République Algérienne Démocratique et Populaire
Ministre de l'Enseignement Supérieur et de la Recherche Scientifique
Université Mouloud MAMMERI de Tizi Ouzou
X●ΘΛ●ΣX [://:V ●X[●Λ[●O
Faculté de Génie Electrique et d'Informatique
Département d'Informatique

Mémoire de fin d'étude

En vue d'obtention du diplôme du master académique en informatique

Option : Systèmes Informatiques (SI)

Défis de sécurité de l'Internet des Objets

Problèmes et solutions

Encadré par :

Encadreur : Mr M. RAMDANI

Présenté par :

- M^elle^ LARRAS Melissa
- M^elle^ KHALFOUNI Djamila

Soutenu publiquement le 11/07/2019 devant le jury composé de :

Président: Mr S. SADI

Examinateur: Mr I .FILALI

Promotion 2018/2019

Remerciements

Nous remercions d'abord Dieu le tout puissant qui nous a donné la force, le courage et la volonté pour accomplir ce travail.

Nous tenons à exprimer nos profondes gratitudes et nos sincères remerciements à notre encadreur Mr RAMDANI Mohammed pour la haute qualité de son encadrement, son suivi, sa disponibilité et ses conseils. Sans vous, la réalisation de ce mémoire n'aurait pas eu lieu. Encore une fois, merci beaucoup.

Nos remerciements s'adressent à monsieur le président S.SADI par l'honneur qu'il nous fait de présider ce jury de soutenance, nous lui exprimons notre gratitude profonde.

Nous tenons également à remercier Mr I.FILALI qui a aimablement accepter d'examiner et de juger notre travail et pour l'intérêt qu'il y porte.

Nous adressons nos sincères remerciements à tous les professeurs du département informatique et toutes les personnes qui par leurs conseils et leurs critiques ont guidé nos réflexions et ont accepté à nous rencontrer et répondre à nos questions durant nos recherches.

Un grand merci pour nos familles, pour leur soutien permanent, leur présence et leur encouragement.

Enfin nous remercions tous ceux qui ont contribué de loin ou de près à la réalisation de ce travail.

Dédicaces

Je dédié ce modeste mémoire qui est le fruit de nombreuses années d'étude et de travail, tout en exprimant ma profonde gratitude et sympathie à toutes les personnes qui ont participé de prés et de loin pour mener à bien ce projet et plus particulièrement :

A mon père qui m'a toujours épaulé, qui peut être fier de trouver ici le résultat de longues années de sacrifices et de privations pour m'aider à avancer dans la vie. Puisse dieu faire en sorte que ce travail porte son fruit. Merci pour les valeurs nobles, l'éducation et le soutien permanent venu de toi.

A ma mère, qui a œuvré pour ma réussite, de par son amour, son soutien tous les sacrifices consentis et ses précieux conseils pour toute son assistance et sa présence dans ma vie.

A mon adorable petit frère «Amayas» que j'aime sans limites.

A la mémoire de ma grande mère «Dahbia».

A mon grand père «Akli» et sa femme.

A toutes mes tantes et leur famille.

A tout mes oncles et leur famille.

A ma chère binôme Djamila, ma meilleure amie avec laquelle que j'ai partagé tous mes années d'étude.

A tous mes ami(e)s avec lesquels que j'ai partagé les bons moments.

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

Melissa

Dédicaces

Je dédié ce modeste mémoire qui est le fruit de nombreuses années d'étude et de travail, tout en exprimant ma profonde gratitude et sympathie à toutes les personnes qui ont participé de prés et de loin pour mener à bien ce projet et plus particulièrement :

A mon père qui m'a toujours épaulé, qui peut être fier de trouver ici le résultat de longues années de sacrifices et de privations pour m'aider à avancer dans la vie. Puisse dieu faire en sorte que ce travail porte son fruit. Merci pour les valeurs nobles, l'éducation et le soutien permanent venu de toi.

A ma mère, qui a œuvré pour ma réussite, de par son amour, son soutien tous les sacrifices consentis et ses précieux conseils pour toute son assistance et sa présence dans ma vie.

A ma plus adorable sœur «Dahbia» que j'aime sans limites, son mari « Hicham » et ses deux petits anges « Iyad, Assir ».

A mes chers frères Slimane, Amar, Samir, Nabil, Yanis

A mes grands parents «Arezki» et « Dahbia ».

A toutes mes tantes et leur famille.

A tout mes oncles et leur famille.

A tout mes cousins et leur famille.

A ma chère binôme Melissa, ma meilleure amie avec laquelle que j'ai partagé tous mes années d'étude.

A tous mes ami(e)s avec lesquels que j'ai partagé les bons moments.

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

Djamila

Résumé

Internet est un réseau informatique mondial, qui se transforme progressivement en un réseau étendu dit Internet des Objets (IdO), reliant des milliards d'êtres humains et des dizaines de milliards d'objets.

Internet des Objets désigne l'omniprésence autour de nous de diverses technologies sans fil telles que les étiquettes, les capteurs, les actionneurs, les téléphones mobiles et les RFID qui, à travers des schémas d'adressage uniques, ces objets interagissent les uns avec les autres et coopèrent pour atteindre les objectifs communs. Cependant, l'IdO pose plusieurs problèmes de l'hétérogénéité, routage et d'identification et de sécurité à cause de ces limites en terme de (mémoire, énergie, puissance de calcul), et vu que l'IdO est déployé dans plusieurs domaines (la santé, l'industrie, la domotique…), elle requiert un niveau de sécurité élevé.

Pour cela, nous allons étudier à travers ce sujet les différentes vulnérabilités et attaques que l'IdO rencontre, les différentes solutions proposées et en particulier les protocoles cryptographiques à base de courbes elliptiques, par la suite nous allons analyser les résultats de quelques travaux réalisés sur la comparaison entre RSA et ECC sur Java Card et Raspberry.

Mots clés : Internet des Objets(IdO), RCSFs, cryptographie des courbes elliptiques, problèmes de sécurité.

Abstract

The Internet is a global computer network, which is progressively evolving into a vast Internet of Things (IoT) network, connecting billions of people and tens of billions of objects.

Internet of Things refers to the ubiquity around us of various wireless technologies such as tags, sensors, actuators, mobile phones and RFIDs that, through unique addressing schemes, these objects interact with each other. Others and cooperate to achieve the common objectives. However, the Internet of Things poses several problems of heterogeneity, routing and identification and security because of these limits in terms of (memory, energy, computing power), and since the IoT is deployed in several fields (health, industry, home automation ...), it requires a high level of security.

For this purpose, we will study through this topic the various vulnerabilities and attacks that the IoT encounters, the various solutions proposed and in particular the cryptographic protocols based on elliptic curves, later we will analyze the results of some work done on the comparison between RSA and ECC on Java Card and Raspberry.

Keywords: Internet of Things (IoT), RCSFs, elliptic curve cryptography, security problems.

Liste des figures:

Liste des tableaux:

Liste des abréviations

IoT	**I**nternet **o**f **T**hings
IdO	**I**nternet **D**es **O**bjets
RFID	**R**adio **F**requency **I**dentification
IoT-GSI	**I**nternet **of T**hings **G**lobal **S**tandards **I**nitiative
ITU	**I**nternational **T**elecommunication **U**nion
IEEE	**I**nstitute of **E**lectrical and **E**lectronics **E**ngineers
CERP-IoT	**C**luster des **p**rojets **e**uropéens de **r**echerche sur l'**I**nternet **d**es **o**bjets
OC	**O**bjet **C**onnecté
M2M	**M**achine **T**o **M**achine
NFC	**N**ear **F**ield **C**ommunication
SCADA	**S**upervisory **C**ontrol **A**nd **D**ata **A**cquisition
WIFI	**W**ireless **F**idelity
IP	**I**nternet **P**rotocol
Ipv6	**I**nternet **P**rotocol **v**ersion 6
3/4 G	**G**eneration
6lowpan	**I**Pv6 **L**ow power **W**ireless **P**ersonal **A**rea **N**etworks
RPL	**R**outing **P**rotocol for **L**ow power and **L**ossy Networks
ETSI	**E**uropean **T**elecommunications **S**tandards **I**nstitute
XDSL	**D**igital **S**ubscriber **L**ine
WIMAX	**W**orldwide **I**nteroperability for **M**icrowave **A**ccess
WLAN	**W**ireless **L**ocal **A**rea **N**etwork
API	**A**pplication **P**rogramming **I**nterface
IPV4	**I**nternet **P**rotocol **v**ersion 4
HTTP	**H**yperText **T**ransfer **P**rotocol
RCSF	**R**éseau de **C**apteurs **S**ans **F**il

CoAP	**C**onstrained **A**pplication **P**rotocol
MQTT	**M**essage **Q**ueue **T**elemetry **T**ransport
TCP/IP	**T**ransmission **C**ontrol **P**rotocol/ **I**nternet **P**rotocol
BLE	**B**luetooth **L**ow**E**nergy
GSM	**G**lobal **S**ystem for **M**obile communication
SIM	**S**ubscriber **I**dentity **M**odule
XMPP	**E**xtensible **M**essaging and **P**resence **P**rotocol
REST	**R**epresentational **S**tate **T**ransfer
UDP	**U**ser **D**atagram **P**rotocol
TCP	**T**ransmission **C**ontrol **P**rotocol
IM	**I**nstant **M**essaging
V2V	**V**ehicule-**T**o-**V**ehicule
NIC	**T**he **N**ational **I**ntelligence **C**ouncil
USB	**U**niversal **S**erial **B**us
JTAG	**J**oint **T**est **A**ction **G**roup
DoS	**D**enial **of S**ervice
MITM	**M**an **I**n **T**he **M**iddle
DDos	**D**estribution **D**enial **o**f **S**ervice
C&C	**C**ommande & **C**ontrole
UID	**U**nique **I**dentifier
SSL	**S**ecure **S**ockets **L**ayer
TLS	**T**rasport **L**ayer **S**ecurity
SMS	**S**hort **M**essage **S**ystem
PIN	**P**ersonal **I**dentification **N**umber
HAN	**H**ome **A**rea **N**etwork
VPN	**V**irtual **P**rivate **N**etwork

RCSF	**R**éseau de **C**apteur **S**ans **F**il
RSA	**R**ivest, Adi **S**hamir **A**dleman
RC4	**R**ivest **C**ipher **4**
AES	**A**dvanced **E**ncryption **S**tandard.
DES	**D**ata **E**ncryption **S**tandard
ECC	**E**lliptic **C**urve **C**ryptography
ECDH	**E**lliptic **C**urve **D**iffie–**H**ellman
ECDSA	**E**lliptic **C**urve **D**igital **S**ignature **A**lgorithm
ECIES	**E**lliptic **C**urve **I**ntegrated **E**ncryption **S**cheme
ECDLP	**E**lliptic **C**urve **D**iscrete **L**ogarithm Problem
KDF	**K**raft **d**urch **F**reude
MAC	**M**edia **A**ccess **C**ontrol
TIC	**I**nformation **T**echnology and **C**ommunication
WSN	**W**ireless **S**ensor **N**etworks
RTOS	**R**eal **T**ime **O**perating **S**ystem

Sommaire

Chapitre II : Problèmes de sécurité dans l'Internet des Objets

Chapitre III : Les différentes solutions proposées pour l'Internet des Objets

Chapitre IV : La cryptographie moderne pour l'Internet des Objets

Introduction générale

Internet a changé notre mode de vie au cours de ces dernières années et continue de le faire, notamment avec le nombre croissant d'objets/appareils nous appartenons ou nous entourons capables de se connecter à Internet. Aujourd'hui, L'Internet des Objets(IdO), ou Internet of Things (IoT) en anglais, est une base pour connecter des objets, des capteurs, des actionneurs et d'autres technologies intelligentes, ajoutant ainsi une nouvelle dimension au monde de technologie d'information et de la communication(TIC).

L'Internet des Objets (IdO) est un concept dans lequel le monde virtuel des technologies de l'information s'intègre parfaitement au monde réel des objets. Il permet de relever certains défis technologiques aux quels la communauté fait face dans la vie de tous les jours. Ce nouveau concept est une solution innovante pour réaliser une analyse quantitative de tous les objets qui nous entourent. Une condition préalable requise pour l'IdO est l'identification des objets. Si tous les objets et les personnes de la vie réelle étaient équipés d'identifiants (physique ou logique :@IP, @MAC, Tag RFID, ou tout autre type d'identifiant), ils pourraient être gérés et inventoriés par des ordinateurs. L'un des éléments importants dans le paradigme IoT est les réseaux de capteurs sans fil (RCSFs). Ces RCSFs ont obtenu une popularité élevée en raison de leur large éventail d'applications. Ces réseaux ont motivé beaucoup de travaux de recherches en raison de leurs caractéristiques uniques qui les différencient des réseaux câblés/sans-fil traditionnels.

Les technologies de communication sans fil sont sujettes à différents types de menaces de sécurité et d'attaques, rendant ainsi les objets et les services IoT, reposant majoritairement sur ces technologies, une cible privilégiée des attaquants. En effet, le déploiement des objets formant l'IdO dans un environnement souvent sans surveillance, ainsi que les limites en protection physique ainsi qu'en ressources (stockage, calcul, mémoire, énergie) de ces objets, rendent l'IdO vulnérable (objets, réseaux, applications) à une variété d'attaques potentielles, pour lesquels les solutions de sécurité conventionnelles sont mal adaptées.

La sécurité est parmi les principaux défis de l'Internet des Objets (IdO). Cependant, aujourd'hui, les chercheurs dans ce domaine tentent de trouver des solutions pour assurer la sécurité des objets connectés, des réseaux et garantir la confidentialité et la sécurité de la vie privée des utilisateurs, tout en prenant en considération les limites des dispositifs de l'IdO (énergie, mémoire, puissance de calcul, etc.) , mais en gardant les performances du réseau.

Vu les domaines d'application de l'IdO, le besoin d'apporter une solution de sécurité fiable parait important voire crucial, mais la problématique posée par la faiblesse de calcul et

de mémoire limitée des objets amènent à se poser des questions nouvelles sur les méthodes de sécurité à utiliser.

La cryptographie est toujours considérée comme une des solutions dominantes pour assurer la confidentialité et l'intégrité des informations, en utilisant des méthodes mathématiques qui nous permettent de rendre les messages illisibles. L'utilisation de la cryptographie implique souvent des calculs compliqués et intensifs, ce qui représente un challenge à relever dans l'IdO. Il existe deux types de cryptographie : symétrique et asymétrique, la première offre une performance de calcul plus intéressante sans utiliser une clé extrêmement longue et comme on partage la même clé pour le chiffrement et le déchiffrement, la mise en place d'une distribution sure des clés au sein d'un réseau contenant un grand nombre de nœuds devient un problème complexe. Contrairement à ce type, la cryptographie asymétrique offre des protocoles sophistiqués pour la génération des clés et permet de chiffrer et signer des messages. Cependant, l'application de cette solution nécessite des calculs plus complexes et l'utilisation des clés beaucoup plus longues. Le cryptosystème le plus utilisé est le RSA, qui pour avoir une sécurité assez robuste, il faut utiliser une clé comprise entre 1024 et 2048 bits. Un autre cryptosystème qui attire l'attention des chercheurs aujourd'hui est celui de ECC (Elliptic Curve Cryptography) et qui offre le même niveau de sécurité que RSA avec une clé beaucoup plus courte.

Dans ce travail, nous avons fait un tour d'horizon sur toutes les solutions de sécurité proposées aux problèmes et aux défis que l'Internet des Objets affronte aujourd'hui, puis nous avons mené quelques expériences sur une carte reprogrammable faible en ressources pour calculer le temps d'exécution de chaque solution proposée dans le cadre de la cryptographie moderne et nous les avons comparé à d'autres résultats obtenus par la communauté des chercheurs dans ce domaine.

Notre travail est organisé en quatre chapitres :

- **Chapitre 1 :** Dans ce chapitre nous avons évoqué l'Internet des Objets, définition de ses concepts de base, son évolution, son architecture, son fonctionnement, un exemple de l'IdO qui est les RCSFs, et ses domaines d'application.
- **Chapitre II :** Nous avons présenté dans ce chapitre les vulnérabilités et les attaques rencontrées dans l'Internet des Objets.
- **Chapitre III :** Le chapitre 3 est dédié aux différentes solutions proposées pour l'Internet des Objets.

- **Chapitre IV :** Nous avons présenté la cryptographie moderne dédiée à l'Internet des Objets qui est la cryptographie des courbes elliptiques et les résultats de son implémentation sur une carte arduino, puis nous avons représenté quelques travaux réalisés sur la comparaison RSA vs.ECC sur Java Card et Raspberry, dans le dernier chapitre. Nous avons terminé notre travail par une conclusion générale.

Chapitre I : L’Internet des Objets : Concepts et définitions

I. Introduction

Internet des Objets (IdO ou IoT pour Internet of Things) est un réseau mondial d'objets qui repose sur l'idée que tous les objets peuvent être connectés un jour à l'internet, ces objets sont adressables de manière unique. Tout objet, y compris (des ordinateurs, des capteurs, des RFID et des téléphones mobiles) seront en mesure d'émettre de l'information et éventuellement de recevoir des commandes. L'IdO ouvre la voie vers une multitude de scenarios basés sur l'interconnexion entre le monde physique et le monde virtuel. Cependant, il fait face à un nombre de problématiques qui nécessitent d'être étudiées pour permettre à l'Internet des objets d'atteindre son plein potentiel. Dans ce chapitre, nous présentons d'abord l'IdO, et quelques définitions des concepts de base de l'IdO, son évolution, et son architecture, ensuite nous allons aborder ses domaines d'application, son fonctionnement et ses contraintes techniques, puis nous allons terminer par la présentation d'un exemple de l'IdO qui est les RCSFs et nous terminons par une conclusion.

II. Définitions

II.1 Internet des Objets (IdO)

Le terme **d'Internet des Objets (IdO)** (en anglais ***Internet Of Things IoT***) ne fait pas encore consensus sur sa définition, ce qui s'explique par la jeunesse de ce concept en pleine mutation. Il existe ainsi autant de définitions que d'entités impliquées dans la réflexion, le développement ou la normalisation de ce nouveau paradigme.

Le groupe de travail Internet of Things Global Standards Initiative (IoT-GSI), piloté par l'International Telecommunication Union (ITU), considère l'IoT comme *«une infrastructure mondiale au service de la société de l'information* » permettant *« d'offrir des services évolués en interconnectant des objets (physiques et virtuels) grâce à l'interopérabilité de technologies de l'information et de la communication existantes ou en évolution»*[1].

De son côté, **l'IEEE** définit l'IoT comme un *« réseau d'éléments chacun muni de capteurs qui sont connectés à Internet »* [1].

Le **CERP-IoT** « Cluster des projets européens de recherche sur l'Internet des Objets » définit l'Internet des Objets comme : *« une infrastructure dynamique d'un réseau global. Ce réseau global a des capacités d'auto-configuration basée sur des standards et des protocoles de communication interopérables. Dans ce réseau, les objets physiques et virtuels ont des*

identités, des attributs physiques, des personnalités virtuelles et des interfaces intelligentes, et ils sont intégrés au réseau d'une façon transparente » [2].

Cette vision de l'Internet des Objets introduira une nouvelle dimension aux technologies de l'information et de la communication : en plus des deux dimensions temporelle et spatiale qui permettent aux personnes de se connecter de n'importe où et à n'importe quel moment, nous aurons une nouvelle dimension **« *objet* »**qui leur permettra de se connecter à n'importe quel objet (Figure 1)[3].

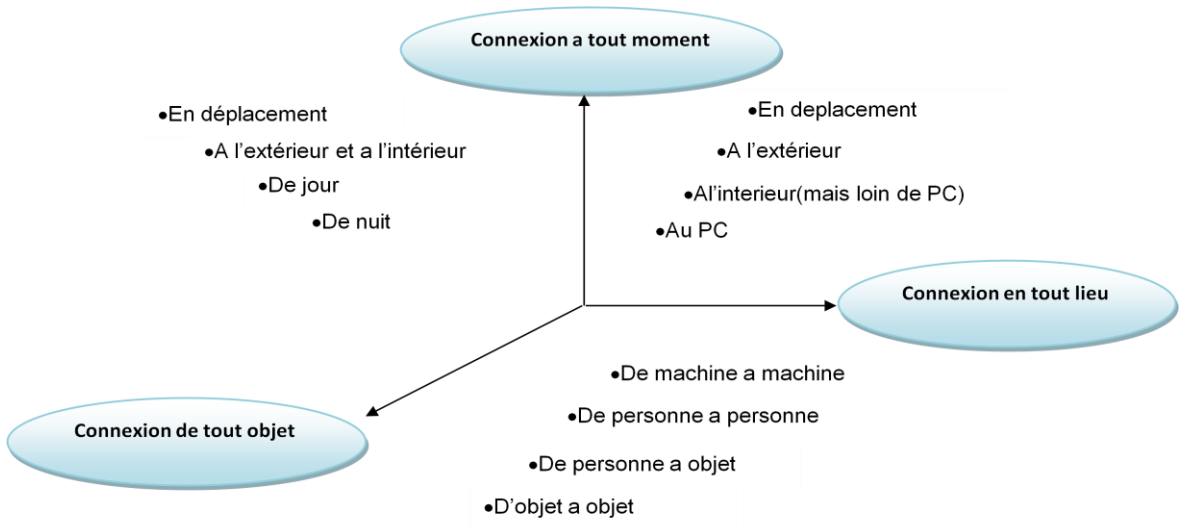

Figure 1:Une nouvelle dimension pour l'IdO [3]

II.2 C'est quoi un objet connecté?

Objet connecté (OC) : Tout objet possédant la capacité d'échanger des données avec d'autres entités physiques ou numériques [4]. Un **OC** peut interagir avec le monde physique de manière indépendante sans intervention humaine. Il possède plusieurs contraintes telles que la mémoire, la bande passante ou la consommation d'énergie, etc. Il doit être adopté à un usage, il a une certaine forme d'intelligence, une capacité de recevoir, de transmettre des données avec des logiciels grâce aux capteurs embarqués. Un objet connecté a une valeur si uniquement est connecté à d'autres objets et briques logicielles, par exemple, une montre connectée n'a d'intérêt qu'au sein d'un écosystème orienté santé/bien-être, qui va bien au-delà de connaître l'heure. Un **OC** à trois éléments clés :

– Les données produites ou reçues, stockées ou transmises.

– Les algorithmes pour traiter ces données.

– L'écosystème dans lequel il va réagir et s'intégrer [5].

En effet, plusieurs contraintes liées aux objets connectés sont à prendre en compte [12] :

- **Ergonomie** : La taille et le design influenceront les mesures de sécurité acceptables par les utilisateurs par exemple, la taille de l'écran pour taper un mot de passe.
- **Puissance** : Les petits objets embarqués actuels ont une puissance de calcul limitée. Plusieurs opérations ne peuvent être réalisées en même temps dans un laps de temps raisonnable. Par exemple, Apple a conseillé aux développeurs de ne pas implémenter des fonctionnalités nécessitant de long temps d'exécution sur l'Apple Watch.
- **Connectivité** : L'Internet des Objets utilise généralement du Bluetooth ou des protocoles NFC, deux technologies ayant une portée et un débit limité, ce qui ne permet pas toujours d'embarquer un niveau de sécurité suffisant.
- **Durée de vie de la batterie** : Les algorithmes cryptographiques (comme du chiffrement / déchiffrement asymétrique en temps réel) peuvent affecter durement la consommation énergétique, même s'ils permettent de procurer un meilleur niveau de protection.
- **Gestion des mises à jour** : Il est indispensable de mettre à jour le système, sans interférer avec l'utilisation de l'objet. Cela est particulièrement frappant dans le cas des voitures connectées que l'on ne peut pas conduire lorsque le logiciel est en train de se mettre à jour. Cela peut prendre plus de 45 minutes.

	Objet connecté	**Equipement de bureau**
Mémoire vive	100 KO	2 GO
Stockage	256 KO	256 GO
Fréquence	32 MHZ	3 GHZ
Consommation d'énergie	10 µW	10 W
Bande passante	1 Kbits/s	10 Mbits

Tableau 1: Tableau comparatif des caractéristiques techniques des objets connectés à un équipement de bureau [53]

II.3 C'est quoi un objet intelligent ?

Pour mieux comprendre le sens que revêt l'expression « objet intelligent » il est essentiel de s'intéresser à la signification du mot intelligence. Selon l'encyclopédie Wikipédia, le mot intelligence vient de la latine intelligentsia (faculté de comprendre). Ce mot peut être vu comme un ensemble de capacités permettant de comprendre les choses et les faits ainsi qu'une capacité d'agir de manière adaptée à une situation particulière.

