareils IoT sont connectés par seconde.

Le principal moteur de croissance sera **:** « l'ajout d'un grand nombre d'appareils IoT au réseau mondial grâce à l'augmentation générale de la bande passante et à la réduction de la latence. En plus d'ajouter simplement des nombres bruts d'appareils exploitables, une latence plus faible signifie que le temps de réponse efficace aux attaques DDoS sera réduit à quelques secondes plutôt qu'à quelques minutes.

Cependant, l'étude souligne que ces facteurs donneront également une impulsion significative aux réponses de sécurité automatisées basées sur l'intelligence artificielle et les systèmes d'apprentissage automatiques (Gaurav et al., 2015)».

4 - Les types d'attaques DDoS dans les appareils Internet des objets (IoT) :

Les plus grandes attaques de botnet à déni de service distribué (DDoS) prennent les appareils Internet des objets (IoT) comme une cible principale depuis un certain temps, c'est une menace qui n'a jamais vraiment diminué car le nombre d'appareils Iot augmente jour après jour et les fabricants continuent de produire des appareils qui ne peuvent pas être correctement sécurisés.

Nous avons pu voir que le domaine des attaques DDoS est un complexe ce qui nécessite de connaitre les types des attaques dans les appareils IoT, nous en discutons certains comme suit (*Cooja Simulator*, n.d.) :

4-1 - Blackhole Attack :

Une attaque Blackhole dans un réseau signifierait qu'un ou plusieurs nœuds malveillants laisseraient tomber totalement ou partiellement les paquets de données qui y sont acheminés, ce qui entraînerait des perturbations dans le flux normal des données sur le réseau . Un nœud malveillant faussera les informations de routage, se présentera comme le meilleur chemin vers le nœud de contrôle (appelé Node Sink), pour forcer le passage des données par lui-même. Sa

seule mission est alors de ne rien transférer, créant une sorte de puits ou de blackhole dans le réseau. L'intrus se place à un emplacement stratégique de routage dans le réseau et supprime tous les messages qu'il doit retransmettre, entraînant la suspension du service de routage du réseau dans les routes qui passent par le nœud du pirate. Si un nœud malveillant a la capacité d'usurper l'identité d'un nœud valide du réseau, il peut le faire lorsque le mécanisme de découverte d'itinéraire répond au nœud initiateur par un message de rediffusion routière en annonçant un chemin avec un coût minimal au nœud demandé. Le nœud émetteur mettra alors à jour sa table de routage avec cette fausse route.

4-2 - Lizard Stresser :

Ce botnet est un outil simple écrit en langage C et capable de fonctionner sur des appareils IoT. Il implémente une méthode de force brute pour se connecter à différentes adresses IP à l'aide des informations d'identification utilisateur définies par défaut par le fabricant.

Les appareils dotés de protocoles d'authentification qui ne peuvent pas être modifiés par l'utilisateur et codés en dur par le fabricant sont susceptibles d'être infectés à l'aide de cet outil.

4-3 - Hello flood Attack :

Le protocole de routage nécessite que les nœuds voisins d'un même réseau échangent des messages HELLO pour indiquer leur présence et leur disponibilité, découvrir des routes et mettre à jour les tables de routage. Le nœud malveillant envoie un nombre énorme de paquets HELLO à différents nœuds pour se présenter comme voisin, afin qu'ils lui transmettent leurs données.

4-4 - Nitol :

Cet outil permet aux logiciels malveillants d'infecter un appareil IoT et communique avec le serveur de commande et de contrôle via un socket TCP. Il transmet les informations de l'appareil à l'attaquant, telles que la puissance de calcul.

4-5 - Mr Black :

Cet outil est utilisé pour infecter les routeurs en contactant des serveurs distants, qui agissent comme une commande et un contrôle. L'appareil envoie ses informations de performances au serveur, le serveur conserve des informations sur tous les appareils infectés. Il

permet également à l'appareil de télécharger un fichier exécutable via une commande de contrôle pour lancer une attaque DDoS, puis mettre fin à la connexion.

4-6 - Mirai code :

Cet outil est écrit dans la langue Go, il localise les appareils IoT non sécurisés en scannant différentes adresses IP.

Une fois qu'il a localisé l'adresse IP d'un appareil IoT non sécurisé, il tente d'y accéder via une méthode de force brute en devinant le mot de passe et l'ID à l'aide des informations d'identification utilisateur définies par défaut par le fabricant.

Il peut lancer des attaques DDoS sur les serveurs et les réseaux tels que les attaques SYN-ACK, UDP, DNS et HTTP flood.

XI - La sécurité internet des objets

1 - La sécurité Technique

La cryptographie joue un rôle important, puisqu'elle permet d'adresser au moins partiellement les problématiques de confidentialité, d'intégrité, de disponibilité et de non-répudiation. Des outils cryptographiques appropriés et prêts à l'emploi existent aujourd'hui pour quasiment tous les besoins de sécurité imaginables. Plus globalement, il est vivement recommandé d'utiliser systématiquement les bonnes pratiques existantes à tous les niveaux, et d'éviter les mesures de sécurité ‘‘ originales ‘‘ ou ‘‘ créées sur mesure ‘‘. Des composants réutilisables, fiables et éprouvés sont toujours bien plus sûrs qu'un code ou protocole créé spécialement pour la solution, et non éprouvé(Blanc, n.d.)

2 - Sur physique de l'objet

Par exemple contre la copie physique ou celle de son micrologiciel.

- Le scellement du boîtier des objets connectés : il s'agit de ‘‘ verrouiller ‘‘ le boîtier de l'objet par (collage, thermocollage, soudure, ...) de façon à empêcher son ouverture normale, au détriment, il est vrai de pouvoir facilement réparer l'objet. Cela permet aussi de voir si l'intégrité physique de l'objet a été atteinte au premier coup d'œil.

- Le moulage des cartes et composants électroniques dans de la résine (si possible opaque aux rayons X) : cela empêchera l'identification des composants utilisés, ainsi que leur analyse par mesure ou débogage.
- La désactivation des ports de débogage et de lecture mémoire des composants pour empêcher l'analyse de leur comportement et des données traitées.
- L'utilisation de composants sécurisés pour le stockage des clés et les traitements cryptographiques : cela rend quasiment impossible l'extraction des secrets stockés dans l'objet.
- L'utilisation de clés et mots de passe tous différents dans chaque périphérique : pour éviter qu'une compromission sur un périphérique ne puisse compromettre l'intégralité du parc.
- Le chiffrement et l'obfuscation du micrologiciel : même s'il s'agit de sécurité par l'obscurité, jamais efficace à long terme, cela ralentit considérablement le travail d'analyse et de rétro-ingénierie du micrologiciel, et donc son altération ou sa copie.(Blanc, n.d.)

3 - Sur les protocoles de communication

Il y a trois principales menaces récurrentes sur les communications : l'écoute passive, le brouillage (volontaire ou involontaire), et l'usurpation, Il y a quelques conseils :

Pour aller plus loin, un audit de la sécurité de la chaîne complète du flux de données afin d'identifier l'ensemble des vulnérabilités pour bien comprendre les risques et les solutions à mettre en place par la suite :

- Le chiffrement des communications sensibles.
- L'authentification des objets les uns avec les autres : on parle alors d'authentification mutuelle, ce qui évite les attaques de type ‘‘ Man-in-the-Middle ‘‘. Habituellement, cette authentification est faite sous forme d'une procédure de pairage, ou par certificat électronique.
- L'utilisation de protocoles sécurisés d'échange de clés : le plus courant étant le protocole Diffue-Hellman, attention ce dernier nécessite auparavant d'avoir authentifié les périphériques concernés pour éviter l'interception par un tiers.
- L'utilisation de mécanismes anti-rejeu, comme les authentifications par challenge ou les numéros de séquence uniques et authentifiés (‘‘ nonce ‘‘ cryptographiques).

- L’utilisation de mesures antibrouillage, comme l’étalement de spectre (‘‘ spread spectrum ‘‘) ou les sauts de fréquence (‘‘ frequency hopping ‘‘ / ‘‘ channel hopping ‘‘), utilisés dans certains protocoles comme Bluetooth.
- Certaines de ces mesures sont implémentées de base dans les protocoles sans fil. Celles qui ne sont pas implémentées peuvent souvent l’être au niveau de la couche applicative, donc restant à la charge du développeur.(Blanc, n.d.)

4 - Sur la sécurité applicative et système

Enfin, la solution connectée peut-être attaquée par son maillon applicatif, que ce soit côté client (smartphone, tablette, micrologiciel, …) ou côté serveur (passerelle, serveur sur le cloud, …).

Il y a les recommandations importantes ci-après :

- Le choix et l’utilisation de briques applicatives répandues et régulièrement mises à jour.
- L’implémentation des contrôles côté serveur, car les contrôles côté client sont manipulables et contournables par un utilisateur malintentionné.
- Le filtrage et la validation de toutes les entrées, et si possible des sorties des traitements effectués. De manière générale, n’accorder aucune confiance aux données reçues.
- L’application d’une sécurité en profondeur, en donnant aux utilisateurs les privilèges minimums à leur utilisation de la solution et en redondant les mécanismes de sécurité eux-mêmes.
- L’utilisation de procédures et référentiels de durcissement système sur les serveurs de la solution : suppression des comptes et services non utilisés, applications de mots de passe forts sur tous les comptes, mises à jour régulièrement appliquées, monitoring actif des accès, veille permanente sur les vulnérabilités affectant les composants de la solution connectée(Blanc, n.d.)

XII - Objectifs de la sécurité

La sécurité informatique d’une manière générale consiste à assurer que les ressources matérielles et logicielles d’une organisation sont uniquement dans le cadre prévu. Elle vise à assurer plusieurs objectifs, dont les cinq principaux sont : L’authentification, L’intégrité, la disponibilité et la non-répudiation (Y.ait mouhoub, 2015)

Service	Solutions proposées	Remarques
Confidentialité	- VPN - TLS - DNS - Onion routing - PIR - Contrôle d'accès - Cloud computing	-La confidentialité est nécessaire pour protéger Les données sensibles. -Difficulté d'appliquer les solutions directement Au contexte de l'IoT en raison de l'extensibilité Et de contrôle d'accès. -Une politique de confidentialité doit être appliquée. -En général l'utilisateur privilégie du bénéfice du service face au risque de sa vie privée.
Authentification	- Mitiger les attaques par Déni de service. - Utilisation des techniques De détection d'intrusions Et d'authentification.	-Les limites de ressources dans l'IoT rendent difficile L'utilisation des algorithmes cryptographiques en Raison de leur consommation en termes de calcul Et de mémoire. - Des recherches sont en cours afin de rendre ces algorithmes peu couteux et robustes à la fois.
Identification	- RFID - 6LoWpAN - IPv6 - Identification biométrique	- L'identification est cruciale pour l'IoT afin de faire correspondre les services avec leur demande. - L'identification permet de connaitre l'identité D'une entité. - Une identification robuste et scalable jouera Un rôle déterminant dans la sécurité de l'IoT. - Les ressources limitées de ces objets rendent aussi difficile l'implémentation de ces technologies.

Tableau 3 : Services de sécurité d'IoT

1 - Les réseaux privés virtuels (VPN) :

Sont des extranets établis par des groupes proches de partenaires commerciaux. Comme seuls les partenaires ont accès, ils promettent d'être confidentiels et d'avoir de l'intégrité. Cependant, cette solution ne permet pas un échange d'informations global dynamique et n'est pas pratique pour les tiers au-delà des frontières de l'extranet (Weber, 2010).

2 - Transport Layer Security (TLS) :

Basé sur une structure de confiance mondiale appropriée pourrait également améliorer la confidentialité et l'intégrité de l'IoT. Toutefois, comme chaque étape de délégation ONS

nécessite une nouvelle connexion LS, la recherche d'informations serait affectée négativement par de nombreuses couches supplémentaires (Weber, 2010).

3 - Les extensions de sécurité DNS (DNSSEC) :

Utilisent la cryptographie à clé publique pour signer des enregistrements de ressources afin de garantir l'authenticité de l'origine et l'intégrité´ des informations livrées. Toutefois, la DNSSEC ne peut assurer l'authentification de l'ONS que si l'ensemble de la communauté internet l'adopte (Weber, 2010).

4 - Onion Routing :

Crypte et mélange le trafic Internet à partir de nombreuses sources différentes, c'est-`a-dire les données sont enveloppées dans plusieurs couches de cryptage, en utilisant les clés publiques des routeurs union sur le chemin de transmission. Ce processus empêcherait l'appariement d'un paquet de protocoles internet particulier à une source particulière. Cependant, le routage d'onion augmente les temps d'attente et entraîne ainsi des problèmes de performance (Weber, 2010).

5 - Les systèmes privés de récupération d'information (PIR) :

Cachent quel client est intéressé par les informations, une fois que les EPCIS ont été localisés. Cependant, des problèmes d'évolutivité et de gestion des clés, ainsi que des problèmes de performance, se poseraient dans un système globalement accessible tel que l'ONS, ce qui rend cette méthode peu pratique (Weber, 2010).

6 - Peer-to-Peer (P2P) system:

est une autre méthode pour augmenter la sécurité et la confidentialité, qui montre généralement une bonne évolutivité et de performance dans les applications, P2P pouvait être basé sur des tables de hachage distribuées (DHT) (Weber, 2010).

7 - Contrôle d'accès :

Assurer la confidentialité dans les systèmes de gestion de la connaissance. Une approche standard, qui correspond bien aux caractéristiques des environnements IoT, est représentée par le contrôle d'accès basé sur les rôles (RBAC)(Miorandi et al., 2012).

8 - Cloud comptant :

Est une autre méthode pour l'assurer la confidentialité, si les périphériques IoT transmettent des données au cloud via la connexion HTTP, l'intégrité des données est atteinte. Dans le cas de HTTPS, la confidentialité et à l'intégrité sont atteintes à la fois (Gaurav et al., 2015).

9 - RFID :

L'identification par radiofréquence (RFID) est l'une des technologies les plus importantes utilisées dans l'IoT, car elle peut stocker des données sensibles, communiquer sans fil avec d'autres Objets et identifier/tracer des Objets automatiquement (He & Zeadally, 2014). La technologie RFID est un outil clé pour l'IoT, car elle permet l'identification simultanée d'un grand nombre d'Objets avec des étiquettes cout efficacité (Aggarwal et al., 2013). Dans le domaine des soins de santé, la technologie RFID est utilisée au sein de l'IoT et les applications courantes, y compris le suivi de localisation des actifs médicaux (He & Zeadally, 2014).

10 - 6LoWpAN :

Définit en particulier des mécanismes d'encapsulation et de compression d'en-têtes permettant aux paquets Ipv6 d'être envoyées ou reçus via le protocole de communication pour réseaux radio IEEE 802.15.4. Le standard 6Lowpan ne prévoit pas de fonctions de sécurité en plus de celles potentiellement mises en œuvre au niveau du 802.15.4 et de Ipv6. 6lowpan permet une intégration complète de WSN dans l'internet (Porambage et al., 2014).

11 - IPv6 :

Une des technologies préconisées `a l'IETF pour l'interconnexion des réseaux de l'IoT est IPv6. Un des avantages majeurs est l'exploitation de l'immense capacité d'adressage de 128 bits d'IPv6 ce qui répondrait aux besoins d'adressage a très large échelle d'un IoT qui comporterait potentiellement plusieurs dizaines de milliards d'Objets (Benghozi et al., 2008).

12 - Identification biométrique :

R. Greenstadt et J. Beal ont proposé l'utilisation d'une imprégnation des Objets puis une identification biométrique continue pour la protection des Objets. Cette identification biométrique peut être diverse et variée comme les empreintes, l'image de la rétine, la fréquence de la voix, le mouvement, la reconnaissance du visage, etc. L'objectif est de permettre une reconnaissance assez naturelle du propriétaire de l'Objet et ainsi éviter un tas de failles et d'attaques de sécurité par de tierces parties non l´légitimes à manipuler les Objets (Greenstadt & Beal, 2008).

