UNIVERSITÉ DU QUÉBEC

MÉMOIRE PRÉSENTÉ À
L'UNIVERSITÉ DU QUÉBEC À TROIS-RIVIÈRES

COMME EXIGENCE PARTIELLE DE

LA MAITRISE EN MATHÉMATIQUES ET INFORMATIQUE

APPLIQUÉES

PAR RABAB BENELKAID

UTILISATION DES CLOUDLETS DE CONFIANCE POUR AMÉLIORER LA SÉCURITÉ DES RESEAUX V2G

Février 2023

Résumé

La croissance démographique exponentielle a poussé les gens à l'expansion urbaine, elle a été accompagnée d'une énorme augmentation de machines et de véhicules, engendrant une grande consommation d'énergie et une émission énorme de déchets gazeux des diverses industries. Cela a eu un impact négatif sur la nature qui s'est reflété sur la population et a dégradé la qualité de vie sur terre.

Pour cette raison, plusieurs chercheurs se sont précipités pour trouver une solution afin de créer un équilibre entre la croissance rapide et l'environnement. Les chercheurs ont constaté que les émissions émises par les voitures jouent un rôle majeur dans la pollution. Ils ont pensé à créer des voitures dégageant moins ou pas de gaz d'échappement, d'où l'idée des véhicules électriques est arrivée. Ces dernières années, ce marché a connu aussi un développement matériel et technologique remarquables qui a incité même les gouvernements à encourager et à financer leur achat et leur commercialisation. D'autre part, les gouvernements ont encouragé les équipes de recherche à trouver des solutions aux problèmes de sécurité électroniques résultant de l'augmentation importante de l'acquisition notoirement élevée des appareils électroniques en général et des véhicules électriques en particulier. De notre côté, nous allons proposer une amélioration d'une solution aux règlements de ces problèmes.

Suite à une étude de l'état de l'art, nous sommes arrivés avec une proposition d'une infrastructure centralisée sur le cloud, afin de mieux gérer les différentes entités du réseau des véhicules électriques et assurer un certain niveau de sécurité de la vie privée, d'anonymat et de confidentialité. Notre solution introduit un bit pour chaque véhicule électrique (VE) enregistré sur le réseau électrique afin de renforcer sa confidentialité et son anonymat. Ce dernier mentionne si le VE est connecté ou non à un instant donné. Nous avons évalué notre protocole en utilisant le logiciel de vérification et de validation Tamarin Prover et nous avons montré qu'il résiste à plusieurs attaques de sécurité dans le réseau,

telles que l'usurpation d'identité, attaque de relecture (rejeux), désynchronisation, l'Homme au Milieu, contre identification du mot de passe hors ligne, ...etc.

Rabab Benelkaid

Boucif Amar Bensaber

Abstract

The exponential population growth pushed people to urban expansion, it was accompanied by a huge increase in machinery and vehicles, resulting in a large consumption of energy and a huge emission of gaseous waste from various industries and of varying gravity, this had a negative impact on nature which was reflected on the population and degraded the quality of life on earth.

For this reason, research centers around the world have rushed to find a solution to create a balance between rapid growth and the environment. Researchers have found that emissions from cars play a major role in pollution. They thought about creating cars with no or less toxins, which is where the idea of electric vehicles came from. In recent years, this market has also experienced remarkable material and technological development that has prompted even governments to encourage and finance their purchase and marketing. On the other hand, to encourage research teams to find solutions to electronic security problems resulting from the significant increase in the notoriously high acquisition of electronic devices in general and especially electric vehicles. In turn, we have assumed our share of responsibility and worked hard to contribute to these solutions.

Following a state of art study, we came up with a proposal for a centralized infrastructure on the cloud, in order to better manage the various entities of the electric vehicle network and ensure a certain level of privacy security, anonymity and confidentiality. We also proposed to introduce a bit for each electric vehicle (EV) registered on the electrical network and a timestamp for each sent message to reinforce its confidentiality and anonymity, this mentions if the EV is connected or not at this moment. We have evaluated our protocol by Tamarin Prover verification and validation software, and we have shown that it is resistant to several security attacks in the network, such as impersonation, replay, desynchronization, Man in the Middle, offline password guessing, etc.

Remerciement

Je remercie tout d'abord, Dieu, le tout puissant de m'avoir donné le courage, la force et la patience d'achever ce modeste travail.

Je tiens à remercier mon directeur de mémoire, le professeur Boucif Amar Bensaber, pour sa patience, sa disponibilité et surtout ses judicieux conseils, qui ont contribué à améliorer ma réflexion. Je suis toujours honorée et reconnaissante d'avoir travaillé avec lui.

Je tiens à remercier mes professeurs Ismail Biskri, Mhamed Mesfioui et François Meunier d'avoir accepté d'évaluer mon travail et pour leurs commentaires et suggestions.

Je remercie également toute l'équipe pédagogique de l'Université du Québec à Trois-Rivières et les intervenants professionnels responsables de ma formation, pour avoir assuré la partie théorique de celle-ci.

Enfin, je tiens à témoigner ma gratitude à mon mari, mes parents et mes petits anges ; DARINE et ABDESSALEM ; pour leur soutien inestimable.

Table des matières

Liste des figures

Liste des tableaux

Nomenclature

5G	Fifth Generation
AWS	Amazon Web Services
BSM	Basic Safety Message
CA	Certification Authority
CS	Charging Station
DoS	Denial of Service
DSRC	Dedicated Short Range Communications
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
EV	Electric Vehicle
EVCC	Electric Vehicle Communication Controller
EVO	Electric Vehicle Owner
EVSE	Electric Vehicle Supply Equipment
EXI	Efficient XML Interchange
GPS	Global Positioning System
ID	Identifier
IoT	Internet of Things
ISO	International Organization for Standardization
LAG	Local Aggregator
LTE	Long-Term Evolution
mmWave	Millimeter Wave

NOx	Nitrogen Oxides
PKI	Public Key Infrastructure
RSA	Rivest–Shamir–Adleman
SASD	Identity-based Sequential Aggregate Signed Data
SCMS	Security Credential Management System
SECC	Supply Equipment Communication Controller
SG	Smart Grid
USDOT	United States Department of Transportation
VANET	Vehicle ad hoc Network
V2G	Vehicle-To-Grid
V2I	Vehicle-To-Infrastructure
V2V	Vehicle-To-Vehicle
WAVE	Wireless Access for the Vehicular Environment
Wifi	Wireless Fidelity
XML	Extensible Markup Language

Chapitre 1 : Introduction

Notre planète est trop chère ! L'évolution technologique ne cesse de la détruire. Les industries et les véhicules routiers consomment beaucoup d'énergie et émettent des gaz à effet de serre. Pour cela, les scientifiques cherchent continuellement à diminuer la pollution. Dans le domaine de l'énergie, ils ont développé des systèmes à base électrique qui remplacent les composants qui se brûlent, notamment dans les transports. Cette transition mène à l'apparition des réseaux véhiculaires comprenant un grand nombre de véhicules connectés. Cependant, cela a conduit à l'apparition d'autres problèmes de sécurité, de connectivité et de débit**.**

En outre, pour clarifier le concept de réseau intelligent dans un système électrique, une nouvelle définition d'un réseau électrique intelligent dans le secteur de la distribution d'énergie est élaborée en tenant compte des effets des réseaux véhiculaires électriques (V2G). Ce concept développé précise que la pénétration des V2G constitue en fait une opportunité de mise en œuvre de la distribution d'énergie intelligente en proposant des stockages d'énergie renouvelables, une communication bidirectionnelle et des injections de puissance réactive et active sur le réseau. En fait, les véhicules électriques (EV) réduisent les émissions de gaz carbonique (CO2) et d'oxides de nitrogène (Nox) et augmentent l'efficacité énergétique en utilisant des générations distribuées (DG) dans le secteur des transports [1].

De plus, le cloud computing, l'informatique de pointe intelligente, le protocole de communication mmWave, le réseau neuronal et d'autres technologies appliquées à l'Internet des véhicules peuvent non seulement améliorer le débit de données et la précision de positionnement, réduire les délais bout en bout, mais également améliorer les performances de sécurité et la qualité de service des véhicules électriques [2].

Le gouvernement du Québec offre un rabais à l'achat ou à la location aux particuliers, aux entreprises, aux organismes et aux municipalités du Québec qui souhaitent faire l'acquisition d'un véhicule électrique neuf admissible. Ce rabais peut atteindre **8 000 $** si le

véhicule est entièrement électrique ou pour un véhicule à pile à combustible (véhicule à hydrogène)**,** entre **500 $** et **8 000 $** si le véhicule est hybride rechargeable selon la capacite de la batterie électrique, **2 000 $** pour une motocyclette électrique et **500 $** pour une motocyclette à vitesse limitée électrique (scooters électriques). Le prix du véhicule doit être inférieur à **60 000 $** [3].

