MINISTÈRE DE L'ENSEIGNEMENT SUPERIEUR DE LA RECHERCHE ET DE L'INNOVATION

Université Assane SECK de Ziguinchor

UFR Sciences et Technologies

Département d'Informatique

Mémoire de fin d'études

Pour l'obtention du diplôme de Master

Mention : Informatique

Spécialité : Génie Logiciel

Sujet :

Optimisation de Protocoles d 'authentification dans le contexte de l'Internet des Objets

Présenté et soutenu par : M. Cheikhou Oumar SOW

Le lundi 20 /12 / 2021

Sous la direction de :

M. Youssou FAYE — Maître de Conférences à UASZ

Devant le jury composé de:

M. Ousmane DIALLO	*Maître de Conférences*	*Président*	*UASZ*
M. Youssou FAYE	*Maître de Conférences*	*Encadreur*	*UASZ*
Mme Marius DASYLVA	*Enseignant-Chercheur*	*Examinatrice*	*UASZ*
M. El Hadji Malick NDOYE	*Maître Assistant*	*Rapporteur*	*UASZ*
M. Abel DIATTA	*Enseignant-Chercheur*	*Rapporteur*	*UASZ*

Année Universitaire 2020-2021

Dédicace

« Il y'a rien de noble au fait d'être supérieur à ses semblables, la vrai noblesse consiste à être supérieur à celui qu'on était avant. »

Ce présent mémoire est dédié, avec amour et gratitude, à toutes les personnes qui m'ont soutenu, encouragé et encadré de l'école coranique jusqu'à ce jour,

A mon défunt Père El Hadji Ousmane SOW

A ma très chère Maman Bineta BA,

A mes sœurs Nafissatou, Aissatou, Ndèye Fatou et Fatoumata,

A mes frères Mouhamadou Habib, Abdou Raby, Ousseynou et Assane.

A mon cousin Amadou Ousmane SOW et mon oncle Samba BA

A Fatou Bintou NOMOKO et Saly Diop NDOUR

A mon Tuteur Dr Daouda DIOUF

À ma seconde famille :

Toute la famille Ségnane sans exception : petits et grands

Toute la famille Bodian sans exception : petits et grands

À Tous les membres du ***Dahira Siratikal Moustakhim*** *de l'UASZ sans exception aucune*

À mes sœurs, mes neveux et nièces, Ami(e)s, mes cousin(e)s, mes tantes, oncles et parents,

À ***Issakha NDIAYE, Bécaye SALL, Ngagne DIOP et Abdou FALL***

Enfin à tous ceux qui se sentent participant à ma réussite,

À vous tous, je vous dédie ce travail et vous dis merci

Remerciements

"Traitez les gens comme s'ils étaient ce qu'ils doivent être et vous les aiderez à devenir ce qu'ils sont capables d'être"

Tout d'abord, je remercie le Tout-Puissant de m'avoir donné la force morale et physique, le courage d'arriver à terme de ce travail ;

C'est avec un grand plaisir que je réserve ces quelques lignes en signe de gratitude et de reconnaissance à tous ceux qui ont contribués de près ou de loin à l'élaboration de ce modeste travail.

Je tiens tout d'abord à exprimer mes plus chaleureux remerciements à mon encadreur :

Un idole, un grand monsieur, un homme de caractère, sérieux, ambitieux et généreux dans l'enseignement, ***Professeur Youssou FAYE,*** *Enseignant chercheur à l'Université Assane SECK de Ziguinchor,*
Vous n'avez pas fait de distinction pour mon encadrement, ni manager aucun effort à mon égard malgré vos calendriers chargés. Je vais faire pareil pour vous témoigner ma gratitude et ma reconnaissance pour m'avoir fait l'honneur de m'encadrer tout en me laissant une grande liberté. Je vous adresse ces quelques mots en guise de reconnaissance pour votre patience, pour votre grande disponibilité et surtout pour vos précieux conseils pertinents et constants, qui ont contribué à alimenter ma réflexion, et aidés à trouver des solutions pour avancer face à certaines difficultés rencontrées. Votre ouverture d'esprit, vos connaissances m'ont été d'une très grande utilité. Nos réunions de présentation me manquent déjà ; j'espère seulement que ça ne s'arrêtera pas là. Je vous en suis infiniment reconnaissant pour tout.

Je souhaite remercier les membres de mon jury de mémoire :

Monsieur Ousmane DIALLO, maître de conférence à l'Université Assane SECK de Ziguinchor, pour le temps qu'il a bien voulu consacrer à l'évaluation de ce travail, mais aussi, de m'avoir fait l'honneur de présider le jury de ma soutenance

Mes respectueux remerciements vont à mon examinateur :

Une grande madame simple, cultivée, modeste et sérieuse, ***Mme MENDY (Marius DASYLVA),***

Enseignant-Chercheur à l'Université Assane SECK de Ziguinchor.

Mes respectueux remerciements vont à mes rapporteurs :

Monsieur El Hadji Malick NDOYE, Maître Assistant à l'Université Assane SECK de Ziguinchor, pour son ouverture et nos discussions riches dans tous les domaines scientifiques. Je vous remercie de m'avoir fait l'honneur d'être rapporteur de mon mémoire.

Et Monsieur Abel DIATTA, Enseignant-Chercheur à l'Université Assane SECK de Ziguinchor, pour m'avoir fait l'honneur de participer à mon jury de mémoire.

Mes respectueux remerciements à un ami, un conseillé, et un frère Amadou Malado NDIAYE

Mes amicaux remerciements vont à tous les camarades de promotion, pour tous les beaux moments passés ensemble.

Enfin je ne manquerai pas d'exprimer ma grande reconnaissance à tous les professeurs de l'UASZ, particulièrement ceux qui ont participé de près ou de loin à notre formation de master.

Je souhaite remercier particulièrement mon défunt père

El Hadji Ousmane SOW

Qui n'est hélas pas présent le jour de ma soutenance pour partager mon stress et ma joie,

Puisse DIEU vous accueillir dans son paradis céleste, j'espère seulement que vous êtes fiers de moi!!!

Résumé

Les objets connectés sont aujourd'hui utilisés dans de nombreux domaines d'applications tels que la surveillance en usine, l'E-santé etc. Toutefois, le dénominateur commun de toutes ces applications de réseaux de capteurs reste la limite des capteurs en raison de leurs ressources matérielles limitées dont la plus contraignante est l'énergie. Dans ce genre d'environnement d'Internet des Objets (IdO), la question de l'authentification entre deux dispositifs de communication est une question de sécurité. Comme beaucoup d'appareils IoT sont alimentés par des batteries et qu'ils doivent transmettre des données périodiquement, il est nécessaire que ces appareils adoptent un protocole d'authentification léger pour réduire leur consommation d'énergie. Dans ce contexte, différentes solutions d'authentification telles que l'authentification statique et l'authentification dynamique ont été proposées mais présentent des limites face aux contraintes d'énergie et de capacité de stockage des capteurs. En effet, l'authentification continue est l'une des solutions pour palier à ce problème, car elle complète l'authentification statique en garantissant l'authenticité d'un expéditeur tout en n'utilisant aucune opération cryptographique. C'est ainsi que dans ce mémoire, en vue d'optimiser la consommation énergétique relative à l'éxécution de protocoles de sécurité, nous améliorons un protocole d'authentification continue. Nous montrons que la solution proposée engendre une consommation plus faible en énergie, et réduit le nombre d'opérations à travers un modèle basé sur les requêtes.

Mots-Clés : Authentification continue; Internet des objets ; Réseaux de capteurs sans fil, Cryptographie, RFID

Abstract

Connected objects are now used in many application areas such as factory monitoring and e-health. However, the common denominator of all these sensor network applications remains the limit of sensors due to their limited hardware resources, the most restrictive of which is energy. In this kind of Internet of Things (IoT) environment, the issue of authentication between two communication devices is a security issue. Since many IoT devices are powered by batteries and need to transmit data periodically, there is a need for these devices to adopt a lightweight authentication protocol to reduce their power consumption. In this context, different authentication solutions such as static authentication and dynamic authentication have been proposed, but prove ineffective in the face of energy and storage capacity constraints of the sensors. In fact, continuous authentication is one of the solutions to overcome this problem, as it complements static authentication by guaranteeing the authenticity of a sender while not using any cryptographic operation. Thus, in this brief, in order to optimize the power consumption related to the execution of security protocols, we are improving a continuous authentication protocol. We show that the proposed solution generates lower energy consumption, and reduces the number of operations through a model based on requests.

Keywords: Continuous authentication; Internet of things; Wireless sensor networks, Cryptography, RFID

Sommaire

Liste des figures

Liste des tableaux

Glossaire

6LoWPAN *IPv6 over Low Power Wireless Area Networks*
AES *Advanced Encryption Standard, Advanced Encryption Standard*
BCTSN *Battery Capacity Threshold*
CA *Autorité de Certificat*
DES *Data Encryption Standard*
DoS *Déni of Service*
DTLS *Datagram transport layer security*
EBCSN *Consommation quotidienne Estimée de la Batterie moyenne*
ECC *Elliptic Curve Cryptography*
ECDH *Elliptique Curve Diffie-Hellman*
ECQV *Elliptic Curve Qu-Vanstone*
GPS *Global Positioning System*
HMAC *hash-based message authentication code*
IBE-ECC *Courbe elliptique basée sur l'identité Cryptographie*
IdO *Internet des Objets*
IETF *Internet Engineering Task Force*
IoT *Internet of Things*
IPSO *IP for Smart Objects*
M2M *Machine à machine*
NFC *Near Fiel Communication*
RCSF *Réseaux de capteurs sans fil*
RFID *Radio-frequency identification*
RSA *Rivest–Shamir–Adleman*
TIC *Technologies dIinformation et de Communication*
WSNs *Wireless Sensor Networks*

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 appartenant ou nous entourant 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, ajoutant ainsi une nouvelle dimension au monde de la 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. 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. 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. Les réseaux de capteurs sans fil (WSNs) ont obtenu une popularité élevée en raison de leur large éventail d'application. 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'attaque, 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, les limites en protection physique ainsi qu'en ressources (stockage, calcule, mémoire, énergie) de ces objets, rendent l'IdO vulnérable (niveau objets, réseaux, applications) à une variété d'attaques potentielles, pour lesquels les solutions de sécurité conventionnelles sont mal adaptés. Les exigences de sécurité dans l'environnement IoT ne sont pas différentes des autres systèmes TIC. Pour assurer des communications sécurisées entre objets, il est nécessaire que ces appareils adoptent un protocole d'authentification léger pour réduire leur consommation d'énergie.

C'est dans ce contexte que s'inscrit notre sujet de mémoire dont l'objectif principal est de garantir la sécurité en minimisant la consommation énergétique, par le biais du nombre d'opérations effectuées au niveau des capteurs. Pour se faire, une étude des différentes solutions d'authentification basée sur la cryptographie symétrique ou asymétrique a été effectuée [25], [24] et [33], cependant, elles ne résolvent pas la question de l'optimisation car ces opérations nécessitent une consommation d'énergie importante. Par ailleurs, des solutions d'authentification statique [29], [32], mais présente toujours des limites pour faire face à l'économie d'énergie.

Ainsi, l'authentification continue a pour la première fois était proposée dans [36], [37-42] pour résoudre la question de la réduction de consommation d'énergie et s'avère légère en terme

d'opération. Dans [52], les auteurs proposent une solution d'authentification continue qui a l'avantage de n'utiliser que des opérations de calcul légères, qui incluent l'authentification de message basée sur le hachage (HMAC)[30], la fonction de hachage, et opération ou-exclusif. Et comme perspectives, les auteurs proposent d'initialiser le processus par la passerelle.

Pour ainsi poursuivre la logique d'optimisation des auteurs, nous proposons une solution qui permet d'initialiser les communications à partir de la Gateway pour soutenir les applications basées sur les requêtes et réduire en même temps le nombre d'opération au niveau des capteurs. Une analyse en termes d'opérations cryptographiques montre que notre solution a un coût meilleur que [52]. Une analyse de sécurité est effectuée pour évaluer la solidité du protocole proposé. En outre, l'analyse du rendement et l'extension du protocole ont montré que le protocole proposé est un concurrent important parmi les protocoles existants pour authentification dans les environnements IoT.

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, ses utilisations les plus répondues, son architecture, ses avantages et inconvénients.

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

Le chapitre trois aborde l'état de l'art sur les protocoles d'authentification et l'étude du protocole de Yo-Hsuan Chuang et all. dans ses différentes phases.

Dans le quatrième chapitre, consacré à la contribution, nous présentons les problématiques et les solutions proposées pour l'optimisation du protocole étudié.

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

Chapitre 1

Introduction à L'Internet des Objets

Introduction

Internet des Objets (IdO) ou (IoT) Internet of Things en anglais s'inscrit dans le contexte de l'évolution naturelle des technologies, il envisage un avenir dans lequel le lien entre le monde numérique et le monde physique est inévitable. L'assistance apportée à nos activités professionnelles et personnelles va permettre de faire une réduction considérable des dépenses dans notre vie quotidienne, permettre aussi de nouvelle classe d'application et de services, au moyen de Technologies d'information et de communication (TIC) appropriées.

Le concept de L'Internet des Objets vise à proposer des solutions qui seront basées sur l'intégration des nouvelles technologies de l'information, qui se réfèrent au matériel et aux logiciels utilisés pour la récupération, le stockage et le traitement des données, y compris les systèmes électroniques utilisés pour la communication.

Le but de ce chapitre consiste à faire une présentation de l'IdO, l'historique et l'architecture dans ses différentes couches, ses utilisations les plus connues à savoir ses principaux domaines d'activités, puis ses avantages, ses limites, et ses défis.

1. Définition de l'IDO

L'Internet des Objets peut être défini comme un ensemble d'objets disposant de capteurs et échangeant de l'information via un réseau. Objet physique possédant une adresse IP qui se connecte reçoit et envoie des données via un réseau de communication. C'est une extension d'internet à des choses et à des lieux du monde physique. Elle représente les échanges d'informations et de données provenant de dispositifs présents dans le monde réel vers le réseau Internet. Un réseau de réseaux qui permet, via des systèmes d'identification électronique normalisés et unifiés, et des dispositifs mobiles sans fil, d'identifier directement et sans ambiguïté des entités numériques et des objets physiques et ainsi de pouvoir récupérer, stocker, transférer et traiter, sans discontinuité entre les mondes physiques et virtuels, les données s'y rattachant.

L'IdO est élargi par un certain nombre de technologies différentes comme les systèmes d'informations de détection telles que les Réseaux de Capteurs Sans Fil (RCSF) ou Wireless Sensor Networks(WSNs) en Anglais, 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[1]comme l'illustre la figure1 ci-dessous le concept d'IdO et la connexion entre tous les composants impliqués.

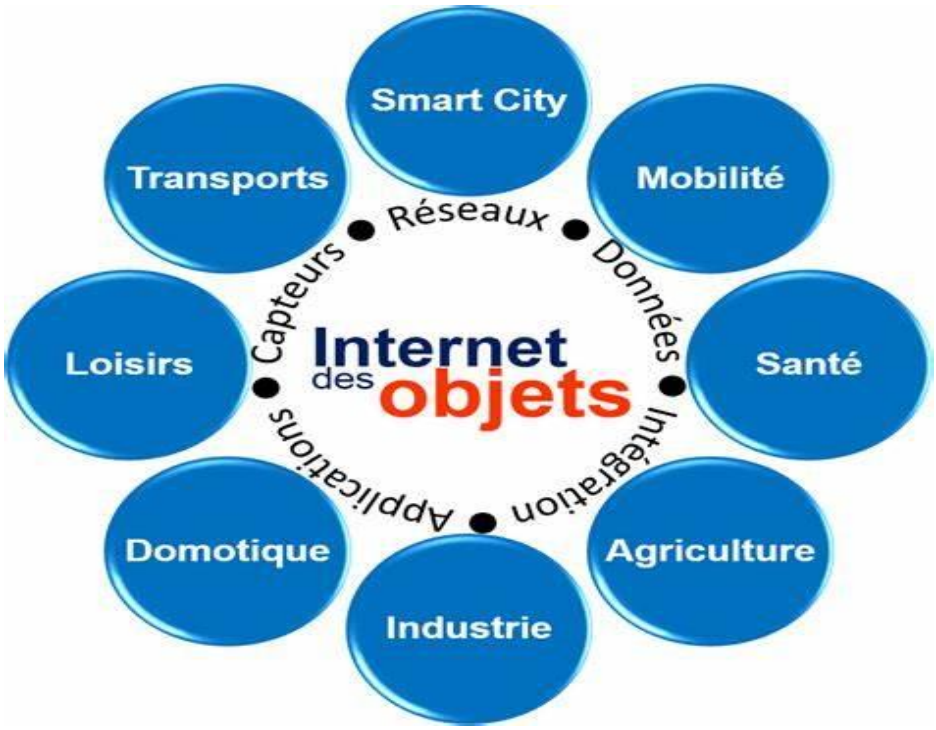


Figure 1: Composants de L'Internet des Objets

2. Historique de l'IDO

1990 : Cette année marque l'apparition des premiers objets connectés, il s'agit de grille-pain, machines à café ou autres objets du quotidien [2].

2000 : Dix ans après, les premières expérimentations d'appareils connectés à Internet verront naissances. 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 [2].

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 [3].

2011 : L'IPV6 va offrir de nouvelles possibilités pour les objets connectés qui disposeront de nouvelles plages d'adresses IP, disponibles et attribuables [2].

A la fin de l'année 2012, il y avait environ 8,7 milliards d'objets connectés dans le monde. Selon la dernière étude de BI intelligence, le nombre d'objet connecté devrait atteindre les 22,5 milliard à l'horizon 2021 contre 6,6 milliard en 2016 avec une augmentation de 17% par an jusqu'en 2025.