Conclusion :

Parmi les défis majeurs de l'IOT c'est Le manque de normes dans l'Internet des Objets est très clairement un frein à la sécurité. Il manque tout d'abord des spécifications ouvertes sur beaucoup de protocoles sans fil et de systèmes embarqués existants. Mais au-delà, même lorsque des spécifications existent, il est rarissime de trouver des référentiels de sécurité sur ces technologies Pour résumer ce que nous venons de voir, nous devons protéger notre infrastructure contre ce type d'attaque, notre système de sécurité doit être robuste et fiable, il est à noter que nous n'avons pas évoqué en détail DDoS, le chapitre suivant on va présenter quelque algo de classification des attaques de ce genre et on va simuler certaines attaques et nous proposons une solution par l'utilisation de l'apprentissage automatique IDS dans le suivant chapitre.

Chapitre 4 : Simulation et Contribution dans la détection d’intrusion

Chapitre 04 : simulation et Contribution dans la détection d'intrusion

Introduction :

Après avoir présenté le cadre théorique de notre travail, on se penche maintenant sur la deuxième partie dans le but de présenter notre simulation et extraire l'ensemble des données nécessaires dans notre test. On va construire un model IDS efficace aux attaques DDos dans l'environnement IoT

Ce chapitre est divisé en trois parties, dans la première nous présentons les travaux antérieurs et les différentes outils utilisés, premièrement le simulateur Cooja pour la simulation des attaques dans un environnement IoT, nous mettrons l'accent beaucoup plus sur l'attaque hello flood, deuxièmement nous utilisons le Wireshark pour capturer les données nécessaires sur l'attaque et extraire notre dataset, et enfin nous présentons notre modèle et les différents résultats d'expérimentation avec notre proposition dans ce travail en utilisant le Weka.

I - Travaux connexes :

En particulier, nous appuyons le travail réalisé par Naeem Firdous Syed, Zubair Baig, Ahmed Ibrahim & Craig Valli à propos de la détection des attaques Dos via Machine Learning.

Le model de détection Dos a montré que les fonctionnalités MQTT proposées offraient des capacités de détection élevées dans les réseaux IoT.

L'efficacité de l'ensemble des fonctionnalités proposées a été validée à l'aide de trois algorithmes d'apprentissage automatique fondamentalement différents, à savoir, AODE basé sur Naïve Bayes, C4.5 basé sur Decision Tress et MLP basé sur ANN. Automatique.

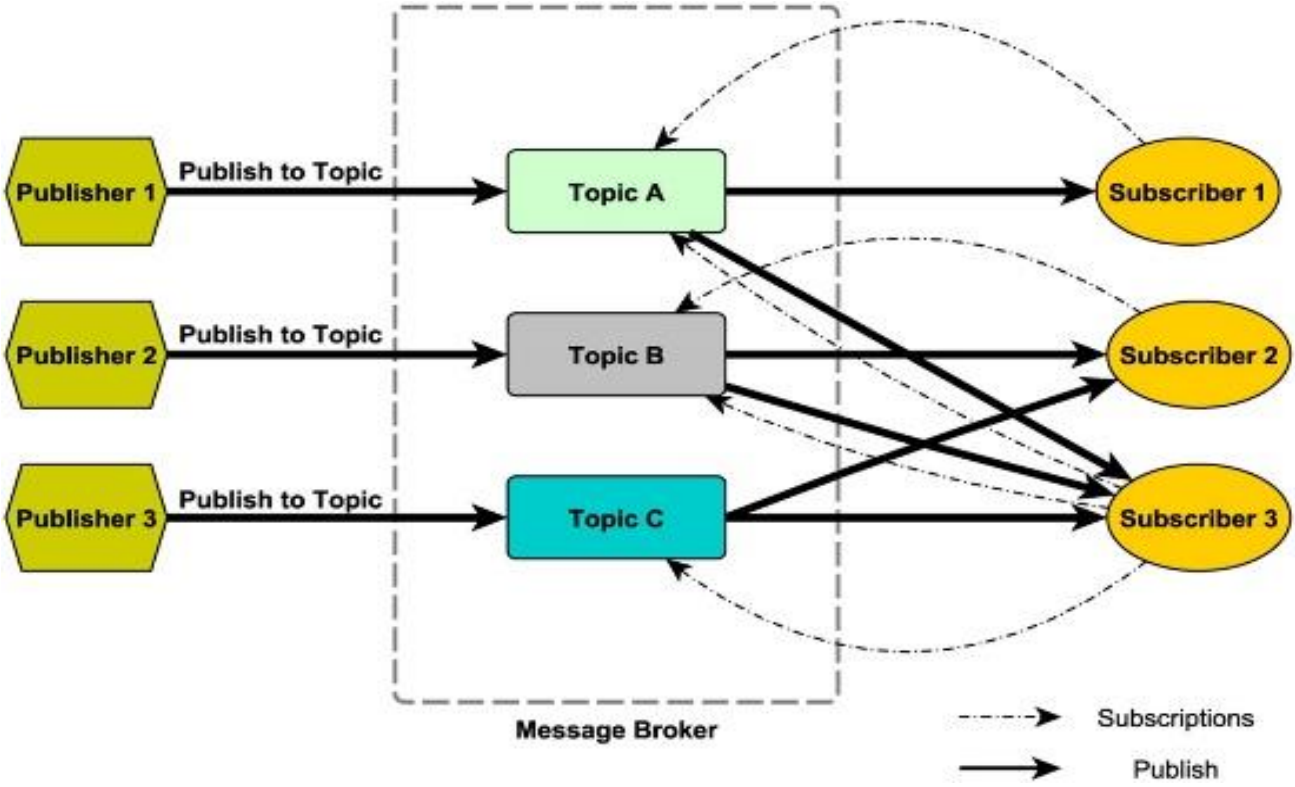


Figure 19 : Publish/subscribe process in MQTT.

Diverses mesures d'attaque ont été mesurées pour évaluer l'impact des attaques DoS contre les courtiers MQTT. Ceux-ci incluent : l'utilisation du processeur, la bande passante et l'utilisation de la mémoire.

Le model de détection DoS a montré que les fonctionnalité MQTT proposées offraient des capacités de détection élevées des attaque DoS dans les différent IoT.

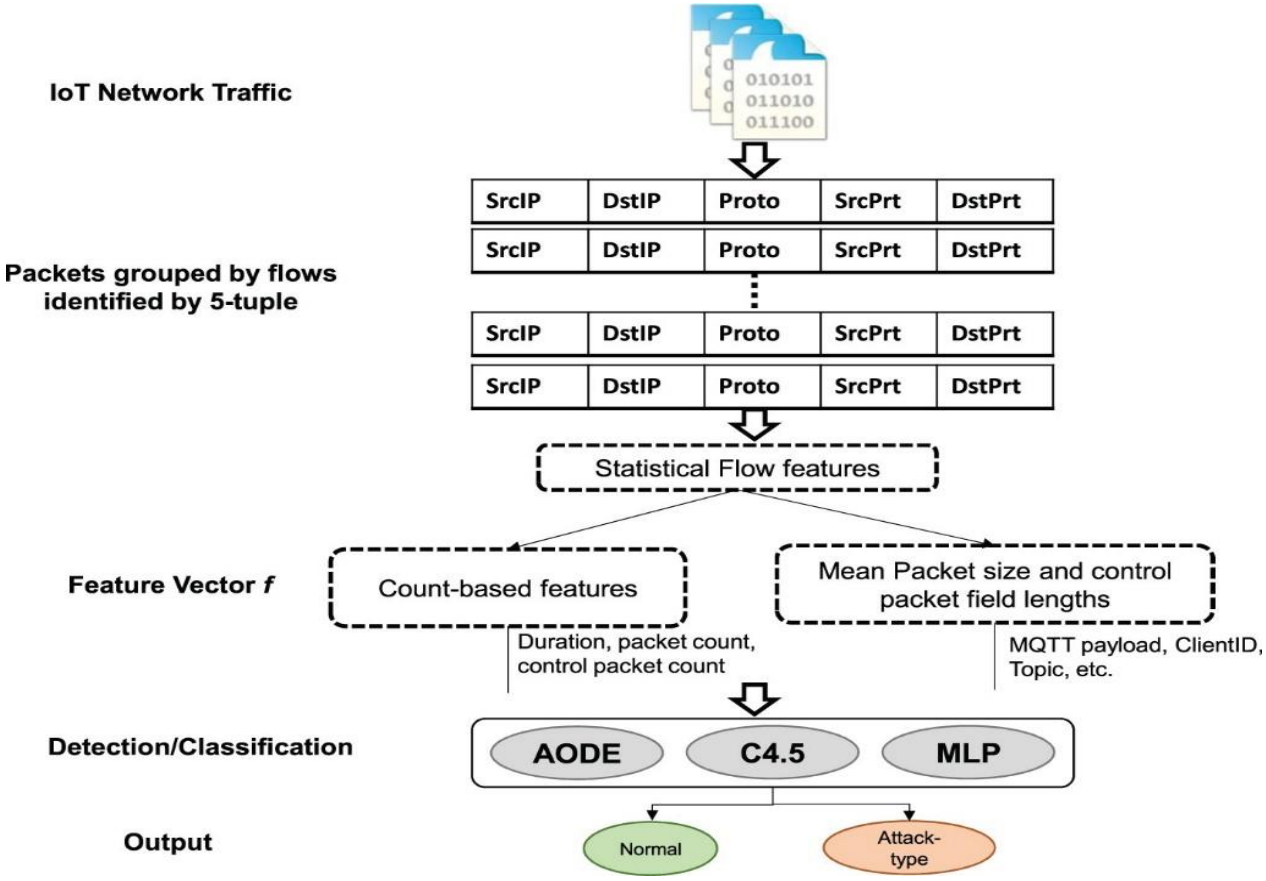


Figure 20 : Flux de travail du cadre de détection pour la détection des attaques MQTT.

II - Le simulateur Cooja Contiki :

Contiki est un système d'exploitation flexible et léger pour les réseaux de capteurs, open source, écrit en C et peut être utilisé dans des systèmes commerciaux et non commerciaux. Il fonctionne avec un minuscule microcontrôleur à faible coût et développe des applications qui utilisent efficacement le matériel et qui fournissent une communication sans fil standardisée à faible consommation pour la variété des plates-formes de matériel (*No Title*, n.d.-a)**.**

Contiki dispose l'un des outils majeurs appelé Cooja qui permet aux développeurs de tester leur code avant de s'exécuter sur le matériel cible. Cooja est un simulateur logiciel conçu pour les réseaux de capteurs sans fil, il est open source, construit en java, capable d'exécuter des programmes C, C+++, supporte IPV4, IPV6, ainsi que les derniers standards pour les réseaux sans fil basse consommation tels que 6LoWPAN, RPL et permet le déploiement de nombreux types de moteurs comme Z1, Skymote, MicaZ etc.

Nous expliquons maintenant les étapes suivis pour accéder au simulateur :

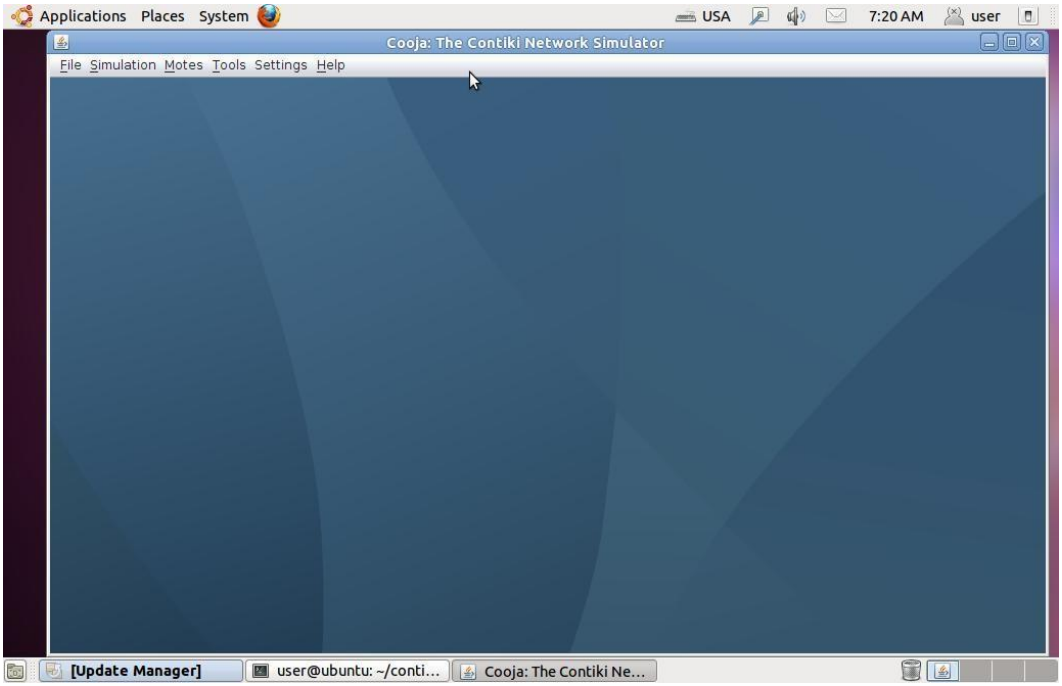


Figure 21 : Premier affichage Cooja

On clique sur File (Fichier), puis sur New Simulation (Nouvelle simulation) et l'écran illustré à la Figure 22 s'affiche à nouveau. Il n'est pas nécessaire de modifier les paramètres de cet écran.

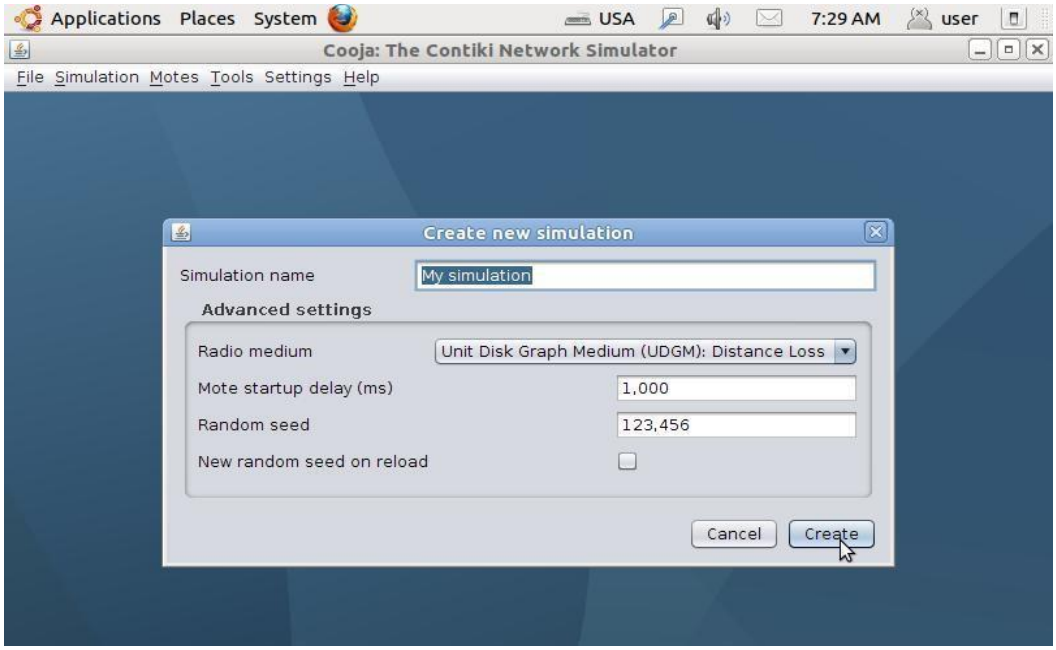


Figure 22 : Création d'une nouvelle simulation

Le bouton Create permet de lancer l'écran de simulation initial, comme le montre la Figure 23

