République Algérienne Démocratique et Populaire
Université Abou Bakr Belkaid– Tlemcen
Faculté des Sciences
Département d'Informatique

Mémoire de fin d'études

pour l'obtention du diplôme de Master en Informatique

Option : *Réseaux et Systèmes Distribués (R.S.D)*

Thème

Etude de l'authentification d'une source de diffusion dans le contexte de l'Internet des Objets

Réalisé par :

- **AMIMER** HANANE
- **CHEKROUN** FADIA

Présenté le 03 juillet 2017 devant la commission d'examination composée de MM.

- **BEKARA** *Chakib* (Encadreur)
- **LEHSAINI** *Mohammed* (Examinateur)
- **BENMOUNA** *Youcef* (Examinateur)

Année universitaire: 2016-2017

Remerciement

Enfin Hamdelillah …

Nous remercions DIEU le tout puissant de nous avoir donné le courage, la patience et la force morale et physique afin de pouvoir accomplir ce travail.

On tient tout d'abord à remercier notre encadreur M. « BEKARA Chakib » de nous avoir acceptés pour effectuer ce projet de fin d'études, pour son temps précieux, ses conseils et sa disponibilité tout au long du déroulement de ce travail.

- *Nous exprimons également nos remerciements à les membres du jury M. « LEHSAINI Mohamed » et M. « BENMOUNA Youcef », nos remerciements les plus vifs pour avoir acceptés d'honorer par leur jugement notre travail.*

Nous adressons nos remerciements à tous les professeurs, pour leurs conseils et leurs critiques qui ont guidé nos réflexions durant nos recherches.

Nous souhaitons exprimer nos profondes gratitudes à nos parents qui nous ont supportées tout au long de notre projet, ainsi que toute la famille, les amis pour leur soutien indéfectible.

A toutes les personnes qui nous ont aidées nous présentons nos remerciements, nos respects et nos gratitudes.

Dédicace

Je dédie ce mémoire

A mes chers parents ma Mère et mon Père pour leur patience, leur amour, leur soutien et leur encouragements

A mon Frère et sa femme

A mes Sœurs et leurs Époux

A mes Neveux et Nièces

A toutes ma Famille

A ma chère Binôme Fadia

A toutes mes Amies

Hanane

Dédicace

Je dédie ce modeste travail a:

A Mon Mari,

A Mon Fils LOUEY

A Mon Cher Papa ; Aucun Mot Ne Saurait Exprimer Ma Gratitude, Mon Amour Et Mon Profond Respect.

A Ma Chère Maman ; La Plus Douce Des Mamans.

A Mon Frères Et Mes Sœurs : REDA ET FATIMA KAWTHER.

A Mes Chers Beaux-Parents,

A Ma Binôme Et Meilleure Amie ''HANANE''

A Tous Mes Amis

A Toutes Les Personnes Qui Ont Contribue A La Réalisation De Ce Travail,

Veuillez Accepter Tous Mes Remerciements Et Gratitude.

FADIA

Sommaire

Chapitre III :l'authentification d'une source de diffusion

dans l'Internet des Objets

Chapitre IV : Réalisation et simulation

Introduction générale

Internet a changé notre mode de vie au cours des 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. Le Web 2.0, les réseaux sociaux et l'accès Internet mobile ne sont que quelques-uns des développements actuels dans ce contexte. 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[1], ajoutant ainsi une nouvelle dimension au monde de technologie d'information et 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 auxquels la communauté fait face dans la vie de tous les jours[2].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 [3].En fait, l'un des éléments importants dans le paradigme IoT est les réseaux de capteurs sans fil (WSN). La connexion entre WSN et d'autres éléments IoT a l'avantage de construire des systèmes d'information hétérogènes pouvant collaborer et fournir des services communs [4].Les réseaux de capteurs sans fil (WSNs) 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, calcule, mémoire, énergie) de ces objets, rend l'IdO vulnérable (niveau objets, réseaux, applications) à une variété

d'attaques potentielles, pour lesquels les solutions de sécurité conventionnelles sont mal adaptés [5].

Les exigences de sécurité dans l'environnement IoT ne sont pas différentes des autres systèmes TIC. Par conséquent, assurer les services et la sécurité IoT nécessite de maintenir la valeur intrinsèque la plus élevée des objets tangibles et intangibles (services, informations et données).

L'authentification d'une source de diffusion est l'un des services de sécurité critique dans l'IdO, notamment pour ce qui est de la mise à jour logiciel, l'échange d'information de routage (niveau locale, globale), dissémination de requêtes dans tout le réseau, et en générale dans toute application ou protocole nécessitant l'envoi d'une données simultanément à un ensemble de récepteurs (broadcast ou multicast). Il existe deux approches principales pour l'authentification d'une source de diffusion [6] : les approches basées sur l'asymétrie des clés cryptographique entre l'émetteur (source de diffusion) et les récepteurs (ex : les signatures numériques)réalisant une authentification immédiate, et les approches basées sur l'asymétrie de temps entre l'émetteur et les récepteurs (ex : techniques basées sur µTESLA) réalisant une authentification différée. Cependant, ces approches sont vulnérables aux attaques de déni de services (DoS) par épuisement de ressources : 1) pour l'authentification basée sur la signature, un attaquant peut injecter des paquets de diffusion faux pour forcer les nœuds de capteurs à effectuer des vérifications de signature coûteuses, 2) ou le stockage/dissémination de faux paquets dans le cas d'une authentification basée sur µTESLA.

Dans ce mémoire on s'est intéressé à l'étude et l'implémentation du protocole µTESLA, dans le contexte de ldO, où les objets seront des capteurs sans-fil supportant la une version légère de la pile de communication IPv6, et l'implémentation sera réalisée en utilisant l'OS Contiki et son simulateur réseau associé COOJA.

Le manuscrit s'articule autour de quatre chapitres en plus d'une introduction générale et d'une conclusion générale.

Le premier chapitre, est une présentation générale de l'IdO et ces utilisations les plus répondues, son architecture, ses avantages et inconvénients.

Dans le deuxième chapitre, nous listons les attaques qui menacent l'IdO et les services de sécurité adéquats faisant face à ces attaques.

Dans le troisième chapitre nous abordons la problématique de l'authentification d'une source de diffusion, et nous décrivons trois solutions d'authentification existantes basées sur le protocole µTESLA.

Le chapitre 4 décrit la phase conception, l'environnement et les outils utilisés, ainsi que l'implémentation du protocole d'authentification µTESLA, et donne les tests de performances

Nous terminons notre manuscrit par une conclusions générale, ainsi que les perspectives futures pouvant faire suite à notre travail

Chapitre I
Introduction Internet des Objets

1 Introduction :

Internet des Objets (IdO) ou (IoT en anglais) envisage un avenir dans lequel les entités numériques et physiques peuvent être liées, au moyen de technologies d'information et de communication (TIC)appropriées, pour permettre une nouvelle classe d'applications et de services.

Le concept de L'Internet des Objets vise à proposer des solutions basées sur l'intégration des technologies de l'information, qui se réfèrent au matériel et aux logiciels utilisés pour stocker, récupérer et traiter les données et les technologies de communication, y compris les systèmes électroniques utilisés pour la communication entre individus ou groupes.

Le but de ce chapitre est de présenter l'IdO et ces utilisations les plus répondu puis, ses avantages, ses limites, et ses défis. Nous nous intéressons notamment en matière de contraintes de ressources des objets.

2 Définition de l'IdO:

l'Internet des Objets est une infrastructure mondiale pour la société de l'information, qui permet de disposer de services évolués en interconnectant des objets (physiques ou virtuels) grâce aux technologies de l'information et de la communication interopérables existantes ou en évolution [7].Ainsi, l'IdO est en fait une combinaison d'une poussée technologique et d'une attraction humaine pour une connectivité de plus en plus croissante avec tout ce qui se passe dans l'environnement.

L'IdO est activé par un certain nombre de technologies différentes comme les systèmes d'informations de détection telles que les réseaux de capteurs(WSNs), des dispositifs de lecture RFID (code à barres), de systèmes de localisation et de communication courte portée basés sur la communication machine à machine (M2M), à travers le réseau internet pour former un réseau plus grand et plus intelligent[8]comme montre La figure1.1 ci-dessous le concept d'IdO et la connexion entre tous les composants impliqués.

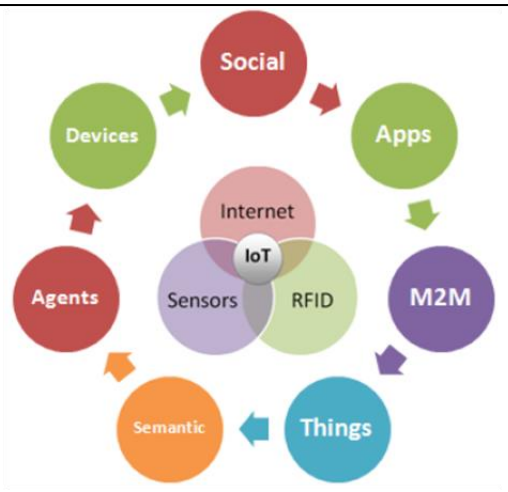

Figure I.1 : Composants Internet des Objets[3]

3 Historique de l'IdO :

- 1990 :Apparition des premiers objets connectés ,il s'agit de grille-pain, machines à café ou autres objets du quotidien[9].
- 2000 : Verront les premières expérimentations d'appareils connectés à Internet. Ils l'utilisent notamment pour consulter des informations de matière automatique notamment Ambient Orb vers 2002, LG est le premier industriel à parler sérieusement d'un appareil électroménager relié à internet[9].
- 2008 : À la fin de 2008, Atmel, Cisco, Intel, SAP, Sun Microsystems et d'autres entreprises ont fondé l'alliance corporative "IP for Smart Objects" (IPSO) pour promouvoir la mise en œuvre et l'utilisation de l'IP pour les périphériques à faible puissance tels que les capteurs radio, Les compteurs de consommation et autres objets intelligents. Plus précisément, le groupe de travail "IPv6 over Low Power Wireless Area Networks" (6LoWPAN) mis en place par Internet Engineering Task Force (IETF) s'attaque au problème du support d'IPv6 à l'aide de la norme de communication sans fil 802.15.4.[10].
- 2011 : L'IPV6 offre de nouvelles possibilités pour les objets connectés qui disposent de nouvelles plages d'adresses IP disponibles et attribuables[9].

- A la fin de l'année 2012, il y avait environ 8,7 milliards d'objets connectés dans le monde. Cisco estime que ce nombre atteindra les 50 milliards d'objets connectés en 2020.Exemples d'objets connectés[9].

