République Algérienne Démocratique et Populaire

Ministère de l'enseignement supérieur et de la recherche scientifique

Université de 8 Mai 1945 – Guelma -

Faculté des Mathématiques, d'Informatique et des Sciences de la matière

Département d'Informatique

Mémoire de Fin d'études Master

Filière : Informatique

Option : Système informatique

Thème :

Un système d'authentification pour l'internet de l'énergie (IoE)

Encadré Par :

Dr. Mohamed Amine Ferrag

Présenté par :

Mahdjoubi imane

Juillet 2019

Remerciement

Remerciement

Nos vifs remerciements vont d'emblée à Dieu tout puissant qui nous a doté d'une grande volonté et d'un savoir adéquat pour mener à bien ce modeste travail.

Nous tenons tout d'abord à remercier Mr Mohamed Amin ferrag pour l'honneur qu'il nous a fait en acceptant de nous encadrer. Ses conseils précieux nous ont permis une bonne orientation dans la réalisation de ce modeste travail.

Nos remerciements sont adressés également à nos chers parents pour tous les sacriices consentis à notre égard et leur énorme soutien.

Tous mes frères et tous mes proches amis (e).

Dédicaces

Ce modeste travail est dédié :

A mes chers parents qui soutenu et encouragé durant toute mon scolarité,

A mes frères et sueurs,

A mes proches,

A mes amis(e),

A toutes les personnes qui ont apportés de l'aide.

A tous mes frères et tous mes proches amis (e).

Résumé

Résumé :

Un réseau électrique est un ensemble d'infrastructures énergétiques plus ou moins disponibles permettant d'acheminer l'énergie électrique des centres de production vers les consommateurs d'électricité.

Dans ce projet de fin d'études, nous abordons le problème de sécurité et d'authentification de ce type de réseaux avant la consommation d'énergie. Nous nous concentrons essentiellement sur l'authentification des données transférées entre le réseau et l'utilisateur.

Dans notre proposition, nous avons choisi un type de protocole connu sous le nom **EAP-IKEv2** pour assuré la protection totale d'échanges entre le réseau et l'utilisateur. Ainsi à l'aide des méthodes automatisées des protocoles présentées par le logiciel **AVISPA,** on a pu implémenter notre protocole.

Table des matières

Table des matières

Table des matières

Table des matières

Table des matières

Liste des figures

Liste des figures :

Les tableaux

Liste des tableaux

Introduction générale

Introduction générale :

Dans la société actuelle le réseau électrique intelligent joue un rôle important dans la technologie et le savoir comme un réseau de transport et de distribution d'électricité bénéficiant d'un contrôle intégré complet et de nouvelles capacités en matière de technologies de l'information et des télécommunications. Il assure un flux énergétique et informationnel bidirectionnel en temps réel, entre tous les acteurs de la filière électrique, de la centrale de production à l'utilisateur final.

Cependant, les fonctionnalités silencieuses du réseau intelligent, le cyber sécurité est devenu un problème critique, car des millions d'appareils électroniques sont interconnectés via des réseaux de communication via des installations d'alimentation critiques, ce qui a un impact immédiat sur la fiabilité d'une infrastructure aussi étendue.

Dans ce perspective, plusieurs contre-mesures et protocoles des sécurités ont été conçus afin de protéger les utilisateurs des réseaux électriques, en essayant de garder pour chaque utilisateur son consommation d'énergie lors sa connectivité à ces réseaux, et de faire face au maximum de menaces connues dans ces réseaux, et de couvrir les vulnérabilités qui donnent de l'occasion aux adversaires de mettre l'utilisateur et le réseau d'une façon générale dans le risque.

Dans mémoire, nous abordons le problème d'authentification d'un système d'un réseau d'internet avant la consommation d'énergie.

En plus, de cette introduction générale et conclusion générale, le mémoire est structuré en quatre chapitres, qui sont les suivant :

- Le premier chapitre : Etat de l'art sur les réseaux électriques intelligents (IoE).
- Le deuxième chapitre : Sécurité et l'authentification de réseau électrique intelligent.
- Le troisième chapitre : Conception d'un protocole d'authentification pour un réseau électrique.
- Le quatrième chapitre : La simulation du protocole d'authentification proposé.

On termine le manuscrit par une conclusion générale, Par ailleurs, une riche bibliographie du domaine et des travaux connexes est listée en fin du document.

1. Chapitre 01 : état de l'art sur les réseaux électriques intelligents (IoE)

1.1 Introduction

A nos jours, les réseaux électriques intelligents jouent un rôle très important, ainsi qu'ils satisfont plusieurs besoins de notre vie quotidienne sur l'aspect technologique.

Dans ce chapitre, on va présenter les réseaux électriques intelligents, ensuite leurs objectifs, leurs systèmes, en plus leurs architectures et enfin les technologies de communication utiliser dans des tels systèmes.

1.2 L'internet d'énergie

L'internet d'énergie est un réseau électrique de la nouvelle génération, il utilise l'internet qui fusionne les technologies de l'information et de la communication (TIC). L'internet d'énergie devienne «intelligente» lorsqu'elle prend totalement en charge les informations bidirectionnelles (communication) et les flux d'énergie bidirectionnels qui sont contrôlés efficacement sur la base d'informations en un temps réel [3].

Plus précisément, l'internet d'énergie peut être considérée comme un appareil électrique système, qui utilise des informations, une communication bidirectionnelle et sécurité technologique et intelligence informatique intégrée dans la production, le transport, les sous-stations, la distribution et la consommation d'électricité afin de créer un système propre, sûr, sécurisé, fiable, résilient, efficace et durable.

Cette description couvre tout le spectre du système énergétique, de la génération au point de consommation de l'électricité [11].

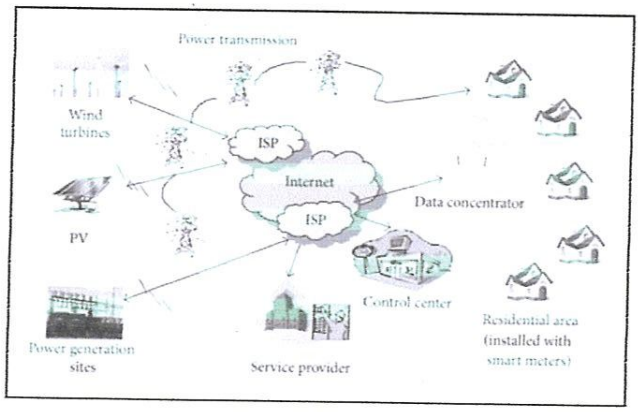

Figure1 : modèle d'un réseau électrique intelligent [7]

1.3 La production d'énergie

De multiples formes de conversion de l'énergie, tel que les systèmes d'alimentation en gaz, les systèmes d'alimentation en chaleur et les systèmes de production combinée de chaleur et d'électricité, sont intégrées dans les pôles énergétiques pour un rendement d'utilisation de l'énergie supérieur. Jouent le rôle de nœuds de réseau,

Les pôles énergétiques sont interconnectés dans le réseau de distribution d'énergie (EDN). Le réseau EDN est un concept novateur consistant à intégrer les flexibilités du côté de la demande en inter opérant différentes énergies telles que l'électricité, le gaz et la chaleur au sein d'une zone locale [25].

1.4 La mise en place des réseaux électriques intelligents

La mise en place d'un réseau électrique intelligent nous permet de développer la consommation d'énergie dans une région donnée. L'internet d'énergie continue de combiner les technologies de l'information et de la communication, cette communication entre différents points du réseau permet de prendre en compte les actions des différents acteurs du système électrique, notamment les consommateurs [13].

1.5 Objectifs des réseaux électriques intelligents

L'internet d'énergie a plusieurs objectifs. Tout d'abord, elle vise à diminuer l'impact du système électrique sur l'environnement. De même, elle cherche à sensibiliser les usagers et à les rendre plus actifs par rapport à leur consommation d'électricité, tout en leur permettant de la contrôler efficacement. Ce système intelligent a également pour but de développer la production d'électricité décentralisée [12].

Réseau existant	internet d'énergie
Électromécanique	Numérique
Communication à sens unique	Communication bidirectionnelle
Génération centralisée	Génération distribuée
Peu de capteurs	Des capteurs tout au long
Surveillance manuelle	Auto-surveillance
Restauration manuelle	Auto-guérison
Échecs et pannes	Adaptatif et îlotage
Contrôle limité	Contrôle envahissant
N'utilise pas l'internet	Utilise l'internet
Peu de choix de clients	Beaucoup de choix de clients

Tableau 1 : comparaison entre réseaux existent et internet d'énergie [11].

1.6 Les systèmes du réseau électrique intelligent

Les trois systèmes principaux dans les réseaux électriques intelligents sont présentés comme suite [11] :

1.6.1 Système d'infrastructure intelligente

L'infrastructure intelligente système est l'énergie, l'information et la communication infrastructure sous-jacente d'internet d'énergie prenant en charge

- production, livraison et consommation d'électricité
- mesure, surveillance et gestion avancées de l'information
- technologies de communication avancées.

1.6.2 Système de gestion intelligent

Est le sous-système dans l'internet d'énergie, il fournit les services de gestion et de contrôle.

1.6.3 Système de protection intelligent

Est le sous-système du réseau électrique intelligent qui fournit une grille d'analyse de fiabilité, protection contre les défaillances, sécurité et services de protection de la vie privée

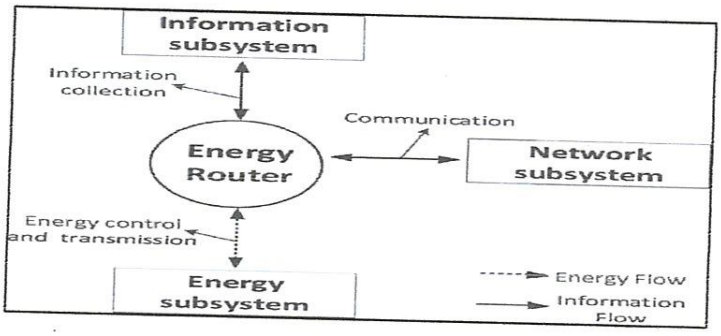

Figure 2 : Energy routers in EI [27]

.17 L'architecture d'internet d'énergie

Il ya différents chercheurs dérivent l'architecture de l'industrie et du monde universitaire, ils ont proposé le modèle le plus largement adapté qui est de loin le modèle de référence proposé par l'institut national américain de norme et de la technologie (NIST). Ce modèle conceptualise l'internet d'énergie comme un ensemble de sept domaines interconnectés [4], on les subdivise en deux parties:

- **Partie 1 (les quatre premiers domaines) :**

Constitue de (génération, transmission, distribution et client), elles sont chargées de la production du transport et de la distribution de l'énergie.