3. 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. comme montre la figure 2 :

Figure 2: L'Architecture en couche de l'IDO

I.3.1 Couche de Reconnaissance

Egalement connue sous le nom de couche perceptuelle 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 Radio-frequency identification **(**RFID), différentes types de capteurs, Global Positioning System(GPS) et autres équipements. Les principaux composants de cette couche sont les capteurs pour capturer et représenter le monde physique dans le monde numérique [4].

I.3.2 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 périphéries [4].

I.3.3 Couche 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[4].

I.3.4 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.[4].

4. Les Domaines d'Application de l'IDO

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

I.4.1 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 [5].

I.4.2 Ville Intelligente

Une ville intelligente est un nouveau modèle de développement d'une ville utilisant de nouvelles technologies, telles que l'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 [6].

I.4.3 Industrie de transport

Les voitures, les trains, les autobus, les avions et les bicyclettes avancés sont équipés de 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. [7].

I.4.4 Industrie de Télécommunication

L'IDO créera la possibilité de fusionner diverses technologies de télécommunication et créer de nouveau services. Un exemple illustratif est l'utilisation de GMS, (NFC) Near Fiel Communication, Bluetooth à faible puissance, Zigbee, wifi à faible puissance, WiMax, un réseau de capteur ainsi que la technologie de la carte SIM

I.4.5 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 [7].

I.4.6 Smart Energie

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 gérer leur consommation pour le rasage des coûts et l'optimisation des résultats [8].

Figure 3: Domaines d'application de l'IDO

5. Avantages de l'IDO

Il y'a 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.

6. Inconvénients de l'IDO

✓ Problème de 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.

✓ Problème de 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.

7. Les Défis de l'IDO

Dans le concept de l'IdO, on peut trouver une pléthore de dispositifs connectés à l'Internet générant des quantités énormes de données. Ces données si elles sont 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 :

I.7.1 Evolutivité

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.

I.7.2 Infrastructure du Réseau

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 [7].

I.7.3 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 [9].

I.7.4 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 [9].

I.7.5 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 termes de calcul, stockage ou transmission d'information.

I.7.6 Sécurité

Dans le domaine de la sécurité les défis sont les suivants:[7]

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

• L’identification proactive et la protection de l’IdO contre les attaques arbitraires (DoS et DDoS, par exemple) et les abus.

• 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.

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 différentes attaques, les services et mécanismes de sécurité appropriée.

Chapitre 2

La Sécurité dans L'Internet des Objets

Introduction

L’évolution d’internet vers l’internet des objets se fait grâce à l’intégration des systèmes complexes, des objets intélligents, 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. Permettant ainsi une communication internet En effet, l’IdO étend la connectivité jusqu’à l’environnement des objets via l’Internet traditionnel, le réseau mobile, les réseaux de capteurs et actionneurs etc., d’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 éfficaces, 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.

1. Les Vulnérabilités

Dans le domaine de la sécurité informatique, une vulnérabilité est une faiblesse dans un système informatique, permettant à un attaquant de porter atteinte à l'intégrité du système, c'est-à-dire à son fonctionnement normal, à la confidentialité et l'intégrité des données qu'il contient. Dans le domaine de l’IoT, nous distinguons deux catégories de vulnérabilité: les vulnérabilités physiques et les vulnérabilités technologiques.

II.1.1 Vulnérabilités Physiques

La vulnérabilité physique s’explique par le fait qu’un capteur est très souvent installé dans un lieu peu sur. Nous pouvons citer les lieux de détection d’incendies ou de chaleur dans les industries, les appareils électroménagers, ainsi que les bâtiments, maisons intelligentes et musées ("smart environnent").

II.1.2 Vulnérabilités Technologiques

La vulnérabilité est liée à la technologie sans-fil sous-jacente, les attaquants possédant un récepteur adéquat peuvent potentiellement écouter ou perturber les messages échanges entre les utilisateurs et le nœud capteur. Les mécanismes de routage sont d'autant plus critiques dans le domaine de l’IoT, surtout dans le cas où plusieurs nœuds participent à l'acheminement des paquets à travers le réseau. La puissance de calcul et la capacité de stockage d’un nœud sont fortement limitées.

2. Les attaques visant l'IDO

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.

II.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[10]. En fait, beaucoup d'informations nous concernant provenant d'objets connectés à nous ou nous entourant pourraient ainsi être facilement collectés.

II.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 [11].

✓ Déni de service : Il se traduit par l'échec des nœuds-suite à une action malveillante, d'accéder aux services et/ou aux ressources auxquelles ils n'ont pas 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 par Déni of Service (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 [12].

✓ 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 [12].

✓ 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 [13].

✓ 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 [13].

✓ Renvoi sélectif: un nœud malveillant joue le rôle de routeur, en refusant de transmettre certains messages, en les écartant tout simplement [14].

✓ 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 [13].

✓ Epuisement : Consommer toutes les ressources énergétiques du nœud victime, en l'obligeant à effectuer des calculs ou à recevoir ou transmettre inutilement des données[14].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 [13].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 envois 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 [15].

3. Les 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 champ 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'IdO seront 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 :

II.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.

II.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 [10].La confidentialité peut être assurée en utilisant les algorithmes de cryptographie asymétrique comme le Rivest–Shamir–Adleman (RSA) ou les algorithmes de cryptographie symétrique comme Advanced Encryption Standard (AES) et le Data Encryption Standard (DES).

II.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 [16].

II.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 [17]. 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.

II.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 [18].

II.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 [18].

Figure 4: Les principaux Services de Sécurité

4. Les Mécanismes de Sécurité

Dans les réseaux informatiques, les mécanismes de sécurités correspondent à l'ensemble des moyens techniques et algorithmiques misent en place pour pourvoir sécuriser un réseau. Dans le contexte de l'Internet des Objets, les mécanismes de sécurités dépendent de l'application utilisée, qui dépendent en retour des services de sécurités demandés par l'application. Plusieurs mécanismes de sécurités, sont mis en place afin de répondre à la question de la sécurité dans le domaine de l'IoT.

II.4.1 La Cryptographie

Etant sans doute la technique la plus utilisée dans la plupart des mécanismes de sécurisation actuelle, la Cryptographie désigne l'ensemble des méthodes ou techniques (chiffrement, signature numérique, fonction de hachages et certificat) permettant de garantir intégrité, authenticité, confidentialité des informations sensibles. La figure suivante illustre le fonctionnement des chiffrements

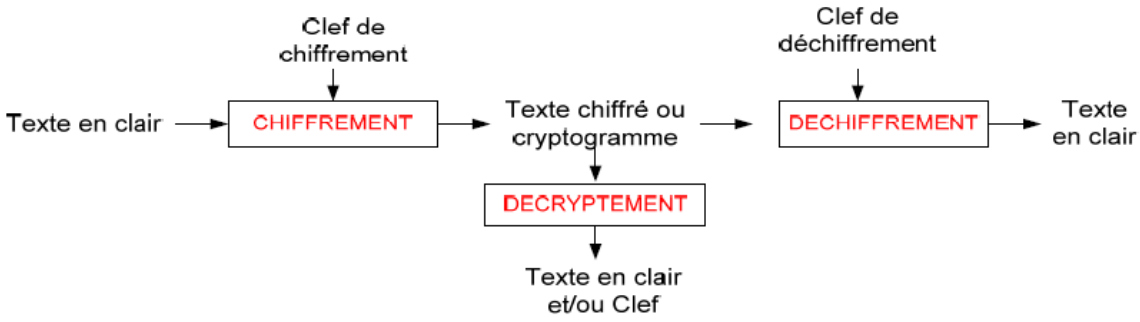


Figure 5: Description de la Cryptographie

II.4.1.1 Le Chiffrement

Le chiffrement (ou cryptage) est un procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de chiffrement. Autrement dit, il permet de rendre des données transmis dans un réseau sans fil illisibles sans la possession d'informations supplémentaires. Ces informations supplémentaires sont la méthode utilisée pour chiffrer et la clé utilisée par la méthode. Cette méthode est une fonction appliquée à deux entrées, qui sont les données à chiffrer (généralement appelé texte en clair) et la clé. La clé et le texte en clair déterminent la version chiffrée des données, aussi appelée texte chiffrée.

a. Chiffrement Symétrique

Le principe du chiffrement symétrique est basé sur le partage d'une clé privé k entre deux entité communiquant dans un réseau. Cela signifie que la clé k chiffrement est égale à la clé de déchiffrement. La figure ci-dessous illustre le fonctionnement du chiffrement symétrique

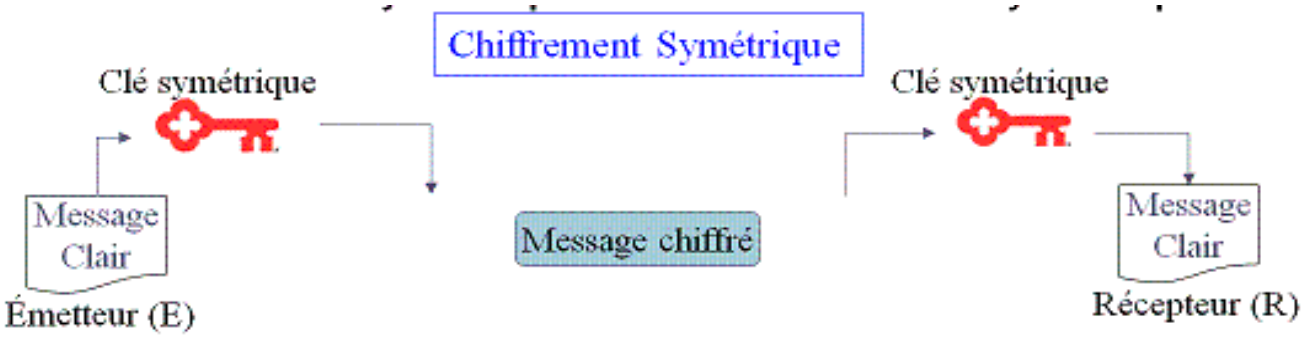


Figure 6: Scénario du Chiffrement à clé privé

Il existe deux types de chiffrement symétrique. Les chiffrements par flux et le chiffrement par bloc.

• Le chiffrement par bloc

Dans ce type de chiffrement, il y a une séparation du texte clair en blocs d'une longueur fixe. La plupart des chiffrements par bloc combinent plusieurs tours d'opération répétées, où la clé appliquée à chaque tour est obtenue par une transformation de la clé d'origine en utilisant un mode opératoire. Parmi les algorithmes de chiffrement par bloc on a :

Advanced Encryption Standard (AES) : il prend en entrée un bloc de 128 bits et la clé fait 128, 192 et 256 bits. Il est connu sous le nom de Rijindael, et il est l'un des algorithmes les plus populaires des algorithmes de chiffrement symétrique. Il comprend une phase de distribution de clé, une phase de chiffrement et une phase de déchiffrement.

RC5 (« Ron's Code) : il prend en entrée des blocs de 32, 64, et 128 bits et la clé varie de 0 à 255 bits. Il est résistant aux attaques linéaires.

• Le Chiffrements par flux

Les algorithmes de chiffrement de flux (peuvent être définis comme étant des algorithmes de chiffrement par blocs, où le bloc a une dimension unitaire (1 bit, 1 octet, etc.) ou relativement petite. Leurs avantages principaux viennent du fait qu'ils soient extrêmement rapides. Les modes opératoires d'OFB (Output FeedBack), CFB (Cipher FeedBack) et CTR (CounTer)

transforment un chiffrement par bloc en chiffrement par flux. Ceci signiefie que la longueur du texte chiffré est la même que la longueur du texte en entrée.

b. Chiffrement Asymétrique

Le chiffrement asymétrique se base sur deux clés (une privée et une autre publique). La clé publique est diffusée à tous les nœuds et servant au chiffrement de données qu'ils vont émettre au récepteur, et une clé privée maintenue secrète chez le récepteur servant pour le déchiffrement de ces données lorsque ce dernier les reçoit. Le point fondamental sur lequel repose la sécurité du chiffrement asymétrique est l'impossibilité de déduire la clé privé à partir de la clé publique. Ici la clé de chiffrement est différente de la clé de déchiffrement. La figure suivante illustre le fonctionnement des algorithmes à clé asymétrique.

Figure 7: Scénario du chiffrement à clé publique

Parmi ces algorithmes de chiffrement asymétrique on peut citer :

- **RSA**

Publié en 1978 par trois personnes Rivest, Shamir et Adleman, d'où le nom RSA, Il est utilisé presque dans toutes les applications notamment dans le commerce électronique. Il est basé sur les nombres premiers et est composé de trois étapes : la génération de clés, le chiffrement et le déchiffrement. Pour casser l'algorithme du RSA, il faut donc pourvoir factoriser des nombres, c'est-à-dire trouver tous les nombres premiers qui divisent un nombre. La figure suivante illustre le fonctionnement du RSA.

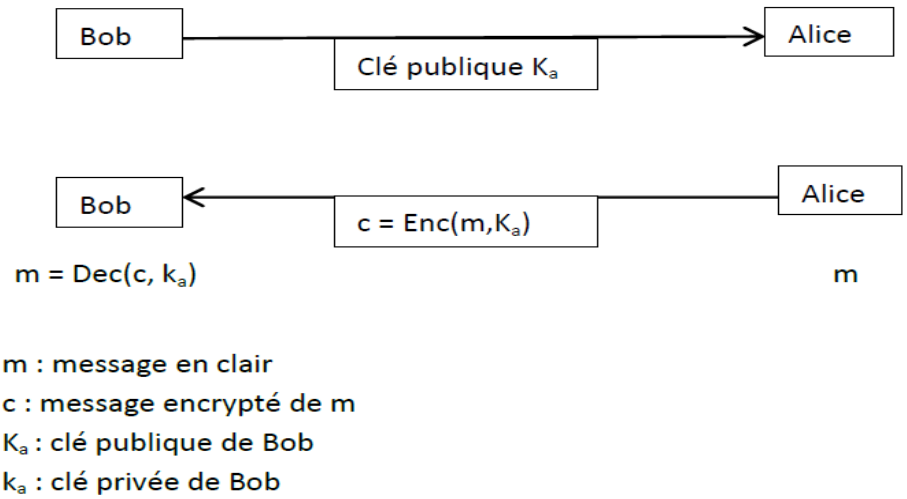


Figure 8: Le chiffrement RSA

Avantage : Comme tout système asymétrique, RSA ne nécessite pas d'avoir un canal sécurisé pour échanger la clé. Par ailleurs l'algorithme RSA est relativement simple et son principal atout est sa sécurité.

Inconvénients : Il est plus couteux d'utiliser le système RSA qu'un système symétrique car les clefs sont plus grandes pour le RSA et donc le chiffrement et le déchiffrement sont plus longs. Le RSA est gourmant en termes de consommation d'énergie.

- **ECC**

La cryptographie basée sur les courbes elliptiques ou Elliptic Curve Cryptography (ECC) en Anglais a été proposée dans les années 80. Récemment, ECC a attiré beaucoup l'attention des chercheurs en raison de son exigence de clés de plus courte taille comparativement à d'autres techniques de cryptographie à clé publique à l'instar de RSA en particulier dans le domaine des systèmes embarqués où les dispositifs ont une puissance de calcul très limitée. Ils ont démontré qu'une clé de 160 bits dans ECC est équivalente à une clé de 1024 bits dans RSA.
Une courbe elliptique sur un champ k est l'ensemble de solution défini par l'équation suivante.

$$y^2 = x^3 + ax + b \bmod p \qquad 4a^3 + 27b^2 \bmod p \neq 0$$

Une courbe elliptique qui est définie sur un corps fini et représentée par les paramètres suivants : a, b et p. la Figure suivante illustre deux exemples de courbes elliptiques.

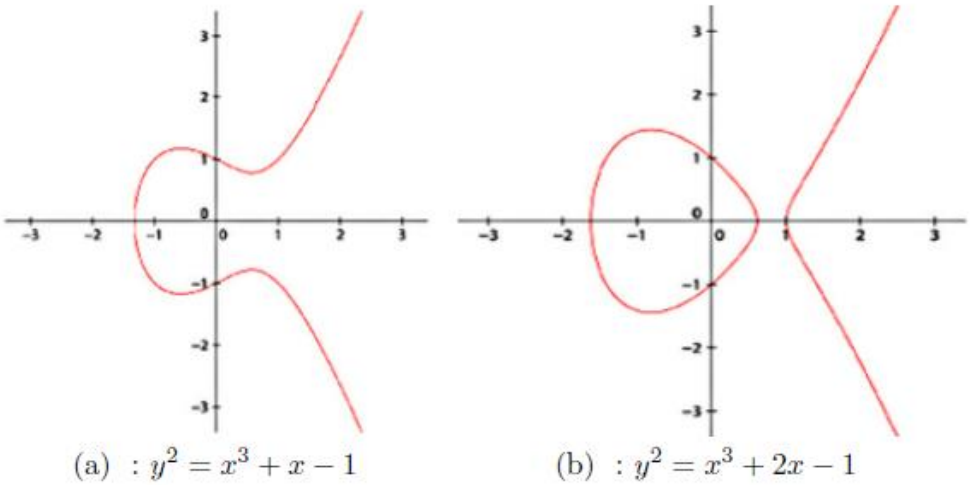


Figure 9: Le chiffrement ECC

Comparaison *RSA et ECC*

Le tableau ci-dessous compare la taille des clés utilisées en cryptographie dans RSA et ECC.

RSA (taille de la clé en bits)	**ECC** (taille de la clé en bits)
1024	*160*
2048	*224*
3072	*256*

Tableau 1: Tableau Comparatif du chiffrement RSA et ECC

Ce tableau comparatif montre que la cryptographie basée sur les courbes élliptiques permet d'utiliser des clés de taille moyenne comparativement à celles du RSA tout en fournissant les mêmes performances. Ce constat permet de favoriser l'utilisation des courbes élliptiques pour les systèmes possédant des ressources limitées en termes de mémoire et CPU tels que les capteurs (IoT). Dans ce contexte, nous pourrons parler de cryptographie légère.