4 Architecture de l'IdO :

L'architecture en couches doit être conçue de manière à satisfaire les exigences de diverses industries, entreprises, sociétés, instituts, gérants, etc. come montre la figure I.2 :

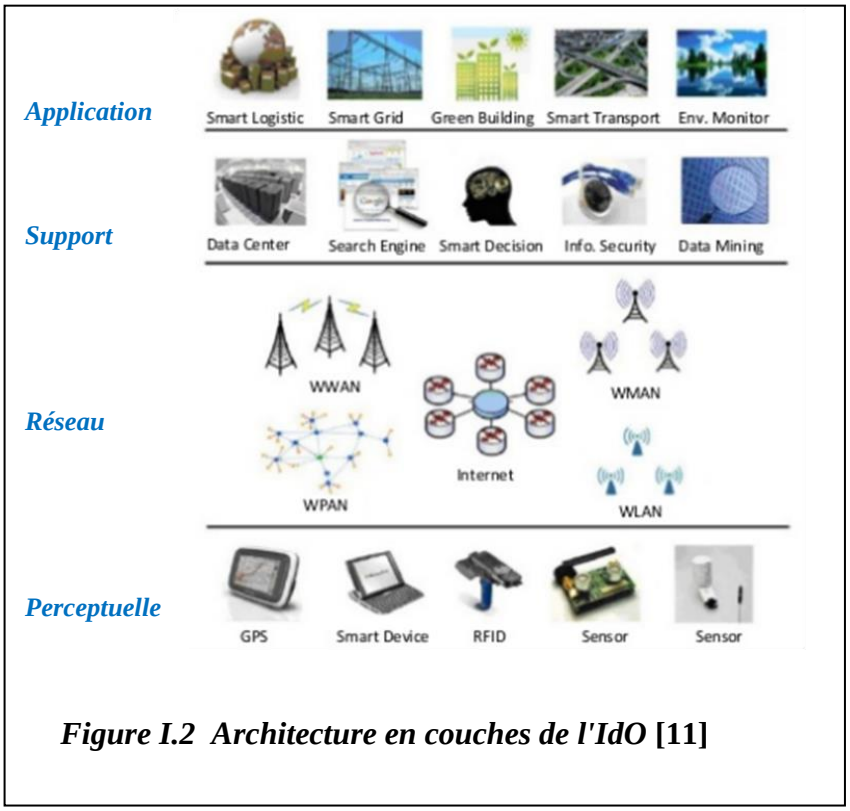

Figure I.2 Architecture en couches de l'IdO **[11]**

4.1 La couche perceptuelle :

également connue sous le nom de couche de reconnaissance ou d'identification, recueille toutes sortes d'informations par le biais d'équipements physiques et identifie le monde physique, les informations
comprennent les propriétés de l'objet, l'état de l'environnement, etc. Et les équipements physiques comprennent le lecteur RFID, différentes types de capteurs, GPS et autres équipements. Le principale composant de cette couche

sont les capteurs pour capturer et représenter le monde physique dans le monde numérique[11].

4.2 La couche réseau :

La couche réseau est responsable de la transmission fiable des informations qui repose sur plusieurs réseaux de base, Internet, réseau de communication mobile, réseaux de satellites, réseau sans fil, infrastructure de réseau et protocoles de communication, sont également essentiels à l'échange d'informations entre les périphériques[11].

4.3 La couche de support :

La couche de support mettra en place une plate-forme de support fiable pour la couche d'application, sur cette plate-forme de support, tous les types de puissances informatiques intelligentes seront organisés par réseau et cloud computing. Il joue le rôle de combiner la couche d'application vers le haut et la couche réseau vers le bas[11].

4.4 La couche d'application :

La couche d'application fournit les services personnalisés en fonction des besoins des utilisateurs. Les utilisateurs peuvent accéder à l'IdO via l'interface de la couche d'application à l'aide de la télévision, de l'ordinateur personnel ou de l'équipement mobile, etc[11].

5 Les domaines d'applications de l'Internet des objets :

Différents secteurs et domaines d'applications peuvent tirer profit de la vision de l'Internet des Objet, parmi lesquels :

5.1 E-Santé :

Le contrôle et la prévention sont deux des principaux objectifs des futurs soins de santé. Aujourd'hui, les gens ont la possibilité d'être suivi et surveillés

par des spécialistes même si le patient et le spécialiste ne sont pas au même endroit. Les applications d'affaires pourraient offrir la possibilité de services médicaux pour les patients, et les spécialistes, qui ont besoin d'informations pour procéder à leur évaluation médicale. Dans ce domaine, l'IdO rend l'interaction humaine beaucoup plus efficace car elle permet non seulement la localisation, mais aussi le suivi et la surveillance des patients. Fournir des informations sur l'état d'un patient rend l'ensemble du processus plus efficace, aussi les gens beaucoup plus satisfait. Les acteurs les plus importants dans ce scénario seront les hôpitaux et les instituts publics et privés [12].

5.2 Ville intelligente :

Ville intelligente est un nouveau modèle de développement d'une ville utilisant de nouvelles technologies, telles que IoT, l'infonuagique (cloud computing) et l'analyse des *grandes* masses de *données*, pour stimuler le partage et la coordination de l'information dans un système urbain. L'IdO est un moyen important et l'un des outils de construction de la ville intelligente. La construction d'une ville intelligente dépend de nombreuses applications IdO pour différentes industries. Un grand nombre de projets de villes intelligentes offrent d'énormes opportunités, des entreprises d'intégration de systèmes, des entreprises d'agrégation et d'analyse de données et des opérateurs de télécommunications[13].

5.3 Industrie de Transport :

Les voitures, les trains, les autobus, les avions et les bicyclettes avancés sont équipés capteurs avancés, actionneurs à puissance de traitement accrue. Les applications dans l'industrie des moyens de transport incluent l'utilisation de objets intelligentes pour surveiller et rapporter divers paramètres de la pression, vitesse, vent, température, accélération, etc. [14].

5.4 Industrie des télécommunications :

l'IdO créera la possibilité de fusionner diverses technologies de télécommunication et créer de nouveaux services. Un exemple illustratif est l'utilisation de GSM,NFC (Near Field Communication), Bluetooth à faible

puissance ,Zigbee,Wifi faible puissance,WiMax, et réseaux de capteurs ainsi que la technologie de la carte SIM[14].

Figure I.2 : Domaines d'applications de l'IdO

5.5 Autonomie de vie :

Les applications et les services d''IdO auront un impact important sur les personnes fragiles et ou nécessitant une certaine assistance, en apportant un soutien au vieillissement de la population en détectant les activités de la vie quotidienne à l'aide de capteurs portables et ambiants, ainsi que la surveillance des maladies chroniques avec des capteurs de signaux vitaux corporels[14].

5.6 Smart energy :

IdO permet une grande variété de fonctions de contrôle et de surveillance d'énergie, avec des applications dans les appareils, la consommation d'énergie commerciale et résidentielle. IdO simplifie le processus de gestion de l'énergie tout en maintenant un faible coût et un niveau de précision élevé. Il aborde tous les points de la consommation d'une organisation à travers les périphériques , sa profondeur d'analyse et de contrôle fournit aux entreprises un moyen fort de gérant leur consommation pour le rasage des coûts et l'optimisation des résultats[15].

6 Avantages de l'IdO:

Il ya de nombreux avantages d'incorporer l'IdO dans nos vies, qui peuvent aider les individus, les institutions les entreprises et la société au quotidien. Les entreprises peuvent également tirer de nombreux avantages de l'IdO, notamment le suivi des biens et le contrôle des stocks , la sécurité et la capacité de suivre les consommateurs individuels (ex : électricité, gaz, eau) et de cibler ces consommateurs sur la base des informations fournies par les dispositifs intelligents déployés (ex : compteurs intelligents).

Les avantages de l'IdO s'étendent à tous les domaines de la vie. Voici certains des avantages que l'IdO :

Amélioration de la collecte de données :La collecte de données moderne souffre de ses limites et de sa conception pour une utilisation passive. Avec l'IdO, c'est tout l'environnement qui nous entoure qui peut être intégrer au monde numérique grâce à l'utilisation de capteurs et actionneurs pour pouvoir interagir avec l'environnement et le monde physique (collecte de données/informations, et agir sur l'environnement, etc.). L'IdO nous permet d'avoir une image précise et à granularité fine sur le monde réel.

Etendre la connectivité d'Internet et ses applications à notre environnement physique et aux objets du quotidien (électroménager, voitures, domotique, industrie, etc.). Ceci permet d'améliorer sensiblement les services fournis au quotidien ainsi que l'apparition de nouveaux services innovants.

7 Inconvénient de l'IdO:

- ✓ Sécurité : l'IdO crée un écosystème de périphériques constamment connectés qui communiquent sur des réseaux. Le système offre peu de contrôle malgré toutes les mesures de sécurité. Cela laisse les utilisateurs exposés à divers types d'attaquants et risques sécuritaire.
- ✓ Complexité : Certains trouvent les systèmes IdO complexes en termes de conception, de déploiement et de maintenance, étant donné qu'ils utilisent de multiples technologies et un grand nombre de nouvelles technologies hétérogènes.
- ✓ La flexibilité : Beaucoup s'inquiètent de la flexibilité d'un système IdO pour s'intégrer facilement à un autre. Ils s'inquiètent de se retrouver avec plusieurs systèmes conflictuels ou verrouillés.

8 Les défis de l'IdO:

Dans le concept de l'IdO, on peut trouver une pléthore de dispositifs connectés à l'Internet générant de ses quantités énormes de données. Ces données si analysées et utilisées correctement, pourront être une source d'information précieuse aux applications dites context-aware, qui suivant les informations collectés, fournirons le meilleur service ou le service le plus adéquat. Néanmoins, il y a des défis majeurs que l'IdO doit surmonter et faire face avant que l'IdO soit une réalité largement adoptée et approuvée :

8.1 Évolutivité :

Comme les objets de tous les jours se connectent à une infrastructure d'information globale, des problèmes d'évolutivité se posent à différents niveaux, notamment : la taille du système résultant, l'interconnexion entre un grand nombre d'entités, la possibilité de construire une contrepartie numérique pour toute entité et / ou phénomène dans le domaine physique, la nécessité de gérer des ressources hétérogènes.

8.2 Infrastructure du réseaux :

Les limitations de l'architecture Internet actuelle en termes de mobilité, de disponibilité, de gestion et d'évolutivité sont quelques-uns des principaux obstacles à l'IdO[14].

8.3 Hétérogénéité:

Les périphériques IdO sont déployés par différentes personnes / autorités / entités. Ces dispositifs ont des conditions de fonctionnement différentes, des fonctionnalités, des résolutions, etc. Ainsi, permettre une intégration transparente de ces appareils est un énorme défi. Le degré de complexité augmente de nombreux plis lorsque certains de ces simples dispositifs sont fusionnés pour former un réseau complexe[16] .

8.4 Interopérabilité:

Dans une application IdO, il existe de nombreux acteurs composés d'objets humains et non humains. Un acteur peut jouer plusieurs rôles en fonction des situations et de l'environnement actuels tels que les ressources disponibles dans l'application IdO, le fournisseur de données, le consommateur de données, le fournisseur de services, etc. L'interaction transparente entre les différents acteurs est cruciale pour envisager la vision d'IdO. L'interaction entre différents objets augmente, surtout lorsque chaque acteur est géré différemment[16] .

8.5 L'alimentation des objets:

Les techniques liées à la récolte d'énergie soulageront les dispositifs des contraintes imposées par les opérations de batterie, l'énergie sera toujours une ressource rare à manipuler avec précaution. De ce fait, la nécessité de concevoir des solutions qui tendent à optimiser la consommation d'énergie deviendra de plus en plus attrayante, que ce soit en terme de calcul, stockage ou transmission d'information.

8.6 Sécurité :

Dans le domaine de la sécurité les défis sont les suivants:[14]

- sécurisation de l'architecture de l'IdO : sécurité à garantir au moment de la conception et du temps d'exécution.

