Université Abou Bekr Belkaid
Tlemcen Algérie
جامعة أبي بكر بلقايد
تلمسان الجزائر

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

Approche distribuée basée sur la diffusion pour la gestion des clés dans l'Internet des Objet

Réalisé par :

- **MESELLEM Ahmed**
- **MOULA Mohammed Zineddine**

Présenté le 13 Septembre 2018 devant le jury composé de :

- *Mr MERZOUG Mohammed* *(Président)*
- *Mr MANA Mohammed* *(Encadreur)*
- *Mr BENAMAR Abdelkrim* *(Examinateur)*

Année universitaire : 2017-2018

Remerciements

Nous remercions en premier lieu ALLAH de nous avoir donné non seulement le courage mais aussi la force et la volonté nécessaire pour la réalisation de ce modeste travail.

Nous tenons à exprimer nos profondes gratitudes et nos sincères remerciements à notre encadreur M. MANA Mohamed 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 vifs remerciements s'adressent à nos parents, nos frères et sœurs pour leur soutien moral et leur encouragement.

Nous remercions nos chers ami(e)s qui sont toujours présents et fidèles.

Nous adressons nos remerciements aux membres de jury qui ont fait l'honneur d'évaluer, examiner et enrichir notre modeste travail.

Notre reconnaissance va particulièrement à l'ensemble des enseignants du département Informatique de l'université DE TLEMCEN tout ce qui nous a été transmis tout au long de notre formation.

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

Abstract

The proliferation of mobile networks and heterogeneous connected objects without pre-established infrastructure have given rise to the paradigm of the Internet of Things (IoT). However, the inherent vulnerability of these autonomous networks introduces new security challenges due to the limits of its objects in terms of storage capacity, computing and energy. We are interested in the security domain in key management, and around this context, our work has been focused.

Our Broadcast-based distributed approach uses elliptic curve cryptography, and particularly Diffi-Hellman exchange to provide robust key negotiation, lightweight authentication, and Replays-style attack protection.

The protocol developed under Contiki is tested with the Cooja simulator in Z1 low energy wireless network modules, and the results of the simulation are shown.

Key words: IoT, Key management, Contiki, Cooja, Distributed systems.

Résumé

La prolifération des réseaux mobiles et les objets hétérogènes connectés sans infrastructure préétablie ont donné naissance au paradigme de l'Internet des Objets (IdO). Or, la vulnérabilité inhérente de ces réseaux autonomes introduit de nouveaux challenges de sécurité grâce aux limites de ses objets en termes de capacité de stockage, puissance de calcul et l'énergie. Nous nous intéressons dans le domaine de sécurité à la gestion des clés, et autour de ce contexte, notre travail s'est articulé.

Notre approche distribuée basée sur la diffusion utilise la cryptographie à courbe elliptique, et particulièrement l'échange de Diffi-Hellman pour assurer une négociation robuste des clés, une authentification légère et une protection contre les attaques de type « Replays ».

Le protocole développé sous Contiki, est testé avec le simulateur Cooja dans des modules de réseaux sans fil à basse consommation d'énergie Z1, et les résultats de la simulation sont représentés.

Mots Clés : IdO, gestion des clés, Contiki, Cooja, systèmes distribués.

Table des matières

Liste des figures

Liste des tableaux

Abréviation

6Lowpan	IPv6 Low power Wireless Personal Area Networks ou IPv6 LoW Power wireless Area Networks.
ACK	Acquittement
AKMS	Area Key Management Server
AOL	Active Object List
BS	Base Station
CCM	Counter with CBC-MAC
CN	Constrained node
CoAP	Constrained Application Protocol
DABBKM	Distributed Approach Broadcast-Based Key Management Protocol
DH	Diffi-Hellman.
E2E	End-to-End
ECC	Elliptic Curve Cryptography
ECDH	Elliptic curve Diffie–Hellman
ECQV	Elliptic Curve Qu-Vanstone
EPC	*Electronic Product Code*
HMAC	keyed-hash message authentication code
ID	Identifier
IdO	Internet des objets
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of things
IPSO	IP for Smart Object
IPv4	IP version 4
IPv6	IP version 6
ITU	International Telecommunication Union
JNI	Java Native Interface
K_{CN}	Constrained node key
LR WPAN	Low Rate Wireless Personal Area Network
MD2	Message Digest 2

NFC	Near Field Communication
RCSFs	Réseaux de capteurs sans fil
RFID	radio frequency identification
RSA	Rivest–Shamir–Adleman
SHA-1	(Secure Hash Algorithm
TEK	Traffic Encryption Key
TP	Third Parties
UN	Unconstrained node
WSN	Wireless Sensors Network

Introduction générale

1. Contexte

La prolifération des réseaux mobiles et les objets hétérogènes connectés sans infrastructure préétablie (étiquettes, capteurs, actionneurs, téléphones mobiles, RFID) ont donné naissance au paradigme de l'Internet des Objets [1]. Les capacités de ce dernier ; d'assurer des communications sans fil n'importe quand et n'importe où ; d'adaptation à toute situation ; d'auto-organisation et auto-recouvrement après pannes rendent ce paradigme favorite pour diverses applications civiles et militaires [1].

La majorité des objets déployés dans l'Internet des Objets sont caractérisés par de fortes contraintes dues à la limitation de ressources (énergie, stockage, calcul et bande passante). Ces limitations introduisent un nouveau challenge de sécurité vu l'impossibilité d'application des protocoles de sécurité classiques essentiellement pour faire face à la vulnérabilité inhérentes due des attaques internes menées par des entités malveillantes [1].

Nous nous intéressons dans notre travail à la partie de gestion des clés pour sécuriser les communications entre les nœuds, et nous visons d'améliorer une approche distribuée en se basant sur des échanges de type Broadcast.

2. Structure du document

Ce mémoire est organisé comme suit :

Dans le premier chapitre, nous présentons les concepts de base de l'Internet des Objets, ses domaines d'application et ses challenges. Dans le second chapitre, nous étudions quelques approches déployés de gestion de clé et nous comparons entre elles. Après cela, nous proposons une amélioration à une approche présentée déjà dans le second chapitre avec présentation des résultats de simulation. Nous finissons notre mémoire par une conclusion générale et quelques perspectives.

1 L’Internet des Objets

1. Introduction

L’évolution importante de l’Internet en termes de services offerts aux utilisateurs et de nombre d’entités connectées, rend de ce réseau mondial indispensable dans tous les domaines de la vie quotidienne (économie, communication, militaire, etc.).

Depuis sa création en 1969, Internet était « ***L’Internet des ordinateurs*** » où il regroupait des milliards de connexions et d’échanges entre des équipements informatiques et offrait aux utilisateurs un ensemble de services (navigation web, téléchargements, etc.) ; jusqu’à sa migration vers « ***L’Internet des personnes*** » grâce à la tendance des services de messageries et des réseaux sociaux où des flux de données sont échangés entre des personnes connectées. Dans nos jours, les équipements d’accès à Internet varient de grosses stations de travail à des miniatures appareils mobiles intelligents (Tablettes, Smartphone, etc.) équipés de plus en plus par des capteurs et d’actionneurs permettant l’interagir avec l’environnement physique. L’étendage d’Internet d’un réseau offrant des services sur des données stockées dans des machines à des services d’accès à des objets physiques est connu sous le nom de « ***L’Internet des objets*** » [2].

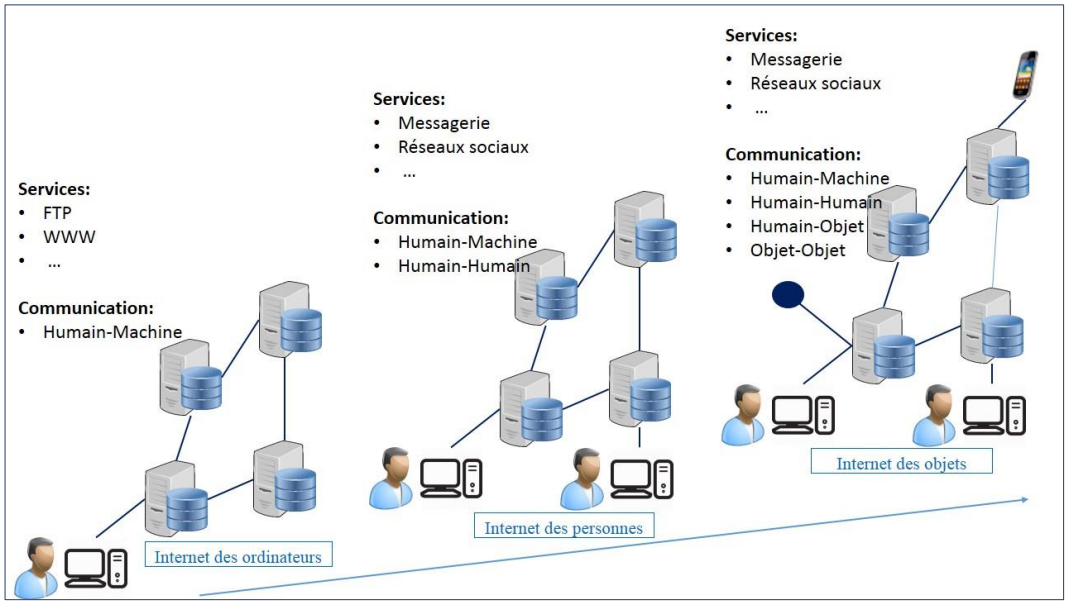

Figure 1 L'évolution de l'Internet [2]

2. Qu'est-ce que l'Internet des Objets ?

Vu la nouveauté de l'Internet des objets (IdO), plusieurs définitions ont été proposées. Ces dernières se diffèrent les unes des autres selon le domaine d'intérêt et le champ d'application.

Focalisant sur l'aspect technique et l'avancement technologique offert par l'Internet des objets, cette technologie se définie comme « un réseau des réseaux qui permet, via des systèmes d'identification électroniques normalisés et unifiés, et des dispositifs mobiles sans fil, d'identifier directement et sans ambigüité des entités numériques et des objets physiques et ainsi de pouvoir récupérer, stocker, transférer et traiter, sans discontinuité entre les mondes physique et virtuels, les données s'y rattachant » [3].

Autrement, si on focalise sur la signification des aspects qui le compose, et le considérer comme une extension de l'Internet à part entière, on peut définir l'IdO comme « un terme qui réfère à la nouvelle évolution de l'Internet dans laquelle il est étendu à des objets réels présents dans notre vie quotidienne (capteurs, actionneurs, livres, voitures, etc.). A travers un schéma d'adressage unique, l'IdO connecte plusieurs objets capables d'interagir avec l'environnement physique et de coopérer entre eux et avec les utilisateurs dans le but d'atteindre un objectif commun». [4].

En d'autres termes, l'IdO est l'amélioration d'Internet qui offre la possibilité d'accès à un monde intelligent supportant la connexion en plus de matériel informatique, tout objet (physique ou virtuel) qui peut être individuellement adressable [système d'identification électronique, RFID,@IP, etc.] pour permettre plus d'interaction et assurer un environnement ubiquitaire en terme d'autonomie de communication entre des objets hétérogènes. Cela permet aussi une haute disponibilité des données et de communication de tous genres [humain-machine, humain-humain, humain-objet, objet-objet] [5].

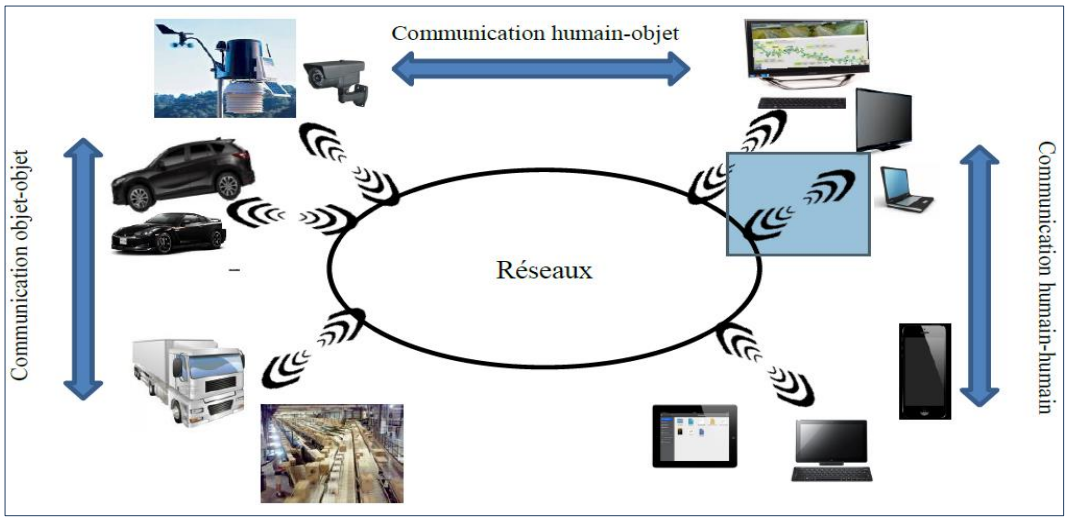

Figure 2 Différents types de communication dans l'Internet des Objets [5]

3. Nature des objets communicants

L'incorporation des objets du monde physique au monde virtuel (Internet) est le paradigme sur lequel repose l'Internet des Objets.

Selon les critères posés par [6], une entité est considérée comme un objet de l'IdO :

- Si elle a une existence physique (poids et une forme dans l'espace).
- Si elle est identifiée de manière unique et son identifiant ne doit pas se changer quel que soit la raison.
- Si elle a une adresse qui peut servir pour la trouver. Cette adresse est associée à un nom lisible par l'être humain.
- Si elle est capable de communiquer (ex : recevoir et répondre à une requête).
- Si elle est en mesure d'effectuer des calculs : une requête et sa réponse (Tags RFID passifs, calculs, mesure des phénomènes physiques, actions sur l'environnement).

De ces critères, la majorité des appareils électroniques peuvent être des objets de l'Internet des Objets (Tablettes, Smartphone, caméra IP, etc.), cependant plusieurs entités qui nous entourent ne répondent pas à ces critères (produits alimentaire, etc.) et doivent augmentés par une autre technologie pour pouvoir être incorporés eux même dans l'Internet des Objets.

4. Historique et évolution

Entre 1999 et 2003, *Kevin ASHTON* du laboratoire «*Auto-ID Research Center* » avec son équipe ont réalisé un projet de production qui vise l'incorporation dans un réseau de communication « *Network of Bits* » des objets physiques identifiables « *Network of Atoms*». Pour ce projet, ils ont conçu un système mondial d'identification EPC (*Electronic Product Code*) à base de la technologie RFID (identification par radio). Cette technologie est utilisée pour marquer les objets physiques avec des tags RFID ; puis lire et écrire des informations relatives aux objets de manière sans fil et à partir des équipements connectés aux réseaux informatiques [7].

En 2005, l'ITU (*International Telecommunication Union*) a publié un rapport sur l'IdO en montrant la puissance d'exploiter ce concept pour développer un réseau d'accès ubiquitaire [n'importe qui, n'importe où, n'importe quand, de n'importe quel objet] comme l'illustre la figure 3.