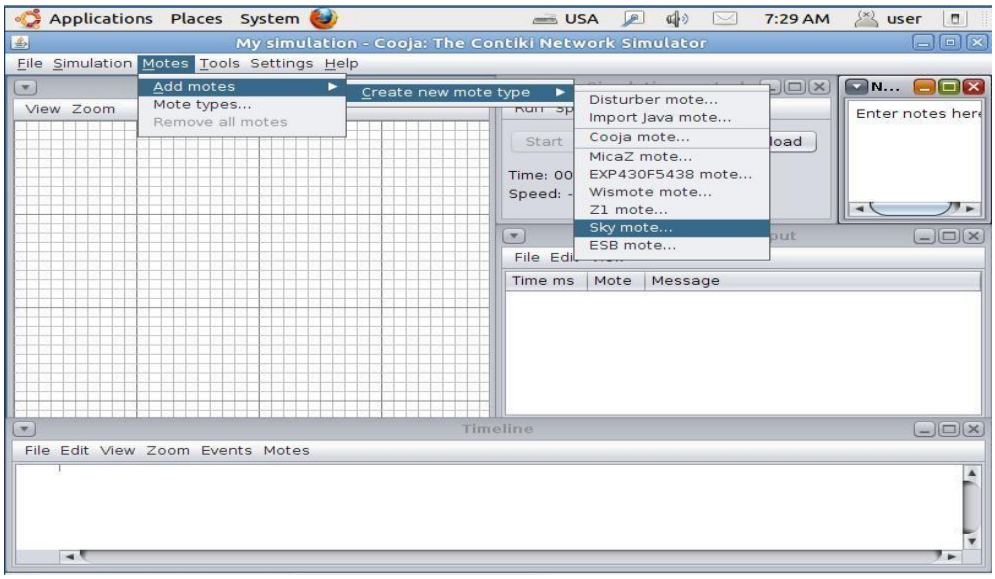


Figure 23 : Écran initial de simulation Cooja

Pour l'instant, il n'y a rien à faire car il n'y a pas encore de Motes dans le réseau. Celles-ci sont ajoutées en cliquant sur Motes, Add motes, (Ajouter des motes) Créer un nouveau type de Mote et ensuite Sky Mote à partir du menu qui en résulte, comme le montre la Figure 24

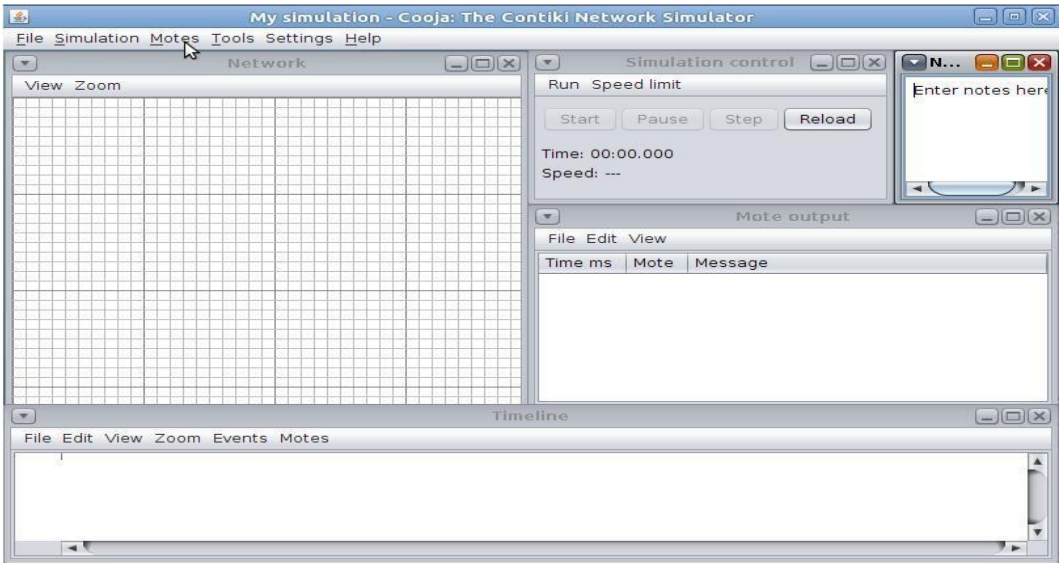


Figure 24 : Ajouter Motes

La Sky Mote est la plus simple des Motes à utiliser dans un WSN et idéal pour les configurations initiales dans une simulation Cooja. L'écran qui en résulte est affiché à la Figure 25

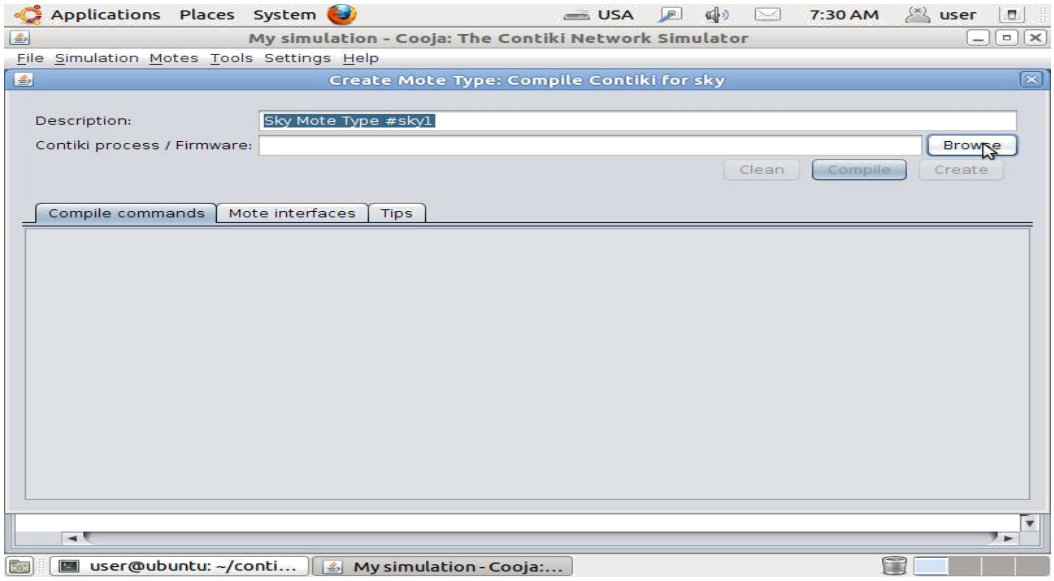


Figure 25 : parcourir le Mote

Comme on peut le voir dans la Figure 26, il y a un dossier exemples et c'est là que se trouve le Firmware, avec de très nombreuses options disponibles. Comme cet exemple implique l'utilisation de RPL, le chemin sélectionné est

/home/user/contiki/examples/ipv6/rpl-collect/udp-sink.c. udp-sink.c. udp-sink c'est le firmware en langage C du mote qui va maintenant être créé.

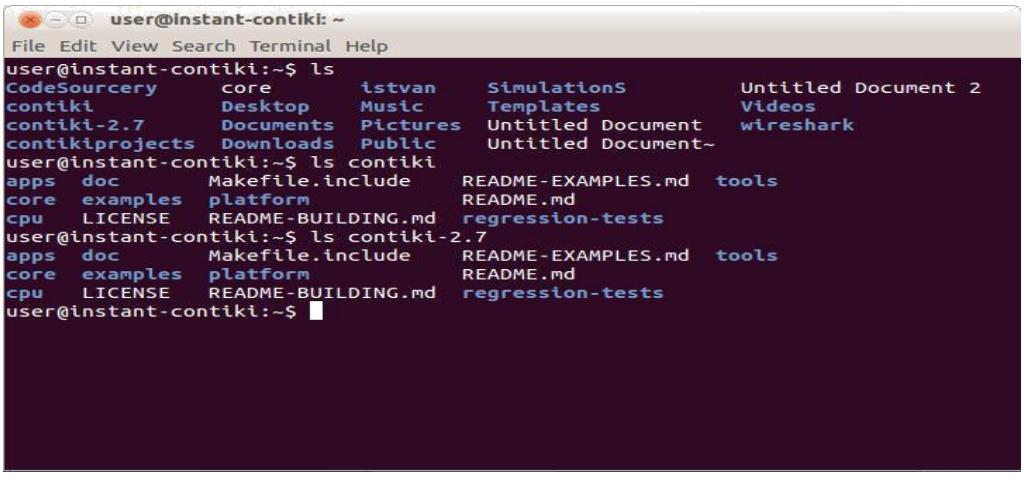


Figure 26 : Les fichiers contiki

On clique sur Clean (Nettoyer) pour effacer toute compilation précédente de la mote, puis sur Compile. Il en résultera une sortie comme dans la Figure 27 qui montre la sortie de compilation. Il y aura toujours un code d'avertissement en rouge, à condition qu'il n'y a pas des erreurs en rouge, à la fin de la sortie que le mote a compilé avec succès.

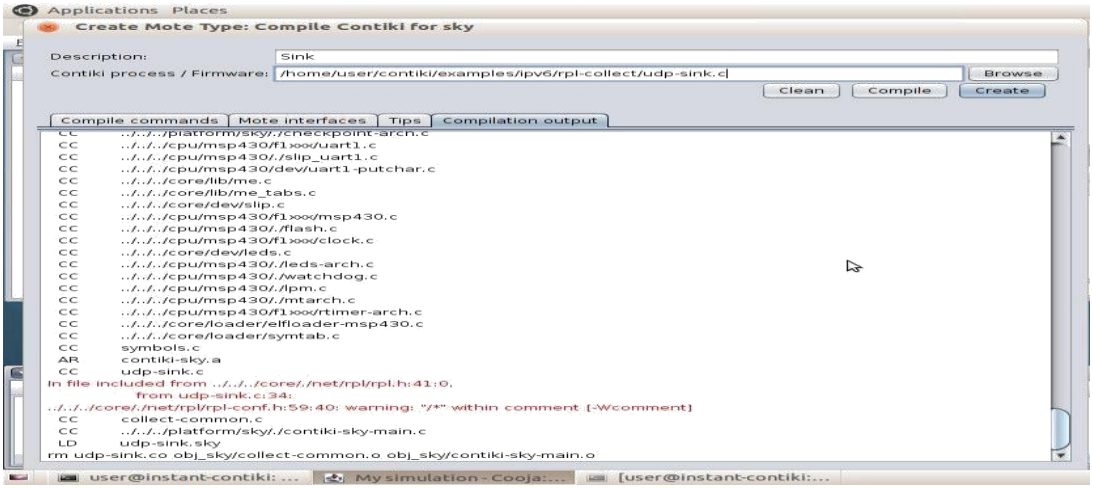


Figure 27 : Compilation de Mote Cooja

On clique maintenant sur Create pour faire apparaître l'option permettant de créer le nombre de Motes requises. Une case apparaîtra comme sur la figure 28.

Comme il s'agit d'une Mote Sink seulement un est nécessaire, cliquez sur Ajouter des Motes et la Mote est ajoutée. Ce processus doit être répété pour les Motes expéditeur avec le chemin du firmware Mote maintenant /home/user/contiki/examples/ipv6/rplcollect/udp-sender.c. Dans cet exemple nous allons ajouter 5 Motes expéditeur.

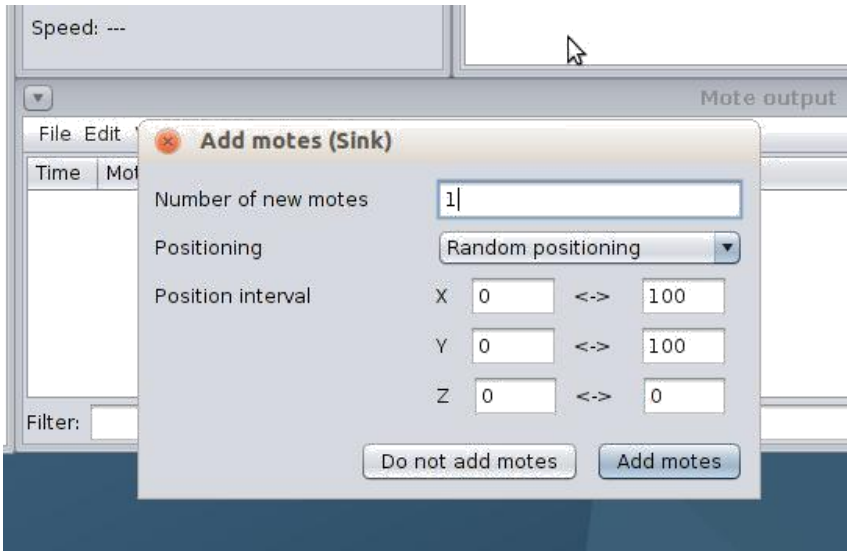


Figure 28 : Ajouter des Motes Cooja

Une fois qu'on clique sur le bouton Ajouter des Motes, un écran similaire à celui de la Figure 29 est affiché, montrant les Motes du réseau avec le numéro 1 étant Sink Mote.

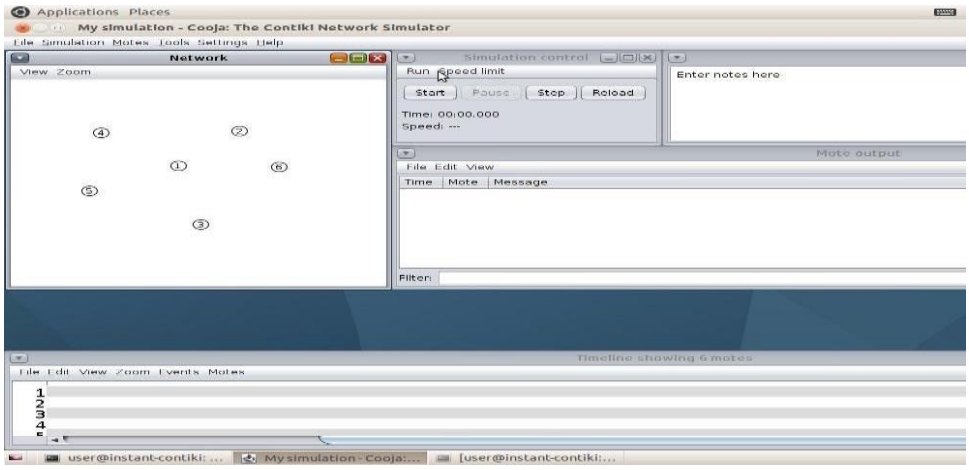


Figure 29 : Topologie initiale crée

1 - Installation :

Sous Ubuntu 14.7

1-1 - Cloner ce dépôt :x

```
$ git clone https://github.com/dhondta/rpl-attacks.git
```

1-2 - Créer la VM :

```
$ vagrant login
[...]
$ vagrant up
```

1-3 - Descriptions :

Cela fera 3 exemples d'attaques complets : hello flood, numéro de version et blackhole. On ouvre la console comme avant et on tape :

```
user@instant-contiki:rpl-attacks>> demo
```

Ou lancez simplement la commande de demo avec Fabric :

```
./rpl-attacks$ fab demo
```

1-4 - Démarrage rapide (à l'aide de la console intégrée) :

On ouvre la console, nous devons voir apparaitre l'une des lignes suivantes :

```
./rpl-attacks$ fab console
```

Ou

```
./rpl-attacks$ python main.py
```

Ou

```
./rpl-attacks$ python main.py
```

Puis :

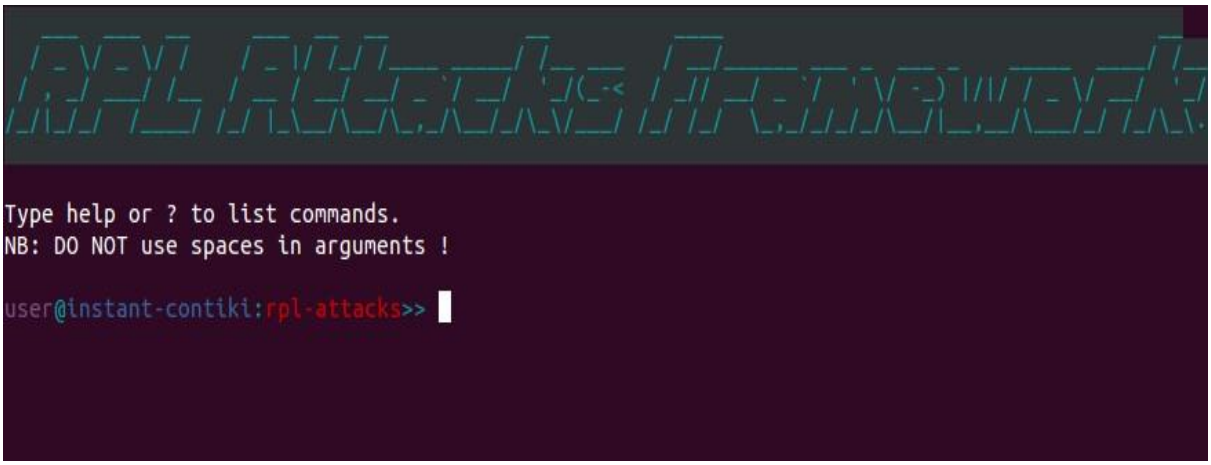


Figure 30 : terminal de RPL Framework

2 - Simulation d'attaque hello-flood :

2-1 - Introduction :

L'objectif de cette partie est de démontrer que ce type d'attaque peut avoir un impact dramatique sur un WSN via un épuisement énergétique important.