- identification proactive et protection de l'IdO contre les attaques arbitraires (DoS et DDoS, par exemple) et les abus.
- L'sidentification proactive et la protection de l'IdO contre les logiciels malveillants.
- Dans le domaine de la vie privée des utilisateurs, les défis spécifiques sont les suivants: le contrôle des renseignements personnels (confidentialité des données) et le contrôle de l'emplacement physique et des déplacements (intimité des lieux),Le besoin de technologies d'amélioration de la protection de la vie privée et les lois de protection pertinentes, Des normes, des méthodologies et des outils pour la gestion de l'identité des utilisateurs et des objets.
- Dans le domaine de la confiance, certains des défis spécifiques sont: Nécessité d'un échange facile et naturel de données critiques, protégées et sensibles par ex : Les objets intelligents communiqueront au nom des utilisateurs / organisations avec les services qu'ils peuvent faire confiance, et la confiance doit faire partie de la conception de l'IdO et doit être intégrée.

9 Conclusion :

L'Internet des objets est une nouvelle révolution de l'internet qui peut représenter le prochain grand bond en avant dans le secteur des technologies de l'information et de la communication (TIC). La possibilité de fusionner le monde réel et le monde virtuel, grâce au déploiement massif d'appareils embarqués, ouvre de nouvelles voies intéressantes pour la recherche et les affaires. Dans le chapitre suivant on va parler de la sécurité dans l'IdO, les principales attaques et les services de sécurité appropriées.

Chapitre II
Sécurité dans l'Internet des Objets

1 Introduction :

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 rendant de plus en plus autonomes.

Concernant la sécurité, l'IdO sera confronté à des défis plus critiques que ceux déjà posé dans l'Internet classique. En effet, l'IdO étend la connectivité jusqu'à l'environnement des objets via l'Internet traditionnel, le réseau mobile ,les réseau de capteurs et actionneurs etc., permettant ainsi une communication inter-objets et une interaction avec ces objets. Ainsi, plusieurs entités hétérogènes situées dans des contextes différents peuvent échanger des informations entre elles, ce qui aura comme conséquence immédiate la complication de la conception et du déploiement de mécanismes de sécurité efficaces, interopérables et évolutifs. Nous devrions accorder plus d'attention au problème de la sécurité dans l'IdO, notamment les services de la confidentialité, l'authenticité et l'intégrité des données, ainsi que le respect de la vie privée.

Dans ce chapitre nous allons illustrer les attaques visant l'internet des objets et les services de sécurité nécessaires contre ces attaques.

2 Les attaques visant l'Internet des Objets :

L'IdO est caractérisé par la présence d'objets le plus souvent miniaturisé, à contraintes de ressources et communicant principalement de façon sans-fil, tels que les réseaux de capteurs sans fil. Ces objets sont ainsi vulnérables aux attaques, et ceci est dû en grande partie du fait de la nature diffusée du support de transmission ainsi que la faible protection physique de ces objets. En outre, ces objets présentent une vulnérabilité supplémentaire car sont souvent placés dans un environnement hostile ou dangereux et ne sont pas physiquement protégés. Les acteurs d'attaque sont des personnes qui menacent le monde numérique ou physique. Ils pourraient être des pirates, des criminels, voire des gouvernements. Les attaques sont classées comme des attaques actives et des attaques passives.

2.1 Attaques passives :

La surveillance et l'écoute du canal de communication par des attaquants est connue sous le nom d'attaque passive. Le problème majeur dans ce type d'attaque est l'atteinte à la vie privée des personnes[17]. En fait, beaucoup d'informations nous concernant provenant d'objets connectés à nous ou nous entourant pourraient ainsi être facilement collectés.

2.2 Attaques actives :

Dans ce cas, Les attaquants surveillent, écoutent et modifient le flux de données dans le canal de communication. Dans ce qui suit un bref aperçu de ces attaques est présenté.

- ✓ L'attaque du trou de la base (sinkholeattack): Les attaques de Sinkhole fonctionnent généralement en rendant l'attaquant ou un nœud compromis particulièrement attrayant pour les nœuds du réseau, et exploitent pour cette fin les algorithmes de routage (en se déclarant proche de la destination par exemple). Ainsi, tous les données ou une grande partie envoyés par les objets, et transitant dans le réseau passeront à travers l'attaquant ou le nœud compromis[18].
- ✓ Déni de service :Il se traduit par l'échec des nœuds-suite à une action malveillante- à d'accéder aux services et/ou aux ressources auxquelles ils ont droit L'attaque DoS la plus simple tente d'épuiser les ressources disponibles pour le nœud victime (stockage, énergie, etc.), en envoyant des paquets inutiles, qu'il devra stocker/forwarder.. L'attaque DoS est destinée non seulement à la tentative de l'adversaire de subvertir, perturber ou détruire un réseau, mais aussi pour tout événement qui diminue la capacité d'un réseau à fournir un service[19].
- ✓ Sybil attack: Dans une attaque de type "Sybil attack",un nœud malveillant (attaquant ou nœud compromis), apparaîtra au reste du réseau comme un ensemble de nœuds avec des identifiants différents, et enverra des informations incorrectes dans le réseau, afin de perturber son fonctionnement[19].
- ✓ Attaque Jamming: une attaque bien connue dans les communications sans fil, qui consiste à occuper le canal radio en envoyant des informations inutiles sur la bande de fréquence utilisée. Ce brouillage peut être temporaire, intermittent ou

permanent, et résultera dans l'incapacité des nœuds légitime du réseau à envoyer et/ou recevoir des données [20].

- ✓ Tampering(Altération) : il est le résultat de l'accès physique au nœud par un attaquant. Le but sera de récupérer du matériel cryptographique comme les clés utilisées pour le chiffrement, ou autres informations sensible, ainsi que le chargement du nœud victime par un logiciel malveillant[20].

- ✓ Renvoi sélectif: un nœud malveillant joue le rôle de routeur , en refusant de transmettre certains messages, en les écartant tout simplement[20].

- ✓ Attaque du trou noir (black holeattack) :un nœud falsifie des informations de routage pour forcer le passage des données par lui. Plus tard; son seul objectif est alors, de ne rien transférer, créant ainsi un puit ou un trou noir dans le réseau[20].

- ✓ Epuisement : Consommer toutes les ressources énergétiques du nœud victime, en l'obligeant à effectuer des calculs ou à recevoir ou transmettre inutilement des données[20].Cette attaque peut être considérée comme une attaque de type DoS.

- ✓ Attaque d'inondation « HELLO »: de nombreux protocoles de routage utilisent le paquet "HELLO" pour découvrir les nœuds voisins et ainsi établir une topologie du réseau. L'attaque la plus simple pour un attaquant consiste à envoyer une inondation de tels messages pour inonder le réseau et empêcher les autres messages d'être échangés [20].Cette attaque peut être considéré comme une attaque de type jamming.

- ✓ L'attaque du trou de ver (wormholeattack) : Dans une attaque de ver, un attaquant reçoit des paquets en un point A du réseau, puis les envoi via une connexion à faible latence/haut débit appelée «tunnel» vers un autre point éloigné B du réseau, qui va ensuite les injecter dans le réseau[21].

3 Services de sécurité dans l'IdO :

La sécurité de l'information et du réseau devrait exiger certaines propriétés telles que l'authentification, la confidentialité et l'intégrité. Vu l'immense champs d'application de l'IdO, en particulier dans des secteurs cruciaux de l'économie nationale (le service médical et les soins de santé, le transport intelligent, réseau électrique intelligent, etc.), les besoins de sécurité dans l'IdOseront élevés en terme de disponibilité et fiabilité. Pour mettre au point une sécurité fiable et efficace dans IdO, nous devons être conscients des principaux objectifs/besoins de sécurité :

3.1 Intégrité des données :

Pour fournir des services fiables aux utilisateurs d'IdO, l'intégrité est une propriété de sécurité obligatoire dans la plupart des cas. Différents systèmes dans l'IdO ont diverses exigences d'intégrité .ce service prévoit la détection de toute modification, insertion, suppression des données.

L'intégrité de données peut être assurée par différents moyens, tel que les fonctions de hachage, comme à titre d'exemple : MD4, MD5 (MessageDigest), SHA-1(SecureHashAlgorithm1) ou SHA-2, mais le plus souvent associés avec des clés secrètes.

3.2 Confidentialité des données :

La confidentialité est la capacité de dissimuler des messages à toute entité non autorisée (attaquant ou autres) de sorte que tout message transmis via le réseau reste confidentiel ou illisible. C'est l'un des aspects les plus importants en matière de sécurité réseau[17].La confidentialité peut être assurée en utilisant les algorithmes de cryptographie asymétrique comme RSA ou les algorithmes de cryptographie symétrique comme AES et DES.

3.3 Contrôle d'accès:

Le contrôle d'accès empêche l'utilisation non autorisée d'une ressource,(lecture, écriture, modification, copie, accès, etc.) . Parfois, il existe une confusion entre le contrôle d'accès et la confidentialité. Cependant, le contrôle d'accès peut englober plus qu'un accès «lu» aux données et, Il peut traiter plus que la confidentialité. Par contre, certaines techniques de confidentialité ne contrôlent pas l'accès aux données, de sorte que les deux services ne sont pas équivalents [22].

3.4 Authentification :

L'authentification est un service utilisé pour s'assurer de l'identité (login, @ email, @ IP, @ MAC, etc.) que prétend détenir/présenter une entité. L'identification de l'utilisateur, en particulier des utilisateurs distants, est difficile parce que de nombreux utilisateurs, en particulier ceux qui ont l'intention de causer un préjudice, peuvent se faire passer pour les utilisateurs légitimes lorsqu'ils ne le sont pas[23].

Il est essentiel de considérer comment gérer l'identité et l'authentification dans l'Internet des objets, car plusieurs entités (par exemple, sources de données, fournisseurs de services, systèmes de traitement de l'information) doivent s'authentifier mutuellement afin de créer des services fiables, pour cela différentes exigences d'authentification nécessitent des solutions différentes dans différents systèmes. Certaines solutions doivent être fortes, par exemple l'authentification de cartes bancaires ou de systèmes bancaires.

3.5 Disponibilité :

Dans l'IdO, les utilisateurs doivent pouvoir accéder à des services chaque fois qu'ils en ont besoin. En conséquence, les différents éléments matériels et logiciels du réseau doivent être suffisamment robustes pour pouvoir fournir des services même en présence d'entités malveillantes ou de situations défavorables

(pannes partiels, etc.). Néanmoins, cette propriété est liée non seulement à la protection des services, mais aussi aux mécanismes de sécurité eux-mêmes: tous les mécanismes de protection doivent être aussi économes en énergie que possible afin de ne pas drainer rapidement les batteries des objets [24].

3.6 Non-répudiation :

Cette propriété, qui vient en complément à l'authentification est décrite comme suit: un objet ne peut pas nier avoir envoyé un message qu'il a envoyé précédemment. Notant que la non-répudiation peut également considérer la répudiation de la réception, où le destinataire tente de nier la réception du message. Pour obtenir la non-répudiation, il est nécessaire de produire certaines «preuves» en cas de litige. En utilisant la preuve, il est possible de prouver qu'un dispositif du réseau a accompli une tâche[24].

4 Conclusion :

L'avènement de l'air IdO, et les innombrable occasions et opportunités de ses utilisations dans nombreuses applications et domaines, le plus souvent pouvant être critique, soulève beaucoup de questions sur les aspects liés à la sécurité de l'IdO. Ainsi, le besoin de sécurité devient primordial. Cependant, les objets formant l'IdO(capteurs sans fil, etc.) souffrent le plus souvent de nombreuses contraintes telles que l'énergie limitée, la capacité de traitement et de stockage, ainsi que la communication non fiable et le fonctionnement sans surveillance, des contraintes qui imposent un choix judicieux des techniques et mécanismes de sécurité à implémenter dans l'IdO.