Les objets intelligents sont donc des objets qui sont dotés d'une certaine intelligence mais on ne peut cependant pas encore prétendre que l'intelligence d'un objet soit égale à celle d'un être humain. On appelle donc 'objet intelligent' les objets capables d'imiter une réflexion humaine. Ces objets doivent être capables de s'identifier et d'agir sur leur environnement. Ils doivent aussi pouvoir communiquer avec d'autres objets intelligents à l'aide de réseaux [13].

II.4 Machine-to-Machine (M2M)

II.4.1 Qu'est-ce que le M2M ?

Le **M2M (Machine-to-Machine)** constitue un ensemble de technologies réseaux sans fil ou filaires rendant des systèmes communiquant et leur permettant de s'échanger automatiquement des informations, sans intervention humaine.

II.4.2 Historique de la technologie machine à machine

Les racines du M2M sont bien implantées dans l'industrie manufacturière, où d'autres technologies, telles que le SCADA (Supervisory Control And Data Acquisition)et la surveillance à distance, ont permis de gérer et de contrôler à distance les données d'équipements.

Bien que l'origine de l'acronyme ne soit pas vérifiée, la première utilisation de la communication de machine à machine est souvent attribuée à Theodore Paraskevakos, qui a inventé et breveté une technologie liée à la transmission de données sur des lignes téléphoniques, à la base de l'identification du correspondant moderne.

Nokia a été l'une des premières entreprises à utiliser cet acronyme à la fin des années 90. En 2002, elle s'est associée à Opto 22 pour offrir des services de communication sans fil M2M à ses clients.

En 2003, M2M Magazine a été lancé. La publication a depuis défini les six piliers du M2M comme la surveillance à distance, la RFID, la mise en réseau de capteurs, les services intelligents, la télématique et la télémétrie.

II.4.3 Comment fonctionne le M2M ?

L'objectif principal de la technologie machine à machine est d'exploiter les données des capteurs et de les transmettre à un réseau. Les systèmes M2M utilisent souvent des réseaux publics et des méthodes d'accès, par exemple cellulaires ou Ethernet, pour le rentabiliser.

Les principaux composants d'un système M2M incluent, entre autres, des capteurs, une RFID, une liaison de communication Wi-Fi ou cellulaire et un logiciel informatique autonome programmé pour aider un périphérique réseau à interpréter les données et à prendre des décisions. Ces applications M2M traduisent les données, ce qui peut déclencher des actions automatisées préprogrammées.

L'un des types les plus connus de communication entre machines est la télémétrie , utilisée depuis le début du siècle dernier pour transmettre des données opérationnelles.

Outre le fait de pouvoir surveiller à distance des équipements et des systèmes, les principaux avantages du M2M sont les suivants:

- Réduction des coûts en minimisant la maintenance de l'équipement et les temps d'arrêt.
- Augmentation des revenus en révélant de nouvelles opportunités commerciales pour le service des produits sur le terrain.
- Amélioration du service client en surveillant et en entretenant de manière proactive les équipements avant qu'ils ne tombent en panne ou uniquement lorsque cela est nécessaire.

II.4.4Applications M2M

La communication de machine à machine est souvent utilisée pour la surveillance à distance. Les entreprises de services publics comptent souvent sur les appareils et les applications M2M non seulement pour récupérer l'énergie, comme le pétrole et le gaz, mais aussi pour facturer les clients via l'utilisation de compteurs intelligents et pour détecter les facteurs de chantier, tels que la pression, la température, le statut des équipements.

En télémédecine, les appareils M2M peuvent permettre de surveiller en temps réel les statistiques de l'état civil des patients, de délivrer des médicaments si nécessaire ou de suivre les actifs de soins de santé.

Le M2M est également un aspect important du contrôle à distance, de la robotique, du contrôle du trafic, de la sécurité, de la logistique et de la gestion de flotte, et de l'automobile.

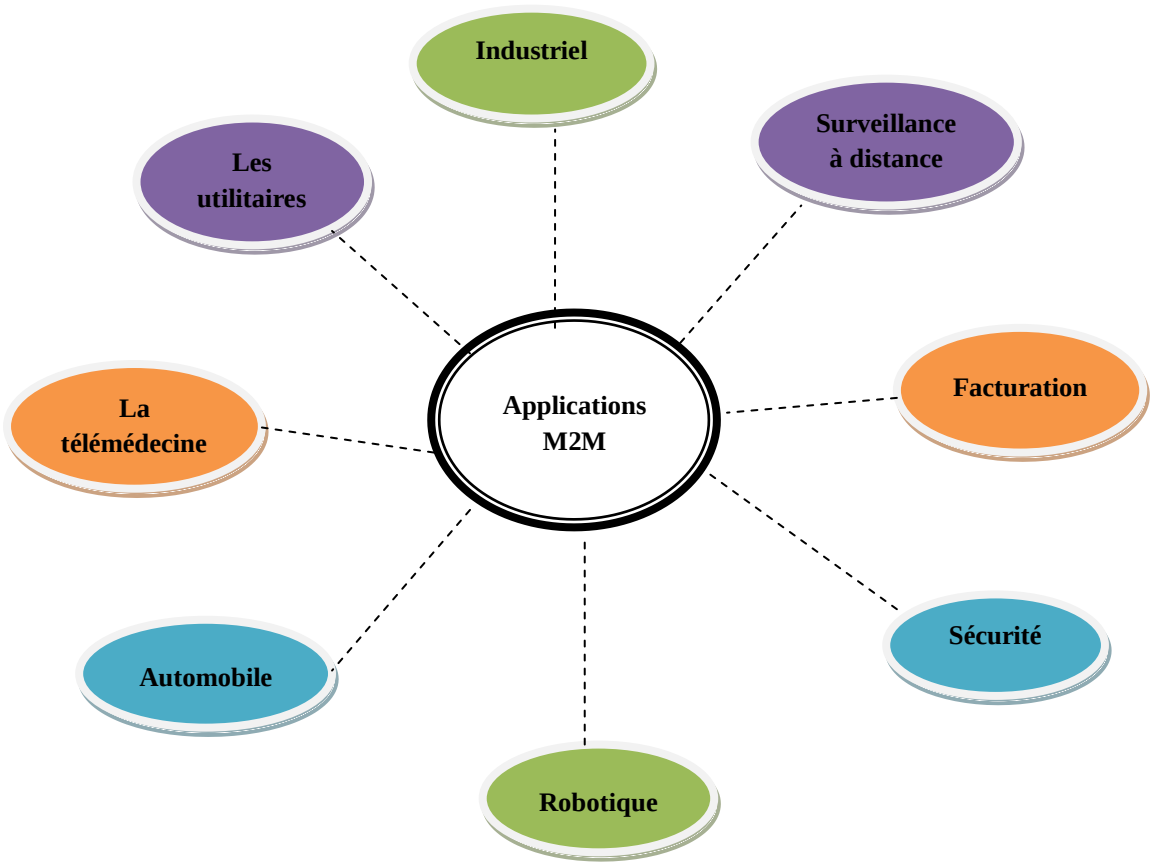

Figure 2:Applications M2M

II.4.5 M2M vs. IoT

Tandis que beaucoup de chercheurs utilisent les termes indifféremment, M2M et IoT ne sont pas identiques. L'IoT a besoin de M2M, mais le M2M n'a pas besoin d'IoT. Les deux termes concernent la communication des périphériques connectés, mais les systèmes M2M sont souvent des équipements isolés et mis en réseau. Les systèmes IoT poussent le M2M à un niveau supérieur en rassemblant des systèmes disparates au sein d'un vaste écosystème connecté.

Les systèmes M2M utilisent des communications point à point entre les machines, les capteurs et le matériel sur des réseaux cellulaires ou câblés, tandis que les systèmes IoT

s'appuient sur des réseaux IP pour envoyer les données collectées à partir d'appareils connectés à des objets IoT à des passerelles, des plateformes Cloud ou middleware.

M2M vs. IoT : Quelle est la différence ?	
M2M	**IoT**
Machines	Capteurs
Basé sur le matériel	Basé sur le logiciel
Applications verticales	Applications horizontales
Déployé dans un système fermé	Se connecte à un plus grand réseau
Machines communiquant avec des machines.	Machines communiquant avec des machines, humains avec des machines, machines avec des humains.
Utilise des protocoles non IP.	Utilise les protocoles IP.
Peut utiliser le Cloud mais pas obligé.	Utilise le Cloud.
Les machines utilisent la communication point à point, généralement intégrée au matériel.	Les appareils utilisent les réseaux IP pour communiquer.
Communication souvent à sens unique (one-way)	Communication dans les deux sens (back and forth).
Le but principal est de surveiller et de contrôler.	Application multiples : communication à plusieurs niveaux.
Fonctionne via des réponses utilisant des triggers basées sur une action.	Peut mais ne doit pas nécessairement opérer sur des réponses déclenchées (triggers).
Options d'intégration limitées, les appareils doivent avoir des normes de communication complémentaires.	Options d'intégration illimitées, mais nécessite un logiciel de gestion des communications / protocoles
Données structurées	Données structurées et non structurées

Tableau 2: M2M vs. IoT

II.4.6 Sécurité M2M

Les systèmes de machine à machine sont confrontés à un certain nombre de problèmes de sécurité, allant de l'accès non autorisé à l'intrusion sans fil du piratage de périphérique. La sécurité physique, la confidentialité, la fraude et l'exposition des applications critiques doivent également être prises en compte.

Les mesures de sécurité M2M classiques consistent notamment à rendre les périphériques et les machines inviolables, à incorporer une sécurité intégrée dans les machines, à assurer la sécurité des communications via le cryptage et à sécuriser les serveurs principaux, entre autres. La segmentation des périphériques M2M sur leur propre réseau et la gestion de l'identité, de la confidentialité des données et de la disponibilité des périphériques peuvent également aider à lutter contre les risques de sécurité liés au M2M.

III. Evolution de l'IdO

Les premiers objets connectés n'apparaissent que dans les années 1990. Il s'agit de grille-pain, machines à café ou autres objets du quotidien. En 2000, le fabricant cornée LG est le premier industriel à parler sérieusement d'un appareil électroménager relié à internet. Les années 2000 verront les premières expérimentations d'appareils connectés à Internet. Ils l'utilisent notamment pour consulter des informations de manière automatique.

En 2003, la population mondiale a frôlé les 6 milliards d'individus et un demi-milliard d'appareils connectés à Internet. L'idée de l'Internet des Objets est apparue en 2009, boosté par l'apparition des Smartphones, le nombre d'appareils connectés à Internet a atteint 12,5 milliards en 2010, alors que la population mondiale était de 6,8 milliards.

Aujourd'hui l'IoT prend de l'ampleur et en ce qui concerne l'avenir, Les experts estiment que 50 milliards d'appareils seront connectés d'ici 2020, ces estimations ne prennent pas en considération l'évolution rapide d'Internet ni des avancées technologiques, mais uniquement les faits de l'heure actuelle. Le nombre de capteurs connectés à Internet pourrait augmenter de plusieurs millions, voire de plusieurs milliards du fait que tout ce qui existe se connecte (Animaux, lampes, maisons, personnes, chaussures, arbres,…) [14].

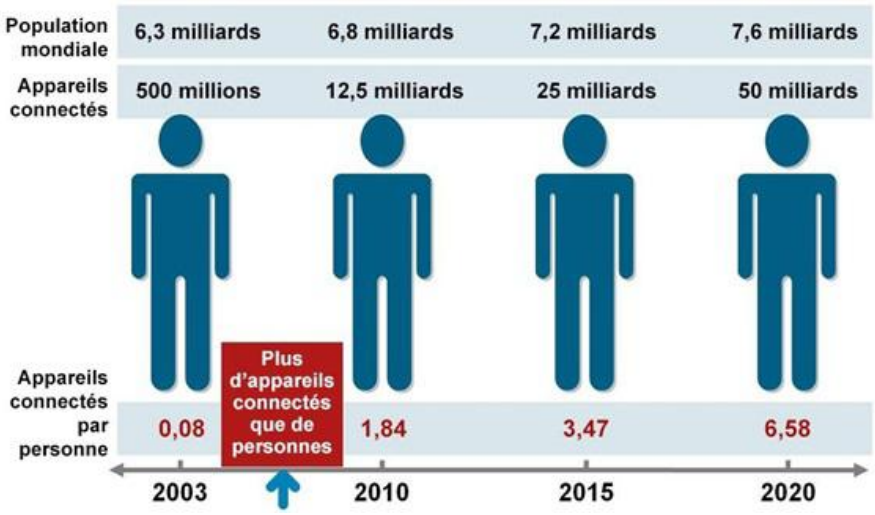

Figure 3:L'évolution d'IdO entre 2003 et 2020.

IV. Architecture et standardisation de l'IdO

L'IdO ne doit pas être considéré comme un concept utopique. En réalité, il sera fondé sur plusieurs technologies habilitantes tels que la RFID, la communication en champ proche (NFC : Near Field Communication), les capteurs et actionneurs sans fil, les communications machine-à-machine **(M2M),** l'ultralarge bande ou 3G/4G, IPv6, 6LowPAN et RPL, etc. qui devraient tous jouer un rôle important dans le développement de l'IdO. L'IdO voit ses racines remonter aux technologies **M2M (Machine-to-Machine)** pour le contrôle de processus de production à distance. Cette technologie a évolué vers le concept d'Internet des Objets depuis l'apparition d'IP sur réseaux mobiles cellulaires durant les années 2000.

L'ETSI préconise une évolution du paradigme M2M vers l'Internet des Objets. Cet organisme de normalisation propose une architecture à base de trois domaines comme illustré sur la Figure 4 : le domaine du réseau d'objets (Device Domain), le domaine du réseau cœur d'accès (Network), et le domaine des applications M2M et applications clientes (Application Domain) [3].

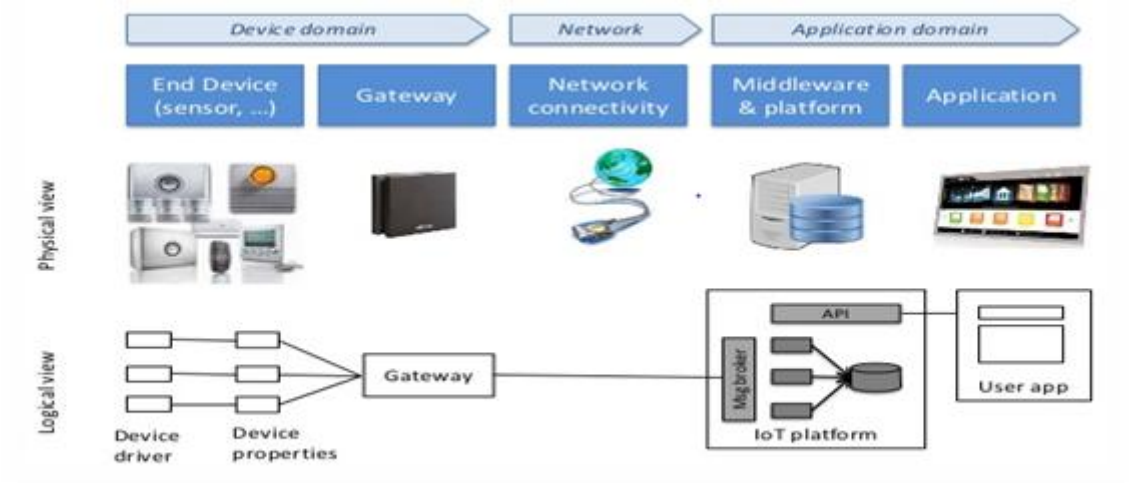

Figure 4:Architecture M2M [3]

- **Le domaine du réseau d'objets**

  Dans ce domaine, nous trouvons les différentes technologies d'interconnexion des objets M2M, RFID, Bluetooth, et des passerelles vers les réseaux cœur de transport [6].

- **Le domaine du réseau cœur d'accès**

  Dans ce domaine, nous trouverons les différentes technologies de réseaux de transport et d'accès comme xDSL, WIMAX, WLAN, 3G/4G, etc [6].

- **Le domaine des applications M2M et applications clientes**

  Ce domaine est composé de plateformes M2M, les Middlewares et API des applications M2M, processus métiers exploitant l'IdO, etc[6].

V. Domaines d'application de l'IdO

L'IdO couvrira un large éventail d'applications et touchera quasiment à tous les domaines que nous affrontons au quotidien. Ceci permettra l'émergence d'espaces intelligents autour d'une informatique omniprésente. Parmi ces espaces intelligents, on peut citer [3] :

- ✓ **La domotique :** Les objets connectés sont une réelle révolution, ils permettent de la rendre connectée, d'où le nom très utilisé de smart home des nombreux dispositifs de sécurité, surveillance, serrure connecté, dans le domaine de l'électroménager : réfrigérateur connecté. De la décoration de la maison des designs, lampe connectée, cadre lumineux. L'Internet des Objets change les modalités d'accès au réseau et produit de nouvelles interactions homme-machine. Il existe aussi le concept des villes intelligentes (Smart Cities) utilisé pour désigner l'écosystème cyber physique

émergeant par le déploiement d'une infrastructure de communication avancée et de nouveaux services sur des scénarios à l'échelle de la ville. Grace à des services avancés, il est en effet possible d'optimiser l'utilisation des infrastructures physiques de la ville (par exemple, les réseaux routiers, le réseau électrique, etc.) et la qualité de vie des citoyens [7].

- ✓ **L'énergie :** La gestion des grilles électriques se verra améliorée grâce à la télémétrie, permettant une gestion en temps réel de l'infrastructure de distribution de l'énergie. Cette interconnexion à large échelle facilitera la maintenance et le contrôle de la consommation et la détection des fraudes.
- ✓ **Le transport :** Dans ce domaine l'IdO appuiera les efforts actuels autour des véhicules intelligents au service de la sécurité routière et l'aide à la conduite. Cela portera sur la communication inter-véhicule et entre véhicules et infrastructure routière. L'IdO constituera ainsi un prolongement naturel des « systèmes de transport intelligents » et leurs apports en termes de sécurité routière, confort, efficacité de la gestion du trafic et économie du temps et de l'énergie.
- ✓ **La santé :** Dans le domaine de la santé, l'IdO permettra le déploiement de réseaux personnels pour le contrôle et le suivi des signes cliniques, notamment pour des personnes âgées. Ceci permettra ainsi de faciliter la télésurveillance des patients à domiciles, et apporter des solutions pour l'autonomie des personnes à mobilité réduite.
- ✓ **L'industrie :** Dans l'industrie l'IdO permettra un suivi total des produits, de la chaîne de production, jusqu'à la chaîne logistique et de distribution en supervisant les conditions d'approvisionnement. Cette traçabilité de bout en bout facilitera la lutte contre la contrefaçon, la fraude et les crimes économiques transfrontaliers.
- ✓ **L'agriculture :** Dans ce domaine, des réseaux de capteurs interconnectés à l'IdO peuvent être utilisés pour la supervision de l'environnement des cultures. Ceci permettra une meilleure aide à la décision en agriculture, notamment pour optimiser l'eau d'irrigation, l'usage des intrants, et la planification de travaux agricoles. Ces réseaux peuvent être aussi utilisés pour lutter contre la pollution de l'air, du sol et des eaux et améliorer la qualité de l'environnement en général.

VI. Fonctionnement de l'IdO

VI.1 Etapes de mise en place d'un IdO

Les objets connectés (OC) sont au sein de l'IdO, mais il est important de pouvoir connecter l'ensemble de ces objets, les faire échanger des informations et interagir au sein d'un même environnement.

La mise en place de l'IdO passe par les étapes suivantes :

1. L'identification : Rendre possible l'identification de chaque élément connecté (IPV4, IPV6).

2. L'installation de capteurs : Mise en place de dispositifs nous rapprochant du monde réel.

3. La connexion des objets entre eux : Etablir une connexion entre tous les objets afin qu'ils puissent échanger des informations (SigFox, LoRa, NFC, Bluetooth).

4. L'intégration : C'est Intégration des objets pour que les données soient transmises d'une couche à une autre (middlewares).

5. La connexion à un réseau : Relier les objets et leurs données au monde informatique via un réseau internet par exemple en utilisant (HTTP, REST, CoAP, MQTT) [5].

VI.2 Technologies de l'IdO

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, mais aussi entre des contextes physiques et des univers virtuels.

En effet, bien qu'il existe plusieurs technologies utilisées dans le fonctionnement de l'IoT, nous mettons l'accent seulement sur quelques-unes citées ci-dessous [6].

VI.2 .1 Les technologies de courte portée

NFC (Near Field Communication) : Les protocoles NFC sont fondés sur la technologie d'identification par radio fréquence RFID. Les objets équipés d'une puce électronique RFID possèdent une « étiquette » et sont automatiquement identifiés par radio fréquence lorsqu'ils se trouvent à proximité d'un équipement appelé interrogateur. Le protocole NFC est un standard de communication radiofréquence sans contact à très courte

distance, de l'ordre de quelques centimètres, permettant une communication simple entre deux équipements électroniques [15].

Bluetooth : Inventé en 1994 par la société suédoise Ericsson, le protocole Bluetooth est un standard de transfert de données sans fil. Il utilise une faible bande passante, ce qui ne lui permet de transférer que peu de données à de courtes distances, mais est également très peu énergivore. Inclus à l'immense majorité des téléphones mobiles, afin de réaliser une communication entre deux téléphones, ou entre un téléphone et un objet connecté de nature différente, il possède désormais de nombreuses applications : oreillette de discussion téléphonique sans fil, montre intelligente, moniteur de fréquence cardiaque, etc[15].

Zigbee : C'est un protocole de communication radio développé spécifiquement pour les applications de domotique. D'une portée moyenne de 100 mètres, il utilise une faible bande passante et est idéal pour le transfert de données en faible volume. Peu énergivore et conçu pour des échanges de données à bas débit, le dispositif Zigbee convient aux appareils alimentés par une pile ou une batterie, et en particulier aux capteurs[15].

VI.2.2 Les technologies de moyenne portée

Wi-Fi : Le Wi-Fi désigne un ensemble de protocoles de communications sans fil, permettant des connexions à haut débit sur des distances de 20 à 100 mètres. Il s'agit d'un réseau local sans fil très énergivore, qui ne convient que pour les appareils branchés sur secteur ou dont l'alimentation électrique peut être aisée et fréquente. Il permet de transférer rapidement beaucoup de données [15].

Bluetooth LowEnergy (BLE) : Aussi connue sous l'appellation Wibree, la technologie BLE est un protocole de réseau personnel sans fil à très basse consommation d'énergie. Comme la technologie Bluetooth originelle, le BLE ne permet de transférer qu'une quantité limitée de données à une distance moyenne de 60 mètres. La différence entre les dispositifs Bluetooth et BLE se situe au niveau de la consommation électrique nécessaire à la communication, qui est dix fois moindre pour BLE [15].

VI.2.3 Les technologies de longue portée

- **Réseaux cellulaires mobiles**

Fournis par les opérateurs de télécommunication, les réseaux cellulaires mobiles**,** basés sur la technologie GSM, permettent de transférer une quantité importante de données à une

longue portée. Ils nécessitent l'installation d'une carte SIM dans l'appareil à connecter, afin d'identifier celui-ci sur le réseau de communication [15].

- **Réseaux radio bas-débit**

SigFox : c'est un réseau de communication radio sans fil à bas débit et à basse fréquence, d'une portée moyenne de 10 kilomètres en milieu urbain et de 30 à 50 kilomètres en milieu rural. Ce réseau convient à des appareils à basse consommation, dotés ainsi d'une grande autonomie, qui transfèrent une faible quantité de données [15].

LoRa : c'est un protocole de communication radio à très basse consommation, qui permet de transmettre des données en petite quantité, à des distances de 2 à 5 kilomètres en ville et jusqu'à 45 kilomètres en milieu urbain. À l'instar de SigFox, il s'agit d'un dispositif qui convient particulièrement aux équipements peu énergivores n'émettant que périodiquement, notamment les capteurs [15].