- **Partie 2(les trois restantes) :**

Constitue de (marchées, opération et fournisseurs de services), inspiré du modèle NIST, cette architecture conceptualise l'internet d'énergie selon une approche multicouche.

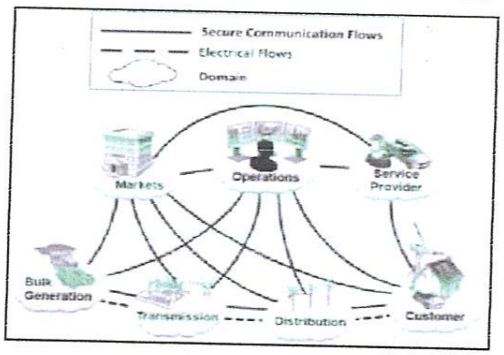

Figure 3: NIST modèle d'internet of énergie [9]

.18 L'architecture de smart home

Smart home devrait être connectant avec ses environnement internes et externe, les externes consiste de tous les entités appartient à l'internet d'énergie de l'entité unique responsable de l'interconnexion des réseaux.

D'autre part, les internes sont tous les appareils et les périphériques de smart home qui gèrent de manière centralisée par une entité de celui-ci. Les deux environnements président sont représentés par des entités spécifiques, une entité appelée interface ESI (Energy Services Interface) représente l'environnement externe tandis qu'une entité appelé système de gestion de l'énergie représente l'environnement interne.

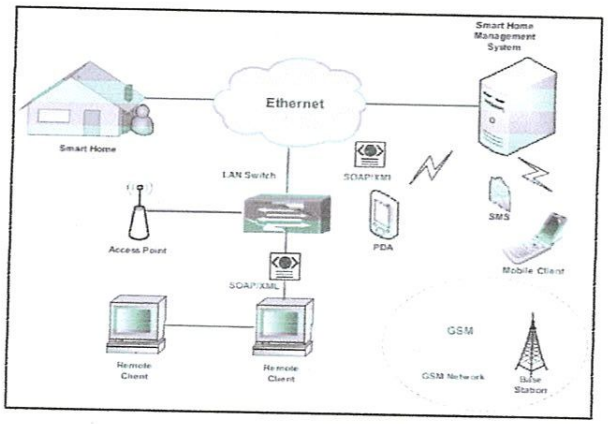

Figure 4 : modèle home *[8]*

.19 Les avantages des réseaux électriques intelligents

Dans ce qui suit, nous citons quelques avantages [17] :

- Meilleure connaissance de la situation et assistance des opérateurs.
- Actions de contrôle autonomes pour améliorer la fiabilité.
- Amélioration de l'efficacité en maximisant l'utilisation des actifs.
- Résilience améliorée contre les attaques malveillantes.
- Intégration des ressources renouvelables.
- Intégration de tous types de stockage d'énergie et autres ressource.
- Communication bidirectionnelle entre le consommateur et le service public.
- Amélioration de l'efficacité du marché.
- Qualité de service supérieure pour alimenter une économie de plus en plus numérique.

Chapitre 01

1.10 Les aspects d'internet d'énergie

Dans l'internet d'énergie, les aspects de communications sont [3]:

- L'infrastructure de livraison.
- Les system des utilisateurs finaux et les ressources en distribuées associées.
- Les réseaux de communication.
- Les systèmes de gestion à différents niveaux de génération.
- L'environnement financier et réglementaire.

1.11 Les Technologies de communications utilisées dans l'internet d'énergie

1.11.1 Le système AMI

Ce système est une réalisation importante des réseaux électriques intelligents. Il est utilisé pour mesurer, calculer et analyser des données relatives à la consommation et la qualité de l'énergie. Tout réseau électrique intelligent avec une infrastructure AMI implique des installations de communication avec des dispositifs de mesure personnalisés. La communication bidirectionnelle entre le fournisseur de services publics et le consommateur est mise en œuvre pour améliorer la maintenance, la gestion de la demande et la planification des ressources (6).

1.11..2 La technologie clé d'AMI

Les capteurs intelligents, sont des dispositifs programmables à semi-conducteurs capable de lire l'énergie en temps réel. Consommation, ainsi que d'autres données opérationnelles, tel que la tension, angles de phase et fréquences, constitué de compteurs intelligents.

AMI permet le transfert de données bidirectionnel automatisé entre les compteurs, les utilisateurs finaux et les gestionnaires de réseau, de sorte que des analyses et traitements de données supplémentaires puissent être effectués pour faciliter la tarification du marché et les contrôles opérationnels [5].

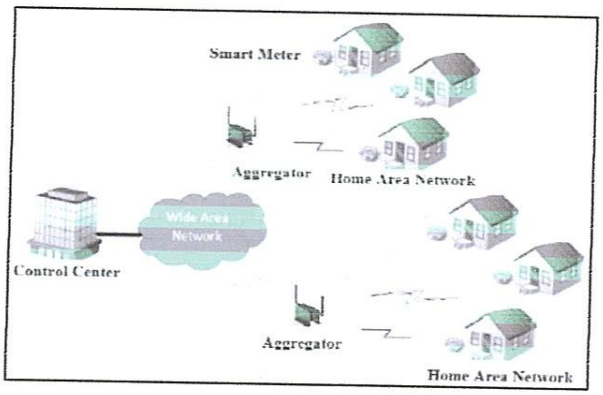

Figure 5 : modèle AMI dans smart grid [10]

1.11.3 Power Line Communication (PLC)

Filaires technologie qui utilisent une ligne conductrice de transmission de puissance pour transmettre des données. Son coût est inférieur à celui des modes de communication sans fil car il utilise l'infrastructure de ligne électrique existante. Il existe trois classes de technologie de communication CPL: large bande, bande étroite et bande ultra étroite. Le haut débit fournit un débit de données allant jusqu'à 200 Mbps et est applicable aux infrastructures résidentielles AMI (infrastructure de comptage avancée) / AMR (lecture automatique des compteurs), mais ne convient pas aux sous-stations. La bande étroite fournit un débit de données pouvant atteindre 500 kbps et est applicable aux communications entre sous-stations. La bande fournit jusqu'à 100 Pb et s'applique aux IAM, AMR, Réponse à la demande (à des fins de contrôle direct de la charge) [5].

1.11.4 ZigBee normes IEEE 802.15.4

Les normes adoptent le mode balise et le mode non balise pour la communication. Dans la communication en mode balise, le dispositif recherche la balise réseau pour l'intervalle de transmission des données, tandis qu'en mode non balise, il envoie simplement les données au nœud de coordination du réseau. Les appareils compatibles Zig-Bee utilisent les mêmes fonctionnalités de manière légèrement différente. Ils ont deux types d'appareils. L'un est le dispositif à fonction complète (FFD) et l'autre est le dispositif à fonction réduite (RFD). Le réseau formé sur la base de périphériques Zig-Bee est constitué de ces deux périphériques. L'établissement et la gestion du réseau, ainsi que le routage des données, relèvent de la FFD. Les RFD sont là pour prendre en charge les fonctions des FFD [6].

1.11.5 Wifi

Un réseau local sans fil (WLAN), relie deux périphériques ou plus à fréquence étalée ou orthogonale et fournissent généralement une connexion via un point d'accès à l'Internet au sens large. Cela donne aux utilisateurs la possibilité de se déplacer dans une zone de couverture locale tout en restant connectés au réseau. La plupart des WLAN modernes sont basés sur les normes IEEE 802.11, commercialisées sous la marque Wifi, pourrait être facilement intégré au réseau intelligent en raison de son vaste déploiement dans le monde entier. Le WLAN fonctionne dans les fréquences 2,4 GHz - 3,5 GHz [6].

1.11.6 Cellular Networks

Les réseaux cellulaires peuvent être utilisés pour assurer la communication entre différents composants et appareils du réseau intelligent. Il existe plusieurs technologies pour les communications cellulaires telles que (2G, 3G, 4G et Wi-MAX ...etc.)(6).

1.12 Conclusion

Dans ce chapitre, on présenté les réseaux électriques intelligents. Sous prétexte que le succès d'internet d'énergie dépend d'un système de communication fiable, robuste et sécurisé avec une capacité de débit de données élevée, on fait une comparaison entre le futur système de télécommunication et l'internet d'énergie.

Dans le prochain chapitre, nous verrons la sécurité et l'authentification d'un système intelligent.

2. Chapitre 02 : sécurité et l'authentification de réseau électrique intelligent

2.1 Introduction

Selon l'Institut de recherche sur l'énergie électrique (EPRI), l'un des plus grands défis du développement de l'internet d'énergie est lié au cyber sécurité des systèmes. Selon le rapport de L'EPRI, le cyber sécurité est un problème critique en raison du potentiel croissant de cyber attaques et d'incidents contre ce secteur critique, qui devient de plus en plus interconnecté [15]. Le cyber sécurité doit traiter non seulement les attaques délibérées, telles que celles perpétrées par des employés mécontents, mais également les compromissions involontaires de l'infrastructure informatique résultant d'erreurs utilisateur, de pannes d'équipement et de catastrophes naturelles. Des vulnérabilités pourraient permettre à un attaquant de pénétrer dans un réseau, d'accéder à un logiciel de contrôle et de modifier les conditions de charge pour déstabiliser le réseau de manière imprévisible [16].

2.2 Réseau électrique intelligent

Basé sur la définition du réseau électrique intelligent en tant qu'infrastructure de réseau dynamique intégrée reposant sur des protocoles de communication standard et interopérables qui interconnectent le réseau d'énergie avec Internet, permettant ainsi aux unités d'énergie d'être envoyées où et quand cela est nécessaire, il est facile de comprendre que L'authentification dans l'environnement IoE n'est pas un problème facile à résoudre. IoE combine les technologies M2M, V2G, IoT (Internet des objets industriels), la domotique intelligente, les services cloud et l'IoS. Il serait préférable de définir l'IoE comme une application de l'IdO dans le domaine de l'énergie. L'authentification sur le domaine IoE ne peut être sécurisée sans traiter avec chacun des sous-domaines susmentionnés. Les techniques d'authentification de la sécurité et du matériel ainsi que les solutions traitant de la sécurité des inters logiciels doivent être combinées [28].

2.3 Authentification

L'authentification est une procédure, par laquelle un système informatique certifie l'identité d'une personne ou d'un ordinateur. Le but de cette procédure est d'autoriser

l'accès à certaines ressources sécurisées. Qui va comparer les informations des utilisateurs stockées dans une base de données (en local ou sur un serveur d'authentification) à celles fournies. L'accès sera autorisé seulement si les informations sont identiques. C'est l'administrateur du système d'information qui octroie les droits et paramètre l'accès. L'utilisateur possédant un compte d'accès (identifiant + mot de passe) n'aura accès qu'aux ressources dont il est autorisé à utiliser [18].