Un aperçu des services de sécurité IdO les plus importants a été présenté brièvement dans ce chapitre. Dans le chapitre qui suit, en mettra l'accent sur l'authentification et les différents approches afin d'authentifier une source de diffusion dans l'Internet des Objets.

Chapitre III
L'authentification d'une source de diffusion dans l'Internet des Objets

1 Introduction :

Vu l'ampleur et le champs d'applications de l'IdO, la sécurité de l'IdO émerge comme une préoccupation critique. Il est donc nécessaire d'utiliser des mécanismes efficaces pour protéger les objets contre les attaques, ainsi que des schémas de communication sécurisés pour protéger les différents échanges entres objets et autres équipements du réseau. L'authentification par diffusion est un service de sécurité critique ,Il permet à un expéditeur de diffuser des messages vers plusieurs nœuds de manière authentifiée .Cependant, la communication broadcats/multicast, englobant un émetteur et un ensemble de destinataires à un risque considérablement augmenté et des menaces de sécurité spécifiques, par rapport aux mêmes menaces en unicast où une sorte d'asymétrie doit introduire entre la source et les récepteurs, par lesquels les récepteurs ne pouvaient que vérifier l'authenticité des données de diffusion, sans pouvoir communiquer au nom de la source, ou Générer / forger des authentificateurs valides sur les données qu'ils créent.

Une grande partie de la recherche actuelle a mis l'accent sur les protocoles et les schémas d'authentification pour protéger les informations de transmission. En ce qui suit, nous présentons deux protocoles d'authentification, destinés principalement aux WSNs -mais applicable aussi à l'IdO, connue sous le nom de µTESLA et BABRA. Ces deux protocoles, sont basées sur l'approche d'utilisation d'une clé partagée entre la source et les récepteurs, adoptant le principe de stocker les données en premier, les transmettre, puis les vérifier plus tard une fois la clé de vérification sera divulguée, ce qu'on appelle l'authentification différée, qui a comme principale faiblesse d'être cible à des attaques de type déni de service par épuisement de ressources , pour cela nous présentons aussi un autre protocole H2BSAP qui est une amélioration de µTESLA.

2 Protocoles d'authentification d'une source de diffusion :

L'authentification d'entité est une fonction de sécurité essentielle pour tout système. Les méthodes d'authentification traditionnelles basées sur la cryptographie à clé publique ne conviennent pas à l'IdO vu les faibles ressources des objets (ex :

capteurs) qui ont une puissance de traitement, un stockage, une bande passante et une énergie limités. Des lignes directrices ont introduit pour la construction d'une infrastructure à clés symétriques a l'aide des protocoles d'authentification de diffusion comme µTESLA et BABRA .

Notation	Signification
H	Fonction de hash à une voie de sortie de 8 octets
$\{K_n\}$	Une chaîne de longueur unidirectionnelle n
K_i	Le i ème élément de la chaîne, avec Ki= H (Ki + 1), pour i = 0 ...n - 1
K_0	La clé d'engagement de la chaîne de clés
I_i	Intervalle i
T_{int}	La durée de chaque intervalle de temp
MAC	Code d'Authentification de Message de 8 octets produit par l'algorithme MAC
d	Le décalage d'affichage des clé authentification.
Tc	L'heure locale où le paquet est reçu .
T1	Le début Temps de l'intervalle de temps 1 .
Δ	La différence d'horloge maximale entre l'expéditeur et récepteur.
T_{delay}	période de retard

Tableau III.1 : Les notations utilisées pour décrire les protocoles

2.1 µTESLA :

µTESLA est un protocole d'authentification d'une source de diffusion dans les WSNs. Il est basé sur une chaîne de clés de hachage unidirectionnelle, qui est une séquence de clés symétriques K_0, K_1,. . . , K_n. Il est utilisé pour sécuriser les informations de routage, les messages d'agrégation de données, etc. [25].

µTESLA introduit l'asymétrie entre émetteur, souvent la SB (Station de Base), et récepteurs, en retardant la divulgation des clés symétriques utilisées .Un émetteur diffuse un message avec un code d'authentification de message (MAC) généré avec une clé secrète K_i, qui est divulguée après une certaine période de temps, correspondant au moins au temps nécessaire pour que le message soit reçu par l'ensemble des récepteurs dans le réseau.

Lorsqu'un récepteur reçoit ce message, il s'assure que le paquet a été envoyé avant que la clé ne soit divulguée, il tamponne ce paquet puis vérifie son authenticité lorsqu'il reçoit ultérieurement la clé correspondante divulguée[26].

µTESLA est basé sur le principe que les capteurs soient synchronisés, c'est à dire que la différence entre l'horloge de l'émetteur et récepteurs est inférieur à une borne connue (Δ). Aussi, il suppose que le délai de propagation d'un message dans le réseau est aussi connue, et qui correspond au temps maximal pour qu'un message arrive au nœud le plus éloigné de l'émetteur (T_{delay}).

Comme montre la figure III.1, l'émetteur génère la chaine de clés à sens unique $\{K_n\}$ (à l'aide de la fonction de hachage à sens unique H) , L'émetteur utilise la clé d'authentification K_i pour authentifier (générer des MACs) les paquets envoyés dans l'intervalle de temps I_i, et divulgue ultérieurement K_i dans l'intervalle de temps I_{i+d}(d=2 dans l'exemple) .

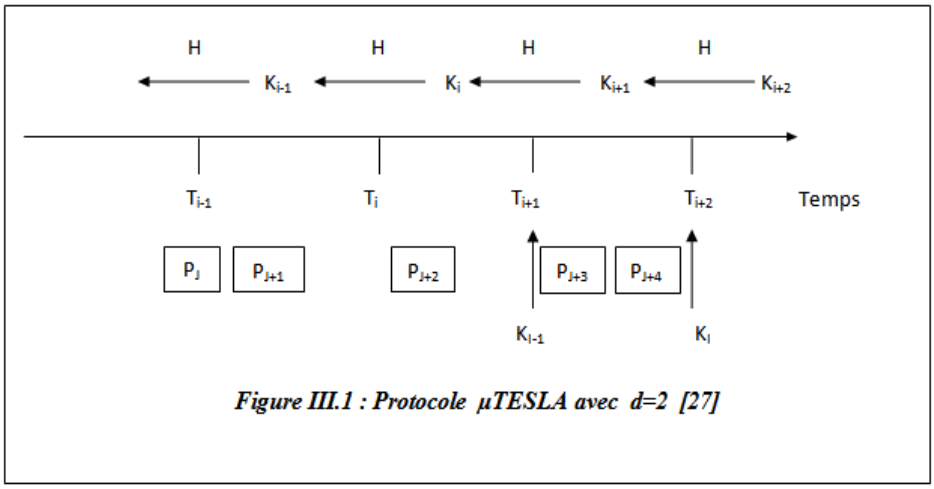

Figure III.1 : Protocole µTESLA avec d=2 [27]

2.1.1 Présentation du protocole µTESLA [27] :

L'expéditeur divise le temps en n intervalles de temps de durée uniforme (T_{int}). Ensuite, il forme une chaîne unidirectionnelle de clés d'authentification $\{K_n\}=K_1, \ldots, K_n$, en sélectionnant une clé aléatoire K_n de l'intervalle n, et en appliquant successivement une fonction de hachage H à K_n pour calculer le reste des clés, où $K_i = H(K_{i+1})$, avec $1 \leq i \leq n-1$, est la clé utilisée par

l'émetteur pour authentifier les paquets envoyés durant l'intervalle de temps I_i. La clé K_0 appelée l'engagement de la chaîne de clés (commitment key) n'est pas utilisé pour authentifier les données, mais plutôt les clés de la chaine, et est connue par tous les récepteurs avant leur déploiement (ex : pré-chargée en mémoire).Etant donné $K_j$dans la chaîne de clés, n'importe qui peut calculer toutes les clés précédentes K_i,$0 \leq i < j$, mais personne ne peut calculer une quelconque clé future K_i, $j< i \leq n$, et ceci grâce à la propriété unidirectionnelle de H. Ainsi, à la connaissance de la clé initiale K_0, un récepteur peut authentifier(vérifier) toute clé dans cette chaîne en exécutant simplement des opérations de fonction de hachage. Lorsqu'un message de diffusion (ex : paquet P_{ij}) est disponible dans le i-ème intervalle de temps (I_i), l'émetteur génère un MAC pour ce message la clé K_i, en utilisant une fonction d'intégrité (ex : HMAC) et diffuse ce message avec son MAC. Chaque clé K_i de la chaine de clés $\{K_n\}$, utilisée par l'émetteur durant l'intervalle $I_i$sera divulguée après un certain délai d (après d intervalles de temps) ; donc la clé K_i sera connue durant l'intervalle I_{i+d}. Ce délai garantit qu'une fois une clé K_i divulguée, tous les paquets de l'intervalle I_i ayant été authentifiés par cette clé auraient déjà été reçus par les récepteurs, évitant ainsi des manipulation de ces paquets par un attaquant. Lorsqu'un récepteur reçoit un paquet de diffusion P_{ij} appartenant à l'intervalle de temps I_i(chaque paquet contient un champ indiquant son intervalle), ce dernier vérifie que le temps de l'intervalle $I_{i\ a}$ déjà débuté, que l'expéditeur n'a pas encore divulgué la clé K_i(le récepteur ne se trouve pas encore dans l'intervalle I_{i+d}) et que P_{ij} n'est pas déjà stocké afin de stocker le paquet et de le forwarder, autrement il l'écarte car il soupçonne que ce paquet soit modifié par un attaquant. Lorsque le récepteur reçoit la clé divulguée K_i à partir de l'intervalle I_{i+d}, il peut l'authentifier avec une clé précédemment reçue $K_j(i>j)$ en vérifiant si $K_j = H^{i-j}(K_i)$, stocke K_i(en remplacement de K_j)puis vérifie l'authenticité/intégrité des les paquets tamponnés qui ont été envoyés pendant l'intervalle I_i.

2.1.2 Avantages µTESLA : [28]

- ✓ Le protocole µTESLA fournit une authentification de diffusion efficace, avec un coût acceptable, et pouvant accommoder un grand nombre de récepteurs dans le réseau.
- ✓ Robustesse à la perte de paquets puisque chaque paquet porte son propre MAC.
- ✓ Assurer l'authentification/intégrité des informations. Faible charge de calcul : un MAC par paquet.
- ✓ Faible niveau de communication : un Mac de 8-16 octet par paquet, un paquet de divulgation de clé par intervalle .
- ✓ Mise en mémoire Tampon limité requise pour l'expéditeur et le Récepteur, donc authentification en temps opportun pour chaque paquet individuel. Supporte la perte de clés d'authentification : À la réception d'une clé K_i, tous les paquets stockés authentifiés avec des clés $K_j (j<i)$ perdus peuvent êtres vérifiés car les clés K_j peuvent être calculées à partir de K_i.

2.1.3 Inconvénients µTESLA:[29]

- ✓ Le problème essentiel de µTESLA est de savoir comment distribuer et authentifier les paramètres µTESLA, y compris les engagements des chaînes de temps, la durée de chaque intervalle de temps, durée de divulgation, etc. Souvent ceci se fait à l'initialisation avant le déploiement des capteurs dans le réseau, mais vue qu'une seule chaine de clés ne peut couvrir toute la durée de vie du réseau, il faudrait périodiquement distribués de façon sécurisée, les paramètres d'une nouvelle chaine de clés.
- ✓ La conséquence de retard d'authentification – authentification différée) est qu'un attaquant peut lancer des attaques DoS, en envoyant des fausses données à un récepteur , ce dernier ne pouvant pas vérifier immédiatement les paquets, il est obliger de les stocker et de les forwarder, pour s'apercevoir ultérieurement que ce sont de paquets non authentique. Ce type d'attaque vise principalement à saturer le tampon de stockage des capteurs, perturbant ainsi le stockage de paquets légitime, ainsi que l'épuisement des batteries des capteurs en leur faisant forwarder des paquets inutilement.