Le tableau suivant résume quelques caractéristiques techniques des différentes technologies citées en haut :

	Courte portée			**Moyenne portée**		**Longue portée**	
Technologies	**NFC**	**Bluetooth**	**Zigbee**	**Wi-Fi**	**BLE**	**SigFox**	**LoRa**
Portée moyenne (en intérieur)	<10 cm	10 m	100 m	100 m	60 m	>2 km	>2km
Débit (Mbit/s)	1.10^{-3}	1.10^{-3}	1.10^{-2}	1.10^{2}	1.10^{-3}	1.10^{-3}	1.10^{-3}
Fréquence	2.4 GHZ	2.4 GHZ	2.4 GHZ	2.4 GHZ 5 GHZ	2.4 GHZ	868 GHZ	868 GHZ
Usages	Téléphonie, carte de paiement	Périphériques informatiques et multimédia	Domotique	Navigation Internet. Transfert conséquent de données.	Périphériques informatiques et multimédia	Prévention d'incidents. Collecte de données. Gestion de réseaux.	

Tableau 3: Quelques caractéristiques techniques des différentes technologies de l'IdO [50]

VI.3 Protocoles

De nombreuses normes IoT sont proposées pour faciliter et simplifier les tâches des programmeurs d'applications et des fournisseurs de services. L'IoT ambitionne de faire communiquer chaque système avec tous les autres au moyen de protocoles communs [2].

CoAP (Constrained Application Protocol) :C'est un protocole de couche d'application pour les applications IoT. Il définit un protocole de transfert Web basé sur les fonctionnalités HTTP, est lié à UDP (et non TCP) par défaut qui le rend plus approprié pour les applications IoT. En outre, CoAP modifie certaines fonctionnalités HTTP pour répondre aux exigences de l'IoT telles que la faible consommation d'énergie et le fonctionnement en présence de liens à perte et bruyants [10].

MQTT (Message Queue Telemetry Transport) : Représente un protocole de messagerie idéal pour les communications IoT et M2M. Il vise à connecter des périphériques et des réseaux intégrés aux applications et au middleware. Il convient aux périphériques à ressources limitées qui utilisent des liens peu fiables ou à faible bande passante. MQTT est construit en haut du protocole TCP. Il se compose de trois composants, abonnés, éditeurs et courtiers. De nombreuses applications utilisent MQTT telles que les soins de santé, la surveillance, le compteur d´énergie. Par conséquent, le protocole MQTT permet d'acheminer les périphériques de petite taille, à faible consommation et à faible mémoire dans des zones vulnérables et réseaux à faible bande passante [7][10].

XMPP (Protocole de messagerie et de présence extensible) : XMPP est une norme de messagerie instantanée (IM) qui est utilisée pour les conversations multipartis, les appels vocaux et vidéo et la télé-présence. Il permet aux utilisateurs de communiquer entre eux en envoyant des messages instantanés sur Internet quel que soit le système d'exploitation qu'ils utilisent. XMPP permet aux applications de messagerie instantanée d'accéder à l'authentification, au contrôle d'accès, à la mesure de la confidentialité, au cryptage hop-by-hop et à la compatibilité avec d'autres protocoles.

Beaucoup de fonctionnalités XMPP en font un des protocoles préférés par la plupart des applications de messageries instantanées et pertinentes dans le cadre de l'IoT. Il fonctionne sur une variété de plateformes basées sur Internet de manière décentralisée. XMPP est sécurisé et permet d'ajouter de nouvelles applications au-dessus des protocoles de base [10].

VII. Contraintes techniques de l'IdO

L'évolution d'internet vers l'Internet des Objets se fait grâce à l'intégration des systèmes complexes, des objets communicants, localisables et mobiles les rendent de plus en plus autonomes. Ceci indique que l'IoT va fournir des bases pour lancer bientôt une nouvelle phase technologique (estimé en 2020), qui exposera de nouveaux moyens et d'opportunités dans notre vie quotidienne. En raison de ses vastes applications, l'IoT a été ciblé et de nouvelles idées ont été proposées à cet égard par de nombreux chercheurs au cours de ces dernières années. Cette section analyse les contraintes techniques liées à la normalisation, limitations matérielles, problèmes de middleware, gestion de base de données, problèmes de sécurité et de confidentialité décrits ci-dessous [16] :

A. Problème d'adressage et de détection

Dans l'IdO, chaque objet en environnement temps réel, est une chose vivante ou non-vivante, devait être adressée par une identité unique. Plusieurs chercheurs ont analysé et détecté les problèmes dans la perspective de l'IdO tels qu'adaptation IPv6. En utilisant les réseaux de capteurs, il est évident d'avoir un grand nombre de nœuds qui doivent être adressable séparément. D'autre part, le problème est le nombre d'objets qui est beaucoup plus grand que le schéma d'adressage IPv4.

Les estimations futures prédisent que le nombre d'appareils ou d'objets augmentera au lieu de diminuer. B.Stockebrand [52] a affirmé qu'IPv4 était déjà en infériorité numérique et toutes les adresses IP étaient occupées. Par conséquent, IPv6 a été défini par le moyen de 128 bits qui remplira les demandes d'adresses IP en constante augmentation.

B. Problème de mise en réseau

En réseau, les protocoles jouent un rôle critique pour la connexion et transformation de données. Le protocole réseau agit en tant que pilier d'acheminement des données entre le monde extérieur et les capteurs. L'Internet actuelle utilise le protocole TCP pour la transmission des données, ce qui n'est pas réalisable pour l'IdO en raison de ses limites. Il y a beaucoup de protocoles existants en fonction des différents critères pour les réseaux mobiles, mais tous ont des inconvénients qui les rendent impraticables pour l'IdO. Alors il existe un besoin de protocole pour une gestion efficace en traitement des données. Plusieurs chercheurs ont analysé les principaux problèmes liés au protocole TCP, qu'on peut classer comme suit :

1) Configuration de la connexion: Le protocole TCP crée une connexion d'abord avant toute transmission de données. Il faut beaucoup de temps pour créer cette connexion. Il semble que c'est un gaspillage de temps inutile dans le cas de l'IdO parce que la quantité de données et le temps de connexion sont très courts. De plus, une connexion est créée entre deux terminaux dont l'énergie est très limitée, donc ce n'est pas faisable.

2) Contrôle de congestion: Le protocole TCP est responsable d'effectuer un contrôle de congestion sur les deux terminaux pendant la transmission des données, ce qui n'est pas réalisable dans le cas de l'IdO en raison de sa nature hétérogène. La plupart du temps, les données qui doivent être transférées sont de petite taille et le contrôle de la congestion dans ce cas est une surcharge. De plus, la communication se fait entre différents types de réseaux et de supports sans fil, le contrôle de la congestion dans ce scénario diminuera les performances. Ainsi, le contrôle de congestion TCP avec son état existant est peu pratique dans la perception de l'IdO.

3) Mise en mémoire tampon des données: Le protocole TCP stocke les données à la fois dans les terminaux pour assurer la transmission sécurisée des données. Par la suite, en cas de dommage ou de perte au cours de la transmission des données, ces données peuvent être renvoyées, ce qui nécessite des tampons sur les deux terminaux pour stocker les données qui seront très coûteuses en terme de l'énergie et de stockage pour les appareils qui sont petits avec faible capacité de stockage et la durée de vie de la batterie très limitée.

4) Problème de contrôle du trafic et de surcharge: Contrôle du trafic dans L'IdO est une autre tâche difficile liée à la mise en réseau. Il est une transmission facile en termes de contrôle de la circulation quand il est seulement entre les nœuds de capteurs dans le réseau sans fil. Mais il devient compliqué lorsque les capteurs font partie de l'ensemble du réseau ayant des buts hétérogènes. En machine à machine (M2M), le contrôle du trafic est totalement différent que la communication homme à machine.

C. Problème de protocole de routage

M2M est une clé facilitateur pour les villes intelligentes. Avec l'avancement des technologies, le M2M nécessitera le routage des données en raison de la nécessité de débits de données élevés. C'est une clé défi de créer un protocole de routage fiable ayant une haute vitesse de transmission et délai de livraison réduit.

D. Problème de normalisation

Le nombre d'articles dans l'IdO est extrêmement élevé. Par conséquent, les problèmes liés à la représentation de l'information, au stockage d'informations, interconnexions, recherche et organisation des informations produites par l'IdO deviendront très difficiles. Dans l'Internet actuelle, les domaines d'application sont distincts, ce qui rend les domaines commerciaux séparés et donc l'objectif de l'IdO n'est pas atteint. Ainsi, il y a un besoin de techniques de normalisation pour joindre tous les domaines d'applications séparées de manière sophistiquée.

W. Pollard [29] souligne que dans le scénario de communication M2M, les techniques de normalisation fournissent un middleware pour gérer les mécanismes de communication, gestion des appareils et accessibilité entre les terminaux d'extrémité.

E. Problèmes de logiciel et d'algorithme :

Il existe un besoin de logiciel commun (en termes de nouveaux protocoles) et des algorithmes pour fournir une base de middleware indépendante des ressources et de la fonction de réseau pour la connectivité dans différents environnements. De nouveaux microsystèmes d'exploitation permettant de fonctionner efficacement pour les petits appareils en termes d'énergie et puissance.

F. Contrainte d'alimentation

Le dispositif IoT est contraint par l'entité qui est en état de surveillance physique et la position de l'entité change fréquemment sans accès à un point d'alimentation d'énergie [7]. La plupart des appareils de l'IdO ont une taille extrêmement réduite et sont non fixées. En raison de leur taille et de leur changement fréquent d'emplacement, les périphériques des utilisateurs ne sont pas en mesure d'accéder à un point d'alimentation tout le temps. La faible consommation d'énergie est donc la contrainte universelle de l'IdO. Ils utilisent des technologies de batterie ou ils peuvent utiliser certaines techniques pour prendre le pouvoir de leur environnement en utilisant d'autres appareils. Des scientifiques ont annoncés la création d'un nano générateur sur le plan commercial, il s'agit d'une puce flexible capable de générer de l'électricité à partir de mouvement corporels.

G. Problème lié à l'architecture et à la relation réseau

Dans la perspective IoT, on ne s'attend pas à ce que les appareils tiennent leurs positions. Cependant, la connectivité fiable demande à traiter et à détecter les appareils tout le

temps. Le nombre de nœuds mobiles à adresse énorme dans le réseau est également considéré comme un problème majeur d'évolutivité.

Des chercheurs ont analysé la nécessité de traiter le problème d'architecture et de gestion de la relation réseau. Ils ont souligné la nécessité de construire une architecture avec de tels mécanisme efficace qui peut découvrir toutes les ressources du capteur et peut enregistrer et mettre à jour de nouveaux systèmes de détection dans un réseau plus large.

H. Problème matériel

Le domaine des nanotechnologies a beaucoup évolué ces dernières années, mais certains logiciels sont encore très volumineux pour pourvoir fonctionner dans ce domaine (dans la perspective de l'IoT), par exemple, Linux avec toutes ses fonctionnalités. En outre, le problème matériel lié à l'alimentation et aux contraintes de stockage doit également être géré.

J. Problème de congestion et de surcharge

Un problème d'encombrement survient lorsque des messages simultanés venus de plusieurs appareils conduit finalement à l'extrême situation de surcharge qui provoque un effet énorme sur le réseau, ce qui affecte les performances du réseau et conduit à un échec sur le réseau. Cette situation est visible dans M2M et V2V communication. La congestion peut également être due au serveur ou dysfonctionnement de l'application. Une solution à ce contrôle de congestion est pour spécifier la durée de la connexion. Les appareils peuvent seulement se connecter au réseau quand il n'y a pas de surcharge et si le réseau est surchargé, désactiver toutes les autres connexions. La deuxième solution consiste à refuser la connexion de périphériques qui créent un problème de congestion.

K. Sécurité et confidentialité (problème de transfert de données)

La sécurité et la confidentialité sont l'un des obstacles les plus importants à l'IoT. Comme la sécurité et la vie privée sont des domaines de recherche séparés mais collaborent indirectement avec des contraintes techniques donc ils ne se concentrent pas dessus mais au lieu de cela, ils fournissent juste l'idée principale. Techniquement, l'IdO ne sera applicable que si au moins que les gens l'acceptent. Et cette acceptation est corrélée à la garantie de leur sécurité et confidentialité. Le futur Internet n'affectera pas seulement les utilisateurs de l'Internet des objets mais même les non-utilisateurs seront également ciblés.

La confidentialité et la sécurité ne peuvent être garanties que si un utilisateur a pleinement le contrôle de ses informations. Un utilisateur doit savoir que les données

personnelles sont collectées, qui les collectent, où elles se trouvent, traitées et quand il a été collectées. En outre, les données personnelles ne doivent être utilisées que par des services agréés par exemple, autoriser les organisations médicales, autoriser les instituts de recherche, autoriser les systèmes de gestion, etc.

VIII. Problématique

L'Internet des Objets (IdO) prend depuis quelque temps une ampleur de plus en plus importante. Il concerne, avec des frontières plus ou moins floues, la mise en connectivité massive d'objets, tel que des capteurs, téléphones, ou plus généralement d'objets du quotidien auparavant déconnectés (serrure, climatiseur, etc.).

L'utilisation de l'IdO permet le développement de plusieurs applications intelligentes qui touchent plusieurs domaines tels que : la santé, l'agriculture, les villes intelligentes, les maisons intelligentes, le transport…etc. Cependant, il ouvre la voie afin de prendre en considération plusieurs aspects avant le déploiement de cette technologie. L'un des aspects les plus importants est la sécurité et le respect de la vie privée des utilisateurs. Donc :

- Comment assurer la sécurité matérielle et logicielle des objets connectés ?
- Comment assurer la confidentialité de la vie privée des utilisateurs ?
- Comment assurer l'intégrité des données et leurs disponibilités ?
- Comment sécuriser les communications entre deux objets communicants ?

IX. Exemple d'un IdO : Réseaux de capteurs sans fils (RCSfs)

Pour avoir un **« Internet des Objets »,** nous avons besoin de plusieurs éléments : des capteurs**,** des protocoles permettant d'échanger des données entre capteurs et des moyens d'optimiser le traitement des données suivant diverses contraintes (environnementales, techniques, sécurité, etc.…).

Pour créer et harmoniser tout cela, les chercheurs rédigent beaucoup de papiers autour des réseaux de capteurs sans fil. Ces réseaux de capteurs sont au cœur même de l'Internet des Objets. Il s'agit comme son nom l'indique de réseaux formés par un grand nombre de **« nœuds »** tous équipés de capteurs permettant de détecter un phénomène particulier (lumière, température, pression…etc.). Comparé aux solutions utilisant des câbles, le réseau de capteurs présente plusieurs avantages : déploiement plus rapide, coût moindre, plus de flexibilité [7].

IX.1 Architecture d'un RCSF

Un **RCSF** est composé d'un ensemble de nœuds capteurs. Ces nœuds capteurs sont organisés en champs «sensorfields» (Figure 5). Chacun de ces nœuds a la capacité de collecter des données et de les transférer au nœud passerelle (dit **"sink"** en anglais ou **puits**) par l'intermédiaire d'une architecture multi-sauts. Le puits transmet ensuite ces données par Internet ou par satellite à l'ordinateur central «Gestionnaire de taches» pour analyser ces données et prendre des décisions [8].

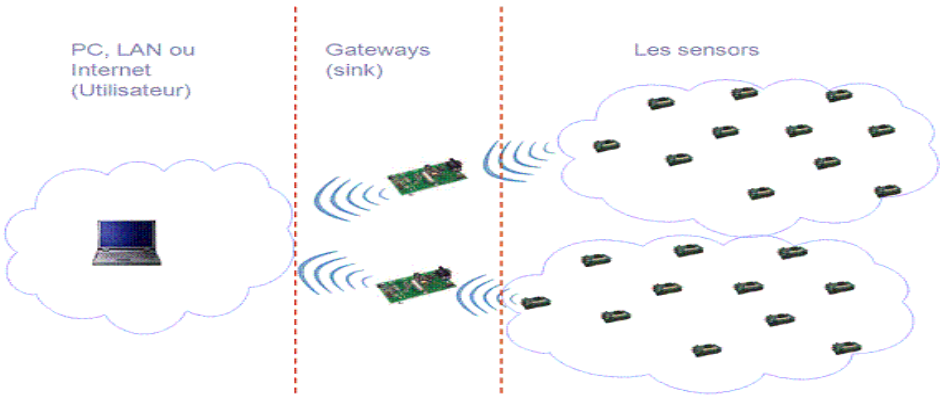

Figure 5:Architecture d'un RCSF.

IX.2 Anatomie d'un capteur

Un nœud capteur (dit **"mote"** en anglais) est composé principalement d'un processeur, une mémoire, un émetteur/récepteur radio, un ensemble de capteurs, et une pile (i.e., source d'énergie) (voir la figure 6). Il existe plusieurs modèles commercialisés dans le marché. Parmi les plus célèbres, les "mote" MICAx et TelosB de Crossbow [8]. .

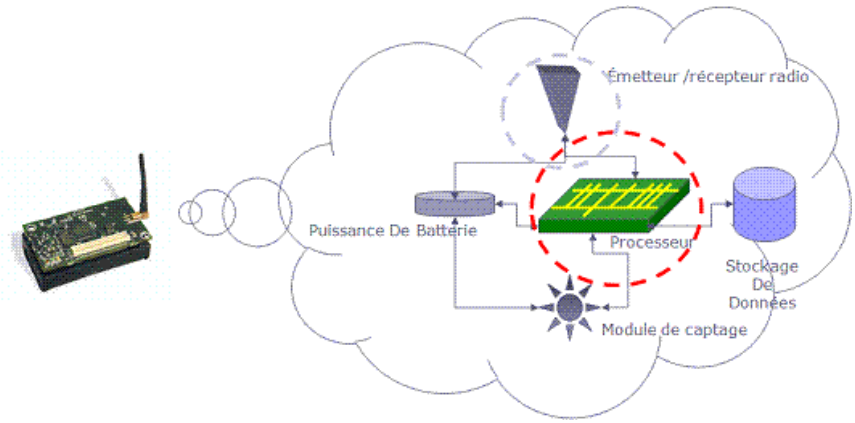

Figure 6:Anatomie d'un capteur

Les caractéristiques techniques de quelques nœuds capteurs sans fil sont représentées dans le tableau suivant [35]:

Nœud capteur	MicaZ	TelosB	WSN430
Processeur	Atmega128L	TI MSP 430	TI MSP 430
Vitesse de processeur	16 MHZ	8 MHZ	8 MHZ
Taille RAM	4 KO	10 KO	10 KO
Espace programme	128 KO	48 KO	48 KO
Radio	TI CC2420 IEEE 802.15.4		TI CC 1100
Fréquence	2400-2483	315/433/686/915	
Voltage(Batterie)	2.7 V	1.8V - 3.6 V	3.7 V

Tableau 4: Caractéristiques techniques de quelques nœuds capteurs sans fil [35]

IX.3 Contraintes de conception des RCSFs

Les principaux facteurs et contraintes influençant l'architecture des réseaux de capteurs peuvent être résumés comme suit [8]:

- ✓ **La tolérance aux fautes :** Certain nœuds peuvent générer des erreurs ou ne plus fonctionner à cause d'un manque d'énergie, un problème physique ou une interférence. Ces problèmes n'affectent pas le reste du réseau, c'est le principe de la tolérance aux fautes. La tolérance aux fautes est la capacité de maintenir les fonctionnalités du réseau sans interruptions dues à une erreur intervenue sur un ou plusieurs capteurs.
- ✓ **L'échelle :** Le nombre de nœuds déployés pour un projet peut atteindre le million. Un nombre aussi important de nœuds engendre beaucoup de transmissions inter nodales et nécessite que le puits "sink " soit équipé de beaucoup de mémoire pour stocker les informations reçues.
- ✓ **Les coûts de production :** Souvent, les réseaux de capteurs sont composés d'un très grand nombre de nœuds. Le prix d'un nœud est critique afin de pouvoir concurrencer un réseau de surveillance traditionnel. Actuellement un nœud ne coûte souvent pas

beaucoup plus que 1$. A titre de comparaison, un nœud Bluetooth, pourtant déjà connu pour être un système lowcost, revient environ à 10$.

- ✓ **L'environnement :** Les capteurs sont souvent déployés en masse dans des endroits hostiles (exemple : champs de bataille, intérieur de grandes machines, fond d'un océan). Par conséquent, ils doivent pouvoir fonctionner sans surveillance dans des régions géographiques éloignées;
- ✓ **La topologie de réseau :** Le déploiement d'un grand nombre de nœuds nécessite une maintenance de la topologie. Cette maintenance consiste en trois phases : Déploiement, Post-déploiement (les capteurs peuvent bouger, ne plus fonctionner,...), Redéploiement de nœuds additionnels.
- ✓ **Les contraintes matérielles :** La principale contrainte matérielle est la taille du capteur. Les autres contraintes sont la consommation d'énergie qui doit être moindre pour que le réseau survive le plus longtemps possible, qu'il s'adapte aux différents environnements (fortes chaleurs, eau,..), qu'il soit autonome et très résistant vu qu'il est souvent déployé dans des environnements hostiles.
- ✓ **Les médias de transmission :** Dans un réseau de capteurs, les nœuds sont reliés par une architecture sans-fil. Pour permettre des opérations sur ces réseaux dans le monde entier, le média de transmission doit être normé. On utilise le plus souvent l'infrarouge (qui est license-free, robuste aux interférences, et peu onéreux), le Bluetooth et les communications radio ZigBee.
- ✓ **La consommation d'énergie :** Un capteur, de par sa taille, est limité en énergie (<0.5Ah, 1.2V) [51]. Dans la plupart des cas le remplacement de la batterie est impossible. Ce qui veut dire que la durée de vie d'un capteur dépend grandement de la durée de vie de la batterie.

X. Conclusion

Dans ce chapitre nous avons présenté l'IdO, et quelques définitions de ses concepts de base, son évolution et son architecture, puis nous avons abordé ses domaines d'application, son fonctionnement et ses contraintes techniques, et nous avons terminé par la présentation des réseaux de capteurs sans fils.

Le chapitre suivant sera consacré à l'étude des problèmes de sécurité rencontrés dans l'IdO.

Chapitre II : Problèmes de sécurité dans l'Internet des Objets

I. Introduction

« *The National Intelligence Council (NIC)*» américain considère que les avancées technologiques combinées à une forte demande des marchés encourageraient une adoption et un déploiement à large échelle de l'IdO. Néanmoins, la plus grande crainte est que les objets du quotidien deviennent des risques potentiels d'attaque de sécurité. Pire encore, la pénétration à large échelle de l'IdO diffuserait ces menaces d'une façon beaucoup plus large que l'Internet d'aujourd'hui.

En effet, l'ubiquité de l'IdO amplifiera les menaces classiques de sécurité qui pèsent sur les données et les réseaux. Mais en plus, le rapprochement du monde physique et du monde virtuel à travers l'IdO ouvre la voie à de nouvelles menaces qui pèseront directement sur l'intégrité des objets eux-mêmes, et la vie privée des personnes. Dans ce chapitre nous présentons les principales vulnérabilités et attaques présentes dans l'IdO.

II. La différence entre vulnérabilité – menace – risque

II.1 Vulnérabilité

Une vulnérabilité peut aussi être appelée "faille", un "défaut" ou "faiblesse". Une vulnérabilité est une faiblesse du système qui le rend sensible à une menace [16]. Ou bien «Une faiblesse dans un système ou dans sa conception qui permet à un intrus d'exécuter des commandes, d'accéder à des données non autorisées et / ou de mener des attaques par déni de service» [17].

II.2 Menace

Une menace est un danger qui existe dans l'environnement d'un système indépendamment de celui-ci : accident, erreur, malveillance passive si elle porte sur la confidentialité, malveillance active si elle modifie le contenu de l'information ou le comportement des systèmes de traitement [16].

II.3 Risque

Le risque est la probabilité qu'une menace particulière puisse exploiter une vulnérabilité donnée du système. L'écart entre la menace virtuelle et son niveau de protection correspond au risque, accepté ou résiduel [16].

III. Les vulnérabilités de l'IdO

- **Interface web non sécurisée**

Pour exploiter cette vulnérabilité, l'attaquant utilise des informations d'identification faibles ou capture des informations d'identification en texte brut pour accéder à l'interface Web. L'impact entraîne une perte de données, un déni de service et peut conduire à une prise en charge complète de l'appareil. Des pirates informatiques ont exploité une interface Web non sécurisée pour compromettre les routeurs ASUS livrés avec le nom d'utilisateur et le mot de passe par défaut de l'administrateur [19].

- **Service réseau non sécurisé**

Services réseau inutiles ou non sécurisés s'exécutant sur le périphérique lui-même, en particulier ceux exposés à Internet, qui compromettent la confidentialité, l'intégrité, l'authenticité ou la disponibilité des informations ou permettent un contrôle à distance non autorisé.