L'authentification peut être définie comme le processus de prouver une identité revendiquée. La confidentialité, l'intégrité des données, et la répudiation dépendent tous de l'authentification appropriée. Un système sans cette fonctionnalité ne pouvait pas fournir les objectifs de sécurité mentionnée de manière satisfaisante [20]. Un problème d'identification important pour toute communication réseau. Des systèmes d'authentification puissants sont nécessaires pour les clients et les dispositifs électroniques afin de garantir des communications en toute sécurité et de répondre aux exigences strictes du réseau de communication du réseau intelligent, telles que les contraintes de délai de message et de la consommation d'énergie [14].

2.4 Les Facteurs d'authentification

Les facteurs de l'authentification du réseau électrique intelligent sont [19] :

2.4.1: Facteurs mémoriels :

Cette catégorie de données d'authentification se compose des informations que l'utilisateur connaît, par exemple un code confidentiel, un nom d'utilisateur, un mot de passe ou la réponse à une question secrète.

2.4.2 Facteurs matériels :

Cette catégorie s'appuie sur des objets que l'utilisateur possède. Il s'agit généralement d'un dispositif matériel, comme un jeton de sécurité ou un téléphone mobile utilisé conjointement à un jeton logiciel.

2.4.3 Facteurs corporels :

Cette catégorie d'informations d'authentification d'un utilisateur, est formée des éléments constitutifs de la personne en question sous forme de données.

2.5 Authentification du réseau électrique intelligent

Afin de fournir l'authentification mutuelle entre les compteurs intelligents et le serveur de sécurité et d'authentification dans le réseau intelligent à l'aide de mots de passe, Nicanfar et autre [41]. Proposer un schéma d'authentification mutuelle et un protocole de gestion de clé, appelés respectivement SGMA et SGKM. Le schéma SGMA se concentre sur les communications de données via l'infrastructure de comptages avancés (AMI) en dehors du domaine HAN, chaque nœud ayant un identifiant unique et chaque compteur intelligent possédant un numéro de série unique SN intégré par le fabricant et un mot de passe secret initial. D'autre part, le protocole SGKM se concentre sur les communications sécurisées nœud à nœud, dans lesquelles les nœuds disposent des clés privées publiques appropriées à utiliser pour la monodiffusion. Basé sur le mécanisme de clé de multidiffusion, le schéma SGMA peut empêcher diverses attaques tout en réduisant les frais de gestion, mais manque de non-répudiation par rapport au schéma PBA [42] de Shim et autre. [43] Considérons un réseau de réseau intelligent basé sur une architecture hiérarchique, c'est-à-dire des réseaux HAN, BAN, NAN. Le travail proposé l'enregistrement préservant la confidentialité et l'authentification assistée par passerelle des informations d'utilisation de l'énergie. Le filtrage de messages au niveau des compteurs intelligents de passerelle peut être utile pour réduire l'impact d'attaque de trac. Semblable au schéma, Mahmoud et autres, [44] ont proposé un schéma d'authentification de message léger. Basé sur deux processus principaux, à savoir, l'authentification et la transmission de messages, le système peut détecter et omettre certaines attaques, à savoir la relecture, l'injection de faux messages, l'analyse de messages et les attaques de modification. En outre, le schéma est efficace en termes de coût de communication et de calcul par rapport aux schémas [45] proposé, mais la confidentialité de la localisation n'est pas prise en compte [28].

2.6 Les normes et les protocoles du réseau électrique intelligent

Afin de concrétiser la vision des communications EI (internet énergie), il est essentiel de disposer d'un ensemble complet de normes et de protocoles de communication intégrés dans l'assurance-emploi, de nombreuses fonctions importantes nécessitaient la prise en charge des protocoles appropriés, telles que l'efficacité du transport d'énergie, la mesure de la micro-puissance, l'optimisation du réseau, la gestion et le fonctionnement du réseau. De plus, afin de

répondre à la demande personnalisée, la prise en charge des protocoles de communications en temps réel est essentielle pour garantir la production d'énergie et l'équilibre de la charge. Les normes et les protocoles **EI** doivent donc être respectés pour les fonctions principales suivantes : (communication bidirectionnelle, interopérabilité pour les applications énergétiques avancées, communications fiables et sécurisées de bout en bout et capacités contre les cybers attaques potentielles).

Cette section récapitule les normes et protocoles existants pour la création d'IE, puis présente la nouvelle norme pour les entreprises d'assurance emploi [29].

2.7 L'objectif de la sécurisation

L'objectif du cyber sécurité est de protéger les données, à la fois en transit et au repos. Par conséquent, notre enquête est centrée sur les problèmes de sécurité inhérents au cycle de vie complet des données du réseau qui peuvent être systématiquement décomposées en quatre étapes séquentielles: génération, acquisition, stockage et traitement des données [24].

2.8 Les vulnérabilités

Le réseau intelligent apporte des améliorations et des capacités pour le réseau électrique conventionnel, afin de rendre plus complexe et vulnérable à différents types d'attaques.

Ces vulnérabilités peuvent permettre à des attaquants d'accéder au réseau, casser la confidentialité et l'intégrité des données transmises et rendre le service indisponible. Comme proposé dans, les vulnérabilités suivantes sont les plus graves des réseaux intelligents [15]:

2.8.1 Sécurité des clients

Les compteurs intelligents collectent de manière autonome des quantités énormes de données et les transmettent à l'entreprise de services publics, au consommateur et aux fournisseurs de services. Ces données incluent des informations sur les consommateurs privés pouvant être utilisées pour déduire leurs activités, les appareils utilisés et les heures où le domicile est vacant.

2.8.2 Plus grand nombre d'appareils intelligents

Un réseau intelligent comprend plusieurs appareils intelligents impliqués dans la gestion de la fourniture d'électricité et de la demande du réseau. Ces dispositifs intelligents peuvent faire office de points d'attaque dans le réseau. De plus, la masse du réseau intelligent (100 à 1 000 fois plus grande qu'Internet) rend la surveillance et la gestion du réseau extrêmement difficiles.

2.8.3 Sécurité physique

. Contrairement au système électrique traditionnel, le réseau intelligent comprend de nombreux composants, dont la plupart ne se trouvent pas dans les locaux de l'entreprise. Ce fait augmente le nombre d'emplacements physiques non sécurisés et les rend vulnérables à l'accès physique.

2.8.4 La durée de vie des systèmes d'alimentation

Les systèmes d'alimentation coexistant avec des systèmes informatiques à durée de vie relativement courte, il est inévitable que des équipements obsolètes soient toujours en service. Cet équipement pourrait agir comme un point de sécurité faible et pourrait même être incompatible avec les dispositifs actuels du système d'alimentation.

2.8.5 Confiance implicite entre les périphériques d'alimentation traditionnels

La communication entre périphériques dans les systèmes de contrôle est vulnérable à l'usurpation de données lorsque l'état d'un périphérique affecte les actions d'un autre. Par exemple, un périphérique envoyant un état faux entraîne le comportement indésirable d'autres périphériques.

2.8.6 Origines différentes des équipes

Une communication inefficace et non organisée entre les équipes peut causer beaucoup de mauvaises décisions menant à beaucoup de vulnérabilités.

2.8.7 Utilisation du protocole Internet (IP)

L'utilisation des normes IP et du matériel et des logiciels commerciaux dans les réseaux intelligents constitue un avantage considérable, car elle offre une compatibilité entre les divers composants. Cependant, les périphériques utilisant IP sont intrinsèquement vulnérables à de nombreuses attaques réseau basées sur IP, telles que l'usurpation d'adresse IP, le largage instantané, le déni de service.

2.8.8 Avantages des parties prenantes

Le fait d'avoir de nombreuses parties prenantes pourrait donner lieu à un type d'attaque très dangereux: les attaques internes.

2.9 Menasses de sécurité à l'égard des réseaux électriques intelligents

Un réseau de communication d'intente d'énergie est un agrégat de plusieurs réseaux avec différents niveaux de communication et de coordination entre les fournisseurs d'électricité, les opérateurs et les clients.

Ces réseaux de communication complexes nécessitent une conception de sécurité complète, car ils sont probablement la cible d'attaques informatiques sophistiquées peuvent être lancées à partir de n'importe quel composant vulnérable du système hautement distribué.

Cependant, énumérer toutes les menaces possibles dans le réseau intelligent n'est pas pratique en raison de sa complexité et de certaines attaques sophistiquées qui n'ont pas encore été identifiées. Ainsi, dans cette section, nous utilisons une approche descendante pour classer les attaques malveillantes en trois types principaux, en fonction de leurs objectifs: la disponibilité du réseau, intégrité des données, confidentialité des informations, comme indique [21].

2.9.1 Disponibilité du réseau

La disponibilité des services de bout en bout pour les applications des réseaux électriques intelligent et de comptage intelligent dépend de la disponibilité de l'emplacement et de l'heure. Alors que la disponibilité de localisation des réseaux fixes dépend uniquement

des foyers connectés et de la redondance mise en œuvre, la disponibilité de localisation des réseaux sans fil est connectée à la couverture radio [22].

2.9.2 Intégrité des données et confidentialité des informations

De telles attaques tentent de modifier délibérément les informations partagées au sein du réseau intelligent afin de corrompre l'échange de données critiques dans le réseau intelligent. Au contraire, les attaquants qui s'intéressent à la confidentialité des informations ne tentent pas de modifier les informations transmises sur les réseaux électriques, mais bien d'écouter les communications sur ces réseaux pour acquérir les informations souhaitées, telles que le numéro de compte du client et la consommation d'électricité [23].

2.10 Les attaque sur les réseaux électriques intelligents

De nombreuses attaques de différentes catégories peuvent être perpétrées contre l'ensemble du SG ou contre des composants spécifiques de celui-ci. Le premier pas vers la défense contre de telles attaques est l'identification et la détection appropriée, nous essayons de catégoriser différents types d'attaques et contre-mesures qui existent contre le SG. En particulier, nous classons les attaques en fonction de leur service ou dispositif d'aide respectif, ainsi que du type d'attaque. Les cinq catégories de cyber-attaques et de contre-mesures de réseau intelligent que nous soulignons dans le présent document sont répertoriées comme suit [40].

- Attaques de contrôle et d'acquisition de données (SCADA),
- Attaques de compteurs intelligents
- Attaques de la couche physique
- Injection de données et attaques par rejoue, et
- Attaques basées sur le réseau.