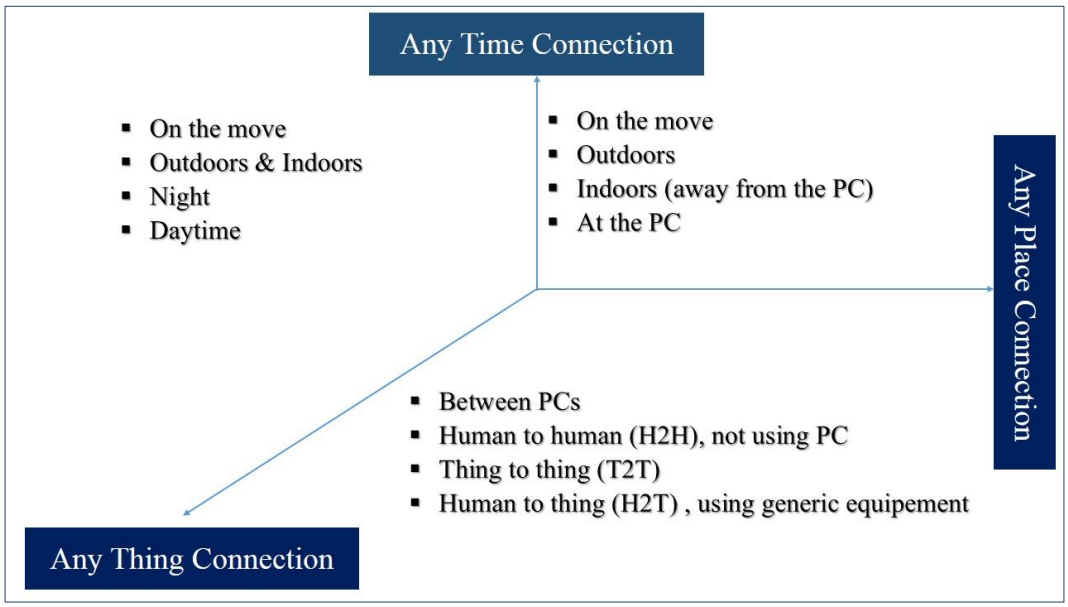

Figure 3 La vision ubiquitaire de l'ITU [24]

En 2007, l'Union Européen a adopté ce concept dans « *The Commission Communication On RFID* » et par les Etas Unies dans « *National Intelligence Council* » en 2008.

Aujourd'hui, L'internet des Objets est considéré comme l'extension d'Internet englobant plusieurs technologies Software / Hardware, modélisation des données, stockage, réalité virtuelle, traitement et technologies de communication. Il ne correspond plus à la vision de Kevin ASHTON ; il regroupe trois visions comme l'illustre la figure 4. [4]

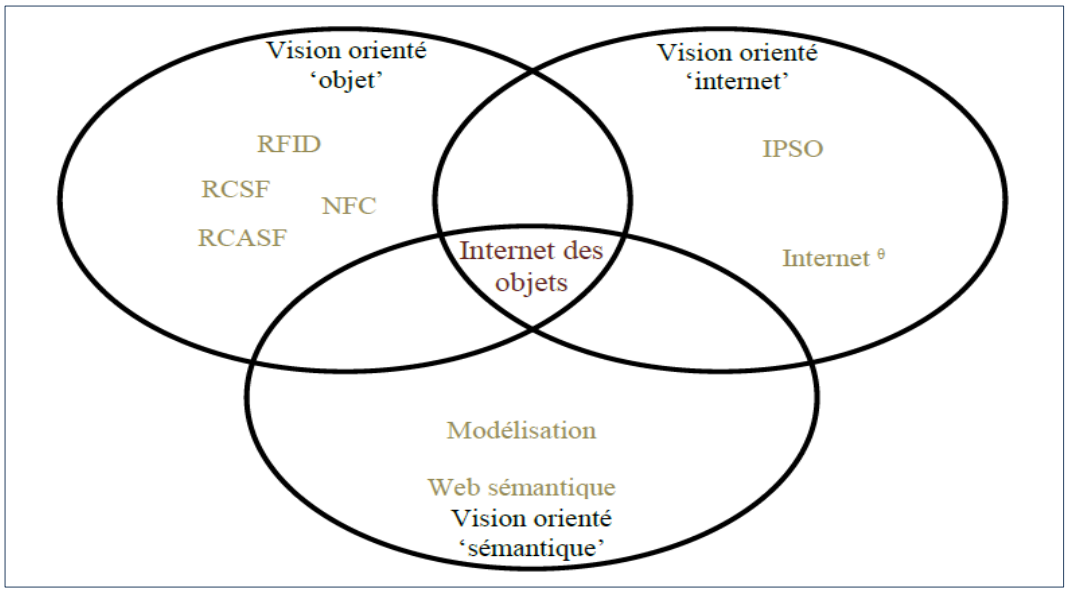

Figure 4 Visions de l'Internet des Objets [4]

- **Vision orientée Objet**

  L'IdO ne se limite pas à des tags RFID, mais il comprend aussi des capteurs, des actionneurs et même des appareils intelligents (Smartphone, caméra, etc.).

- **Vision orientée Internet**

  L'Internet constitue l'élément clef de cette infrastructure, donc il doit tenir compte des caractéristiques des objets connectés (consommation d'énergie, scalabilité, etc.). IPSO[1] un exemple d'alliance crée pour ça.

- **Vision orientée Sémantique**

  L'interaction entre les objets communicants doit avoir un sens. Pour cela, les outils de modélisation sont très utilisés pour permettre la présentation, le stockage, la recherche et l'organisation des données générées.

[1] IPSO: IP for Smart Object.

5. Architecture

Selon les fonctionnalités, L'Internet des Objets peut être vu comme trois couches superposées comme l'illustre la figure 5. [8]

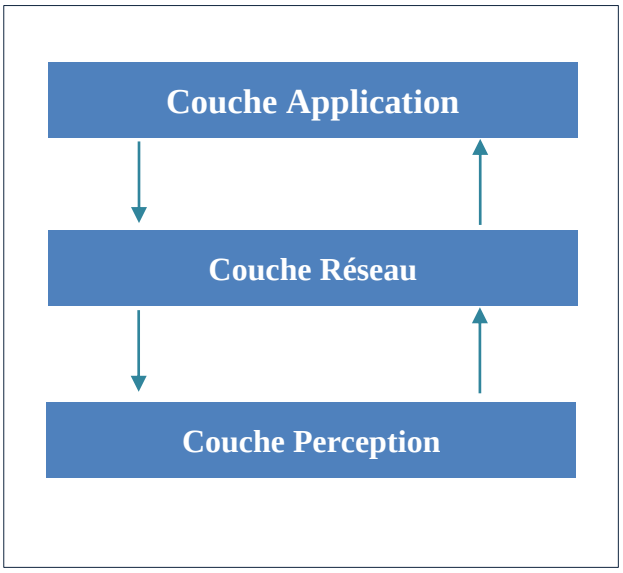

Figure 5 Architecture de l'Internet des Objets [8]

- **Couche perception**

  Son rôle est l'identification des objets réels, la collecte d'informations et apporte des actions sur l'environnement physique. Cette couche regroupe les capteurs, les actionneurs, les caméras, les tags et les lecteurs RFID, etc. Les informations perçues par cette couche sont converties au numérique pour exploitation par les autres couches.

- **Couche réseau**

  C'est l'infrastructure de communication qui transporte les informations collectées par la couche perception, et qui donne à l'Internet des Objets son aspect ubiquitaire. Cette couche représente un réseau de convergence qui réunit l'Internet avec les autres réseaux de communication. Elle est responsable du stockage et du traitement des données.

- **Couche application**

  Cette couche offre plusieurs applications et services à partir des données traitées par la couche réseau.

6. Domaines d'application

- **Domaine médical || E-Heath**

  L'Internet des Objets joue un rôle important dans le domaine médical. Un réseau de miniatures capteurs avalés ou implantés sous la peau, peut être déployé pour assurer la surveillance des patients (température, pression du sang, activités de respiration, rythme cardiaque, etc.) indépendamment de leurs environnements. Ce réseau communique l'état de santé du patient au médecin en temps réel via une application mobile qui joue la passerelle entre le réseau corporelle et l'Internet [9].

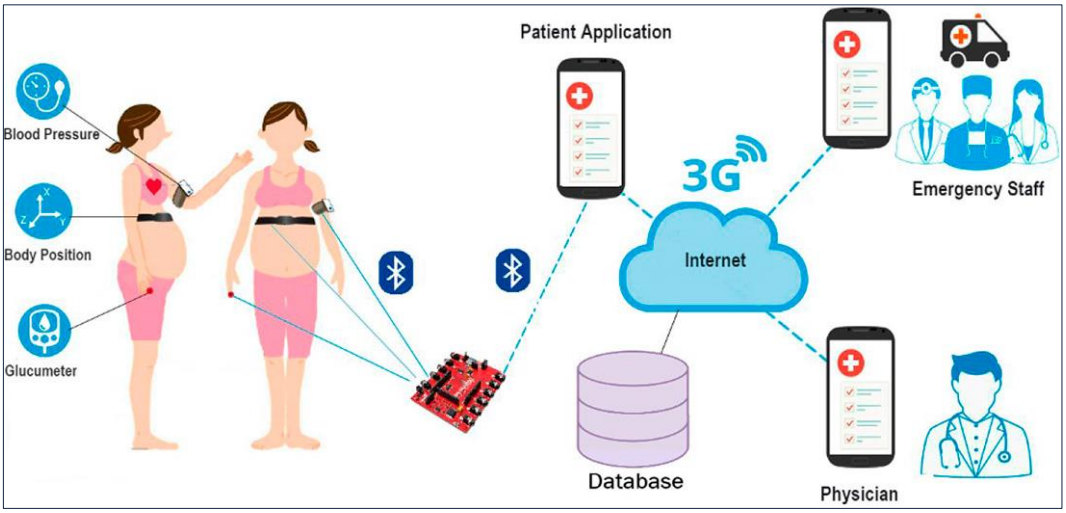

Figure 6 Application intelligente e-Health pour le suivi de grossesse à l'aide du diagramme de projet Body Area Networks [10]

- **Domotique || Smart Home**

  L'IdO permet l'accès à un monde ambiant, ou les objets domestiques collaborent entre eux pour améliorer l'habitat humain. Ce concept permet de gérer tous les équipements (tâches ménagères, verrouillage des portes / fenêtres, vidéo surveillance, etc.) en-site ou à distance via un réseau de communication [11].

Figure 7 Services de la domotique [12]

- **Réseaux électriques intelligents || Smart Grid**

  Un réseau électrique intelligent est un réseau amélioré grâce à l'intégration des énergies renouvelables et des TIC en garantissant la communication bidirectionnelle entre les différents acteurs du réseau et en temps réel. Il vise à garantir la disponibilité, l'efficacité, le coût réduit et la sécurité de l'énergie fournie [13].

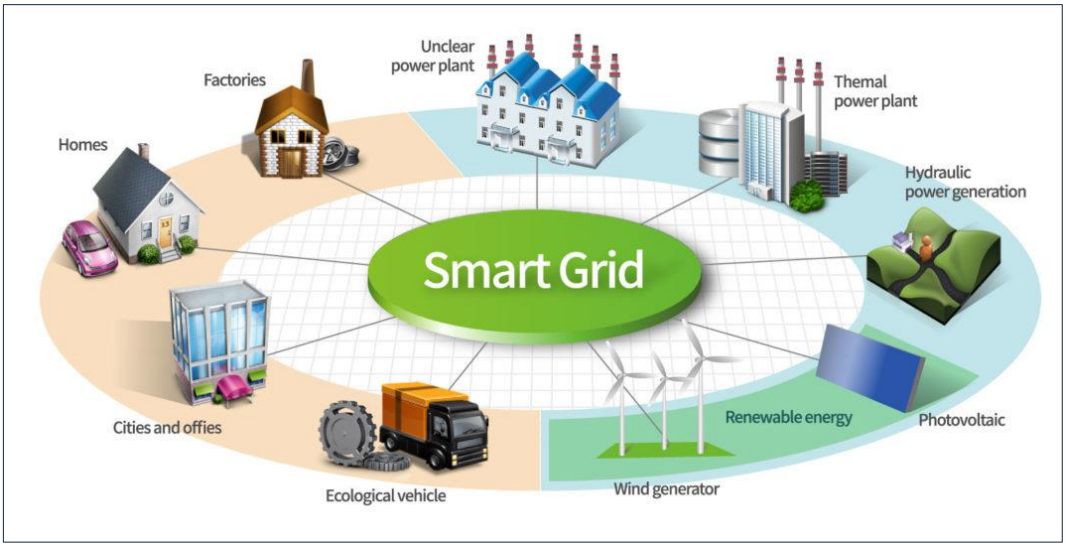

Figure 8 Services du Smart Grid [14]

- **Transport**

  Les cartes touristiques peuvent être équipées par des balises à base de la technologie NFC[2], et permettre au Smartphone de récupérer via le web les informations qui peuvent intéresser les touristes (hôtels, restaurants, évènements) [13].

Figure 9 IoT dans les transports [15]

- **L'industrie**

  Le problème des pièces non homologues résultant de l'utilisation des pièces qui ne répondent pas aux exigences (Suspected Unapproved Parts) particulièrement dans le secteur de l'aéronautique peut être résolu à l'aide de l'IdO en marquant chaque pièce avec des tags contenant des identifiants et permettant la récupération automatique des informations relatives à la pièce [13].

[2] NFC (Near Field Communication) : une technologie sans fil à haute fréquence et courte portée [59].

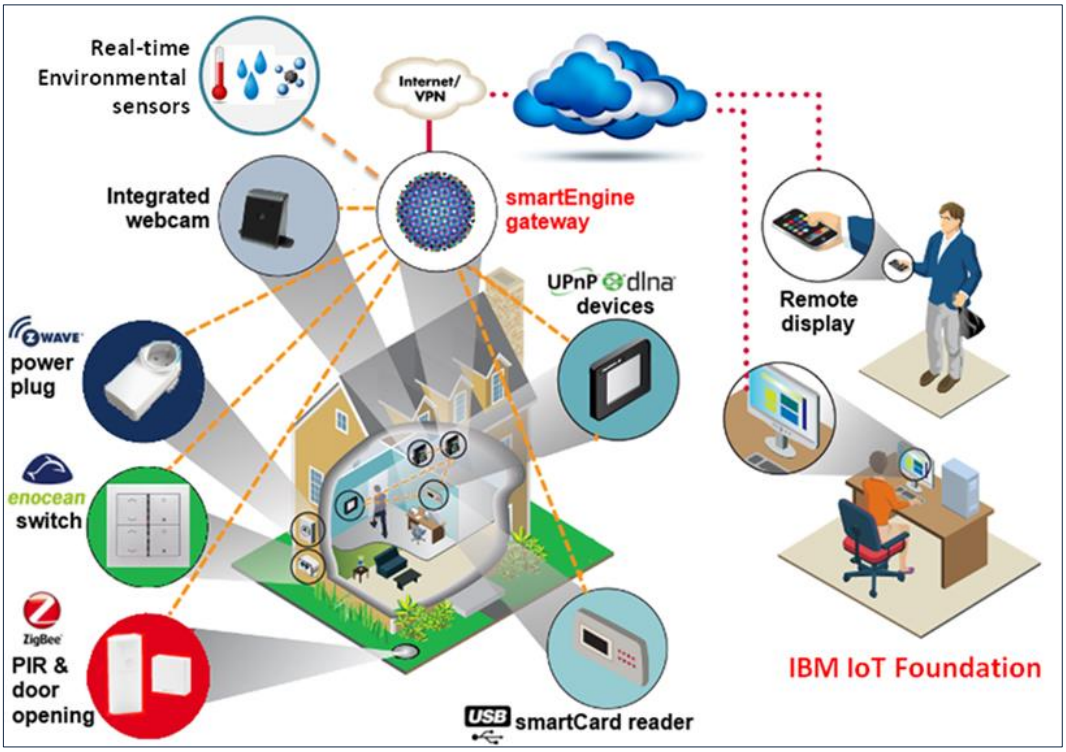

Figure 10 IoT dans l'industrie [16]

- **Prévision de catastrophes**

  Un réseau de capteurs peut être déployé pour mesurer des paramètres afin de prédire des catastrophes naturelles. En analysant ces paramètres à base d'un modèle alimenté des données collectées, le centre de traitement prédit des catastrophes [13].