Un réseau véhiculaires électriques (V2G) est composé de plusieurs entités : le réseau électrique, les agrégateurs [4] qui gèrent et contrôlent les véhicules électriques (VE) et qui sont les intermédiaires entre les VEs et les compagnies d'électricité/les marchés de l'électricité, les bornes de recharge (CS), les véhicules électriques (VE) et les propriétaires de VE (EVO) [5]. Aussi, les menaces de sécurité ne cessent de s'intensifier et de se diversifier. Elles touchent toute entité du réseau électrique, partant de la plus haute entité jusqu'à la vie privée de l'utilisateur du véhicule électrique, la confidentialité de ses informations financières et sociales et elles peuvent mener à sa propriété privée comme sa maison et sa famille, elles peuvent même nuire à ses vacances en interceptant ses déplacements.

Afin de contribuer aux efforts déployés au développement du réseau véhiculaires électriques (V2G) et renforcer sa sécurité et sa fiabilité et celles de ses utilisateurs et de notre planète, nous avons proposé une architecture V2G sur le Cloud. Elle ressemble, dans sa composition, aux architectures existantes avec plus de moyens en termes d'outils matériels, technologiques et de sécurité afin de combler les défis actuels et les limitations matérielles et logicielles du réseau électrique. Nous avons essayé d'améliorer l'aspect de la confidentialité et de l'anonymat, en reposant sur une nouvelle définition de cette dernière, qui autorise une seule connexion pour un véhicule électrique à un instant donné [6]. Nous avons proposé l'attribution d'un bit au véhicule électrique pour mentionner s'il est connecté ou non, en utilisant l'authentification hybride de l'architecture à clé publique (PKI) avec cryptographie SCS très rapide basée sur les courbes elliptiques (ECC). Les Autorités et les agrégateurs ont été proposés sur le cloud pour qu'on puisse profiter aux maximums des services de stockage, de mémoire, de gestion de sécurité et de localisation par rapport aux utilisateurs, aux stations de recharge et autres fournisseurs de service, et aussi, afin de décharger les autorités de certification (CA) de plusieurs tâches de gestion,

rendant ainsi le réseau V2G plus efficace, plus sécurisé, extensible, redondant et mondiale (sans frontières).

Le processus global de notre proposition suit les phases suivantes : 1) Initialisation du système, 2) Enregistrement, 3) Authentification mutuelle avec le cloudlet, 4) Demande de service et, 5) Authentification mutuelle avec la borne de recharge et chargement/déchargement. Nous supposons que les éléments du réseau comme les cloudlets (agrégateurs) et les bornes de recharge (CSs) sont déjà enregistrés aux systèmes dès leur installation.

Notre proposition, assure la haute disponibilité du réseau électrique, en réglant, par la redondance, le problème de l'architecture CA Bridgé décrit dans le chapitre 3. Elle offre une authentification anonyme entre le véhicule électrique, l'agrégateur et la centrale de certification (CA).

Aussi, notre proposition résout le problème de l'interopérabilité en divisant le réseau en plusieurs zones. Chaque zone est dirigée par un cloudlet (agrégateur), qui échange ses informations avec l'autorité la plus proche. Elle assure, ainsi, la révocabilité, la traçabilité et la non-répudiation. Ainsi, elle protège contre l'attaque d'usurpation d'identité, l'homme du milieu, l'attaque de désynchronisation, de relecture, d'initié privilégié, de contre identification du mot de passe hors ligne et de vol de carte à puce.

La suite de ce mémoire se présente comme suit, le chapitre 2 introduit les réseaux véhiculaires électriques (V2G) modernes, les modèles, les architectures cloud, les infrastructures à clé publique (PKI) et les différentes menaces de sécurité existantes. Le chapitre 3 consiste en une revue de littérature sur les cloudlets de confiance dans les réseaux VANETs (Vehicle Adhoc Network), le standard ISO 15118, la sécurité au sein des grilles intelligentes, et les différentes solutions proposées pour remédier aux problèmes de sécurité. Le schéma de notre solution est proposé au chapitre 4. Nous présentons, dans le chapitre 5, l'analyse des résultats de la modélisation de notre protocole avec l'outil Tamarin Prover en mentionnant les défis relevés. Enfin, au chapitre 6, nous présentons une conclusion générale.

Chapitre 2 : Les réseaux V2G modernes

2.1 Introduction

Les réseaux véhiculaires électriques (V2G) gagnent actuellement en importance alors que l'attention mondiale se tourne vers la production d'énergie électrique propre [7]. Dans ce chapitre, nous allons présenter les principales unités d'une communication V2G : les acteurs, la communication entre eux et les différents défis sécuritaires.

2.2 Acteurs

D'après le standard ISO 15118-1, il existe plusieurs acteurs primaires et secondaires comme illustré dans la figure ci-après.

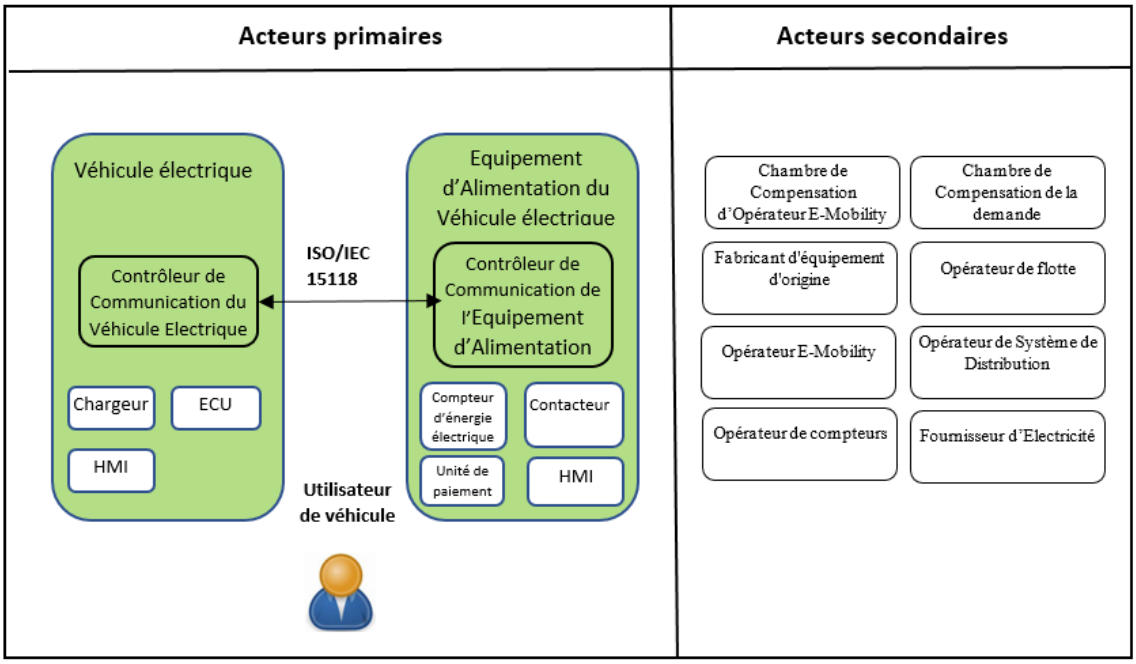


Figure 1 : Acteurs primaires et secondaires [ISO 15118-1]

2.2.1 Acteurs primaires

Les acteurs primaires sont des entités qui interagissent directement dans l'opération de charge / décharge.

Véhicule électrique (VE)

Tout véhicule propulsé par un moteur électrique tirant le courant d'une batterie d'accumulateur rechargeable qui est principalement fabriqué pour être utilisé sur les rues publiques, routes ou autoroutes **[ISO 15118-1]**, aussi, mené d'une interface homme-machine et d'un contrôleur **EVCC (**Electric Vehicle Communication Controller).

Borne de recharge (EVSE : Electric Vehicle Supply Equipment**)**

Les conducteurs, les coupleurs **VE**, les fiches connectées et tous les autres accessoires, appareils, prises de courant ou appareils installés spécifiquement dans le but de fournir l'énergie du câblage des locaux au **VE** et de permettre la communication entre eux si nécessaire **[ISO 15118-1]**. Il a un contrôleur **SECC (**Supply Equipment Communication Controller**)** avec lequel il communique.

2.2.1 Acteurs secondaires

Ce sont des entités qui interagissent d'une manière indirecte dans le processus de charge et de décharge. On trouve :

a) La chambre de Compensation d'Opérateur E-Mobility (**EMOCH)**, b) la chambre de compensation de la demande **(DCH)**, c) le fabricant d'équipement d'origine **(OEM)**, d) l'opérateur de flotte **(FO)**, e) l'opérateur E-Mobility **(EMO)**, f) l'opérateur de Système de distribution **(DSO)**, g) l'opérateur de compteurs **(MO) et** h) le fournisseur d'électricité **(EP) [ISO 15118-1]**.

Nous allons discuter principalement des acteurs primaires qui sont les éléments essentiels d'une communication sur un réseau V2G.