- ✓ µTESLA ne s'adapte bien aux scénarios dans lesquels plusieurs sources de diffusion existent dans le réseau.
- ✓ Vu le caractère différé, les nœuds les plus proches de l'émetteur se voient pénalisés par le nœud le plus éloigné, vu que la durée de divulgation d'une clé dépend principalement du délai d'acheminement de données entre l'émetteur et ce nœud éloigné.

2.2 Protocole BABRA :

BABRA est un protocole d'authentification de diffusion par lots qui a été proposé par Zhou et Fang dans [30] . Contrairement à µTESLA, BABRA utilise des clés indépendantes à la place d'une chaine de clés $\{K_n\}$ et donc peut supporter une longue diffusion de paquets.

2.2.1 Avantage BABRA [30] :

- ✓ Bien que BABRA introduit une surcharge de paquet supplémentaire (8 octets MAC + 8 octets du haché d'une clé), il vaut la peine en raison de l'élimination de l'exigence de synchronisation de temps.
- ✓ BABRA n'utilise pas une chaîne de clés limitée (n éléments) et ne suppose pas que chaque lot soit envoyé juste après la fin du lot précédent, de sorte que BABRA puisse supporter une durée de vie plus longue d'un flux de diffusion.
- ✓ Dans BABRA, chaque clé est indépendante des autres. L'élimination d'un porte-clés rendent BABRA adapté à la fois au réseau diffusé par une station de base et à la diffusion locale par nœud de capteur.

2.2.2 Inconvénients BABRA [31] :

- ✓ Comme µTESLA la divulgation retardée des clés rend BABRA également vulnérables aux attaques DoS causés par l'injection de paquets forgés, où un attaquant diffuse de faux paquets, que les capteurs vont tamponner et renvoyer.

- ✓ BABRA ne prend pas en charge efficacement plusieurs sources, puisque chaque source doit distribuer de manière sécurisée le hachage de sa première clé H (K_1) à tous les nœuds du réseau.
- ✓ Vu que les clés sont indépendantes, la déploiement ultérieur de nouveaux nœuds nécessite la distribution de $H(K_j)$ où K_j est la futur clé divulguée après leur déploiement, étant donnée qu'avec $H(K_1)$ ces nouveaux nœuds ne sont pas en mesure d'authentifier les nouvelles clés. De même, si un nœud échoue à recevoir une clé K_i, il n'est plus en mesure d'authentifier les clés futur K_j (j>i) ainsi que les lots associés.

2.3 H2BSAP :

Dans ce chapitre, nous présentons une troisième solution H2BSAP [33], qui atténue le risque d'attaque DoS dans le contexte d'une authentification d'une source de diffusion. Cette solution se base sur une authentification différée saut par saut(hop-by-hop) , limitant ainsi le dommage d'un attaquant à ses voisins direct d'un saut au lieu de l'ensemble du réseau, comme c'était le cas dans µTESLA [33][32].Ce protocole est une amélioration de µTESLA mais en adoptant le principe de stocker les données, les vérifier une fois la clé associée est divulguée puis, si ces données sont correct les transmettre aux voisins.

2.3.1 Description de H2BSAP :

comme montre la Figure IV.1 ,H2BSAP procède en effectuant une diffusion/vérification par niveau. Le protocole de déroule en trois phrases, décrites ci-dessous.

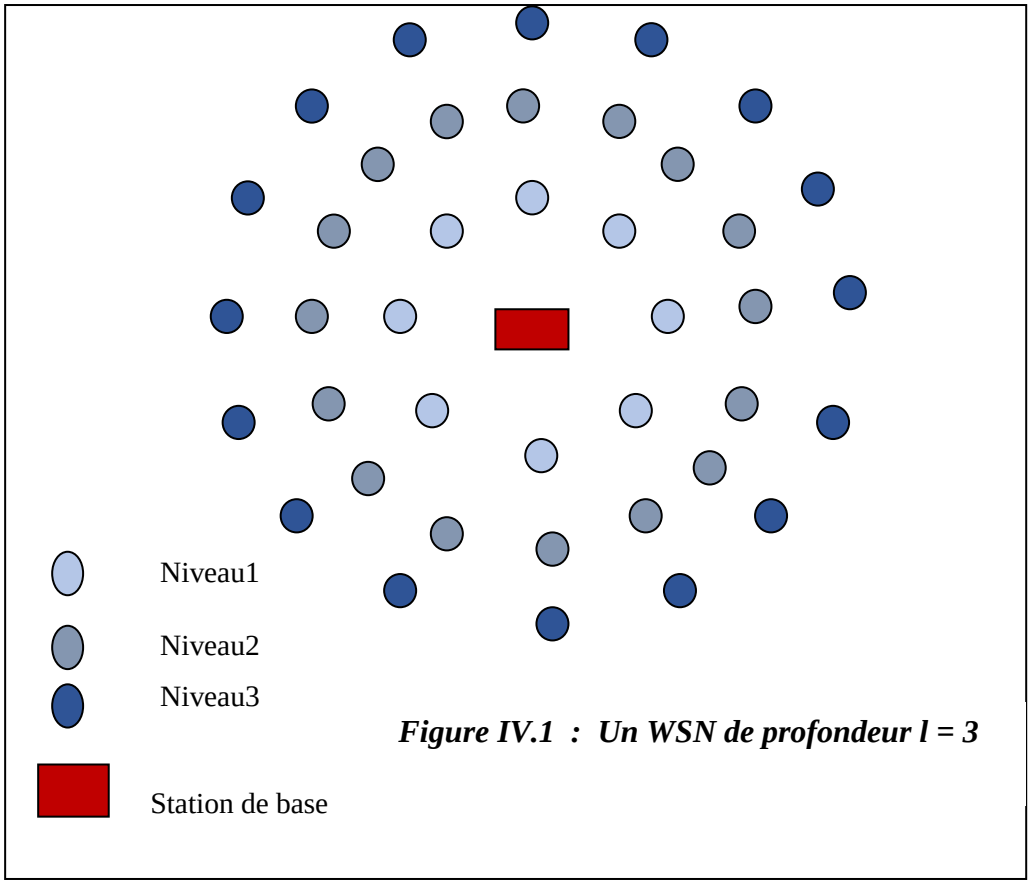

Figure IV.1 : Un WSN de profondeur l = 3

- **Phase d'initialisation :** la S.B divise le temps en n intervalles de temps égaux de durée T_{int}. Pour une profondeur l du réseau(en terme de nombre de sauts autour de la SB), la SB génère l chaines de clés unidirectionnelle indépendantes en utilisant une fonction de hachage H, chaque chaine $\{K_n^r\} = K_0^r, K_1^r, \dots, K_n^r (K_i^r = H(K_{i+1}^r))$a un délai de divulgation de clé d_r avec r=1…l et$d_1<d_2<\dots<d_r$.et est utilisée par la SB pour authentifier ses messages auprès des nœuds se trouvant à **r** sauts autour d'elle. Les nœuds du réseau sont initialement pré-chargés avec les paramètres :T_0 (début du 1er intervalle)T_{int},$K_0^r d_r$ de toutes les chaines$\{K_n^r\}$, r=1…l
- **Phase de diffusion des données :** la SB divise les données à envoyer pendant l'intervalle de temps i (I_i)dans plusieurs petits messages $M_{i,j}$ avec j l'index du message dans I_i . $M_{i,j}$ est authentifié puis acheminé dans un paquet P_{ij}, comme suit : Tout d'abord la SB utilise la clé courante K_i^lde la dernière chaine de clé $\{K_n\}$ pour calculer un MAC afin de définir le paquet :$P_{i,j}$= i,j,$M_{i,j}$,$MAC_{K_i^l}$ (i||j||$M_{i,j}$).Ensuite, la SB utilise la

clé K_i^r de la chaine$\{K_n^r\}$, pour calculer $MAC_{K_i^r}(P_{i,j})$, et l'ajouter à la fin du paquet pour r=l-1, ….,1.Enfin un compteur Cpt=1 est ajouté à la fin du paquet, afin de permettre à chaque nœud de savoir sa distance par rapport à la SB. Au final, on obtient :

$$P_{ij} = \underbrace{\underbrace{i, j, M_{ij}, \mathrm{MAC}_{K_i^l}\left(i||j||M_{ij}\right)}_{1}, \underbrace{\mathrm{MAC}_{K_i^{l-1}}(\mathbf{1})\, MAC_{K_i^{l-1}}(\mathbf{2}), \ldots\ MAC_{K_i^1}(l-1), Cpt}_{2\ldots}}_{l-1}$$

Après la diffusion de $P_{i,j}$, la SB divulgue les clés K_i^r(r=1, …, l) selon leur calendrier de divulgation prévu : La clé K_i^1 est la première à être divulgué, ensuite K_i^2,jusqu'à K_i^l.Chaque nœud 'h' recevant une clé K_i^r,la vérifie et, si elle est authentifiée($K_t^r = H^{i-t}(K_i^r)$ où K_t^rest la dernière clé vérifié de la chaine $\{K_n^r\}$)'h' la sauvegarde puis la retransmet à ses voisins afin de permettre aux autres nœuds du réseau d'avoir une clé à jour.

- **Phase de mise en mémoire tampon / vérification des données :** Un nœud 'h' recevant un paquet $P_{i,j}$à l'instant T_c, envoyé par la SB durant l'intervalle I_i procède de la manière suivante :

  - Si $P_{i,j}$ a déjà été reçu(en tampon),h l'écarte.

  Sinon, 'h' vérifie si $P_{i,j}$ respecte la condition de sécurité afin de le tamponner à savoir : Il faut que l'intervalle (I_i) a déjà débuté et que la clé d'authentification utilisée correspondant à son niveau (la distance en nombre de sauts séparant 'h' de la SB) n'a pas encore été divulguée par la SB. Pour savoir qu'elle chaine de clé utilisée, 'h' utilise le champ Cpt contenu dans P_{ij}. en vérifiant que la clé K_i^r où r=Cptn'a pas encore été divulguée. Ces deux conditions peuvent être vérifié avec l'expression suivante :$T_0+(i-1)*T_{int}<T_c<T_0+T(i-1)*T_{int}+d_r$. En raison de l'authentification différée saut par saut, les voisins se trouvant à r-sauts de la SB, ne recevront P_{ij} que si et seulement si les voisins se trouvant à r-1-sauts de la SB l'ont déjà reçu et vérifié .Lorsque la SB divulgue la clé K^r ,'h'la vérifie en utilisant la dernière clé divulguée/vérifiée $K_t^r(K_t^r = H^{i-t}(K_i^r))$ Si K_i^rest vérifiée avec succès, 'h' la stocke en

remplacement de K_t^r, la diffuse à ses voisins, puis vérifie ensuite l'authenticité des paquet tamponner P_{ij} en vérifiant que le Mac calculée en utilisant K_i^rest égale au dernier MAC contenu dans P_{ij} Enfin, 'h' met à jour chaque P_{ij} vérifié avec succès, en supprimant le dernier MAC, et en incrémentant Cpt, puis diffuse le paquet à ses voisins se trouvant à r+1 sauts de la SB.