II.4.1.2 Les Fonctions de hachage

Une fonction de hachage est une fonction particulière à sens unique qui à partir d'une donnée fournie en entrée, calcul une empreinte servant à identifier rapidement la donnée initial. Elles prennent en entrée des blocs de texte de n-bit pour produire de valeur hachées de **m_bit**. Elles sont utilisées entre autre pour l'intégrité des données et l'authentification. La figure suivante illustre le fonctionnement général des fonctions de hachages.

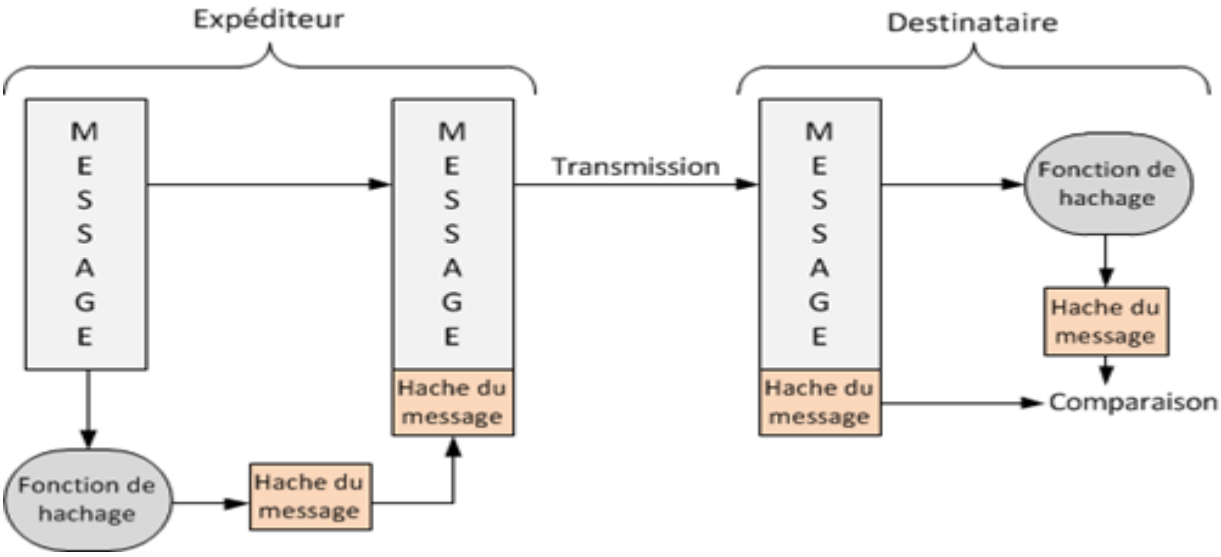


Figure 10: Scénario de la Fonction de Hachage

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, on mettra l'accent sur l'authentification et ses différentes approches, ensuite nous allons faire une étude complète sur un protocole d'authentification continue dans l'Internet des Objets.

Chapitre 3

Etat de l'Art et Etude du protocole d'authentification continue de Yo-Hsuan Chuang et All.

L'authentification est un service de sécurité indispensable. L'objectif est d'identifier la légitimité d'une entité telle qu'un appareil ou un utilisateur. Basé sur la littérature précédemment publiée, l'authentification des utilisateurs est divisée en deux catégories : authentification statique et authentification continue [19]. Un général processus statique d'authentification de l'utilisateur sera invoqué au début d'une session de communication pour authentifier l'identité d'un utilisateur, qui tente de se connecter à un serveur de service correspondant [19,20].

Introduction

Vu l'ampleur et les champs d'applications de l'IdO, la sécurité des objets connectés 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. En général, un secret connu, possédé ou biologiquement hérité par l'utilisateur authentique, tel que le mot de passe, carte à puce, jeton de sécurité, traits du visage et empreintes digitales seront utilisés comme demande d'authentification [21,22]. Malheureusement, l'authentification statique ne peut pas se défendre contre les attaques de détournement de session. Afin de renforcer la sécurité, le concept d'authentification continue est développé. Elle permet d'authentifier à plusieurs reprises la légitimité d'un utilisateur pour l'usage de l'appareil. Cependant, l'authentification continue ne remplace pas l'authentification statique [22]. En fait, il complète l'authentification statique pour améliorer la force de sécurité.

1. Travail Connexe de l'Authentification

Comme les environnements IoT sont ouverts ou semi-ouverts à leurs utilisateurs potentiels en général, les adversaires peuvent facilement accéder aux périphériques déployés dans un environnement IoT. Par conséquent, ces dernières sont vulnérables à diverses menaces à la sécurité. En outre, des mécanismes d'authentification devraient être mis en œuvre pour assurer une communication sécurisée entre les appareils. Dans cette section, la littérature connexe sur les authentifications et authentification continue des environnements IoT sont discutées.

III.1.1 Authentification Statique

Dans cette sous-section, nous catégorisons les protocoles d'authentification statique existants d'un appareil à l'autre pour l'environnement IoT en trois groupes : l'authentification basée sur la certification, l'authentification basée sur le cryptage, et l'authentification non basée sur le chiffrement.

- **Authentification basée sur la certification**

Elle désigne l'utilisation d'un certificat numérique pour identifier un utilisateur, une machine ou un périphérique avant de lui octroyer l'accès à une ressource. Cette méthode est souvent déployée conjointement à d'autres méthodes classiques comme l'authentification basée sur un nom d'utilisateur et un mot de passe. Le protocole Datagram Transport Layer Security (DTLS) [23] est une norme existante. En 2013, Kothmayr et all. [24] ont proposé un système d'authentification de sécurité pour IoT basé sur le DTLS, qui a utilisé le chiffrement asymétrique basé sur RSA et X.509 Certification. Par conséquent, pour mettre en œuvre ce système, des coûts de consommation plus élevés et plus d'espace de stockage sont nécessaires,

les dispositifs de détection sont contraints par les ressources. En 2014, Porambage et all. [25] ont proposé un protocole d'authentification en utilisant un certificat implicite dans les environnements IoT distribués. Mais, depuis que la cryptographie sur les courbes élliptiques ou Elliptic Curve Cryptography en anglais (ECC) consomme moins de ressources informatiques par rapport au RSA, le protocole dans [25] utilise le système de certificat implicite Elliptic Curve Qu-Vanstone (ECQV) et l'Elliptique Curve Diffie-Hellman (ECDH) pour l'échange de clé. Le protocole utilise des certificats implicites pour l'authentification de bout en bout dans des environnements IoT distribués. Le protocole contient deux phases qui sont : la phase d'enregistrement et la phase d'authentification. Bien que le travail proposé adopte ECC pour réduire les frais généraux de calcul pour les dispositifs de détection, le protocole nécessite encore un certain espace de stockage dans les appareils pour stocker les certificats implicites et il exige également une Autorité de Certificat (CA). Ainsi, la solution basée sur les clés asymétriques surmonte les défis de sécurité avec une évolutivité élevée. Cependant, leurs inconvénients est qu'ils nécessitent un grand coût de calcul.

- **Authentification basée sur le chiffrement**

Elle est basée sur les touches chiffrées, stockées dans chaque routeur et le client (ordinateur) autorisés à être sur le réseau. Dans cette catégorie d'authentification le chiffrement est basé essentiellement sur l'algorithme Advanced Encryption Standard (AES). En 2015, Shivraj et coll.[26] ont proposé une authentification à mot de passe unique (BdP) pour les infrastructures IoT. Le protocole adopte la Courbe elliptique basée sur l'identité cryptographique (IBE-ECC) pour fournir une authentification légère de bout en bout entre les appareils. L'avantage du protocole est que les dispositifs de détection n'ont pas besoin de stockage supplémentaire pour stocker les clés. Toutefois, si les appareils doivent communiquer, ils doivent demander fréquemment au cloud central de générer le BdP. En 2015, Mahalle et all.[14] ont proposé un protocole d'authentification de groupe pour les environnements IoT. Le protocole pourrait effectivement authentifier les appareils dans le même groupe. Le programme TCGA [27,28] établit une clé de session pour chaque authentification de groupe afin d'obtenir une authentification efficace entre les membres du groupe. L'inconvénient de ce schéma est que si un nouveau membre rejoint le groupe, les clés du groupe doivent être régénérés et redistribués à tous les membres du groupe à nouveau. Ainsi, si l'environnement IoT ciblé doit fréquemment changer les membres de l'appareil dans leur groupe, il peut causer des authentifications supplémentaires pour les appareils. En 2015, Khemissa et Tandjaoui [29] ont proposé une authentification légère pour les environnements IoT sans utiliser d'opérations cryptographiques complexes. Le protocole employait des opérations de code d'authentification des messages basés sur le hachage ou hash-based message authentication code (HMAC)[30] pour établir l'authentification mutuelle. L'Advanced Encryption Standard (AES) [31], est le mécanisme de cryptage qui a été utilisé pour générer une clé de session. Par conséquent, le système nécessite des dispositifs de détection possédant la capacité d'effectuer des opérations cryptographiques à clé privé. En 2016, Khemissa et Tandjaoui [32] ont étendu leur travail dans [29] pour soutenir les utilisateurs distants. Le protocole pourrait faire une authentification mutuelle entre un nœud capteur et un utilisateur distant. Un utilisateur peut utiliser son mobile pour gérer les ressources de détection hétérogènes. En 2016, Kumar et coll. [33] ont présenté un protocole d'établissement de clé de session, léger et basé sur l'authentification pour une maison intelligente. Ce protocole nécessite un fournisseur de services de sécurité, qui est un serveur de confiance. Le fournisseur de services de sécurité assigne les paramètres importants, génère des jetons et les distribue aux appareils de communication dans un environnement familial

intelligent. Les appareils utilisent un jeton authentifié pour établir une clé de session pour parvenir à l'authentification mutuelle. Ainsi, ces mécanismes de sécurité ont été proposés sur la base de la cryptographie à clé privé en raison de son efficacité en termes de calcul et de consommation d'énergie, par contre le problème de l'évolutivité et l'exigence de stocker les clés dans une mémoire le rend inefficace et hétérogène pour le contexte de l'IoT.

- **Authentification non basée sur le chiffrement**

Dans cette catégorie, les approches proposées n'utilisent aucune technique de certification ou toute autre opération de cryptage. En 2015, Gope et coll. [34] ont proposé un protocole d'authentification non-traçable dans l'architecture IoT distribuée. Le système n'utilise que des fonctions de hachage et le ou-exclusive (XOR) ou des opérations pour construire un mécanisme d'authentification léger. En outre, le schéma utilise des nombres de séquences et des nombres aléatoires pour générer un lien unique d'identité. Le régime proposé garantit non seulement la légalité d'un nœud capteur, mais l'anonymat identitaire est introuvable. En 2015, Kawamoto [35] a présenté un système d'authentification dans les environnements IoT. Le protocole utilise des informations ambiantes sur les appareils pour l'authentification. Le système doit collecter en permanence des informations ambiantes à partir des capteurs. Ainsi, cette approche semble être le plus adapté avec le contexte des objets connectés car elle n'utilise aucune opération cryptographique tout en surmontant les défis de sécurité avec une évolutivité considérable.

III.1.2 Authentification Continue

La validité de l'utilisateur est supposée être la même pendant toute une session. Malheureusement, dans de nombreux cas, un utilisateur/appareil peut être laissé sans surveillance pendant des périodes plus ou moins longues ; périodes pendant lesquelles toute personne malveillante peut avoir accès au canal en tant que véritable utilisateur. Ce type de contrôle d'accès est appelée authentification statique. D'autre part, on trouve l'authentification continue où l'authenticité d'un utilisateur/appareil est vérifiée en permanence sur la base de l'activité de l'utilisateur actuel opérant sur le canal. Ainsi, quand le doute surgit sur l'authenticité de l'utilisateur, le système peut verrouiller ou interrompre la communication et l'utilisateur doit revenir au contrôle d'accès, autrement dit au mécanisme d'authentification statique pour continuer la transmission de données. Dans cette sous-section, nous passons en revue la littérature connexe sur l'authentification continue. Nous classons ces protocoles d'authentification en deux modèles : les modèles utilisateur-appareil et les modèles d'appareil à appareil :

- **Modèles utilisateur-appareil**

Plusieurs schémas d'authentification continue des utilisateurs ont été proposés ces dernières années[36,37-38]. L'objectif de ces solutions proposées est d'aider à authentifier constamment l'utilisateur actuel pour éviter que les utilisateurs usurpés d'identité ou illégaux d'accéder aux appareils. Le modèle de communication de ces schémas est d'utilisateur à appareil et la plupart des systèmes utilisent la biométrie pour construire leur processus d'authentification continue. En 2010, Shimshon et all.[37] ont présenté un mécanisme d'authentification continue qui vérifie à plusieurs reprises l'identité des utilisateurs et de l'appareil, basé sur la dynamique de frappe. Le projet proposé recueille plusieurs frappes d'un utilisateur authentique pour créer des vecteurs de fonctionnalités correspondants et utilise ces vecteurs comme base de référence. Une fois

qu'un véritable utilisateur est authentifié pour utiliser l'appareil avec un module d'authentification continue, dans un délai prédéfini, le module recueillera à plusieurs reprises ces frappes, génèrent des vecteurs de fonctionnalités correspondants et les comparent à la base de référence afin de valider que l'utilisateur actuel est en effet celui authentifié. En 2012, Shen et all.[39] ont proposé un protocole d'authentification continu basé sur des modèles dynamiques d'utilisation de la souris par un véritable utilisateur. Il existe d'autres approches adoptant la biométrie multi-comportementale pour construire des mécanismes d'authentification continue. En 2014, Bailey et all.[40] ont proposé un système d'authentification continue utilisant les modèles combinés de clavier, de souris et d'utilisateur Graphique Interactions Interface (GUI), générées à partir d'un utilisateur authentique comme base de référence, pour obtenir une plus grande précision d'authentification. En 2015, Buduru et Yau[36] ont introduit un système d'authentification de l'utilisateur basé sur les motifs des gestes des doigts de l'utilisateur sur l'écran tactile d'un dispositif ciblé. Modèles modifiés de Processus de Décision Markov (MDP) pour différents contextes d'utilisation sont adoptés par le régime de Buduru et Yau. En 2010, Niinuma et all.[41] ont adopté des caractéristiques, y compris la peau du visage et la couleur des vêtements pour construire leur mécanisme d'authentification continue de l'utilisateur. En 2012, Mock et all.[42] ont proposé leur système d'authentification continue des utilisateurs basé sur un mécanisme de reconnaissance de l'iris. Ce système pourrait également ajouter l'option mot de passe de l'utilisateur pour établir une solution d'authentification utilisateur multi facturé. En 2017, Peng et all.[43] ont introduit un mécanisme d'authentification continue pour les utilisateurs qui portent des lunettes intelligentes pour protéger la vie privée des utilisateurs. Ce mécanisme utilise des gestes de toucher des doigts et des commandes vocales pour construire leur biométrie. En 2017, Zhou et all.[44] ont proposé un système d'authentification transparent, authentifier l'utilisateur ciblé par le jeton d'authentification, qui contient les modèles d'ondes cérébrales de l'utilisateur.

- **Modèles d'appareil à appareil**

D'après ces auteurs, la recherche faite pour ce modèle montre qu'il n'existe pour le moment aucune étude sur le modèle d'appareil à appareil dans les environnements IoT. En 2015, Bamasag et Youcef-Toumi[46] ont proposé une authentification continue légère de l'utilisateur pour les environnements IoT. Leur travail a identifié le besoin d'authentification continue dans les environnements IoT. En tant que dispositifs de détection dans de scénarios particuliers, tels que la surveillance de la santé personnelle et les systèmes de contrôle industriel[45], le besoin de transmettre fréquemment des données détectées aux passerelles dans un court laps de temps, un mécanisme d'authentification pourrait accomplir une authentification plus rapide. Dans le schéma proposé, des données secrètes sont utilisées pour construire des jetons d'authentification et seule les jetons et les messages doivent être transmis de l'utilisateur au serveur dans un intervalle de temps prédéfini pour une authentification continue. Le serveur peut vérifier que les messages reçus sont envoyés à partir d'un véritable utilisateur en se basant sur les jetons associés. Même si le protocole proposé dans[46] est en norme un modèle utilisateur-appareil, il a inspiré les chercheurs à concevoir un nouvel protocole léger d' appareil à appareil d'authentification continue.

En résumé, nous avons constaté que les détails de l'ensemble des données, dans la littérature précédente, sont différentes les unes des autres. Quelques études ont collecté un grand nombre d'échantillons de données auprès de quelques sujets, tandis que d'autres études ont acquis une petite quantité de données à partir d'un grand nombre de sujets.

De plus, différentes approches sont toujours évalués à l'aide de différentes données (souvent arbitraires). Cela a causé un problème pratique pour la recherche biométrique, d'où la difficulté de comparer ces résultats les uns aux autres. Ainsi, la proposition d'un schéma d'authentification sans l'utilisation d'opération cryptographique et l'avantage de ne pas conserver des informations à caractères personnelles à la différence des approches adoptant la biométrie nous ont motivé pour le choix du protocole dans[44].