Le tableau suivant présente une vue d'ensemble des propriétés de sécurité affectées par les différentes attaques SG, ainsi que de l'emplacement du réseau sur lequel ces attaques sont perpétrées.

Type d'attaque	Quelle propriété de sécurité est affectée?	Lieu de la victime
SCADA	Confidentialité, déni de service, intégrité	Réseaux de zone de rattachement
Compteur intelligent	Confidentialité, intégrité, disponibilité, non répudiation	Réseaux de zone de rattachement / de voisinage
Couche physique	Intégrité des données, déni de service, confidentialité	Région d'origine / zone de voisinage / réseaux étendus
Attaques par injection de données et rejoue	Confidentialité	Zone de résidence / zone de voisinage / réseaux étendus
Basé sur le réseau	Disponibilité, confidentialité	Zone de résidence / zone de voisinage / réseaux étendus

Tableau 2 : type d'attaque avec descriptions

2.10 Conclusion

Dans ce chapitre, nous avons présenté une vue sur la sécurité et l'authentification d'un réseau électrique d'énergie afin d'éviter les différentes attaques possibles. Après cette étude on peut faire une proposition sur ce domaine, c'est ce que nous allons aborder dans le prochain chapitre.

3. Chapitre 03 : conception d'un protocole d'authentification

3.1 Introduction

Dans ce chapitre nous allons proposer un protocole d'authentification pour protéger un réseau électrique intelligent basé sur le protocole EAP-IKV (The Extensible Authentication Protocol-Internet Key Exchange Protocol version 2).

3.2 Définition

Un protocole d'authentification est un protocole de communication réseau embarquant de multiples méthodes d'authentification, pouvant être utilisé sur les liaisons point à point , les réseaux filaires et les réseaux sans fil tels que les réseaux Wifi. Il se constitué d'un échange de trames dans un format spécifique à EAP pour réaliser l'authentification d'un partenaire. Un protocole extensible : quelques méthodes d'authentification sont prédéfinies (MD5, OTP) mais d'autres peuvent être ajoutées sans qu'il soit nécessaire de changer le protocole réseau ou d'en définir un nouveau [30].

3.3 Vue générale sur le protocole

L'exécution complète du protocole EAP-IKEv2 est spécifiée. Tous les messages sont envoyés entre deux parties, à savoir un homologue EAP et un serveur EAP. Dans EAP-IKEv2, le serveur EAP assume toujours le rôle d'initiateur (I) et le pair EAP celui de répondeur (R) d'un échange. La sémantique et les formats des messages EAP-IKEv2 sont similaires, bien que non identiques, à ceux spécifiés dans IKEv2 pour l'établissement d'une association de sécurité IKE. L'exécution complète du protocole EAP-IKEv2 comprend deux allers-retours suivis d'un message EAP-Succès ou d'un message EAP-Fail ure. Un aller-retour optionnel pour l'échange de PAE les identités peuvent précéder les deux échanges [31].

3.4 Méthode d'EAP-IKEv2

- 1. R<-I: EAP-Requête /Identité
- 2. R->I: EAP Réponse/Identité(Id)
- 3. R<-I: EAP-Req (HDR, SAi, KEi, Ni)
- 4. R->I: EAP-Res (HDR, SAr, KEr, Nr, [CERTREQ], [SK {IDr}])
- 5. R<-I: EAP-Req (HDR, SK {IDi, [CERT], [CERTREQ], [NFID], AUTH})

- 6. R->I: EAP-Res (HDR, SK {IDr, [CERT], AUTH})
- 7. R<-I: EAP-Succès

Le symbole	Description
AUTH	Indique un champ de données contenant un code d'authentification de message (MAC) ou une signature. Ce champ est intégré à une charge d'authentification,
CERT	certificat de clé publique ou structure similaire.
CERTREQ	demande de certificat
NFID	charge utile prochain rapide –ID
EMSK	clé de session maîtresse étendue
HDR	en-tête EAP-IKEv2
I	initiateur, partie qui envoie le premier message d'une exécution du protocole EAP-IKEv2. C'est toujours le serveur EAP.
MAC	code d'authentification du message. Résultat d'une opération cryptographique impliquant une clé symétrique
MSK	clé de session principale
Prf	fonction pseudo-aléatoire: fonction cryptographique dont la sortie est supposée impossible à distinguer de celle d'une fonction réellement aléatoire.
R	répondeur, partie qui envoie le deuxième message d'une exécution du protocole EAP-IKEv2. C'est toujours le pair EAP.
SA	Association de sécurité. Dans ce document, SA désigne un type de charge utile utilisé pour la négociation des algorithmes cryptographiques doivent être utilisés dans une exécution de protocole EAP-IKEv2. Spécifiquement, SA i désigne un ensemble de choix acceptés par un initiateur, et SAr indique le choix du répondant.
Signature	résultat d'une opération cryptographique impliquant une clé asymétrique. En particulier, il s'agit de la partie privée d'une paire de clés publique / privée.
SK	clé de session. Dans ce document, la mention SK {x} indique que x est incorporé dans une charge chiffrée, c'est-à-dire que x est chiffré et protégé en intégrité à l'aide de clés internes EAP-IKEv2. Ces touches sont différentes dans chaque direction
SK_xx	clé interne EAP-IKEv2
SKEYSEED	Matériel de chiffrement

Tableau 3 symbole –description

Chapitre 03

3.5 Explication de la méthode

- Les messages 1 et 2 sont une demande et une réponse d'identité EAP standard La premier demande d'une session IKE négocie les paramètres de sécurité pour IKE-SA, envoie des valeurs. La deuxième demande (IKE-AUTH) transmet les identités, la connaissance de secrets correspondant aux deux identités et établit une association de sécurité pour la premier
- Le message 3 est le premier message spécifique à EAP-IKEv2. Avec cela, le serveur démarre l'échange d'authentification EAP réel. Il contient le SPI (Security Parameter Index) de l'initiateur dans l'en-tête EAP-IKEv2 (HDR) (l'initiateur sélectionne un nouveau SPI pour chaque exécution de protocole), l'ensemble des algorithmes de chiffrement que le serveur est prêt à accepter pour la protection de EAP-IKEv2. trafic (chiffrement et protection de l'intégrité) et la dérivation de la clé de session
- Dans le message 4 le répondeur choisit une suite cryptographie parmi les choix proposés par l'initiateur et exprime ce choix dans la charge utile SRA1.
- A la réception de message 5, le répondeur authentifie l'initiateur, la vérification effectuée à cette fin dépond du cas d'utilisation. Ces vérification incluent le déchiffrement de la chiffrée, la vérification de son intégrité et la vérification que la charge d'authentification contient la valeur attendue. Si tous les contrôles est juste le répondeur construit le message 6.
- Message 6 : ce message doit contient l'entête (HDR) de EAP-IKE v2 suivi d'un seul charge utile crypté, dans lequel au moins deux autre charge d'utile. La réception du message 6 l'initiateur authentifie le répondeur, les vérifications effectuées à cette fin dépendent du cas d'utilisation des politiques locales.
- Si l'authentification réussit, un message EAP-Succès est envoyé au répondeur en tant que message 7. Le serveur EAP et l'homologue EAP génèrent une clé de sessions maîtresses (MSK) et une clé de session maîtresse étendue (EMSK) après une exécution réussie du protocole EAP-IKEv2.

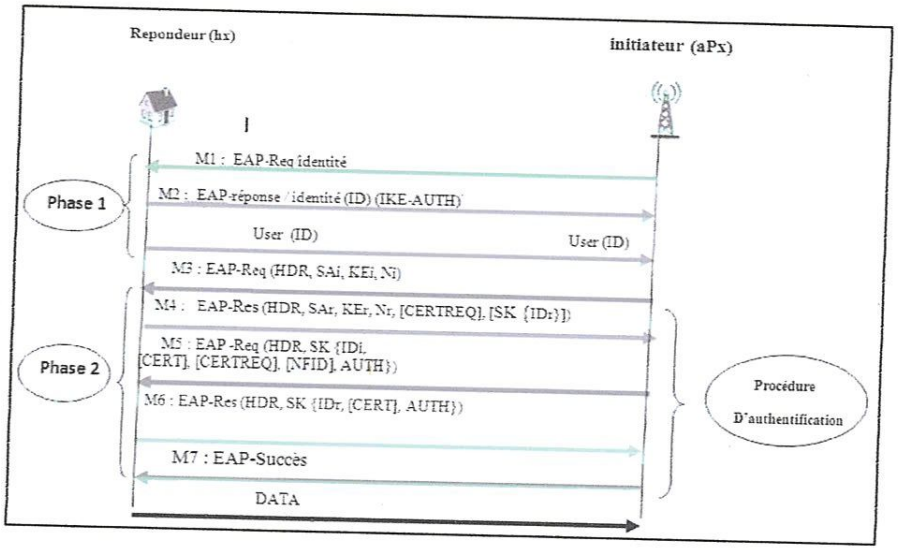

Figure 6 : EAP-IKE V2

3.6 L'échange CREATE_CHILD_SA

- L'échange CREATE_CHILD_SA est utilisé pour créer de nouveaux SA enfant et pour recréer à la fois les SA IKE et les SA Enfant. Cet échange consiste en un seul couple requête /réponse. Une SA est redéfinie en créant une nouvelle SA puis en supprimant l'ancienne
- Chaque point d'extrémité peut initier un échange CREATE_CHILD_SA. Le terme initiateur désigne le point d'extrémité à l'origine de cet échange. Une implémentation peut refuser toutes les demandes CREATE_CHILD_SA au sein d'un SA IKE.
- La demande CREATE_CHILD_SA peut facultativement contenir une charge utile KE pour un échange Diffie-Hellman supplémentaire afin de permettre des garanties plus strictes de confidentialité pour la SA enfant.
- Le matériel de chiffrement pour la SA d'enfant est une fonction de SK_d établie lors de l'établissement de la SA IKE, les informations échangées lors de l'échange CREATE_CHILD_SA et la valeur Diffie-Hellman (si des charges KE sont incluses dans l'échange CREATE_CHILD_SA).
- Si un échange CREATE_CHILD_SA inclut une charge utile KEi, au moins une des offres SA doit inclure le groupe Diffie-Hellman de KEi. Le groupe Diffie Hellman du KEi DOIT être un élément du groupe que l'initiateur attend du répondeur qu'il accepte.
- Si le répondeur sélectionne une proposition utilisant un groupe Diffie-Hellman différent (autre que NONE), il doit rejeter la demande et indiquer son groupe Diffie-Hellman préféré dans la charge utile

- Le répondeur envoie une notification pour indiquer qu'une demande CREATE_CHILD_SA est inacceptable car le répondeur ne souhaite pas accepter d'autres SA de l'enfant sur ce SA IKE.
- Cette notification peut également être utilisée pour rejeter la nouvelle clé IKE SA. Certaines implémentations minimales peuvent n'accepter qu'une seule configuration SA enfant dans le contexte d'un échange IKE initial et rejeter toute tentative ultérieure d'en ajouter d'autres [39].