3 Conclusion :

La sécurité est la principale préoccupation pour les WSNs à faible consommation d'énergie en raison des applications de sécurité étendues, et par extension à l'IdO. Ces dernières années, la sécurité a attirée beaucoup d'attention, notamment en ce qui concerne l'authentification des communicants et d'une source de diffusion. La plupart des mécanismes d'authentification se concentrent uniquement sur la sécurité, tandis que d'autres offrent une évolutivité adéquate et une communication minimisée. L'authentification est une méthode efficace pour repousser les différentes attaques car elle nécessite le partage des clés. Il est donc évident qu'un schéma d'authentification doit réduire le coût de calcul et économiser l'énergie, pour qu'il puisse être utilisé dans le contexte de l'IdO. précédemment nous avons présenter deux protocoles d'authentification d'une source de diffusion efficaces mais qui souffrent tous les deux de certains problèmes, notamment celui d'être cible à une attaque de type DoS par épuisement de ressources (stockage, calcul, énergie) résultant ainsi en l'augmentation inutile du trafic de réseau et l'épuisement de l'énergie des nœuds (objets) du réseau. Pour réduire l'impact de l'attaque DoS, on va présenter un autre protocole dans le chapitre suivante.

Chapitre IV

Réalisation et simulation

1 Introduction :

Dans ce chapitre, nous décrivons la partie conception et implémentation de notre PFE. A l'origine, notre PFE consistait à implémenter et évaluer les performances de H2BSAP , mais pour cela on devait au préalable implémenter µTESLA puis modifier cette implémentation pour obtenir H2BSAP. Toutefois, vu la courte durée de notre stage (commencé début février) ainsi que la difficulté d'apprentissage et développement sous Contiki, nous avons dû nous contenter d'implémenter uniquement µTESLA.

2 Environnement de travail et outils de développement :

2.1 Système d'exploitation Contiki OS :

En 2004 Contiki a été proposé. Contiki est un système d'exploitation open source, hautement portable et multitâches pour les systèmes embarqués en réseau et les réseaux de capteurs sans-fil .Contiki est devenu très populaire et a atteint une bonne position dans la communauté des WSN[34]. Il est conçu pour les microcontrôleurs avec une taille de mémoire très limitée. Une configuration typique Contiki nécessite 2 kilo-octets de RAM et 40 kilobytes de ROM[35]. Les applications du système contiki sont implémentés dans le langage de programmation C. Contiki se compose d'un noyau basé sur les événements, sur lequel les programmes d'application peuvent être chargés et déchargés dynamiquement au moment de l'exécution[34].

Contiki fournit tout un environnement qui aide à la programmation des applications d'objets intelligents, des bibliothèques pour l'allocation de mémoire [36], d'autres pour la communication sans-fils, .un mécanisme de profil de puissance basé sur un logiciel qui permet de suivre la consommation énergétique de chaque nœuds capteur. Il a trois environnements de simulation: l'émulateur MSPsim, le simulateur de réseau multicouches Cooja et le simulateur de niveau de processus Netsim[34].Il a également deux piles protocolaire pour la communication : Rime et UiP.

- ✓ La couche uIP(micro IP): Contiki fournit une communication IP à la fois pour IPv4 et IPv6, via les piles uIP et uIPv6 . Sa plate-forme IP lui permet de communiquer directement avec d'autres applications IP et services Web, y compris les services Internet [34].
- ✓ La couche Rime : Rime est une pile de communication légère conçue pour les radios de faible puissance. Rime fournit une large gamme de primitives de communication adaptées à la mise en œuvre d'applications liées à la communication ou de protocoles réseau[37].

Nous avons installer contiki 2.7 comme montre la figure ensuite ,Lancer le fichier instant Contiki 2.7.vmx dans VMware Player, et attendre le démarrage d'Ubuntu linux puis, entrer le mot de passe: user.

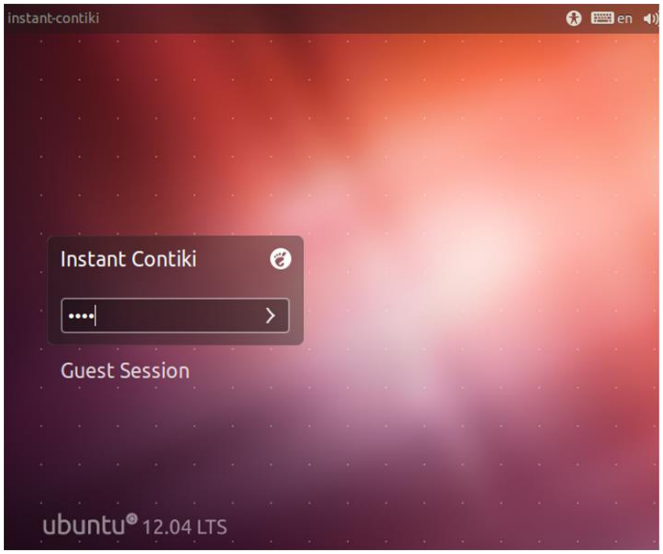

Figure IV.1 : Authentification de Contiki

2.2 Le simulateur Cooja :

Cooja est un simulateur basé sur Java conçu pour simuler des réseaux de capteurs utilisant le système d'exploitation du réseau de capteurs Contiki . Le simulateur est implémenté en Java mais permet de rédiger un logiciel de nœuds capteur en C.L'utilisateur peut interagir avec les nœuds utilisant une interface

utilisateur graphique (GUI). Cooja prend en charge différents niveaux de simulation (niveau réseau, niveau de code et niveau d'instruction) [38].Dans Cooja, toutes les interactions avec les nœuds simulés sont effectuées via des plugins comme Simulation Visualizer, Timeline et Radio Logger. Il stocke la simulation dans un fichier xml avec extension 'csc' (configuration de simulation Cooja). Ce fichier contient des informations sur l'environnement de simulation, les plugins, les nœuds et ses positions etc[36].La figure suivante représente l'interface de simulateur cooja .

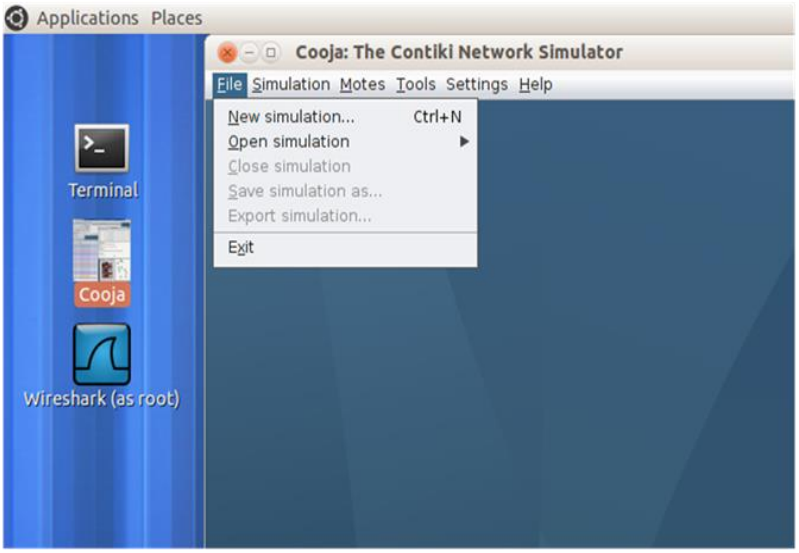

Figure IV.2 :Démarrage de simulateur Cooja

2.3 Le protocole IPv6 :

Ipv6 a été conçu pour être une évolution d'IPv4. Ce n'est pas un changement radical. Seul les fonctions stables d'IPv4 ont été gardées mais avec un routage intelligent et une capacité d'adressage qui est passé de 32 bits à 128bits, pour supporter un adressage hiérarchique et un plus grand nombre de nœud adressable, et un mode d'auto configuration[39].Afin de pouvoir réaliser la vision de l'Internet des Objets, en supportant la pile protocolaire TCP/IP au sein de capteurs à contraintes de ressources, et dont la couche liaison manipule des trames de petites taille (127 octets en générale), le

standard (couche d'adaptation) 6LoWPAN a été adopté et implémenté par Contiki. au-dessus de la couche de liaison IEEE 802.15.4 (la plus répondu au sein des capteurs) pour la fragmentation et le réassemblage des paquets[41].6LoWPAN définit la façon d'exécuter la version IP 6 (IPv6) sur des réseaux radio faible débit et à faible puissance. La réussite de 6lowpan permettrait le développement d'un véritable Internet des objets, connectant des engins qui ne sont en général pas classés parmi les ordinateurs[42].

3 Implémentation du protocole µTESLA :

Le code de notre implémentation du protocole µTESLA, comprend deux parties : une partie concerne la station de base (la source de diffusion de données) et l'autre partie concerne les autres capteurs (les récepteurs des données).

3.1 La partie station de base :

Chaque paquet diffusé par la SB est une structure de 5 champs, comme le montre la figure IV.5 : type : définit le type du paquet, il peut être un paquet de données où un paquet de clé, contenant la clé divulguée

msg : Contient les données à envoyer.

numI : C'est le numéro d'intervalle.

numS : C'est le numéro de séquence du paquet dans l'intervalle .

MAC :Contient le code d'authentification/intégrité de message, calculé en utilisant une Fonction MAC (ex : HMAC,SHA1) sur les champs (type, msg,numI,numS), en utilisant la clé courante . on calcule le mac du paquet qui est théoriquement sur 20 octets dans notre cas on prend juste les 8 premiers octets comme max.

Pour générer la chaine de clé K_{n-1}, K_{n-2}, ... K_1,K_0 nous avons utiliser la fonction de hachage SHA1, la clé Kn a été initialiser a partir de laquelle seront dérivés le reste des clés de la chaine de clé par exemple :

key[20]= {1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20}

Donc notre chaine de clés a une taille d'éléments 21 (de K0 ... K20) chaque clé faisant 20 octets.

Comme le paquet est un structure on peut pas l'envoyé directement pour cela nous avons définir une fonction pour convertir le paquet en une seul chaine puis l'envoyée .Pour chaque intervalle nous avons envoyé trois paquets c.à.d. (trois séquence) .

```
struct  paquets   {
        char* type ;
        char *msg;
        uint8_t  numI;
        uint8_t   numS;
        uint8_t mac[8];//chaque paquet contient un mac de 8 octets
                                } ;
```

Figure IV.3 :La structure de paquet

Les principales fonctions que nous avons utilisées dans cette partie :

simple_udp_register*(*&broadcast_connection,UDP_PORT,NULL,UDP_ PORT,receiver*);*

Cette fonction enregistre une connexion UDP de type broadcast et lui attribue une fonction de rappel *receiver*. La fonction de rappel est appelée pour les paquets entrants, où à chaque fois qu'un paquet entrant est reçu sur le numéro de port, Contiki invoque la fonction de rappel afin de traiter ce paquet. Le port UDP local (1er UDP_PORT) peut être mis à 0 pour indiquer qu'un port UDP éphémère doit être alloué, Le 2eme champs UDP_PORT indique le numéro de port sur lesquels les récepteurs sont censé écouter les paquets de cette connexion, et doit être spécifié. Cette fonction a été utilisée côté émetteur (SB) et récepteur (Capteurs), mais la fonction de rappel a été redéfinit uniquement côté récepteurs, vu que le traitement des paquets reçus est effectué côté récepteurs dans le protocole µTESLA, l'émetteur étant seulement la SB.

simple_udp_send (struct simple_udp_connection *c, constvoid *data, uint16_t datalen) ;

Le paquet sera envoyés à l'adresse IP et aux ports UDP qui étaient spécifié lorsque la connexion a été enregistrée avec Simple_udp_register ().

```
uip_create_linklocal_allnodes_mcast(&addr);
```

Cette instruction définit d'abord une minuterie et lorsque la minuterie expire, elle définit une nouvelle génération (Entre 1 et l'intervalle d'envoi) pour éviter d'inonder le réseau. Ensuite, il définit L'adresse IP à l'adresse de multidiffusion locale de tous les nœuds de liaison .