La communication entre le véhicule électrique (EV) et la borne de recharge (EVSE) se fait par des messages selon le modèle de données et le format de représentation des données basé sur XML / EXI **[ISO 15118-2].**

2.3 Menaces de sécurité

La grille intelligente (SG) est, sans aucun doute, la future infrastructure électrique du monde de l'énergie [8]. Elle est destinée pour répondre aux besoins des différents types d'utilisateurs. Ces derniers doivent lui fournir des informations et des données personnelles qui peuvent être critiques et qui, par conséquent, doivent être protégées de toutes sortes de dévoilement, de vol, d'usurpation, ...etc.

La sécurité est considérée comme l'un des défis majeurs des systèmes actuels constituant la grille intelligente en raison de sa communication longue portée sur des réseaux ouverts. Les cybercriminels, les pirates informatiques, les terroristes tentent d'attaquer cette infrastructure nationale en raison de leurs intentions malveillantes ou de prendre le contrôle de la surveillance automatisée de l'énergie et du contrôle à distance pour des gains personnels. La caractéristique de la communication bidirectionnelle entre le consommateur et le système de service électrique dans le réseau intelligent est de faciliter le système de réponse à la demande, les sources d'énergie distribuées, les composants télécommandés avec vérifications des pannes, la capacité à s'auto-guérir en cas de pannes ou de bogues et la sécurité contre les attaques physiques et informatiques. Les objectifs de la cybersécurité sont de protéger la communication et les données opérationnelles dans les réseaux intelligents conformément aux règles de la centrale de certification (CA), à savoir la confidentialité, l'intégrité et la disponibilité. Les cybercriminels et les attaquants ont un haut niveau de connaissance des systèmes et sont technologiquement bien formés pour perturber l'intégrité, la confidentialité et la disponibilité des services. La responsabilité de protéger les infrastructures critiques contre les cyber-terroristes et les pirates informatiques incombe non seulement aux opérateurs de services publics, aux ingénieurs et aux chercheurs, mais également aux gouvernements et aux consommateurs d'électricité [8].

Protéger la vie privée du client ou du vendeur revient à protéger ses données confidentielles : ses informations sensibles, son ID, son emplacement, ... lors des différents contacts durant : le chargement/déchargement, l'interaction entre véhicules électriques et les agrégateurs locaux (LAGs), les communications bidirectionnelles, la collecte, l'agrégation, le stockage et la publication de données et lors du paiement et de la facturation, entre différentes parties dans les réseaux véhiculaires électriques (V2G) [9].

A partir de la connaissance des données de puissance en temps réel de chaque véhicule électrique (VE), il est susceptible de déduire l'habitude de vie du propriétaire de ce dernier. Par exemple, avec une forte probabilité de deviner correctement la période pendant laquelle le propriétaire du VE est en train de sortir d'une consommation d'énergie élevée du VE, l'adversaire peut lancer avec succès certaines activités criminelles dans la maison du propriétaire du VE, telles que le vol et le cambriolage, sans se faire prendre [10]. Les informations transmises pourraient être complètement exposées aux attaquants, et un attaquant pourrait facilement déduire les informations privées de l'utilisateur, telles que son comportement de divertissement, ses habitudes de vie [11], etc.

Il existe trois approches générales pour assurer la préservation de la vie privée dans les réseaux véhiculaires électriques (V2G) : minimisation des données, généralisation des données et suppression des données. La minimisation consiste à éliminer les données personnelles stockées inutilement pour réduire le risque d'éventuelles fuites d'information et d'usurpation d'identité. Bien que la généralisation des données consiste à afficher une information générale sur le client au lieu de préciser la valeur exacte afin d'améliorer la confidentialité, par exemple, afficher une plage pour l'état de charge d'un VE peut rendre l'adversaire confus entre plusieurs VEs ayant la même plage. La suppression des données signifie la non-divulgation sélective de certaines valeurs de données comme le ID pour assurer la préservation de la vie privée. Cette dernière pourrait être divisée en anonymat, indissociabilité, indétectabilité, inobservabilité et pseudonymité. L'anonymat signifie qu'un élément dans le réseau V2G ne peut pas être identifié dans tous les sujets possibles. Alors que l'indissociabilité signifie qu'un adversaire ne peut pas suffisamment distinguer si deux sujets ou plus dans les réseaux sont liés ou non. L'indétectabilité signifie qu'un

adversaire ne peut pas suffisamment distinguer si un élément existe ou non. Bien que l'inobservabilité signifie qu'un adversaire ne peut pas suffisamment distinguer si une cible a effectué certains types d'actions. La pseudonymité consiste à utiliser le ID d'un VE au lieu de son nom réel. Tandis qu'il y a beaucoup de problèmes et défis liés à la vie privée**,** les auteurs ont cité : la collecte et l'agrégation des données, l'authentification du VE avec succès, la facturation et le paiement fiable, l'indissociabilité sans révéler celles qui sont confidentielles du client et la protection de son identité, son emplacement et ses données publiées [9].

2.4 Vers la décentralisation des informations et des tâches

Pour minimiser l'interférence humaine face au développement technologique, l'industrie automobile a rapidement adopté un grand changement : des véhicules connectés, des voitures intelligentes avec une pléthore de capteurs embarqués et d'applications avec connectivité Internet pour offrir des services de sécurité et de confort aux utilisateurs. L'idée est de permettre aux véhicules d'échanger des informations sur l'emplacement et la position avec leur infrastructure où les véhicules récepteurs regrouperont ces messages et prendront des décisions intelligentes [12].

Pour informer le véhicule électrique (VE), des bornes de recharge disponibles et fonctionnelles, plus proches et qui offrent les services demandés (chargement, déchargement, informations sur ces deux) par le VE, aussi pour avoir une liste des VEs autorisés, ce qui optimise la vie en matière du temps et de qualité de service, des changements au système du réseau V2G seront nécessaires.

En utilisant des communications dédiées à courte portée (DSRC) pour échanger des paquets de données, appelés messages de sécurité de base (BSM), entre les véhicules et des entités proches (cloudlets les plus proches) entre 300 et 500 mètres de portée, les messages seront envoyés jusqu'à 10 fois par seconde offrant une vue à 360 degrés de la proximité, avec des applications embarquées utilisant les informations pour les alertes et les avertissements [13]. Ces services seront présentés en détail dans ce qui suit.

2.4.1 Les composants de l'infrastructure

L'infrastructure est composée d'une partie *Cloud* pour tout ce qui est nécessaire à la gestion des certificats, et à l'enregistrement des éléments de l'infrastructure, et d'une partie *de périphérie* (*Edge)* pour tous les éléments participants à la communication (**VE** et **EVSE**).

Nous avons choisi l'infrastructure Cloud pour la facilité de gestion et le bon système de sécurité, néanmoins, nous pouvons simplement utiliser des systèmes simples (non-cloud).

2.4.2 Infrastructure Cloud

Elle est composée de deux parties :

a) Contrôleur AWS (Services Web Amazon) Cloud qui est un outil pour la gestion des services AWS (de contrôle, de sécurité et de gestion).
b) AWS Grenngrass qui est un logiciel qui étend les fonctionnalités du cloud aux appareils locaux. Il permet aux appareils de collecter et d'analyser les données plus près de la source des informations, de réagir de manière autonome aux événements locaux et de communiquer en toute sécurité sur les réseaux locaux [14].

2.4.3 Infrastructure de périphérie (Edge)

Elle comporte les Cloudlets (nous les détaillons dans le paragraphe 2.5.1).

2.5 Modèles et architectures dans les réseaux VANETs

Simplifier, faciliter et sécuriser la vie aux utilisateurs des véhicules électriques est un objectif commun entre tous les chercheurs. Vu que les ressources dans le réseau V2G ne sont pas suffisantes, une architecture qui optimise le temps et par la suite l'énergie électrique aux véhicules EVs et à l'infrastructure est nécessaire. Nous nous sommes orientés vers une architecture disponible partout où circule le véhicule, d'où est venue l'idée de centraliser les informations dans une plateforme disponible 24h/24. Suite à notre recherche dans la littérature sur la centralisation des données, nous avons trouvé le travail présenté dans [13] qui utilise une idée semblable à la nôtre mais qui a été réalisé sur les réseaux VANETs (Vehicle Adhoc Network).

Les réseaux intelligents conventionnels ne peuvent pas satisfaire la demande croissante de stockage et de gestion des données. Le cloud computing gère exactement ces problèmes et il est parfaitement intégré au réseau intelligent pour un fonctionnement plus efficace du système. Cependant, le système de réseau intelligent basé sur le cloud est vulnérable à diverses failles de sécurité. L'implémentation de la confidentialité des données est indispensable pour protéger la vie privée des utilisateurs [7].

2.5.1 Les Cloudlets

Une architecture est un modèle de communication V2V (Vehicle-To-Grid) et V2I (Vehicle-To-Infrastructure) basé sur des attributs utilisant des cloudlets de périphérie (Edge) qui sont installés dans des emplacements géographiques selon leur couverture limitée et selon la circulation routière.

Les deux figures ci-après illustrent l'architecture et le modèle de la solution proposée dans [13].