Les attaquants utilisent des services de réseau vulnérables pour attaquer le périphérique lui-même ou pour faire échec aux attaques du périphérique. Les attaquants peuvent ensuite utiliser les périphériques compromis pour faciliter les attaques sur d'autres périphériques. Cette vulnérabilité a été exploitée par des pirates informatiques qui utilisaient 900 caméras de vidéosurveillance dans le monde pour attaquer un service de plate-forme en nuage [19].

- **Mot de passe faible, devinable ou codé en dur**

Pratiquées par les hackers depuis que les codes d'accès existent, les attaques par force brute consistent à deviner un mot de passe en multipliant les tentatives de connexion à un compte en essayant toutes les combinaisons possibles de caractères pouvant former le mot de passe. C'est une attaque souvent faite hors-ligne car elle nécessite un temps et des capacités de calcul considérables. Il est tout de même possible de réaliser cette attaque à distance sur un service d'authentification disponible sur le réseau mais, dans ce cas précis, les attaquants préfèrent souvent limiter les tentatives à des listes de mots de passe. Il s'agit ici non plus d'une attaque réseau par force brute, mais d'une attaque par dictionnaire. Un exemple concret de l'efficacité d'une telle attaque est le botnet Mirai, ayant infecté des centaines de milliers d'équipements IoT à partir de listes d'identifiants par défaut [43].

- **Manque de mise à jour sécurisées**

Manque de capacité à mettre à jour le périphérique en toute sécurité. Cela inclut le manque de validation du micro logiciel sur le périphérique, le manque de livraison sécurisée (non chiffré en transit), le manque de mécanismes anti-restauration et le manque de notifications des changements de sécurité dus aux mises à jour [19].

Absence de chiffrement et de signature pour les mises à jour des micros logiciels [16].

- **Utilisation des composants non sécurisés ou obsolètes**

Utilisation de composants logiciels / bibliothèques obsolètes ou non sécurisés qui pourraient permettre de compromettre le périphérique. Cela inclut la personnalisation non sécurisée des plates-formes de système d'exploitation et l'utilisation de logiciels ou de composants matériels tiers à partir d'une chaîne d'approvisionnement compromise [20].

- **Protection insuffisante de la vie privée**

Les informations personnelles de l'utilisateur stockées sur l'appareil ou dans l'écosystème qui sont utilisées de manière non sécurisée, incorrecte ou sans autorisation.

Cette vulnérabilité provoque un manque de confidentialité [20] : Les pirates informatiques utilisent différents vecteurs pour afficher et / ou collecter des données personnelles qui ne sont pas correctement protégées. L'impact de cette attaque est la collecte de données utilisateur personnelles. Cette vulnérabilité a été illustrée par le piratage de VTech qui permettait aux pirates de voler les données personnelles des parents ainsi que celles des enfants utilisant la tablette de VTech [19].

- **Transfert et stockage de données**

Manque de cryptage ou de contrôle d'accès aux données sensibles n'importe où dans l'écosystème, y compris au repos, en transit ou pendant le traitement [20].

Cryptage des données au repos et en transit entre les périphériques de pointe IoT et les systèmes principaux à l'aide d'algorithmes cryptographiques standards, contribuant ainsi au maintien de l'intégrité des données et empêchant le piratage des données. La large gamme de périphériques IoT et de profils matériels limite la possibilité de disposer de processus et de protocoles de chiffrement standard. En outre, tout le cryptage IoT doit être accompagné de processus équivalents de gestion du cycle de vie des clés de cryptage complet, car une mauvaise gestion des clés réduira la sécurité globale [44].

- **Manque de durcissement physique**

Manque de mesures de durcissement physique (manque de processus destinés à sécuriser un système), permettant aux attaquants potentiels d'obtenir des informations sensibles qui pourraient être utiles lors d'une future attaque à distance ou prendre le contrôle local du périphérique [20].

- **Présence des interfaces de débogage**

Possibilité de prendre le contrôle des composants matériels de l'objet [16]. Les plateformes de développement extrêmement flexibles offrent une haute accessibilité aux composants et utilisent des connectivités très répandues comme l'USB. Elles permettent également un débogage sur carte avec une interface JTAG. Autant toutes ces capacités de connexion peuvent faciliter le développement d'une conception IoT autant elles rendent vulnérable la technologie aux attaques des hackers [45].

- **Sécurité mobile médiocre**

Une sécurité mobile médiocre dans les systèmes IoT le rend plus vulnérable et plus risqué. Les données sont stockées de manière non sécurisée dans les appareils mobiles. Cependant, les appareils IOs sont plus sécurisés que les appareils Android. Si un utilisateur perd son Smartphone et que ses données ne sont pas sauvegardées, il va perdre ses données et il ne pourra pas les récupérer [21].

- **Authentification / autorisation insuffisante**

L'exploitation de cette vulnérabilité implique que l'attaquant se force brutalement à forcer des mots de passe faibles ou des identifiants peu protégés pour accéder à une interface particulière. L'impact de ce type d'attaque est généralement un déni de service et peut également compromettre l'appareil. Des pirates éthiques ont exploité cette vulnérabilité pour accéder à l'unité principale de Jeep Cherokee via une connexion WiFi. Le mot de passe WiFi de l'unité Jeep Cherokee est généré automatiquement en fonction du moment où la voiture et l'unité principale sont démarrées. En devinant le temps et en utilisant des techniques de force brute, les pirates ont pu accéder à l'unité principale.

Notons que si ces vulnérabilités offrent aux attaquants la possibilité de manipuler un objet connecté et ses données, la compromission des serveurs d'appui permet souvent le contrôle de toutes les solutions connectées déployées par un constructeur [19].

IV. Les attaques dans l'IdO

IV.1 Menaces sur les données et les réseaux

Le manque de surveillance et de protection physique des objets communicants peut engendrer des attaques potentielles portées sur le matériel telles que le vol, la corruption ou la contre façon de ces derniers pour la récupération des données qui sont stockées sur ces dispositifs ou pour interrompre le bon fonctionnement des réseaux ou les systèmes complexes qui les hébergent. De plus, les transmissions sans fil sont réputées par leur forte vulnérabilité aux attaques de l'écoute passive, mais aussi les attaques actives [14].

IV.1.1 Attaques passives

Elles consistent à écouter sans autorisation et sans modifier les données ou le fonctionnement du réseau. Elles sont généralement indétectables car elles n'impliquent aucune modification dans les données ou les ressources système. Mais une prévention est possible [21]. Typiquement les données sont envoyées et reçues de façon apparemment normale et ni l'émetteur ni le récepteur ne sont conscients qu'un tiers a lu les messages ou a analysé le trafic. Il existe deux types d'attaques passives [22]:

- **Lecture du message :** Les données sont envoyées en claire (conversation téléphoniques, emails, fichier, etc.).Ces données peuvent contenir des informations sensibles ou confidentielles pour empêcher la lecture des messages, on peut utiliser le cryptage.
- **Analyse du trafic :** Si les messages sont illisibles, l'adversaire ne peut pas les lire mais peut analyser le trafic, l'adversaire peut déterminer l'emplacement et l'identité des hôtes de la communication et peut observer la fréquence et la longueur des messages échangés. Ces informations peuvent être utiles à deviner la nature de la communication qui se déroule.

IV.1.2 Attaques actives

Elles consistent à modifier des données ou des messages, à s'introduire dans des équipements réseau ou à perturber le bon fonctionnement de ce réseau. Noter qu'une attaque active peut être exécutée sans la capacité d'écoute. De plus, il n'y a généralement pas de prévention possible pour ces attaques, bien qu'elles soient détectables [21].

- **Usurpation d'identité (spoofing) :** Consiste à se faire passer pour quelqu'un d'autre, parmi les exemples d'usurpation, on trouve [22] :

- **Usurpation de l'adresse IP (IP spoofing) :** Est une technique consistant à remplacer l'adresse IP de l'expéditeur par l'adresse IP d'une autre machine. Cette technique permet ainsi à un attaquant d'envoyer des paquets anonymement.
- **Usurpation de l'adresse e-mail :** Lors de la réception d'un courrier électronique, nous pouvons lire l'adresse de l'expéditeur mais il est possible de changer l'adresse. Ainsi, un attaquant peut envoyer un mail en usurpant l'adresse d'un autre utilisateur.

- **Rejeu (Replay) :** Cette attaque est réalisée en deux phases : la capture passive d'un message et la retransmission ultérieure de ce message pour produire un effet non autorisé. Exemple : Rejeu d'une transaction bancaire dont l'attaquant est bénéficiaire. Le principe est très simple. Il suffit juste qu'un attaquant rejoue un ancien message plusieurs fois dans le réseau. Cependant, l'impact pourrait être assez négatif, comme cet acte peut entraîner des fausses alertes ou alors, empêcher le signalement d'une urgence. La situation risque d'être encore plus grave si l'attaque est effectuée par un attaquant interne (un nœud de compromission) car elle sera difficile à détecter.
- **Modification des messages :** Cette attaque implique la modification du contenu du message original, ou que les messages sont retardés ou réordonnés pour produire un effet non autorisé.
- **DOS (Denial Of Service):** Ce type d'attaque est une tentative de rendre une machine ou une ressource réseau indisponible pour les utilisateurs auxquels elle est destinée. En raison de capacités mémoire insuffisantes et de ressources de calcul limitées, la majorité des périphériques dans l'IoT sont vulnérables aux attaques d'environnement [23].
- **Man in the middle :**

Le concept de Man-in-the-Middle (MITM) désigne une attaque menée par un pirate informatique qui cherche à interrompre et intercepter une communication entre deux systèmes distincts. Ce type d'attaque peut être dangereux, car le pirate informatique intercepte discrètement les messages entre deux parties pour les retransmettre, alors qu'elles pensent communiquer directement entre elles. En possession du message d'origine, l'attaquant est en mesure de piéger le destinataire en lui faisant croire que le message qu'il reçoit est légitime. De nombreux cas d'attaques

MITM ont déjà été signalés, comme le piratage de véhicules et de réfrigérateurs intelligents.

Du fait de la nature des « objets » piratés, ces attaques peuvent être extrêmement dangereuses dans l'IoT. Elles peuvent notamment viser des outils et équipements industriels, des véhicules ou des objets connectés inoffensifs comme des téléviseurs connectés ou des systèmes d'ouverture de portail automatique [18].

Le tableau suivant résume les différentes attaques citées ci-dessus :

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 et contrôler la conversation. -Ecouter, modifier ou supprimer des données.	-Intégrité. -Confidentialité.	Active
L'usurpation d'identité	-Vol d'identité.	-Confidentialité. -Authentification.	Active
Lecture du message	-Ecouter et lire les données envoyées entre deux entités.	-Confidentialité.	Passive
Analyse du trafic	-Analyse des informations concernant les données transmises.	-Confidentialité.	Passive
Rejeu	-Ecouter, modifier ou supprimer des données.	-Intégrité. -Confidentialité. -Disponibilité.	Active
Modification des messages	- Modifier, retarder, réordonner des données.	-Intégrité. -Disponibilité.	Active

Tableau 5: Les types d'attaques dans l'IdO

IV.2 Menaces sur les systèmes et l'environnement physique des objets

L'attaquant peut entreprendre d'attaquer directement le matériel (attaque physique), ou bien de compromettre un objet connecté en lui injectant un code malveillant (attaque logicielle) [14].

IV.2.1 Les attaques physiques

Ces types d'attaques altèrent les composants matériels et elles sont relativement difficiles à exécuter car ils nécessitent un matériel coûteux. En raison de la nature sans surveillance et distribuée de l'IdO, la plupart des appareils fonctionnent généralement dans des environnements extérieurs, qui sont très susceptibles aux attaques physiques [23].

Les principales attaques ciblant le matériel et les composants des systèmes IoT sont décrites plus en détail ci-dessous :

- **Attaques par réplication d'objets :** Un attaquant, dans ce type d'attaque, a la capacité d'ajouter physiquement un nouvel objet au réseau. Par exemple, un objet malveillant pourrait être ajouté par identification de l'objet en cours de réplication. Une telle attaque, donc, pourrait entraîner une baisse considérable des performances du réseau. En addition, risque de dégradation des performances, de corruption ou d'orientation erronée, les paquets reçus peuvent facilement être remplis par l'objet malveillant, permettant à l'attaquant d'avoir accès à des données et extraire les clés secrètes [24].
- **Interférences RF sur RFID (brouillage):** Envoi d'un grand nombre de signaux de bruit sur les fréquences radio, qui sont principalement utilisés pour la communication RFID, est le principal objectif de ce type d'attaque [24].

  La couche physique est très sensible aux attaques qui exploitent l'accessibilité du support de transmission pour intercepter les communications ou pour causer des problèmes plus graves comme, le brouillage qu'un attaquant puisse provoquer en envoyant des signaux parasites qui interfèrent avec les fréquences radio qu'utilisent les nœuds capteurs pour la communication. Si l'attaquant est assez puissant, ou encore s'il utilise plusieurs nœuds à faibles puissances, la perturbation de communication peut s'étaler sur tout le réseau [46].
- **Falsification d'objets:** La possibilité d'accéder à des objets IoT physiquement par les attaquants est très élevée en raison que certains objets IoT peuvent être déployés dans des environnements hostiles. Par conséquent, ces objets sont vulnérables aux

attaques matérielles, les plus notables sont l'extraction de clés cryptographiques, la modification du système d'exploitation ou du micro-logiciel, et le circuit modification. Le remplacement du thermostat Nest avec un malicieux est un exemple de telles attaques [24].

- **Ingénierie sociale:** Les auteurs montrent qu'une attaque d'ingénierie peut être considérée comme une attaque physique, car un attaquant pourrait modifier physiquement les utilisateurs du système IoT afin d'obtenir leurs données sensibles [24]. L'arme privilégiée des attaques par ingénierie sociale est bien souvent l'e-mail de phishing qui pousse un utilisateur à donner des informations ou le rediriger vers des sites bancaires ou d'e-commerce qui, malgré une apparente légitime, sont en fait usurpés. Le but est d'inciter un utilisateur à saisir ses informations de paiement [25].

- **Injection de nœud malveillant:** Pour obtenir un accès non autorisé sur un réseau IoT, l'attaquant pourrait insérer un objet malveillant parmi les légitimes du réseau. En conséquence, il pourrait accéder à n'importe quel objet, insérer de fausses données pour gêner les messages livraison, et peut-être contrôler l'ensemble du réseau. Ceci est également connu sous le nom de Man in The Middle Attack [24].

- **Attaque de privation de sommeil :** La plupart des nœuds de capteurs du système IoT sont alimentés par des batteries non remplaçables et sont programmés pour suivre des routines de sommeil afin de prolonger leur durée de vie. Cette attaque maintient les nœuds en fonction, ce qui entraînera une consommation électrique accrue et entraînera leur fermeture [26].

IV.2.2 Les attaques logicielles

Les attaques logicielles constituent la principale source de vulnérabilité en matière de sécurité dans tout système informatisé. Les attaques logicielles exploitent le système en utilisant des programmes de cheval de Troie, des vers, des virus, des logiciels espions et des scripts malveillants qui peuvent voler des informations, altérer des données, nier le service et même endommager les périphériques d'un système IoT [26].

- **Les botnets :**

Un botnet est un réseau de systèmes associés entre eux dans le but de prendre le contrôle à distance et de diffuser des logiciels malveillants (malware). Contrôlés par des opérateurs de botnets via des serveurs C&C (Commande et Contrôle), ils sont utilisés à grande échelle par des cybers malfaiteurs pour commettre plusieurs types de forfaits : vol de

données confidentielles, exploitation de données bancaires en ligne, attaques par DDoS (Déni de service distribué)ou encore pourriels et hameçonnage (e-mails d'arnaques de type Phishing) [18].

- **Injection de code malveillant:** Dans ce type d'attaque, un attaquant injecte un code malveillant dans certains paquets pour voler ou modifier des données sensibles [24].
- **Malware:** Un processus d'infection des applications Web avec un programme malveillant s'appelle un malware. Récemment, un grand nombre de logiciels malveillants ont été conçus pour attaquer les applications de l'Internet des Objets [24].
- **Déni de service distribué (DDoS):** L'un des principaux techniques qui peuvent être utilisées pour établir une attaque DDoS est un botnet. Un exemple de cette attaque est la prévention d'accès à une ressource en l'inondant de tant de demandes [24].
- **Attaque de hameçonnage (Phishing):** Un attaquant pourrait avoir accès aux données confidentielles telles que : mots de passe, crédits cartes et autres données sensibles via le piratage d'un email, de téléphones, ou les médias sociaux [24].
- **Backdoors:** Avec l'avènement de la vision IoT, beaucoup de développeurs ont proposé différents systèmes d'exploitation IoT comme RTOS et Contik. Ces systèmes d'exploitation peuvent contenir une porte dérobée qu'ils pourraient reprogrammer pour avoir un accès à des données sensibles à tout moment [24].
- **Virus, vers, cheval de Troie, logiciels espions et logiciels malveillants:**

  De nos jours, l'homme virus et vers, comme Mirai, Stuxnet et Brickerbot, ont été conçus pour attaquer certaines faiblesses telles que le manque de mécanismes de mise à jour trouvé dans les objets IoT [24].

  Un adversaire peut endommager le système en utilisant un code malveillant. Ces codes se propagent via des pièces jointes, le téléchargement de fichiers depuis Internet. Le ver a la capacité de se répliquer sans aucune action humaine [27].

  Les logiciels espions ou cheval de Troie infectent silencieusement l'ordinateur grâce à une application en apparence légitime. Une fois dans l'ordinateur, le logiciel peut faire ce qu'il veut : enregistrer les mots de passe ou accéder à la caméra pour enregistrer les moindres faits et gestes de l'utilisateur [28].
- **Attaque à la recherche par force brute:** Ce type d'attaque a été conçu pour pirater un système IoT en cassant sa sécurité par des mécanismes tels que la cryptographie et l'authentification à l'aide différentes techniques [24].

IV.3 Menaces sur la vie privée

La protection de la vie privée dans l'IdO est devenue de plus en plus difficile en raison de grands volumes d'informations facilement disponibles via des mécanismes d'accès distant. Les attaques les plus courantes contre la vie privée des utilisateurs sont [23] :

- **Data mining:** Permet aux attaquants de découvrir des informations qui ne sont pas anticipées dans certaines bases de données.
- **Cyber espionnage:** Utilisation de techniques de piratage et de logiciels malveillants pour espionner ou obtenir des informations secrètes d'individus, d'organisations ou du gouvernement.
- **Eavesdropping (écoute clandestin) :** Ecouter une conversation entre deux parties.
- **Tracking (le suivi):** Les mouvements des utilisateurs peuvent être suivis par le numéro d'identification unique (UID). Le suivi de la localisation d'un utilisateur facilite l'identification du thème dans les situations dans lesquelles il souhaite rester anonyme.
- **Attaques basées sur un mot de passe:** Des intrus tentent de dupliquer un mot de passe d'utilisateur valide. Cette tentative peut être faite de deux manières différentes:
    - **Attaque par dictionnaire** : Essayer des combinaisons possibles de lettres et de chiffres pour deviner les mots de passe des utilisateurs.
    - **Attaques par force brute** : Utilisation d'outils de piratage pour essayer toutes les combinaisons possibles de mots de passe afin de découvrir des mots de passe valides.

X. Conclusion

Dans ce chapitre nous avons vu les différentes vulnérabilités et menaces que présente l'IdO sur les données et les réseaux, les systèmes et l'environnement physique des objets, et la vie privée. Le prochain chapitre sera consacré à une étude complète sur les solutions proposées.

Chapitre III : Les différentes solutions proposées pour l’Internet des Objets

I. Introduction

L'Internet des Objets est composé de diverses technologies qui prennent en charge des services avancés dans différents domaines d'application. La sécurité et la confidentialité sont des aspects très importants pour les domaines d'applications IoT. Ces applications nécessitent la confidentialité, l'authenticité, l'intégrité et le contrôle d'accès des données au sein du réseau IoT. Pour les utilisateurs et les objets, la sécurité est obtenue en appliquant les politiques de sécurité et de confidentialité. En raison des normes différentes et des piles de communication impliquées dans les solutions de sécurité traditionnelles, il ne peut pas être directement appliqué aux technologies IoT. En ce qui concerne l'IoT, le nombre de périphériques interconnectés devrait augmenter considérablement, de sorte que l'évolutivité est le principal défi du développement IoT.

Un besoin immédiat est le développement de mécanismes de sécurité efficaces pour l'informatique embarquée miniaturisée. Les développements actuels des réseaux de capteurs, actionneurs, de la technologie RFID et de l'informatique mobile montrent les limites des dispositifs qui constitueront l'IdO en termes de ressources et capacités. Plusieurs chercheurs évoquent la nécessité de vérifier l'applicabilité de la cryptographie moderne dans le contexte de l'IdO. En effet, les limitations de ressources et les capacités des objets embarqués miniaturisés rendent difficile l'utilisation des algorithmes cryptographiques actuels en raison de leur consommation en termes de calcul et de mémoire.

Plusieurs travaux de recherche ont montré que la cryptographie à base de courbes elliptiques [42] offrait un niveau de robustesse de la sécurité semblable à la cryptographie asymétrique classique avec l'avantage d'être peu coûteuse en termes de ressources (Mémoire, calcul, bande passante). Dans ce chapitre nous allons présenter les mesures de sécurité à mettre en œuvre et les protocoles de sécurité applicables dans l'IdO.

II. La sécurité dans l'Internet des Objets

II.1. Définition

La sécurité informatique est l'ensemble des moyens techniques qui visent à empêcher l'utilisation non autorisée des ressources matérielles ou logicielles. On peut dire aussi que la sécurité informatique est un ensemble des moyens mis en œuvres pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles [6].

II.2. Exigences de la sécurité

Lorsque nous abordons le problème de sécurité, nous visons à atteindre certains objectifs. Les objectifs de sécurité sont classés comme principaux et secondaires.

Les principaux objectifs sont connus comme objectifs standards de sécurité tel que : la confidentialité, l'authentification, l'intégrité et la disponibilité. Les objectifs secondaires sont : la fraicheur de données, la non-répudiation, le contrôle d'accès, l'auto-organisation, la synchronisation et la localisation sécurisée.

II.2.1 les principaux objectifs

- **Confidentialité**

  La confidentialité est le problème le plus important dans la sécurité réseau. La confidentialité est le fait de s'assurer que l'information n'est accessible qu'à ceux dont l'accès est autorisé, permet de garder la communication des données privées entre un émetteur et un destinataire. La cryptographie ou le chiffrement des données est la seule solution fiable pour assurer la confidentialité des données [6].

- **Authentification**

  C'est le mécanisme de vérifier l'identité d'un nœud qui veut communiquer avec d'autres nœuds. Il arrive qu'un attaquant puisse forger et injecter des paquets falsifiés dans le réseau, dans ce cas, le nœud capteur doit être capable de vérifier la validité de l'identité du nœud source [29].

- **Intégrité**

  C'est le mécanisme de sécurité qui doit garantir qu'un message envoyé par un nœud capteur à l'autre n'est pas modifié ou altéré par un nœud intermédiaire malveillant. Par d'autres termes, l'intégrité permet de garantir que les données sont bien celles que l'on croit être, donc permet de garantir la protection des données contre les modifications et les altérations non autorisées [6] [29].

- **Disponibilité**

  La disponibilité est un service réseau qui permet de donner l'assurance aux entités autorisées d'accéder aux ressources réseaux. L'objectif est d'éviter les attaques de type deni de service [6].

II.2.2 les objectifs secondaires

- **Fraîcheur de données**

  Elle concerne la fraicheur de données et la fraicheur des clés. Puisque tous les réseaux de capteurs fournissent quelques formes de mesures variables dans le temps, nous devons assurer que chaque message est frais. La fraicheur de données implique que les données doivent être récentes et garantit qu'aucun attaquant ne peut réinjecter les anciens messages [30**].**

  Cette exigence est particulièrement importante quand il s'agit de stratégies de sécurité basée sur l'utilisation de clé partagée. Typiquement les clés partagées ont besoin d'être changé au fil du temps. Cependant, il faut du temps pour que de nouvelles clés partagées soient propagées à l'ensemble du réseau [31].

- **Non répudiation**

  La non-répudiation permet de garantir qu'une transaction ne peut être niée et qu'un message a bien été envoyé par un émetteur et reçu par un destinataire où aucun des deux ne pourra nier l'envoi ou la réception du message [6].