7. Les challenges de l'Internet des Objets

Dans l'IdO, tout objet doit être identifiable, capable de communiquer et d'interagir avec l'environnement auquel il appartient [6]. Pour satisfaire ces contraintes, et avec les caractéristiques des nœuds ; de nouvelles techniques doivent être mises en place. Parmi les challenges les plus important de l'IdO :

- **Déploiement de l'IPv6**

  Le nombre d'entités à connecter dans l'IdO augmente et d'une manière exponentielle. Et vu, la limite de l'IPv4 en termes d'espace d'adressage (2^{32}), il est primordial de recourir à un adressage IPv6 (2^{132}) [17]. Aussi la taille des identifiants du RFID (64 || 96 bits) est une contrainte pour l'intégration de ces derniers dans IPv6 [18], [4].

- **L'auto-configuration**

  L'auto-configuration et l'adaptation avec l'environnement est un défi majeur devant l'IdO vu le nombre important d'objets à connecter et leurs hétérogénéité et la limites de la configuration manuelle [19].

- **Sécurité**

  La sécurité est l'élément le plus important qui pose des obstacles devant l'adaptation des êtres humains des applications de l'IdO suite aux menaces concernant la vie privées des utilisateurs [19].

8. Sécurité de l'Internet des objets

Sécuriser un système informatique implique directement l'atteinte des objectifs suivants :

- **L'Authentification**

  En contrôlant et identifiant les nœuds au sein d'un réseau, l'authentification permet la coopération entre eux. Cette phase précède toutes les autres phases, et on ne peut jamais assurer une confidentialité et intégrité de donnée si l'authentification est mal gérée, et un simple attaquant peut rejoindre le réseau et injecte des messages erronés. L'utilisation d'un code d'authentification de message MAC[3] permet d'assurer l'authentification de l'origine et l'intégrité de message [20].

- **L'intégrité**

  Les données reçues par le nœud récepteur doivent être identiques à celles envoyées par le nœud émetteur sans aucune altération. Pour chaque message envoyé, une empreinte digitale est générée par une fonction de hachage pour assurer une intégrité[4].

- **La confidentialité**

  Cette propriété est assurée par l'utilisation de clés cryptographiques (symétrique || asymétrique). Elle consiste à préserver le secret du message échangé et de ne pas le révéler aux adversaires.

[3] HMAC : exemple de MAC [20].
[4] Message Digest 2 (MD2) [53], Message Digest 5 (MD5) [54], Secure Hash Algorithm (SHA-1) [55] : exemples des fonctions de hachage.

- **La disponibilité**

  Le réseau doit être disponible à tout moment et autorise les parties communicantes l'utilisation du medium quand c'est nécessaire.

- **La fraicheur**

  Les données échangées doivent être actuelles, et ne sont pas des réinjection des échanges précédents interceptés par des attaquants.

  Les propriétés citées précédemment constituent un défi majeur devant l'Internet des Objets avant que ce paradigme devient une réalité. La vulnérabilité des objets de l'IdO aux attaques de sécurité est due de l'impossibilité d'application des standards de sécurité classique grâce à la densité importante du réseau et sa topologie dynamique, la limite des nœuds en ressource (stockage, calcul, énergie) et le type de communication (sans-fil).

9. Conclusion

Nous avons présenté dans ce chapitre le concept de l'Internet des Objets, son architecture, ses domaines d'applications, et ses challenges. Parmi les challenges cités, on retient la sécurité qui constitue un défi majeur devant sa popularité.

Nous nous intéressons dans notre étude à une partie importante de la sécurité de l'Internet des Objets, il s'agit de la gestion des clés. Le chapitre suivant présente les travaux réalisés dans cet axe, et une comparaison de performance pour les différentes méthodes présentées.

2
Gestion des clés dans l'Internet des Objets

1. Introduction

La gestion des clés constitue une partie importante de la sécurité des systèmes informatiques basés sur la communication. Sous les contraintes posées par les caractéristiques des nœuds de l'IdO présentées précédemment, la conception d'une approche de gestion des clés constitue un défi majeur.

La solution la plus performante en cryptographie est celle à clé publique[5] (cryptographie asymétrique) car elle fournit des mécanismes fiables pour l'authentification et la distribution des clés. Cette solution nécessite une capacité de calcul et un espace mémoire importants.

Les études [21], [22] ont montré qu'il est possible d'appliquer la cryptographie asymétrique dans des réseaux de capteurs si on arrive à choisir les algorithmes et les paramètres adaptés. D'autres études [22], [23], [24] ont montré que l'utilisation de la cryptographie à courbe elliptique ECC [6] donne de meilleures performances en termes de niveau de sécurité et taille des clés par rapport à l'application de RSA[7] [25]. Aussi plusieurs adaptations de la cryptographie à courbe elliptique ont été réalisées dans d'autres études sur les réseaux de capteurs sans-fil [26], [27], [28].

[5] On distingue deux classes de cryptographie : symétrique (utilisation de la même clé pour le chiffrement et le déchiffrement) et asymétrique (utilisation de deux clés la publique pour le chiffrement et la privée pour le déchiffrement.) [57].

[6] ECC signifie la cryptographie sur les courbes elliptiques qui regroupe des techniques cryptographiques qui utilisent des propriétés des courbes elliptiques, ou plus généralement d'une variété abélienne

[7] Le chiffrement RSA est *asymétrique*, il utilise une paire de clés (des nombres entiers) une *clé publique* pour chiffrer et d'une *clé privée* pour déchiffrer des données confidentielles.

2. La gestion des clés

L'aspect le plus difficile à configurer dans un système cryptographique est la gestion des clés. Toutes les parties communicantes doivent disposer de clés cryptographiques ou paires de clés qui sert au chiffrement et de déchiffrement des messages. Le protocole dans sa totalité doit être capable de générer et de distribuer d'une manière sécurisée les clés et chacune de ces parties capable de vérifier et de stocker ces clés. La figure 11 illustre les fonctions de la gestion des clés [29].

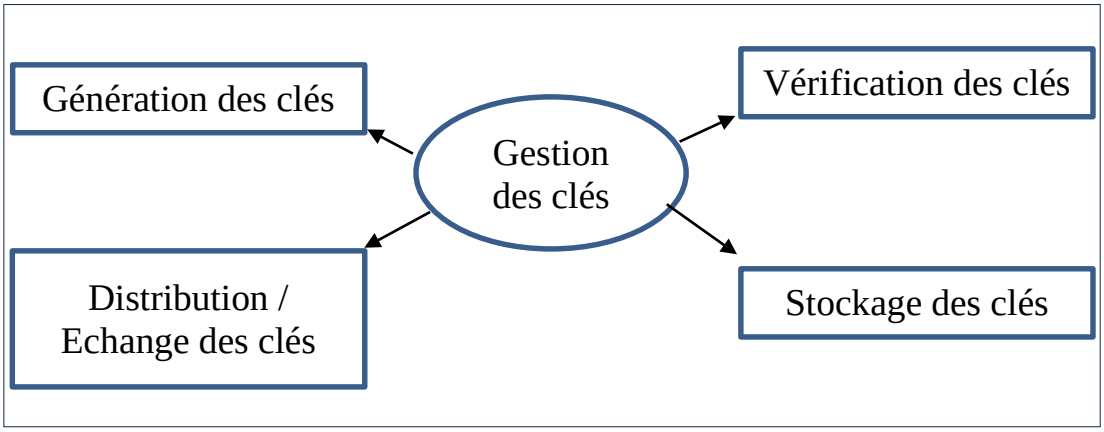

Figure 11 Fonctions de la gestion des clés [58]

3. Approches de gestion des clés dans l'IdO

3.1. Approches centralisées

3.1.1. Système coopératif de gestion des clés point à point

An End-to-End Secure Key Management Protocol for E-health Applications [30]

L'approche proposée dans cet article est basée sur la collaboration pour création un canal de communication sécurisé. Ce dernier permet un transfert confidentiel et authentique des données entre un nœud à ressource limitée (Constrained node CN) et une entité distante (Unconstrained node UN). Dans cette approche, Les primitives cryptographiques hautement consommatrices sont déchargées vers des tiers (élément clé du protocole). La figure 12 présente l'architecture sur laquelle est basé le protocole [30].

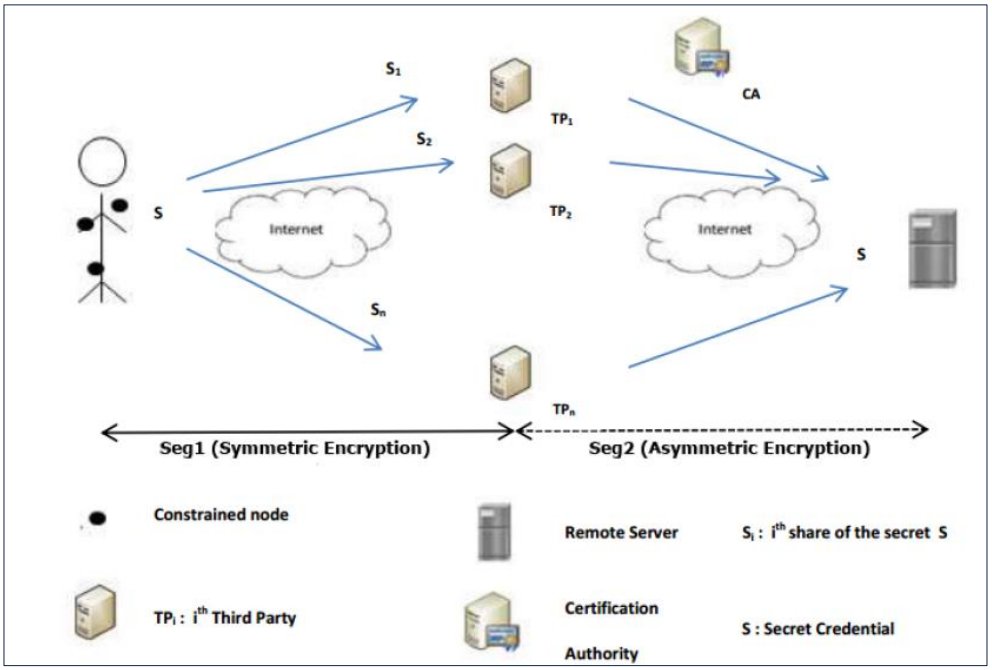

Figure 12 Le système utilisé [30]

Comme l'illustre la figure 13, les étapes du protocole sont [30]:

- **Phase initiale :** Chaque nœud CN est pré chargé avec $\begin{cases} Identités\ des\ tiers\ TPi \\ Clés\ pré\ partagées\ (KCN, TPi) \end{cases}$
- **Phase d'échange initial :** Le CN initie l'échange avec UN en lui envoyant un message CN_Hello contenant les politiques de sécurité et le processus d'établissement de la clé coopérative. Le UN sélectionne une des politiques de sécurité proposées et répond avec un message UN_Hello[8].
- **Phase de sécurisation de connexion entre les entités :** cette phase vise de sécuriser le canal de communication soit entre le CN et le TP_i ou le TP_i et le UN. Le CN informe les TP_i sur l'identité de UN par un message qui contient un code d'authentification des messages (MAC), et il est crypté à l'aide du $K_{CN;TPi.}$ Les tiers répondent avec un message en exprimant leurs volontés de participer au protocole d'échange de clé. Chaque TP_i envoie à UN sa clé publique délivré par l'AC et demande à l'UN son propre certificat. L'UN vérifie la clé publique fournit par le tiers et répond avec le certificat demandé.

[8] Chaque message échangé contient des nonces pour faire face aux attaque de répétions.

- **Phase Prouver la représentativité des tiers du CN à l'UN :** L'authentification est réalisée en utilisant des clés pré-partagées entre CN et TP_i. Le UN demande au CN les clés par pairs. Après application d'une fonction de hachage pour garder les clés confidentielles, le CN envoie les clés à UN qui seront comparé plus tard après réception des clés de la part des tiers.
- **Phase Génération et livraison secrètes :** Un secret S est généré par le CN, divisée en m parties et sera utilisé plus tard entre CN et UN. Chaque partie S_i est envoyée à son tiers approprié. Chaque TP_i envoie la partie du secret S approprié, le $K_{CN;TPi}$ et sa signature. Le UN vérifie la représentativité de CN par le TPi par le biais de la comparaison de ce message avec celui reçu dans la phase précédente. UN reconstruit le secret S après réception de toutes les parties envoyées par les tiers pour dériver d'autres informations non échangées.
- **Phase de terminaison :** Cette phase conclut l'échange par un message prouvant au CN la connaissance du secret S.

  Le secret S et les nonces sont utilisés après par le CN et le UN pour dérivation d'une autre clé.