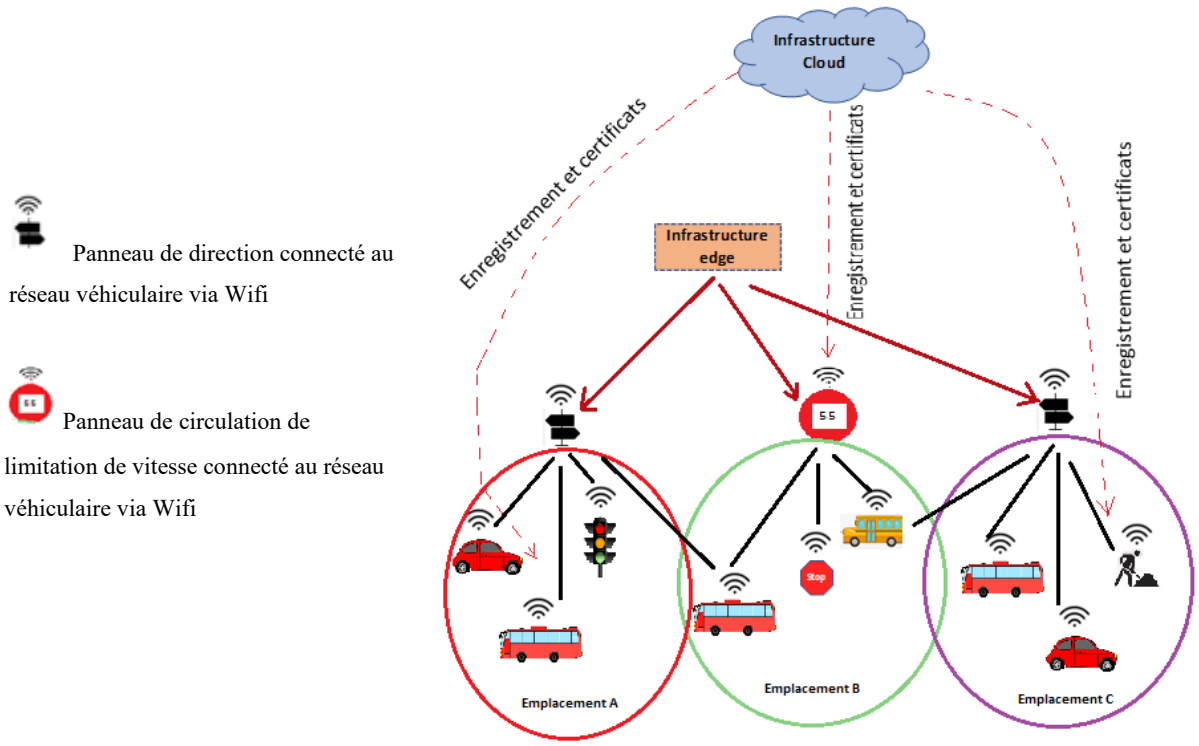


Figure 2 : Architecture Cloudlets de confiance de communication V2V

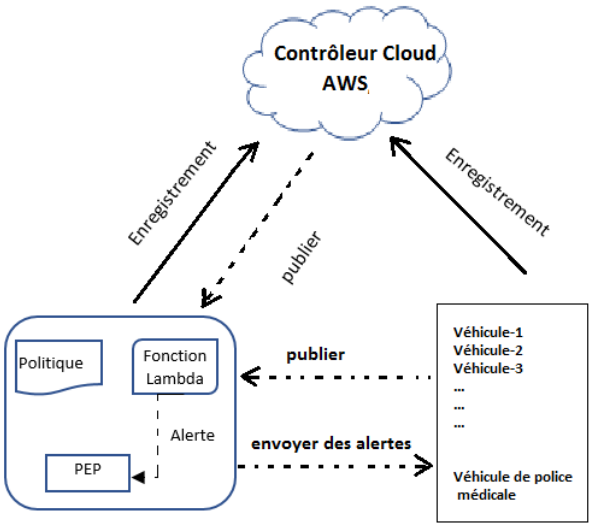


Figure 3 : Architecture Système de communication V2V et V2I

L'architecture système consiste à enregistrer chaque entité intelligente statique (véhicule, infrastructures de périphérie) auprès d'un contrôleur cloud AWS. Ce dernier fournit la liste des cloudlets dans le chemin désigné du véhicule. Ce dernier publie et s'abonne à des sujets MQTT (Message Queuing Telemetry Transport) sécurisés dans chaque cloudlet. Les cloudlets (AWS Greengrass) contiennent les politiques de sécurité décrites ci-après, ils envoient les alertes aux véhicules enregistrés dedans.

Policy

Plusieurs politiques sont exécutées, dépendamment du besoin, comme la *Gestion des utilisateurs :*

a) AWSGreengrassFullAccess : Autorise toutes les actions AWS IoT Greengrass pour toutes vos ressources AWS.

b) AWSGreengrassReadOnlyAccess : Autorise les actions List et Get AWS IoT Greengrass pour toutes vos ressources AWS.

c) AWSGreengrassResourceAccessRolePolicy : Autorise l'accès aux ressources de AWS services. Il s'agit de la stratégie par défaut utilisée pour le rôle de service Greengrass.

d) GreengrassOTAUpdateArtifactAccess : Autorise l'accès en lecture seule aux artefacts de mise à jour en direct (OTA) pour le logiciel AWS IoT Greengrass Core dans toutes les régions AWS [15].

Fonction Lambda

AWS Lambda est un service de calcul qui répond aux besoins de nombreux scénarios d'application, à condition que nous soyons en mesure d'écrire le code de notre application dans des langages pris en charge par AWS Lambda et que nous utilisons l'environnement d'exécution standard AWS Lambda et les ressources fournies par Lambda [16].

2.5.2 L'architecture PKI avec cryptographie SCS basée sur ECC

Binod et al., dans [17], ont proposé une architecture à clé publique (PKI) avec cryptographie SCS basée sur ECC pour remédier aux lacunes de la PKI et qui est *douze fois plus rapide* que le RSA (Rivest–Shamir–Adleman) à 128 bits, et deux fois plus courte que ECDSA (Elliptic Curve Digital Signature Algorithm) avec un système évolutif. Dans la grille traditionnelle, les certificats émis peuvent être utilisés pour l'authentification, la signature numérique et le cryptage des données. L'architecture PKI est composée principalement de la centrale d'authentification (CA), l'autorité d'enregistrement (RA), l'entrepôt et une entité finale. La centrale d'authentification (CA) génère les certificats et lie la clé appropriée au certificat, ainsi, elle assure le contenu de ce dernier. Le Certificat Racine V2G est utilisé pour valider celui du contrat ainsi que des certificats EVSE (borne de recharge) dans les communications V2G. Le certificat implicite est trop long et prend beaucoup de temps à vérifier son chemin, de plus ce mécanisme n'est pas évolutif car il est limité à trois centrales d'authentification racines (RCA), et on ne peut stocker que cinq certificats dans une entité finale. Pour cela, les auteurs ont employé la SCS basé sur la cryptographie à courbe elliptique et la technique de clé publique auto-certifiée ayant un certificat implicite pour réduire la taille du certificat et le temps de vérification du certificat. Dans ce système, le traitement du certificat implique également deux processus pour former la chaîne des approbations : la construction implicite du chemin du certificat et la validation du chemin. Comme illustré dans la figure 4 ci-après, la construction forme une

chaine de certificats implicites : $б_{A,}$ $б_{CA2}$, $б_{CA1}$ et $б_{RCA}$ alors que dans la vérification, tous les certificats implicites sont vérifiés par une forme généralisée (équation)**.**

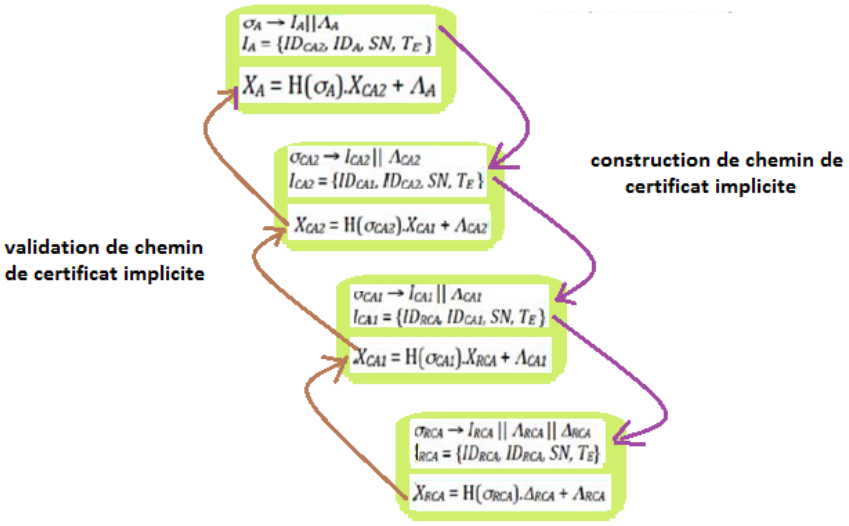


Figure 4 : Construction et validation du chemin de certificat implicite pour SCS basé sur ECC[17]

2.6 Conclusion

Dans ce chapitre, nous avons présenté l'infrastructure V2G, ses acteurs primaires, le moyen de communication entre eux, les acteurs secondaires et les différents problèmes de sécurité engendrés par le développement exponentiel du réseau V2G et qui touche aux données confidentielles des différents éléments du réseau intelligent. Aussi, nous avons présenté l'infrastructure des cloudlets qui sera le point central de notre proposition. L'utilisation d'une infrastructure PKI avec cryptographie SCS basée sur ECC sera un plus pour optimiser le temps d'exécution afin de sécuriser les réseaux V2G. Dans le chapitre suivant, nous présenterons une revue de littérature sur la sécurité des grilles intelligentes (SG) et des réseaux V2G.