2. Protocole d'authentification continue

Dans un environnement IoT, l'authentification d'un appareil à l'autre est devenue une question pratique et fondamentale. La plupart des appareils de détection ont des ressources informatiques et de capacité de stockage limitées[46]. Ces appareils ne peuvent pas effectuer des calculs complexes tels que le cryptage et opérations de décryptage à moins qu'elles n'aient été équipées d'une quantité suffisante de mémoire flash et suffisamment de microcontrôleurs avec de grande puissance de calcul (ex. Dispositifs contraints classés comme classe 2 dans[47,48]). Les approches existantes ont proposé des protocoles légers pour authentifier la légitimité d'un utilisateur lorsqu'un message doit être transmis à l'appareil[26,49 - 25]. Toutefois, il est possible que beaucoup de messages instantanés soient transmis en peu de temps entre un nœud capteur et une passerelle dans un environnement IoT. Dans de telles circonstances, les solutions d'authentification peuvent consommer beaucoup de temps dans le processus d'authentification par rapport aux temps nécessaire au traitement du message reçu. Par conséquent, l'objectif de cette étude est de concevoir un protocole d'authentification continue d'un appareil à l'autre pour authentifier les données échangées entre deux appareils dans un délai prédéfinis pour un environnement IoT. Le protocole d'authentification continue proposé dans[44] comporte les caractéristiques suivantes :

- Le protocole prend en charge l'authentification mutuelle, c'est-à-dire que les deux appareils pairs peuvent s'authentifier avant de transmettre des messages ;
- Le protocole n'utilise que des opérations de calcul légères, qui incluent l'authentification de message basée sur le hachage (HMAC)[30], la fonction de hachage, et opération ou-exclusive (XOR), de sorte que la plupart des appareils de détection avec une ressource informatique limitée auront une bonne chance d'adopter ce protocole et d'installer le module de protocole correspondant ;
- Le protocole contient deux phases : la phase d'authentification statique pour générer dynamiquement les jetons initiaux pour les parties communicantes et la phase d'authentification continue pour la transmission du jeton authentifié ainsi que les données détectées par le capteur à la passerelle. Le protocole adopte des jetons techniques et le prise en charge de l'authentification continue dans laquelle le jeton de session contient secrètement la dynamique (ou dépendante du temps) de l'appareil de détection, c'est-à-dire la capacité restante de la batterie du dispositif de détection dans le schéma proposé. En outre, il y'a le concept de temps d'authentification, une période de temps valide est proposée pour améliorer la robustesse de sécurité de l'authentification entre les appareils IoT. L'analyse de la sécurité et l'analyse du rendement sont effectuées pour évaluer la force de sécurité et le temps d'exécution du protocole étudié[44]. Ce protocole peut également être étendu en deux aspects

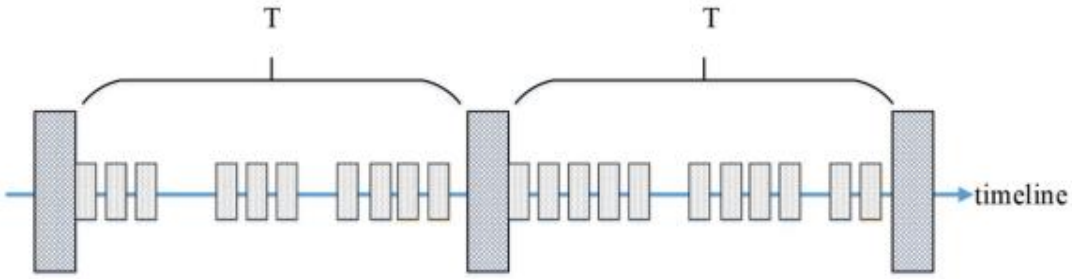
: l'adoption de l'option de mise en œuvre du protocole d'initialiser les communications par la passerelle et l'ajout de l'anonymat de l'identité sur les dispositifs de détection. Dans notre mémoire, nous allons proposer un schéma pour la demande d'initialisation de la passerelle et essayer de réduire, le mieux possible, les opérations de calcul et la taille des données à hacher.

3. Etude du protocole dans[52]

Dans cette section, nous étudions le protocole d'authentification proposé par Yo-Hsuan Chuang et all.[52]. Nous décrirons le concept de conception, les hypothèses et notations du protocole. Il est composé de trois phases : une phase d'initialisation, la phase d'authentification statique et la phase d'authentification continue.

III.3.1 Concept de Conception

Dans certains environnements IoT tels que la surveillance en usine et les systèmes d'hospitalisation intelligents, les nœuds capteurs transmettent fréquemment un grand nombre de données détectées à la passerelle dans un court laps de temps. Depuis que le temps d'intervalle de chaque session de transmission de données est très court, la passerelle doit fréquemment authentifier les communications avec les dispositifs (nœuds capteurs) au début de chaque session de transmission de données. Afin de rapidement assurer l'authenticité des appareils pour chaque donnée reçue lors d'une session valide, nous adoptons la conception de l'authentification continue. Elle peut faire gagner du temps d'authentification pour chaque session de transmission de données. Le protocole dans[52] utilise la valeur de la capacité restante de la batterie comme facteur dynamique pour authentifier un dispositif de détection. Ce protocole contient deux phases d'authentification, qui sont la phase d'authentification statique et la phase d'authentification continue. Dans chaque phase, un système d'authentification correspondant est développé. Le schéma d'authentification statique est similaire au schéma général ou traditionnel et il est appliqué pour authentifier les dispositifs au début d'une période d'authentification T. Le système d'authentification continue est appliqué à chaque transmission de données (période d'authentification actuelle T). Pour clarifier davantage ce mécanisme, la Figure 11 montre le protocole par chronologie, dans lequel les blocs de points indiquent des sessions d'authentification statiques et les blocs réticulaires indiquent des sessions d'authentification continues. Si un capteur transmet des données détectées vers une passerelle, le nœud capteur et la passerelle s'authentifient mutuellement. Après avoir passé la phase d'authentification statique, l'authentification continue est appliquée à chaque transmission de données détectée du capteur à la passerelle durant la période d'authentification T. Il peut y'avoir des intervalles de temps dans lesquels aucune transmission de données ne se produit pendant une période d'authentification T.



Session d'authentification statique pour générer le jeton initial.

Session d'authentification continue pour la transmission de données.

T La période d'authentification définie par la passerelle pour les sessions de transmission de données à authentification rapide après une authentification statique réussie.

Figure 11: Le Cadre de protocole d'authentification proposé à travers le calendrier

Dans la période d'authentification prédéfini T, le processus d'authentification statique est d'abord invoqué, pour les dispositifs de communication, pour mettre en place un jeton authentifié, qui sera utilisé pour chaque session d'authentification. Ensuite, pendant la période d'authentification T, la passerelle peut rapidement vérifier la légalité du nœud capteur lorsqu'un nouveau message ou données doit être transmis entre les deux parties. Avec l'utilisation d'un jeton authentifié, le système d'authentification continue passe moins de temps pour le calcul que le schéma d'authentification statique. Le protocole dans[52] n'utilise aucune opération cryptographique; par conséquent, il s'agit d'un protocole d'authentification léger.

III.3.2 Hypothèses et Notations

III.3.2.1 Hypothèses

Les hypothèses pour le protocole étudié sont énumérées comme suit :

1. Les nœuds capteurs sont des dispositifs limités en ressources, alimentés par une ou plusieurs batteries, qui ont une capacité de calcul et espace de stockage très petite. Chaque nœud capteur est capable d'effectuer le fonctionnement du hachage et dispose d'un générateur de nombres aléatoires.

2. Les passerelles sont des dispositifs illimités en ressources, qui ont une capacité de calcul suffisante pour effectuer le fonctionnement du hachage et générer des nombres aléatoires, et un espace de stockage pour stocker temporairement des valeurs et tableaux de données prédéfinis.

3. Plusieurs capteurs peuvent être gérés par une seule passerelle. Chaque nœud capteur et la passerelle partagent une valeur secrète distincte qui est définie dans la phase d'initialisation du protocole d'authentification.

4. Le nœud capteur ne peut pas numériser ni afficher avec précision sa capacité d'énergie (ou de batterie) restante sur son panneau d'affichage (s'il en a un).

III.3.2.2 Notations

Les notations utilisées sont définies dans le Tableau 2.

Notations	*Définitions*
SN	Nœud Capteur
GW	Passerelle
ID_{SN}	L'identité d'un nœud de capteur SN
ID_{GW}	L'identité d'une passerelle GW
T	La période d'authentification définie par la passerelle pour les sessions de transmission de données à authentification rapide après une authentification statique réussie. L'unité de temps est par minute
t_s , t_c	Les horodatages
H(·)	Une fonction de hachage à sens unique SN
SK_{SN}	La valeur secrète d'un nœud de capteur
r_1 , r_2 , v	Nombres aléatoires générés par un nœud de capteur SN
n_1,n_2, w	Nombres aléatoires générés par une passerelle GW
$HMAC_{J(\cdot)}$	Fonction de code d'authentification de message basée sur le hachage associée à la clé secrète J
||	Une opération de concaténation
⊕	Une opération ou exclusive au niveau du bit

Notations	*Définitions*
Sd	Données détectées à partir d'un nœud de capteur SN
Ms	La valeur masquée des données détectées à partir d'un nœud de capteur SN
rb	La capacité énergétique actuelle de la batterie du capteur
Er	L'enregistrement de la capacité d'énergie restante de la batterie du capteur après la dernière session
Mb	La valeur masquée de la capacité énergétique de la batterie
TKI_{SN}	Le jeton initial généré par un nœud de capteur et la passerelle communicante
EBC_{SN}	La valeur de la consommation moyenne quotidienne estimée de la batterie pour un nœud de capteur
BCT_{SN}	Energie minimale d'un capteur
ACK	Accusé de réception
***m*, *X*, *Y*, Y_1, M_0, M_1, M_2, M_3, M_4, M_5**	Valeurs intermédiaires

Tableau 2: Notation utilisées dans le protocole

III.3.3 Consommation de Batteries

• Consommation quotidienne de la Batterie (EBC_{SN}) : Afin de calculer les estimations quotidiennes de consommation de la batterie pour un nœud capteur, ils ont proposé une consommation quotidienne de la batterie.

Équation basée sur la durée de vie de la batterie et la capacité de la batterie d'un nœud capteur :

$$\boldsymbol{EBC_{SN} = BC/BL} \qquad \textbf{(1)}$$

Dans l'équation **(1)**, EBC_{SN} indique la valeur de la consommation quotidienne de batterie pour un nœud capteur dans l'unité de milli ampère-heure (mAh) par jour. BC est la capacité de la batterie entièrement chargée d'un nœud capteur dans l'unité de mAh. BL est la durée de vie de la batterie d'un nœud capteur pendant une journée. Nous utilisons le temps d'autonomie de la batterie et la capacité de la batterie (mAh) d'un nœud capteur pour le calcul. L'unité de mesure est le mAh/jour.

•Capacité minimale de la batterie ou Battery Capacity Threshold en Anglais (BCT_{SN}) : Afin de vérifier le reste de la capacité de la batterie dans une valeur raisonnable pour un nœud capteur pendant une période d'authentification T, ils ont conçu une deuxième équation pour estimer le seuil de capacité de la batterie restant tel qu'il est indiqué dans Équation (2):

$$BCT_{SN} = \left[rb - \left(\frac{EBC_{SN}}{24 \times 60} \times T \right) \right] \times s \qquad (2)$$

Dans l'équation **(2)**, BCT_{SN} indique la capacité minimale de la batterie d'un capteur et l'unité de mesure de BCT_{SN} est mAh. EBC_{SN} indique la valeur moyenne quotidienne de consommation de la batterie pour un nœud capteur dans l'unité de mAh par jour. rb est la capacité d'énergie actuelle d'une batterie de capteur. $\left(\frac{EBC_{SN}}{24 \times 60}\right)$ Indique la consommation quotidienne de batterie par minute pour le nœud capteur. $\left(\frac{EBC_{SN}}{24 \times 60} \times T\right)$ Indique cette valeur par période d'authentification T pour le nœud capteur. Par souci de simplicité, ils supposent que la consommation de la batterie du capteur est une relation linéaire en association avec le temps de fonctionnement d'un nœud capteur. Le symbole **s** indique un coefficient d'estimation pour tenir compte d'un écart possible sur la valeur seuil calculée $\left[rb - \left(\frac{EBC_{SN}}{24 \times 60} \times T \right) \right]$. Cette valeur seuil est multipliée par le coefficient **s** pour former la valeur finale de BCT_{SN}. En général, le modèle de consommation de batteries ainsi que la valeur du coefficient **s** d'un dispositif de capteur pourrait être évalué et révélé par le fournisseur du capteur correspondant, où $0 < s < 1$.

III.3.4 Scénario du Protocole

Cette sous-section présente les détails du protocole de Yo-Hsuan Chuang et all.[52], qui se compose de trois phases : la phase d'initialisation, la phase d'authentification statique et la phase d'authentification continue.

III.3.4.1 La phase d'initialisation

Dans la phase d'initialisation, des paramètres importants doivent être mis en place pour les nœuds capteurs et leur passerelle. Cette étape se produit une seule fois entre un nœud capteur et la passerelle ce qui rend négligeable les menaces durant cette phase. Tout d'abord, le nœud capteur soumet son identité ID_{SN} et les informations relatives à la batterie qui comprennent la durée de vie de la batterie et la capacité de la batterie vers la passerelle via un canal sécurisé. Il existe de nombreux moyens pour fournir les valeurs secrètes requises aux capteurs et aux passerelles; par exemple, les fournisseurs de capteurs peuvent préinstaller la valeur secrète dans les capteurs pendant la phase de production et une passerelle peut acquérir les valeurs secrètes d'un serveur tiers de confiance (un site Web de courtier ou le service Web de capteur ciblé fournisseur). Si les capteurs sont des dispositifs de type classe 2 tels que définis dans[47], il est possible qu'une passerelle utilise un canal sécurisé avec ces capteurs grâce à des opérations de cryptage. Dès que la passerelle reçoit la demande d'un nœud capteur, elle génère automatiquement une valeur secrète SK_{SN} qui est liée à l'identité du nœud capteur. Par la suite, la passerelle va calculer également EBC_{SN} qui est la valeur de la consommation quotidienne moyenne estimée de la batterie pour ce nœud capteur SN. Ensuite, la passerelle définit une période d'authentification pour authentifier rapidement les sessions de transmission de données après une tentative d'authentification statique réussie. Après avoir effectué ces taches, la passerelle renvoie en toute sécurité la valeur secrète SK_{SN} au nœud capteur via un canal sécurisé. Dès que le nœud capteur obtient la valeur secrète SK_{SN} de la passerelle, il stocke cette dernière dans son stockage sécurisé. Ensuite, la passerelle enregistre également la valeur secrète du nœud capteur SK_{SN}, la période d'authentification T et l'estimation de la valeur moyenne de consommation quotidienne de la batterie EBC_{SN} pour ce nœud capteur SN dans sa base de données. Par conséquent, la passerelle stocke chaque nœud capteur pour gérer les informations importantes dans le tableau de liaison dont le champ contient l'identité ID_{SN}, la valeur secrète SK_{SN}, la période d'authentification T, et la valeur moyenne estimée de la consommation quotidienne de la batterie EBC_{SN} pour le nœud capteur SN.

III.3.4.2 La phase d'authentification statique

Dans la phase d'authentification statique, un nœud capteur et une passerelle s'authentifient mutuellement. Les deux parties négocient simultanément un jeton initial TK^{I}_{SN} qu'ils vont utiliser pour l'authentification continue pendant la période d'authentification T. La passerelle va calculer l'estimation seuil de capacité restante de la batterie BCT_{SN} qui est utilisé pour vérifier si la valeur de la capacité restante de la batterie d'un nœud capteur est raisonnable, lorsque la passerelle reçoit des données envoyées à partir du capteur dans une session de transmission de données.

La phase d'authentification statique du protocole est selon les étapes suivantes :

1. Nœud capteur ⟶ Passerelle: ID_{SN}, X, M_1, M_2, mb, r_1

Un nœud capteur génère des nombres aléatoires r_1 et v. Ensuite, il obtient la valeur de la capacité énergétique actuelle de la batterie du capteur qui est rb et obtient sa valeur secrète SK_{SN} de son stockage sécurisé. Ensuite, il cache les données de la capacité énergétique actuelle de la batterie du capteur rb dans mb avec l'opérateur du ou-exclusif ce qui donne le calcul : mb = rb $\oplus$ H ($SK_{SN} \oplus r_1$). Après cela, le nœud capteur va calculer X = $\upsilon \oplus$ H(rb) et M_1 = H ((υ || ID_{SN}) $\oplus$ H (SK_{SN})), respectivement.

Par la suite, le nœud capteur utilise la valeur secrète SK_{SN} pour calculer $M_2 = HMAC_{SKSN}$ (ID_{SN}, X, M_1, r_1, mb) afin de garantir son authenticité. Enfin, le nœud capteur envoie ID_{SN}, X, M_1, M_2, mb et r_1 à la passerelle.

2. Passerelle ⟶ Nœud capteur: M_3, M_4, Y, n_1

Lors de la réception d'ID_{SN}, X, M_1, M_2, mb et r_1, la passerelle utilise l'identité du nœud capteur ID_{SN} pour récupérer la valeur secrète correspondante SK_{SN} de sa base de données.

La passerelle utilise ensuite cette valeur secrète SK_{SN} pour calculer $M'_2 = HMAC_{SKSN}$ (ID_{SN}, X, M_1, r_1, mb). Après cela, la passerelle vérifie si la valeur calculée M'_2 est équivalente à la valeur reçue M_2. Si M'_2 et M_2 sont équivalentes, le capteur est authentifié par la passerelle. Dans le cas contraire, la passerelle mettra fin au protocole. Ensuite, la passerelle va calculer rb'= mb$\oplus$ H ($SK_{SN} \oplus r_1$) et utilise rb' pour calculer $\upsilon' = X \oplus H(rb')$. Après la récupération de rb' et υ', la passerelle prend le nombre aléatoire υ' pour calculer $M_1' = H(\upsilon' \| ID_{SN}) \oplus H(SK_{SN})$). Ensuite, la passerelle vérifie si la valeur calculée M_1' est équivalente à la valeur reçue M_1. Si M_1' et M_1 sont équivalents, cela indique que les valeurs obtenues de υ' et rb' sont correctes. Sinon la passerelle mettra également fin au protocole. Le calcul de M_1 permet de garantir l'intégrité des données reçu du capteur.