Contiki contient un ensemble de bibliothèques de minuterie qui peuvent être utilisés pour contrôler des tâches périodiques et implémenter des algorithmes sophistiqués. Il existe 4 types de minuteries fournies par Contiki:

- Struct timer : La minuterie passive, ne fait que suivre son temps d'expiration.
- Struct etimer : Temporisateur actif, envoie un événement lorsqu'il expire.
- Struct ctimer : Temporisateur actif, appelle une fonction lorsqu'il expire.
- Struct rtimer : Temporisateur en temps réel, appelle une fonction à un moment précis.

On s'intéresse uniquement à la bibliothèque « etimer »

```
etimer_set(&periodic_timer,2*CLOCK
SECOND);
```

Pour réinitialiser le etimer :

```
etimer_reset(&periodic_timer);
```

Et pour vérifiez si la minuterie a expiré :

```
etimer_expired(&periodic_timer)
```

Dans cette « etimer » Nous avons défini le temps de chaque intervalle Tint par 2s (c.à.d. 2*CLOCK SECOND) avec « CLOCK SECOND »correspond à

une seconde de l'heure du système fournit par la bibliothèque d'horloge. Donc à chaque expiration de « etimer » une fonction va être appeler pour surcharger et envoyer une paquet de données .après deux intervalle de temps la divulgation de clé sera commencé on appelant une autre fonction pour la divulgation de clés K_{I-2} au début de intervalle de temps I donc avec une durée de divulgation d=2.

3.2 La partie capteurs (récepteurs):

comme montre la figure IV.5 la fonction « receiver »Cela passe à l'application simple-udp les ports pour gérer les diffusions, et la fonction de rappel pour gérer les émissions reçues. Nous passons le paramètre NULL comme l'adresse de destination pour permettre les paquets à partir de n'importe quelle adresse.

```
static void receiver(struct simple_udp_connection *c,
         const uip_ipaddr_t *sender_addr,
         uint16_t sender_port,
         const uip_ipaddr_t *receiver_addr,
         uint16_t receiver_port,
         const uint8_t *data,
         uint16_t datalen)
```

Figure IV.4 :Les paramètres de la fonction « receiver »

Lors de la réception d'une paquet on va vérifier le type si c'est une paquets de données(type= « d »),ou une paquet de clé (type= « k »).

- ✓ Paquets de données :Vérifier la condition de sécurité c.à.d. que l'intervalle a commencer correctement leur temps associer et que leur clé n'a pas encore été divulguée .On utilise la fonction « clock_time() » pour connaitre le temps courant de réception.

$((t_c<(t_0+(I-1)*T_{int}+d)) \&\&(t_c>(t_0+(I-1)*T_{int})))$

Avec d est la durée de divulgation .

Si la condition précédente est vrai on vérifie si le paquet n'existe pas dans le tampon des paquets afin de le tamponner, puis le transmettre.

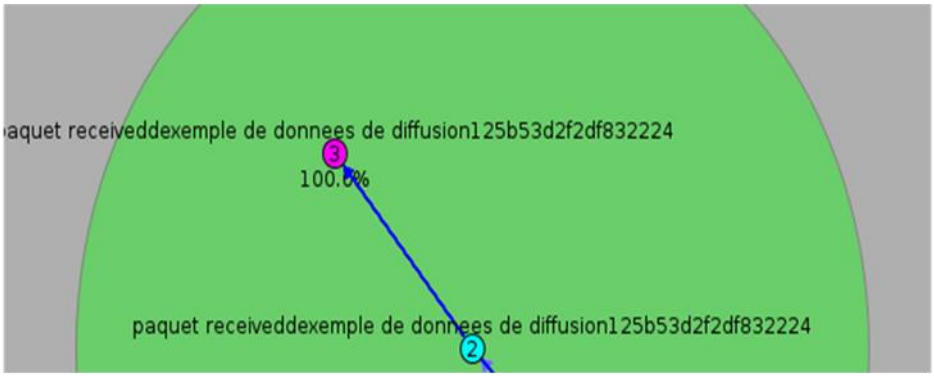

Figure IV.5 : Exemple d'envoie d'un paquet de données dans l'intervalle I=1

- ✓ Paquet de clé : On vérifie que la clé divulguée est plus récente que la dernière clé connue(initialement par exemple contient la dernière clé divulguée vérifiée K0), puis on vérifie la validité de cette clé par le calcule de hachage de la clé reçu avec la clé précédemment reçu, si la clé est valide on stocke cette dernier dans une variable temporaire pour vérifier la prochaine clé.

  Dans cette étape on parcourt le tampon à la recherche de paquets appartenant à l'intervalle I_k qui correspond à la dernière clé vérifiée mise à jours afin de calculer le MAC du paquet et on le compare avec le MAC originale contenu dans le paquet ,si le MAC est valide (c.à.d. le MAC calculé et le MAC de paquet sont égaux) on peut dire que le paquet est authentifier .

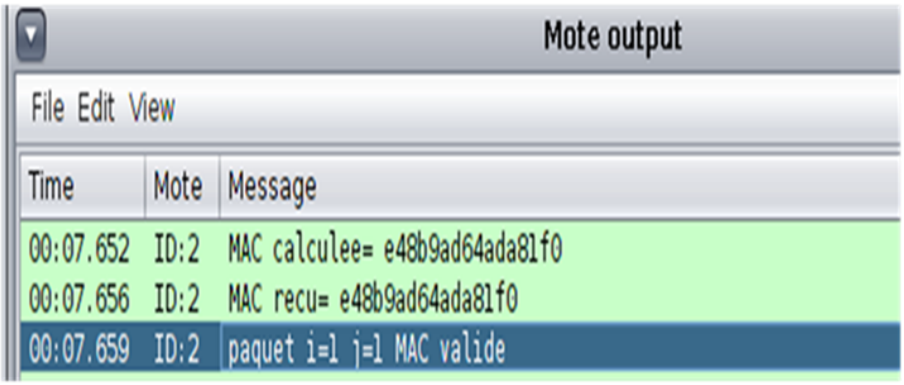

Figure IV.6 : Exemple d'authentification d'un paquet dans l'intervalle I=1

4 Conclusion :

A travers ce chapitre, nous avons commencé par présenter notre protocole, et ses différentes étapes. Comme nous avons présenté le système d'exploitation Contiki ainsi que le simulateur Cooja ,ensuite nous avons détaillée les étapes d'implémentation .nous avons mettrons les contextes générales de notre étude le travail demandé ainsi les résultats attendus de notre protocole.

Conclusion et Perspectives

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 intéressé à la problématique de l'authentification d'une source de diffusion dans l'IdO, qui est un service de sécurité important dans l'IdO, surtout que le modèle de communication en diffusion (broadcast/multicast) est largement utilisé dans l'IdO (découverte de voisins, routage, diffusion requêtes, mise à jour logiciels, etc.). Pour cela, il est nécessaire d'utiliser une procédure d'authentification sécurisée et performante permettant à un ensemble de récepteurs d'authentifier les paquets diffuséspar une source de diffusion, afin de s'assurer de l'identité de l'émetteur et l'intégrité des données.

Dans notre mémoire, nous avons étudié 3 protocoles d'authentification : µTESLA, BABRA et H2BSAP, où chaque protocole a été détaillé. Ces 3 protocoles sont basés sur l'asymétrie de temps pour mettre en œuvre une authentification différée, où l'émetteur utilise une (plusieurs) chaine(s) de clés pour authentifier ses paquets, chaque clé servant à authentifier la clé précédente, et où chaque clé utilisée durant l'intervalle i est divulguée ultérieurement durant l'intervalle i+d. Nous avons vu que le problème majeure de l'authentification différée -où un récepteur stocke un paquet, le propage puis vérifie son authenticité ultérieurement, est qu'elle est cible aux attaques de DoS par épuisement de ressources. Dans ce cadre, H2BSAP limite l'impact d'une telle attaque aux voisins direct de l'attaquant, alors que dans BABRA et µTESLA l'attaquant peut affecter tout le réseau.

Initialement, le but de notre mémoire, était l'implémentation et études de performances de H2BSAP en comparaison à µTESLA, mais pour cela il fallait

d'abord implémenter µTESAL puis étendre cette implémentation pour obtenir H2BSAP.

Toutefois, vu la courte durée de stage, la nouveauté de la problématique traitée dans le PFE, ainsi que la difficulté de l'apprentissage et la programmation sous Contiki, nous avons réorienté notre problématique vers l'étude et l'implémentation du protocole µTESLA.

Comme perspectives de notre travail, nous envisageons l'implémentation de H2BSAP puis la comparaison de ses performances avec µTESLA, notamment en ce qui concerne la résistance. aux attaques de DoS avec épuisement de ressources. Aussi, nous considérons l'utilisation mixte d'une authentification basée sur l'asymétrie des clés (ex : signatures) et celle basée sur l'asymétrie de temps (ex : µTESLA, etc.) afin de tirer profits des deux avantages à savoir une authentification immédiate et à bas coûts, et où plusieurs sources de diffusions peuvent exister.

Références bibliographiques

[1] Uckelmann, Dieter, Mark Harrison, and Florian Michahelles. “An Architectural Approach towards the Future Internet of Things.” In Architecting the Internet of Things, 1–24. Springer, 2011.

[2] Nait-Sidi-Moh, Ahmed, David Durand, Jérôme Fortin, and others. “Internet Des Objets et Interopérabilité Des Flux Logistiques: État de L’art et Perspectives. ” In UbiMob2014, 8, 2014.

[3] . Cristian, Toma, Cristian Ciurea, and Ion Ivan. “Approaches on Internet of Things Solutions.” Journal of Mobile, Embedded and Distributed Systems 5, no. 3 (2013): 124–129.

[4] Alcaraz, Cristina, Pablo Najera, Javier Lopez, and Rodrigo Roman. “Wireless Sensor Networks and the Internet of Things: Do We Need a Complete Integration” In 1st International Workshop on the Security of the Internet of Things (SecIoT’10), 2010.

[5] Jung, Bumsuk, Ingoo Han, and Sangjae Lee. “Security Threats to Internet: A Korean Multi-Industry Investigation.” Information & Management 38, no. (2001).

[6] Wang, Ronghua, Wenliang Du, and Peng Ning. “Containing Denial-of-Service Attacks in Broadcast Authentication in Sensor Networks.” In Proceedings of the 8th ACM International Symposium on Mobile Ad Hoc Networking and Computing,71-79,2007.

[7] Présentation générale de l'Internet des objets , (rapport ITU-T Y.2060),ITU-T Study Group 20,(2012) .

[8] David R. Gnimpieba Z,Ahmed Nait-Sidi-Moh ,David Durand ,Jérôme Fortin, ’’Internet des objets et interopérabilité des flux logistiques: état de l'art et perspectives’’, Université de Picardie Jules Verne (UPJV),2014

[9] “[Infographie] Histoire de L’internet Des Objets Au Fil Du Temps.” Aruco, August 11, 2014.