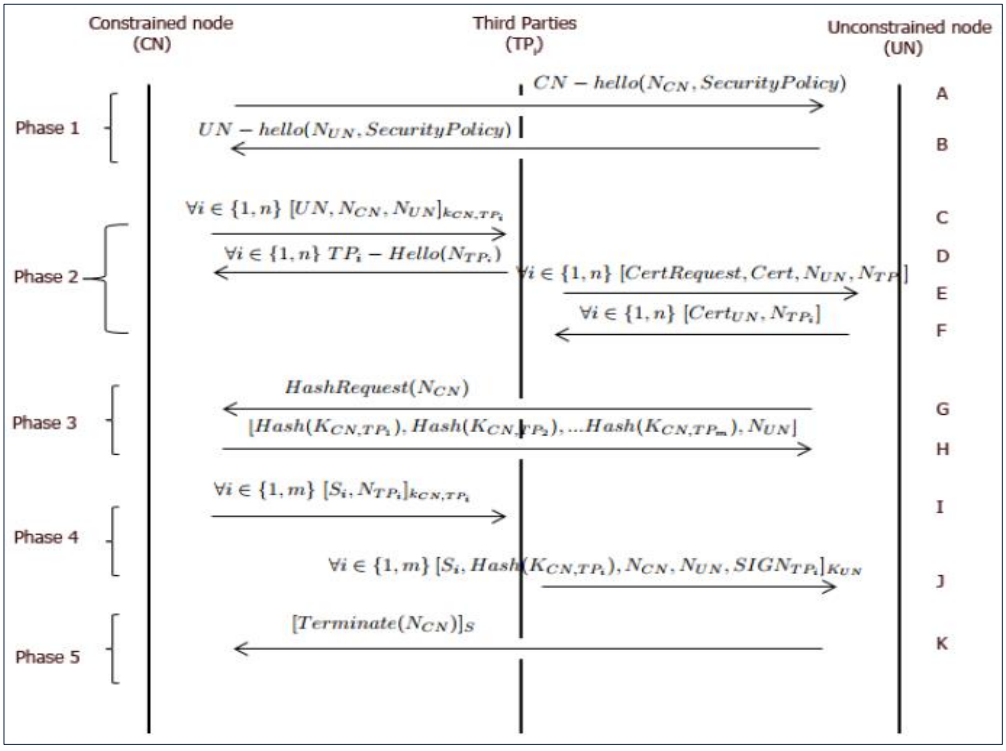

Figure 13 détails du protocole développé [30]

3.2. Approches décentralisées

3.2.1. Protocole de gestion de clé de groupe décentralisé par lot

A Decentralized Batch-based Group Key Management Protocol for mobile IoT [31]

Cette approche a pour objectif de sécuriser les communications multicast dans l'Internet des Objets mobile. Elle implique le protocole de gestion de clés[9] suivant [31] :

- Protocole optimisé et adaptable avec la topologie proposée comme l'illustre la figure 14.
- Tenir en compte les différents types d'applications multicast (un à plusieurs, beaucoup à plusieurs, beaucoup à un), la limite des ressources et la mobilité des nœuds.
- Faire face au problème de point unique d'échec, et le phénomène de 1-affects-n en proposant une architecture décentralisée[10] comme l'illustre la figure 15.
- Ne concerne que les objets actifs du réseau ce qui diminue la consommation d'énergie.
- Basé sur un modèle de réseau divisé en zones. Chacune des zones regroupe un ensemble d'objets et elle est sécurisée par une clé de groupe valide dans un intervalle de temps et différente des clés des autres groupes.
- Pour chaque zone, un AKMS[11] est responsable de l'établissement d'une clé de chiffrement $TEK_{i,t}$[12] pour chaque objet, et qui sert à sécuriser les communications à l'intérieur de la zone. La mise à jour des $TEK_{i,\ t}$ se fait par le AKMS lors d'un évènement (arrivé d'un nouvel objet, mouvement d'un objet entre les zones ou départ d'un objet).

[9] Protocole de gestion de clés : générer, distribuer et maintenir une clé partagée.
[10] Architecture décentralisée : Le GKMS est un back-up d'AKMS, en cas de défaillance de ce dernier, le GKMS assure la disponibilité.
[11] AKMS (Area Key Management Server) : serveur de gestion de clés de zone.
[12] $TEK_{i,\ t}$ (Traffic Encryption Key) : Clé de cryptage de clé pour l'objet i à la période t.

- Une liste des objets actifs AOL[13] dans l'AKMS mémorise les informations d'identification livrées aux objets pour chaque intervalle de temps.
- Les AKMS des différentes zones sont gérés par un General Key Management Server GKMS qui définit les politiques de sécurité pour l'ensemble des groupes et particulièrement la politique d'accès pour chaque domaine.
- Le réseau est hétérogène et contient deux types d'entités avec des capacités de calcul et des ressources différentes.
- Une fonction à sens unique[14] est utilisée pour la génération des clés. Elle a comme entrées la clé à long terme SK et un ticket valide $T_{i,t}$.
- Chaque zone est gérée par une seule gestion de clé approuvée, et l'ensemble du groupe est géré par une clé de confiance du serveur de gestion GKMS.
- La défaillance d'un membre par échec ou attaque n'affecte pas les autres membres, et la disponibilité est assurée à l'intérieur de la zone par le GKMS dans le cas de défaillance du AKMS.

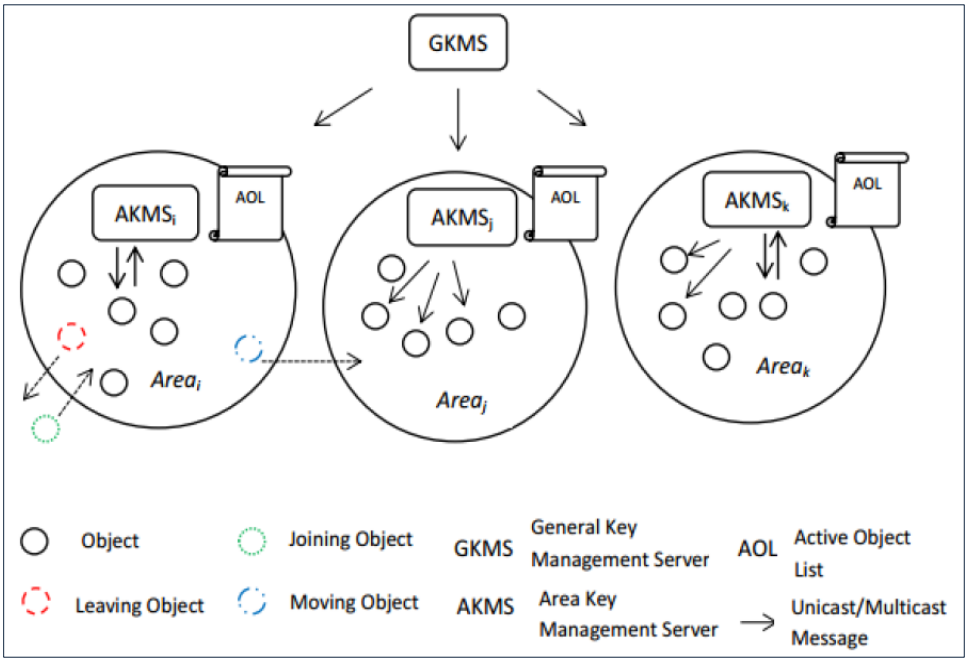

Figure 14 Modèle du réseau utilisé pour le protocole développé dans [31]

[13] AOL : Active Object List.

[14] Une fonction à sens unique garantie que les données utilisées comme entrée ne peuvent pas être récupérées à partir de la sortie résultante.

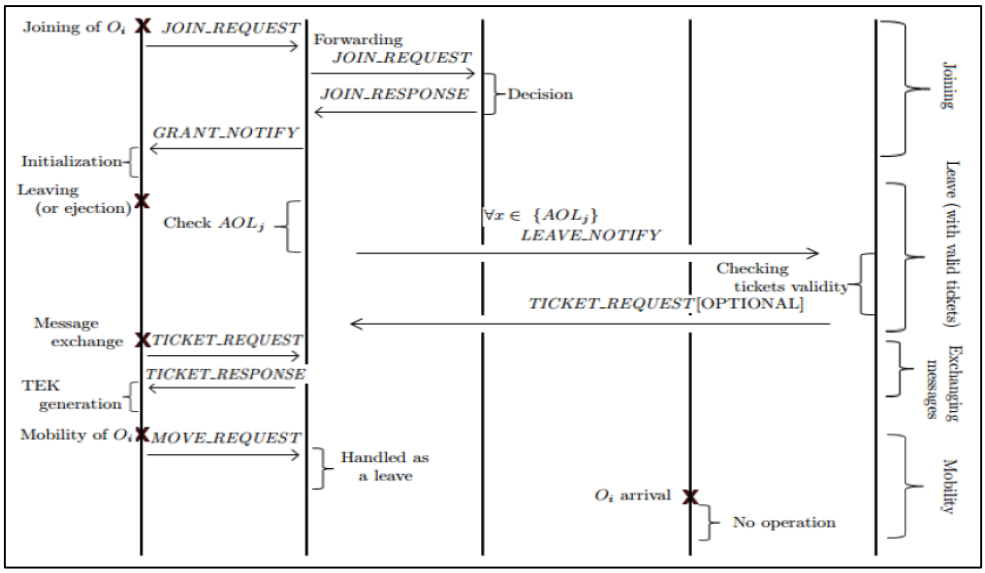

Figure 15 Echanges du protocole proposé en [31]

3.2.2. Protocole de gestion de clés hybride et efficace pour les RCSFs hétérogènes dans le context de l'IdO

An efficient and hybrid key management for heterogeneous WSN in context of IoT

Comme l'illustre la figure 16, ce protocole est développé en se basant sur une architecture de réseau hiérarchique et hétérogène de réseau de capteurs [32]. L'approche proposée combine entre la cryptographie sur les courbes elliptiques et la cryptographie symétrique pour amélioration de sécurité en tenant compte de la limitation des capteurs en termes de ressources. Trois types d'entités sont déployés dans ce réseau : [32]

- **Base Station (BS)**

  C'est un dispositif avec grande capacité de calcul, et source de confiance pour tous les nœuds, ce qui rend le traitement des différentes informations collectées possible à son niveau.

- **High-end Sensor(H-Sensor)**

  Présente le Cluster-Head, puisqu'il dispose d'une capacité énergétique importance, une large bande passante, espace de stockage et capacité de calcul. Il est doté par un matériel inviolable.

- **Low-end Sensor(L-Sensor)**

  Ces entités sont statiques avec des ressources limitées qu'H-Sensor.

La sécurisation des communications entre les nœuds est hybride combinant des clés symétriques et asymétriques, et la communication entre la station de base et H-Sensor est soit directe soit par l'intermédiaire d'autres H-Sensor.

Des pairs de clés partagées générées avant le déploiement par le biais d'ECC sont utilisés dans la communication entre deux entités ; et les clés partagées entre les nœuds sont générées au niveau d'H-Sensor par l'algorithme de Diffie-Hellman. [32]

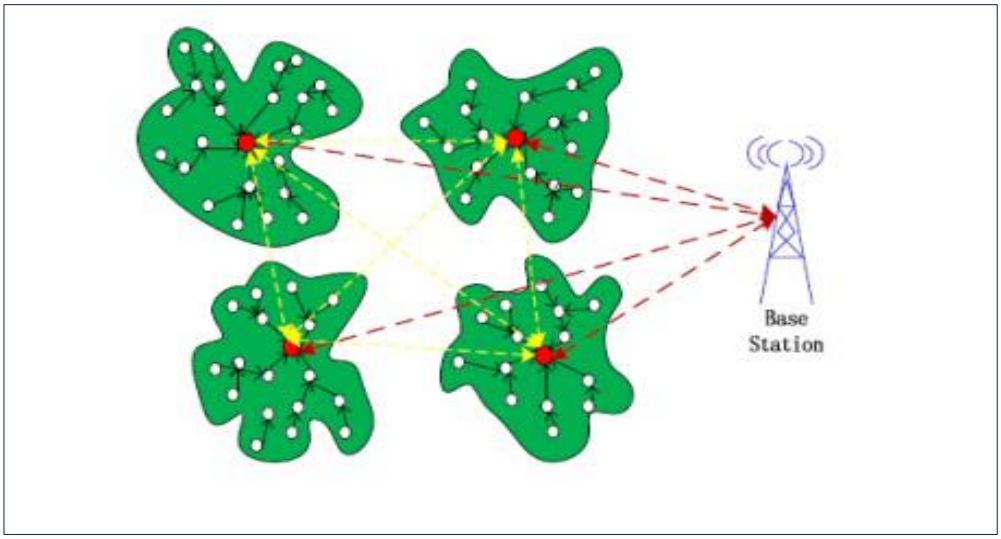

Figure 16 Le modèle réseau utilisé pour le protocole proposé dans [32]

3.3. Approches distribuées

3.3.1. Protocole de gestion de clés avec certificats implicites pour l'IdO

Key Management Protocol with Implicit Certificates for IoT systems [33]

Ce protocole de gestion de clés KPM (Key Protocol Management) est conçu pour les systèmes industriels et mobiles de l'IdO. Il est intégré à la couche 2 de la pile protocolaire 802.15.4[15] pour sécuriser les différents scénarios de l'IdO. Ce protocole est basé sur l'échange fixe de ECDH (Elliptic Curve Di_eHellman) et des certificats implicites par ECQV (Elliptic Curve Qu-Vanstone). Comme l'illustre la figure 17, le protocole est complété par l'échange des nonces et l'authentification des messages

[15] Le **802.15.4** est un protocole de communication défini par l'IEEE. Il est destiné aux réseaux sans fil de la famille des LR WPAN (Low Rate Wireless Personal Area Network) du fait de leur faible consommation, de leur faible portée et du faible débit des dispositifs utilisant ce protocole.

pour garantir une authentification mutuelle et une fraicheur dans la dérivation de clés [33].

Le protocole échange quatre messages logiques, les deux premiers contiennent les certificats implicites et les nonces. Des authentifications sont offertes par les certificats ECQV et chaque nœud est capable de calculer, via ECDH, un secret partagé à partir de la clé publique. Les deux derniers messages serrent à finaliser l'authentification mutuelle.

Les champs d'authentification des messages sont calculés en tenant compte des nonces échangé initialement pour faire face aux attaques de répétition.

Le secret négocié est utilisé pour la génération des clés utilisées dans l'algorithme CCM[16] de la norme IEEE 802.15.4.

La figure 17 détaille les échanges du protocole. [33]

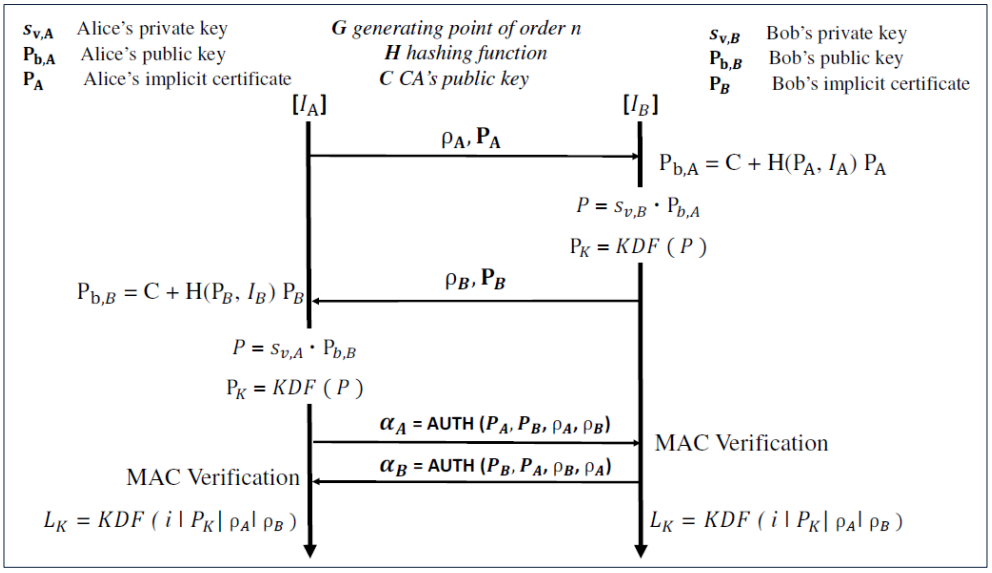

Figure 17 Protocole de négociation de clé [33].

[16] CCM : Les primitives cryptographiques de la norme IEEE 802.15.4

3.3.2. Protocole d'établissement de clés point à point base sur les proxies pour l'IdO

Proxy-based End-to-End Key Establishment Protocol for the Internet of Things [34]

Ce protocole distribué est basé sur le proxy de l'IdO. Il permet à deux dispositifs à haute performance d'établir une communication sécurisée E2E[17] entre eux. Ces dispositifs doivent maintenir une connexion avec les nœuds voisins déployés dans le même réseau local.

Les nœuds à ressources limités fonctionnent comme des proxies et collaborent pour le traitement des primitives cryptographiques consommatrices pour le calcul de la clé de session entre l'initiateur A et le répondeur B comme l'illustre la figure 18.