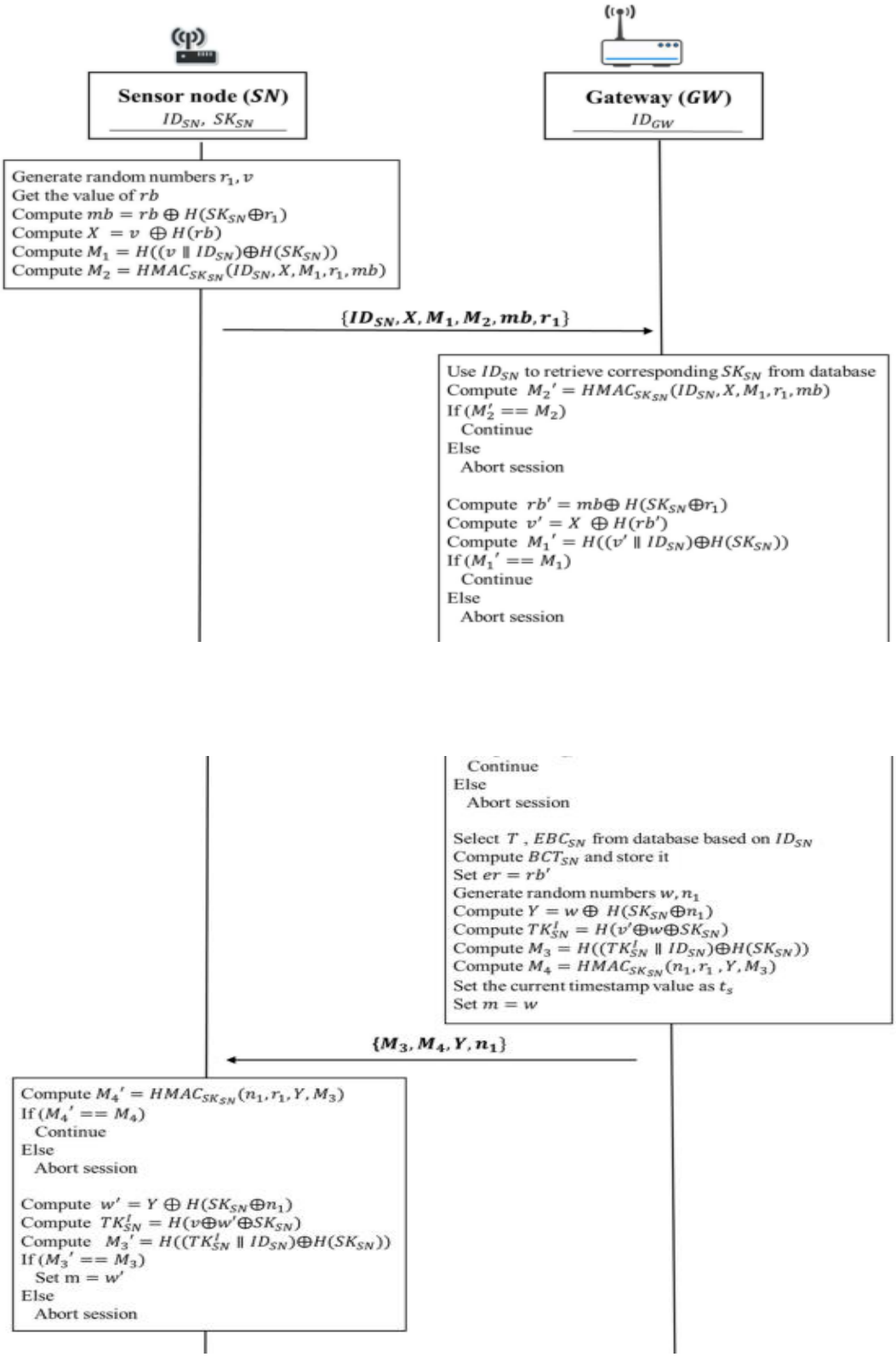


Figure 12: La phase d'authentification statique du protocole étudié

Une fois les tâches de vérification ci-dessus terminées, la passerelle récupère la période d'authentification T et la valeur moyenne estimée de la consommation quotidienne de la batterie EBC_{SN} à partir de sa base de données associée à ID_{SN}. Par la suite, la passerelle utilise la période d'authentification T et la valeur moyenne estimée de la consommation quotidienne de batteries EBC_{SN} pour calculer la valeur de l'estimation seuil de capacité de la batterie restant BCT_{SN} pour le nœud capteur. Ensuite, la passerelle définit er = rb'. Après cela, elle génère deux nombres aléatoires w et n_1.

La passerelle effectue les deux calculs suivants $Y = w \oplus H(SK_{SN} \oplus n_1)$ et $TK^I_{SN} = H(\upsilon' \oplus w \oplus SK_{SN})$, respectivement. La passerelle utilise le jeton initial TK^I_{SN} pour calculer $M_3 = H(TK^I_{SN} \| ID_{SN}) \oplus H(SK_{SN}))$. Par la suite, la passerelle utilise la valeur secrète SK_{SN} et le nombre aléatoire n_1 pour calculer $M_4 = HMAC_{SKSN}(n_1, r_1, Y, M_3)$. Ensuite, la passerelle stocke BCT_{SN} et TK^I_{SN} dans sa base de données. Il a également définit la valeur actuelle de l'estampille de temps comme ts et définit m = w. Enfin, la passerelle envoie M_3, M_4, Y et n_1 au nœud capteur.

En recevant M_3, M_4, Y et n_1 de la passerelle, le capteur utilise la valeur secrète SK_{SN} pour calculer $M'_4 = HMAC_{SKSN}(n_1, r_1, Y, M_3)$. Après ce calcul, il vérifie si la valeur calculée M'_4 est équivalente à la valeur reçue M_4. Cette opération permet de garantir l'authentification mutuelle entre le capteur et la passerelle. Si M'_4 et M_4 sont équivalents, il indique que tous les messages obtenus ne sont pas modifiés. Dans le cas contraire, le nœud capteur mettra fin au protocole. Ensuite, le nœud du capteur va calculer $w' = Y \oplus H(SK_{SN} \oplus n_1)$. Ensuite, le nœud capteur utilise le nombre aléatoire w' pour calculer $TK^I_{SN} = H(\upsilon \oplus w' \oplus SK_{SN})$. Après cela, le nœud capteur utilise le jeton initial TK^I_{SN} pour calculer $M'_3 = H((TK^I_{SN} \| ID_{SN}) \oplus H(SK_{SN}))$. Ensuite, le capteur vérifie si la valeur calculée M'_3 est équivalente à la valeur reçue M_3. Si M'_3 et M_3 sont les mêmes, il indique que le jeton initial calculé TK^I_{SN} est correcte et la tâche d'authentification est un succès. Le nœud capteur définit m = w' et stocke le jeton initial TK^I_{SN} dans le stockage sécurisé du capteur. Ensuite, il peut effectuer l'authentification continue pour chaque transmission de donnée pendant la période d'authentification actuelle T. Sinon, le capteur devra mettre à terme le processus.

III.3.4.3 La phase d'authentification continue

Cette phase d'authentification continue est appliquée à la transmission de données détectées par le nœud capteur à la passerelle après une l'authentification statique valide. Puisque le capteur avait stocké le jeton initial TK^I_{SN}, et la passerelle aussi avait estimé l'énergie minimale BCT_{SN} pour la période d'authentification actuelle T. Après réception des données d'un capteur, la passerelle va effectuer une série d'instruction pour assurer l'authenticité du nœud capteur. La passerelle vérifie d'abord si le message reçu est généré dans la période d'authentification actuelle T. Deuxièmement, la passerelle vérifie la valeur M_5, qui permet d'authentifier les données envoyées, et le reste de la capacité de la batterie rb, s'il est dans une plage raisonnable. Enfin, la passerelle envoie un accusé de réception ACK au nœud du capteur.

La phase d'authentification continue du protocole étudié est selon les étapes suivantes :

1. Nœud capteur ⟶ Passerelle: ID_{SN}, M_5, mb, ms, r_2

Le nœud capteur génère un nombre aléatoire r_2 et obtient la valeur de la capacité énergétique actuelle de la batterie du capteur rb. Ensuite, le nœud capteur obtient le jeton initial TK^I_{SN} de son stockage sécurisé et utilise la capacité énergétique actuelle de la batterie du capteur rb pour calculer $mb = rb \oplus H(TK^I_{SN} \| (m \oplus r_2))$. Ensuite, le nœud capteur utilise le nombre aléatoire m qui avait été généré à la phase de l'authentification statique pour le calcul de $ms = sd \oplus H((TK^I_{SN} \oplus m) \| r_2)$ pour masquer les données collecté sd. Après cela, le nœud capteur calcul $M_5 = HMAC_{TK^I_{SN}}$ (IDSN, ms, mb, r_2. Ensuite, le nœud capteur envoie ID_{SN}, M_5, mb, ms et r_2 à la passerelle.

2. Passerelle ⟶ Nœud capteur: Y_1, ACK

Après avoir reçu ID_{SN}, M_5, mb, ms et r_2 du nœud capteur, la passerelle effectue une série de tâche de vérification. Tout d'abord, la passerelle définit la valeur de l'estampille de temps actuelle (timestamp) comme tc. Ensuite, la passerelle vérifie si le message reçu est généré dans la période d'authentification actuelle T.

Si $((tc - ts) \geq T)$, il indique que le temps tc est hors de portée de la période T. Ce qui veut dire que la transmission de données dépasse le temps préalablement définie. C'est-à-dire que le capteur doit lancer l'authentification statique à nouveau.

Donc la passerelle doit calculer $rb' = mb \oplus H(TK^I_{SN} \| (m \oplus r_2))$, $Y_1 = (m \| TK^I_{SN}) \oplus H((TK^I_{SN} \oplus r2) \| m)$ et $ACK = H(m \oplus rb) \| (rb \oplus r_2) \| (m \| TK^I_{SN})$ pour informer le capteur qu'il doit relancer le processus d'authentification statique. Ensuite, la passerelle envoie ACK et Y1 au capteur.

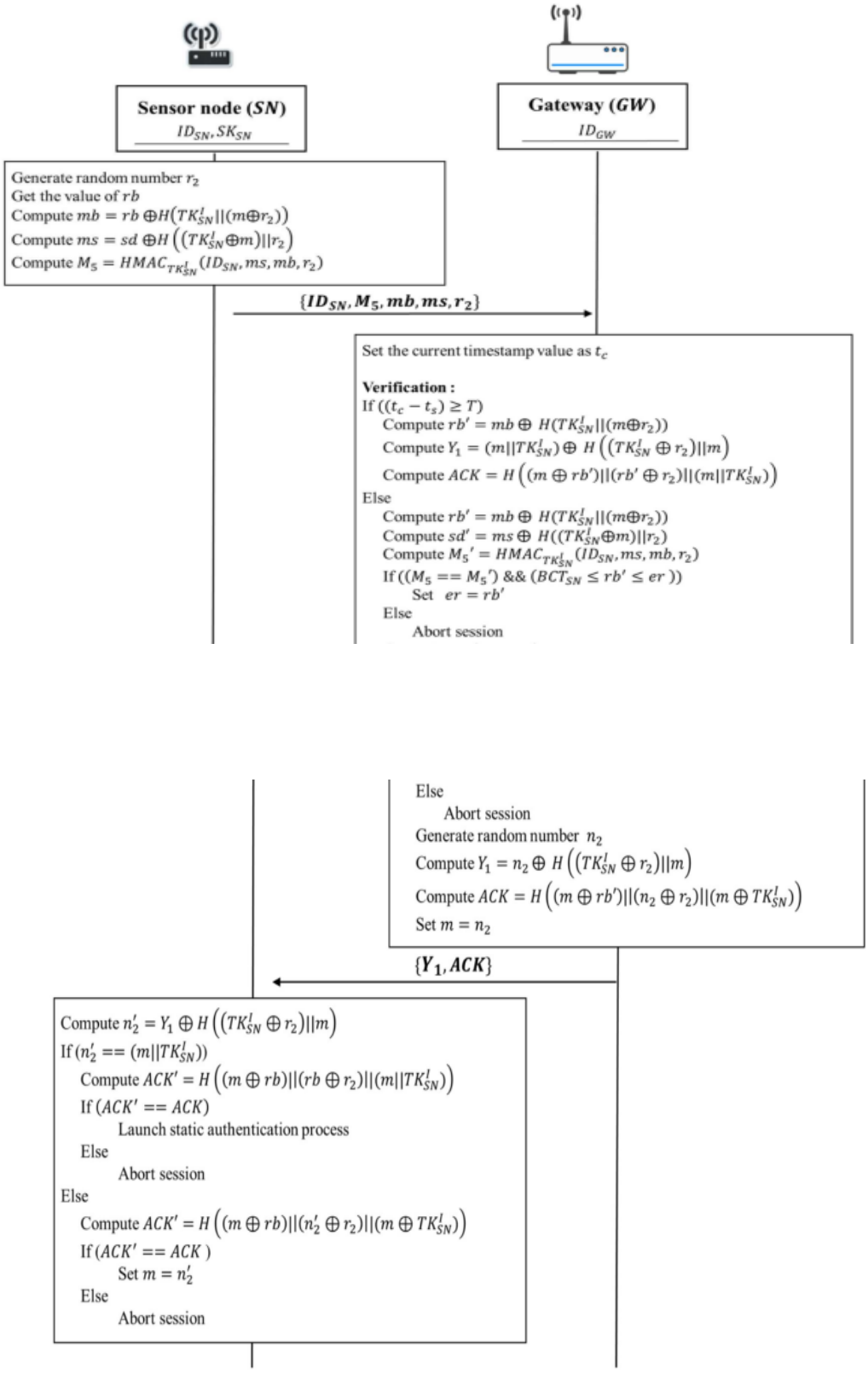


Figure 13: La phase d'authentification continue du protocole étudié

Sinon, après vérification de l'estampille de temps, la passerelle vérifie l'intégrité des données du message pendant les transmissions. Sur la base de l'ID_{SN} reçu, la passerelle reçoit le jeton initial correspondant TK^{I}_{SN} de sa base de données. La passerelle utilise le jeton initial TK^{I}_{SN} pour calculer rb' = mb$\oplus$ H (TK^{I}_{SN} || (m $\oplus$ r_2)), sd' = ms$\oplus$ H (($TK^{I}_{SN}\oplus$ m)|| r_2)) et M'_5 = $HMAC_{TK^{I}_{SN}}$ (ID_{SN}, ms, mb, r_2), respectivement. Ensuite, la passerelle vérifie si la valeur calculée M'_5 est équivalente à la valeur reçue M_5. Si M'_5 et M_5 sont identiques, il indique que le message obtenu n'est pas modifié pendant la transmission. En outre, la passerelle vérifie également si la capacité restante de la batterie rb' est dans un Gamme. Si ($BCT_{SN} \leq rb' \leq er$), il indique que la capacité énergétique actuelle de la batterie du capteur rb' est dans une plage raisonnable et la validité du nœud capteur est authentifiée. Sinon, la passerelle interrompt la session. Une fois les tâches de vérification ci-dessus terminées, le nœud capteur est authentifié avec succès et la passerelle peut s'assurer que les données sd' transmis par le capteur sont valides. La passerelle définit er = rb'. Ensuite, la passerelle génère un nombre aléatoire n_2 pour calculer $Y_1 = n_2 \oplus H((TK^{I}_{SN} \oplus r_2) \| m)$ et ACK = H (m $\oplus$ rb')|| (n2 $\oplus$ r2) || (m $\oplus$ TK^{I}_{SN})) . Après cela, la passerelle définit m = n_2. Enfin, la passerelle envoie un accusé de réception ACK et Y_1 au nœud capteur.

Une fois que le nœud du capteur reçoit Y_1 et ACK, le nœud capteur calcul $n'_2 = Y_1 \oplus H((TK^{I}_{SN} \oplus r_2) \| m)$. Si la valeur de n'_2 est équivalente à (m || TK^{I}_{SN}), cela signifie que ce processus d'authentification continue est expiré, et que le capteur devrait relancer l'authentification statique à nouveau. Avant de lancer l'authentification statique, le capteur doit calculer ACK' = H (m $\oplus$ rb) || (rb $\oplus$ r_2) || (m || TK^{I}_{SN}) pour vérifier l'intégrité des données du message reçu. Si (ACK' == ACK), il indique que le message n'a pas été modifié pendant la transmission des données. Ensuite, le capteur relance le processus d'authentification statique. Sinon, le capteur interrompt la session.

D'autre part, si la valeur de n'_2 n'est pas équivalente à (m || TK^{I}_{SN}), cette l'authentification devrait être couronnée de succès. Afin de vérifier l'intégrité des données du message reçu, le capteur calcule ACK' = H ((m $\oplus$ rb) || ($n'_2 \oplus r_2$) || (m $\oplus$ TK^{I}_{SN})) et le compare avec la valeur reçue d'ACK. Si la valeur d'ACK' est équivalente à ACK, cette authentification continue est réussie. Enfin le nœud capteur définit m = n'_2 et va à la prochaine authentification continue pour chaque transmission de données. Dans le cas contraire, le protocole sera résilié. Ainsi le nœud capteur doit recevoir l'accusé de réception ACK pour indiquer une fin de session gracieuse.

III.3.5 Analyses du Protocole

III.3.5.1 Analyse de la Sécurité

Dans cette partie, une analyse de sécurité est effectuée afin d'évaluer la solidité de la sécurité du protocole étudié[52]. Il existe six propriétés de sécurité prises en charge par la conception du protocole : résistance à l'attaque par répétition, résistance aux attaques d'usurpation d'identité, résistance à l'attaque de l'homme au milieu, intégrité des données, authentification, et le secret avant.