Le nœud malveillant commence immédiatement à envoyer des messages DIS à ses voisins, puis déclenche la réinitialisation des messages DIO et des minuteries de maintien.

2-2 - Configuration :

Le WSN contient :

- 1 nœud racine de type root-dummy construit sur un Z1
- 10 capteurs de type capteur-mannequin construits sur un Z1
- 1 grain malveillant de type malware-sensor construit sur un Z1

Les capteurs sont répartis sur une zone de 200,0 mètres de côté et centrés autour du nœud racine à une distance minimale de 20,0 mètres et une distance maximale de 200,0 mètres. Ils ont une portée de transmission maximale de 50,0 mètres et une portée d'interférence maximale de 100,0 mètres.

1.

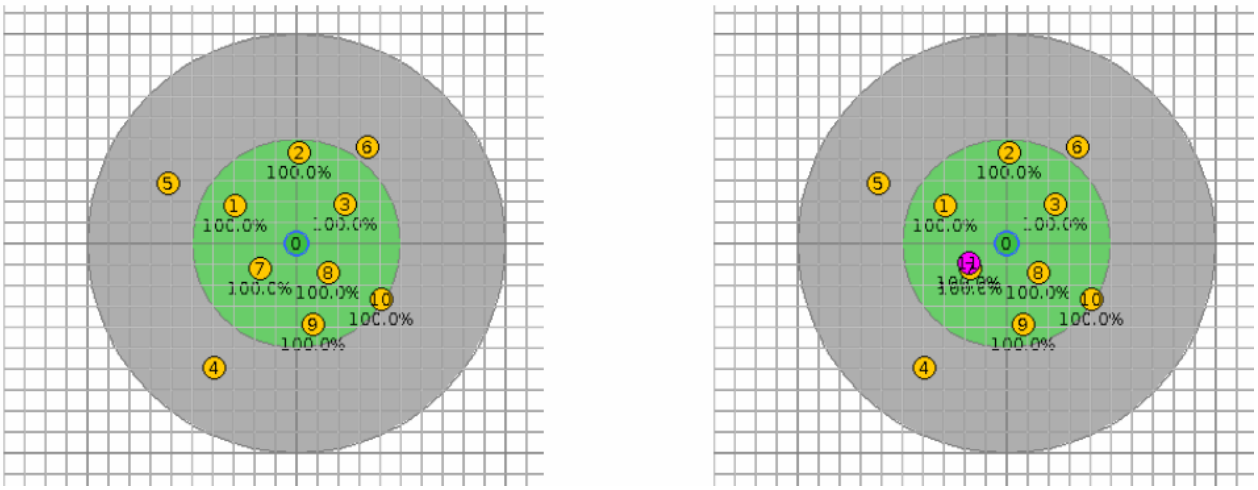


Figure 31 : Configuration WSN sans le malveillant et avec le malveillant

3 - Capturer les données avec Wireshark :

3-1 - Introduction :

Wireshark est un logiciel d'analyse de protocole réseau open source lancé par Gerald Combs en 1998. Wireshark est absolument sûr à utiliser. Les agences gouvernementales, les entreprises, les organisations à but non lucratif et les établissements d'enseignement utilisent Wireshark à des fins de dépannage et d'enseignement. Il n'existe pas de meilleur moyen d'apprendre la mise en réseau que de regarder le trafic sous le microscope Wireshark (Adrien Haccoun, n.d.).

3-2 - Téléchargement de Wireshark :

À partir d'une invite de terminal (Ubuntu), exécutez ces commandes :

- Sudo apt-get install wirehark
- Sudo dpkg-reconfigure wireshark-common
- Sudo adduser $ USER WireShark

3-3 - Capture de paquets de données sur Wireshark :

Lorsque vous ouvrez Wireshark, vous voyez un écran qui vous montre une liste de toutes les connexions réseau que vous pouvez surveiller. Vous disposez également d'un champ de filtre de capture, de sorte que vous ne capturez que le trafic réseau que vous souhaitez voir.

3-4 - Filtres Wireshark :

On peut filtrer les paquets selon plusieurs options, les filtres vous permettent d'afficher la capture de la manière dont vous avez besoin de la voir afin que vous puissiez résoudre les problèmes rencontrés.

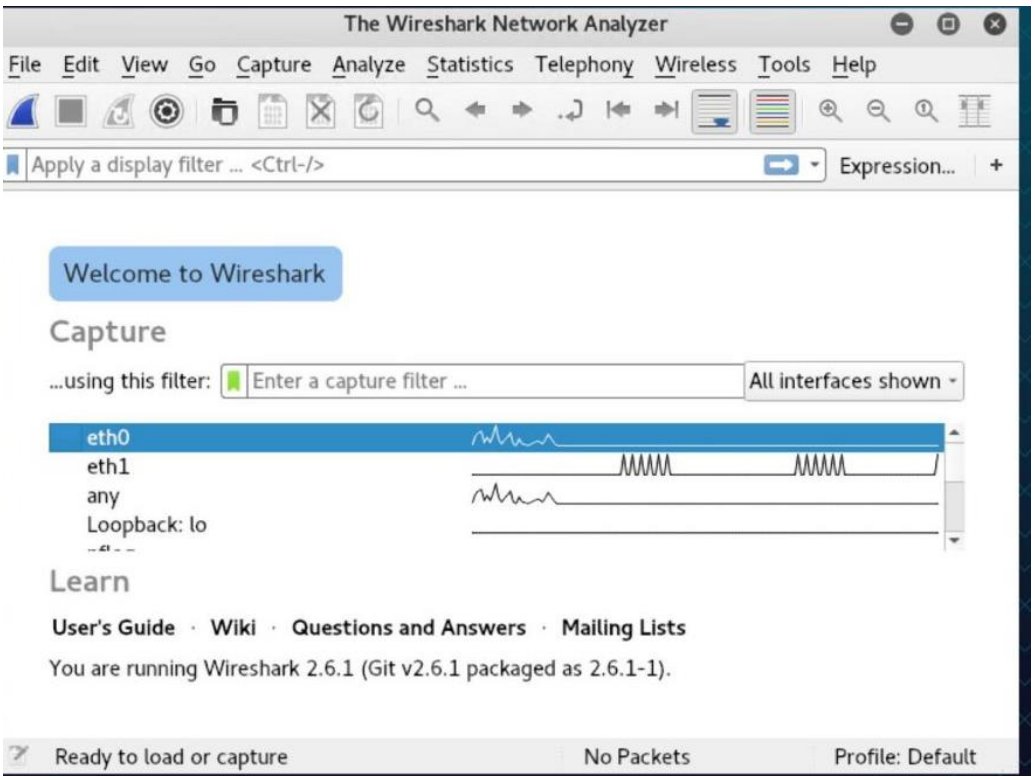


Figure 32 : Interface de démarrage de l'outils Wireshark

Cliquez sur le premier bouton de la barre d'outils, « Démarrer la capture des paquets ».

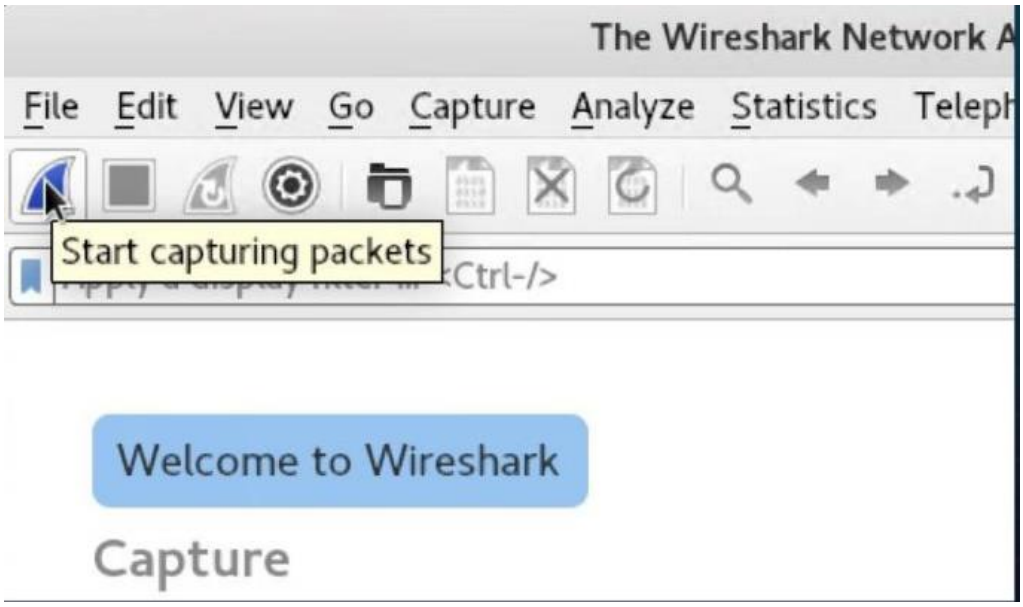


Figure 33: Start capturing Wireshark

Pendant la capture, Wireshark vous montrera les paquets qu'il capture en temps réel

.

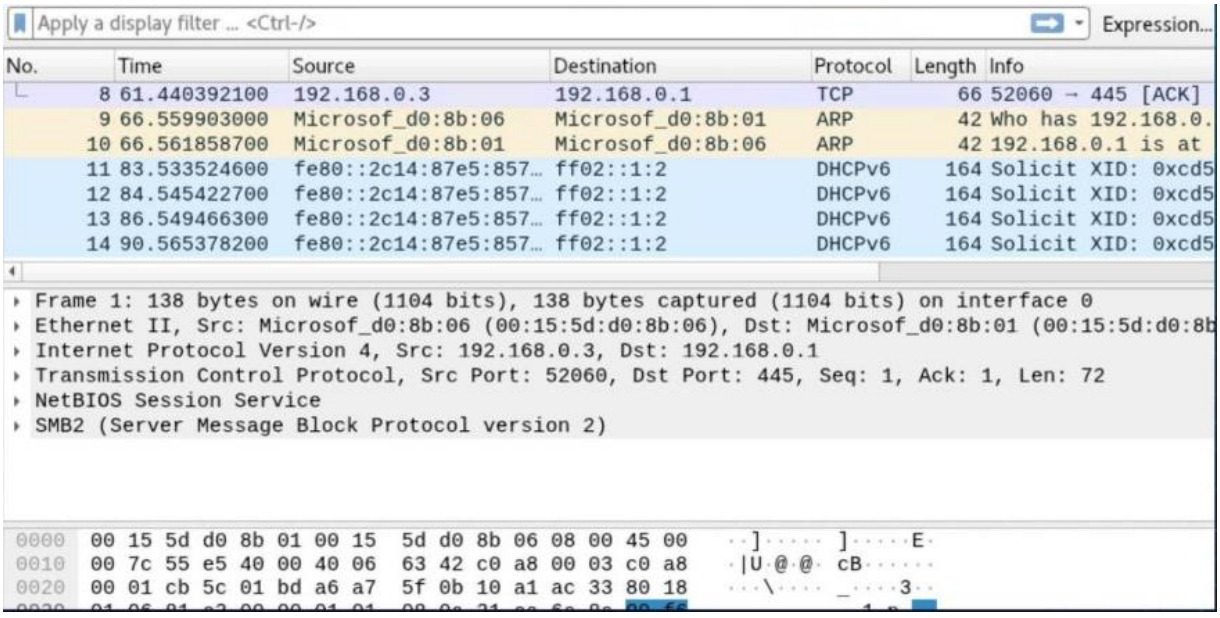


Figure 34 : Échantillon des paquets capturés

III - Techniques de classification :

1 - Apprentissage automatique :

L'apprentissage automatique (« *machine Learning* ») est une méthode utilisée en intelligence artificielle. Il s'agit d'algorithmes (*procédures traduites en langages*

informatiques) qui analysent un ensemble de données afin de déduire des règles (une étape dite « d'entraînement ») constituant des connaissances permettant d'analyser de nouvelles situations. De grands ensembles de données (des *big data*) sont nécessaires pour l'entraînement des algorithmes d'intelligence artificielle(*No Title*, n.d.-b).

2 - Apprentissage Supervisé :

Dans ce type d'apprentissage, nous disposons d'un ensemble de données contenant des caractéristiques, mais chaque exemple est également associé à une étiquette (Label) ou à une cible.

Parmi les modèles phares de ce type d'apprentissage nous comptons les Réseaux de neurones, cette technique a été utilisée avec succès dans la reconnaissance de formes, Traitement automatique de la langue et d'autres applications innovantes(*Apprentissage Supervisé*, n.d.).

3 - Apprentissage Non-Supervisé :

L'apprentissage non supervisé consiste à apprendre à un algorithme d'intelligence artificielle (IA) des informations qui ne sont ni classées, ni étiquetées, et à permettre à cet algorithme de réagir à ces informations sans supervision(*No Title*, n.d.-b).

IV - Les Algorithmes de classification :

1 - SVM (Support Victor Machine) :

SVM Est un algorithme d'apprentissage automatique supervisé qui peut être utilisé à la fois pour des problèmes de classification ou de régression. Cependant, il est principalement utilisé dans les problèmes de classification. Dans cet algorithme, nous plaçons chaque donnée sous forme de point dans un espace à n dimensions (où n est le nombre de caractéristiques que vous avez), la valeur de chaque caractéristique étant la valeur d'une coordonnée particulière. Ensuite, nous effectuons la classification en trouvant l'hyper-plan qui différencie très bien les deux classes(Adrien Haccoun, n.d.).

2 - Arbre j48 :

J48 est une méthode à base d'arbre de décision, l'objectif de ce type de méthode est de construire une fonction de classement représentable par un arbre qui est construit en partant de la racine et en allant vers les feuilles. On cherche à discriminer les exemples selon leur classe

et en fonction d'attributs considérés comme les meilleurs parmi tous les autres au sens d'un critère donné(A, 2015).

Une méthode très efficace d'apprentissage supervisé. Partitionne un ensemble de données en des groupes les plus homogènes possible du point de vue de la variable à prédire. On prend en entrée un ensemble de données classées, On fournit en sortie un arbre où : chaque nœud final (feuille) représente une décision (une classe) chaque nœud non final (interne) représente un test. Les branches représentent les résultats des tests Chaque feuille représente la décision d'appartenance à une classe des données vérifiant tous les tests du chemin menant de la racine à cette feuille(*No Title*, n.d.-c).

3 - Random Forest :

Forêt aléatoire crée plusieurs arbres de décision et les fusionne pour obtenir une prédiction plus précise et plus stable. Comme je l'ai déjà mentionné, Random Forest est un ensemble d'arbres de décision, mais il existe quelques différences. Si vous entrez un jeu de données d'apprentissage avec des entités et des étiquettes dans un arbre de décision, il formulera un ensemble de règles, qui seront utilisées pour effectuer les prédictions. Par exemple, si vous souhaitez prédire si une personne cliquera sur une publicité en ligne, vous pouvez collecter la publicité de la personne sur laquelle vous avez cliqué dans le passé et certaines fonctionnalités décrivant sa décision. Si vous mettez les caractéristiques et les étiquettes dans un arbre de décision, des règles seront générées. Ensuite, vous pouvez prédire si la publicité sera cliquée ou non. En comparaison, l'algorithme Random Forest sélectionne de manière aléatoire des observations et des entités pour créer plusieurs arbres de décision, puis effectue la moyenne des résultats (A, 2015).