Chapitre 3 : Revue de la littérature

3.1 Introduction

Une grille intelligente (SG) est une évolution du réseau électrique qui repose principalement sur une architecture en couches pilotée par l'informatique. Le couplage des systèmes de communication et physique permet à la grille intelligente d'améliorer son efficacité, sa résilience, sa fiabilité et son interopérabilité [18]. Plusieurs recherches ont abordé l'aspect sécuritaire des données confidentielles dans la grille intelligente ainsi que dans le réseau véhiculaire électrique (V2G) qui y fait partie.

Dans ce chapitre, nous allons aborder l'introduction des cloudlets dans le réseau VANET (Vehicle Adhoc Network) qui ne fait pas partie du réseau V2G mais qui nous a donné une idée sur l'implémentation des cloudlets dans les réseaux intelligents. Ensuite, nous présenterons la norme ISO 15118, ses différentes parties, les travaux connexes sur la sécurité au sein de la grille intelligente, des réseaux V2G et les solutions proposées pour remédier à leurs problèmes.

3.2 Les cloudlets de confiance

Les auteurs dans [13] ont introduit des cloudlets de confiance pour autoriser, contrôler et vérifier l'authenticité, l'intégrité et assurer l'anonymat des messages échangés dans le système V2V (Vehicle-To- Vehicle) et V2I (Vehicle-To-Infrastructure). Des politiques de sécurité sont appliquées aux véhicules connectés dynamiquement et aux infrastructures en bordure, pour désinfecter le réseau de tout échange non-autorisé. Ils ont présenté un modèle formel basé sur des attributs pour la communication V2V et V2I, ainsi que la mise en œuvre de la preuve de concept de la solution proposée dans la plate-forme AWS IoT (Internet of Things). Elle complète la communication directe V2V ou V2I et sert des cas d'utilisation importants tels que l'avertissement d'accident ou de menace de glace et d'autres applications de sécurité. L'USDOT (United States Department of Transportation) a proposé un système de gestion des informations d'identification de sécurité (SCMS : Security Credential

Management System) qui peut assurer des communications fiables entre Véhicule-à-Véhicule (V2V) et Véhicule-à-Infrastructure (V2I). Le contrôle d'accès basé sur les attributs (ABAC : Attribute-based access control) a la capacité de capturer des environnements contextuels et dynamiques. Chaque cloudlet reçoit des messages des véhicules de sa portée et les transmet de manière appropriée à d'autres véhicules associés, où (cloudlets) sont déployées des politiques de sécurité pour restreindre ou bloquer les faux messages. Elles assurent l'anonymat et la confidentialité, transmettent des listes de révocation de certificats (CRL) aux véhicules et bloquent les véhicules eux-mêmes, mettent à jour les listes des véhicules bloqués. Cette approche basée sur MQTT3 (Message Queuing Telemetry Transport) pour l'échange de messages peut fonctionner avec la norme DSRC (Dedicated Short Range Communications) pour permettre des cas d'utilisation avec une latence minimale, sans nécessiter de coût matériel supplémentaire et fonctionner avec du Wifi, du LTE (Long-Term Evolution) ou du 5G (Cinquième Génération). Elle complète le SCMS proposé par l'USDOT et peut être utilisée comme un complément à la communication actuelle entre pairs. Ces systèmes sont conçus pour prendre en charge les applications des systèmes de transport intelligents (STI).

3.3 Standard ISO 15118

Le Standard ISO 15118 est une norme internationale qui décrit le protocole de communication numérique qu'un véhicule électrique (VE) et une station de charge (EVSE) doivent utiliser pour recharger la batterie haute tension du VE. Dans le cadre du système de charge combiné (CCS), **l'ISO 15118** couvre tous les cas d'utilisation liés à la charge à travers le monde. Ceci implique les applications de charge filaire (CA et CC) et sans fil et les pantographes qui sont utilisés pour charger les véhicules plus gros comme les bus. **ISO 15118** permet un transfert d'énergie bidirectionnel. La nomenclature officielle de l'ISO 15118 est « Véhicules routiers - Interface de communication entre le véhicule et le réseau ». **ISO 15118** se devise en neuf (9) parties, liée à une ou plusieurs des sept couches de communication du modèle OSI (Open Systems Interconnection) qui définissent la manière dont les informations sont traitées dans un réseau de télécommunications. Nous les résumons brièvement ci-après.

15118-1 : Les informations générales et définition de cas d'utilisation, fusionné avec les contenants de ISO 15118-6, 2ème édition, liée aux sept (7) couches.

15118-2 : Définit tous les messages et les exigences techniques associées qui sont nécessaires à mettre en œuvre pour réaliser les cas d'utilisation, liée aux couches 7 à 3.

15118-3 : Définit la communication de niveau inférieur (la couche liaison de données et la couche physique). Ces couches établissent la communication de niveau supérieur décrite dans l'ISO 15118-2. Cette troisième partie fait également référence à la CEI 61851-1, une norme qui décrit comment traiter les signaux analogiques de modulation de largeur d'impulsion (PWM) liés à la sécurité qui codent l'ampérage disponible à une station de charge.

15118-4 : Concerne les tests de conformité aux exigences spécifiées dans l'ISO 15118-2.

15118-5 : Concerne les tests de conformité aux exigences définies par l'ISO 15118-3.

15118-8 : Une partie distincte qui spécifie les exigences techniques pour la communication sans fil sur les deux couches de communication les plus basses en utilisant IEEE 802.11n comme technologie Wifi.

15118-9 : Fournit des tests de conformité pour les cas d'utilisation de la huitième partie et complète la liste actuelle des tests de conformité requis pour les communications filaires et sans fil.

15118-20 : Est une version mise à jour de l'ISO 15118-2, avec des fonctionnalités supplémentaires telles que la charge sans fil, le transfert d'énergie bidirectionnel et les bus de charge via des pantographes, et qui ne sera pas compatible avec 15118-2, ce qui signifie : un véhicule électrique qui communique uniquement via ISO 15118-2 ne pourra pas se recharger sur une station de charge qui prend uniquement en charge ISO 15118-20 et vice versa [19].

Bien que la norme **ISO 15118** définit les différentes solutions de communication et d'échange dans le réseau V2G, ces solutions ont fait l'objet de critique de plusieurs auteurs,

notamment dans la sécurité des communications. Dans ce qui suit, nous allons aborder quelques travaux qui traitent les problématiques reliées à la sécurité des communications.

3.4 Les travaux connexes

3.4.1 La sécurité au sein des grilles intelligentes et les réseaux V2G

Il faut sécuriser la grille intelligente des différentes menaces de sécurité pour assurer sa disponibilité, son intégrité, sa confidentialité, sa scalabilité, la préservation de la vie privée, l'authentification d'entité et la non répudiation [20], [21] et [17].

Le réseau V2G est une infrastructure critique qui doit être défendue contre les attaques potentielles et le conducteur doit être correctement facturé pour l'énergie fournie au véhicules électriques (VEs). Sans communication sécurisée entre les VEs et les bornes de recharge, des tiers malveillants peuvent intercepter, modifier les messages et falsifier les informations de facturation [19]. Pour cela, nous avons étudié les articles traitant des problèmes de protection de la vie privée dans les réseaux V2G, y compris la confidentialité des lieux, l'identité privée, l'authentification anonyme, etc [20].

D'après Wenlin et al. [20], protéger la vie privée est essentiel, ce qui concerne les informations sensibles du client ou du vendeur de l'électricité, ceux qui touchent l'identité (ID), l'emplacement, la politique de contrôle d'accès et le payement et la tarification. D'autres informations touchent la vie privée en écoutant le réseau, en interceptant les messages, en forceant l'identité, en créant beaucoup d'IDs pseudonymes ou en profitant des pannes/changement matérielles.

Les auteurs dans [21], ont présenté une vision de la grille intelligente. Elle est divisée en trois parties : le centre de contrôle, la sous stations et les appareils intelligents, comme l'illustre la figure 4. La communication entre l'appareil intelligent et les sous stations n'est pas encore sécurisée. Les auteurs ont comparé plusieurs protocoles de sécurité, ceux qui souffrent des attaques d'identité, des attaques de mot de passe et d'autres vulnérables à l'écoute, et qui n'offrent pas une sécurité à un niveau acceptable.