• Résistance aux attaques par répétition: un attaquant malveillant peut écouter des messages valides envoyés lors d'une session d'authentification. Plus tard, l'attaquant rejoue certains de ces messages à usurper l'identité d'une entité légitime pour établir une session authentifiée avec le pair cible. Dans ce protocole, si un attaquant écoute des messages et effectue une attaque par relecture, le récepteur de message (la passerelle ou un capteur) peut détecter que ces messages sont invalides. Dans le protocole étudié, les valeurs M_2, M_4, M_5 et ACK contenant des messages déjà envoyés, sont toutes construit avec de nouveaux nombres aléatoires et chaque valeur sera transmise avec son nombre aléatoire correspondant qui est utilisé comme l'une des variables pour générer dynamiquement la valeur. Ces nombres aléatoires sont fraîchement générés par les deux parties de session d'authentification. Le récepteur de message vérifiera la validité du message reçu pour utiliser le nombre aléatoire reçu pour générer un message provisoire et évaluer l'équivalence entre le message reçu et le message provisoire. Si les deux messages sont équivalents, le récepteur de message détermine que le message reçu est valide. Comme le protocole intègre des nombres aléatoires dans les messages individuels pour garder la fraîcheur des messages, ce protocole est capable de résister à toute attaque par répétition. A noter aussi la notion de temps d'aller-retour d'un message.

• Résistance aux attaques d'usurpation d'identité : une attaque d'usurpation d'identité indique qu'un attaquant malveillant peut essayez de se faire passer pour un nœud capteur valide. Dans la phase d'authentification statique, si un attaquant veut se faire passer pour capteur, l'attaquant devra forger le message $\{ID_{SN}, X, M_1, M_2, mb, r_1\}$ envoyé à la passerelle. Si un attaquant veut forger la valeur M_2, l'attaquant doit apprendre la valeur secrète SK_{SN}. L'attaquant peut connaître l'identité du capteur ID_{SN} à partir de l'écoute de messages, mais il est incapable d'apprendre la valeur secrète SK_{SN}. Sans connaître la valeur secrète SK_{SN}, l'attaquant ne peut pas calculer un M_2 valide. Par conséquent, l'attaque d'usurpation d'identité échouera. Dans la phase d'authentification continue, si un attaquant veut se faire passer pour un nœud capteur valide, l'attaquant devra forger le message $\{ID_{SN}, M_5, mb, ms, r_2\}$ envoyé à la passerelle. Donc l'attaquant doit forger la valeur M_5. En conséquence, l'attaquant doit connaître les jetons TK^I_{SN}, les nombres aléatoires r_2 et m, et la capacité énergétique actuelle de la batterie du capteur rb. L'attaquant peut apprendre les nombres aléatoires r_2 à partir de messages espionnés, mais il ne peut pas apprendre le jeton initial TK^I_{SN} à partir de messages espionnés. Par conséquent, l'attaquant ne peut pas calculer une valeur symbolique initiale valide TK^I_{SN} sans connaître la valeur de la clé secrète SK_{SN}. En résumé, l'attaquant ne peut pas se faire passer pour un nœud capteur valide avec succès. Par conséquent, le protocole peut résister l'attaque d'usurpation d'identité.

• Résistance aux attaques de l'homme au milieu : une attaque de l'homme au milieu indique qu'un attaquant actif relaie et manipule secrètement les messages transmis entre deux parties qui communiquent directement les unes avec les autres. Dans la phase d'authentification statique, si un attaquant veut relayer et manipuler la transmission de messages, l'attaquant doit apprendre la valeur secrète SK_{SN} et la capacité énergétique restante de la batterie du capteur rb. Depuis que l'attaquant ne peut pas connaître la valeur secrète SK_{SN} et la capacité énergétique restante de la batterie du capteur rb à partir des messages précédemment écoutés, l'attaquant ne peut pas apprendre les données authentiques et manipuler les messages avec succès. Dans la phase d'authentification continue, si l'attaquant malveillant veut relayer et manipuler la transmission de messages, l'attaquant doit obtenir le jeton initial TK^I_{SN}. Comme le jeton initial TK^I_{SN} est généré et envoyé en toute sécurité dans la phase d'authentification statique, l'attaquant ne peut pas apprendre le jeton initial TK^I_{SN}. L'attaquant ne peut qu'espionner les valeurs de mb et ms, mais il ne peut toujours pas apprendre les données authentiques rb et sd qui sont soigneusement cachés dans mb et ms. En conséquence, l'attaquant ne peut pas modifier ou manipuler la transmission de messages sans connaître le jeton initial TK^I_{SN}. Ainsi, le protocole peut résister aux attaques de l'homme au milieu.

• Intégrité des données : l'intégrité des données indique qu'un récepteur de message peut s'assurer que le message n'est pas trafiqué pendant la transmission. Ce protocole adopte une fonction HMAC pour assurer l'intégrité les données. Dans la phase d'authentification statique, si un attaquant tente de falsifier les messages, l'attaquant doit apprendre la valeur secrète SK_{SN}.

Puisque l'attaquant ne peut pas apprendre la secrète valeur SK_{SN} des messages espionnés, il ne peut pas calculer les valeurs valides de M_2 et M_4. Par conséquent, un attaquant malveillant ne peut pas falsifier les messages de transmission. Dans la phase d'authentification continue, si un attaquant tente de trafiquer la transmission de données, l'attaquant doit apprendre le jeton initial TK^I_{SN}. Comme l'attaquant ne peut pas apprendre le jeton TK^I_{SN} à partir de messages espionnés, il ne peut pas calculer une valeur valide M_5 sans savoir le jeton initial TK^I_{SN}. Par conséquent, le protocole étudié atteint la propriété d'intégrité des données.

• Authentification mutuelle : L'authentification mutuelle indique que deux entités peuvent s'authentifier entre elles. Dans la phase d'authentification statique, la passerelle authentifie le nœud capteur en vérifiant la valeur M_2 avec la valeur secrète partagée SK_{SN}. Si la valeur calculée M'_2 équivaut à la valeur reçue M_2, la passerelle sera en mesure d'assurer la validité du nœud du capteur. Ensuite, le nœud du capteur authentifie également la passerelle en vérifiant la valeur M_4 avec la valeur secrète SK_{SN}. La valeur M_4 intègre les nombres aléatoires r_1 et n_1. Si la valeur calculée M'_4 est équivalente à la valeur reçue M_4, le nœud capteur assure la validité de la passerelle.

Dans la phase d'authentification continue, le capteur et la passerelle peuvent s'authentifier via le jeton initial TK^I_{SN} et des nombres aléatoires. Tout d'abord, la passerelle authentifie le nœud capteur en vérifiant la valeur de M_5 qui est crypté avec le jeton initial TK^I_{SN}. Si la valeur de M'_5 est équivalente à M_5, la passerelle garantit que le nœud capteur est valide. Ensuite, le capteur authentifie la passerelle en vérifiant la valeur de ACK qui est composée de TK^I_{SN} et des nombres aléatoires n_2 et r_2. Par conséquent, le protocole proposé appuie authentification mutuelle entre un nœud capteur et la passerelle.

• Secret avant : L'objectif du secret avant est de protéger les clés de session générées dans le passé contre compromis des clés de session générées à l'avenir. Si le jeton initial TK^I_{SN} est

appris par un attaquant qui veut tirer le jeton initial $H(v \oplus w \oplus SK_{SN})$ utilisé dans la session précédente, l'attaquant doit connaître les nombres aléatoires précédemment générés v et w. Les nombres aléatoires v et w ont été générés par le nœud capteur et la passerelle dans la session d'authentification précédente. Étant donné que l'attaquant ne peut pas obtenir les nombres aléatoires précédemment générés v et w ni les messages espions précédents, par conséquent, l'attaquant ne peut pas utiliser le jeton initial actuel TK^{I}_{SN} pour dériver le jeton initial précédant. Par conséquent, le protocole étudié atteint la propriété du secret avant.

III.3.5.2 Analyse du Rendement

Comme nous l'avons mentionné dans ce chapitre, dans la partie Authentification continue, les auteurs n'ont pas trouvé d'autres protocoles d'authentification à comparer avec le protocole dans[52]. Par conséquent, ils ont prévu de trouver un protocole d'authentification utilisateur-appareil traditionnel à comparer avec leur protocole. Dans cette sous-section, nous comparons le protocole dans[52] avec le protocole de Khemissa et all.[29] et d'autres protocoles en termes de performance. La raison de la sélection du protocole dans[29] à comparer avec le protocole dans[52] est que celui dans[29] est un protocole d'authentification presque léger. Par conséquent, son coût de calcul est déjà inférieur à celui des autres protocoles d'authentification existants que nous avons étudiés à la section 2 de ce chapitre. Depuis la consommation de temps de l'exécution d'une opération de concaténation et le ou-exclusif est beaucoup moins que les autres opérations informatiques, nous ignorons la consommation de temps générée par ces deux opérations lors du calcul du coût d'opération dans ce protocole. Comme les nœuds capteurs sont des équipements avec des ressources informatiques limitées et que les passerelles ont une ressource informatique suffisante, nous nous concentrons par la suite sur la comparaison de la consommation de temps du processus d'authentification du côté nœud capteur entre les protocoles ciblés.

Le Tableau 3 montre le résultat de comparaison du coût de calcul entre le protocole de Khemissa et al.[29], des autres protocoles d'authentification existants que nous avons étudiés à la section 2 de ce chapitre et du protocole étudié[52]. Dans la phase d'authentification statique, le protocole étudié exige $4T_{Random} + 16T_{Hash} + 4T_{HMAC}$ .Les longueurs d'ID_{SN}, de nombres aléatoires (r_1, r_2, n_1, n_2, v, w) et de SK_{SN} sont toutes 128 bits.

	Phases	Hash	HMAC	S-key encrypt	P-key encrypt	Rand. No. gen.
Protocol studied[52]	Stat Auth	16	4			4
	Cont Auth	8	2			2
Khemissa et al.[29]	authentication phase	2	4			2
	key establishment phase			K*2 AES		-
IoT-Ellipic Curve 2012[53]	Init	1		Comm. Crypté	4 ECC	2
	Verif	1			2 ECC	1
Command & control-RSA 2014[54]	gen. Sig	1			1	2 (key gen)
	Verif Sig	k			1	-
RFID-Elliptic Curve 2013[30]	Reader	3			5 ECC	3

	Tag	-			1	-

Tableau 3: Comparaison du protocole étudié, celui de Khemissa et al. Et des travaux connexes

D'après le travail dans[50], la consommation de temps de l'opération de cryptage AES (T_{AES}) est environ 2,76 ms, la consommation de temps de l'opération de hachage (THash) est d'environ 1,5 ms et la consommation de temps de l'opération HMAC (T_{HMAC}) est d'environ 3,54 ms. L'opération de génération de nombre aléatoire est approximativement 0.65 ms comme montré dans[51].

En résumé, le coût de calcul de la phase d'authentification statique du protocole dans[52] est d'environ 40,76 ms alors que le coût de calcul du protocole dans[29] ne prend que 23,98 ms. Cependant le coût de calcul de la phase d'authentification continue du protocole étudié[52] est d'environ 18.34~20.38 ms. Notons que le coût de calcul du protocole dans[29] ne compte que pour la génération de clés de session authentifiée. Il y aura un coût de calcul supplémentaire lorsque les deux parties commencent à chiffrer leurs messages transmis à l'aide de la clé de session convenue. En revanche, ce protocole ne génère que le jeton initial convenu par le capteur et la passerelle dans la phase d'authentification statique. Au cours de la phase d'authentification continue, les données, le jeton initial et d'autres valeurs de contrôle temporaires sont transmis du capteur à la passerelle. Par conséquent, ce protocole étudié propose de meilleures performances sur l'authentification continue en termes de coût de calcul.

Conclusion

Dans ce chapitre, nous avons fait un état de l'art sur les protocoles d'authentification pour les IoTs, en plus nous nous sommes focaliser sur le protocole dans[52], qui est à la base de notre contribution. Cela nous a permis de découvrir les multiples protocoles qui interviennent dans le domaine de l'IdO. Ainsi nous les avons regroupés par catégories pour mieux faire la différence entre eux. Nous avons aussi découvert que beaucoup de mécanisme de sécurité ont été proposé sur la base de la cryptographie, soit à clé publique ou privé. Ces solutions surmontent les défis de sécurité mais ils nécessitent un grand coût de calcul et de consommation d'énergie. Ce qui les rendent insuffisantes dans le contexte des Iots. D'où l'adoption d'une authentification continue pour surmonter les défis de sécurité tout en minimisant la consommation d'énergie. Ces défis sont bien pris en compte dans le protocole étudié[52], car il n'utilise aucune opération cryptographique, de plus il a l'avantage de ne pas conserver des informations sensibles, à la différence des authentifications via le visage ou les empreintes digitales et rétiniennes[37-41], ce qui lui donne un aspect particulièrement intéressant à l'heure où le respect de la vie privée et des données personnelles est devenu un enjeu sociétal. Dans le chapitre qui suit, consacré à notre contribution, nous présentons les problématiques et les solutions proposées pour l'optimisation du protocole dans[52].

Chapitre 4

Optimisation du Protocole d'authentification continue de Yo-Hsuan chuang et all.[52]

Introduction

Dans ce chapitre, nous passons en revue le protocole d'authentification de Yo Hsuan Chuang et all.[52] en vue de l'optimiser. Dans leurs perspectives, les auteurs avaient souligné et mis en relief l'initialisation d'une requête d'authentification par la passerelle. Et cela permettrait à la Gateway de pouvoir interroger les capteurs sans attendre une initialisation venant de ces derniers. Ainsi, ils ont proposé une solution qui modifie la phase d'authentification statique, dans laquelle la Gateway initialise une requête. Les deux solutions réunies, permettent aussi bien aux capteurs qu'à la Gateway d'initialiser une authentification. Dans une logique d'optimisation de cette solution globale, nous avons amélioré la phase d'authentification continue en vue de l'adapter aux besoins des applications basées sur les requêtes. Notre solution proposée, en plus de garder tous les avantages de celles proposées par les auteurs, réduit le nombre d'opération qui impacte la consommation énergétique. Dans la suite de ce chapitre, nous passons d'abord en revue les deux solutions des auteurs, ensuite nous présentons notre méthode d'optimisation et enfin nous analysons ses performances en termes d'opérations.

1. Présentation du Protocole étudié

Le protocole de Yo- Hsuan Chuang et all.[52] est un protocole d'authentification continues léger et favorable pour les applications IoTs notamment dans le domaine de E-Santé. Elle comprend trois phases : une phase d'initialisation pour l'échange des informations secrètes entre un capteur et une passerelle et de deux d'authentifications dont une Statique et une autre dite Continue (Authentification des données). Dans la phase d'authentification statique (voir Figure 12) les deux parties communicantes sont authentifiées avant de pouvoir se partager des données. D'autre part l'authentification continue (voir Figure 13) qui est un service complémentaire à l'authentification statique car permettant de garantir que l'expéditeur qui a été authentifié au début d'une session de transmission est le même tout au long de cette session. Ainsi la notion de continuité est liée à l'établissement d'un canal de transmission sécurisé pour une période de temps défini par la passerelle. Dans leur article ils ont proposé deux solutions, une première qui part d'une initialisation uniquement par les capteurs et une autre proposition complémentaire pour permettre aux différentes passerelles d'avoir la possibilité d'initialiser une communication, mais celle-ci laisse intacte la phase d'authentification continue.

2. Problématique du Protocole

Tout comme dans les réseaux sans fil traditionnels, l'authentification des parties communicantes dans l'internet des objets ne cessent d'attirer l'attention de beaucoup de chercheurs. Pour une variété de solutions d'authentification proposées, garantir une utilisation dans tout type d'application IoT tout en tenant en compte le coût en énergie et en capacité de stockage des nœuds capteur reste un véritable défi.

IV.2.1 Non-conformité avec d'autres types d'applications

Dans le scenario du protocole de Yo- Hsuan Chuang et all.[52] les nœuds capteurs collectent des informations et les transmettent à la passerelle après une authentification statique réussie. Dans ce cas de figure la passerelle ne pourra pas gérer les évènements du nœud capteur car ce dernier fera des demandes d'authentification au besoin, ce qui sera un inconvénient pour les applications basé sur les requêtes où les capteurs doivent répondre à une interrogation de la station de base. Ainsi notre contribution à ce travail va dans le sens d'une modification partielle du protocole étudié pour permettre aux différentes passerelles d'envoyer activement des demandes d'authentification à un nœud pour soutenir ces types d'applications dans le contexte de l'internet des objets.

IV.2.2 Le coût en ressource très élevé

Dans la phase d'authentification continue nous constatons que le processus d'initialisation d'une nouvelle authentification statique, après le laps de temps choisi par la passerelle, peux se faire de façon continue et nécessite un certain nombre d'opérations avant de lancer cette nouvelle authentification ; ce qui nuit aux capteurs qui vont continuellement envoyer des messages à la passerelle. Etant donné que ces appareils sont limités en termes de stockage et d'énergie, une authentification répétée leur contraint à réaliser beaucoup d'opérations et à stocker plus de données dans leur mémoire flash. Notre solution permettra d'optimiser la consommation d'énergie et le temps d'exécution, réduire sans pour autant compromettre à la sécurité le nombre d'opération au niveau des nœuds capteurs.