4 - Optimisation minimale séquentielle (SMO) :

Optimisation minimale séquentielle ou SMO. La formation d'une machine à vecteurs de support nécessite la résolution d'un très gros problème d'optimisation de la programmation quadratique (QP). SMO divise ce gros problème de QP en une série de problèmes de QP les plus petits possibles. Ces petits problèmes de QP sont résolus de manière analytique, ce qui évite d'utiliser une optimisation de QP numérique fastidieuse comme une boucle interne. La quantité de mémoire requise pour SMO est linéaire dans la taille du jeu d'apprentissage, ce qui permet à SMO de gérer des jeux d'entraînement très volumineux. Etant donné que le calcul matriciel est évité, SMO bascule quelque part entre linéaire et quadratique dans la taille du jeu

d'apprentissage pour divers problèmes de test, tandis que l'algorithme SVM de segmentation standard varie entre linéaire et cubique dans la taille du jeu d'apprentissage. Le temps de calcul de SMO étant dominé par l'évaluation SVM, SMO est donc le plus rapide pour les SVM linéaires et les fichiers fragmentés. Sur des ensembles de données clairsemés du monde réel, SMO peut être plus de 1000 fois plus rapide que l'algorithme de segmentation (A, 2015).

5 - Les réseaux bayésiens naïfs :

Les réseaux bayésiens sont des outils de représentation de connaissances en présence d'incertitude. Le succès de ces modèles est fortement lié à leur capacité de représenter et de manipuler des relations de (in)dépendance qui sont importantes pour une gestion efficace des informations incertaines. Les réseaux bayésiens utilisent une représentation basée sur le conditionnement, où les connaissances sont structurées sous la forme d'un graphe acyclique orienté. Les nœuds représentent des variables et les arcs qui codent le lien causal (ou l'influence) entre ces variables. L'incertitude est représentée au niveau de chaque nœud en explicitant toutes les probabilités conditionnelles attachées aux valeurs associées à ce nœud sachant celles de ses parents. Cette incertitude exprime la force de la relation de causalité entre les variables. Une simple variante des réseaux bayésiens est appelée réseaux bayésiens naïfs. Ces réseaux ont une structure unique qui se compose de deux niveaux seulement. Le premier contient un seul nœud parent qui n'est pas observé et le second plusieurs enfants de ce nœud correspondant aux nœuds observés (PARENT & EUSTACHE, 2006).

Réseaux bayésiens naïfs travaillent sous la forte hypothèse d'indépendance entre les nœuds enfants dans le contexte de leur parent. L'utilisation des réseaux bayésiens naïfs est assurée en considérant le nœud parent comme un nœud caché précisant à quelle classe appartient chaque objet de la base de données et les nœuds enfants représentent les différents attributs spécifiant cet objet. En présence d'un ensemble d'apprentissage on doit juste calculer les probabilités conditionnelles puisque la structure du graphe est unique. Ce calcul peut être résumé comme suit :

- Les probabilités conditionnelles pour les attributs discrets sont calculées à partir des fréquences en comptant combien de fois chaque valeur d'attribut apparaît avec chaque valeur possible du nœud parent.

$$P(c_i / A) = \frac{f(A/c_i)}{f(c_i)} \quad (1)$$

- Une fois le réseau quantifié, il peut être utilisé pour classer de nouveaux objets étant donné leurs valeurs d'attributs en utilisant la règle de Bayes exprimée par :

$$P\,(c_i/A) = \frac{P\,(A_1\,/c_i)\ *\ P\,(c_i)}{P(A)} \quad (2)$$

- Où ci est une valeur possible de la classe C et A est l'évidence totale sur les attributs. L'évidence A peut être vue comme un vecteur d'instances a1, a2, ans relatifs aux attributs a1, a2, …, an respectivement. Puisque les réseaux bayésiens naïfs travaillent sous l'hypothèse que ces attributs sont indépendants (Sachant le nœud parent C), leur probabilité jointe peut être calculée comme suit (PARENT & EUSTACHE, 2006):

$$P\,(c_i/A) = \frac{P\,(a_1\,/c_i)\ P\,(a_2/\,c_i)\ \ldots.P\,(a_n/c_i) * P\,(c_i)}{P(A)} \quad (3)$$

V - Weka :

Weka est un logiciel d'exploration de données qui utilise une collection d'algorithmes d'apprentissage automatique. Ces algorithmes peuvent être appliqués directement aux données ou appelés à partir du code Java (*Weka*, n.d.).

Weka est une collection d'outils pour :

- Regression
- Clustering
- Association
- Data pre-processing
- Classification
- Visualisation

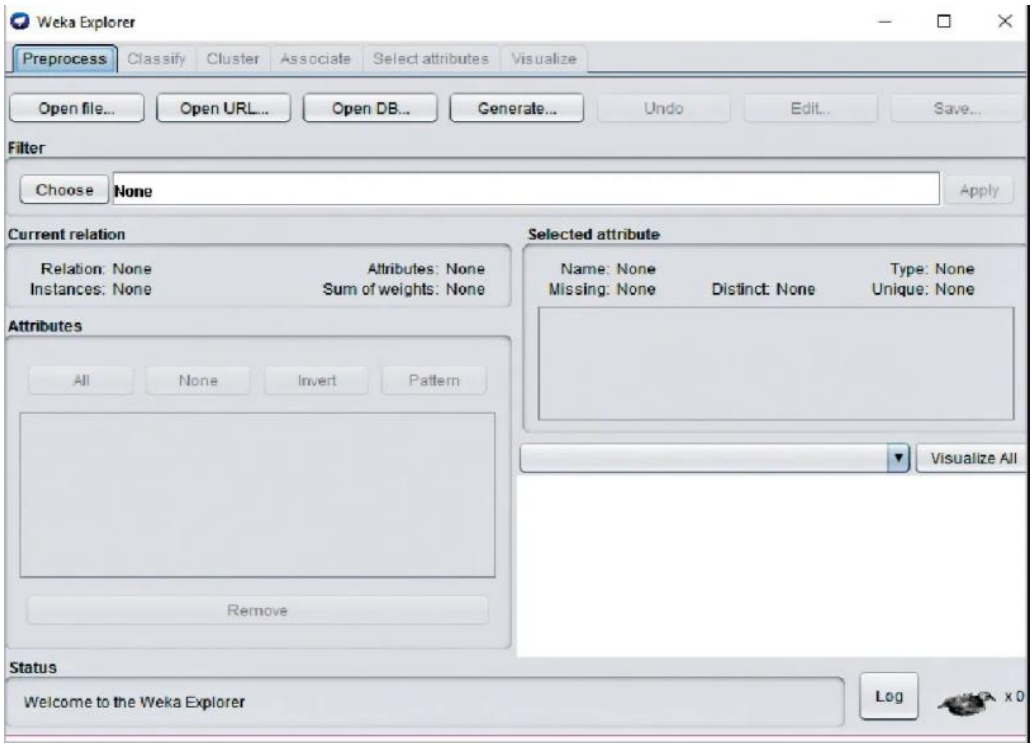


Figure 35 : Weka exploiter

VI - Proposition d'un système de détection d'intrusion avec une grande capacité de détection :

Le but de cette proposition et de créer un système de détection d'intrusion qui possède une grande capacité de détection des attaques, on va présenter trois scenarios différents voilà le premier scenario :

1 - Premier Scenario :

Ce scenario basé sur l'extraction des données par la simulation d'un seul nœud malveillant en utilisant l'outil de capture de trafic WireShark, Cela nous a permet d'obtenir ces attributs dans le tableau suivant :

Nom de l'attribut	Description
Time	Son temps de capture
Source	Sa source
Destination	Sa destination
Protocol	Le protocole de plus haut niveau décodé
Length	La taille de la Paquet
Info	Le résumé des champs caractéristiques de ce protocole
Class	Classer l'attaque par leur type

Tableau 4: Description des attributs

Par suite, Nous avons appliqués plusieurs classificatrices sur notre dataset pour choisir le meilleur classificateur selon le résultat obtenu à propos de taux de détection pour chaque classificateur ci-dessus un tableau de comparaison de déférentes algorithme de classification total :

Classifieur	_normal, %	Helloflooding, %	Blackhole, %
Naivebayesien	18,2	93,4	71,6
J48	95,3	97,0	98,7
RandomForest	94,4	97,1	94,4
LibSVM	88,3	94,9	88,2
SMO	46,1	80,2	65,2

Tableau 5 : Les performances (le taux d'exactitude) des classificateurs avec une seule attaque

Par suite on va faire une élimination de quelques classificateurs parmi ces derniers en comparant les différents classificateurs, les résultats sont obtenus sur un PC Windows avec i-5 2,40 GHz et 8 Go de RAM. La performance d'un IDS est mesurée par sa capacité de classer

chaque connexion de la bonne catégorie. Les indicateurs de performance les plus utilisés pour évaluer le système de détection d'intrusion sont taux de détection et l'exactitude et les Faux d'alarme :

Mesures → / Classificateurs ↓	DR, %	Exactitude, %	FAR, %	Décision
Naivebayesien	60,4	66,5	19,4	
J48	97,0	97,0	1,5	
RandomForest	95,3	95,3	2,3	
LibSVM	90,5	90,5	4,2	
SMO	63,6	62,8	18,2	

Tableau 6 : Les performances des classificateurs avec une seule attaque détails

Comme le montre le tableau précédent, nous avons choisi le J48 car il a le moins de taux Faux d'alarme et le plus de taux de détection.

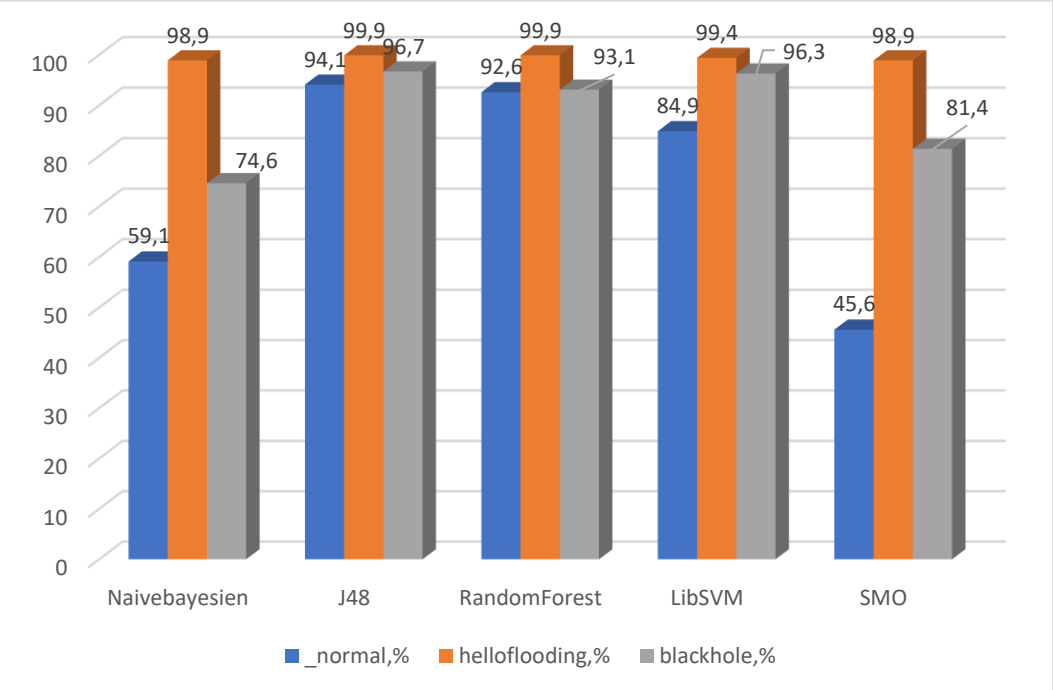


Figure 36 : Etude comparative entre les cinq classificateurs pour le premier model.

2 - Deuxième Scenario :

Aussi, nous avons essayé d'améliorer notre model par la simulation de plusieurs nœuds malveillants de chaque type d'attaques, le but de cette étape est de donner plus d'information afin de mieux détecter le trafic anormal.

Classifieur	**_normal, %**	**Helloflooding, %**	**Blackhole, %**
Naivebayesien	59,1	98,9	74,6
J48	94,1	99,9	96,7
RandomForest	92,6	99,9	93,1
LibSVM	84,9	99,4	96,3
SMO	45,6	98,9	81,4

Tableau 7: Les performances (le taux d'exactitude) des classificateurs avec quatre attaques

Mesures → **Classificateurs ↓**	**DR, %**	**Exactitude, %**	**FAR, %**	**Décision**
Naivebayesien	78,7	78,5	10,2	
J48	97,1	97,1	1,4	
RandomForest	95,4	95,4	2,2	
LibSVM	94,0	94,0	3,0	
SMO	77,0	77,3	11,4	

Tableau 8 : Les performances des classificateurs avec quatre attaques détails

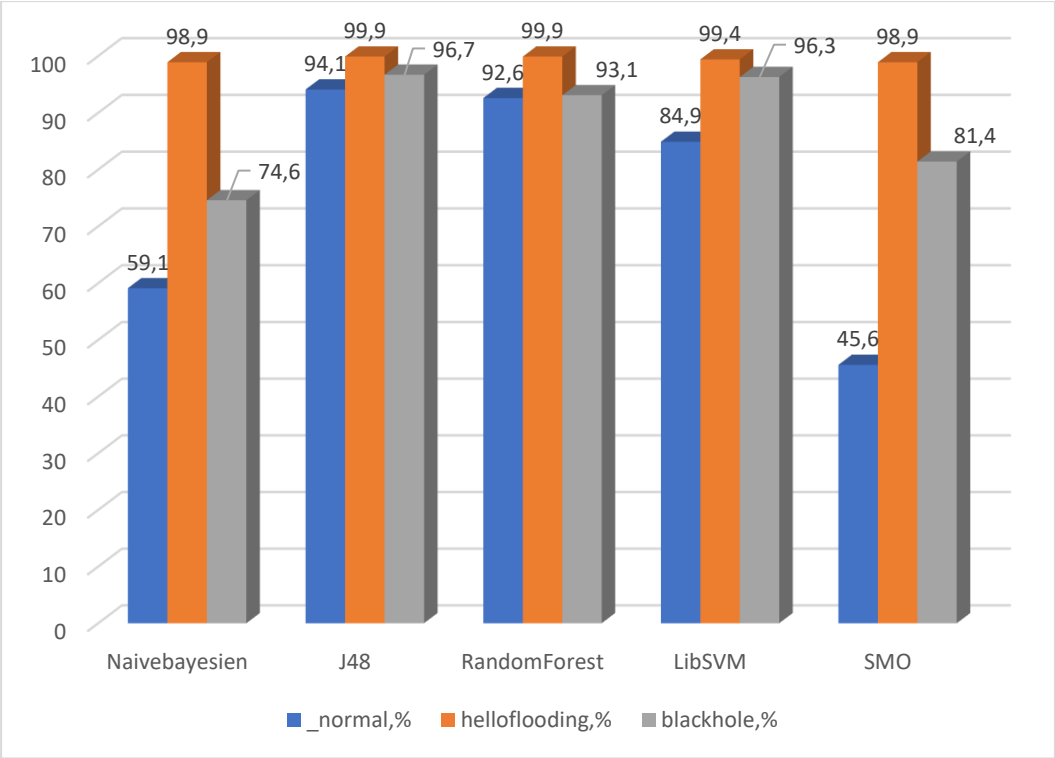


Figure 37 : Etude comparative entre les cinq classificateurs pour le deuxième model.

Comme indiqué dans le tableau suivant, il y a une différence notable entre les deux scenarios en termes de taux de précision :

Mesures →	**Exactitude %**		**FAR %**	
Classificateurs ↓	Scenario 1	Scenario 2	Scenario 1	Scenario 2
Naivebayesien	66,5	78,5	19,4	10,2
J48	97,0	97,1	1,5	1,4
RandomForest	95,3	95,4	2,3	2,2
LibSVM	90,5	94,0	4,2	3,0
SMO	62,8	77,3	18,2	11,4

Tableau 9 : table comparative entre les deux scenarios

3 - Troisième Scenario

3-1 - Prétraitement (Dataset) :

Nous allons d'abord expliquer les outils utilisés dans la simulation des différents scénarios de la communication en réseau IOT, l'environnement de la simulation est le célèbre Cooja, l'outil de simulation multicouche (application, système d'exploitation et couche de code machine) intégré dans la d'exploitation Contiki qui est en effet un flexible pour capteurs miniatures en réseau.

Les capteurs du réseau simulé fonctionnent avec le système d'exploitation Contiki et implémentent le protocole RPL, le Contiki permet de charger et de décharger des programmes et des services individuels sur les capteurs simulés.