- **Contrôle d'accès**

  Un service très important consiste à empêcher un accès au réseau à tout élément étranger au système. Le contrôle d'accès donne aux participants légitimes un moyen de détecter les messages provenant de sources externes au réseau [30].

II.3 Sécurité de l'objet connecté

- **Connexion Wi-Fi**

  Avec tous ces dispositifs connectés librement sur les réseaux sans fil, il devient impératif de s'assurer que les routeurs Wi-Fi sont sécurisés [38] :

  - Utiliser des mots de passe sécurisés.
  - Donner un nom aux routeurs et réseaux de façon à les rendre difficiles à identifier comme des actifs de votre entreprise.
  - Maintenir le logiciel du routeur à jour.

- **Utilisation des mots de passes forts**

  Non seulement on ne devrait pas utiliser toujours les mêmes, mais on devrait aussi s'assurer que les mots de passe sont forts, c'est-à-dire qu'ils contiennent au moins 12 caractères, incluant des chiffres et des symboles, des lettres majuscules et minuscules. Il est nécessaire de ne pas utiliser des mots de passe par défaut du dispositif, ni un mot

de passe que l'on peut aisément deviner ou former d'informations personnelles facilement accessibles [38].

- **Sécuriser l'interface web du périphérique**

  Des choses simples, comme s'assurer que les noms d'utilisateur et les mots de passe par défaut sont modifiés lors de la configuration initiale sont d'une grande aide. Et les modifications ne devraient pas permettre l'utilisation de mots de passe faibles. Des mesures telles que le verrouillage du compte après trois à cinq tentatives de connexion infructueuses devraient peut-être envisagées [38].

- **Protection des données**

  La protection des données pendant le transit du réseau est très important. Tout trafic de données entre un appareil et le Cloud (y compris les informations transmises via des applications mobiles) doit être examiné pour s'assurer qu'il est sécurisé. Le chiffrement de transport, tel que les méthodes SSL (Secure Sockets Layer) ou TLS (Transport Layer Security), peut protéger les données, s'il est utilisé correctement. Cela commence généralement par éviter les protocoles de chiffrement propriétaires et s'en tenir aux protocoles couramment utilisés et validés par la cryptologie [38].

- **Mise à jour des périphériques**

  Les périphériques doivent être mis à jour régulièrement pour que tous les problèmes découverts après leur publication puissent être corrigés, mais le mécanisme de correction lui-même peut être un moyen pour les acteurs malveillants d'accéder à un périphérique. Pour se protéger contre cette menace, les données sensibles telles que les informations d'identification ne doivent jamais être codées en dur dans la mise à jour. Le chiffrement doit toujours être utilisé dans le processus de mise à jour afin que le correctif ne soit pas lisible par une personne utilisant un éditeur hexadécimal [38].

- **Sécurité physique de l'objet connecté [14]**

  - **Scellement du boitier des objets connectés :** Il s'agit de «verrouiller» le boîtier de l'objet par (collage, thermocollage, soudure, ...) de façon à empêcher son ouverture normale. Cela permet aussi de voir si l'intégrité physique de l'objet a été atteinte au premier coup d'œil.
  - **Moulages des cartes et composants :** Le moulage des cartes et composants électroniques dans la résine (si possible opaque aux rayons X) : cela empêchera l'identification des composants utilisés, ainsi que leur analyse par mesure ou débogage.

- **Désactivation des ports de débogage :** La désactivation des ports de débogage et de lecture mémoire des composants (« readout protection ») : pour empêcher l'analyse de leur comportement et des données traitées.
- **L'utilisation des composants sécurisés :** L'utilisation des composants sécurisés (« Secure Element ») pour le stockage des clés et les traitements cryptographiques : cela rend quasiment impossible l'extraction des secrets stockés dans l'objet.

➢ **Sécurité des protocoles de communication**

- Chiffrement des communications sensibles.
- L'utilisation de protocoles sécurisés d'échange de clés : le plus courant étant le protocole Diffie-Hellman, mais 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.
- L'utilisation de mesures anti-brouillage, comme l'étalement de spectre «spread spectrum» ou les sauts de fréquence «frequency hopping» /«channel hopping», utilisés dans certains protocoles comme Bluetooth [38].

➢ **Activer l'authentification à deux facteurs**

L'authentification à deux facteurs est une couche de sécurité supplémentaire sur le mot de passe pour un dispositif qui nécessite une authentification secondaire, un code unique envoyé par courriel ou par SMS avant que l'accès soit accordé.

Lorsqu'elle est utilisée correctement, l'authentification à deux facteurs peut empêcher les méchants d'accéder aux comptes des utilisateurs et de prendre le contrôle des appareils IdO [40].

➢ **Utiliser un VPN (Virtual Private Network)(réseau privé virtuel)**

Désigne un réseau crypté dans le réseau Internet, qui permet à une société dont les locaux seraient géographiquement dispersés de communiquer et partager des documents de manière complètement sécurisée, comme s'il n'y avait qu'un local avec un réseau interne [32].

➢ **Changer le mode d'accès des objets connectés**

L'accès aux objets connectés via leur application Smartphone est généralement protégé par un code PIN ou un mot de passe. Il est impératif qu'on change le code par

défaut. Le but sera de définir le code le plus aléatoire possible, pour le mot de passe combiner minuscules, majuscules, et caractères spéciaux.

Certaines applications pour objets connectés poussent la sécurisation plus loin : elles permettent aux utilisateurs de s'identifier [39]:

- Par reconnaissance faciale.
- Avec empreinte digitale.
- En double authentification.

II.4 Sécurité des objets intelligents

II.4.1 Exemple : maison intelligente ou maison connectée

II.4.1.1 Principe de maison intelligente

La maison intelligente, appelée également maison connectée, est une maison dans laquelle un ensemble d'actions peuvent être programmées et/ou commandées à distance. Elle vise à générer plus de confort de vie, plus de facilité.

Grâce à la domotique, le concept de maison connectée est né. Grâce aux installations domotiques (technologie par câbles ou sans-fil comme l'infrarouge, WiFi ou encore champ magnétique), il est désormais possible de contrôler tout ce qui passe dans une habitation via un Smartphone, un ordinateur ou encore une tablette ainsi que des récepteurs placés dans les différentes pièces. Que ce soit pour la consultation de la consommation d'eau, le déclenchement de l'alarme ou encore le réglage de la température des pièces, tout est simplifié avec la maison connectée [36]**.**

II.4.1.2 Défis de sécurité de la maison intelligente

La connectivité à Internet, associée à la capacité limitée du processeur des périphériques de la maison intelligente et à la popularité croissante de tels systèmes, pose de sérieux défis en matière de sécurité / confidentialité et de gestion efficace de la maison intelligente. Les défis les plus importants sont les suivants: Premièrement, les nœuds utilisés dans les réseaux domestiques HAN (Home Area Network) ont généralement des ressources matérielles limitées (puissance de calcul et mémoire). Il est donc très difficile, voire impossible, de mettre en œuvre des algorithmes complexes garantissant la sécurité. Deuxièmement, un nombre croissant de systèmes domestiques intelligents utilisent le Cloud pour fournir certaines de leurs fonctionnalités, cela signifie que les interfaces sont disponibles sur Internet, ce qui permet potentiellement leur accès à des personnes non autorisées.

Troisièmement, les protocoles de communication sans fil utilisés dans les appareils IoT ne sont pas totalement protégés contre les attaques. Dans le cas où les appareils qui les utilisent sont connectés à Internet, les pirates informatiques peuvent les utiliser comme points d'entrée et autres attaques. Il est connu que des dispositifs IoT, tels que des caméras de vidéosurveillance, ont été utilisés pour des attaques DDoS. Ensuite, la multitude de normes sans fil conduit à un manque de compatibilité entre les appareils proposés sur le marché et à la mise en œuvre complexe d'applications grand public complètes [41].

Les autres problèmes des maisons intelligentes sont les suivants:

- **Configuration difficile :** Actuellement, en dehors des solutions proposées par les fabricants individuels, la configuration des appareils de la maison intelligente peut être trop compliquée pour l'utilisateur moyen. Le problème de la sécurité et de la vie privée est particulièrement visible ici. L'utilisateur n'est pas en mesure de contrôler facilement quelles données et dans quelle mesure les appareils connectés au réseau HAN (Home Area Network) ont accès à son domicile.
- **Absence d'une interface de programmation uniforme :** Il est impossible de créer des applications génériques permettant la lecture de données et l'exécution de commandes sur des appareils du même type (avec les mêmes fonctionnalités) proposés par différents fabricants (par exemple, des ampoules intelligentes).
- **La disponibilité continue des appareils :** Du point de vue de nombreuses applications de maison intelligente (dont une grande partie est axée sur l'amélioration de la sécurité des membres du ménage), il est essentiel de garantir un travail fiable et correct.

II.4.1.3 Exemple de vulnérabilité du système domotique

Une étude récente de l'université de Ben-Gurionde Néguev situé dans le sud d'Israël indique que 70 % des appareils domestiques connectés à internet présentent des failles de sécurité. Lors d'un test, un journaliste de Forbes a pu accéder à huit foyers différents, révélant des informations sensibles telles que les adresses IP, les appareils et même les noms des enfants. Le journaliste a pu découvrir où se trouvaient certaines des maisons et a même allumé et éteint les lumières de la chambre principale.

Le journaliste a pu accéder aux systèmes des maisons simplement en cherchant sur Google une liste de maisons intelligentes. Ces maisons intelligentes particulières utilisaient un

produit qui n'exigeait pas de nom d'utilisateur ni de mot de passe, ce qui les laissait ouvertes aux pirates informatiques (ou aux journalistes de test) pour manipuler leurs maisons.

Chaque maison connectée est potentiellement vulnérable au piratage domotique. Il est important de travailler en étroite collaboration avec le fournisseur du système domotique pour se renseigner sur les mesures de sécurité et la façon de maximiser les paramètres de sécurité. On devra également prendre des mesures indépendantes pour verrouiller le système domotique de façon sécurisée [37].

II.4.1.4 Mettre en œuvre ces mesures de sécurité pour améliorer la sécurité du système domotique [37]

- Définir un mot de passe.
- Changer le mot de passe régulièrement.
- Utiliser un routeur sécurisé.
- **Créer un réseau séparé pour le système domotique**

  Il faut penser également à créer plusieurs points d'accès sur le routeur afin d'avoir deux réseaux différents : un pour l'ordinateur et les appareils mobiles et un autre pour le système domotique et les appareils domestiques connectés. De cette façon, si un pirate informatique vole le mot de passe réseau du téléphone d'un utilisateur ou son ordinateur portable, il ne pourra toujours pas accéder au système domotique.

  C'est également une bonne idée de mettre en place un réseau d'invités avec un mot de passe distinct pour tous les visiteurs de la maison, y compris les entrepreneurs.

- **Cacher le réseau**

  Les pirates informatiques ne peuvent pas s'introduire dans ce qu'ils ne peuvent pas trouver. Pour cela utiliser les paramètres du routeur sans fil pour rendre le réseau domotique invisible de la recherche automatique.

- **Utiliser des signaux cryptés**

  Exiger de l'entreprise de domotique si les signaux envoyés pour les vidéos et les commandes sont cryptés.

- **Vérifier les journaux de bord**

  Jeter un coup d'œil à l'historique des adresses IP sur les journaux des caméras de surveillance. S'il y a une adresse IP qu'on ne reconnait pas, il se peut que ce réseau ait piraté. Dans ce cas, on devra contacter le système de sécurité et changer le mot de passe immédiatement.

- **Éviter l'accès physique aux périphériques dotés de ports USB**

  Les experts pensent que les appareils comme Google Nest sont particulièrement vulnérables physiquement, car ils sont dotés d'un port USB. Les pirates informatiques peuvent y accéder à l'aide d'une clé USB qu'ils ont configuré pour prendre la relève, mais ils doivent se trouver physiquement où se localise l'appareil ou y avoir accès, lors par exemple d'une réparation.

- **Mettre régulièrement à jour le firmware du routeur**

  Il est nécessaire de mettre régulièrement à jour le logiciel du système domotique, et aussi l'application mobile. Suivre les actualités de la marque de la domotique pour qu'on tienne au courant des derniers correctifs de sécurité lancés par le fabricant.

- **Changer le port des caméras IP**

  On rend plus difficile pour les pirates informatiques de trouver la caméra en changeant le port par défaut. De nombreuses caméras IP utilisent un port par défaut qui est facile à découvrir.

- **Ne pas utiliser le Wi-Fi public**

  Si on utilise un appareil mobile pour accéder au domicile à distance, il faut faire attention à la connexion qu'on utilise. On Evite d'utiliser des connexions Wi-Fi lorsque on se connecte au domicile, ou dans ce cas on utilise impérativement un VPN pour chiffrer la connexion et la rendre à la fois anonyme et imperméable.

II.5 Sécurité des RCSFs

Pour se protéger contre les attaques qui menacent les réseaux de capteurs sans fil, plusieurs équipes de recherche tentent de trouver des solutions appropriées. Ces solutions doivent bien sûr prendre en compte les spécificités des réseaux de capteurs sans fil. Il faut donc trouver des solutions simples qui permettent de sécuriser le réseau tout en consommant le moins d'énergie possible et adapter ces solutions à une puissance de calcul faible.

Dans l'éventail de ces solutions, on trouve des mécanismes tels que le partitionnement de données, l'utilisation de méthodes cryptographiques adaptées, l'indice de confiance, et aussi différents protocoles qui ont été proposés pour sécuriser ces réseaux de capteurs.

II.5.1 Mécanismes de sécurité déployés

II.5.1.1 Le partitionnement des données

Comme son nom l'indique le but est de découper l'information en plusieurs parties. Si un capteur cherche à envoyer une information, celui-ci va la découper en plusieurs paquets de

taille fixe. Chaque paquet sera ensuite envoyé sur des chemins différents, c'est à dire qu'ils ne passeront pas par la même route et donc pas par les mêmes nœuds. Ces paquets seront finalement reçus par la base, qui pourra ensuite les rassembler pour pouvoir reproduire l'information. Ce mécanisme oblige un attaquant à récupérer l'ensemble des paquets s'il veut pouvoir lire l'information. Il doit aussi être capable d'écouter l'ensemble du réseau, pour récupérer les différents paquets qui circulent sur des chemins différents [41].

Un exemple de cette solution est représentée par la figure 7, où un capteur A divise un message en 3 paquets qui vont suivre respectivement 3 chemins différents.

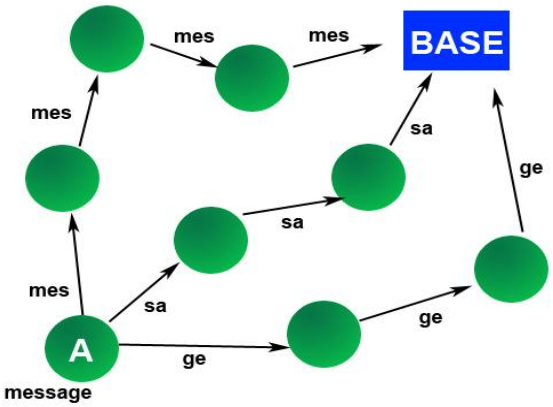

Figure 7:Exemple de partitionnement

Cette solution oblige un attaquant à écouter l'ensemble du réseau et à récupérer l'ensemble des messages pour parvenir à récupérer l'information. Cependant cette solution augmente considérablement la consommation d'énergie (avec un risque de surcharge de traitement), car elle sollicite un nombre de nœuds plus importants.

II.5.1.2 Génération de clés d'authentification dynamique

A chaque période ou génération, la base envoie une nouvelle clé à l'ensemble du réseau. Cette clé sert de certificat à chacun des nœuds, pour prouver son appartenance au réseau. Si un nœud non identifié tente de rentrer dans le réseau de capteurs sans fil et qu'il ne possède pas cette clé de génération, il ne pourra être accepté en son sein. Un autre intérêt de cette technique est qu'elle permet de limiter les attaques de substitution d'un capteur et de sa reprogrammation pour être réinjecté dans le réseau. Si ce nœud est subtilisé à l'instant 0 avec la clé de génération K(0), le temps qu'un attaquant le reprogramme pour le remettre dans le réseau il se sera écoulé un temps "x". Quand le capteur sera repositionné dans le réseau, la nouvelle clé de génération sera alors K(x). Le nœud malicieux demandera à ses nœuds voisins de rentrer dans le réseau avec la clé K(0) et non pas K(x), car il n'a pas pu recevoir la

nouvelle clé. Comme K(0)!=K(x), les nœuds voisins n'accepterons pas sa requête et le nœud malicieux ne pourra pas rentrer dans le réseau [41].

Un exemple est donné par la figure 8, où quatre capteurs A, B, C, D font partie d'un réseau de capteurs qui communiquent par clés symétriques par paire de nœuds. A l'étape I, les capteurs ont pour clé de génération 5. A l'étape II, le nœud A est subtilisé par un attaquant, et pendant son absence sur le réseau, la base transmet une nouvelle clé de génération 7. A l'étape III, le capteur A reprogrammé et réinséré dans le réseau fait une demande d'insertion dans le réseau à B et C. A l'étape IV, les nœuds B et C refusent la demande de A, car en comparant leur clé de génération, ils se sont aperçus qu'elles ne correspondaient plus.

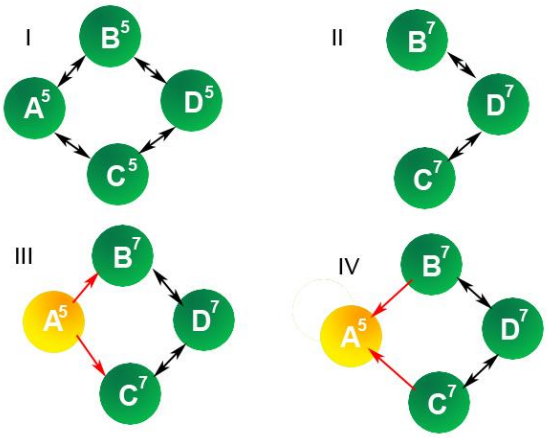

Figure 8:Détection de nœud malicieux par clé de génération

Cette technique est peu coûteuse en terme d'énergie et facile à déployer. Cependant elle ne s'adresse qu'à des réseaux fermés, qui ne peuvent pas accepter de nouveaux nœuds. De plus, se pose le problème d'un nœud sain qui n'aurait pas pu recevoir une clé au cours du temps.

II.5.1.3 L'indice de confiance et la réputation

Dans ce type de réseau tout comme dans les réseaux de capteurs sans fil, vu le nombre de nœuds déployés, il est difficile de savoir, quel nœud peut être un nœud malicieux. Pour le détecter et conserver l'intégrité du réseau, chaque nœud du réseau va surveiller ses nœuds voisins et leurs actions au cours du temps. En fonction des actions réalisées par ses nœuds voisins, un nœud va augmenter une note de l'indice de confiance de ces nœuds, basée sur sa réputation. Si un nœud ne répond jamais à une requête, son indice de confiance va diminuer, de la même manière que si ce nœud retransmet toujours correctement l'information qu'on lui a demandé de transmettre, son indice de confiance va augmenter.

A l'aide de ces indices de confiance, un nœud va alors choisir le routage le plus adapté pour transmettre son information. Contrairement à des protocoles classiques de routage où le nœud chercherait le chemin le plus rapide en nombre de sauts ou de distance géographique, il va choisir ici de transmettre son information via les nœuds avec les indices de confiance les plus élevés, en d'autre terme, la route qui lui semble la plus sûre [41].

Ce mécanisme est représenté par la figure 9, où un nœud A doit transmettre une information à un nœud D. Au lieu de passer par le chemin le plus court qui passe par X, qui est un nœud avec un indice de confiance faible de 3 (sur une note de 10), et donc est potentiellement un nœud à risque, le nœud A va transmettre l'information par les nœuds B et C qui avec des indices de confiance de 8 et 9 proposent le chemin le plus sûr.

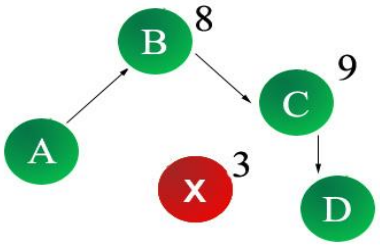

Figure 9:Choix de routage par réputation

Les solutions basées sur l'indice de confiance sont peu coûteuses en termes d'énergie et permettent, selon le type de sécurité voulu, de ne pas avoir recours à la cryptographie. Cependant pour des réseaux qui demandent une sécurité maximale, elles ne sont pas toujours adaptées. Ainsi un nœud malicieux qui enregistrerait des informations sur le réseau, et par ailleurs, se comporterait de manière normale, est difficilement détectable.

Le partitionnement des données	**Génération de clés d'authentification dynamique**	**L'indice de confiance et la réputation**
- Ecouter l'ensemble du réseau pour parvenir à récupérer l'information. - Augmente considérablement la consommation d'énergie.	- Peu coûteuse en termes d'énergie. - Facile à déployer. - S'adresse qu'à des réseaux fermés.	- Peu coûteuses en termes d'énergie. - Ne sont pas toujours adaptables pour des réseaux qui demandent une sécurité maximale.

Tableau 6: Récapitulatif des mécanismes de sécurité

II.5.1.4 Cryptographie

Dans la plupart des mécanismes de sécurisation actuelle, la cryptographie est sans doute la technique la plus utilisée. Le chiffrement des données permet d'empêcher l'écoute des données transitées sur un réseau sans fil et de garantir la confidentialité des données.

Dans le cadre des réseaux filaires et des réseaux sans fil traditionnels disposant d'une capacité de calcul et de mémoire conséquente, les solutions de cryptographie sont réputées comme des solutions sûres qui répondent à l'ensemble des problèmes liés à la sécurité des données.

- **Définition**

Le mot «cryptographie» est composé des mots grecs: « crypto » signifie caché et «graphy» qui signifie écrire [29]. La cryptographie est un mécanisme de sécurité qui est relativement beaucoup plus sûr et fiable, basée sur l'utilisation des méthodes mathématiques pour la transformation des messages originaux en une suite de données incompréhensibles et qui ne peuvent pas être interpréter directement par des tierces parties.

La cryptographie est mise en place afin de garantir la confidentialité, l'intégrité et l'authentification de données échangées. Il existe principalement deux catégories de cryptographie, qui sont respectivement la cryptographie symétrique et la cryptographie asymétrique :

- **Cryptographie symétrique**

La cryptographie symétrique utilise une seule clé pour le chiffrement et le déchiffrement des données, elle est considérée comme une solution moins couteuse et plus facile à implémenter, cependant cette solution possède aussi des inconvénients inhérents. Pour que deux nœuds puissent communiquer entre eux, ils doivent utiliser exactement la même clé, et la distribution de clés est devenue un défi inévitable. En effet, la distribution de clés est difficile car dans un système symétrique, chaque nœud a besoin d'une clé partagée avec chaque autre nœud du réseau. Donc on aura à gérer n*(n-1)/2 clés, si on considère que le nombre de nœuds dans le réseau est égal à n [33].

Il existe dans la littérature 4 types de distribution de clé [34]:

- **Clé globale**: Une clé est partagée par l'ensemble du réseau. Pour envoyer un message, l'information est chiffrée avec cette clé. Une fois le message reçu, le

message peut être déchiffré avec cette même clé (principe de la clé symétrique). C'est la solution la moins coûteuse en termes d'énergie, mais avec la sécurité la moins importante. Si un attaquant récupère la clé, il peut déchiffrer tout le réseau.

- **Clé partagée par paire de nœuds:** Chaque nœud possède une clé différente pour communiquer avec un nœud voisin qui partage cette clé. Ainsi si un nœud possède "n" voisins, il aura "n" clés à stocker pour pouvoir communiquer avec ses voisins. Dans cette solution, un nœud qui cherche à envoyer un message, doit l'encrypter avec la clé du voisin qui recevra l'information. Le nœud voisin devra déchiffrer l'information pour la chiffrer à nouveau avec la clé qui correspond au destinataire suivant. C'est la solution cryptographique la plus sécurisée (l'attaquant doit récupérer chaque clé par paire de nœuds pour avoir accès à toute l'information), mais aussi la plus coûteuse en terme d'énergie et de latence. Chaque nœud intermédiaire doit déchiffrer le message du prédécesseur, puis le chiffrer avant de l'envoyer au nœud suivant.
- **Clé partagée par groupe de nœuds:** Dans ce cas de figure, chaque groupe ou cluster partage une clé en commun qui lui permet de communiquer à l'intérieur du groupe. Les nœuds maîtres communiquent entre eux avec, soit une clé commune à tous les clusters heads, soit une clé commune par paire de cluster head. Cette solution est une solution hybride des deux premières techniques de chiffrement et apporte un compromis entre sécurité et consommation d'énergie.
- **Clé individuelle**: Dans cette solution chaque nœud possède une clé personnelle pour chiffrer son information. Cette clé n'est connue que de la base. Ainsi un message envoyé par ce nœud circulera de manière cachée sur le réseau jusqu'à atteindre la base. Si cette solution est intéressante en termes de sécurité, elle n'apporte qu'une possibilité de communication sécurisé entre un nœud et la base, mais pas entre nœuds.