3.7 Renouvellement des SA avec l'échange CREATE_CHILD_SA

La demande CREATE_CHILD_SA permettant de ressaisir un IKE_SA est la suivante:

- L'initiateur envoie une ou des offres SA dans la charge utile SA, vers la charge Ni, et éventuellement une valeur Diffie-Hellman dans la charge KEi.

La réponse CREATE_CHILD_SA permettant de ressaisir un IKE_SA est la suivante:

- Le répondeur répond (en utilisant le même ID de message pour répondre) avec l'offre acceptée dans une charge SA, vers la charge Nr et, éventuellement, une valeur Diffie-Hellman dans la charge KEr.
- Les compteurs de messages de la nouvelle IKE_SA sont définis sur 0, indépendamment de ce qu'ils étaient dans la version précédente de IKE_SA. La taille de la fenêtre commence à 1 pour toute nouvelle IKE_SA. Les nouveaux SPI initiateur et répondeur sont fournis dans les champs SPI des données utiles SA.

La demande CREATE_CHILD_SA permettant de saisir à nouveau un CHILD_SA est la suivante:

- La charge de notification identifie le CHILD_SA en cours de recomposition et contient le SPI attendu par l'initiateur dans les en-têtes des paquets entrants. En outre, l'initiateur envoie une ou plusieurs offres SA dans la charge utile SA, un non-élément dans la charge Ni, éventuellement une valeur Diffie-Hellman dans la charge KEi et les sélecteurs de trafic proposés dans les deux autre charges La demande peut également contenir des données un utiles indiquant des détails supplémentaires pour CHILD_SA.

La réponse CREATE_CHILD_SA permettant de saisir de nouveau un CHILD_SA est la suivante:

- Le répondeur répond avec l'offre acceptée dans une charge utile SA et une valeur Diffie-Hellman dans la charge KEr si KEi était inclus dans la demande et si la suite cryptographique sélectionnée incluait ce groupe.
- Les sélecteurs de trafic pour le trafic à envoyer sur cette SA sont spécifiés dans les données un utiles de la réponse, ce qui peut être un sous-ensemble de ce que l'initiateur de CHILD_SA a proposé [39].

3.8 Les fonctions d'hachage

3.8.1 La description :

Il existe trois d'algorithmes de cryptographie : la clé secrète, la clé publique et les fonctions de hachage. Contrairement aux algorithmes a clé secrète et a clé publique, les fonctions de hachage, sont également appelées digests de massage ou cryptage unidirectionnel, elles n'ont pas de clé [32]. Une fonction de hachage est une fonction mathématique qui convertit une valeur d'entrée numérique en une autre valeur numérique compressée. L'entrée de la fonction de hachage est de longueur arbitraire mais la sortie est toujours de longueur fixe. Les valeurs envoyées par une fonction de hachage sont appelées message digest ou simplement valeurs de hachage [33].

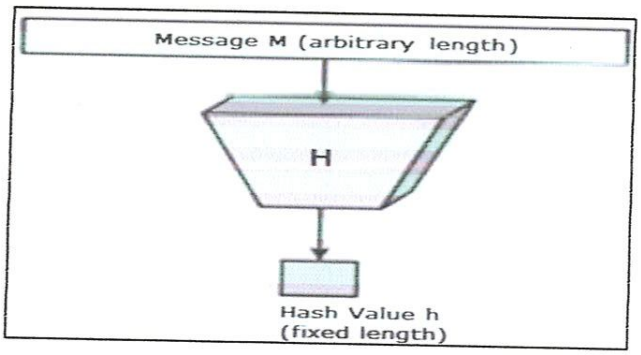

Figure 7 : Une fonction de hachage

3.8.2 Finalité d'un condensat et réputation d'un algorithme de calcul de condensats :

La réputation de l'algorithme de calcul d'un hash-code (calcul d'un condensat - fonction de hachage) est de ne jamais produire deux hash-codes identiques si les objets (fichiers) contiennent la moindre différence. La fonction de hachage doit donc produire une clé unique d'identification d'une donnée unique (calcul homogène) [36].

3.7.3 Conception d'algorithmes de hachage :

Au cœur d'un hachage est une fonction mathématique qui fonctionne sur deux blocs de données de la taille fixe pour créer un code de hachage. Cette fonction de hachage constitue la partie de l'algorithme de hachage. La taille de chaque bloc de données varie en fonction de l'algorithme. Typiquement, les tailles de bloc vont de 128 bits a 512 bits. L'illustration suivante montre la fonction de hachage [34].

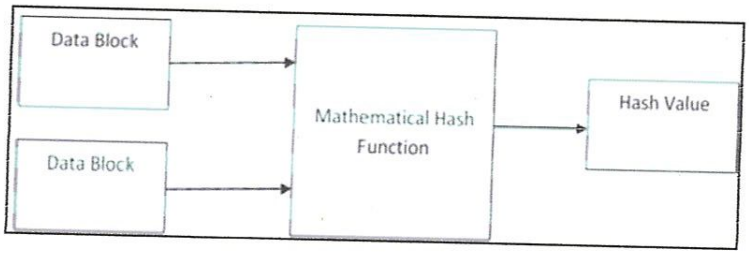

Figure 8 : structure de la fonction [33]

L'algorithme de hachage implique des tours de hachage ci-dessus comme un chiffrement par bloc. Chaque tour prend une entrée de taille fixe, généralement une combinaison du bloc de message le plus récent et de la sortie du dernier tour. Ce processus est répété pour autant de tours que nécessaire pour hacher le message en entier. Le schéma de l'algorithme de hachage est décrit dans l'illustration suivante.

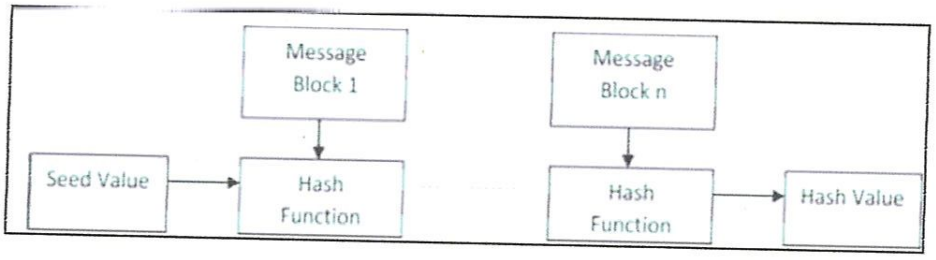

Figure 9 : algorithme de hachage [34]

3.8.4 Fonctions de hachages populaires

Il existe plusieurs fonctions de hachage bien connues actuellement :

- Code d'authentification de message haché (HMAC) : combine l'authentification via secret partagé avec le hachage.

- Message digest 2 (MD5) : orienté octet, produit une valeur de hachage de 128 bits a partir d'un message de longueur arbitraire, conçu pour les cartes puce.
- MD4 : similaire à MD2, spécialement conçu pour un traitement rapide dans les logiciels.
- MD5 : similaire à MD4, mais plus lent car les données sont plus manipulées. Développé après les faiblesses potentielles ont été signalées dans MD4.
- Algorithme de hachage sécurisé (SHA) : modélisé après MD4 proposé par le NIST pour la norme SHS (Secure Hash Standard), produit une valeur de hachage de 160bits.

3.8.5 Algorithme de hachage (SHA-256) :

Est une fonction de hachage cryptographique avec une longueur de résumé dc 256. Morceaux. C'est une fonction de hachage sans clé ; c'est-à-dire un code de détection de manipulation (MDC). Un message est traité par blocs de 512 = 16 × 32 bits, chaque bloc nécessitant 64 tours.

3.8.6 Opérations de base :

- Opérations booléennes AND, XOR et OR.
- Complément au niveau du bit.
- Addition entière, modulo 232, notée A + B

Chacun d'entre eux opère sur des mots de 32 bits. Pour la dernière opération, les mots binaires sont interprétés comme des entiers écrits en base 2.

- RotR (A, n) indique le décalage droit circulaire de n bits du mot binaire A.
- ShR (A, n) indique le décalage à droite de n bits du mot binaire A.
- AkB désigne la concaténation des mots binaires A et B.

3.8.7 Les Constantes :

SHA-256 utilise 64 valeurs constantes de mots de 32 bits, notés dans le tableau en bas. Ces nombres représentent les 32 premiers bits de la partie décimale des racines cubiques des 64 premiers nombres premiers. Les valeurs suivantes sont exprimées en notation hexadécimale (base 16) [35].

$K_0^{\{256\}}, \ldots, K_7^{\{256\}}$	0x428a2f98	0x71374491	0xb5c0fbcf	0xe9b5dba5	0x3956c25b	0x59f111f1	0x923f82a4	0xab1c5ed5
$K_8^{\{256\}}, \ldots, K_{15}^{\{256\}}$	0xd807aa98	0x12835b01	0x243185be	0x550c7dc3	0x72be5d74	0x80deb1fe	0x9bdc06a7	0xc19bf174
$K_{16}^{\{256\}}, \ldots, K_{23}^{\{256\}}$	0xe49b69c1	0xefbe4786	0x0fc19dc6	0x240ca1cc	0x2de92c6f	0x4a7484aa	0x5cb0a9dc	0x76f988da
$K_{24}^{\{256\}}, \ldots, K_{31}^{\{256\}}$	0x983e5152	0xa831c66d	0xb00327c8	0xbf597fc7	0xc6e00bf3	0xd5a79147	0x06ca6351	0x14292967
$K_{32}^{\{256\}}, \ldots, K_{39}^{\{256\}}$	0x27b70a85	0x2e1b2138	0x4d2c6dfc	0x53380d13	0x650a7354	0x766a0abb	0x81c2c92e	0x92722c85
$K_{40}^{\{256\}}, \ldots, K_{47}^{\{256\}}$	0xa2bfe8a1	0xa81a664b	0xc24b8b70	0xc76c51a3	0xd192e819	0xd6990624	0xf40e3585	0x106aa070
$K_{48}^{\{256\}}, \ldots, K_{55}^{\{256\}}$	0x19a4c116	0x1e376c08	0x2748774c	0x34b0bcb5	0x391c0cb3	0x4ed8aa4a	0x5b9cca4f	0x682e6ff3
$K_{56}^{\{256\}}, \ldots, K_{63}^{\{256\}}$	0x748f82ee	0x78a5636f	0x84c87814	0x8cc70208	0x90befffa	0xa4506ceb	0xbef9a3f7	0xc67178f2

Tableau 4 : les constantes de SHA-256

3.9 L'algorithme de SHA-256

SHA-256 est une fonction de hachage cryptographique (un algorithme) qui permet d'obtenir l'empreinte numérique d'un fichier. Cette empreinte est, en théorie, unique, et jamais deux contenus ne peuvent produire le même condensat. Corolaire : le condensat d'un contenu devrait être une signature unique de ce contenu [36]. L'algorithme peut être découpé en deux phases :

- Le prétraitement : le message est complété par remplissage comprenant la taille du message de façon à pouvoir le découper en blocs de 512 bits.
- Le calcul du condensé par itération de la fonction de compression sur la suite des blocs obtenus en découpant le message.