C'est pour cette raison qu'avons effectué une simulation de chaque attaque comme mentionné ci-dessus, en exécutant le code réel des capteurs dans le simulateur Cooja, en utilisant une machine virtuelle avec 08 Go de RAM et 2 V-CPU monter sur un PC de Processor : Intel(R) Core (TM) i3-3437U CPU, Fréquence de base est 1.80GHz (4 CPUs), et La fréquence Turbo maxi est 2.4GHz.

Le Contiki comprend l'environnement d'exécution Java 64 bits en plus du système d'exploitation Ubuntu 64 bits.

Nous avons construit de différentes topologies de réseau pour simuler les attaques de routage de l'IOT, ensuite nous avons simulé ces scénarios par le biais du simulateur de réseaux Cooja, en évitant de produire l'ensemble de données synthétiques, vu que Cooja permet d'exécuter du code RPL réel sur les nœuds simulés, et permettre de prendre les messages radio transmis dans le réseau simulé sous forme d'un fichier PCAP que nous devons le convertir ensuite en format CSV (Comma Separated Values) afin de le traiter en mode texte par le biais de notre bibliothèque de prétraitement de données Python, et Après, un processus d'extraction de fonctionnalités sera appliqué sur les fichiers CSV générés.

Après avoir simulé les scénarios, des ensembles de données ont été produits sous forme de fichiers PCAP. Nous avons disséqué le fichier PCAP en CSV en utilisant Wireshark et en l'introduisant dans le prétraitement. Un échantillon de l'ensemble de données brutes est présenté dans le tableau 2.

No.	Time	Source	Destination	Protocol	Length	Info
228	4,932379	fe80::c30c:0:0:b	fe80::c30c:0:0:0	ICMPv6	76	RPL Control (Destination Advertisement Object)
204	2,334325	fe80::c30c:0:0:0	ff02::1a	ICMPv6	97	RPL Control (DODAG Information Object)
194	1,001214	fe80::c30c:0:0:1	ff02::1a	ICMPv6	64	RPL Control (DODAG Information Solicitation)
21626	87,740032	fe80::c30c:0:0:4	fe80::c30c:0:0:a	ICMPv6	102	RPL Control (DODAG Information Object)

Tableau 10 : Un échantillon de l'ensemble de données brutes capturés

a) Les attaques et Les fonctionnalités de données (d'attributs) pour la phase de l'apprentissage automatique :

RPL (Routing Protocol for Low-Power and Lossy Net-works) est un protocole de routage IPv6 arborescent pour 6LoWPAN. Il crée des graphiques acycliques dirigés orientés vers la destination (DODAG), appelés arbre DODAG(Vasseur et al., 2011).

Chaque réseau a un ou plusieurs nœuds racine DODAG comme nœud central, et chaque réseau a un identifiant unique DODAG ID à identifier. En outre, chaque nœud a un numéro de rang et une table de routage en raison des numéros de rang des autres nœuds. Le numéro de rang est utilisé pour déterminer la distance entre le nœud et la racine.

Dans le protocole RPL, il existe trois types de paquets de contrôle : DODAG Information Object (DIO), Destination Advertisement Object (DAO) et DODAG Information Solicitation (DIS). Les paquets DIO sont d'abord envoyés par le nœud de base (ou racine) sous forme de paquets de diffusion pour établir l'arbre DODAG. Les autres nœuds reçoivent les paquets DIO et créent leur table de routage en sélectionnant leur nœud parent. Ils envoient les paquets DAO au nœud parent, en demandant la permission de se connecter au nœud parent. Le nœud parent

accepte cette offre en renvoyant un paquet DIO ACK. Un nouveau nœud envoie des paquets DIS pour rejoindre l'arbre DODAG. Si un nouveau nœud rejoint l'arbre, tous les nœuds envoient à nouveau un paquet DIO pour réformer DODAG (ou topologie du réseau).

Les attaques de routage ont lieu au niveau de la couche réseau. Parmi les attaques de routage les plus importantes, on trouve les attaques de type "hello-flood" (HF) ,"Blackhole " (BH)(Framework, 2016)

- Hello flood Attack :

Le protocole de routage nécessite que les nœuds voisins d'un même réseau échangent des messages HELLO pour indiquer leur présence et leur disponibilité, découvrir des routes et mettre à jour les tables de routage. Le nœud malveillant envoie un nombre énorme de paquets HELLO aux différents nœuds pour se présenter comme nœud voisin, afin qu'ils lui transmettent leurs données(Framework, 2016).

L'objectif principal du message HELLO est d'introduire et d'intégrer de nouveaux nœuds dans le réseau. Les nœuds diffusent des messages HELLO avec leurs propres paramètres tels que la puissance du signal et le numéro d'identification. Tous les autres nœuds créent leur propre table de routage pour envoyer leurs messages. Le nœud malveillant envoie des messages HELLO par paquets DIS à ses victimes par une forte puissance de signal et des mesures de routage appropriées, apparaissant comme un nœud voisin, par suite ce nœud attaquant devient le nœud le plus favorable pour ces victimes ce qui est appelée l'attaque "Hello-flood".

Suite à cette attaque, le nombre de paquets transmis par le nœud malveillant augmente. C'est pour cette raison, nous devons calculer le nombre de paquets transmis, le temps moyen de transmission le nombre de paquets transmis, le temps total de transmission et les fonctionnalités DIS pour identifier cette attaque(Framework, 2016).

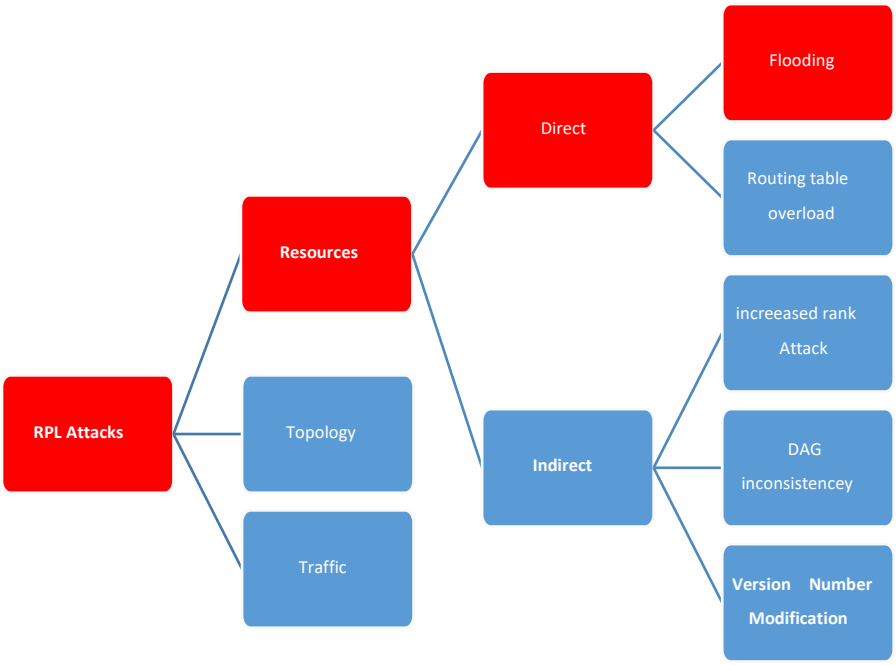


Figure 38: Attaque Direct en RPL sur les ressources(Framework, 2016)

- Blackhole Attack :

Une attaque Blackhole dans un réseau signifierait qu'un ou plusieurs nœuds Malveillants laisseraient tomber totalement ou partiellement les paquets de données qui y sont acheminés, ce qui entraînerait des perturbations dans le flux normal des données sur le réseau.

Un nœud malveillant faussera les informations de routage, se présentera comme le meilleur chemin vers le nœud de contrôle (appelé Node sink), pour forcer le passage des données par lui-même(Framework, 2016).

Sa seule mission est alors de ne rien transférer, créant une sorte de puits ou de blackhole dans le réseau. L'intrus se place à un emplacement stratégique de routage dans le réseau et supprime tous les messages qu'il doit retransmettre, entraînant la suspension du service de routage du réseau dans les routes qui passent par le nœud du pirate. Si un nœud malveillant a la capacité d'usurper l'identité d'un nœud valide du réseau, il peut le faire lorsque le mécanisme de découverte d'itinéraire répond au nœud initiateur par un message de rediffusion routière en annonçant un chemin avec un coût minimal au nœud demandé. Le nœud émetteur mettra alors à jour sa table de routage avec cette fausse route(Framework, 2016).

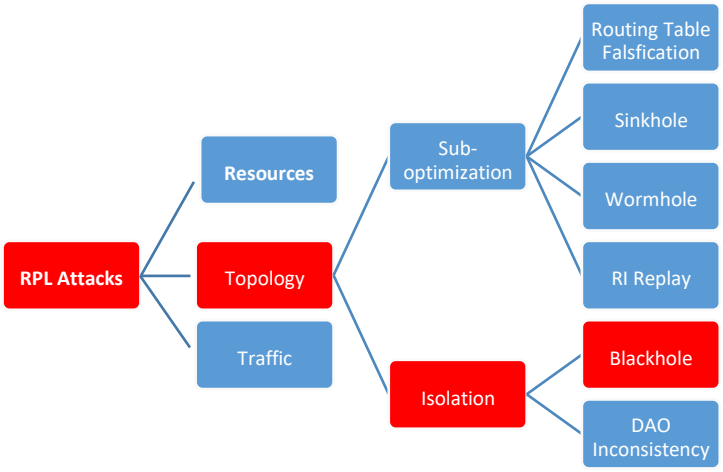


Figure 39 : Attaques d'isolation en RPL sur la topologie(Framework, 2016)

En utilisant la Position géographique et le rang (Position sur topologie logique) afin de déterminer la distance entre le nœud et la racine comme un outil de détection des trafics anormal dans notre réseau, elle nous permet de mieux comprendre le comportement des nœuds malveillants (BH)

Nous capterons la Position géographique et rang afin d'utiliser aussi comme un mécanisme de sécurité basé sur la force du signal et les informations géographiques pour détecter les nœuds malveillants qui lancent l'attaque. L'idée est de comparer la force du signal d'une réception avec sa valeur attendue (calculée à l'aide des informations géographiques), et de la spécification d'émetteur-récepteur prédéfinie(Framework, 2016).

b) Prétraitement des données et extraction de fonctionnalités :

Pour les attaques BH, HF, nous avons généré de différents scénarios d'attaque. Les simulations nous ont permis de produire des ensembles de données brutes.

Après, avoir obtenus des fichiers de données brutes de la simulation. Cependant, les fichiers de données ne seront pas suffisants pour être inclus dans l'algorithme d'apprentissage automatique, car l'ensemble de ces données brutes comprend des informations telles que l'adresse des nœuds source/destination et la longueur des paquets, ce qui provoque du bruit et de l'Overfitting (le sur-apprentissage) dans l'algorithme d'apprentissage automatique. Pour cette raison, nous avons implémentés un prétraitement des données et un algorithme

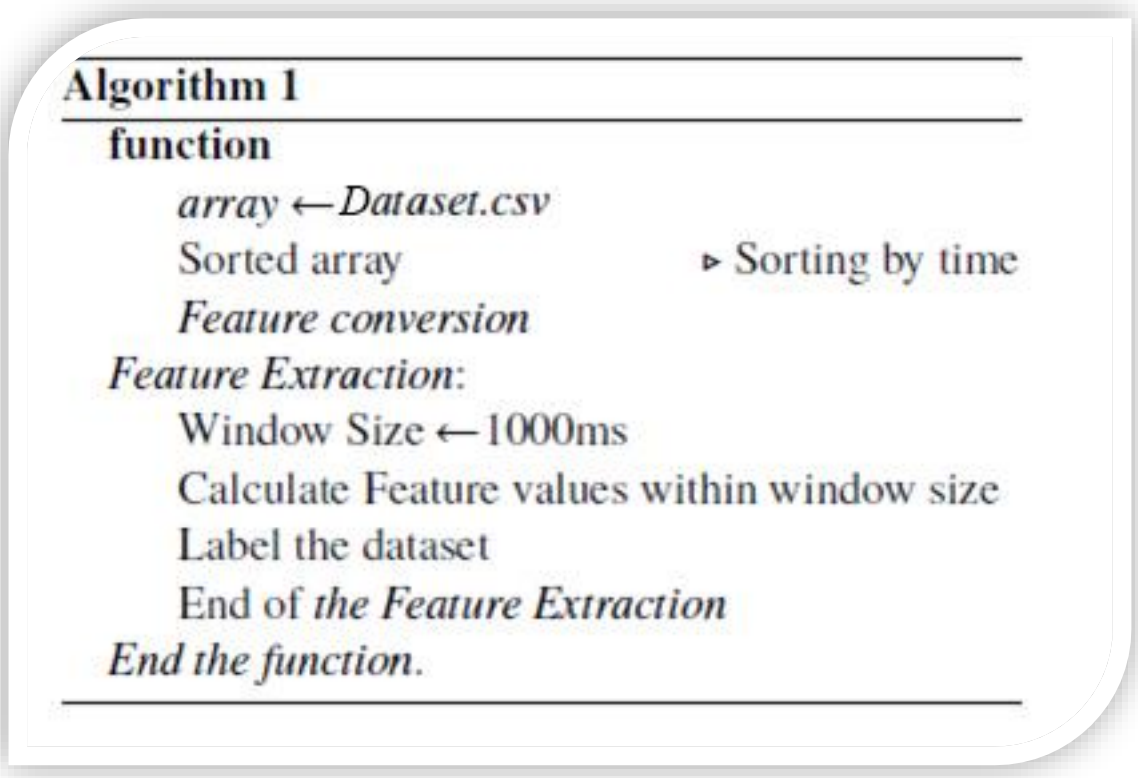
d'extraction de fonctionnalités en utilisant le lagunage Python et ces bibliothèques Pandas33, ces dernières effectuent les opérations de prétraitement qui sont nécessaires pour faciliter l'extraction de fonctionnalités.

Nous avons mis en place une structure de dictionnaire pour traiter un grand nombre de nœuds, tout en choisissant de ne pas calculer de statistiques globales sur le temps total simulé ou le nombre total de paquets, parce que ce type de calcul pourrait nuire au calcul des poids des fonctionnalités extraites.

Nous avons divisé toute la simulation en périodes de temps, ou fenêtres d'une durée de 1000 ms.

Avant ce processus, il est nécessaire de trier les ensembles de données par temps de simulation, car une séquence correcte du temps de simulation des paquets est nécessaire pour calculer correctement la valeur des fonctionnalités.

Le pseudocode de l'algorithme de prétraitement des données et d'extraction des fonctionnalités est fourni dans l'algorithme 1.



Algorithm 1

function

array ← *Dataset.csv*

Sorted array ▷ Sorting by time

Feature conversion

Feature Extraction:

Window Size ← 1000ms

Calculate Feature values within window size

Label the dataset

End of *the Feature Extraction*

End the function.

Figure 40 : l'algorithme de prétraitement des données

Les ensembles de données brutes comprennent des types de données qui ne peuvent pas être traités par l'algorithme d'apprentissage automatique, comme les adresses IP. Les adresses de source et de destination sont converties du format IPv6 en ID de nœud. Par exemple :

Les paquets de diffusion sont traités comme suit. Dans un ensemble de données brutes, si l'adresse de destination est ff02::1a, cela signifie que le nœud source envoie des paquets de diffusion. Cette valeur est convertie en 99 pour éviter toute coïncidence avec un autre nœud

Nous avons également encodé les informations des paquets, comme indiqué dans le tableau 11.

Info	Value
DODAG Information Sollicitation	1
DODAG Information Object	2
Destination Advertisement Object	3

Tableau 11: Normalisation des Messages de contrôle DODAG

Le DAO est utilisé dans le protocole RPL pour envoyer des informations de destination unicast sur les parents sélectionnés. DIO est le type de message le plus important dans le protocole RPL. Il conserve le rang actuel du nœud, détermine la meilleure route à travers le nœud de base en utilisant des métriques spécifiques comme la distance ou le nombre de sauts. Un autre type de message est DIS. Les nœuds utilisent DIS pour recevoir les messages DIO. Ces messages sont codés respectivement en 1, 2, 3.