  La figure suivante représente le mécanisme de chiffrement Symétrique.

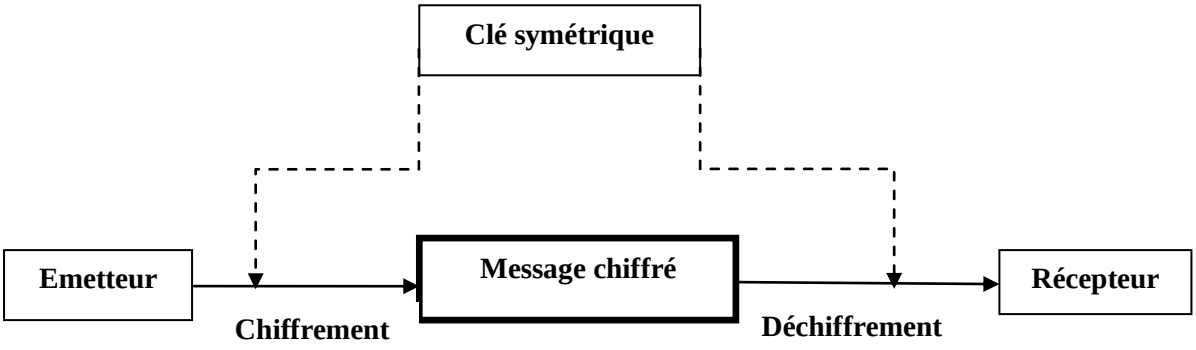

Figure 10:Chiffrement symétrique.

Cependant, les algorithmes de chiffrement symétrique peuvent être les plus appropriés pour les applications des RCSFs. En effet, ils ne requièrent pas d'opérations mathématiques complexes pour crypter ou décrypter les données. Par conséquent, ils n'exigent pas de grandes dissipations énergétiques durant les phases de chiffrement et de déchiffrement.

❖ **Les algorithmes de gestion de clés symétriques**

Les algorithmes de chiffrement symétriques sont décomposés en deux catégories [34] :

- Le chiffrement en chaîne est fait bit à bit sans attendre la réception entière des données. L'algorithme le plus connu est : RC4 (Rivest Cipher 4).
- Le chiffrement par bloc consiste à fractionner les données en blocs de taille fixe (64 bits, 128 bits). Chaque bloc sera ensuite chiffré une fois qu'il atteint une taille envisagée. Les algorithmes les plus utilisés sont : DES (Data Encryption Standard), AES (Advanced Encryption Standard).

➢ **Cryptographie asymétrique :**

Deux clés différentes sont générées par le récepteur : une clé publique diffusée à tous les nœuds servant au chiffrement de données qu'elles vont émettre au récepteur, et une clé privée maintenue secrète chez le récepteur servant pour le déchiffrement de ces données lorsque ce dernier les reçoit. Le point fondamental sur lequel repose la sécurité du chiffrement asymétrique est l'impossibilité de déduire la clé privée à partir de la clé publique. L'algorithme de chiffrement asymétrique le plus connu est : RSA (Rivest Shamir Adleman). La figure 11 présente le mécanisme de chiffrement asymétrique.

Dans ces algorithmes, différents problèmes mathématiques se présentent à cause des calculs utilisés pour déchiffrer les données reçues. La complexité de telles opérations est très importante parce que les nœuds capteurs exigent une capacité de traitement plus élevée et une dissipation d'énergie plus haute. En utilisant le chiffrement asymétrique, chaque nœud capteur souffre d'un autre problème dû au stockage de clés publiques de tous les nœuds restant du réseau. Cela provoque une forte occupation des mémoires de chaque nœud. Cependant, la distribution de clés est moins pénible car leur échange est fortement simplifié. En effet, avec un système asymétrique, chaque nœud a besoin d'une paire de clés. Si on considère que le nombre de nœuds dans le réseau est égal à n, il faudra donc gérer 2n clés. Bien que le chiffrement asymétrique comporte des

avantages, il est inutilisable directement dans les RCSFs. Cela est dû à sa lenteur d'exécution et son coût en termes de capacité des ressources [34].

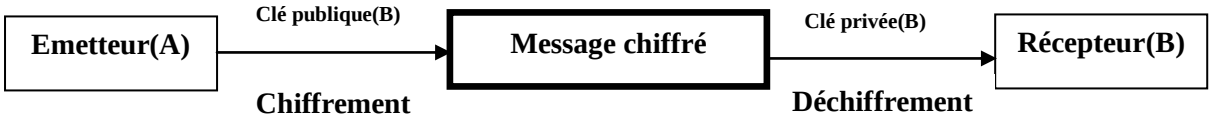

Figure 11:Chiffrement asymétrique.

❖ **Les algorithmes de gestion de clé asymétrique**

- **RSA (Rivest-Shamir-Adleman)**

  RSA est un algorithme asymétrique de cryptographie à clé publique. L'algorithme est fondé sur l'utilisation d'une paire de clés composée d'une clé publique et d'une clé privée. La clé publique correspond à une clé accessible par n'importe quelle personne souhaitant chiffrer des informations, la clé privée, quant à elle, est réservée à la personne ayant créée la paire de clés et est nécessaire pour déchiffrer les message s[31].

- **ECC (Elliptic Curve Cryptosystem)**

  "Elliptic Curve Cryptosystem" est une approche de cryptographie à clé publique basée sur les aspects mathématiques des courbes elliptiques. Son avantage par rapport à un algorithme comme RSA basé sur les nombres premiers est d'utiliser des clés de taille bien plus petite.

  Une comparaison entre ces deux types de cryptographie est présentée dans le tableau suivant :

Cryptographie symétrique	**Cryptographie asymétrique**
Une seule clé pour le chiffrement et le déchiffrement.	Une clé publique pour le chiffrement, une clé privée pour le déchiffrement.
Moins couteuse en termes d'énergie.	Couteuse en termes d'énergie.
Facile à implémenter (Simplicité des calculs).	Gourmande en ressources : calculs plus complexes.
Grand espace de stockage : n (n-1)/2 clés.	Faible espace de stockage : 20 clés uniquement.
Basé sur la pré-distribution de clés.	Ne nécessite pas une pré-distribution de clés.

Tableau 7: Cryptographie Symétrique VS Cryptographie Asymétrique

III. Conclusion

Dans ce chapitre nous avons évoqué la sécurité dans l'Internet des Objets, nous avons abordé la façon de sécuriser un objet connecté, un objet intelligent puis nous avons parlé sur la sécurité des RCSFs, et nous avons clos le chapitre par la définition de la cryptographie ainsi ses deux types symétrique et asymétrique. Dans le prochain chapitre nous allons présenter la cryptographie moderne dédiée pour l'IdO qui est la cryptographie basée sur les courbes elliptiques.

Chapitre IV : La cryptographie moderne pour l’Internet des Objets

I. Introduction

La cryptographie est toujours considérée comme une des solutions dominantes pour assurer la confidentialité des informations. La nature de cette solution permet de rendre un message illisible en utilisant un ensemble de méthodes mathématiques, ce qui implique souvent des calculs compliqués et intensifs, qui posent de problèmes sérieux pour les systèmes avec contraintes de ressources notamment l'Internet des Objets (l'IdO). Actuellement, la cryptographie moderne se base en partie sur certaines notions difficiles en théorie des nombres comme la factorisation des grands nombres (RSA) ou le problème du logarithme discret (cryptographie à base de courbes elliptiques).

La différence entre les algorithmes de chiffrement à base de courbes elliptiques et les algorithmes basés sur les entiers comme RSA ou El-Gamal est que, pour les vaincre, la résolution d'un problème de logarithme discret sur une courbe elliptique est nécessaire. Cette résolution est réputée être un problème plus difficile que le problème similaire dans les entiers modulos n utilisé par RSA. C'est pourquoi on n'estime qu'une clé de 192 bits qui mesure, pour une courbe elliptique, la taille du corps fini K de cette courbe pour les chiffres basés sur les courbes elliptiques est plus sûre qu'une clé de 1024 bits pour le RSA. Comme les calculs sur les courbes elliptiques ne sont pas bien compliqués à réaliser, c'est un grand avantage pour les objets connectés où on dispose de peu de puissance, et où la taille de la clé influe beaucoup sur les performances.

Niveau de sécurité (bits)	Taille de la clé RSA (bits)	Taille de la clé ECC (bits)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	512

Tableau 8: Comparaison des tailles de clés RSA et ECC

Pour expliquer le fonctionnement d'ECC dans le contexte de l'IdO, nous étudions dans ce chapitre les concepts mathématiques fondamentaux des courbes elliptiques, ainsi que leur approche géométrique. Ensuite nous présentons quelques protocoles de sécurité basés sur les courbes elliptiques.

II. Les courbes elliptiques pour la cryptographie

Les algorithmes de cryptographie asymétriques sont généralement plus couteux par rapport aux algorithmes de la cryptographie symétriques, ainsi les clés générées sont plus longues et nécessitent des calculs importants. De ce fait, la cryptographie asymétrique est moins souhaitée dans le cas des réseaux de capteurs sans fil à cause des ressources limitées de ces derniers. En effet, un nœud capteur est muni d'une petite taille mémoire, une faible puissance de calcul et d'une ressource énergétique critique, l'utilisation de la cryptographie asymétrique est donc rarement utilisée dans ce domaine. Cependant, des optimisations de ces algorithmes a rendu possible l'implémentation de tels algorithmes dans les réseaux de capteurs. La cryptographie des courbes elliptiques est un nouveau cryptosystème asymétrique basé sur le problème de logarithme discret sur les courbes elliptiques, il permet d'améliorer les primitives cryptographiques existantes en réduisant la taille des clés [11].

II.1 Généralités

Avant de présenter les courbes elliptiques, nous étudions d'abord les notions mathématiques dont nous avons besoin pour comprendre son fonctionnement [33].

II.1.1 Groupe

En mathématique, un groupe est un couple (E, ·) où E est un ensemble et (·) est une loi de composition interne qui combine deux éléments a et b de E pour obtenir un troisième élément (a · b). Il faut que la loi satisfasse les quatre axiomes ci-dessous [33] :

- **Fermeture :** $\forall (a, b) \in E \mid a \cdot b \in E$
- **Associativité :** $\forall (a, b) \in E \mid (a \cdot b) \cdot c = a \cdot (b \cdot c)$
- **Élément neutre :** $\exists e \in E \mid a \cdot e = e \cdot a = a$
- **Symétrique :** $\forall a \in E, \exists b \in E \mid a \cdot b = b \cdot a = e$

II.1.2 Groupe abélien

Un groupe abélien, ou un groupe commutatif, est un groupe dont la loi de composition interne est commutative. Un ensemble E est un groupe commutatif lorsque [33]:

$$\forall (a, b) \in E \mid a \cdot b = b \cdot a$$

II.1.3 Corps

Un corps est un ensemble E muni de deux lois de composition, notée respectivement + et ·. Il faut que les deux lois satisfassent les conditions suivantes [33] :

- Le couple (E, +) forme un groupe abélien, il existe un élément neutre, noté 0, tel que $\forall a \in E \mid a + 0 = 0 + a = a$.
- Le couple (E\ {0}, ·) forme aussi un groupe abélien dont l'élément neutre est 1, $\forall a \in E \mid a \cdot 1 = 1 \cdot a = a$.
- La multiplication · est distributif pour l'addition, c'est-à-dire : $\forall (a, b, c) \in E \mid a \cdot (b + c) = a \cdot b + a \cdot c$ et $(b + c) \cdot a = b \cdot a + c \cdot a$. Autrement dit, un corps est un anneau dont les éléments non nuls forment un groupe abélien pour la multiplication.

II.1.4 Corps fini

Un corps fini F est un corps dont le nombre d'éléments est fini. Le nombre d'éléments est l'ordre du corps, noté q, qui peut être représenté par la puissance d'un nombre premier $q = p^n$, où p est un nombre premier, appelé la caractéristique du corps, et $n \in Z^+$. Pour étudier la cryptographie sur les courbes elliptiques, il faut que nous comprenions les deux types de corps ci-dessous [33]:

- **Corps premier**

  Un corps est premier, noté F_q lorsque l'ordre du corps $q = p^n$ avec p un nombre premier. Le corps est constitué des nombres entiers $\{0, 1, 2, ..., p - 1\}$, et $\forall a \in Z$, a mod p donne le reste unique r qui est compris entre $[0, p - 1]$ [33].

- **Corps binaire**

  Un corps fini de l'ordre 2^n est un corps binaire, noté F_2^n, qui peut être construit en utilisant une représentation polynomiale. Les éléments du corps sont des polynômes binaires dont les coefficients $a_i \in \{0, 1\}$ et les degrés sont inférieurs à n. C'est-à-dire [33] :

$$F_2^n = \{a_{n-1}z^{n-1} + a_{n-2}z^{n-2} + ... + a_1z + a_0 : a_i \in \{0, 1\}\}$$

II.2 Présentation des courbes elliptiques

Après la présentation des notions mathématiques nécessaires, nous allons passer, dans cette section, à la définition des courbes elliptiques avec l'ensemble d'opérations que nous pouvons effectuer sur elles [33].

II.2.1 Définition d'une courbe elliptique

La courbe elliptique E est une courbe algébrique qui peut être représentée par l'équation de Weierstrass (formule II.1).

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad \textbf{(II.1)}$$

On suppose que la courbe est définie dans un corps K et les paramètres a_1, a_2, a_3, a_4, $a_6 \in K$. Pour que la courbe soit lisse et ne contienne aucun point de rebroussement, il faut que le discriminant de la courbe $\Delta \neq 0$.

La forme de la courbe peut varier en fonction des paramètres choisis comme illustré sur la figure 12 où nous avons présenté deux exemples de courbes elliptiques. Dans le domaine cryptographique pour les dispositifs ayant des ressources limitées, nous utilisons les courbes elliptiques qui sont définies dans un corps fini dont l'ordre $q = p^n$. Ce corps peut être soit premier, soit binaire, et le choix de corps n'a pas une influence importante sur la performance du cryptosystème. Dans la littérature, il existe différents algorithmes et techniques qui nous permettent d'optimiser les performances de calcul sur les courbes qui sont définies sur les deux types de corps. L'équation de Weierstrass d'une courbe elliptique peut être simplifiée, si la courbe est définie sur un corps premier F_p dont la caractéristique est différente de 2 et de 3. Nous pouvons transformer la formule II.1 à l'équation de Weierstrass simplifiée (formule II.2).

$$y^2 = x^3 + ax + b \quad \textbf{(II.2)}$$

Où à, $b \in F_p$.

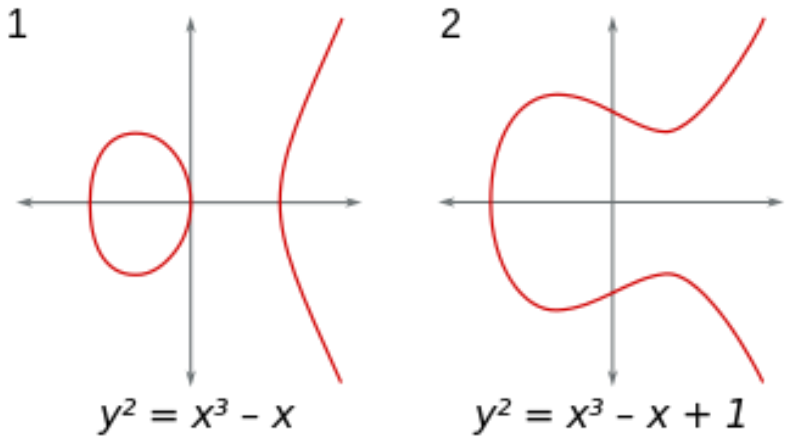

Figure 12:Exemples de courbe elliptique

II.2.3 Approche Géométrique

Soient E une courbe elliptique définie sur un corps K, et deux points P, Q ∈ E(K), L est la droite reliant P à Q (la tangente à E si P = Q) et R le troisième point d'intersection de L avec E. Soit L_0 la droite verticale passant par R. On définit P + Q ∈ E(K) comme étant le deuxième point d'intersection de L' avec E. (E(K), +) muni de la loi de composition est un groupe abélien dont l'élément neutre est le point à l'infini (O) [34] .

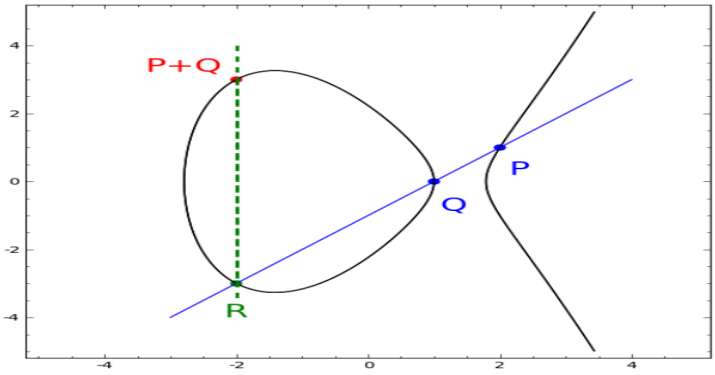

Figure 13:Addition de deux points sur une courbe elliptique sur R.

Cas particuliers :

- Si P1 et P2 sont symétriques par rapport à l'axe des abscisses, on considère alors que la somme des deux points est nulle. Il s'agit donc du point à l'infini.
- Si la droite (L) est tangente en un point de la courbe, on considère qu'elle intersecte deux fois la courbe en ce point et par conséquent la somme de P1 et P2 (ou bien le doublement de P) est le symétrique du point de tangence.

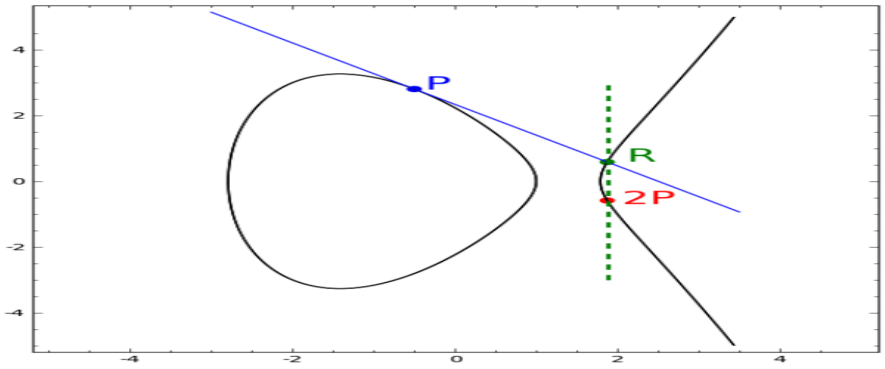

Figure 14:Doublement d'un point sur une courbe elliptique sur R.

II.2.4 Logarithme discret

Le principe de la cryptographie à clé publique repose sur un couple de clés, l'une publique et l'autre privée. Retrouver la clé privée à partir de la clé publique doit revenir à

résoudre le problème du logarithme discret considéré comme difficile. Si p est un point de la courbe elliptique $E(F_p)$ d'ordre n, et Q un autre point de la courbe, la difficulté de trouver l'entier k € [0, n-1] tel que Q = kP est appelé le problème du logarithme discret. La solution la plus naïve pour résoudre ce problème est de calculer exhaustivement 1P, 2P, 3P… jusqu'à ce que nous trouvions Q, mais le calcul peut devenir extrêmement long si la valeur de k est plus grande. Il n'y a pas de preuve mathématique qui peut démontrer que l'ECDLP est insoluble, mais la résolution d'un tel problème est toujours considérée comme infaisable en prenant compte l'état actuel des technologies informatiques [35].

- **Génération de clés avec le Logarithme Discret Elliptique :** Une paire de clés est associée à un ensemble de paramètres publiques (p,E ,P,n) où p est un nombre premier, E une courbe elliptique, P le point générateur et n son ordre, c'est-à-dire :
  $nP = \infty$.
  Une clé privée d est sélectionnée au hasard dans l'intervalle [1, n-1] et la clé publique correspondante est Q = dP. Le problème du logarithme discret consiste à déterminer d à partir des paramètres publics (p,E,P,n).

Algorithme : Génération de clés avec le logarithme discret elliptique

---

Entrées :p,E ,P,n // les paramètres publiques générés

Sortie : clé publique(Q) et clé privée d générée

1. Sélectionner au hasard d dans l'intervalle [1, n-1]
2. Calculer Q = dP
3. Retourner (Q,d)

II.3 Les protocoles de sécurité basés sur les courbes elliptiques

II.3.1 Protocole d'échange de clés de Diffie-Hellmann

Alice et Bob veulent avoir une clé en commun pour s'échanger des données en toute sécurité. Supposons que leur seul moyen de communication soit public. Un des moyens de sécuriser leurs données est qu'ils établissent une clé privée entre eux. La méthode de Diffie-Hellmann permet justement de faire cela (voir la figure15).

1. Alice et Bob choisissent une courbe elliptique E définie sur un corps fini F_q tel que le logarithme discret soit difficile à résoudre. Ils choisissent aussi un point $P \in E(F_q)$ tel que le

sous-groupe généré par P ait un ordre de grande taille, (En général, la courbe E et le point P sont choisis de manière à ce que l'ordre soit un grand nombre premier).

2. Alice choisit un nombre entier secret a, calcule $P_a = aP$ et envoie P_a à Bob.

3. Bob choisit un nombre entier secret b, calcule $P_b = bP$ et envoie P_b à Alice

4. Alice calcule $aP_b = abP$.

5. Bob calcule $bP_a = baP$.

6. Alice et Bob utilisent une méthode quelconque connue pour extraire une clé secrète de abP. Par exemple, ils peuvent utiliser les derniers 256 bits de la première coordonnée de abP comme clé, ou ils peuvent hacher une des coordonnées de abP avec une fonction de hachage pour laquelle ils se sont mis d'accord.

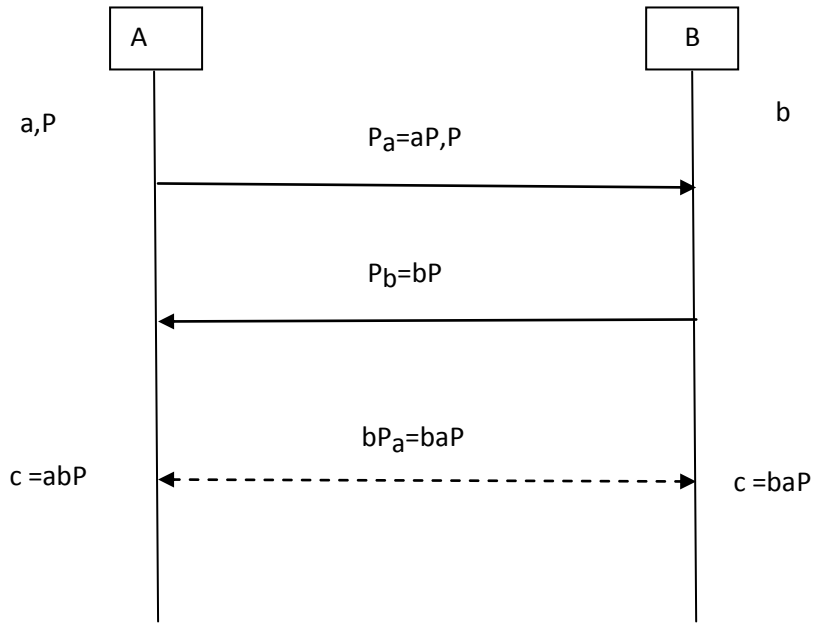

Figure 15:Echange de clés Diffie-Hellman ECC

II.3.2 ECIES (Elliptic Curve Integrated Encryption Scheme)

Le protocole d'Elgamal est rarement utilisé directement avec les courbes elliptiques. Avant de chiffrer un message, il faut d'abord le convertir à un point sur la courbe elliptique utilisée. Le protocole ECIES est un système de chiffrement, variante de l'algorithme ElGamal à clé publique. Il a été standardisé par ANSI X9.63 et ISO/IEC 15946-3, il est aussi défini dans le standard IEEE P1363.