3.9.1 Les paramètres utilisés

Paramètre	Description
a, b, c..... h	variables de travail (en l'occurrence des mots de w bits), utilisées dans le calcul des hachés
H^(i)	la valeur de hachage n° i. H^(0) est la valeur initiale du hachage. H^(n) est la dernière valeur de hachage.
Hj^(i)	le mot (w bits) n° j de la valeur de hachage n° i, où H^(i) est le mot de poids le plus fort (à gauche) de la valeur de hachage i.
Kt	constantes itératives selon la valeur de t, utilisées dans le calcul de hachage.
K	nombre de 0 ajoutés au message lors du prétraitement (complément).
L	longueur du message M, en bits
M	nombre de bits contenus dans un bloc, soit 512
M	message à traiter
M^(i)	bloc n° i (m bits), du message M
Mj^(i)	mot (w bits) n° j, du bloc (m bits) n° i, du message M
N	nombre de bits de décalage ou de rotation à appliquer au mot quand associé à une fonction binaire

N	nombre de blocs de m bits contenus dans le message M après complément
T	variable temporaire, mot de w bits, utilisée dans le calcul de condensé
W	nombre de bits contenus dans un mot, soit 32 bits.
Wt	le mot n° t du tableau déduit du message.

Tableau 5 : les paramètres d'algorithme de SHA-256

- **Le mode de fonctionnement de la fonction de hachage :** Le calcul du hachage d'un message commence par la préparation du message :

- **Complétez le message de la manière habituelle** : supposons que la longueur du message M, en bits, soit `. Ajoutez le bit \ 1 « à la fin du message, puis k zéro bits, où k est la plus petite solution non négative de l'équation` + 1 + k = 448 mod 512. A cela est ajouté le bloc de 64 bits qui est égal au nombre écrit en binaire. Par exemple, le message (abc 8 bits) \ abc « a une longueur de 8 * 3 = 24 et est donc complété avec un, puis 448- (24 + 1) = 423 bits nuls, puis sa longueur pour devenir le message 512 bits rempli. La longueur du message complété devrait maintenant être un multiple de 512 bits.
- **Analyser le message :** en N blocs de 512 bits M puissance 1 jusqu'à M puissance n. Les premiers 32 bits du bloc de messages i sont notés M de range 0 puissance i, les 32 bits suivants sont M range 1 puissance i Nous utilisons la convention big-endian dans l'ensemble, de sorte que dans chaque mot de 32 bits, le bit le plus à gauche est stocké dans la position de bit la plus importante [35].

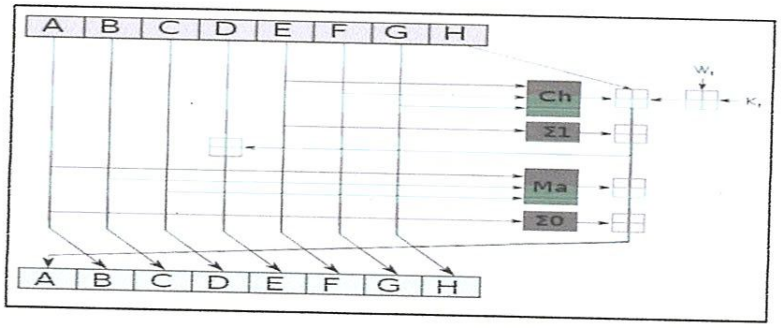

Figure 10 SHA-256

3.10 Conclusion

Dans ce chapitre on a conçu notre protocole d'authentification proposé avec la fonction de hachage pour l'initialisation des entités, l'initiateur et le répondeur, pour réalisé une conception de notre travaille.

Le prochain chapitre sera dédié à la simulation du protocole d'authentification proposé, afin d'accèdes à un résultat parfaitement.

4. Chapitre 04 : la simulation du protocole d'authentification proposé

4.1 Introduction

Dans ce chapitre, nous présentons une simulation de la conception déjà faite du protocole proposé, protocole d'authentification. En même temps nous présentons un outil très intéressant dans le domaine des protocoles de sécurité, ainsi que les tests de simulation et leurs résultats d' analyses.

4.2 Les outils de développement

Pour la simulation des protocoles de sécurité, la liste des suggestions des langages de simulation est aussi courte, chacune représente une technique de vérification différente.

Les outils de développements utilisés:

4.2.1 AVISPA :

AVISPA (Automated Validation of Internet Security Protocols and Applications) ou c'est la validation automatisée des protocoles et des applications de sécurité Internet en français, AVISPA est un outil utilisé pour la vérification de sécurité formelle des protocoles et des applications sensibles sur internet.

Il fournit un langage formel modulaire et expressif pour spécifier les protocoles et leurs propriétés de sécurité, et intégrer des différents back-end qui implémentent une variété de techniques d'analyse [37] :

- OFMC (vérification de modèle Onth-Fly) : le vérificateur de modèle à la volée.
- CL-ATSE (constraint-Logic Attack Searcher) : chercheur des attaques et contrôleur de modèle CL constraint-Logic.
- SATMC : vérificateur de modèle basé sur STA.
- TA4SP : Automate s d'arbres basés sur des approximations Automatiques pour l'Analyse de protocoles de Sécurité.

Le compteur de protocole interagit avec l'outil en spécifiant un problème de sécurité, il utilise le langage de spécification de protocole de haut niveau HLPSL.

Les quatre derniers outils de vérification utilisent un format intermédiaire (IF),

Dont la spécification écrite en HLPSL est traduite comme il est décrit dans la figure suivante.

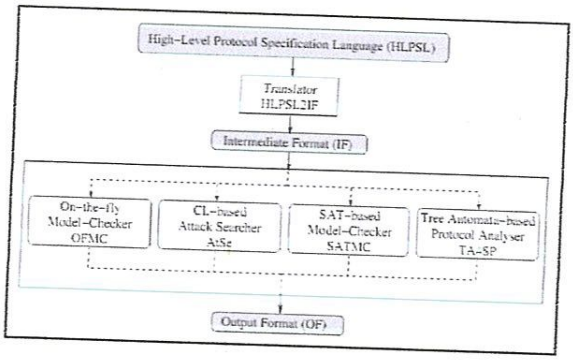

Figure 11 : Système d'architecture AVISPA [37]

4.2.2 Le langage HLPSL

HLPSL (high level protocoles specification langage) est utilisé pour implémenter les protocoles dans AVISPA. Ce langage est base sur les rôles :

- Rôles de base pour représenter chaque rôle de participant.
- Rôles de composition pour représenter des scénarios de rôles de base (rôle session, environnement).

Chaque rôle est indépendant des autres rôles, ce qui suppose des paramètres d'information initiaux et ensuite communique avec les autres rôles par les canaux. Dans HLPSL, l'intrus est toujours modélisé à l'aide du modèle Dolev-Yao, où modifier le contenu des messages transmis.

HLPSL prend en charge plusieurs types de base qui sont comme suit :

- Agent : il s'agit d'un nom principal. L'intrus est toujours supposé avoir l'identifiant spécial i.
- Public_key (Clé publique) : ce type représente les clé publiques des agents dans un système cryptographique a clé publique.
- Symmetric_key (clé symétrique) : elle représente les clés pour un système cryptographique a clé symétrique.
- Text : il est représente les nombres naturels dans les contextes sans message.
- Const : li représente les constantes.
- Nat : ce type représente les nombres naturels dans les contextes sans message.
- Hash_func : il s'agit d'une fonction de hachage cryptographique.la fonction de type base représente également des fonctions sur l'espace des messages. Il est supposé que l'intrus

- Simulation de protocole pour simuler le protocole et construire un MSC particulier correspondant à la spécification HLPSL.
- Simulation d'intrus pour simuler le protocole avec une intrus active/ passif.
- Simulation d'attaque pour la construction automatique d'attaques MSC à partir de la sortie des outils OFMC ou CL-ATSE.

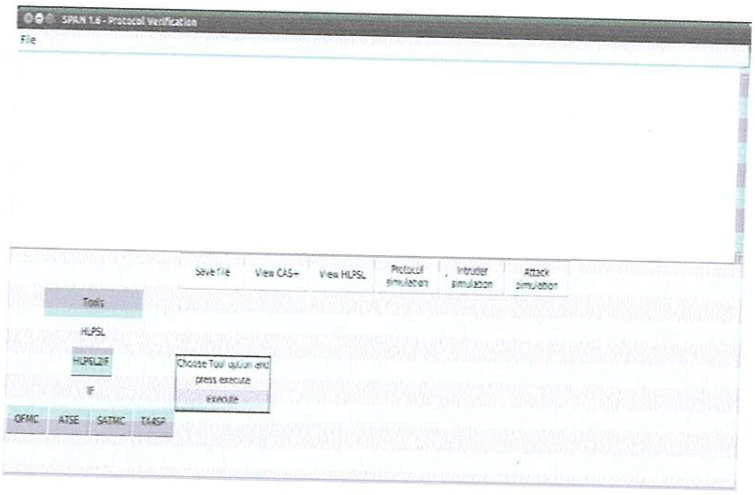

Figure 13 : interface SPAN AVISPA

Dans notre travail, nous allons exploiter SPAN AVISPA pour l'analyse OFMS et ATSE

4.2.4 L'installation :

Pour installer SPAN AVISPA, il utiliser Virtual Box pour réaliser premièrement la plate-forme linux(Ubuntu) et cela se fait gratuitement du site :

http://www.oracle.com/technetwork/server-storage/virtualbox/downlaods/index.html

Puis, nous avons mis une machine virtuelle linux Ubuntu, pour qu'on puisse importer l'application de SPAN AVISPA, qu'a déjà téléchargé de ce site :

http://people.irisa.fr/Thomas.Genet/span/#VDI

La figure suivante montre le SPAN AVISA après son importation :

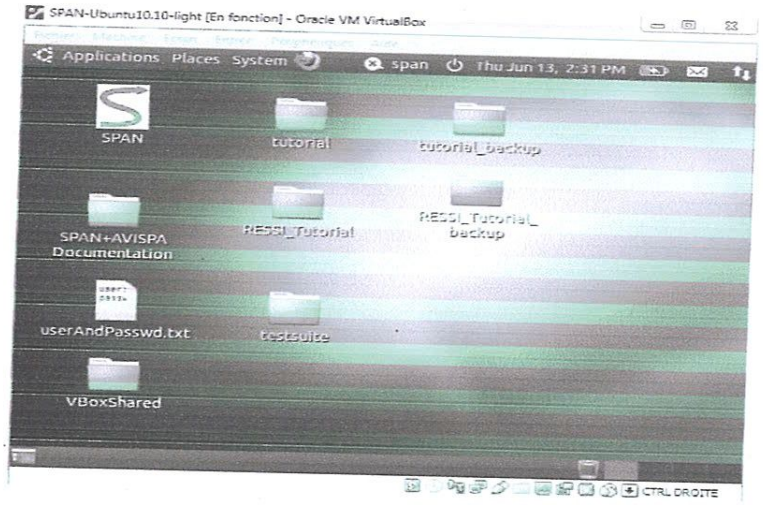

Figure 14 : SPAN AVISPA installé sur la plate-forme Linux (Ubuntu)

4.3 La simulation du protocole proposé

Dans cette section, nous simulons notre schéma d'authentification pour la vérification de sécurité à l'aide de l'outil AVISPA et montrons que notre protocole est sécurisé.