L'extraction de fonctionnalités a permis de produire un total de 23 attributs. Ces valeurs sont calculées comme suit. Tout d'abord, nous calculons le nombre de paquets transmis et reçus pour chaque nœud en 1000 ms dans un délai donné. Ensuite, nous divisons ces valeurs à 1000 ms et obtenons le taux de transmission et le taux de réception pour chaque nœud, respectivement, pour toutes les périodes.

On calcule le temps de transmission et de réception de chaque paquet. Le temps total de la durée de chaque paquet de transmission et de réception en 1000 ms. Ensuite, on calcule le temps moyen de transmission et de réception pour chaque nœud, Le nombre de paquets de contrôle transmis de chaque nœud (concernent les paquets de contrôle : DAO, DIO et DIS) est calculé dans la taille de fenêtrage, 1000 Ms.

c) Paramètre d'évaluation :

Nous nous sommes focalisés sur le paramètre de la consommation d'énergie dans le but d'évaluer la précision de l'IDS que nous avons proposé. Nous présentons en graphique les informations recueillies lors du suivi de la puissance de chaque mote, en termes d'énergie (radio ON), énergie d'émission (radio TX : mode émission), énergie de réception (radio RX : mode réception) et enfin l'énergie INT (radio interférée) :

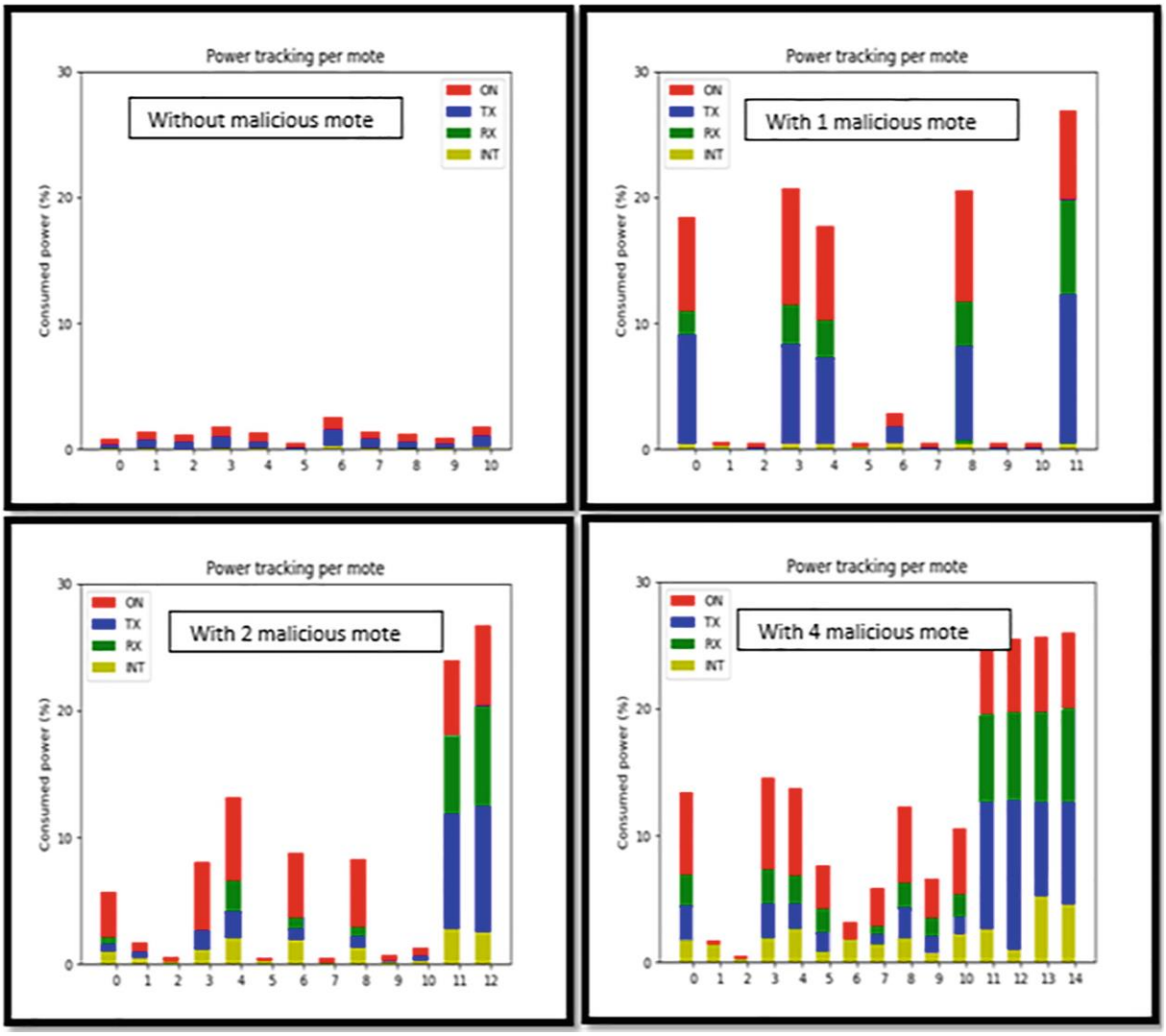


Figure 41 : Suivi de puissance pour chaque mote

Les figures suivantes illustrent les informations obtenues lors de la simulation de l'attaque avec et sans le nœud malveillant, respectivement à droite et à gauche. Une comparaison de la consommation d'énergie été nécessaire pour déduire l'impact de l'attaque en présence et en absence du nœud malveillant.

Nous pouvons remarquer l'impact de l'attaque sur le réseau au fil du temps et en particulier sur les nœuds 3,7 et 10 :

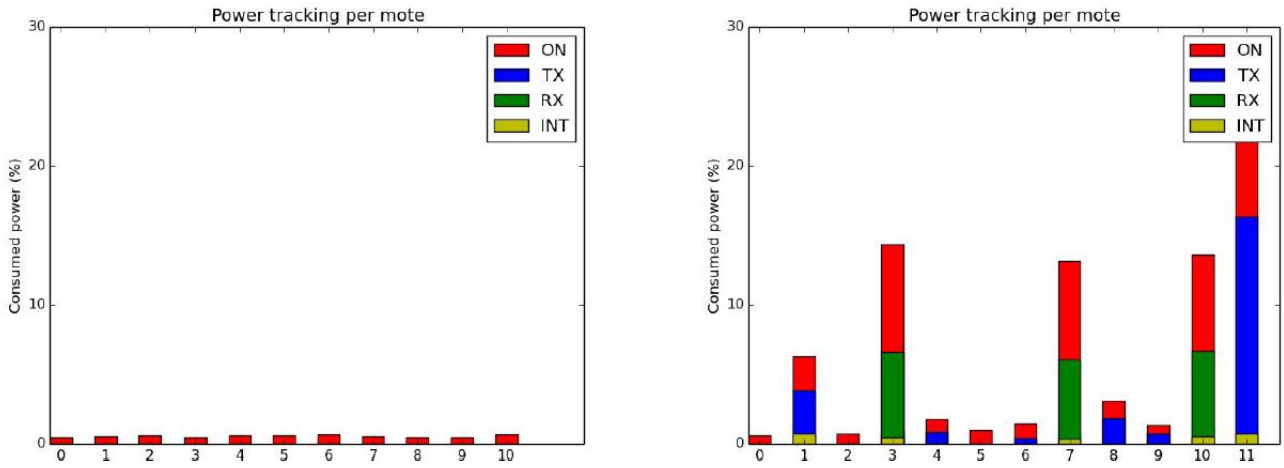


Figure 42 : Suivi de puissance sans mote malveillant et avec mote malveillant

Enfin, toutes les données résultant du fichier csv (déjà traité) sont concaténées avec les Paramètres d'évaluation de l'énergie.

La valeur de l'énergie varie selon le temps. Elle a été enregistrée par intermittence. Les données ont été collectées à l'aide d'un capteur pour finalement produire un ensemble de données contient toutes les informations nécessaires pour l'apprentissage automatique afin de rendre notre model final efficace contre ces types d'attaque de routage IOT

d) Normalisation des fonctionnalités :

Les données résultant de différents scénarios d'attaque par routage IoT ont une moyenne et une variance différentes en raison de leur topologie de réseau, ce qui réduit la performance de l'algorithme d'apprentissage automatique. Par conséquent, un processus de normalisation des fonctionnalités est effectué. Nous avons appliqué une transformée de quantification et une mise à l'échelle min-max aux ensembles de données, respectivement. La transformation quantile ajuste la distribution des valeurs des fonctionnalités à la distribution normale. Elle vise à réduire l'effet négatif des valeurs marginales. Ensuite, nous mettons à l'échelle toutes les valeurs des ensembles de données dans la plage [0-1] par une mise à l'échelle min-max.

Les ensembles de données sont normalisés par un processus de normalisation des fonctionnalités afin de rendre le processus de formation plus rapide.

Enfin, toutes les données résultant des différentes topologies de réseau sont concaténées pour produire un ensemble de données pour un type d'attaque de routage IOT. Nous obtenons en suite trois ensembles de données d'attaque, La collecte de ces ensembles de données

construisent notre Dataset final par suite nous appliquons des algorithmes d'apprentissages automatiques afin d'obtenir Notre IDS.

Enfin, toutes les données résultant des différentes topologies de réseau sont concaténées pour produire un ensemble de données pour un type d'attaque de routage IOT. Nous obtenons en suite trois ensembles de données d'attaque, La collecte de ces ensembles de données (qui sont intégrées dans un algorithme d'apprentissage automatique), est le résultat final (data set).

Tous ce qui été décrit précédemment pour dégager l'ambigüité de notre contribution est illustré dans le diagramme cité ci-dessous (figure 45).

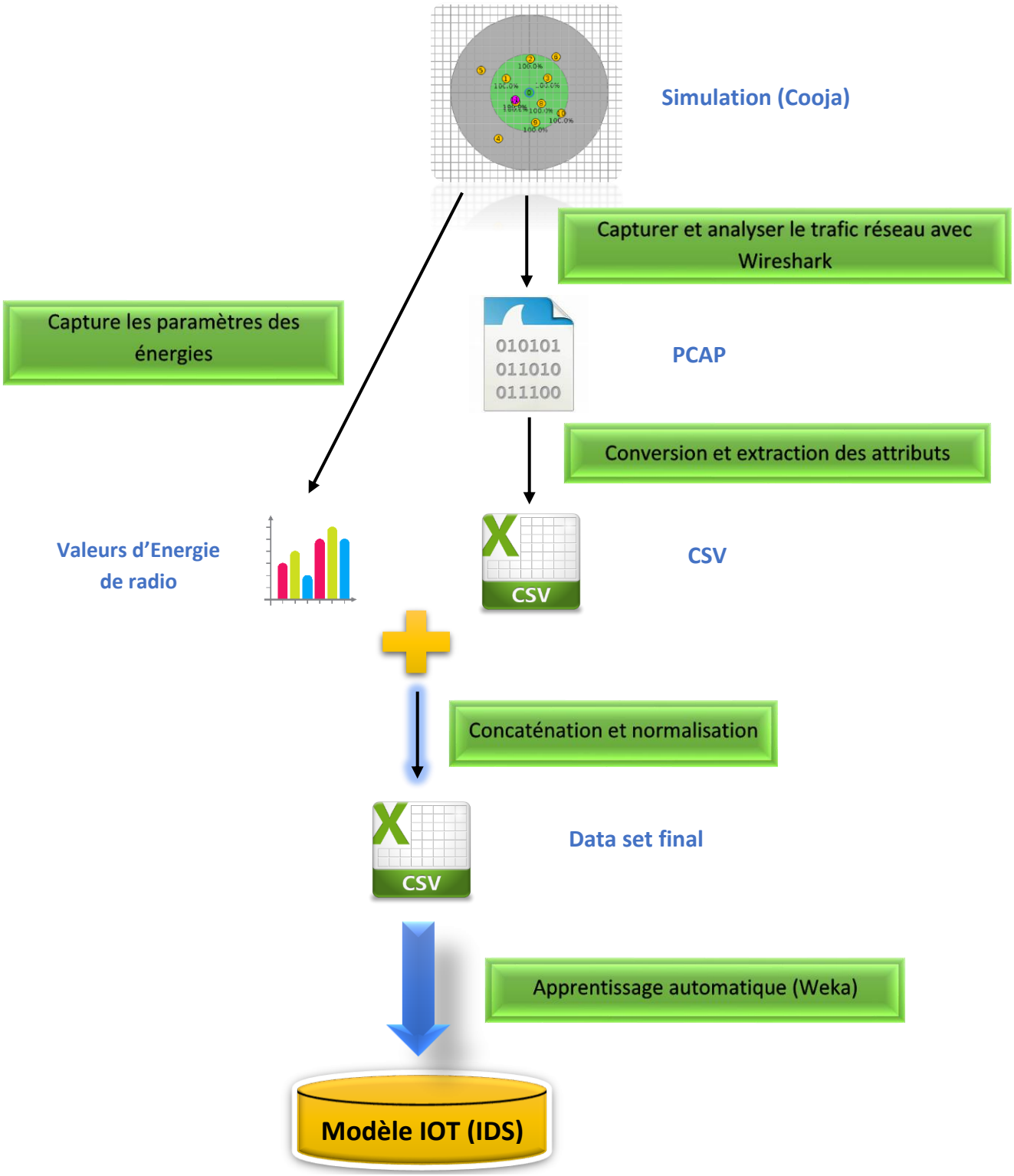


Figure 43 : les différentes étapes (phases) du processus de notre modèle

e) Sélections d'attributs :

Nous avons choisi les fonctionnalités de données pour construire notre model d'apprentissage automatique, le choix peut être une cause très essentielle sur les résultats obtenus. Les caractéristiques irréductibles ou partiellement pertinentes peuvent avoir un impact négatif sur les performances du modèle.

Nom de l'attribut	Description
Src	Source
Dst	Destination
T	Time
Protocol	Le protocole de plus haut niveau décodé
Dure_tr	Dure de transmission pendant une fenêtre de time
Moy_tr	Moyen de transmission
Length_tr	La taille du Paquet transmits
DIS_tr	Dodag information solicitation transmits
DIO_tr	Dodag information object transmits
DAO_tr	Dodag advertisement object transmits
Dure_rec	Durée de reception pendant une fenêtre de time
Moy_rec	Moyen de reception
Length_rec	La taille du Paquet reçu
DIS_rec	Dodag information solicitation reçu
DIO_rec	Dodag information object reçu
DAO_rec	Dodag advertisement object reçu
Rang	Statue de connecter directement ou non
ON	Energie d'activité radio
TX	Radio d'énergie d'émission
RX	Radio d'énergie de reception
INT	Radio interférée
Pos_x	Position géographique sur l'axe X
Pos_y	Position géographique sur l'axe y
Class	Classer l'attaque par leur type

Tableau 12: Description de différents attributs

Classifieur	_normal, %	Helloflooding, %	Blackhole, %
Naivebayesien	95,9	100	97,0
J48	100	100	100
RandomForest	100	100	100
LibSVM	98,5	100	100
SMO	99,3	100	100

Tableau 13 : Les performances (le taux d'exactitude) des classificateurs avec 21 attributs

Dans la figure suivante, notre model final a montré sa haute performance pour le taux d'exactitude le plus élevé, un taux de faux d'alarme minimal, et un fort taux de détection

Mesures → / Classificateurs ↓	DR, %	Exactitude, %	FAR, %	Décision
Naivebayesien	98,0	98,1	0,6	
J48	100	100	0	
RandomForest	100	100	0	
LibSVM	99,4	99,4	0,1	
SMO	99,7	99,7	0,1	

Tableau 14 : Les performances des classificateurs avec 21 attributs détails

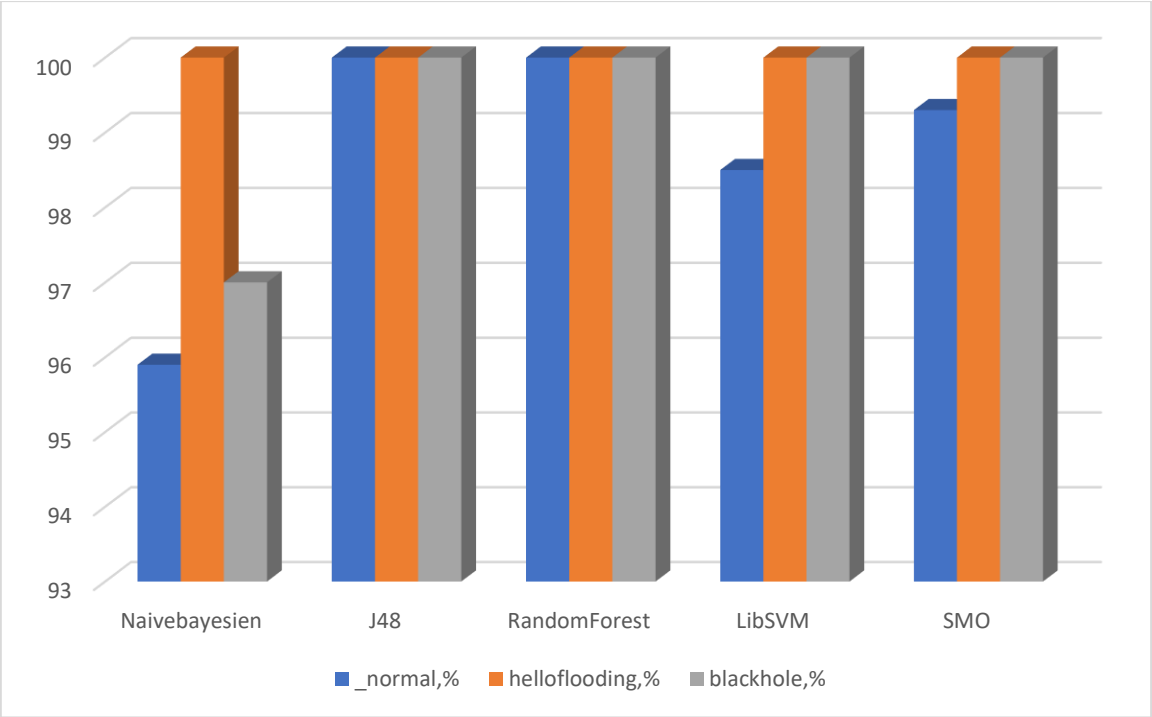


Figure 44 : Etude comparative entre les cinq classificateurs pour le troisième model.