Aucun proxy des participants ne dispose d'informations des autres proxies participant à la génération de la clé finale K_{AB}, et ne peut collaborer pour dériver cette clé autre fois. [34]

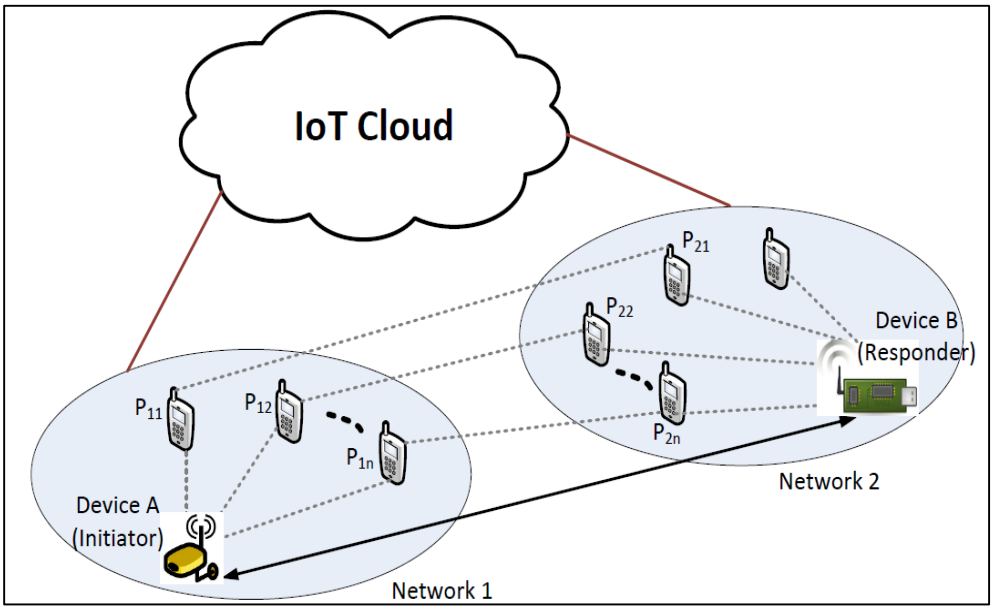

Figure 18 Modèle du réseau de l'approche proposée dans *[34]*

[17] E2E (End-to-End) : communication de bout en bout.

3.3.3. Protocole d'authentification à deux phases pour les réseaux de capteurs sans fil dans des applications distribuées

Two-phase Authentication Protocol for Wireless Sensor Networks in Distributed IdO Applications [35]

Ce mécanisme d'authentification est basé sur un certificat implicite ECQV pour les réseaux de capteurs sans fil dans des applications distribuées. Il permet l'authentification et l'établissement des connexions sécurisées entre des nœuds capteurs et des utilisateurs. Le réseau peut contenir des dispositifs hétérogènes et permet aux utilisateurs (réels ou virtuels) de collaborer avec les nœuds pour obtenir des informations sur un service particulier. Comme le montre la figure 19, les différents types de communications qui peuvent se produire : [35]

- Deux nœuds capteurs dans le même réseau RCSF (lien A).
- Deux nœuds capteurs dans des réseaux RCSF distincts (lien B).
- Un utilisateur et un nœud capteur (lien C).

Cette solution est composée de deux phases. Son schéma d'authentification est basé sur l'Elliptic Curve Cryptography et les certificats implicites utilisés sont générés par ECQV en s'appuyant sur l'échange de clé ECDH

- **Phase d'enregistrement :** consiste à obtenir les informations d'identification de sécurité pour chaque entité.
- **Phase d'authentification :** permet à deux entités du réseau l'établissement d'une communication sécurisée. [35]

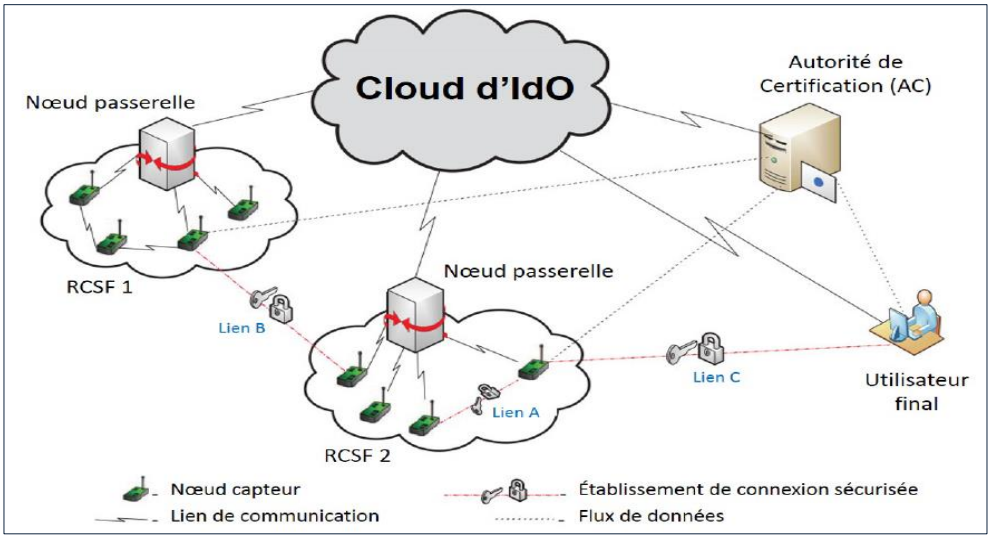

Figure 19 Différents types de communications possibles [35]

3.3.4. Un protocole de gestion de clés basé sur des nœuds de sécurité à haute efficacité énergétique pour les RCSFs

An Energy-efficient Security Node-based Key Management Protocol for WSN [36]

Pour les réseaux de capteurs sans fil, et afin d'améliorer le degré de sécurité des clusters-Heads et de minimiser l'énergie consommée pour l'établissement des clusters, un nouveau schéma de gestion de clé basé sur les nœuds de sécurité a été proposé. Les nœuds du réseau choisissent différentes clés pour le chiffrage selon le type de paquet des données ; ce qui impose au protocole l'utilisation de différents genres de clés.

Dans les RCSFs, le Cluster-Head joue un rôle important, alors sa sécurité doit être assurée, et lors de détection d'un comportement anormal doit être remplacé immédiatement. Les étapes de ce schéma sont les suivantes : [36]

- Chaque nœud génère un nombre aléatoire. Si ce nombre est supérieur à un nombre T, alors ce nœud peut jouer le rôle d'un nœud de sécurité. Lors de la détection d'un comportement anormal, les nœuds voisins envoient des rapports aux nœuds de sécurité.
- A l'arrivé d'un nouveau nœud au réseau, il diffuse son ID et attend des réponses de leurs voisins pour les découvrir. Quand un nœud reçoit ce message, il répond par un ACK en chiffrant le message par une clé publique ; et dès que l'ACK est reçu le nouveau calcule la clé par-paire entre eux.
- Une clé appelée clé de cluster est négocié entre les nœuds de sécurité. Chacun des nœuds de sécurité produit une clé et l'envoie aux autres avec une estampille de temps. La clé avec l'estampille minimale est considérée comme clé de cluster. Le cluster-Head diffuse cette clé à tous les nœuds de sécurité en la chiffrant avec une clé par-paire.
- Une clé publique est utilisée lors de la diffusion. Cette clé doit être mise à jour régulièrement en utilisant une fonction aléatoire unidirectionnelle pour la génération de la chaine clé d'authentification. Que les nœuds de sécurité qui traitent les messages de diffusion, et dans certains cas les autres nœuds peuvent

recevoir les messages de diffusion et ne communiquent qu'avec les clusters-Head et les nœuds de sécurité.

3.4. Approches hybrides

3.4.1. Etablissement de clé de groupe pour les communications MultiCast dans les RCSFs

Group Key Establishment for Enabling Secure Multicast Communication in Wireless Sensor Networks Deployed for IoT Applications

Dans [37], deux solutions sont développées pour l'établissement de clés de groupe pour les communications multicast dans l'Internet des Objets. Pour chaque scénario d'application, des conditions et des exigences sont décrites. Le tableau 1 résume et compare entre les deux protocoles proposés.

	Protocole 1	**Protocole 2**
principe	Le nœud initiateur diffuse des messages dans le réseau afin de démarrer le processus d'établissement de clé. A la réception de ces messages, seuls les nœuds du groupe de multicast continuent le reste du processus de dérivation de clé.	Les concepts ECIES sont déployés pour l'établissement d'une clé partagée entre les nœuds du groupe de multicast.
NBR messages	Quatre (04) messages	Deux (02) messages
performance	Moins performant à cause du nombre d'opérations effectuées à chaque extrémité et le nombre de messages échangés.	Plus performant
Rétablissement des clés	Dans les deux protocoles, la clé doit être rétablie l'ajout ou la suppression des nœuds	
Dérivation de la clé	Dans les deux protocoles, la clé est dérivée avec la participation de tous les nœuds membres du groupe de diffusion.	

Tableau 1 Récapitulatif des différences entre les deux protocoles proposés dans [35]

4. Evaluation et comparaison des approches de gestion des clés

L'évaluation des travaux cités précédemment doit être basée sur les performances de ces derniers par rapport aux caractéristiques de l'Internet des Objets pour ce qui concerne la limite en ressources, la vulnérabilité en rapport avec leurs environnements de déploiement, et aussi la taille du réseau supporté.

- **Résilience**

  Pour un protocole de gestion de clé, la résilience est la propriété la plus importante à tester lors de son évaluation et elle se définit comme la capacité de faire face aux vols d'informations, et la divulgation de ces derniers ne menace pas la totalité du réseau [38].

- **Scalabilité**

  Le changement dynamique de la taille du réseau est une caractéristique principale de l'IdO. Cette caractéristique doit être assurée par le protocole de gestion de clé [39].

- **Consommation d'énergie**

  La plupart des nœuds de l'IdO sont alimentés par des batteries vu leurs environnements de déploiement. Cette caractéristique limite les nœuds en termes de calcul et de communication. Un bon protocole de gestion de clés doit prendre en considération toutes ces contraintes [33].

Le tableau suivant récapitule la comparaison des différentes approches selon les caractéristiques définies précédemment.

Approche	Consommation d'énergie	Scalabilité	Résilience
An End-to-End Secure Key Management Protocol for E-health Applications	Déchargement des primitives cryptographiques consommatrices vers des tiers pour diminuer la consommation d'énergie des nœuds limités.	Le modèle permet d'intégrer un nombre illimité de nœuds.	Par le rassemblement de toutes les clés échangées entre CNs et les TPis, on peut avoir la clé secrète.
A Decentralized Batch-based Group Key Management Protocol for mobile IoT	Le nombre important des messages échangés et le calcul intense augmentent la consommation d'énergie selon le nombre de nœuds.	Le dynamisme du réseau est assuré et la mobilité des nœuds ne cause pas de perturbation du réseau.	chaque sous-groupe du réseau est sécurisé avec une clé différente, ce qui rend ce protocole sécurisé contre les attaques de 1-affects-n
An efficient and hybrid key management for heterogeneous WSN in context of IoT	Gain considérable en matière d'énergie.	Ce protocole assure la scalabilité.	Amélioration de la sécurité du réseau, et réduction de l'espace d'adressage des clés.
Key Management Protocol with Implicit Certificates for IoT systems	Utilisation des certificats implicites réduit la consommation d'énergie	Le protocole n'est pas conçu pour les réseaux de grande taille.	Protection contre les attaques de répétions.
Proxy-based End-to-End Key Establishment Protocol for the Internet of Things	Génère beaucoup moins de frais en termes de consommation d'énergie.	Scalabilité assurée.	Le protocole est sécurisé vu sa politique.
Two-phase Authentication Protocol for Wireless Sensor Networks in Distributed IdO Applications	Les certificats de petites tailles assurent une consommation faible d'énergie.	Possibilité de déploiement dans les RCSFs	La résilience n'a pas été prise en charge lors de la conception de la solution.
An Energy-efficient Security Node-based Key Management Protocol for WSN	Consommation réduite d'énergie.	Réseau à grande échelle.	Sécurité collaborative de clé.
Group Key Establishment for Enabling Secure Multicast Communication in Wireless Sensor Networks Deployed for IoT Applications	Consommation réduite d'énergie.	Garantie de changement fréquent du groupe de diffusion.	Sécurisé.

Tableau 2 Tableau comparatif des protocoles de gestion des clés dans IoT.

5. Conclusion

Après avoir présenté dans le chapitre 1 les concepts de base de l'Internet des Objets et ses challenges, nous avons étudié dans le second chapitre quelques approches de gestion de clés qui datent récemment. Ces protocoles se diffèrent les uns des autres selon le principe et le mode de fonctionnement, les types d'échanges. Dans la section suivante, nous présentons notre amélioration à une approche distribuée présentée précédemment.

3
Proposition et simulation

1. Introduction

La communication et l'échange des données entre les nœuds sont le cœur de l'Internet des Objets, ce qui nécessite une meilleure sécurité. La majorité des primitives cryptographiques existantes sont couteuses en termes de puissance de calcul, capacité de stockage et consommation d'énergie, ce qui présente un challenge de l'IdO vu les caractéristiques limitées des nœuds.

Comme présenté dans le chapitre 2, plusieurs approches ont été proposées (entre centralisée, distribuée, etc.) et chacune d'elles présente des avantages et des inconvénients.

Nous nous intéressons dans notre étude à l'approche distribuée «**Protocole de gestion de clés avec certificats implicites pour l'IdO »**[18] avec proposition de quelques améliorations.

[18] Key Management Protocol with Implicit Certificates for IoT systems

2. Proposition

2.1. Aperçu de la sécurité dans les systèmes mobiles à ressources limitées

Nous présentons dans cette section les solutions importantes non consommatrices d'énergie qui peuvent être déployées dans les systèmes mobiles et les applications de l'IoT industriels.

2.1.1. Algorithme de référence pour la négociation de clé

Malgré sa simplicité, l'approche de pré distribution des clés cryptographiques présente deux limites qui ont contraint son déploiement [33] :

- Le non sécurité du réseau en cas d'utilisation d'un même secret, et l'intrusion d'un seul nœud menace la totalité du réseau.
- Le non scalabilité en cas de configuration du secret pour chaque couple de nœuds.

Les meilleures solutions proposées pour altérer à ces limites sont basées sur les approches de Diffie-Hellman (DH) et l'échange de clé de Diffie-Hellman basé sur les courbes elliptiques (ECDH).

- DH : la sécurité du protocole réside dans la difficulté du problème du logarithme discret.
- ECDH : la négociation de la clé est basée sur les cuves elliptiques en gardant le même niveau de sécurité du protocole de Diffie-Hellman.

2.1.2. Authentification des pairs communicants

Pour protéger les communications entre les pairs des attaques de l'homme du milieu ; plusieurs travaux de recherche ont montré que la meilleure technique d'authentification est l'échange de certificats contenant l'identité des nœuds et leurs clés publiques.

Dans les travaux [40] [41] [42], des certificats de type X.509 sont utilisés. Ces derniers contiennent en plus de la clé publique et l'identité, une signature explicite fournisse par une autorité de certification CA. Pour une clé publique issue des courbes elliptiques de 40 bytes de taille, l'OpenSSL

Tool[19] génère un certificat de 864 bytes ce qui nécessite une bande passante importante et consomme de l'énergie pour son échange.