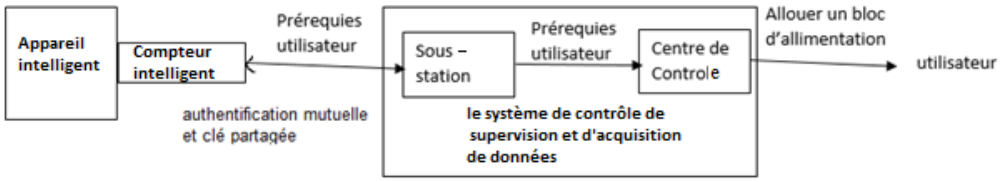


Figure 5 : Grille intelligente [21]

Binod Vaidya et al., dans [17], ont proposé une amélioration des lacunes de l'infrastructure à clé publique (PKI) reposant sur la cryptographie ECC, ils ont pu diminuer le temps de vérification de certificats et augmenter le nombre de certificats stockés dans l'entité finale qui était limitée à cinq (voir 2.5.2).

Les auteurs dans [22], ont voulu compléter les fonctions de la PKI, en introduisant de nouveaux mécanismes, particulièrement pour résister aux attaques DoS et quelques suggestions pour les différentes applications. Ils ont défini trois couches dans le réseau de la grille intelligente : Réseau de voisinage (NAN), réseaux de zone de bâtiment (BAN) et réseaux domestiques (HAN) et ils ont présenté les risques de sécurité pour chacune d'elles où ils se sont basés sur les réseaux sans fil. Ils ont proposé une infrastructure à clé publique (PKI) comme solution à ces problèmes. Ils ont présenté les limitations et ont introduit un ensemble de mécanismes pour les atténuer, spécialement l'attaque DoS.

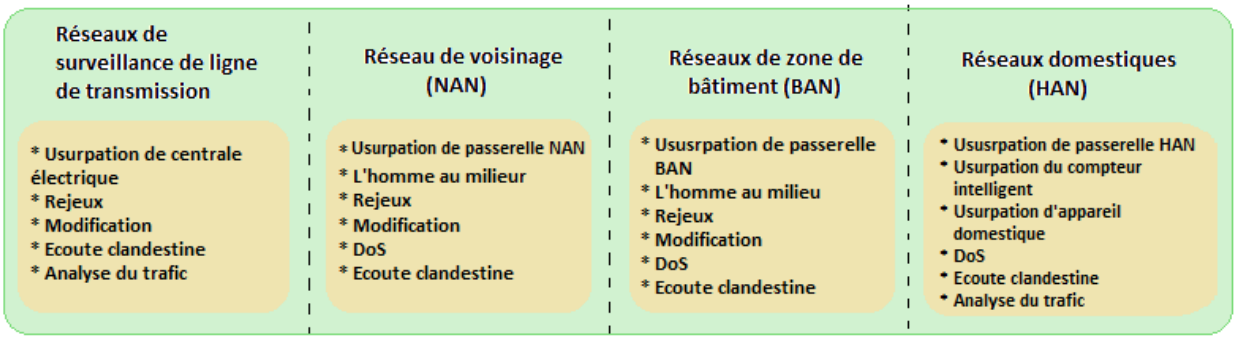


Figure 6 : Les menaces de sécurité sur les réseaux sans fil [22]

Les auteurs dans [22] ont implémenté une infrastructure PKI basée sur l'algorithme de cryptographie à courbe elliptique (ECC) dans une expérience sur des motes MikaZ et TelosB et les résultats sont acceptables (sans attaques DoS). Les limitations de la PKI dans la grille intelligente se résument à :

- Les attaques DoS pendant l'authentification qui nuisent à la disponibilité.
- La centralisation de la politique de gestion de PKI dans un seul serveur.
- Limitation du matériel.
- Ne peut pas prendre en charge la préservation complète de l'identité et la préservation de la confidentialité contre l'analyse du trafic.

Asif et al. dans [18], ont classé les attaques selon l'aspect ou le point sécuritaire touché : la confidentialité, l'intégrité ou la disponibilité. Les attaques qui bloquent le principe DIC (Disponibilité, Intégrité et Confidentialité) dans les grilles intelligentes.

S.no	**Confidentialité**
1	Attaque de l'Homme au milieu
2	Vol de mot de passe
3	Usurpation
4	Injection de données
5	Synchronisation de l'heure
6	Modification de données
	Intégrité
1	Falsification, Trou de ver
2	Rejeux
3	Usurpation
4	Injection de données
5	Synchronisation de l'heure
6	Modification de données
	Disponibilité
1	Trou de ver, inondation
2	Attaque de marionnettes
3	DOS/DDOS
4	Brouillage
5	Débordement de tampon

Tableau 1 : Les attaques qui bloquent le principe DIC dans les grilles intelligentes [15]

Dans [13], les auteurs ont cité quelques menaces concernant les réseaux VANETs (Vehicle Adhoc Networks) qui chevauchent avec les réseaux V2G dans plusieurs problèmes de sécurité, puisque le facteur en commun principale est le véhicule:

- Les cyberattaques : les mises à jour hertziennes non autorisées du micrologiciel, le vol de données privées d'utilisateurs, l'usurpation de capteurs, les attaques coordonnées sur l'infrastructure routière ou l'injection de logiciels malveillants.
- L'usurpation d'identité et les faux messages.
- Le suivi continu de leurs mouvements ou les données collectées.

Afin de remédier à ces problèmes, les travaux [5], [17], [21], [22], [23], [24], [25], [26], ont proposé des améliorations de l'infrastructure à clé publique (PKI). Parmi ces améliorations, on retrouve la cryptographie à courbe elliptique (ECC), la technologie de la blockchain et l'utilisation de crypto-système. D'autres travaux [2], [13], [20], [27], [28], [29], [6], [30], [31], [32], ont utilisé différentes techniques comme la signature d'anneau, le partage de clé, la régression, le relai, la non utilisation du pseudonyme, le fractionnement de données, le OU EXCLUSIF, le hachage et le moteur de détection d'anomalies. Nous les discuterons dans ce qui suit.

Les auteurs dans [21], ont proposé un protocole d'authentification robuste et efficace basé sur la cryptographie à courbe elliptique (ECC) avec une protection d'identité pour les grilles. Il est encore impossible de briser la cryptographie ECC avec les ressources informatiques existantes et elle est plus puissante que la méthode RSA ou Diffie-Hellman (D-H) et beaucoup plus courte en termes de clé, elle est robuste et efficace. Un dispositif inviolable a été utilisé pour stocker des informations secrètes pour aider à fournir la protection de la vie privée par le processus d'authentification. Le protocole proposé a deux phases : Initialisation et authentification. Dans l'initialisation, le centre de contrôle et la sous-station calculent l'agrément de clé et différents paramètres de sécurité (la fonction de hachage, le point P, la clé publique, la paire secrète (C1, C2)) pour l'authentification. La sous station les écrit dans le dispositif inviolable (DI) pour initialiser l'appareil intelligent SA(Ui). Dans l'authentification, l'appareil intelligent SA(Ui) envoie la clé à la sous station qui fait les calculs et les vérifications nécessaires pour réaliser l'authentification mutuelle et l'agrément de clé avec lui.

Quand nous avons examiné cette proposition et ses différentes étapes, nous avons remarqué qu'il y a des lacunes, spécifiquement en ce qui concerne la sécurisation de l'information et

des données. Sur leur démonstration [21] , les auteurs ont supposé que S | ≡ Φ (IDi || s || r1) alors que S ne possède pas r1, il peut être modifié avant sa réception par S dans C3, et c'est U qui croit que r1 est vrai et non pas S. r1 est stocké dans U et non pas dans S. (page 10 : Authentication proof using GNY logic : 1) the first run). Nous proposons de copier r1 sur S via un canal sécurisé par exemple, si c'est possible, et S compare r1 du message crypté avec le sien.

Pour le 2ème point « The second run », [21] même chose pour r2 côté U dans le message C4, U n'est pas sûr que la valeur de r2 n'ait pas été modifiée par un tiers. U | ≡ Φ (SIDj || r2). Nous proposons la même solution que r1. Même cas pour U | ≡ S ∃ r1.

D'après la logique GYN, les auteurs dans [21] ont supposé que U | ≡ S | ≡* : U croit que S est honnête et compétent, mais elle ne concerne pas les critères que nous avons déjà cité. Dans la majorité des autres étapes, la sureté de r1 et r2 est très importante pour la sécurité des messages et de la communication.