3. Présentation de notre Contribution

Dans cette partie, nous décrivons dans un premier temps, les améliorations qu'on a apportées au protocole de Yo- Hsuan Chuang et all.[52] . Ces améliorations sont de deux ordres. Il s'agit d'une part d'optimiser les consommations d'énergies induites par les opérations en équilibrant les temps de calcul et la taille des données à hacher tout en gardant les propriétés de sécurités et d'autre part rendre ce protocole plus flexible à tout type d'application comme celles basés sur les requêtes. Dans un second temps nous apportons une analyse de toutes ces contributions. Les hypothèses, équations de consommation de la batterie ainsi que les étapes de la phase d'initialisation du protocole dans[52] sont maintenus dans notre contribution.

IV.3.1 Flexibilité de la Solution

L'initialisation des communications à partir de la passerelle va rendre notre solution plus flexible dans la mesure où les modèles d'application basés sur les requêtes pourront utiliser ce protocole tout en gardant les propriétés de sécurité. Dans le protocole étudié nous nous sommes

rendu compte que les capteurs peuvent initier les communications de façon continue car après chaque commit, le nœud peux envoyer une nouvelle demande qui sera sans doute validée par la passerelle ce qui n'est pas du tout favorable pour les applications qui interrogent le capteur seulement en cas de besoin, en plus de cela le capteur n'aura pas à faire des opérations supplémentaires avant de relancer une nouvelle demande d'authentification statique. Ce qui nous a motivés à proposer cette nouvelle solution pour soutenir ces types d'application.

IV.3.2 Présentation de la Solution

La solution proposée permet de réduire le nombre d'authentifications côté nœuds capteur qui sont des appareils très limités en termes d'énergie et en capacité de stockage. De plus nous allons soutenir les modèles d'applications événementielles ou à base de requêtes pour partir d'une demande d'initialisation de la passerelle.

IV.3.2.1 La phase d'authentification statique

La phase d'authentification statique de l'extension du protocole proposé pour appuyer la demande de l'initialisation est selon les étapes suivantes :

1. Passerelle ⟶ Nœud capteur: M_0, n_1

Dans la phase d'authentification statique, la passerelle génère un nombre aléatoire n_1 et va calculer $M_0 = HMAC_{SK_{SN}}(ID_{SN} \| n_1)$ en premier. Ensuite, la passerelle envoie n_1 et M_0 comme une demande à la cible nœud capteur pour demander des données détectées. Après la réception de n_1 et M_0 par le nœud du capteur, il utilise ensuite l'identité du nœud du capteur ID_{SN} qu'il avait stocké dans sa base de donné durant la phase d'initialisation pour calculer $M'_0 = HMAC_{SK_{SN}}(ID_{SN} \| n_1)$. Après ce calcule il teste si la valeur calculée M'_0 et la valeur reçue M_0 sont équivalente, si c'est le cas le nœud capteur assure l'authenticité de la passerelle et poursuit les phases de l'authentification statique, sinon il interrompt la session.

2. Nœud capteur ⟶ Passerelle: ID_{SN}, X, M_1, M_2, mb

Un nœud capteur génère un nombre aléatoire v. Ensuite, il obtient la valeur de la capacité énergétique actuelle de la batterie du capteur qui est rb et obtient sa valeur secrète SK_{SN} de son stockage sécurisé. Ensuite, il cache les données de la capacité énergétique actuelle de la batterie du capteur rb dans mb avec l'opérateur du ou-exclusif ce qui donne le résultat : $mb = rb \oplus v$. Après cela, le nœud du capteur calcule $X = \upsilon \oplus H(n_1)$ et $M_1 = H((rb \| ID_{SN}) \oplus H(SK_{SN}))$, respectivement.

Par la suite, le capteur utilise la valeur secrète SK_{SN} pour calculer $M_2 = HMAC_{SK_{SN}}(ID_{SN}, X, M_1, mb)$ afin de garantir que le message ne sera pas modifié pendant la transmission des données. Enfin, le nœud du capteur envoie ID_{SN}, X, M_1, M_2 et mb à la passerelle. Lors de la réception d'ID_{SN}, X, M_1, M_2 et mb à partir du nœud du capteur, la passerelle utilise l'identité d'un nœud capteur ID_{SN} pour récupérer la valeur secrète correspondante SK_{SN} de sa base de

données. La passerelle utilise ensuite cette valeur secrète SK_{SN} pour calculer M'_2= $HMAC_{SK_{SN}}$ (ID_{SN}, X, M_1, mb). Après cela, la passerelle vérifie si la valeur calculée M'_2 est équivalente à la valeur reçue M_2. Si M'_2 et M_2 sont équivalent, il indique que les messages obtenus ne sont pas modifiés par tout attaquant malveillant et permet également de garantir l'authentification mutuelle entre les deux entités. Ce calcul de M_2 permet aussi de garantir l'authentification entre le nœud capteur et la passerelle puise qu'ils partagent une clé que seule ces deux entités détiennent. Dans le cas contraire, la passerelle mettra fin au protocole.

Ensuite, la passerelle va calculer $v' = X \oplus H(n_1)$ et utilise la valeur de υ' pour calculer $rb' = mb \oplus \upsilon'$. Après la récupération de rb' et υ', la passerelle prend la valeur de rb' pour calculer $M_1' = H(rb' \| ID_{SN}) \oplus H(SK_{SN})$). Ensuite, la passerelle vérifie si la valeur calculée M'_1 est équivalente à la valeur reçue M1. Si M'_1 et M_1 sont équivalents, cela indique que les valeurs obtenues de υ' et rb' sont correctes. Sinon la passerelle mettra également fin au protocole. Le calcul de M_1 permet de garantir l'intégrité des données reçu du nœud capteur. Une fois les tâches de vérification ci-dessus terminées, la passerelle reprend le même procédé que dans le protocole étudié sans altérer aucune propriété de sécurité. Ensuite elle envoie au nœud capteur M_3, M_4 et Y pour que le capteur effectue les opérations de vérification avant de pouvoir envoyer les données collectées à la passerelle selon le délai défini. Ce que nous avons illustré dans la Figure 14

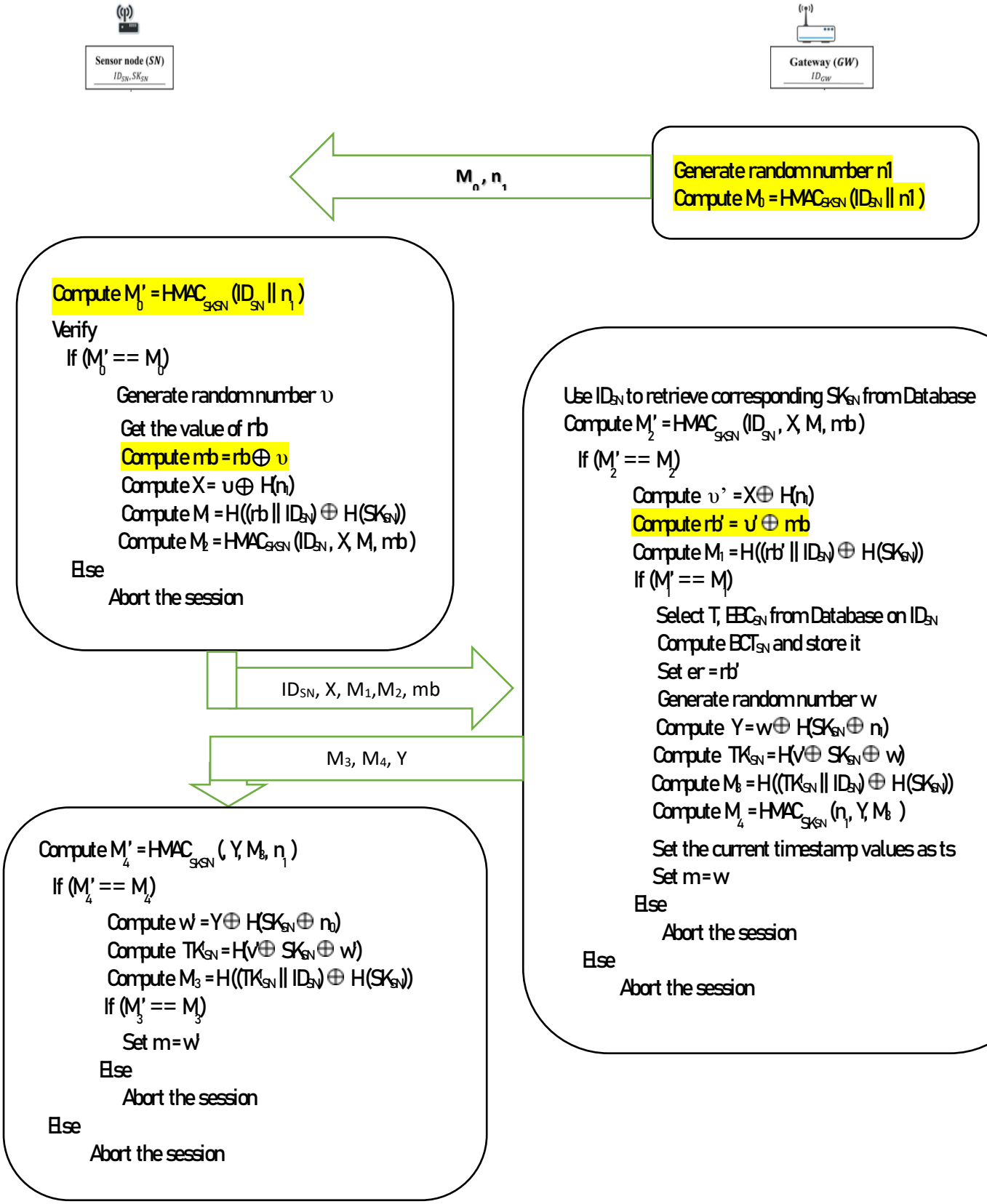


Figure 14: Phase d'authentification Statique de notre proposition

IV.3.2.2 Phase d'authentification Continue

L'authentification continue est appliquée à la transmission de données recueillis du nœud capteur à la passerelle après que l'authentification statique entre eux eut été initiée par la passerelle au cours de l'actuelle période T. Puisque l'authentification continue se produit après une authentification statique réussie, le nœud capteur a stocké le jeton initial TK^{I}_{SN}, et la passerelle a estimé le seuil de capacité de la batterie restante BCT_{SN} pour la période d'authentification actuelle T. Après réception des données d'un nœud de capteur, la passerelle effectue une série de tâches de vérification pour assurer l'authenticité d'un nœud capteur. Tout d'abord, la passerelle vérifie si le message reçu est généré dans la période d'authentification actuelle T, pour éviter l'attaque par rejet ou l'attaque de l'homme du milieu. Deuxièmement, la passerelle vérifie la valeur M_5 qui indique l'intégrité des données du message et le reste de la capacité de la batterie rb est dans une plage raisonnable. Enfin, la passerelle envoie un accusé de réception ACK au nœud du capteur.

La phase d'authentification continue de notre protocole proposé est selon les étapes suivantes :

Nœud capteur ⟶ Passerelle: ID_{SN}, M_5, mb, ms, r_2

Le nœud capteur génère un nombre aléatoire r_2 et obtient la valeur de la capacité énergétique actuelle de la batterie du capteur rb. Ensuite, le nœud capteur obtient le jeton initial TK^{I}_{SN} de son stockage sécurisé et utilise la capacité énergétique actuelle de la batterie du capteur rb pour calculer $mb = rb \oplus H(TK^{I}_{SN} \| (m \oplus r_2))$. Ensuite, le nœud du capteur utilise le nombre aléatoire m qui avait été généré à la phase de l'authentification statique pour le calcul de $ms = sd \oplus H((TK^{I}_{SN} \oplus m) \| r_2)$ pour masquer les données sd. Après cela, le nœud capteur va calculer $M_5 = HMAC_{TK^{I}_{SN}}(ID_{SN}, ms, mb, r_2)$ afin de détecter toute modification pendant la transmission des données et assurer son authenticité. Ensuite, le capteur envoie ID_{SN}, M_5, mb, ms et r_2 à la passerelle.

Passerelle ⟶ Nœud capteur: Y_1, ACK

Après avoir reçu ID_{SN}, M_5, mb, ms et r_2 du nœud capteur, la passerelle effectue une série des tâches de vérification. Tout d'abord, la passerelle définit la valeur de l'estampille de temps actuelle (timestamp) comme tc. Ensuite, la passerelle vérifie si le message reçu est généré dans la période d'authentification actuelle T.

Si $((tc - ts) \geq T)$, il indique que le temps tc, qui indique la période de réception du message, est hors de portée de la période T. Ce qui veut dire que la transmission de données dépasse le temps préalablement défini. C'est-à-dire, le capteur doit attendre que la passerelle initialise une nouvelle demande d'authentification statique. Ainsi la session est interrompue par la GW.

Après vérification de l'estampille de temps, la passerelle vérifie l'intégrité des données du message pendant les transmissions de données. Sur la base de l'ID_{SN} reçu, la passerelle reçoit le jeton initial correspondant TK^{I}_{SN} de sa base de données.

La passerelle utilise le jeton initial TK^{I}_{SN} pour calculer rb' = mb$\oplus$ H (TK^{I}_{SN} || (m$\oplus$ r_2)), sd' = ms$\oplus$ H (($TK^{I}_{SN}\oplus$ m)|| r_2)) et M'_5 = $HMAC_{TK^{I}_{SN}}$ (ID_{SN}, ms, mb, r_2), respectivement. Ensuite, la passerelle vérifie si la valeur calculée M'_5 est équivalente à la valeur reçue M_5. Si M'_5 et M_5 sont équivalentes, il indique que le message obtenu n'est pas modifié pendant la transmission. En outre, la passerelle vérifie également si la capacité restante de la batterie rb' est dans le Gamme, si ($BCT_{SN} \leq rb' \leq er$), il indique que la capacité énergétique actuelle de la batterie du capteur rb' est dans une plage raisonnable et la validité du nœud du capteur est authentifiée. Sinon, la passerelle interrompt la session. Une fois les tâches de vérification ci-dessus terminées, le nœud du capteur est authentifié avec succès et la passerelle peut s'assurer que les données reçues proviennent du capteur. La passerelle définit ensuite er = rb', génère un nombre aléatoire n_2 pour calculer $Y_1 = n_2 \oplus H((TK^{I}_{SN} \oplus r_2) \| m)$ et $ACK = H (m \oplus rb')\| (n_2 \oplus r_2) \| (m \oplus TK^{I}_{SN}))$. Après cela, la passerelle définit $m = n_2$ et enfin, la passerelle envoie un accusé de réception ACK et Y_1 au nœud capteur.

Une fois que le nœud capteur reçoit Y_1 et ACK, il est sûr que les données ont été envoyées dans une estampille de temps raisonnable, l'authentification devrait être couronnée de succès. Il va d'abord récupérer la valeur de n_2, en calculant $n'_2 = Y_1 \oplus H((TK^{I}_{SN} \oplus r_2) \| m)$. Afin de vérifier l'intégrité des données du message reçu, le capteur va calculer $ACK' = H ((m \oplus rb) \| (n'_2 \oplus r_2) \| (m \oplus TK^{I}_{SN}))$ à comparer avec la valeur reçue d'ACK. Si la valeur d'ACK' est équivalente à ACK, cette authentification continue est réussie. Enfin le nœud capteur définit $m = n'_2$ et va à la prochaine authentification continue pour chaque transmission de données. Comme dans l'authentification statique, la réception de ACK et Y_1 permettra au nœud capteur de poursuivre la transmission de données détectées.

D'autre part, il va attendre la prochaine demande de la GW pour relancer une nouvelle demande d'authentification statique. Ce que nous avons illustré dans la Figure 15

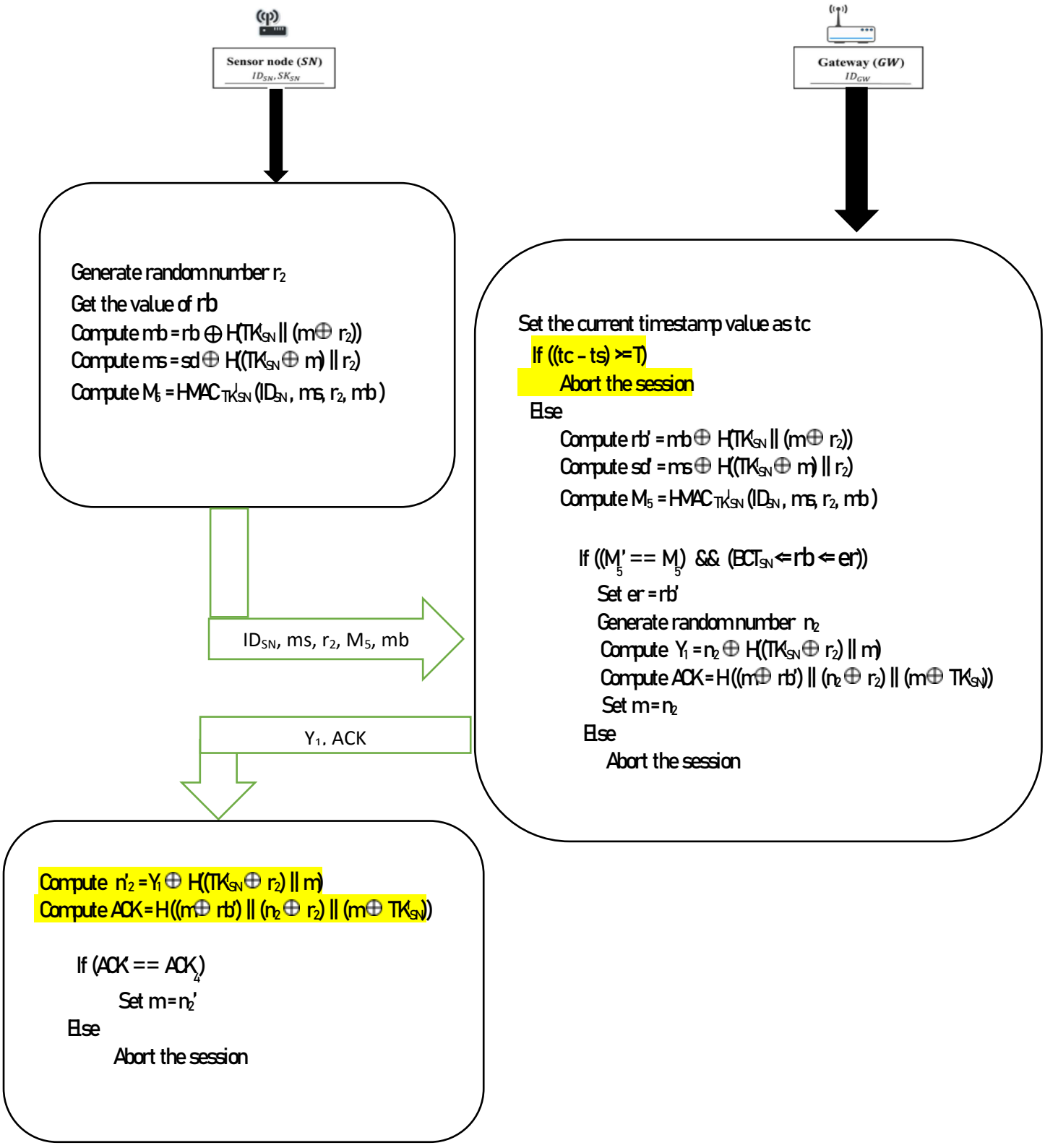


Figure 15: La phase d'authentification Continue de notre Proposition

IV.3.3 Analyse des Performances

Dans la partie analyse de sécurité de notre proposition, toutes les propriétés de sécurité ont été gardées. Aucun service de sécurité n'a été altéré. Nous définissons les notations suivantes pour indiquer la consommation de temps pour les différentes opérations informatiques :

1. T_{Hash}: Le temps consommé pour exécuter une fonction de hachage
2. T_{AES}: Le temps consommé pour l'exécution d'une opération AES
3. T_{HMAC} : Le temps consommé pour exécuter une opération HMAC
4. T_{Random}: Le temps consommé pour générer un nombre aléatoire.