Dans ECIES, un secret partagé de type Diffie-Hellman est utilisé pour dériver deux clés symétriques k1 et k2. La clé k1 est utilisée pour chiffrer le texte clair en utilisant un algorithme de chiffrement symétrique, k2 est utilisé pour authentifier le texte chiffré résultant.

Pour chiffrer un message clair m, on l'encode comme un point dans une courbe elliptique. Si Alice veut envoyer un message secret à Bob en utilisant l'algorithme ECIES, ils doivent d'abord disposer de toutes les informations suivantes [6] :

– KDF (Key Derivation Function) : Une fonction de dérivation de clé qui permet de générer plusieurs clés à partir d'une valeur secrète de référence.

– MAC (Message Authentication Code) : Code transmis avec les données dans le but d'assurer l'intégrité de ces dernières.

– SYM : Algorithme de chiffrement symétrique.

– $E(F_p)$: La courbe elliptique utilisée avec le point de générateur P dont $ord_p(P) = n$.

– K_B : La clé publique de Bob $K_B = k_B.P$ où $k_B \in [1, n-1]$ est sa clé privée.

L'échange se passe comme suit :

Algorithme : ECIES

Chiffrement du message

Entrées : clé privée k_A, P, clé publique K_A, le message M.

Sortie : un message chiffré (R, C, t).

1. Choisir un nombre entier $k \in [1, n-1]$ et calculer $R = k.P$.
2. Calculer $Z = k.K_B$.
3. Générer les clés $(k_1, k_2) = KDF$ (abscisse(Z), R).
4. Chiffrer le message $C = SYM (k_1, M)$.
5. Générer le code MAC $t = MAC (k_2, C)$.
6. Envoyer (R, C, t) à Bob.

Déchiffrement du message

Entrés : clé publique K_A, clé privée k_B, le message chiffré (R, C, t).

Sortie : un message clair M.

---

1. Rejeter le message si R n'appartient pas a $E(F_p)$.

2. Calculer $Z = k_B.R = k_B.k.P = k.K_B$.

3. Générer les clés $(k_1, k_2) = KDF(abscisse(Z), R)$.

4. Générer le code MAC $t' = MAC(k_2, C)$.

5. Rejeter le message si $t' =/= t$.

6. Déchiffrer le message $M = S\ Y\ M^{-1}\ (k_1, C)$.

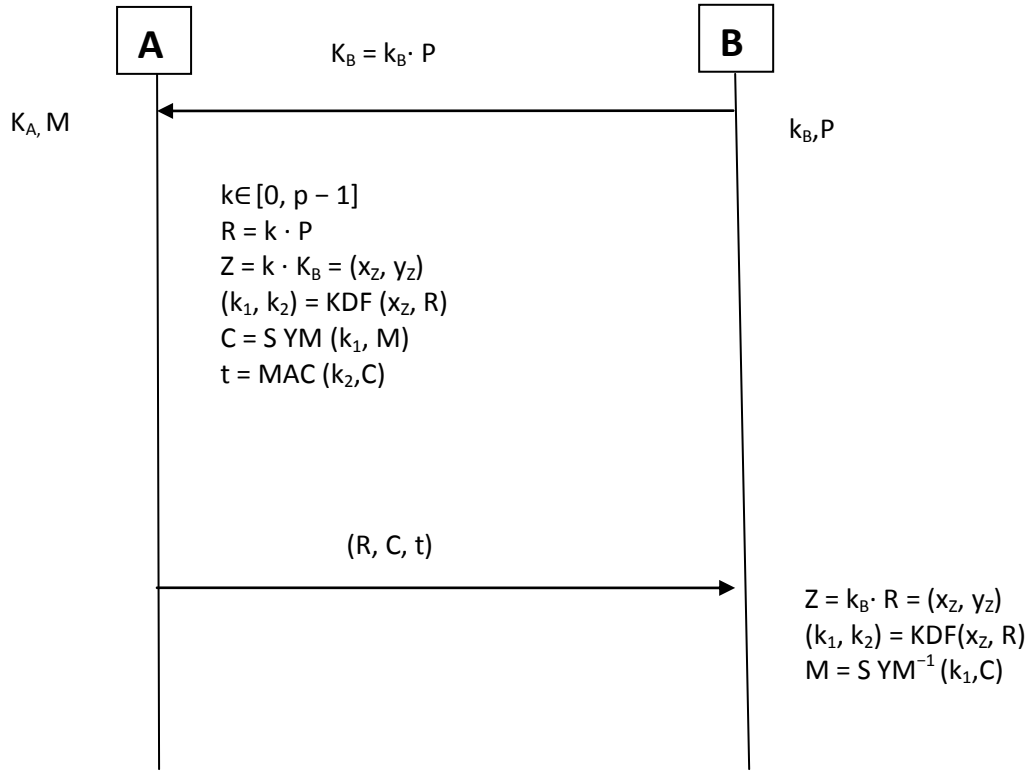

Figure 16:Protocole de chiffrement ECIES

II.3.3 ECDSA (Elliptic Curve Digital Signature Algorithm)

Le protocole ECDSA est proposé par Johnson et al. C'est une variante de DSA qui utilise les techniques de cryptographie sur les courbes elliptiques. Le protocole DSA signifie Digital Signature Algorithm en Anglais, c'est un algorithme de signature numérique standardisé par le NIST aux États-Unis. Le protocole est basé sur l'idée du protocole de signature d'Elgamal [6].

Nous supposons qu'Alice et Bob utilisent la même courbe elliptique $E(F_p)$ pour sécuriser la communication entre eux. Nous supposons que la clé publique d'Alice est $K_A=k_A.P$ où k_A est sa clé privée et P est le point générateur de l'ordre n.

Algorithme : ECDSA

Génération d'une signature ECDSA

Entrées : P, clé privée k_A, un message M.

Sortie : signature (r,s).

1. Choisir un nombre aléatoire $k \in [1, n-1]$.
2. Calculer $R = k.P$.
3. Calculer $r = abscisse(R) \pmod n$. Si $r = 0$, retourner à l'étape 1.
4. Calculer $s = k^{-1} (H(M) + k_A r) \pmod n$ où H est une fonction de hachage. Si $s = 0$, retourner à l'étape 1.
5. Envoyer (r, s) à Bob.

Vérification d'une signature ECDSA :

Entrées : P, clé publique K_A, message M, signature (r,s).

Sorties : acceptation ou rejet de la signature.

1. Vérifier si $K_A \neq \infty$ (point à l'infini) et $K_A \in E(F_p)$.
2. Vérifier si $n.K_A = \infty$ car $n.K_A = n.k_A.P$ et $ord_p(P) = n$.
3. Vérifier si $(r, s) \in [1, n-1]$.
4. Calculer $R = (H(M)s^{-1} \bmod n)P + (rs^{-1} \bmod n)K_A$.
5. Vérifier si $r \equiv abscisse(R) \pmod n$.

$R = (H(M)s^{-1})P + (rs^{-1})K_A \pmod n$

$= (H(M)s^{-1})P + (rs^{-1})k_AP \pmod n$

$= s^{-1}P(H(M) + rk_A) \pmod n$

$= k(H(M) + k_Ar) -1P(H(M) + rk_A) \pmod n$

$= kP.$

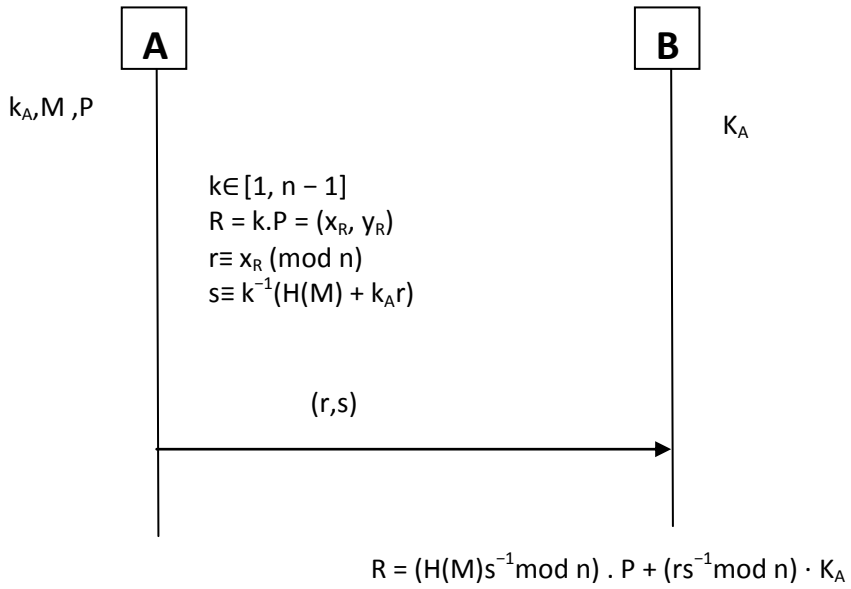

Figure 17:Protocole de signature numérique ECDSA

III. Implémentation :

La partie implémentation de notre projet consiste à implémenter les différents protocoles cryptographiques basés sur les courbes elliptiques sur une carte Arduino et évaluer les temps de calcul de génération des clés, de chiffrement, de déchiffrement, de signature et de la vérification de la signature.

III.1 Environnement et choix du matériel

Pour calculer le temps d'exécution de chaque protocole cryptographique, nous avons utilisé l'environnement suivant :

- Une carte Arduino UNO R3.
- L'IDE Arduino 1.6.9.
- La bibliothèque cryptographique micro-ecc (µECC).

III.1.1 Arduino UNO R3

La carte Arduino Uno est basée sur un ATMega328 cadencé à 16 MHz. C'est la plus récente et la plus économique carte à microcontrôleur d'Arduino. Des connecteurs situés sur les bords extérieurs du circuit imprimé permettent d'enficher une série de modules complémentaires.

Elle peut se programmer avec le logiciel Arduino. Le contrôleur ATMega328 contient

un bootloader qui permet de modifier le programme sans passer par un programmateur. Le logiciel est téléchargeable gratuitement[47].

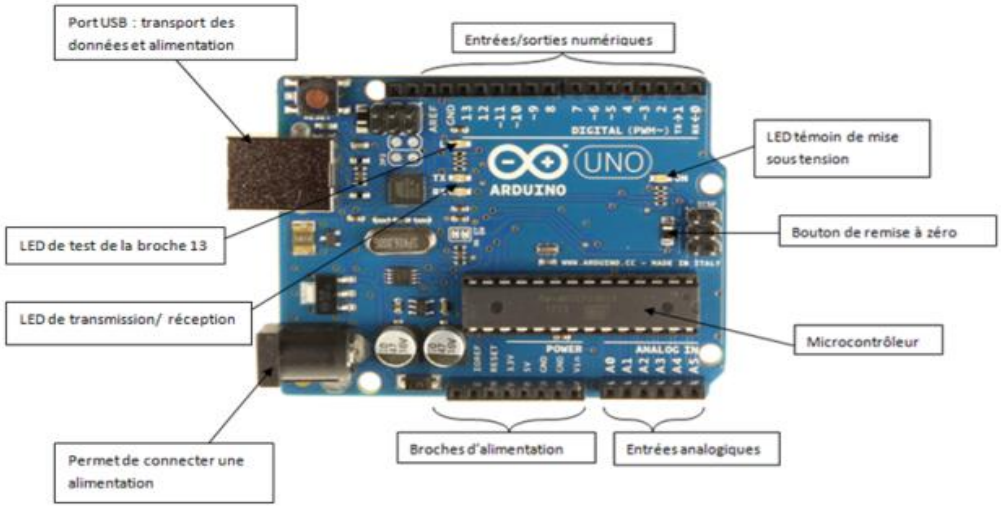

Figure 18:Architecture d'une carte Arduino Uno

- **Caractéristiques principales**

- Version: Rev. 3
- Alimentation:
  -Via port USB ou
  - 3.3 à 12 V sur connecteur alim 5,5 x 2,1 mm
- Microprocesseur: ATMega328P
- Mémoire flash: 32 kB
- Mémoire SRAM: 2 kB
- Mémoire EEPROM: 1 kB
- 14 broches d'E/S dont 6 PWM
- 6 entrées analogiques 10 bits
- Intensité par E/S: 40 mA
- Cadencement: 16 MHz
- Bus série, I2C et SPI
- Gestion des interruptions
- Fiche USB

- Dimensions: 74 x 53 x 15 mm

III.1.2 L'IDE Arduino 1.6.9

Le logiciel Arduino Open Source(IDE) facilite l'écriture du code, il fonctionne sous Windows, Mac OS X et Linux. L'environnement est écrit en java et basé sur Processing et d'autres logiciels à code source ouvert. Ce logiciel peut être utilisé avec n'importe quelle carte Arduino.

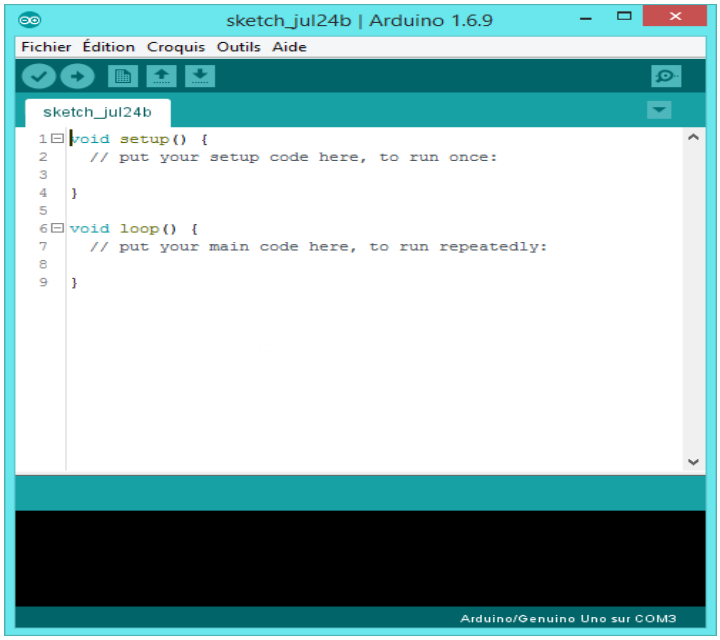

Figure 19:IDE Arduino 1.6.9

Après l'installation de l'IDE Arduino, nous avons passé à l'installation d'une bibliothèque qui nous permet d'implémenter les algorithmes et les fonctions dont on aura besoin pour effectuer notre travail.

III.1.3 La bibliothèque cryptographique micro-ecc (µECC)

Micro-ecc est une implémentation d'ECDH et ECDSA, petite et rapide pour les processeurs 8 bits, 32 bits et 64 bits.

➢ **Caractéristiques :**

- Résistant aux attaques connues sur les canaux secondaires.
- Écrit en C, avec assemblage en ligne GCC en option pour les plates-formes AVR, ARM et Thumb.
- Prend en charge les architectures 8, 32 et 64 bits.
- Petite taille de code.

- Aucune allocation de mémoire dynamique.
- Prise en charge de 4 courbes standard: secp160r1, secp192r1, secp256r1 et secp256k1.
- Licence BSD à 2 clauses.

III.2 Paramètres d'implémentation

Nous avons implémenté notre travail sur plusieurs cryptosystemes avec une taille de clés différente :

- La taille de clé de **uECC_secp160r1 ()** est 160 bits.
- La taille de clé de **uECC_secp192r1 ()** est 192 bits.
- La taille de clé de **uECC_secp224r1 ()** est 224 bits.
- La taille de clé de **uECC_secp256r1 ()** est 256 bits.

Nous avons utilisé les fonctions suivantes pour calculer les temps écoulés dans les différentes phases [48] :

- **Millis () :**
  - **Description :** Renvoie le nombre de millisecondes depuis que la carte Arduino a commencé à exécuter le programme courant. Ce nombre débordera (c'est à dire sera remis à zéro) après 50 jours approximativement.
    - **Syntaxe :** variable_unsigned_long = millis() ;
    - **Paramètres** : Aucun.
    - **Valeur Retournée :** Le nombre de millisecondes depuis que le programme courant a démarré. Renvoie une variable long non signée.
- **Micros () :**
  - **Description :** Renvoie le nombre de microsecondes depuis que la carte Arduino a démarré le programme en cours. Ce nombre déborde (repasse à 0) après approximativement 70 minutes. Sur les cartes Arduino à 16Mhz (par exemple le Duelmilanove et la Nano), cette fonction a une résolution de 4 microsecondes (ce qui veut dire que la valeur retournée est toujours un multiple de quatre, autrement dit que la fonction compte de quatre en quatre). Sur les cartes Arduino à 8Mhz (par exemple Lilypad), cette fonction a une résolution de 8 microsecondes.
    - **Syntaxe**: variable_unsigned_long = micros().
    - **Paramètres** : Aucun.

- **Valeur Renvoyée** : Le nombre de microsecondes écoulées depuis que le programme en cours a démarré, sous la forme d'un nombre de type unsigned long.

➢ **Delay() :**

- **Description :** Réalise une pause dans l'exécution du programme pour la durée (en millisecondes) indiquée en paramètre. (Pour mémoire, il y a 1000 millisecondes dans une seconde...!).
- **Syntaxe :** Delay (ms)
- **Paramètres** : **ms** (unsigned long): le nombre de millisecondes que dure la pause.
- **Valeur Renvoyée** : Aucune.

III.3 Expérimentation

III.3.1 ECDH

Le tableau suivant représente les résultats obtenus après l'exécution du protocole cryptographique ECDH par rapport au temps écoulé pendant la génération des clés et du partage du secret en utilisant les différentes courbes elliptiques 160, 192, 224 , 256 bits.

Taille de la clé/ Temps de calcul	Gen_Public_key1	Gen_Public_key2	Secret1	Secret2
160 bits	1095	1056	1054	1053
192 bits	1761	1763	1760	1762
224 bits	2691	2691	2692	2693
256 bits	4366	4367	4366	4365

Tableau 9: Temps d'exécution d'ECDH en millisecondes

III.3.2 ECDSA

La tableau suivant représente les résultats obtenus après l'exécution du protocole cryptographique ECDSA par rapport au temps écoulé pendant la génération des clés, de signature, et de vérification de la signature en utilisant les différentes courbes elliptiques 160, 192, 224 , 256 bits.

Taille de la clé / Temps de calcul	Gen_Public_key1	Signature	Vérification
160 bits	1093	1223	1236
192 bits	1777	2001	2136
224 bits	2723	3027	3245
256 bits	4410	4790	5166

Tableau 10: Temps d'exécution d'ECDSA en millisecondes

III.3.3 ECIES

Le tableau suivant représente les résultats obtenus après l'exécution du protocole cryptographique ECDSA par rapport au temps écoulé pendant la génération des clés , de chiffrement, et de déchiffrement en utilisant les différentes courbes elliptiques 160, 192, 224 , 256 bits.

Taille de la clé / Temps de calcul	Gen_public-key_Alice	Gen_public-key_Bob	Chiffrement	Déchiffrement
160 bits	1055	1097	1057.004	1057.004
192 bits	1783	1785	1780.004	1781.004
224 bits	2718	2716	2717.004	2713.004
256 bits	4392	4390	4388.004	4387.004

Tableau 11: Temps d'exécution d'ECIES

III.3.3 Comparaison Hybride AES + ECDH vs. ECIES

Taille_clé	Protocole	Gen_clé		Chiffrement	Déchiffrement
192 bits	**Hybride**	**ECDH**	5292	4754	5704
		AES	8.10^{-3}		
	ECIES	1783^{-3}		1780.004	1781.004
256	**Hybride**	**ECDH**	13125	5464	6604
		AES	12.10^{-3}		
	ECIES	4392		4388.004	4387.004

Tableau 12: Comparaison temps d'exécution AES+ECDH / ECIES

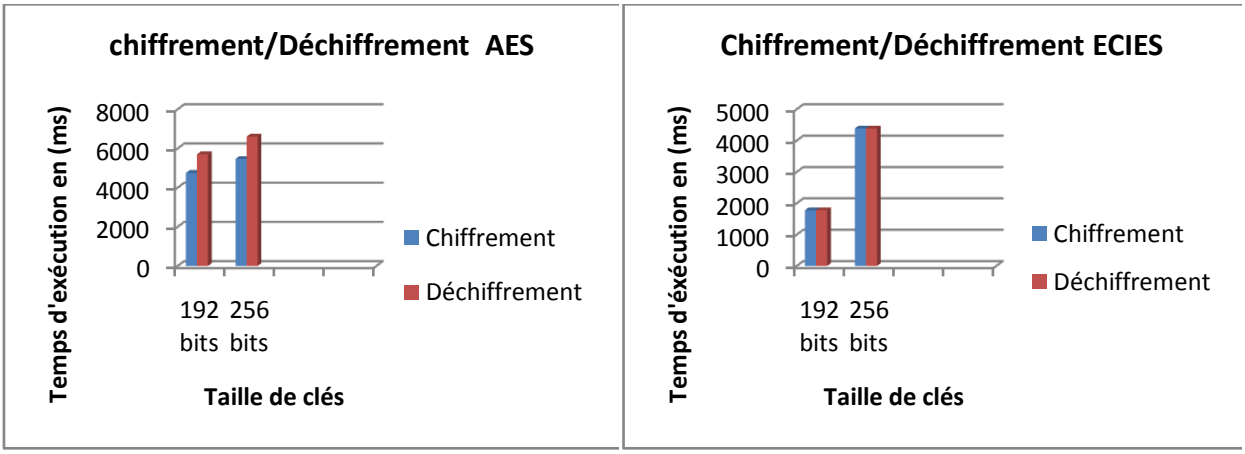

Figure 20:Chiffrement/Déchiffrement AES vs. ECIES

III.4 Discussion des résultats

La problématique principale et importante dans les appareils de l'IdO et les RCSFs est sans doute l'énergie, la mémoire et le temps de calcul et la sécurisation des données. Le défi majeur dans ce cas consiste à garantir le compromis entre un bon niveau de protection, un moindre coût et une meilleure considération des particularités du réseau.

Dans notre implémentation nous sommes concentrés uniquement à l'évaluation des temps de calcul lors de génération de clés publiques/privés, signature et vérification de la signature, chiffrement et déchiffrement. D'après les tableaux 9, 10 et 11, dans la phase de génération de clés on observe que le temps écoulé est presque le même pour ECDH, ECDSA, ECIES. Les résultats du tableau 10 montrent que le temps écoulé pendant la vérification de la signature est plus grand que le temps écoulé lors de la signature du message quelques soit la courbes elliptique utilisée. Dans le tableau 11, on observe que le temps écoulé lors du chiffrement du message est presque le même (on peut dire est égale) au temps écoulé lors de son déchiffrement. Le tableau 12, qui illustre les résultats obtenus après la simulation du chiffrement hybride AES + ECDH, et le protocole ECIES, on observe que le temps écoulé pendant la phase de génération de clés lors de l'utilisation d'AES est plus grand que le temps écoulé pendant la génération de clés d'ECIES, et à chaque fois qu'on augmente la taille de la clé utilisée, le temps écoulé augmente aussi.

Et on remarque que le temps écoulé pendant la phase du déchiffrement est plus grand que le temps écoulé lors du chiffrement lors de l'utilisation d'AES quel que soit la taille de la clé utilisée. On conclue que le protocole ECIES prend moins de temps d'exécution par rapport au protocole hybride (AES+ECDH).

D'après les résultats obtenus, on peut dire que le protocole ECIES est le protocole le mieux adaptable pour les appareils de l'IdO et les RCSFs grâce à sa faible exigence de ressources en termes de temps d'exécution.

IV. D'autres travaux réalisés

Plusieurs travaux ont été réalisés sur la comparaison entre RSA et ECC sur les smart cartes et Raspberry.

IV.1 Comparaison ECC vs. RSA dans les Smart Card (Java Card)

IV.1.1 C'est quoi une Java Card ?

Java Card est une petite plate-forme Java conçue pour permettre aux applications Java de s'exécuter sur de petits périphériques de mémoire tels que des cartes à puce. Conçu pour être sécurisé (avec un pare-feu d'applet, encapsulation de données et cryptographie) et portable, il est même utilisé sur des périphériques aussi petits que des cartes de guichet automatique. Il permet à plusieurs applications d'être sur une seule carte, avec la possibilité d'ajouter des applications après que l'utilisateur final ait déjà la carte [59].