Notre contribution est à ce niveau pour diminuer la taille des données échangées en gardant le même niveau de sécurité. Nous gardons toujours la solution qui permet au nœud déployé d'acquérir son certificat, et ses deux clés publiques et privées. La génération de ces trois paramètres est complétée par l'Elliptic Curve Qu-Vanstone (ECQV).

2.2. Choix de l'approche & Motivation

Dans notre travail, nous nous intéressons à l'approche distribuée «**Protocole de gestion de clés avec certificats implicites pour l'IdO »** basée sur la communication point à point. Ce choix est fait pour les raisons suivantes :

- Absence d'un nœud centrale.
- Nombre restreints des messages échangés.
- Primitives cryptographiques utilisées approuvées et moins consommatrices par rapport aux autres.

Ce que nous proposons est d'améliorer l'approche décrite précédemment, en se basant sur un modèle de communication Broadcast. L'approche proposée est constituée des phases suivantes :

- **Phase initiale**

  On considère que les nœuds avant leurs dépoilement, ils sont pré chargés par l'administrateur du réseau par des certificats ECC contenants les clés publiques, les clés privées, et un Ratio. Nous soulignons que pour des Certificat ECC, la clé publique est un multiple de sa clé privée avec un coefficient K.

- **Phase de jonction**

  Au moment de son dépoilement dans le réseau, le nouveau nœud diffuse (clé publique * nonce) modulo ratio. Ce nonce est généré aléatoirement.

  Tous les nœuds recevant ces informations diffusent aussi leurs (clé publique * nonce) modulo ratio.

- **Phase de réception de message**

  A la réception des informations diffusées précédemment, chaque nœud calcule le secret S comme suit :

[19] https://www.openssl.org

S = (la valeur reçue * clé privée * nonce) modulo ratio.

Chaque nœud prépare un MAC de vérification pour l'envoyer en diffusion comme suit : $M = (\rho_A * \rho_B * nonce_A * nonce_B) \% Secret$

A la réception du MAC, le nœud concerné vérifie la validité de ce message, et les autres nœuds mis à jour leurs buffers de clés.

La figure 20 schématise le protocole proposé.

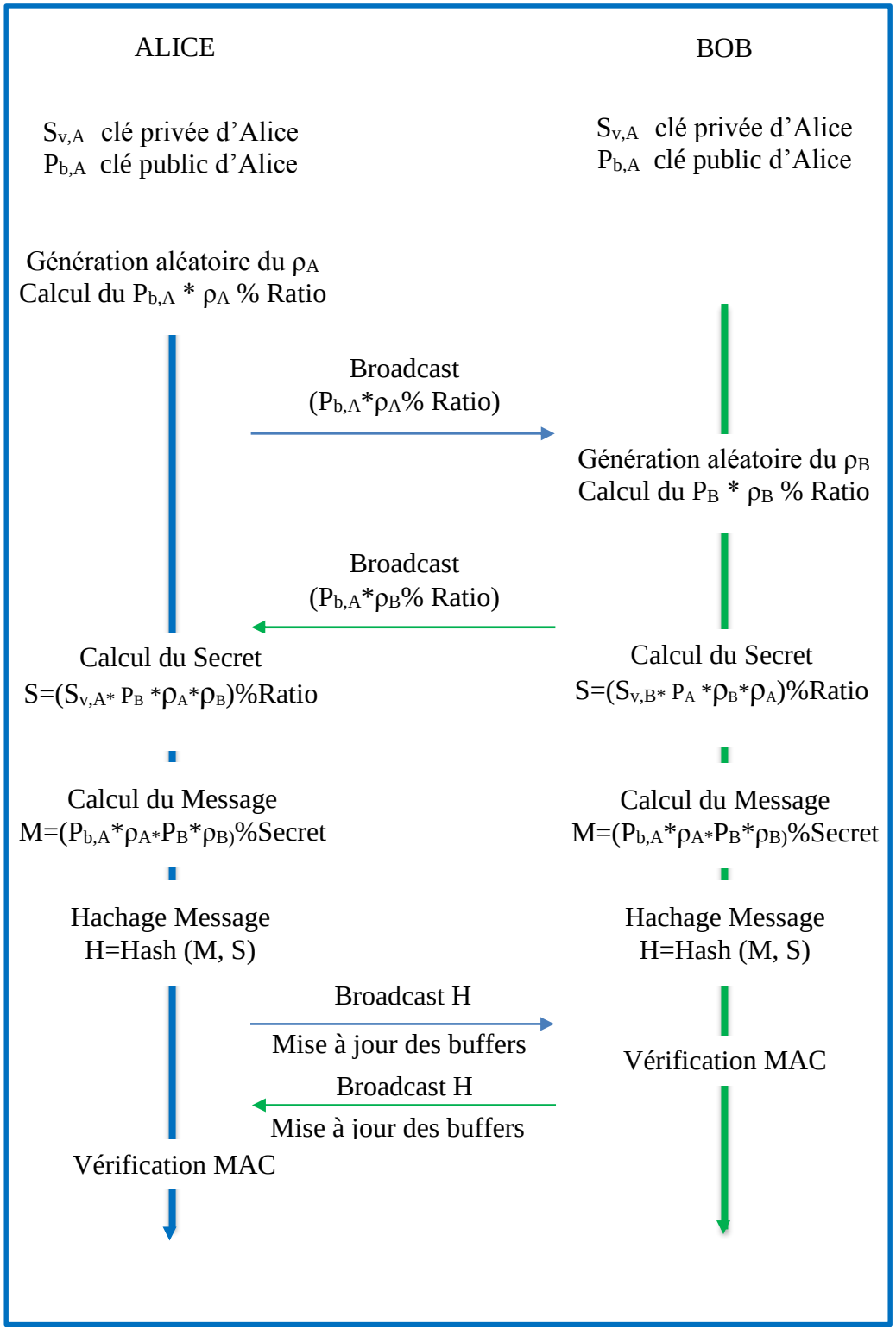

Figure 20 Protocole de négociation de clés.

3. Simulation et détails d'implémentation

3.1. Présentation des outils de simulation utilisés

Pour tester notre approche, nous utilisons le simulateur Cooja.

3.1.1. Cooja

Cooja est un émulateur réseau, il est développé en Java avec une interface utilisateur Swing et conçu pour émuler le fonctionnement des réseaux des capteurs sans fil sous le système d'exploitation Contiki[20]. Il s'agit d'un émulateur flexible et extensible permettant de modifier ou remplacer tous les niveaux du système. Il prend en charge la simulation des supports radio et l'intégration avec des outils externes pour fournir des fonctionnalités supplémentaires à l'application. Cet émulateur interagit avec le Code Contiki à travers le JNI (Java Native Interface) et il est composé de plusieurs plugins présents sous forme de fenêtres.

Cooja peut simuler grands et petits réseaux de motes Contiki (Module Capteur Simulé) sur deux niveaux :

- Niveau moins détaillé : plus rapide et permet la simulation des grands réseaux.
- Niveau plus détaillé (niveau matériel) : plus lent, mais permet une simulation précise du comportement du système réel.

Pour la simulation des modules basés sur Atmel AVR, Cooja utilise le logiciel Avrora, et le logiciel MSPSim pour les modules MSP430.

C'est un outil très utile pour le développement et le débogage des applications sous Contiki, et il permet aux développeurs de tester leurs codes avant l'intégration sur le matériel cible, estimer la consommation d'énergie, et vérifier les transmissions/ réceptions radio [43].

[20] http://www.contiki-os.org

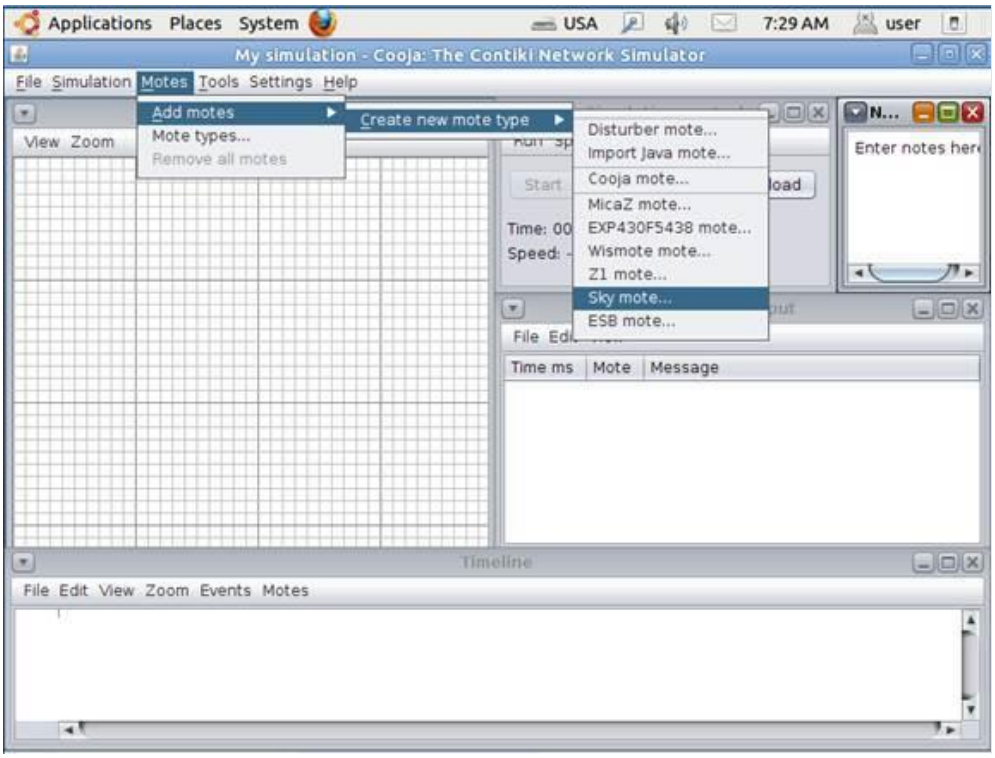

Figure 21 L'interface de l'émulateur Cooja.

3.1.2. Contiki

Contiki est un système d'exploitation Open Source pour les réseaux de capteurs sans fil. Il est développé en langage C par Adam DUNKELS dans l'Institut d'Informatique Suédois. Contiki est un système d'exploitation portable testé sur plusieurs plateformes fonctionnant avec différents types de processeurs. Pour la gestion de la concurrence, Contiki utilise un modèle de programmation évènementiel ouu tous les processus partage une pile permettant d'optimiser la mémoire. Aussi, les protothreads sont utilisés pour la réalisation des attentes bloquantes conditionnelles et inconditionnelles [43]. Contiki est caractérisé par [44]:

- **Les standards de l'Internet**

  Contiki assure des communications Internet à faible consommation d'énergie. Il supporte les standards IPv4 & IPv6 et les standards sans fil récents 6Lowpan, RPL, CoAP.

- **Développement rapide**

  Avec Contiki, le développement est rapide et facile. Ses applications sont écrites dans le langage C standard. Avec Cooja, les réseaux Contiki peuvent être testés avant leurs déploiements sur le Hardware.

- **Sélection du Hardware**

  Contiki exécutent un nombre important de type d'objets sans fil à faible consommation d'énergie.

  Sous Cooja, des programmes sur Contiki peuvent être exécutés sans avoir du matériel.

3.2. Choix et caractéristiques de type de nœuds utilisés

Le test de notre approche se fait sur des nœuds de type Z1 mote qui est un module sans fil à faible consommation d'énergie. Il est destiné à aider les développeurs WSN à tester et déployer leurs propres applications et prototypes avec le meilleur compromis entre le temps de développement et la flexibilité du matériel [43].

Ce type de nœud est caractérisé par [45]:

- Architecture de base basée sur la famille de microcontrôleurs et d'émetteurs-récepteurs radio MSP430 + CC2420 de Texas Instruments. ce qui le rend compatible avec les moteurs basés sur cette même architecture.
- 2ème génération du MSP430 ™ MCU, 16 bits ultra basse consommation d'énergie, 16MHz.
- Accéléromètre numérique à 3 axes, ± 2/4/8/16 g
- 48 KB de mémoire flash.
- 2.4GHz IEEE 802.15.4, compatible avec 6LowPAN et ZigBee ™.
- Plage de température de déploiement (-40ºC à 85ºC).
- Capteur de température numérique à basse consommation avec une précision de ± 0,5ºC (plage de -25 ° C à 85 ° C).
- Connecteur d'extension à 52 broches.
- Antenne externe optionnelle via un connecteur U.FL.
- Connecteur Micro-USB pour l'alimentation et le débogage.

3.3. Détails d'implémentation

L'approche proposée nécessite une capacité de calcul et de stockage qui dépasse les ressources disponibles dans les nœuds utilisés. Dans ce qui suit, nous détaillons l'implémentation de la solution et les optimisations faites pour altérer à ces contraintes.

- **Opérations arithmétiques cryptographiques**

  Pour optimiser l'implémentation des opérations cryptographiques consommatrices de ressources, réduire leurs complexités de calcul, et conserver un niveau de sécurité acceptable, les entiers de grandes tailles sont représentés dans des tableaux à cause de la taille limitée des registres utilisés (16 bits), et les opérations arithmétiques (addition, soustraction, multiplication) sont réalisées entre deux tableaux.

- **Génération des certificats**

  Les certificats utilisés doivent être générés et affectés aux nœuds manuellement par l'administrateur réseau.

  Nous utilisons pour tester la performance de notre approche améliorée des certificats ECC de taille de 80 bits (clé privée). Pour cela, et avec les recommandations de [46] ; on utilise la courbe $E(F_p)$: $y^2 = x^3 + ax + b$. La courbe elliptique E est définit dans le champ primaire F_p où $p=2^{160}-2^{31}-1$. Ces valeurs sont choisisses pour atteindre un niveau de sécurité de 80 bits selon les recommandations de [47].

- **Génération des nonces et entropie des générateurs utilisés**

  Pour la génération des nonces utilisés dans le processus de négociation de clé, on a fait recours à un générateur pseudo-aléatoire classé parmi les meilleurs générateurs implémentés dans nos jours selon [48]. Il s'agit du générateur congruationel linéaire dont $X_{n+1}= (aX_n+c) \bmod m$, $n\geq 0$

- **Calcul du message échangé dans la phase finale et son hachage**

  Pour la vérification du secret généré, un message est échangé à la fin du protocole. Ce message est généré en utilisant la même fonction du générateur pseudo-aléatoire : $M= (P_{b,A}*\rho_{A*}P_B*\rho_{B)}\%Secret$.

L'organigramme suivant détaille cette implémentation.