Les auteurs ont proposé, dans [22], l'infrastructure PKI comme solution aux problèmes liés à la sécurité des communication du réseau V2G et ont cité ses limitations en introduisant un ensemble de mécanismes pour les atténuer spécialement lors de l'attaque DoS. Ils ont implémenté une infrastructure PKI avec l'algorithme de cryptographie à courbe elliptique (ECC). Ils ont résumé d'abord, les limitations de PKI dans la grille intelligente comme suit : les attaques DoS pendant l'authentification qui nuisent à la disponibilité, la centralisation de la politique de gestion de PKI dans un seul serveur, la limitation du matériel, et elle (l'infrastructure PKI) ne peut pas prendre en charge la préservation complète de l'identité et la préservation de la confidentialité contre l'analyse du trafic. Pour cela, ils ont proposé un mécanisme de vérification à base de polynôme léger basé sur la génération d'un polynôme $f(x, y)$, de degré t par l' autorité de confiance (TA) lors de l'enregistrement d'une entité i à cette dernière en vérifiant la légitimité d'une entité avant de vérifier son certificat et sa signature. La vérification de la signature est plus rapide que celle de ECC et atténue les attaques DoS et inconditionnellement sécurisée et cela même pour les attaquants internes qu'externes. Les auteurs ont divisé les entités en groupes et sous-groupes. Ils ont désigné, dans chacun, une entité comme autorité de confiance (TA)

afin d'éliminer le point de défaillance unique (single point of failure), de soulager le goulot d'étranglement et d'améliorer l'efficacité et l'évolutivité. Pour le problème du certificat anonyme unique dans la préservation de la confidentialité de l'identité conditionnelle, les auteurs ont proposé la signature de groupe : seul le manager peut dévoiler l'identité du signataire. ***Et si le manager est compromis ?*** La signature d'anneau a été proposée par les auteurs pour la préservation complète d'identité. Ainsi et à fins de facturation, la signature de groupe a été proposée, où l'utilitaire est le manager qui facture à un membre qui est le compteur intelligent. Pour la production et la distribution de l'énergie, ils ont proposé la signature d'anneau plus la technique de codage du réseau pour assurer la protection de la vie privée contre l'analyse du trafic. Ils ont choisi le cryptage pour compléter l'évolutivité fournie par PKI.

Todd Baumeister a comparé, dans [23], les modèles de PKI pour choisir le meilleur à implémenter. Puisqu'il existe plusieurs critères pour évaluer les modèles de PKI, il a choisi l'impact. Nous avons résumé les critères de chaque modèle dans le tableau ci-après. Il a trouvé que le modèle CA Bridgé est le plus efficient. Li, Ren, Wang, Xie, et Yao dans [33] ont modifié le CA bridgé pour promouvoir la découverte des chemins des certificats. La haute disponibilité (single point of failure), la sécurité et la mise en œuvre des frontières virtuelles ont besoin d'être améliorées.

Modèles de PKI / **Critères**	Listes de certificats de confiance	CA Hiérarchique	CA Maillé	CA Bridgé
Haute disponibilité	✓			
Opération en temps réel	✓	✓		
Interopérabilité	✓	a des problèmes		✓
Évolutivité		✓		
Application des politiques centralisée		✓		✓
Sécurité		✓	✓	✓
Flexibilité			✓	✓
Intégration des structures existantes			✓	✓
Convention d'appellation	limitée	✓	limitée	✓
Frontières virtuelles		✓		

Tableau 2 : Évaluation comparative des modèles de PKI selon l'impact

Les auteurs dans [24], ont proposé un schéma de préservation de la confidentialité basé sur la cryptographie à courbe elliptique (ECC) pour les réseaux V2G, qui permet le partage de données tout en maintenant le niveau de sécurité requis. Ce protocole d'authentification et d'échange de clés sécurisé, léger et préservant la confidentialité est proposé pour les configurations V2G. Le protocole conçu est basé sur la consolidation d'opérations de multiplication, de concaténation et de « XOR ECC » légères et peu coûteuses ainsi que sur des fonctions de hachage unidirectionnelles. Le système proposé résiste à un certain nombre d'attaques de sécurité : usurpation d'identité, suivi, transfert de secret, replay et

attaques de type "man-in-the-middle". Le protocole a besoin d'être amélioré pour couvrir les autres attaques de sécurité.

Uzair et al., dans [25], ont utilisé la technologie de la chaine de blocs « blockchain » qui facilite la production d'énergie décentralisée et le commerce local de l'énergie. Ils ont proposé un framework qui utilise le registre distribué et l'infrastructure PKI d'une blockchain avec un consensus dynamique de preuve de travail (dPoW) et la cryptographie à courbe elliptique (ECC) pour un commerce d'énergie V2G sécurisé. Leur processus a besoin d'un agrégateur (AG) qui héberge la blockchain, l'initialise et diffuse les paramètres publics des fonctions. La borne de recharge (CS) et le véhicule électrique (VE) s'enregistrent auprès de l'agrégateur (AG) et reçoivent les pairs de clés publiques-privées et leurs pseudo-identités (PID) qui sont des adresses du registre de la blockchain. Après une authentification mutuelle entre le véhicule, la borne et l'agrégateur, la borne (CS) accepte les demandes de services du véhicule électrique et lui offre les fonctions de facturation et de décharge et génère la transaction de crédit / débit correspondante. L'agrégateur vérifie la transaction et ajoute le nouveau bloc au registre via le consensus dPoW.

Dans [26], Les auteurs affirment que plusieurs schémas proposés dépendent de la crypto-systèmes à clé publique, ce qui ne garantit pas toutes les propriétés de la sécurité du réseau V2G. Ils ont proposé, comme dans [25], un mécanisme d'authentification hiérarchique orienté blockchain pour récompenser les véhicules électriques. Dans le consensus, le grand livre distribué de la blockchain a été utilisé pour l'exécution des transactions dans des environnements V2G distribués, en combinant avec la cryptographie à courbe elliptique (ECC) qui a été utilisée pour l'authentification hiérarchique. Le mécanisme d'authentification hiérarchique conçu a été utilisé en raison de son potentiel élevé de prise en charge de la décentralisation, de la confiance et de l'intégrité, afin de préserver l'anonymat des véhicules électriques et prendre en charge l'authentification mutuelle entre eux, les bornes de recharge (CS) et l'agrégateur central (CAG). En outre, le mécanisme prend également en charge des frais généraux de communication et de calculs minimaux sur les véhicules électriques à ressources limitées. Cependant, le système consomme

beaucoup d'énergie qu'il faut envisager à réduire, mais cela ne se réglera pas du jour au lendemain.

Wenlin et al. [20] ont proposé plusieurs techniques comme la ***signature aveugle, la signature de groupe, la signature de l'anneau, le partage secret et le cryptage homomorphe.*** Ils pensent que les problèmes liés à la sécurité des communications du réseau V2G peuvent être (ou partiellement) résolus : agrégation de données cachées, authentification anonyme, vie privée du paiement et de la facturation, dissociabilité de chargement, vie privée de l'identité et vie privée de l'emplacement. Les techniques proposées par les auteurs se chevauchent sur certains problèmes.

Les auteurs souhaitent dans [27] masquer ou obscurcir les signatures de charge afin que les événements d'utilisation des appareils intelligents ne puissent pas être détectés. Dû aux limitations physiques et coûts, la confidentialité parfaite ne peut pas être achevée. Ils proposent un algorithme de modération de confidentialité et introduisent trois méthodes pour évaluer différents aspects de la protection de la confidentialité offerte : une information théorique (entropie relative), une classification de clustering, et une corrélation/régression. Ils ont introduit quelques métriques :

- ***Niveaux de confidentialité basés sur l'entropie relative :*** Afin de quantifier deux ensembles et les comparer.
    a) ***Similitude basée sur la classification des clusters :*** les auteurs ont choisi le meilleur n cluster pour les transitions de consommation d'énergie $D_{PA}(t)$, et n cluster pour la version brouillée $D_p(t)$. Ils ont calculé la proximité de $D_p(t)$ à $D_{PA}(t)$, ce qui signifie que les transitions de consommation d'énergie $D_{PA}(t)$ sont cachées.
    b) ***Analyse de régression :*** les auteurs ont combiné la corrélation croisée et la procédure dans [28]**,** qui est la suite de la présente étude.
- Ils ont utilisé dans [28], **la modélisation de la signature de charge de puissance (PLS : Power Load Signature) par les chaînes de Markov :** pour la prévision de la valeur de PLS.
- Ils ont utilisé aussi, **l'algorithme de la protection sélective de confidentialité :** en allouant sélectivement des ressources de batterie logiques (Ei) à différents appareils (Si).

Afin de vérifier et mesurer la protection de la vie privée et compléter les recherches de [27], les auteurs dans [28] ont utilisé : a*) La Distance variationnelle (VD)* pour comparer deux sources d'information. Plus le niveau de sécurité offert est élevé plus la VD est grande, b*) La similitude des clusters* où ils ont utilisé la méthode de maximisation de silhouette pour construire les n clusters (séquence A où les centres sont triés) et ils en appliquent la méthode « Clara ». Ils ont généré n autres clusters (séquence B) en autorisant à changer les centres de clusters appropriés à l'ensemble de données. Ils ont construit les séquences A' et B' à partir du cluster 1 et ils ont calculé les rapports des transitions classifiées incorrectement et, *c) L'analyse de régression* qui est la même que dans [27].