[10] Mattern, Friedemann, and Christian Floerkemeier. “From the Internet of Computers to the Internet of Things.” In *From Active Data Management to Event-Based Systems and More*, 242–259. Springer, 2010.

[11] Suo, Hui, Jiafu Wan, Caifeng Zou, and Jianqi Liu. “Security in the Internet of Things: A Review.” In *Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on*, 3:648–651. IEEE, 2012.

[12] Kramp, Thorsten, Rob van Kranenburg, and Sebastian Lange. “Introduction to the Internet of Things.” In *Enabling Things to Talk*, 1–10. Springer, 2013.

[13] Chen, Shanzhi, Hui Xu, Dake Liu, Bo Hu, and Hucheng Wang. “A Vision of IoT: Applications, Challenges, and Opportunities with China Perspective.” *IEEE Internet of Things Journal* 1, no. 4 (2014): 349–359.

[14] Bandyopadhyay, Debasis, and Jaydip Sen. “Internet of Things: Applications and Challenges in Technology and Standardization.” Wireless Personal Communications 58, no. 1 (2011): 49–69.

[15] Friess, Peter. *Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems*. River Publishers, 2013.

[16] Sarkar, Chayan, SN Akshay Uttama Nambi, R. Venkatesha Prasad, and Abdur Rahim. “A Scalable Distributed Architecture towards Unifying IoT Applications.” In *Internet of Things (WF-IoT), 2014 IEEE World Forum on*, 508–513. IEEE, 2014.

[17] Padmavathi, Dr G., Mrs Shanmugapriya, and others. “A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks.” arXiv Preprint arXiv:0909.0576, 2009.

[18] Karlof, Chris, and David Wagner. “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures.” Ad Hoc Networks 1, no. 2 (2003): 293–315.

[19] Sharma, Kalpana, and M. K. Ghose. “Wireless Sensor Networks: An Overview on Its Security Threats.” IJCA, Special Issue on “Mobile Ad-Hoc Networks” MANETs, 2010, 42–45.

[20] Messai, Mohamed-Lamine. “Classification of Attacks in Wireless Sensor Networks.” arXiv Preprint arXiv:1406.4516, 2014.

[21] Hu, Yih-Chun, Adrian Perrig, and David B. Johnson. “Wormhole Attacks in Wireless Networks.” IEEE Journal on Selected Areas in Communications 24, no. 2 (2006): 370–380.

[22] Lopez, Javier, Rodrigo Roman, and Cristina Alcaraz. “Analysis of Security Threats, Requirements, Technologies and Standards in Wireless Sensor Networks.” In Foundations of Security Analysis and Design V, 289–338. Springer, 2009.

[23] Kizza, Joseph Migga. Guide to Computer Network Security. Springer, 2009.

[24] Jung, Bumsuk, Ingoo Han, and Sangjae Lee. “Security Threats to Internet: A Korean Multi-Industry Investigation.” Information & Management 38, no. 8 (2001): 487–498.

[25] Whillock, Mark Luk Adrian Perrig Bram. “Seven Cardinal Properties of Sensor Network Broadcast Authentication,” 2006.

[26] Ning, Donggang Liu Peng, Sencun Zhu, and Sushil Jajodia. “A Tree-Based μTESLA Broadcast Authentication for Sensor Networks.”

[27] Liu, Donggang, Peng Ning, Sencun Zhu, and Sushil Jajodia. “Practical Broadcast Authentication in Sensor Networks.” In Mobile and Ubiquitous Systems: Networking and Services, 2005. MobiQuitous 2005. The Second Annual International Conference on, 118–129. IEEE, 2005.

[28] Perrig, Adrian, Ran Canetti, J. Doug Tygar, and Dawn Song. “The TESLA Broadcast Authentication Protocol.” Rsa Cryptobytes 5 (2005).

[29] Bohge, Mathias, and Wade Trappe. “TESLA Certificates: An Authentication Tool for Networks of Compute-Constrained Devices.” In Proc. of 6th International Symposium on Wirless Personal Multimedia Communications (WPMC’03), 2003.

[30] Zhou, Yun, and Yuguang Fang. “WSN09-1: BABRA: Batch-Based Broadcast Authentication in Wireless Sensor Networks.” In Global Telecommunications Conference, 2006. GLOBECOM’06. IEEE, 1–5. IEEE, 2006.

[31] Wehbi, Bachar, Anis Laouiti, Wissam Mallouli, and Ana Cavalli. “Un Mécanisme de Synchronisation Pour Les Réseaux Sans Fil Multi-Sauts.”, 2007.

[32] Chakib BEKARA, “Wieless Sensors Networks Security.” ,Thèse de doctorat de l’INSTITUT NATIONAL DES TELECOMMUNICATIONS dans le cadre de l’école doctorale SITEVRY en co accréditation avec l’ NIVERSITE D’EVRY-VAL D’ESSONNE,(2008).

[33] Bekara, Chakib, Maryline Laurent-Maknavicius, and Kheira Bekara. “H 2 BSAP: A Hop-by-Hop Broadcast Source Authentication Protocol for WSN to Mitigate DoS Attacks.” In *Communication Systems, 2008.*

ICCS 2008. 11th IEEE Singapore International Conference on, 1197–1203. IEEE, 2008.

[34] Saadallah, Bilel, Abdelkader Lahmadi, and Olivier Festor. "CCNx for Contiki: Implementation Details." INRIA, 2012. https://hal.inria.fr/hal-00755482/.

[35] . Casado, Lander, and Philippas Tsigas. "Contikisec: A Secure Network Layer for Wireless Sensor Networks under the Contiki Operating System." In *Nordic Conference on Secure IT Systems*, 133–147. Springer, 2009.

[36] Ali, H. "A Performance Evaluation of Rpl in Contiki: A Cooja Simulation Based Study." *School of Computing, Blekinge Institute of Technology*, 2012.

[37] Dunkels, Adam. "1 The Contiki Operating System 2. X." ,2007.

[38] Kugler, Patrick, Philipp Nordhus, and Bjoern Eskofier. "Shimmer, Cooja and Contiki: A New Toolset for the Simulation of on-Node Signal Processing Algorithms." In *Body Sensor Networks (BSN), 2013 IEEE International Conference on*, 1–6. IEEE, 2013.

[39] Mulligan, Geoff. "The 6LoWPAN Architecture." In *Proceedings of the 4th Workshop on Embedded Networked Sensors*, 78–82. ACM, 2007.

[40] Gee Keng, Chee Kyun Ng, Nor Kamariah Noordin, and Borhanuddin Mohd Ali. "A Review of 6LoWPAN Routing Protocols." *Proc. Asia-Pac. Adv. Netw* 30 (2010): 7181.

[41] Kumar, Vinay, and Sudarshan Tiwari. "Routing in IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN): A Survey." *Journal of Computer Networks and Communications* 2012 (2012).

[42] Group, IETF 6LoWPAN Working, and others. *RFC 4919: IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals*. IETF 6LoWPAN Working Group, 2008.

Liste des figures

Liste des tableaux

Liste des abréviations

IdO	Internet Des Objets
IoT	Internet Of Things
TIC	Information Technology and Communication
RFID	Radio Frequency IDentification
WSN	Wireless Sensor Networks
BSAP	Broadcast Source Authentification Protocol
TESLA	Timed Efficient Stream Loss-Tolerant Authentication
DoS	Denial Of Service
MAC	Message Authentication Code
BABRA	BAtch-based BRoadcast Authentication
6lowpan	IPv6 Low power Wireless Personal Area Networks
H2BSAP	Hop-by-Hop Broadcast Source Authentication Protocol
SHA	Secure Hash Algorithm

Résumé :

Le concept de l'IdO (Internet des Objets) est la prochaine évolution de l'Internet classique, permettant la mise en réseau, l'identification (ex : @ IP) et la fourniture/accès aux services à n'importe qu'elle entité/objet virtuelle ou physique, de la vie de tous les jours, ouvrant ainsi les perspectives à de nouveaux domaines d'utilisations et d'applications. Dans ce contexte, la sécurité émerge comme une préoccupation majeure et attire beaucoup d'attention, notamment en ce qui concerne l'authentification des communicants d'une source de diffusion.Plusieurs travaux de recherche ont mis l'accent sur les protocoles et les schémas d'authentification d'une source de diffusion pour s'assurer à la fois de l'identité de la source et l'intégrité de ses données, tout en tenant en compte d'autres contraintes comme les faible ressources des objets et la résistance aux attaques de type DoS (Dénie de Services) par épuisement de ressources.Parmi ces travaux, plusieurs sont basés sur l'asymétrie du temps comme les protocolesµTESLA, BABRA et H2BSAP. Dans notre PFE, nous avons étudié et présenté certains de ces protocoles, puis nous avons implémenté et simuléle protocole µTESLA sous l'OS CONTIKI -considéré l'OS par excellence de l'IdO-

Mots-clefs :IdO, authentification,BSAP,source de diffusion, µTESLA, attaque DoS, épuisement de ressources.

Abstract:

The concept of IoT (Internet of Things) is the next big evolution of Internet, where any logical /physical object of daily-life, will be uniquely identifiedand able to access/deliver services, opening the door for new areas of applications. In this evolution, security appears to be one of the most challenging problems that IoT researchers' need to deal with, especially broadcast data source authentication. Several research works considered broadcast data source authentication, in order to provide source authentication and broadcast data integrity, while taking in account induced overheads at constrained devices and resistance to resources-draining DoS (Deny of Services) attacks. Amongst these works, several are based on time asymmetry such as µTESLA, BABRA and H2BSAP. In our thesis, we studied and presented some of those works, and implemented and simulated µTESLA protocol under CONTIKI OS.

Keywords: IoT,authentication,BSAP,broadcast source, µTESLA ,DoS attacks, resources-draining.

ملخص

مفهوم تقنيات عمليات (إنترنت الأشياء) هو التطور القادم من الإنترنت التقليدية، مما يتيح الربط الشبكي، وتحديد الهوية (مثل IP @) والعرض / وصول الخدمة لأي شخص كان / الكائن الظاهري أو المادي، في الحياة اليومية، وفتح آفاق مجالات جديدة للاستخدامات والتطبيقات.في هذا السياق، الأمن يبرز بوصفه مصدر قلق بالغ ويلفت الكثير من الانتباه خاصة فيما يتعلق بالتصديق على التواصل ومصدر البث, وقد ركزت العديد من الدراسات البحثية على بروتوكولات التوثيق والرسوم البيانية من مصدر البث لضمان كل من هوية المصدر وسلامة البيانات الخاصة به، مع الأخذ بعين الاعتبار قيود أخرى مثل كائنات الموارد المنخفضة ومقاومة هجمات حجب الخدمة (الحرمان من الخدمات) من خلال استنفاد الموارد. ومن بين هذه الأعمال، العديد التي تقوم على التماثل من الوقت مثل البروتوكولات µTESLA BABRAوH2BSAP. في مذكرتنا درسنا وقدمنا بعض من هذه البروتوكولات وقمنا بتنفيذ ومحاكاة بروتوكول µTESLA باستخدام نظام التشغيل CONTIKI الذي يعتبر نظام تشغيل بامتياز في تقنيات العمليات .

الكلمات المفتاحية : تقنيات العمليات, المصادقة ,مصدر بث, هجمات حجب الخدمة, استنفاد الموارد.