Dans la spécification de notre schéma qui sert à sécurisé un réseau électrique d'énergie et cela dans HLPSL nous avons l'implémenter pendant l'étape de l'authentification, en considérant que l'initiateur et le répondeur sont déjà enregistrés.

Dans la table suivante, nous avons listé tous les symboles utilisés sans la partie de simulation, chaque symbole avec sa description.

Le symbole dans la spécificatic	description
A	aPx (initiateur)
B	hx (répondeur)
F	Fonction de hachage
SK	clé de session
SA	Association de sécurité
NR	Nonce par aPx
NI	Nonce par hx
Kei	Echange de clés pour aPx
Ker	Echange de clés pour hx
DHX	Diffie-Hellman pour aPx
DHY	Diffie-Hellman pour hx
SND_A	Canal d'émetteur pour aPx
SND_B	Canal d'émetteur pour hx
RCV_A	Canal de Réception pour aPx
RCV_B	Canal de Réception pour hx
G	Variable
MA	Variable
MB	Variable

Tableau 6 : description des symboles utilisés

Alors « APx» et « Hx » et respectivement les rôles de base pour aPx et le hx, qui sont déclares comme suit :

```
Rolc aPx (A, B: agent,
   G: text,
    F: hash_func,
    SK: symmetric_key,
    SND_B, RCV_B: channel (dy))
Played_by A
Def=

 Local Ni, SA, DHX: text,
 Nr: text,
 KEr: message,
 CSK: hash (text.text.text.message),
 State: Nat,
     MA, MB: text

 Const sec_a_CSK: protocol_id

Init  State := 0
```

Figure 15 : déclaration d'initiateur aPx

```
Role hx (A, B: agent,
   G: text,
   F: hash_func,
   SK: symmetric_key,
   SND_A, RCV_A: channel (dy))
Played_by B
Def=

 Local Ni, SA: text,
 Nr, DHY: text,
 KEi: message,
 CSK: hash (text.text.text.message),
 State: Nat,
    MA, MB: text

 Const sec_b_csk: protocol_id

Init State := 1
```

Figure 16 : déclaration de répondeur hx

- Dans la déclaration des rôles de base « aPx »et « hx » on trouve les agents qui sont en interaction avec le rôle déclaré comme ici (A, B), A représente le rôle du aPx et le B représente le rôle de hx.
- La déclaration play_by A indique que l'agent nommé ou qu'on est en train de définir est manipulé par la variable A de type agent, la mémé chose que l'autre rôle.
- Si une variable doit être gardée secrète en permanence, elle est exprimée par le secret de but « secret » avec son identificateur et les agents que ce secret est claie pour eux.
- Les variables suives de « ' » Dénote une nouvelle valeur de ce variable comme crie dans les code suivants.
- Si vous envoyez une ancienne valeur dans les canaux SND_A et SND_B, n'amorcez pas la variable
- Dans les canaux RCV_A RCV_B, si vous recevez une nouvelle valeur, la variable utilisée pour stocker cette valeur doit être amorcée.
- Lors de l'utilisation de témoin et de requête, le troisième argument est un identifiant de type protocol_id déclaré dans le rôle de niveau supérieur. Ceci est utilisé pour associer les prédicats témoin et pour y faire la référence dans la section des objectifs, comme il est montré dans les codes suivants. Le témoin de déclaration witness (A, B, ni, Ni') indique que A à récemment généré un nombre après la construction de premier message aléatoire

pour B et le témoin déclaration de déclaration witness (B, A, ni, Ni') indique que B à récemment généré un nombre Après la construction de premier message aléatoire pour A.

- Le variable CSK' indique la création d'une nouvelle valeur de SA en fonction d'une fonction de hachage F.
- Une valeur locale doit recevoir une valeur avant la première lecture ou envoi, c'est ce qui a été fait dans la déclaration des rôles sur le variable stat initialisé par 0 et ensuite par 1.

```
Transition

 1. State = 0 /\ RCV_B (start) =|>
State':= 2  /\ SA' := new ()
            /\ Ni' := new ()
            /\ DHX' := new ()
            /\ SND_B ( {SA'.Ni'.exp(G,DHX')}_SK )
     /\ witness (A, B, ni, Ni' )

 2. State = 2  /\ RCV_B({SA. Nr'.KEr'}_SK) =|>
      State':= 4 /\ MA' := new ()
            /\ CSK' := F (Ni. Nr'.SA.exp (KEr', DHX))
            /\ SND_B ( {MA'.zero}_CSK' )

 4. State = 4  /\ RCV  B({MB'.one}  CSK) =|>
   State':= 6  /\ request (A, B, nr, Nr)
            /\ secret (CSK, sec  a  CSK, {A, B})
      End rolc
```

Figure 17 : les messages Relatifs à l'initiation aPx

```
      Transition
1. State = 1  /\ RCV_A ({SA'.Ni'.KEi'}_SK ) =|>
State':= 3       /\ Nr' := new ()
                 /\ DHY' := new ()
                 /\ CSK' := F (Ni'.Nr'.SA'.exp (KEi', DHY'))
                 /\ SND_A ( {SA'.Nr'.exp(G,DHY')}_SK )
       /\ witness (A, B, nr, Nr')

     2. State = 3  /\ RCV_A ( {MA'.zero}_CSK ) =|>
       State':= 5 /\ MB' := new ()
            /\ SND_A ({MB'.one}_CSK )
    /\ request (B, A, ni, Ni)
            /\ secret (CSK, sec_b_csk,{A,B})

     End role
```

Figure 18 les messages Relatifs à l'initiation aPx

Enfin, les implémentations des rôles pour la session, et l'objectif « goal » et l'environnement pour notre protocole sont fournies dans ce qui suit :

```
Role session (A, B: agent,
      SK: symmetric_key,
      G: text,
      F: hash_func)
Def=

 Local SAC, RA, SB, RB: channel (dy)

 Composition
   aPx (A, B, G, F, SK, SAC, RA)
 ∧ hx (B, A, G, F, SK, SB, RB)
End role
```

Figure 19 : codification de rôle session

```
Role environnent ()
Def=

 Const ni, nr        : protocol_id,
A, b          : agent,
      Kab, Kai, kbi : symmetric_key,
      g             : text,
      F             : hash_func,
      Zero, one     : text

 Intruder_knowledge = {g, f, a, b, i, Kai, kbi, zero, one}
Composition

Session (a, b, kab, g, f)
   ∧ session (a, b, kab, g, f)
∧session (a, b, kab, g, f)

end role
```

Figure 20: codification de rôle environnent

Dans la déclaration d'objectif de notre travaille, nous avons identifié le surcuit par la variable le répondeur et l'initiateur par les deux variable « sec_a_csk » et « sec_b_csk ».e en plus l'authentification sur ni et nr.

```
Goal

Secrecy_of sec_a_CSK, sec_b_csk
Authentication_on nr
Authentication_on ni

End goal
Environnent ()
```

Figure 21: codification du goal

4.4 Les résultats

Pour OFMC et CL-ATSE, les résultats de la simulation pour la vérification de sécurité formelle de schéma proposé, garantissent qu'il est sécurisé, en plus l'AVISPA a déclaré que les attaques sont peu concluantes contre notre protocole.

Les figures suivantes présenté les résultats sur AVIPA pour les trois tests Mentionné ci-dessus.

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/PROTOCOLIKEV2.if
GOAL
  As_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  ParseTime: 0.00s
  SearchTime: 0.59s
  VisitedNodes: 264 nodes
Depth: 10 plies
```

Figure 22 : analyse selon OFMC