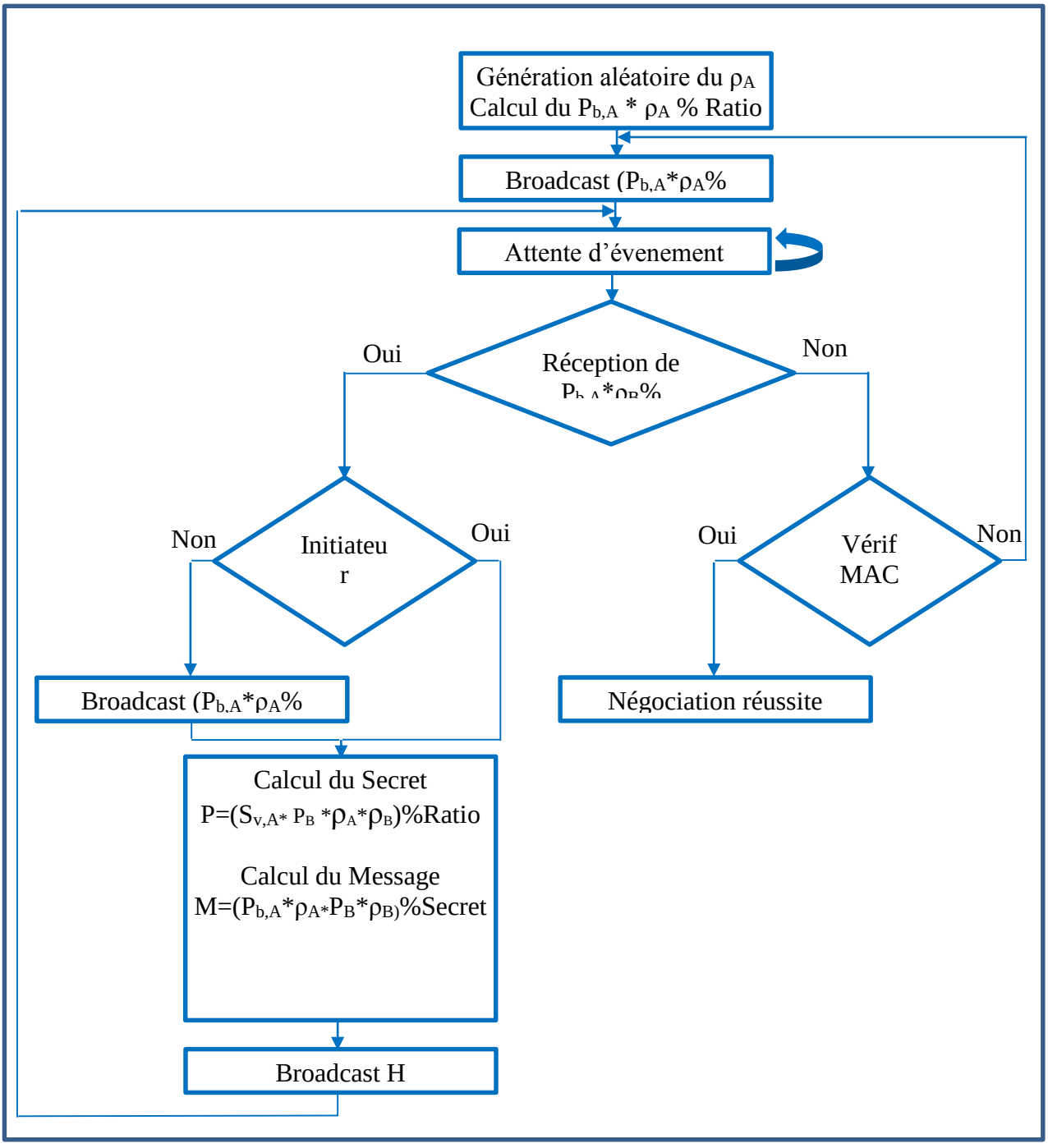

Figure 22 Algorithme détaillé de l'approche proposée.

4. Résultats et analyses

Notre approche améliorée s'inscrit dans le domaine de la sécurité informatique, ce qui nécessite de la tester en termes de confidentialité, d'intégrité, de scalabilité et de résilience. Aussi, et comme notre approche est testée sous Cooja, il est primordiale et selon [43] d'analyser l'utilisation de mémoire, la consommation d'énergie, et le temps d'exécution.

4.1. Analyse de sécurité

Nos tests sont faits avec des certificats ECC de 80 bits (clé privée). Le plus important dans notre proposition en terme de sécurité est la confidentialité. Cette propriété est assurée par l'échange du reste de la division de la clé publique dans la première phase, et le message crypté par le reste de la division par le secret dans la seconde. Aussi, l'utilisation des nonces générés aléatoirement protège le protocole des attaques de l'homme du milieu.

L'intégrité et l'authentification sont assurées par le dernier message échangé, et en cas d'échec (une propriété n'est pas vérifiée) alors le secret doit être négocié autre fois.

4.2. Analyse de performance

Les nœuds capteurs sans fil à base consommation ont des limitations en termes de puissance de calcul, d'énergie et de stockage.

4.2.1. Utilisation de la mémoire

Sous Cooja, les statistiques d'utilisation de mémoire sont visualisées en exécutant la commande : **size DABBKM.z1,** où DABBKM.z1 est le nom du fichier de la plateforme compilée dans Cooja [49].

text	**data**	**Bss**	**dec**	**Hex**	**Filename**
50983	270	6380	57633	e121	DABBKM.z1

Tableau 3 Exécution de la commande size DABBKM.z1

Le tableau 3 présente l'utilisation des différents segments de mémoire : toutes les valeurs sont en décimal et en octets [43].

- **Le segment « Text » :** contient le code et les données en Lecture-Seule (Read-Only) dans l'application.

- **Le segment « Data » :** contient les données en Lecture-Ecriture (Read-Write).
- **Le segment « Bss » :** contient les données initialisées à zéro (Bss & Common).
- **« DEC » :** est la somme des trois segments : Text, Data et Bss.
- **« HEX » :** est l'équivalent de DEC en hexadécimal.

Typiquement, la consommation de la mémoire flash est Text + Data, et pour la RAM est Data + Bss. la RAM n'est utilisée que pour les données globales et non pour la pile d'appels pendant l'exécution [43].

Selon les statistiques du tableau, l'utilisation de la mémoire flash par notre approche est de 51253 octets, et de la RAM est de 6650 octets.

4.2.2. Consommation d'énergie

Pour estimer la consommation d'énergie dans Cooja pour notre approche améliorée, on utilise l'outil **powertrace**. Pour l'exploiter, on ajoute cet outil au programme Makefile par la ligne du code : APPS += powertrace, et dans le code source pour imprimer la consommation d'énergie dans les différentes étapes, on ajoute les lignes suivantes :

```
#include "powertrace.h"
powertrace_start(CLOCK_SECOND * 10);
```

La valeur 10 est la période de mesure de la consommation d'énergie [43].

Les résultats de l'exécution de l'instruction présentés dans les tableaux 4 et 5. Ces résultats consistent aux nombre de tops d'horloge :

- CPU en mode actif (high) : ALL CPU.
- CPU en mode passif (Low Power Mode) : ALL LPM
- Emission (TX) : ALL TX
- Réception (RX) : ALL RX

ALL CPU	ALL LPM	ALL TX	ALL RX
7001	320551	2654	2126
9794	645318	2654	4046
12786	969981	2654	5966
20292	1290060	5392	8150
25756	1612156	5392	10070
28548	1936923	5392	11990
40650	2252416	10780	14402
43501	2 577 125	10 780	16 322

Tableau 4 Tops d'horloge du nœud 1

ALL CPU	ALL LPM	ALL TX	ALL RX
7000	320553	2654	2135
9793	645320	2654	4055
12785	969983	2654	5975
20282	1290070	5392	8155
25746	1612166	5392	10075
28538	1936933	5392	11995
40628	2252439	10780	14356
43479	2577148	10780	16276

Tableau 5 Tops d'horloge du nœud 2

On calcule la consommation d'énergie par la formule suivante [50]:

$$\textbf{Power\_consumption}=\frac{\textbf{Energest}_{\textbf{value}} * \textbf{Current} * \textbf{Voltage}}{\textbf{RTIMER}_{\textbf{SECOND}} * \textbf{Runtime}}$$

- Energest_Value : est le nombre de tops d'horloges dans un intervalle de temps.
- Current : la valeur du courant pour CPU, LPM, TX et RX. Nous utilisons la valeur 2mA cité dans [4].
- Voltage : Nous utilisons la valeur 3 V cité dans [4].

- RTIMER_SECOND : sa valeur est 32768.
- RUNTIME : l'intervalle de mesure, dans notre étude c'est 10 S.

Le temps total de notre simulation est de 122 S.

L'estimation de la consommation d'énergie par les deux nœuds est présentée dans les tableaux 6 et 7.

CPU	LPM	TX	RX	TOTAL
0,00027488	0,0319633	0	0,00018896	0,03242715
0,00029447	0,03195307	0	0,00018896	0,0324365
0,00073873	0,03150192	0,00026947	0,00021495	0,03272507
0,00053776	0,03170043	0	0,00018896	0,03242715
0,00027479	0,0319633	0	0,00018896	0,03242706
0,00119107	0,03105057	0,00053028	0,00023739	0,0330093
0,00028059	0,0319576	0	0,00018896	0,03242715
MOYENNE				**0,0325542**

Tableau 6 Consommation d'énergie du nœud 1

CPU	LPM	TX	RX	TOTAL
0,000274885	0,0319633	0	0,00018896	0,03242715
0,00029447	0,03195307	0	0,00018896	0,0324365
0,000737849	0,0315027	0,00026947	0,00021455	0,03272458
0,000537762	0,03170043	0	0,00018896	0,03242715
0,000274786	0,0319633	0	0,00018896	0,03242706
0,001189888	0,03105184	0,00053028	0,00023237	0,03300438
0,000280593	0,0319576	0	0,00018896	0,03242715
MOYENNE				**0,03255343**

Tableau 7 Consommation d'énergie du nœud 2

La moyenne de la consommation d'énergie par Z1 est autour de 0.032 mW.

4.2.3. Scalabilité

Les résultats présentés dans le graphe suivant sont comparés au protocole de référence d'où on a inspiré notre approche.

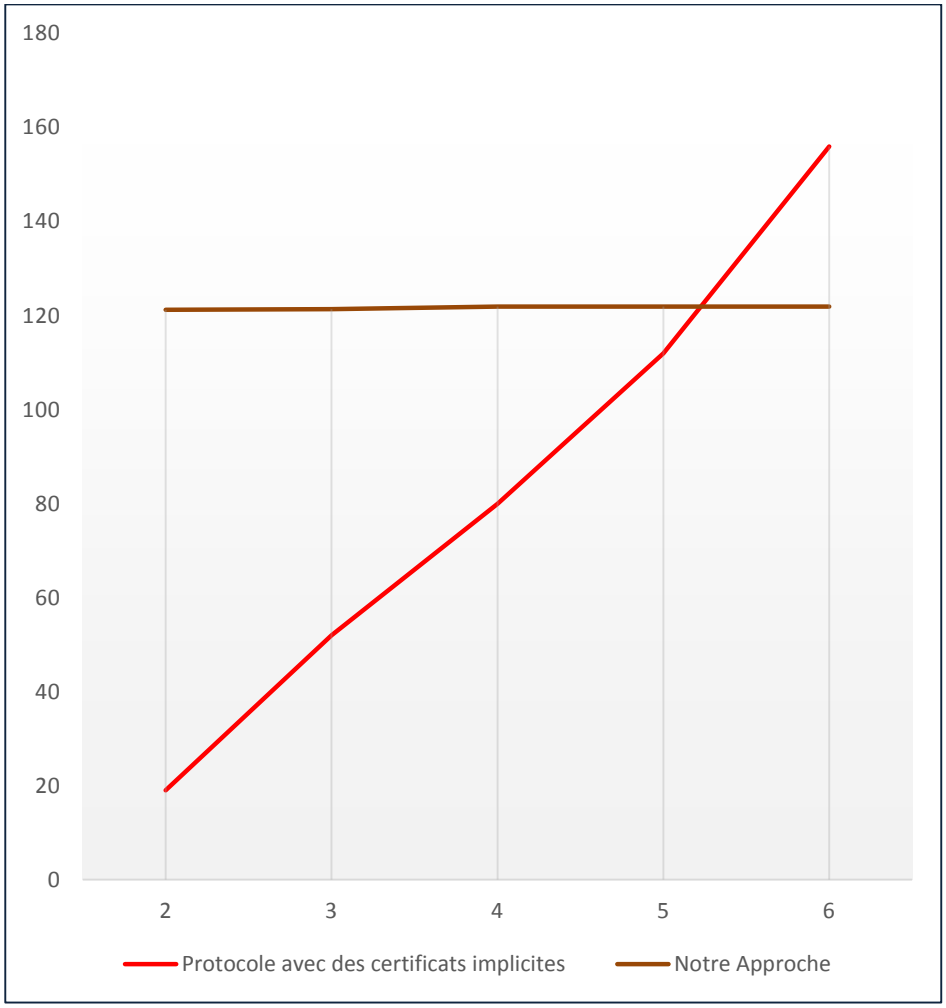

Figure 23 Comparaison des temps d'exécution entre les deux approches

4.2.4. Diagramme d'exécution

Le diagramme suivant détaille les temps d'exécution de chaque phase de l'approche améliorée.

Nous remarquons que les différents temps sont raisonnables, sauf le temps d'émission qui est élevé par rapport à celui présenté dans [33]. Cette différence est due du fait que nous avons développé notre approche à la couche application de la pile protocolaire IEEE 802.15.4 Alors que le deuxième est développé à la couche 2. Aussi, les instructions d'envoi et de réception dans les deux solutions ne sont pas les mêmes.

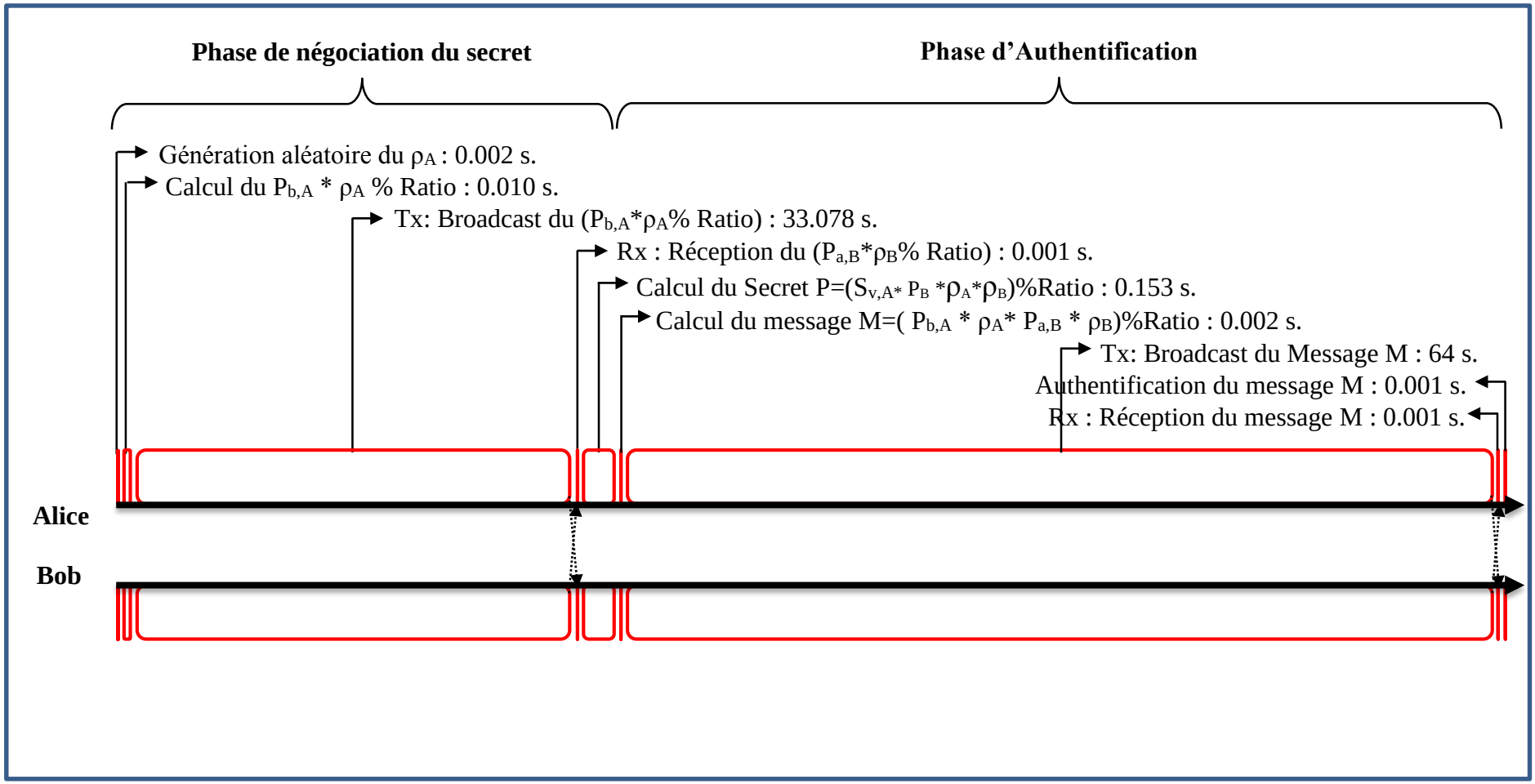

Figure 24 Diagramme d'exécution

5. Conclusion

Nous avons détaillé l'implémentation et les résultats obtenus de notre amélioration à l'approche distribuée pour la négociation des clés.