Conclusion :

Dans ce chapitre, nous avons proposé une solution de détection d'attaque DDOS dans un réseau IoT qui vise le RPL comme protocole de routage. Nous avons simulé à l'aide de Contiki-Cooja pas mal de scénarios réseau, pour pouvoir générer et former les jeux de données à utiliser dans la phase de test et d'apprentissage, dans laquelle nous allons utiliser WEKA, pour décider selon la base de données si le comportement est normal ou malveillant.

Conclusion Générale

Conclusion Général :

L'internet des objets est un nouveau domaine qui englobe un large ensemble de technologies. Notre objectif était de présenter les attaques de sécurité existantes dans l'internet des objets, en nous concentrant sur les techniques de détection d'intrusion.

Au cours de notre travail, nous avons suivi plusieurs étapes afin d'atteindre notre objectif, qui est de sécuriser un réseau IoT contre les attaques DOS (par Blackhole et hello flood) qui perturbent son fonctionnement. Nous avons commencé par la sécurité en général ensuite on a mis l'accent sur le mécanisme de sécurité IDS.

Après nous avons d'abord simulé à l'aide du simulateur Contiki Cooja deux scénarios de réseau, l'un sans attaques, dit normal, et 'autre avec un nœud de capteur malveillant. Ensuite, nous construirons notre ensemble d'entrainement, qui est nécessaire pour la phase d'apprentissage, en utilisant des paramètres importants pour détecter les attaques par Blackhole et hello flood tels que la fraction de livraison de paquets, la fréquence des messages DIO, DIS et DAO échangés , l'énergie et la position des nœuds , L'énergie est la ressource la plus précieuse dans un réseau de capteurs, parce qu'elle influe directement sur la durée de vie des capteurs et du réseau en entier.

Enfin nous avons proposé trois modèles différents avec trois scénarios différents Un scénario avec l'extraction de données par une seule attaque simulée. Deuxième scénario avec l'extraction de données par quartes attaques simulée et le troisième scénario on va essayer d'ajouter plusieurs attributs dans le dataset final pour augmente le pourcentage de la détection des attaque DDOS dans un environnement IoT.

Bien que les objectifs de ce travail soient réussis, les résultats qu'elle nous a permis d'obtenir montrent que le problème de ce nouveau paradigme est toujours présent à diverses menaces qui ne peuvent pas être ignorées et nécessite de puissantes contre-mesures de sécurité.

Enfin, nous devons souligner que ce travail n'est qu'une simple tentative de répondre à l'un des problèmes rencontrés dans les attaques DDOS dans environnement

Bibliography

[1] A, D. (2015). *Classification*.

[2] Adrien Haccoun. (n.d.). *Comparaison de méthodes de classifications*. https://www.lri.fr/~antoine/Courses/Master-ISI/ISI-10/Projets_2012/Projet_DM.pdf

[3] Aggarwal, C. C., Ashish, N., & Sheth, A. (2013). The internet of things: A survey from the data-centric perspective. In *Managing and mining sensor data* (pp. 383–428). Springer.

[4] Ahmed, A. (2014). *Système de détection d'intrusion adaptatif et distribué*.

[5] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*, *17*(4), 2347–2376.

[6] AMAND, M., & NSIRI, M. (2011). Etude d'un système de détection d'intrusion comportemental pour l'analyse du trafic aéroportuaire. *Rapport de Projet LENAC*.

[7] *Apprentissage Supervisé*. (n.d.). Retrieved October 16, 2020, from https://machinelearnia.com/apprentissage-supervise-4-etapes/?fbclid=IwAR2TI466K-dZSzo8ljjvX5pob1TsojLg_UMFp1X1g6aM3BW7TPCkug2SMeE

[8] Arvidson, M., & Carlbark, M. (2003). *Intrusion Detection Systems: Technologies, Weaknesses and Trends*. Institutionen för systemteknik.

[9] Association, I. S. (2011). *IEEE Std 802.15. 4-2011, IEEE standard for local and metropolitan area networks—part 15.4: Low-rate wireless personal area networks (LR-WPANs)*. Sep.

[10] Baudoin, N., & Karle, M. (2004). NT Réseaux: IPS et IDS. *Université de Marne La Vallée, France*.

[11] Belkhatmi Keltouma, O. B. (2016). *Mise en place d'un systéme de détection et de prévention d'intusion. Diss*. Université de Bejaia.

[12] Benghozi, P.-J., Bureau, S., & Massit-Folea, F. (2008). *L'Internet des objets. Quels enjeux pour les Européens?*

[13] Benghozi, P.-J., Bureau, S., & Massit-Folléa, F. (2009). *L'Internet des objets/The Internet of Things*. Paris, Editions de la Maison des Sciences de l'Homme, coll. praTICs.

[14] Berthomier, E. (2005). Formation Sécurité des Réseaux. *Mars*.

[15] Blanc, L. (n.d.). *La sécurité de l'Internet des Objet*.

[16] Bloch, L., Wolfhugel, C., Queinnec, C., Schauer, H., & Makarévitch, N. (2013). *Sécurité informatique: Principes et méthodes à l'usage des DSI, RSSI et administrateurs*. Editions Eyrolles.

[17] Burgermeister, D., & Krier, J. (2006). *Les systèmes de détection d'intrusions*. Article disponible sur http://dbprog. developpez. com.

[18] Chaouki, J., Michaël, S., & Anis, H. (2009). TER Détection d'anomalies sur le réseau. *Rapport de Projet, Université Paris Descartes*.

[19] *Cooja Simulator*. (n.d.). Retrieved July 10, 2020, from https://anrg.usc.edu/contiki/index.php/Cooja_Simulator

[20] Cousin, B. (n.d.). *Sécurité des réseaux informatiques*.

[21] Dagorn, N. (2006). *Détection et prévention d'intrusion: présentation et limites*.

[22] Debar, H., Morin, B., Cuppens, F., Autrel, F., & Mé, L. (2004). Détection d'intrusions: corrélation d'alertes. *TSI. Technique et Science Informatiques*, *23*(3), 359–390.

[23] Desgeorge, G. (2000). *La sécurité des réseaux*. Cour.

[24] Framework, R. P. L. A. (2016). *Mobile and Embedded Computing*.

[25] Gaurav, K., Goyal, P., Agrawal, V., & Rao, S. L. (2015). IoT transaction security. *Proceedings of the 5th International Conference on the Internet of Things (IoT), Seoul, Korea*, 26–28.

[26] Gomez, C., & Paradells, J. (2010). Wireless home automation networks: A survey of architectures and technologies. *IEEE Communications Magazine*, *48*(6), 92–101.
[27] Greenstadt, R., & Beal, J. (2008). Cognitive security for personal devices. *Proceedings of the 1st ACM Workshop on Workshop on AISec*, 27–30.
[28] He, D., & Zeadally, S. (2014). An analysis of RFID authentication schemes for internet of things in healthcare environment using elliptic curve cryptography. *IEEE Internet of Things Journal*, *2*(1), 72–83.
[29] Hodo, E., Bellekens, X., Hamilton, A., Tachtatzis, C., & Atkinson, R. (2017). Shallow and deep networks intrusion detection system: A taxonomy and survey. *ArXiv Preprint ArXiv:1701.02145*.
[30] *Into the Battlefield: A Security Guide to IoT Botnets*. (n.d.). Retrieved June 20, 2020, from https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/into-the-battlefield-a-security-guide-to-iot-botnets
[31] Jones, E. C., & Chung, C. A. (2016). *RFID and Auto-ID in Planning and Logistics: A Practical Guide for Military UID Applications*. CRC Press.
[32] Ko, J., Terzis, A., Dawson-Haggerty, S., Culler, D. E., Hui, J. W., & Levis, P. (2011). Connecting low-power and lossy networks to the internet. *IEEE Communications Magazine*, *49*(4), 96–101.
[33] Lerman, L., Markowitch, O., & Bontempi, G. (2011). *Les systèmes de détection d'intrusion basés sur du machine learning*.
[34] Limbasiya, T., & Doshi, N. (2017). An analytical study of biometric based remote user authentication schemes using smart cards. *Computers & Electrical Engineering*, *59*, 305–321.
[35] Llorens, C., Levier, L., Valois, D., & Morin, B. (2011). *Tableaux de bord de la sécurité réseau*. Editions Eyrolles.
[36] Michel, C. (2003). *Langage de description d'attaques pour la détection d'intrusions par corrélation d'événements ou d'alertes en environnement réseau hétérogène*.
[37] Minoli, D. (2013). *Building the internet of things with IPv6 and MIPv6: The evolving world of M2M communications*. John Wiley & Sons.
[38] Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, *10*(7), 1497–1516.
[39] *No Title*. (n.d.-a). https://www.analyticsvidhya.com/blog/2017/09/understaing-support-vector-machine-example-code/
[40] *No Title*. (n.d.-b). https://www.lemagit.fr/definition/Apprentissage-non-supervise
[41] *No Title*. (n.d.-c). https://www.microsoft.com/en-us/research/publication/sequential-minimal-optimization-a-fast-algorithm-for-training-support-vector-machines/
[42] Palattella, M. R., Accettura, N., Vilajosana, X., Watteyne, T., Grieco, L. A., Boggia, G., & Dohler, M. (2012). Standardized protocol stack for the internet of (important) things. *IEEE Communications Surveys & Tutorials*, *15*(3), 1389–1406.
[43] PARENT, O., & EUSTACHE, J. (2006). Les réseaux bayésiens. *Université Claude Bernard Lyon*, *1*.
[44] Porambage, P., Schmitt, C., Kumar, P., Gurtov, A., & Ylianttila, M. (2014). PAuthKey: A pervasive authentication protocol and key establishment scheme for wireless sensor networks in distributed IoT applications. *International Journal of Distributed Sensor Networks*, *10*(7), 357430.
[45] Porras, P. A., & Valdes, A. (1998). Live Traffic Analysis of TCP/IP Gateways. *NDSS*.
[46] Pujolle, G., & Salvatori, O. (2008). *Cours réseaux et télécoms: avec exercices corrigés*. Eyrolles.
[47] Rhouma, R. (n.d.). *Audit et Sécurité Informatique*. https://sites.google.com/site/rhoouma/teaching-at-esen/cryptographie-et-securite-de-l-

information
[48] Sennoun, Y. (n.d.). *IoT & Les protocoles de communication pour les réseaux sans-fil et filaires : Comment choisir ?* Retrieved June 1, 2020, from https://blog.engineering.publicissapient.fr/2018/08/29/iot-les-protocoles-de-communication-pour-les-reseaux-sans-fil-et-filaires-comment-choisir/
[49] Sethi, P., & Sarangi, S. R. (2017). Internet of things: architectures, protocols, and applications. *Journal of Electrical and Computer Engineering*, *2017*.
[50] Stallings, W. (2006). *Cryptography and network security, 4/E*. Pearson Education India.
[51] Trabelsi, Z., & Ly, H. (2005). *La sécurité sur Internet*. Hermès Science publications.
[52] Ulmann, B. (2004). *Cisco et la sécurité*. Novembre.
[53] Vasseur, J., Agarwal, N., Hui, J., Shelby, Z., Bertrand, P., & Chauvenet, C. (2011). RPL: The IP routing protocol designed for low power and lossy networks. *Internet Protocol for Smart Objects (IPSO) Alliance*, *36*.
[54] Victor MORARU. (2005). *La sécurité dans les réseaux haut débit*. 1–33.
[55] Weber, R. H. (2010). Internet of Things–New security and privacy challenges. *Computer Law & Security Review*, *26*(1), 23–30.
[56] *Weka*. (n.d.). Retrieved October 16, 2020, from https://www.cs.waikato.ac.nz/ml/weka/?fbclid=IwAR2ZaIuZyVXM-v51C3YvCs7NMnuxGLJTeEoHEq67KdxXX3bU9ByLuJqxnhs
[57] Y.ait mouhoub, F. B. (2015). *Propotion d'un modèle de confaince pour l'internet des Objets*. Université A/MIRA de Bejaia.
[58] Yann Berthier, J., & Baptiste. (2004). *Détection d'intrusions et analyse forensique*.

Webography

[1] Adrien Haccoun. (n.d.). *Comparaison de méthodes de classifications*. https://www.lri.fr/~antoine/Courses/Master-ISI/ISI-10/Projets_2012/Projet_DM.pdf
[2] *Apprentissage Supervisé*. (n.d.). Retrieved October 16, 2020, from https://machinelearnia.com/apprentissage-supervise-4-etapes/?fbclid=IwAR2TI466K-dZSzo8ljjvX5pob1TsojLg_UMFp1X1g6aM3BW7TPCkug2SMeE
[3] Burgermeister, D., & Krier, J. (2006). *Les systèmes de détection d'intrusions*. Article disponible sur http://dbprog. developpez. com.
[4] *Cooja Simulator*. (n.d.). Retrieved July 10, 2020, from https://anrg.usc.edu/contiki/index.php/Cooja_Simulator
[5] *Into the Battlefield: A Security Guide to IoT Botnets*. (n.d.). Retrieved June 20, 2020, from https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/into-the-battlefield-a-security-guide-to-iot-botnets
[6] *No Title*. (n.d.-a). https://www.analyticsvidhya.com/blog/2017/09/understaing-support-vector-machine-example-code/
[7] *No Title*. (n.d.-b). https://www.lemagit.fr/definition/Apprentissage-non-supervise
[8] *No Title*. (n.d.-c). https://www.microsoft.com/en-us/research/publication/sequential-minimal-optimization-a-fast-algorithm-for-training-support-vector-machines/
[9] Rhouma, R. (n.d.). *Audit et Sécurité Informatique*. https://sites.google.com/site/rhoouma/teaching-at-esen/cryptographie-et-securite-de-l-information

[10] Sennoun, Y. (n.d.). *IoT & Les protocoles de communication pour les réseaux sans-fil et filaires : Comment choisir ?* Retrieved June 1, 2020, from https://blog.engineering.publicissapient.fr/2018/08/29/iot-les-protocoles-de-communication-pour-les-reseaux-sans-fil-et-filaires-comment-choisir/

[11] *Weka*. (n.d.). Retrieved October 16, 2020, from https://www.cs.waikato.ac.nz/ml/weka/?fbclid=IwAR2ZaIuZyVXM-v51C3YvCs7NMnuxGLJTeEoHEq67KdxXX3bU9ByLuJqxnhs