IV.1.2 Expérimentation

Dans [54] [55], on a effectué une étude sur la comparaison des performances de RSA et ECC en termes de temps de génération de clés, chiffrement, déchiffrement, signature et vérification de la signature. Les résultats sont présentés ci-dessous :

Taille de clé	160 bits	224 bits	256 bits
RSA & RSA-DS	436.87	3755.04	17378.4
ECIES & ECDSA	21.93	24.22	24.79

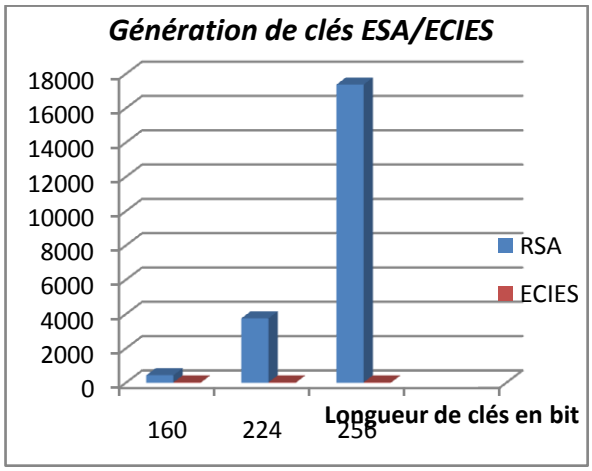

Figure 21:Génération de clés RSA et ECIES en (ms)

Taille de clé RSA	Taille de clé ECC	RSA		ECIES	
		Chiffrement	Déchiffrement	Chiffrement	Déchiffrement
1024 bits	**160 bits**	2.68	10.11	5.68	8.6
2048 bits	**224 bits**	4.2	6.32	14	17.3
3072 bits	**256 bits**	5.12	196.2	18	23.65

Tableau 13: Temps de chiffrement et déchiffrement RSA vs. ECIES en (ms)

Les résultats sont représentés dans les deux graphes suivants :

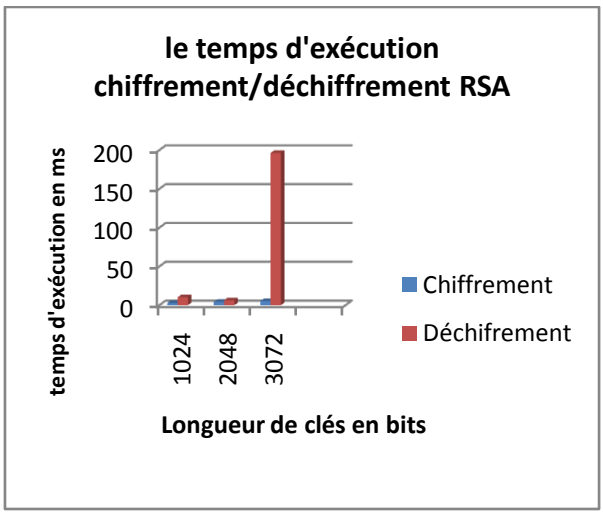

Figure 23:Chiffrement/Déchiffrement RSA

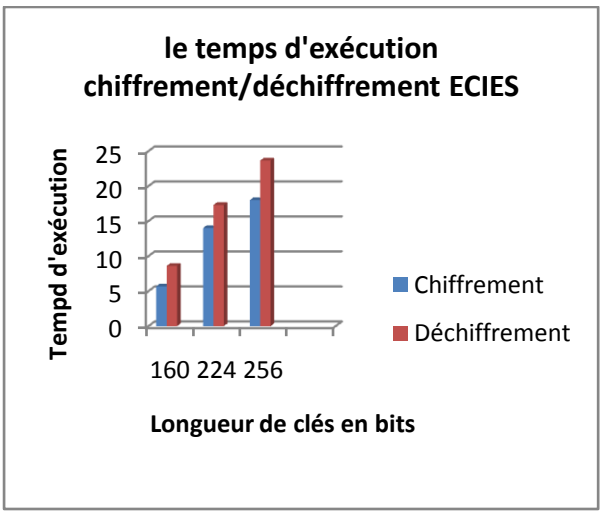

Figure 22:Chiffrement/Déchiffrement ECIES

Taille de clé RSA	Taille de clé ECC	RSA-DS		ECDSA	
		Signature	Vérification	Signature	Vérification
1024 bits	**160 bits**	75.19	4.67	36.82	38.08
2048 bits	**224 bits**	152.45	9.63	42.15	45.67
3072 bits	**256 bits**	228.07	16.62	55.65	58.33

Tableau 14: Temps d'exécution RSA-DS vs. ECDSA en (ms)

Les résultats sont représentés dans les deux graphes suivant :

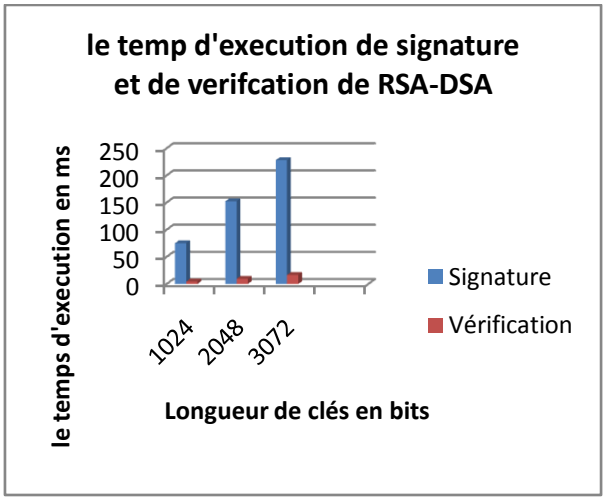

Figure 25:Signature et vérification RSA-DS

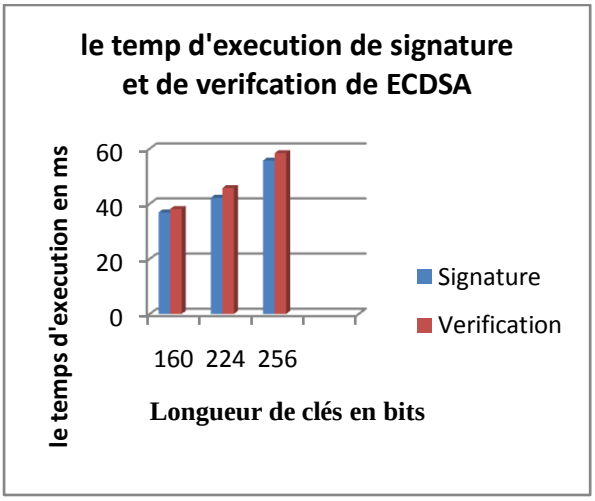

Figure 24:Signature et vérification ECDSA

IV.1.3 Discussion des résultats

Dans cette section, nous discutons les résultats expérimentaux en appliquant les cryptosystemes RSA, ECIES, ECDSA. La figure 21 montre le temps de calcul de RSA et RSA-DS pour la génération de clés de longueur 1024, 2048, 3072 bits avec les clés ECIES et ECDSA de longueur 160, 224 et 256 bits, correspondant à un niveau de sécurité symétrique de 80, 112, 128 bits respectivement.

La simulation montre une génération de clés plus rapide pour ECIES et ECDSA. Les clés publiques ECIES et ECDSA sont des points sur la courbe, et les clés privées sont générées au hasard, cela leur donne un avantage pour générer à la fois des clés dans un temps très court.

Le tableau 13 illustre le temps du chiffrement et du déchiffrement pour RSA (1024, 2048, 3072 bits) et ECIES (160, 224, 256 bits).Sur la base de ces résultats, le temps de chiffrement de l'algorithme RSA est légèrement inférieur au temps de chiffrement de l'algorithme ECC, tandis que l'algorithme de déchiffrement de RSA est extrêmement supérieur à l'algorithme ECC.

Le tableau 14 indique le temps nécessaire pour signer et vérifier une signature RSA-DS (1024, 2048, 3072 bits) et une signature ECDSA (160, 224, 256 bits).Les résultats obtenus montrent que le temps nécessaire pour générer une signature RSA-DS est plus grand que le temps nécessaire pour générer une signature ECDSA. Tandis que la vérification d'une signature RSA-DS nécessite moins de temps que la vérification ECDSA.

Dans une autre étude de T. Abdurahmonov, Eng-ThiamYeoh, Helmi Mohamed Hussain[56], réalisée en 2011, il existe une comparaison entre les différentes longueurs de clés de l'algorithme RSA et de l'algorithme ECDSA [56]. Cette comparaison permet de déterminer quels algorithmes ont un niveau de sécurité supérieur. On a constaté que, dans le même niveau de sécurité, ECDSA utilise une clé de longueur extrêmement inférieure à celle de RSA. Par exemple, la clé de longueur 1024 bits de RSA offre le même niveau de sécurité avec des algorithmes ECC de 163 bits, de sorte qu'il est plus efficace de l'utiliser pour une carte à puce.

IV.2 Comparaison RSA vs. ECC dans Raspberry Pi

IV.2.1 Raspberry Pi

Le Raspberry Pi est un ordinateur (mini-ordinateur) dont les particularités sont la très petite taille (la taille d'une carte de crédit) et le prix modique (25-30 euros). Il a été créé par l'anglais David Braben, dans le cadre de sa fondation Raspberry Pi, dans le but d'encourager l'apprentissage de la programmation informatique. Pour la petite histoire, *raspberry* signifie *framboise* en anglais. Le Raspberry Pi rappelle quelque peu l'Arduino, un circuit imprimé dont les plans sont publiés sous licence libre sur lequel se trouve un microcontrôleur programmable et objet fétiche des partisans de l'*open hardware* [57].

IV.2.2 Caractéristiques techniques :

- Taille : 85.60 mm × 53.98 mm.
- Poids : 45 gr.
- Processeur : 700 MHz ARM1176JZF-S core (ARM11) .
- Système sur puce (Soc) : BroadcomBCM2835.
- Processeur graphique (GPU) : décodeur Broadcom Video Core IV, API logicielle vidéo OpenGL ES 2.0, MPEG-2 et VC-1, décodage vidéo 1080p30 h.264/MPEG-4 AVC.
- Mémoire (SDRAM) : 256 Mo *[Modèle A]* ou 512 Mo *[Modèle B]]* partagée avec le processeur graphique.
- Ports USB 2.0 : 1 *[Modèle A]* ou 2 *[Modèle B]*.

- Sortie vidéo : RCA Composite (PAL et NTSC) et HDMI (rev 1.3 & 1.4).
- Sortie audio : 3.5 mm jack, HDMI.
- Unité de lecture-écriture de carte mémoire : SDHC / MMC / SDIO.
- Réseau : 1 port réseau Fast Ethernet (10/100 Mbits/s) sur le *[Modèle B]]* uniquement.
- Périphériques bas niveau : 8 × GPIO, UART, bus I²C, bus SPI .
- Besoin en alimentation : 5 volt via MicroUSB ou GPIO ; 300 mA (1.5 W) *[Modèle A]* ou 700 mA (3.5 W) *[Modèle B]*.

IV.2.3 Expérimentation :

Dans [58], on a simulé les algorithmes cryptographiques RSA et ECDSA sur une plateforme Raspberry. Les résultats sont présentés ci-dessous :

	Temps (Second)
RSA	**52.87**
ECDH	**2.376**

Tableau 15: Temps d'échange de clés RSA et ECDH en second

	Signature	**Vérification**
RSA	**233.11**	**5.043**
ECDSA	**11.702**	**13.719**

Tableau 16: Temps de génération de signature et de vérification RSA et ECDSA en ms

IV.2.4 Discussion des résultats :

Le tableau 15 illustre les couts en temps de génération de clés asymétriques. D'après ces résultats, nous remarquons que le temps écoulé pour générer les clés asymétriques de RSA est plus grand que le temps écoulé pour générer les clés ECC. La génération de clés ECC est plus rapide que l'algorithme RSA. Le tableau 16 illustre le temps nécessaire pour signer et vérifier un message en utilisant respectivement des clés 1024 bits pour RSA et de 112 bits pour ECDSA. Le graphe suivant indique que la meilleure performance dans Raspberry Pi est ECDSA. En ce qui concerne RSA il obtient les meilleurs résultats en matière de vérification, mais il est clair qu'ECDSA est plus rapide que RSA pour la signature numérique.
Les résultats sont représentés sous forme d'un graphe dans la figure suivante :

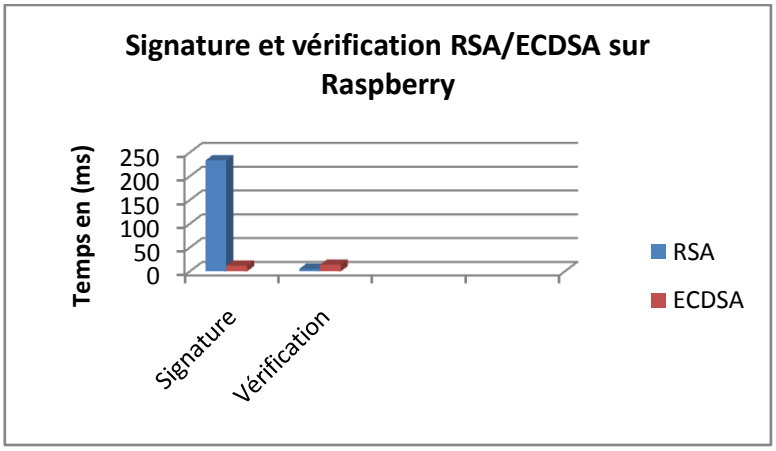

Figure 26:Temps de génération de signature et de vérification RSA et ECDSA sur Raspberry Pi en ms

V. Conclusion

Dans ce chapitre nous avons présenté les concepts de base des courbes elliptiques, puis nous avons présenté quelques protocoles cryptographiques utilisant les courbes elliptiques et nous avons discuté les résultats de simulation de ces algorithmes sur une carte Arduino et nous les avons comparés à d'autres travaux effectués par d'autres chercheurs sur les différents dispositifs de l'IdO. Nous avons conclu que :

- Dans les algorithmes de génération / échange de clés, ECDH est meilleur que RSA.
- Dans les algorithmes de chiffrement / Déchiffrement, ECIES est meilleur que RSA.
- Dans les algorithmes signature / vérification, ECDSA est meilleur pour la signature que RSA, tandis que pour la vérification, RSA est meilleur. En moyenne, ECDSA est meilleur pour les dispositifs de l'Internet des Objets et les RCSFs.

Conclusion générale

L'Internet a connu une mutation de l'Internet classique vers l'Internet des Objets où la possibilité de fusionner parfaitement le monde réel et le monde virtuel, grâce au déploiement massif de périphériques intégrés intelligents, ouvre de nouvelles orientations intéressantes pour la recherche et l'industrie.

La sécurité devient de nos jours une préoccupation majeure pour les objets connectés à internet (téléphone, caméra, PC, capteurs/actuateurs, réfrigérateurs, véhicule, etc.). De plus, l'IdO posera plusieurs nouveaux problèmes liés à l'utilisation efficace des ressources (énergie, stockage, calcul, transmission) dans les objets à faible capacité de ressources. Dans ce mémoire nous nous sommes intéressés au problème lié à la sécurité de l'Internet des Objet, dans lequel nous avons effectué une étude générale sur les vulnérabilités et les attaques que l'IdO rencontre, puis nous avons abordé les différentes solutions proposées en particulier la cryptographie des courbes elliptiques.

Notre implémentation consiste à simuler les différents protocoles cryptographiques basés sur les courbes elliptiques(ECDH, ECDSA, ECIES) sur une carte Arduino et calculer les temps écoulés pendant la génération de clés, chiffrement, déchiffrement, signature et vérification de la signature, puis nous avons analysé et comparé les résultats de quelques travaux réalisés sur RSA vs.ECC sur d'autres plateformes (Java Cards, Raspberry Pi).

Les résultats obtenus montrent que la cryptographie des courbes elliptiques est la meilleure solution pour assurer la sécurité de l'Internet des Objets.

Bibliographie

[1] Christophe Baland, Damien Cauquil, Thomas Gayet, Julia Juvigny, Renaud Lifchitz, Nha-Khanh Nguyen , la sécurité de l'Internet des Objets, livre blanc.

[2] Cluster of European Research Projects on the Internet of Things, "Vision and Challenges for Realising the Internet of Things", March 2010.

[3] Yacine Challal. Sécurité de l'Internet des Objets : vers une approche cognitive et systémique. Réseaux et télécommunications [cs.NI]. Université de Technologie de Compiègne, 2012.

[4] Yassine HADDAB Professeur à l'Université de Montpellier, Introduction à l'internet des objets (IdO – IoT).

[5] Imad Saleh Laboratoire Paragraphe, Université Paris 8. Internet des Objets (IdO) : Concepts, Enjeux, Défis et Perspectives.

[6] Mr Hidjeb Ali, implémentation d'un protocole d'élection d'un serveur d'authentification dans l'internet des objets, Mémoire de fin de Cycle Master 2 Informatique Professionnel Option: ASR Administration et Sécurité des Réseaux, Université Abderrahmane Mira de Bejaïa.

[7] https://www.leblogduhacker.fr/la-securite-dans-internet-des-objets/

[8] CHALLAL Yacine, réseaux de capteurs sans fil version 1.

[9] Mr ABANE Amar, mise en œuvre des concepts NDN et IoT dans le domaine de la domotique 2016, en vue de l'obtention du diplôme de master 2 en Informatique, Spécialité : Réseau, Mobilité et système embarqué.

[10] Mlle CHALAL Lina et M. SIROUAKNE Slimane, Gestion des clés dans l'internet des objets, Master en informatique, Spécialité : Réseaux et Systèmes Distribués.

[11] Mlle BRIK Ouardia, Mlle CHOUGGAR Melissa, Proposer un schéma de gestion de clés dynamiques dans un réseau de capteurs sans fil mobile, en vue de l'obtention du diplôme de master 2 en Informatique, Spécialité : Conduite de Projet Informatique.

[12] https://www.riskinsight-wavestone.com/2016/11/objets-connectes-4-dimensions-de-securite/

[13] https://fr.scribd.com/doc/47361726/Les-Objets-Intelligents-Veille-Technologique

[14] Dave Evans, Livre blanc : L'Internet des Objets, Comment l'évolution actuelle d'Internet transforme-t-elle le monde ?

[15] http://www.smartgrids-cre.fr/index.php?p=objets-connectes-technologies

[16] (IJACSA) International Journal of Advanced Computer Science and Applications, *Vol. 7, No. 11, 2016* 252 | Page www.ijacsa.thesai.org Constraints in the IoT: The World in 2020 and Beyond.

[17] https://www.orange-business.com/fr/blogs/securite/les-5-minutes-du-professeur-audenard/les-5-mins-du-professeur-audenard-episode-14-menace-vulnerabilite-et-impact

[18] https://www.globalsign.fr/fr/blog/cinq-cyberattaques-classiques-dans-l-iot/

[19] https://datafloq.com/read/5-Security-Vulnerabilities-Looming-Internet-Things/2137

[20] https://www.itworldcanada.com/article/top-10-iot-vulnerabilities-of-2018/413433

[21] https://www.securiteinfo.com/conseils/introsecu.shtml

[22] Techniques avancées de sécurité et de cryptographie, Mastère Recherche2 Faculté des Sciences de Monastir 2015/2016

[23] https://www.researchgate.net/publication/277718176_Cyber_Security_and_the_Internet_of_Things_Vulnerabilities_Threats_Intruders_and_Attacks

[24]https://www.researchgate.net/publication/324149744_A_Comprehensive_IoT_Attacks_Survey_based_on_a_Building-blocked_Reference_Mode

[25] https://www.globalsign.fr/fr/blog/cinq-cyberattaques-classiques-dans-l-iot/

[26] https://www.researchgate.net/publication/304408245_Internet_of_Things_Security_vulnerabilities_and_challenges

[27] Security Attacks in IoT: A Survey, auteur JyotiDeogirikar , Dept of Computer Engineering; AmarsinhVidhate, Dept of Computer Engineering organization R.A.I.T

[28] https://conseils.telus.com/securite-des-ti/menaces-courantes-securite-informatique_1/

[29] DOUMI Abdelmoumain, La sécurité des communications dans les réseaux de capteurs sans fil, en vue d'obtention de master académique, 2017/2018

[30] MESSAI Mohamed Lamine, Sécurité dans les réseaux de capteurs sans fil, mémoire magistère en informatique, option réseaux et systèmes distribués, 2007/2008.

[31] BENHAMED Khelifa, Surveillance distribuée pour la sécurité d'un réseau de capteurs sans fil, thèse de doctorat, spécialité informatique, option : sécurité informatique, 2010/2011.

[32] https://cours-informatique-gratuit.fr/dictionnaire/vpn/

[33] YANBO Shou, cryptographie des courbes elliptiques et tolérance aux pannes dans les réseaux de capteurs, pour obtenir le grade de docteur de l'université de franche – compté.

[34] Melle ADJTOUTAH Sabrina, CHELOUCHE Ouidad, sécurité contre l'attaque Sybil dans les réseaux de capteurs sans fil, en vue d'obtention du diplôme master recherche en informatique, réaliser par 2012/2013, option réseaux et systèmes distribués

[35] Melle AIT SI SLIMANE Hayat, Melle OUARGLI Fella, Optimisation des calculs cryptographiques dans un réseau de capteurs sans fil, en vue de l'obtention du diplôme de master en informatique, option : réseaux, mobilité et systèmes embarqués ,2017/2018.

[36] https://www.maison-travaux.fr/maison-travaux/domotique/maison-connectee-securite-optimale-fp-196021.html

[37] https://desgeeksetdeslettres.com/hardware/9-aides-memotechniques-securiser-materiel-a-domicile

[38] https://www.orange-business.com/fr/blogs/securite/bonnes-pratiques/6-conseils-pour-securiser-l-internet-des-objets

[39] https://www.iiro.eu/securiser-objets-connectes/

[40] https://www.maison-connectee.eu/securiser-objets-connectes/

[40] http://www.univ-tebessa.dz/fichiers/master/master_1788.pdf

[41] https://link.springer.com/article/10.1007/s00521-018-3545-7

[42] Ian F. Blake, Gadiel Seroussi, Nigel P. Smart, "Advances in Elliptic Curve Cryptography", London Mathematical Society Lecture Note Series (No. 317), April 2005.

[43] https://www.sentryo.net/fr/comment-se-proteger-dune-attaque-reseau-par-force-brute/

[44] http://www.livetechindia.com/blogs/blog.php?id=3

[45] https://www.rs-online.com/designspark/pourquoi-et-comment-securiser-liot-fr

[46] https://phgarin.wordpress.com/2008/07/28/menace-vulnerabilite-risque/

[47] https://www.gotronic.fr/art-carte-arduino-uno-12420.htm

[48] http://www.mon-club-elec.fr/pmwiki_reference_arduino/pmwiki.php?n=Main.Micros

[49] S. Agrawal and D. Vieira, “A Survey on Internet of Things : Security and Privacy Issues,” Abakós, 2013.

[50]https://www.google.com/search?q=debit+de+la+zigbee+en+mbit/s&source=lnms&tbm=isch&sa=X&ved=0ahUKEwixxszKgvPiAhXJKewKHV8PCggQ_AUIECgB&biw=1242&bih=524#imgrc=qCEYEmM_MB7iEM:

[51] http://www.univ-setif.dz/Tdoctorat/2015/SCIENCES/Boudries.pdf

[52] Stockebrand, “IPv6 Address Basics,” in IPv6 in Practice: A Unixers Guide to the Next Generation Internet, Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 21–34.

[53] http://www.smartgrids-cre.fr/index.php?p=objets-connectes-cybersecurite

[54] M. Savari and M. Montazerolzohour, "All about encryption in smart card," Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), Kuala Lumpur, 2012, pp. 54-59

[55] Ehab M. Alkhateeb, Mohammad A. Alia, Adnan A. Hnaif, Amman, Jordan, Faculty of Science and Information Technology: Al Zaytoonah University of Jordan,” The Generalised Secured Mobile Payment System Based on ECIES and ECDSA”, *2015*

[56] T. Abdurahmonov, MH Helmi, YE Thiam, «Besoins en informations personnelles du système d'information mondial», Conférence internationale sur la recherche scientifique et sociale (CSSR 2010), Kuala Lumpur, Malaisie, 2010, p. 1197-1202.

[57] https://lea-linux.org/documentations/Pr%C3%A9sentation_du_Raspberry_Pi

[58] M. El-Haii, M. Chamoun, A. Fadlallah and A. Serhrouchni, "Analysis of Cryptographic Algorithms on IoT Hardware platforms," 2018 2nd Cyber Security in Networking Conference (CSNet), Paris, 2018.

[59] https://www.computerhope.com/jargon/j/java_card.htm