Le Tableau 4 montre le résultat de comparaison du nombre d'opération entre le protocole de Khemissa et al.[18] , le protocole étudié[52] et notre proposition. D'après le travail de[50], la consommation de temps de l'opération de cryptage AES (T_{AES}) est d'environ 2,76 ms, la consommation de temps de l'opération de hachage THash est d'environ 1,5 ms et la consommation de temps de l'opération HMAC (T_{HMAC}) est d'environ 3,54 ms. Un pseudorandom l'opération de génération de nombre est approximativement 0.65 ms comme montré dans[43]. Dans la phase d'authentification statique, notre proposition exige $4T_{Random} + 14T_{Hash} + 6T_{HMAC}$ tandis que le protocole étudié a besoin de $4T_{Random} + 16T_{Hash} + 4T_{HMAC}$. Dans notre solution, les longueurs d'ID_{SN}, de nombres aléatoires (n1, n2, v, w) et de SK_{SN} sont toutes 128 bits.

Phases	Khemissa et al.	Protocole Etudié	Extension du Protocole étudié
Authentification Statique	$2\ T_{Random} + 2\ T_{Hash} + 4\ T_{HMAC} + 2T_{AES}$	$4T_{Random} + 16T_{Hash} + 4T_{HMAC}$	$3T_{Random} + 14_{THash} + 6T_{HMAC}$
Authentification Continue	---	Condition (1) : $2T_{Random} + 9T_{Hash} + 1T_{HMAC}$	Condition (1) : $1T_{Random} + 2T_{Hash} + 1T_{HMAC}$
		Condition (2) : $2T_{Random} + 8T_{Hash} + 2T_{HMAC}$	Condition (2) : $2T_{Random} + 8T_{Hash} + 2T_{HMAC}$

Tableau 4: Tableau Comparatif des deux protocoles et de notre proposition

Conclusion

En conclusion, le coût de calcul de la phase d'authentification statique de l'extension du protocole que nous avons proposé est d'environ 44,19 ms alors que le coût de calcul du protocole étudié prend 40,76 ms. Cependant le coût de calcul de la phase d'authentification continue du protocole étudié est d'environ 18.34~20.38 ms, tandis que dans la phase d'authentification continue de notre extension du protocole le cout de calcul est d'environ 7.19 ~ 20.38 ms. Notons que le coût de calcul du protocole étudié[52] est inférieure à celui du protocole proposé de 3.43 ms , pour la phase d'authentification statique, car dans ce scénario les communications sont initiés par un nœud capteur, donc il ne prend pas en compte les opérations faites lors de la phase de l'initialisation du protocole par la passerelle. Il y aura un coût de calcul supplémentaire lorsque les deux parties pourront initier des authentifications statiques réciproquement. Notons aussi que la taille des données à chiffrer est considérablement compressée et que le délai de temps pour la transmission des données pourra être aussi plus réduit. Par conséquent, notre proposition à moins de performances sur l'authentification statique en termes de coût de calcul, par contre elle présente une meilleure performance dans la phase d'authentification continue où le temps de calcul est réduit de 11.15 ms dans la première condition. En résumé, cette extension du protocole est très concurrentielle en termes d'efficacité de performance.

Conclusion Générale

L'Internet a connu une mutation de l'Internet classique vers l'Internet des objets d'où la possibilité de fusionner parfaitement le monde réel et le monde virtuel, grâce au déploiement massif de périphériques intégrés et intelligents, s'ouvre de nouvelles orientations intéressantes pour la recherche dans plusieurs domaines d'applications liés à la sécurité routière, la santé, la surveillance en usine, etc. Les protocoles d'authentification sont déterminants dans la sécurité des IoTs. En plus de l'authentification de l'origine des données, ils permettent de contrôler l'accès au réseau et peuvent faire face aux attaques de type DoS. C'est pourquoi l'étude des travaux existants nous a permis de mieux comprendre leur principe de fonctionnement, les avantages et les inconvénients qui leurs sont liés. Une étude approfondie sur les protocoles d'authentification nous a permis de connaître leurs avantages liés surtout à la sécurité, mais aussi nous avons pu souligner des insuffisances relatives à l'économie d'énergie pour les protocoles d'authentification statique. Afin de contribuer à cette économie d'énergie, qui est peut être conséquente sur la durée de vie du réseau et sur la sécurité du canal de transmission, nous avons proposé une extension d'un protocole d'authentification continue dans le but de réduire le nombre d'opération, surtout au niveau des capteurs, pour l'économie d'énergie notamment dans le contexte des applications basées sur des requêtes. . En effet, Il permet une adaptation à l'application basée sur les requêtes par une initialisation des communications par la passerelle, et une économie d'énergie dans la phase de transmission des données (authentification continue) dues à une réduction du nombre d'opération. Le projet d'étendre ce protocole pour l'option de mise en œuvre d'une demande initialisation de la passerelle a été un prolongement très intéressant surtout dans le domaine de l'E-Santé, où la plupart des authentifications sont initiées par la passerelle.

Pour tester son efficacité, nous avons pu démontrer à travers une étude théorique et une analyse des performances basés sur une ´évaluation du nombre d'opération, que notre proposition justifie d'une meilleure performance. En plus, notre idée d'initialiser les requêtes par la passerelle permet de réduire la durée de transmission et d'économiser de l'énergie en faveur des nœuds qui sont très limités en ressource énergétique. Ainsi, inventer un modèle plus précis de consommation d'énergie des batteries et découvrir plus les caractéristiques dynamiques de l'appareil sont deux défis pratiques et intéressants pour les chercheurs.

En perspectives, nos travaux futurs vont dans le sens de faire une implémentation matérielle ou une simulation afin d'évaluer en pratique et de comparer notre technique. Nous projetons également de concevoir des algorithmes pour améliorer la performance en termes de consommation d'énergie. Nous pensons qu'une étude comparative des mécanismes de calcul dans les IoTs nous permettra encore d'améliorer notre proposition.

Table des Matières

Bibliographie

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

[3] 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.

[4] 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.

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

[6] 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.

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

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

[9] 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.

[10] 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.

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

[12] 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.

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

[14] Mahalle, P.N.; Prasad, N.R.; Prasad, R. Threshold Cryptography-based Group Authentication (TCGA) Scheme for the Internet of Things (IoT). In Proceedings of the 2014 4th International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE), Aalborg, Denmark, 11–14 May 2014; pp. 1–5.

[15] 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.

[16] 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.

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

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

[19] Traore, I.; Woungang, I.; Nakkabi, Y.; Obaidat, M.S.; Ahmed, A.A.E.; Khalilian, B. Dynamic Sample Size Detection in Learning Command Line Sequence for Continuous Authentication. IEEE Trans. Syst. Man Cybern. 2012, 42, 1343–1356. [CrossRef] [PubMed]

[20] Mondal, S.; Bours, P. Continuous Authentication in a Real World Settings. In Proceedings of the 2015 Eighth International Conference on Advances in Pattern Recognition (ICAPR), Kolkata, India, 4–7 January 2015; pp. 1–6.

[21] Buduru, A.B.; Yau, S.S. An Effective Approach to Continuous User Authentication for Touch Screen Smart Devices. In Proceedings of the 2015 IEEE International Conference on Software Quality, Reliability and Security (QRS), Vancouver, BC, Canada, 3–5 August 2015; pp. 219–226.

[22] Mondal, S.; Bours, P. Continuous Authentication and Identification for Mobile Devices: Combining Security and Forensics. In Proceedings of the 2015 IEEE International Workshop on Information Forensics and Security (WIFS), Rome, Italy, 16–19 November 2015; pp. 1–6.

[23] Rescorla, E.; Modadugu, N. Datagram Transport Layer Security Version 1.2. RFC 6347, Internet Engineering Task Force (IETF). 2012. Available online: https://www.rfc-editor.org/rfc/rfc6347.txt (accessed on 26 July 2017).

[24] Kothmayr, T.; Schmitt, C.; Hu, W.; Brünig, M.; Carle, G. DTLS Based Security and Two-way Authentication for the Internet of Things. Ad Hoc Netw. 2013, 11, 2710–2723. [CrossRef]

[25] Porambage, P.; Schmitt, C.; Kumar, P.; Gurtov, A.; Ylianttila, M. Two-phase Authentication Protocol for Wireless Sensor Networks in Distributed IoT Applications. In Proceedings of the 2014 IEEE Wireless Communications and Networking Conference (WCNC), Istanbul, Turkey, 6–9 April 2014; pp. 2728–2733.

[26] Alqassem, I.; Svetinovic, D. A Taxonomy of Security and Privacy Requirements for the Internet of Things (IoT). In Proceedings of the 2014 IEEE International Conference on Industrial Engineering and Engineering Management, Bandar Sunway, Malaysia, 9–12 December 2014; pp. 1244–1248.

[27] Goh, E.J. Encryption Schemes from Bilinear Maps. Ph.D. Thesis, Stanford University, Stanford, CA, USA, 2007.

[28] Paillier, P. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. In Advances in Cryptology—EUROCRYPT ’99; Springer: Berlin/Heidelberg, Germany, 1999; pp. 223–238.

[29] Khemissa, H.; Tandjaoui, D. A Lightweight Authentication Scheme for E-Health Applications in the Context of Internet of Things. In Proceedings of the 2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies, Cambridge, UK, 9–11 September 2015; pp. 90–95.

[30] Krawczyk, H.; Bellare, M.; Canetti, R. HMAC: Keyed-Hashing for Message Authentication. RFC 2104, Internet Engineering Task Force (IETF). 1997. Available online: https://www.rfc-editor.org/rfc/rfc2104.txt (accessed on 26 July 2017).

[31] Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, National Institute of Standards and Technology (NIST). Available online: http://nvlpubs.nist.gov/nistpubs/FIPS/ NIST.FIPS.197.pdf (accessed on 26 July 2017).

[32] Khemissa, H.; Tandjaoui, D. A Novel Lightweight Authentication Scheme for Heterogeneous Wireless Sensor Networks in the Context of Internet of Things. In Proceedings of the 2016 Wireless Telecommunications Symposium (WTS), London, UK, 18–20 April 2016; pp. 1–6.

[33] Kumar, P.; Gurtov, A.; Iinatti, J.; Ylianttila, M.; Sain, M. Lightweight and Secure Session-Key Establishment Scheme in Smart Home Environments. IEEE Sens. J. 2016, 16, 254–264. [CrossRef]

[34] Gope, P.; Hwang, T. Untraceable Sensor Movement in Distributed IoT Infrastructure. IEEE Sens. J. 2015, 15, 5340–5348. [CrossRef]

[35] Kawamoto, Y.; Nishiyama, H.; Kato, N.; Shimizu, Y.; Takahara, A.; Jiang, T. Effectively Collecting Data for the Location-Based Authentication in Internet of Things. IEEE Syst. J. 2015, 11, 1403–1411. [CrossRef]

[36] Mondal, S.; Bours, P. Continuous Authentication in a Real World Settings. In Proceedings of the 2015 Eighth International Conference on Advances in Pattern Recognition (ICAPR), Kolkata, India, 4–7 January 2015; pp. 1–6.

[37] Shimshon, T.; Moskovitch, R.; Rokach, L.; Elovici, Y. Continuous Verification Using Keystroke Dynamics. In Proceedings of the 2010 International Conference on Computational Intelligence and Security (CIS), Nanning, China, 11–14 December 2010; pp. 411–415.

[38] Mock, K.; Hoanca, B.; Weaver, J.; Milton, M. Real-time Continuous Iris Recognition for Authentication Using an Eye Tracker. In Proceedings of the 2012 ACM Conference on Computer and Communications Security, Raleigh, NC, USA, 16–18 October 2012; pp. 1007–1009.

[39] Shen, C.; Cai, Z.; Guan, X. Continuous Authentication for Mouse Dynamics: A Pattern-growth Approach. In Proceedings of the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2012), Boston, MA, USA, 25–28 June 2012; pp. 1–12.

[40] Bailey, K.O.; Okolica, J.S.; Peterson, G.L. User Identification and Authentication Using Multi-modal Behavioral Biometrics. Comput. Secur. 2014, 43, 77–89. [CrossRef]

[41] Niinuma, K.; Park, U.; Jain, A.K. Soft Biometric Traits for Continuous User Authentication. IEEE Trans. Inf. Forensics Secur. 2010, 5, 771–780. [CrossRef]

[42] Mock, K.; Hoanca, B.; Weaver, J.; Milton, M. Real-time Continuous Iris Recognition for Authentication Using an Eye Tracker. In Proceedings of the 2012 ACM Conference on Computer and Communications Security, Raleigh, NC, USA, 16–18 October 2012; pp. 1007–1009.

[43] Peng, G.; Zhou, G.; Nguyen, D.T.; Qi, X.; Yang, Q.; Wang, S. Continuous Authentication with Touch Behavioral Biometrics and Voice on Wearable Glasses. IEEE Trans. Hum. Mach. Syst. 2017, 47, 404–416. [CrossRef]

[44] Zhou, L.; Su, C.; Chiu, W.; Yeh, K.H. You Think, Therefore You Are: Transparent Authentication System with Brainwave-oriented Bio-features for IoT Networks. IEEE Trans. Emerg. Top. Comput. 2017. [CrossRef]

[45] Seitz, L.; Gerdes, S.; Selander, G.; Mani, M.; Kumar, S. Use Cases for Authentication and Authorization in Constrained Environments. RFC 7744, Internet Engineering Task Force (IETF). 2016. Available online: https://tools.ietf.org/html/rfc7744 (accessed on 20 May 2017).

[46] Bamasag, O.O.; Youcef-Toumi, K. Towards Continuous Authentication in Internet of Things Based on Secret Sharing Scheme. In Proceedings of the WESS'15: Workshop on Embedded Systems Security, Amsterdam, The Netherlands, 4–9 October 2015; pp. 1–8.

[47] Bormann, C.; Ersue, M.; Keranen, A. Terminology for Constrained-Node Networks. RFC 7228, Internet Engineering Task Force (IETF). 2014. Available online: https://tools.ietf.org/html/rfc7228 (accessed on 20 May 2017).

[48] Sethi, M.; Arkko, J.; Keranen, A.; Back, H. Practical Considerations and Implementation Experiences in Securing Smart Object Networks. Draft-Ietf-Lwig-Crypto-Sensors-06. 2018. Available online: https://tools.ietf.org/pdf/draft-ietf-lwig-crypto-sensors-06.pdf (accessed on 20 May 2017).

[49] Atzori, L.; Iera, A.; Morabito, G.; Giacomo, M. The Internet of Things: A Survey. Comput. Netw. 2010, 54, 2787–2805. [CrossRef]

[50] Pereira, G.C.C.F.; Alves, R.C.A.; da Silva, F.L.; Azevedo, R.M.; Albertini, B.C.; Margi, C.B. Performance Evaluation of Cryptographic Algorithms over IoT Platforms and Operating Systems. Secur. Commun. Netw. 2017, 2017, 2046735. [CrossRef]

[51] Yeh, K.H.; Su, C.; Choo, K.R.; Chiu, W. A Novel Certificateless Signature Scheme for Smart Objects in the Internet-of-Things. Sensors 2017, 17, 1001. [CrossRef] [PubMed]

[52] Yo-Hsuan Chuang 1 , Nai-Wei Lo 1 ID , Cheng-Ying Yang 2,* and Ssu-Wei Tang 1. A Lightweight Continuous Authentication Protocol for the Internet of Things, 5 April 2018

[53] Brocardo, M.L.; Traore, I.; Woungang, I. Toward a Framework for Continuous Authentication Using Stylometry. In Proceedings of the 2014 IEEE 28th International Conference on Advanced Information Networking and Applications, Victoria, BC, Canada, 13–16 May 2014; pp. 106–115.