Les résultats obtenus ont montré l'intérêt de l'utilisation de la diffusion au lieu de la communication point à point.

Les résultats obtenus en ce qui concerne le temps de calculs sont satisfaisantes, mais les temps d'échanges sont élevés par rapport au protocole de référence, et tout ça est du de l'implémentation de l'approche à la couche application au lieu la couche liaison et le non utilisation de la même technologie réseau et les mêmes primitives d'envoi et de réception.

Conclusion générale et Perspectives

L'Internet des Objets (IdO) se considère comme la tendance actuelle de l'Internet où les objets de la vie quotidienne qui nous entourent sont connectés à l'Internet et peuvent communiquer entre eux et avec les utilisateurs afin d'atteindre un objectif commun. L'intérêt des gens à ce concept se traduit dans les domaines d'application : Transport, environnement, santé, etc.

La transition de l'Internet vers l'Internet des Objets conduit à plusieurs changements dans le modèle sous-jacent. Des travaux importants sur plusieurs problématiques ont été initiés pour réaliser le concept de l'Internet des Objets.

Nous nous sommes intéressés dans ce mémoire aux approches de gestion des clés dans l'Internet des Objets. L'objectif principal que nous avons fixé est d'apporter des propositions pour améliorer la sécurité dans un environnement régi par les protocoles de sécurité de l'Internet pour l'Internet des Objets. Nous avons mis en avant les caractéristiques essentielles et les notions fondamentales d'Internet des Objets, et nous avons étudié aussi les notions de sécurité. L'ensemble des protocoles de gestion des clés proposés pour l'IdO se basent généralement sur la cryptographie symétrique et asymétrique pour sécuriser les communications. Nous avons étudié un ensemble de ces protocoles de gestion des clés qui permettent d'offrir des services de sécurités pour n'importe quel système basé sur la communication et nous avons mis une classification aux solutions étudiées.

De cette étude, résulte notre contribution consistant en une amélioration d'un modèle de gestion des clés distribué basé sur la diffusion qui permet la réduction de nombre de messages échangés entre les nœuds., qui implique la diminution de la consommation d'énergie, l'espace de stockage et le traitement. Cette amélioration garde toujours le niveau de sécurité par rapport au protocole de référence et même plus dans certain cas.

Perspectives

Réellement, notre approche n'est pas comparée avec le protocole de référence en termes de performance (temps d'exécution, consommation d'énergie, utilisation de mémoire). Le protocole de référence a été implémenté dans la couche 2 du 802.15.4. Ce qui n'est pas le cas dans notre travail. Aussi, les primitives d'envoi et de réception utilisées dans les deux implémentations ne sont pas les mêmes, ce qui limite la comparaison entre les deux propositions en terme de performance. Nous proposons comme suite de notre travail, d'implémenter notre proposition à la couche 2 du 801.15.4, et d'utiliser soit les mêmes primitives d'envoi et de réception du protocole de référence, soit de chercher les primitives les moins consommatrices de ressources.

Bibliographie

[1] Y. CHALLAL, «Sécurité de l'Internet des Objets : vers une approche cognitive et systémique,» Mémoire d'Habilitation à Diriger des Recherches, 2012.

[2] L.COETZEE, and J.EKSTEEN, «The Internet of Things - promise for the future. An introduction,» *IST-Africa Conference Proceedings*, 11-13 Mai 2011.

[3] Yosra BEN SAIED, «Sécurite Collaborative pour l'Internet des Objets,» thèse de doctorat, conjoint Telecom Sudparis et Universite Pierre et Marie Curie, 2013.

[4] L. ATZORI, A. IERA et G. MORABITO, «The Internet of Things: A survey,» *Computer Networks*, pp. 2787-2805, 2010.

[5] H. HELLAOUI, «L'Internet des Objets,» Mémoire de magister, Ecole Nationale Supérieure d'Informatique, 2015.

[6] D. MIORANDI, S. SICARI, F. DE PELLEGRINI et I. CHLAMTAC, «Internet of things: Vision, applications and research challenges,» *Ad Hoc Networks*, pp. 1497-1516, 2012.

[7] H. CHAOUCHI, The internet of things: connecting objects, ISBN 1118600177: John Wiley & Sons, 2010.

[8] M. WU, T. LU, F. LING, l. SUN, et H. DU, «Research on the architecture of Internet of things,» *3rd International Conference on Advanced Computer Theory and Engineering (IEEE),*, 2010.

[9] D. Niyato, E. Hossain et S. Camorlinga, «Remote patient monitoring service using,» *IEEE Journal on Selected Areas in Communications vol. 27, no 4*, p. 412–423, 2009.

[10] «E-Health application developed with MySignals first winner in health competition ISHIC 2017,» [En ligne]. Available: http://www.libelium.com/e-health-application-developed-with-mysignals-first-winner-in-health-competition-ishic-2017/#!prettyPhoto. [Accès le 07 Juillet 2018].

[11] M. Darianian et M. P. Michael, «Smart Home Mobile RFID-Based Internet-of-Things,» *nternational Conference on Advanced Computer Theory and,* p. 116-120, Aout 2008.

[12] «La domotique,» [En ligne]. Available: http://igm.univ-mlv.fr/~dr/XPOSE2007/aessaidi-ndiop_LA-DOMOTIQUE/intro.htm. [Accès le 07 Juillet 2018].

[13] Y. Ait Mouhoub et F. Bouchebbah, «Proposition d'un modèle de confiance pour l'Internet des Objets,» Mémoire de master de l'université Abderrahmane Mira , Bejaia, 2015.

[14] «Quelles économies vont offrir les smart grids à la France ?,» [En ligne]. Available: http://les-smartgrids.fr/economies-smart-grids-france/. [Accès le 07 Juillet 2018].

[15] «Smart-Transportation,» [En ligne]. Available: http://www.brindleytech.com/smart-transportation/. [Accès le 07 Juillet 2018].

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

[17] «Internet Engineering Task Force (IETF). [En ligne],» http://www.ietf.org/.

[18] «« EPCglobal | Products & Solutions | GS1 - The global language of business ». [En ligne],» http://www.gs1.org/epcglobal.

[19] B. Billet, «Système de gestion de flux pour l'internet des objets intelligents,» Thèse de doctorat de l'université de Versailles Saint-Quentin-En-Yvelines., 2015.

[20] H. Krawczyk, M. Bellare et R. Canetti, «HMAC : Keyed-Hashing for Message Authentication,» RFC 2104, 1997.

[21] e. a. G. Gaubatz, «Public Key Cryptography in Sensor Networks-Revisited,» chez *ESAS '04 : 1st European Wksp, Security in Ad-Hoc and Sensor Networks*, 2004.

[22] K. P. e. al, «How Public Key Cryptography Influences Wireless Sensor Node Lifetime,» chez *SASN'06*, Alexandria, Virginia, USA, Octobre 2006.

[23] A. S.Wander et al, «Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks,» chez *PerCom '05*, Mars 2005.

[24] N. Gura et al, «Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs,» chez *6th InternationalWorkshop on Cryptographic Hardware and Embedded Systems*, Boston, Massachusetts, Aout 2004.

[25] Ian F. Blake, Gadiel Seroussi, Nigel P. Smart, «Advances in Elliptic Curve Cryptography,» *London Mathematical Society Lecture Note Series*, n° %1317, Avril 2005.

[26] A. Liu et P. Ning, «TinyECC : Elliptic Curve Cryptography for sensor networks (version 0.3) available at http ://discovery.csc.ncsu.edu/software/TinyECC/,» Février 2007.

[27] D. J. Malan, M. Welsh et M. D. Smith, «A Public-Key Infrastructure for Key Distribution in TinyOS based on Elliptic Curve Cryptography,» chez *Proc. 1st IEEE Int'l. Conf. Sensor and Ad Hoc Communications and Networks*, Santa Clara, CA, Octobre 2004.

[28] Haodong Wang, Bo Sheng et Qun Li, «Elliptic curve cryptography-based access control in sensor networks,» *Int. J. Security and Networks*, vol. 1, n° %13/4, 2006.

[29] Y. Challal, «Réseaux de capteurs sans fil,» University of Technology in compiegne, France, 2008.

[30] MR.Abdmeziem et D.Tandjaoui, «An end-to-end secure key management protocol for e-health applications,» *Computers & Electrical Engineering*, pp. 44 :184-197, 2015.

[31] MR.Abdmeziem, D.Tandjaoui et I.Romdhani, «A decentralized batch-based group key management protocol for mobile internet of things,» *In Computer and Information Technology ; Ubiquitous Computing and Communications ; Dependable, Autonomic and Secure Computing ; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), 2015 IEEE International Conference*, pp. 1109-1117, 2015.

[32] Y.Zhang et J.Pengfei, «Control and Decision Conference (2014 CCDC), The 26th Chinese,» chez *pages 1881-1885*, 2014.

[33] S.Sciancalepore, A.Capossele, G.Piro, G.Boggia et G.Bianchi, «Key management protocol with implicit certificates for IoT systems,» *Proceedings of the 2015 Workshop on IoT Challenges in Mobile and Industrial Systems*, pp. IoT-Sys'15, pages 37-42, New York, NY, USA,, 2015.

[34] P.Porambage, A.Braeken, P.Kumar et A.Gurtov, «Proxy-based End-to-End Key Establishment Protocol for the Internet of Things,» *Communication Workshop (ICCW), 2015 IEEE International Conference*, pp. 2677-2682, 2015.

[35] P.Porambage, C.Schmitt, P.Kumar et A.Gurtov, «Two-phase Authentication Protocol for Wireless Sensor Networks in Distributed IoT Applications,» *Wireless Communications and Networking Conference (WCNC), 2014 IEEE*, pp. 2728-2733, 2014.

[36] B.Jiana et E.Xu., «An energy-efficient security node-based key management protocol for wsn,» *Applied Mechanics and Materials*, vol. 347, n° %1Trans Tech Publ, pp. 2117-2121, volume 347 2013.

[37] P.Porambage et al., «Group key establishment for enabling secure multicast communication in wireless sensor networks deployed for iot applications,» *IEEE Access*, vol. 3, pp. 1503-1511, 2015.

[38] R.Roman, C.Alcaraz, J.Lopez et N.Sklavos, «Key management systems for sensor networks in the context of the internet of things,» *Computers & Electrical Engineering*, vol. 2, n° %137, pp. 147-159, 2011.

[39] T.Schlossnagle, «Scalable internet architectures,» *Kindle Edition*, 2007.

[40] G.Bianchi, A.Capossele, A.Mei et C.Petrioli, «Flexible Key Exchange Negotiation for Wireless Sensor Networks.,» chez *Proc. of the ACM Int. Workshop on Wirel. Netw. Testbeds, Experim. Evaluation and Characterization*, 2010.

[41] G.Piro, G.Boggia et L.Grieco, «A Standard Compliant Security Framework for IEEE 802.15.4 Networks.,» chez *Proc. of IEEE World Forum on Internet of Things (WF-IoT)*, (Seoul, South Korea), 2014.

[42] G.Piro, G.Boggia et L.Grieco, «Layer-2 security aspects for the IEEE 802.15.4e MAC,»

IETF 6TiSCH WG, 2014.

[43] A. Velinov et A.Mileva, «Running and Testing Applications for Contiki OS Using Cooja Simulator,» chez *International Conference on Information Technology and Development of Education – ITRO 2016*, Zrenjanin, Republic of Serbia, Juin 2016.

[44] «Contiki,» [En ligne]. Available: http://www.contiki-os.org. [Accès le 10 Juillet 2018].

[45] ZOLERTIA™, «Z1 Datasheet v1,» ZOLERTIA™, 2010.

[46] D.Hankerson, S.Vanstone et A.Menezes, «Guide to Elliptic Curve Cryptography,» *Springer*, 2004.

[47] «SECG. Sec 2: Recommended elliptic curve domain parameters version 2.0».

[48] Aviv Sinai, «Pseudo Random Number Generators in Programming Languages,» The Interdisciplinary Center, Herzlia Efi Arazi School of Computer Science, 2011.

[49] «Application Flash and RAM size.,» [En ligne]. Available: http://support.code-red-tech.com/CodeRedWiki/FlashRamSize. [Accès le 30 Juillet 2018].

[50] «Contiki OS: Using Powertrace to estimate power consumption,» [En ligne]. Available: http://thingschat.blogspot.mk/2015/04/contiki-os-using-powertrace-and.html. [Accès le 30 Juillet 2018].

[51] http://www.itu.int, Mars 2018.

[52] D. Miorandi, S. Sicari, F. De Pellegrini et I. Chlamtac, «Internet of things: Vision, applications and research challenges,» *Ad Hoc Netw*, vol. 10, n° %17, p. 1497–1516, 2012.

[53] B. Kaliski, «The MD2 Message-Digest Algorithm,» RFC 1319, Avril 1992.

[54] R. Rivest, «The MD5 Message-Digest Algorithm,» RFC 1321, Avril 1992.

[55] D. Eastlake et P. Jones, «US Secure Hash Algorithm 1 (SHA1),» RFC 3174, Septembre 2001.

[56] H. Krawczyk, M. Bellare et R. Canetti, «HMAC : Keyed-Hashing for Message Authentication,» RFC 2104, Février 1997.

[57] S. Atmani, «Protocole de sécurité Pour les Réseaux de capteurs Sans Fil,» Juillet 2010.

[58] N. Khimoum et N. Merrani, «Simulation et évaluation de protocoles de gestion de clés dans les réseaux de capteur,» Université Abderrahmane Mira Bejaia, 2009.

[59] V.Sharada, «Near Field Communication,» NIRMA UNIVERSITY, 2015.