```
SUMMARY
 SAFE

DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
 TYPED_MODEL

PROTOCOL
 /home/span/span/testsuite/results/PROTOCOLIKEV2.if

GOAL
 As Specified
```

Figure 23 : analyse selon CL-ATSE

4.5 Sécurité contre l'attaque MITM (main in the middle Attack)

Dans cette attaque les données de consommation d'énergie peuvent être modifiées avant la transmission des messages. Aussi, en écoutant le canal de communication sans fil, un attaquant pourrait obtenir les informations échangées entre les compteurs intelligents et le centre de contrôle. Son attaque est d'une validité discutable, car l'intrus n'a pas réellement appris la clé. Ainsi, l'intrus ne peut pas exploiter le défaut d'authentification à d'autres fins. L'attaque peut être exclue si nous ajoutons une confirmation de clé au protocole. Autrement dit, si nous étendons le protocole pour inclure les messages dans lesquels la clé traduite est réellement utilisée

4.6 Sécurité contre l'attaque de rejouer (replay Attack)

Pour lancer une telle attaque, l'adversaire doit (aPx) capturer et analyser les données transmises entre les appareils et les compteurs intelligents afin d'obtenir les caractéristiques de consommation énergétique du client, et (hx) fabriquer et injecter de faux signaux de contrôle dans le système. L'attaque par rejouer a pour objectif: (aPx) de voler de l'énergie en détournant le courant vers un autre emplacement, et (hx) d'endommager physiquement le système.

4.7 Conclusion

Dans ce chapitre nous avons simulé la conception du protocole proposé dans le chapitre précédent, en utilisant AVISPA Tool qui s'impose dans la sécurité informatique grâce à ca performance pour juger et prouver les protocoles par les chercheurs. Nous avons présenté la simulation correspondante, et les résultats par AVISPA Tool qui sont OFMC et CL-ATSE étaient positifs ce qui aboutit à ne pas pouvoir simuler deux type d'attaque, main in the middle attack et le replay attaque.

Conclusion générale

Conclusion générale

Dans ce projet de fin d'études, nous avons abordé le problème d'authentification pour l'internet de l'énergie (IoE), et nous avons proposé un protocole d'authentification d'un système pour les réseaux intelligents. Un réseau intelligent, communément appelé système d'alimentation de prochaine génération, est un système révolutionnaire et en évolution pour les réseaux existant.

Le protocole proposé est basé sur l'intégration de la technologie informatique et de communication avancées. Par ailleurs, nous avons validé notre protocole proposé en utilisant AVISPA, ce qui signifie la validation automatisée des protocoles et des applications de sécurité internet.

- **Sur le plan méthodologique :** Je me suis familiarisée avec AVISPA, ainsi que le langage HLPSL, qui m'ont servi pour réaliser mon travail.
- **Sur le plan scientifique :** J'ai appris la validation d'un protocole, j'ai aussi pu connaitre le peu d'un vaste domaine, le domaine des réseaux intelligents, d'après tout les articles que j'ai lu aussi que les livres. Cela a pu enrichir mes connaissances.
- **Sur le plan pratique :** J'i approfondi mes connaissances opérationnelles par la maitrise du domaine des réseaux intelligents, ainsi que les systèmes d'authentifications

Finalement, on peut déduire que les réseaux intelligents et les systèmes d'authentifications devraient améliorer l'efficacité et la liabilité des sources d'énergie distribuées, et de satisfaire la demande des utilisateurs.

Acronymes

Table des acronymes

L'acronyme	Définition
TIC	Technologie de l'information et de la communication
LOE	Internet of énergie
NIST	National Institute standards and Technology
AMI	Advance metering infrastructure
AMR	Automatic metering Reading
LOT	Internet of things
EI	Internet énergie
IP	Internet protocole
SCADA	Système de contrôle et d'acquisition de données
EAP-IKV2	The extensible Authentication Protocol internet Key exchange Protocol version 2
HMAC	Code d'authentification de message haché
MD5	Message digest 5
MD4	Message digest 4
SHA	Source hash algorithme
WALAN	Wireless local area network
IEEE	Institute of Electrical and Electronics Engineers
SG	Smart Grid

Références

Bibliographie

1. Le, T. N., Chin, W. L., & Chen, H. H. (2016). Standardization and security for smart grid communications based on cognitive radio technologies—A comprehensive survey. IEEE Communications Surveys & Tutorials, 19(1), 423-445.

2. Bera, S., Misra, S., & Rodrigues, J. J. (2014). Cloud computing applications for smart grid: A survey. IEEE Transactions on Parallel and Distributed Systems, 26(5), 1477-1494.

3. Komninos, N., Philippou, E., & Pitsillides, A. (2014). Survey in smart grid and smart home security: Issues, challenges and countermeasures. IEEE Communications Surveys & Tutorials, 16(4), 1933-1954.

4. Rehmani, M. H., Reisslein, M., Rachedi, A., Erol-Kantarci, M., & Radenkovic, M. (2018). Integrating renewable energy resources into the smart grid: Recent developments in information and communication technologies. IEEE Transactions on Industrial Informatics, 14(7), 2814-2825.

5. Aloul, F., Al-Ali, A. R., Al-Dalky, R., Al-Mardini, M., & El-Hajj, W. (2012). Smart grid security: Threats, vulnerabilities and solutions. International Journal of Smart Grid and Clean Energy, 1(1), 1-6.

6. Baimel, D., Tapuchi, S., & Baimel, N. (2016). Smart grid communication technologies. Journal of Power and Energy Engineering, 4(08), 1.

7.https://www.researchgate.net/profile/Jaekel_Arunita/publication/274921915/figure/fig1/AS:320260059222017@1453367356309/An-example-of-communication-architecture-in-smart-grid.png

8. (s.d.). https://www.researchgate.net/profile/Thinagaran_Perumal/publication/23. [En ligne] .consulté le 5 mai 2019.

9.https://www.researchgate.net/profile/Sajid_Qazi/publication/285630227/figure/fig1/AS:304186345443328@1449535084277/Conceptual-model-of-smart-grid.png.

Références

10. (s.d.). https://www.researchgate.net/profile/Neetesh_Saxena/ System-model-for-AMI-network-in-the-smart-grid.png. [En ligne].consulté le 25 mai 2019.

11. Fang, X., Misra, S., Xue, G., & Yang, D. (2011). Smart grid—The new and improved power grid: A survey. IEEE communications surveys & tutorials, 14(4), 944-980.

12. (s.d.). https://www.futura-sciences.com/planete/questions-reponses/energie-renouvelable-smart-grid-gere-t-il-consommation-electricite-4137/.consulté le 7mail 2019 .

13. (s.d.). http://www.smartgrids-cre.fr/index.php?p=definition-smart-grids consulté le 14 mais 2019.

14. Lu, X., Wang, W., & Ma, J. (2012). Authentication and integrity in the smart grid: An empirical study in substation automation systems. International Journal of Distributed Sensor Networks, 8(6), 175262.

15. Metke, A. R., & Ekl, R. L. (2010). Security technology for smart grid networks. IEEE Transactions on Smart Grid, 1(1), 99-107

16. Yan, Y., Qian, Y., Sharif, H., & Tipper, D. (2012). A survey on smart grid communication infrastructures: Motivations, requirements and challenges. IEEE communications surveys & tutorials, 15(1), 5-20.

17. Moslehi, K., & Kumar, R. (2010). A reliability perspective of the smart grid. IEEE Trans. Smart Grid, 1(1), 57-64.

18. (s.d.). https://www.syloe.com/glossaire/authentification/.consulté le mai 2019

19. (s.d.). https://www.lemagit.fr/definition/Authentification/ consulté le 15 mai 2019

20. Cédric Llorens, L. a. Tableaux de bord de la sécurité réseaux .consulté 4 avril 2019

21. Lu, Z., Lu, X., Wang, W., & Wang, C. (2010, October). Review and evaluation of security threats on the communication networks in the smart grid. In 2010-MILCOM 2010 MILITARY COMMUNICATIONS CONFERENCE (pp. 1830-1835). IEEE.

Références

22. Sörries, B. (2013). Communication technologies and networks for Smart Grid and Smart Metering. Rapport for CDG 450 Connectivity Special Interest Group (450 SIG).

23. Ferrag, M. A., Maglaras, L. A., Janicke, H., Jiang, J., & Shu, L. (2018). A systematic review of data protection and privacy preservation schemes for smart grid communications. Sustainable cities and society, 38, 806-835.

24. Tan, S., De, D., Song, W. Z., Yang, J., & Das, S. K. (2017). Survey of security advances in smart grid: A data driven approach. IEEE Communications Surveys & Tutorials, 19(1), 397-422.

25. Song, Y., Lin, J., Tang, M., & Dong, S. (2017). An Internet of energy things based on wireless LPWAN. Engineering, 3(4), 460-466.

26. Wang, K., Hu, X., Li, H., Li, P., Zeng, D., & Guo, S. (2017). A survey on energy internet communications for sustainability. IEEE Transactions on Sustainable Computing, 2(3), 231-254.

27. (s.d.). https://csdl-images.computer.org/trans/su/2017/03/figures/li1-2707122.gif. consulté le 9 juil 2019

28. Ferrag, M. A., Maglaras, L. A., Janicke, H., Jiang, J., & Shu, L. (2017). Authentication protocols for Internet of Things: A comprehensive survey. Security and Communication Networks, 2017.

29. Wang, K., Hu, X., Li, H., Li, P., Zeng, D., & Guo, S. (2017). A survey on energy internet communications for sustainability. IEEE Transactions on Sustainable Computing, 2(3), 231-254.

30. B. Aboba, L. B. (2004). Extensible Authentication Protocol (EAP).

Références

31. H. Tschofenig, D. K. (2008). The Extensible Authentication Protocol-Internet Key Exchange Protocol.

32 .(s.d.). sans technology institute:https://www.sans.edu/cyber-researchsecurity-.

33. (consulté mai 2019). tutorialsPoint:http://www.tutorials.com/cryptography_hash_function.hml. cryptography hash function.

34.Ghassan A. Abed, M. I. (2012). The Evolution to 4G Cellular Systems: Architecture and Key Features of LTE-Advanced Networks. International Journal of Computer Networks and Wireless Communications , 22.

35.(consulté le mai 2019). https://fr.wikipedia.org/wiki/SHA-2.

36.(consulté mai 2019). https://assiste.com/SHA-256.html. 11 5 .

37. Luca Vigan. (2006). Automated Security Protocol Analysis. Electronic Notes in Theoretical Computer Science .

38..P. Eronen, P. H. (2006). ,. IKEv2 Clarifications and Implementation Guidelines. .

39.C. Kaufman, P. H. (2010). Internet Key Exchange Protocol Version 2 (IKEv2) .

40. Baig, Z. A., & Amoudi, A. R. (2013). An analysis of smart grid attacks and countermeasures. Journal of Communications, 8(8), 473-479.

41. H. Nicanfar, P. Jokar, K. Beznosov, and V. C. M. Leung, "Efficient authentication and key management mechanisms for smart grid communications," IEEE Systems Journal, vol. 8, no. 2, pp. 629–640, 2014.

42. C. Lyu, D. Gu, Y. Zeng, and P. Mohapatra, "PBA: Prediction-Based Authentication for Vehicle-to-Vehicle Communications," IEEE Transactions on Dependable and Secure Computing, vol. 13, no. 1, pp. 71–83, 2016.

43. T. W. Chim, S.-M. Yiu, V. O. Li, L. C. Hui, and J. Zhong, "PRGA: Privacy-Preserving Recording amp; Gateway-Assisted Authentication of Power Usage Information for Smart Grid," IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 1, pp. 85–97, 2015.

Références

44. K. Mahmood, S. Ashraf Chaudhry, H. Naqvi, T. Shon, and H. Farooq Ahmad, "A lightweight message authentication scheme for Smart Grid communications in power sector," Computers Electrical Engineering, vol. 52, pp. 114–124

45. M. M. Fouda, Z. M. Fadlullah, N. Kato, R. Lu, and X. S. Shen, "A lightweight message authentication scheme for smart grid communications," IEEE Transactions on Smart Grid, vol. 2, no. 4, pp. 675–685, 2011.