Les auteur dans [2], ont affirmé que la communication dans le réseau V2G peut se faire via la technologie de communication sans fil. À cause de la distance entre une source et sa destination, les obstacles engendrés et les écoutes indiscrètes, ils ont utilisé des intermédiaires (relais) pour envoyer le signal entre eux. Un relai optimal est choisi, il reçoit le message de la source, puis il le décode et le transmet, c'est la destination et l'adversaire qui le reçoivent. Les paramètres de confidentialité des utilisateurs légitimes sont protégés en modifiant les paramètres de sécurité de la couche physique avec plusieurs utilisateurs écoutant dans le réseau. Afin de réduire la probabilité d'interruption du secret de la méthode que les auteurs ont utilisé et y augmenter la probabilité de capacité de sécurité non nulle, ils suggèrent d'augmenter le nombre d'antennes pour les utilisateurs légitimes de véhicules électriques, ce qui n'est pas toujours faisable, même chose pour augmenter la sécurité du réseau, il faut augmenter le nombre de relais intermédiaires pour la stratégie de sélection du relais opportuniste.

Linghui et al., dans [29], ont travaillé sur la protection de la confidentialité de la consommation d'énergie de chaque véhicule électrique (VE) qui doit être garantie. Pour résoudre le problème de la métrique de tarification dynamique dans les réseaux V2G qui dépend de l'agrégation de la consommation d'électricité en temps réel dans une région, un service efficace d'agrégation de données et de tarification dynamique (PADP) dans V2G IoT est proposé, en concevant un agrégat de données signé séquentiel basé sur l'identité, sur l'affacturage et un chiffrement homomorphique à seuil de Paillier. Dans ce dernier (le

chiffrement homomorphique à seuil proposé), un texte chiffré légal peut être généré si et seulement si pas moins du seuil k textes chiffrés illégaux individuels sont agrégés. Par conséquent, les données de consommation d'énergie agrégées peuvent être décryptées avec succès, tandis que la confidentialité de l'identité et la confidentialité de la consommation d'énergie du véhicule électrique peuvent être bien protégée même contre la collusion entre une station de charge électrique malveillante et des véhicules électriques compromis. En outre, la technique des données signées agrégées séquentielles garantit l'authentification de l'entité avec une quantité minimisée de données transmises. La compression des signatures du schéma proposé protège contre les attaques par usurpation d'identité et minimise le coût de communication considérablement.

Nous croyons, qu'en cas de véhicule seul au quartier, et avec un seul chargement, la station de charge reçoit la consommation en temps réelle et si elle est compromise, les informations confidentielles du véhicule électrique seront probablement compromises.

Les auteurs dans [6] ont proposé un mécanisme d'authentification préservant la confidentialité ainsi qu'un échange de clés entre les véhicules électriques (VE) et les agrégateurs locaux, dans lequel les VEs n'utilisent aucun pseudonyme, ce qui garantit une immunité contre le changement périodique des pseudonymes pour le VE et ce dernier n'a pas besoin de stocker un grand nombre de pseudonymes. En plus de satisfaire aux exigences d'anonymat, de confidentialité, de dissociation, de non-répudiation, de traçabilité et de révocation, le régime peut en outre soutenir la sécurité avancée. La solution prend en charge l'authentification bidirectionnelle entre un VE et l'agrégateur local (LAG), intègre la construction d'une clé partagée entre un VE et le LAG dans le processus d'authentification et utilise la clé partagée pour réaliser des transmissions sécurisées. Le processus de révocation n'entraînera pas la fuite des informations privées signalées avant la révocation d'un véhicule électrique.

JINGTANG et al., dans [30], mentionnent que les informations de facturation sont généralement transmises via un réseau public ou une liaison sans fil. Leurs communications n'ont pas de tiers de confiance pour l'authentification d'identité et la distribution de clés, et elles sont constamment exposées à des attaques d'analyse du trafic. Ils ont proposé un

schéma qui intègre de manière créative l'authentification d'identité dans la distribution de clés sans tiers de confiance, ce qui améliore la sécurité de la communication dans les réseaux publics. Ce schéma utilise le protocole Diffie-Hellman pour générer dynamiquement des clés de session et compléter l'authentification d'accès sécurisé. Adoptant une stratégie de transmission anonyme basée sur le fractionnement et la transmission des données, les données collectées par les utilisateurs légaux sont fractionnées et transmises selon un tableau pseudo-aléatoire pour garantir l'indiscernabilité des données. En outre, le schéma proposé est plus résistant à l'analyse du trafic car il préserve l'anonymat des informations de tarification en les fractionnant et en les transmettant de manière pseudo-aléatoire. Les auteurs n'ont pas discuté du cas où une ou plusieurs données sont perdues.

Dans l'environnement V2G au sein de l'Internet social des véhicules (SIoV), les auteurs dans [31] ont introduit un protocole d'accord de clé léger anonyme pour sécuriser les données générées par les SIoV concernant les passagers, les véhicules, les conducteurs et l'environnement. Le protocole conçu vise, principalement, les problèmes de confidentialité et de sécurité. Il rend la communication entre le véhicule électrique (VE) et un agent de confiance sécurisée en utilisant des opérations cryptographiques légères telles que le OU exclusif et le hachage. Une clé de session est utilisée pour garantir la sécurité des canaux de communication entre les deux parties, etc. Les auteurs ont estimé que le protocole est plus efficace en termes de communication, de calcul et de surcharge de stockage pour un environnement aux ressources limitées, bien qu'il génère beaucoup de données.

Dariush et al., estiment, dans [5], que la gestion des clés partagées dans les réseaux V2G est nécessaire. Ils ont utilisé le crypto-système à clé publique efficace basé sur une carte chaotique de Chebyshev sans engagement et qui est trois (3) fois plus rapide que le ECC. Ils ont proposé un schéma d'accord de clé anonyme, qui est exempt des problèmes de sécurité des schémas précédents qui résiste aux attaques bien connues et offre un secret de transmission et un fort anonymat. Il ne nécessite pas de stockage inviolable et se fait à travers seulement deux messages, ce qui peut, non seulement, fournir les exigences de sécurité attendues, mais qui a également un niveau de performance approprié.

Les auteurs dans [32], ont proposé un nouveau moteur de détection des anomalies cyber-physiques qui surveille le comportement du système et détecte les anomalies presque instantanément et le temps d'inspection de cas pour un paquet est de 0,165 seconde. Ce moteur de détection garantit que le composant critique du réseau électrique (à savoir, l'agrégateur), ainsi que le canal de communication qui l'interconnecte avec les autres composants du réseau, restent sécurisés, en surveillant les cyber-messages pour divers changements d'état et contraintes de données ainsi que les données d'alimentation sur le cyber-réseau V2G à l'aide de mesures de puissance à partir de capteurs sur le réseau de distribution physique/ électrique et en surveillant également les exigences de synchronisation des messages de protocole pour améliorer la sécurité de l'agrégateur. Pour cela, ils ont énuméré des séquences de commandes correctes dans le protocole de communication V2G. Ceci est utilisé pour générer une machine d'états d'agrégateur pour le moteur de détection. Ce dernier utilise également des contraintes de temps liées à la fréquence des messages périodiques et à la période d'abonnement pour différencier le comportement correct / incorrect du système. Le travail a été fait selon les normes les normes SAE J2847 / 1 et SAE J2847 / 3 qui ne sont pas encore prises en charge par les EV/EVSE parce qu'ils sont en cours du développement.

3.5 Conclusion

Chaque étude a proposé des solutions pour les menaces de sécurité jugées critiques. Le problème de la vie privée lors du déchargement et de la vie privée de publication de données [20] ne sont pas résolus dans le réseau véhiculaires V2G. [22] recommande des recherches plus avancées pour réduire le nombre de personnel qui gère l'infrastructure PKI. Pour le modèle proposé dans [23], beaucoup de prérequis ne sont pas couverts. Les auteurs dans [27] ont proposé (mais non pas dans V2G) la configuration d'un routeur d'alimentation qui permet aux utilisateurs de gérer leurs consommations et protège, à certain degré, leur vie privée. Un algorithme de confidentialité de mélange de puissance de batterie et des trois métriques ont amélioré plusieurs aspects de sécurité avec l'augmentation de la taille de la batterie aussi. Ces métriques peuvent être élargies dans le futur, et d'autres algorithmes peuvent être conçus, où les auteurs ont continué leurs travaux

dans [28]. Dans ce dernier travail, l'algorithme sélectif aide à protéger les informations sensibles des appareils de l'utilisateur. Il aide à prédire les évènements de consommation d'énergie et le contrôle utilisateur personnalisé. L'étude dans [13] a réduit (dans les VANETs), les problèmes de confidentialité des utilisateurs que nous pouvions en profiter. Ces cloudlets peuvent anonymiser les messages, garantir leur fiabilité et leur pertinence pour les entités qui les reçoivent. Le problème de ressources et du temps d'exécution reste à améliorer, pourtant Amazon possède beaucoup d'outil de gestion dans ce sens. Nous voyons aussi que le problème de l'indétectabilité dans les réseaux V2G n'est pas encore résolu.

Dans le chapitre suivant, nous allons présenter notre proposition, qui comble beaucoup de problèmes de sécurité cités dans ce chapitre.

Chapitre 4 : Modèle proposé

4.1 Introduction

Nos différentes lectures, examinassions des documents ISO 15118-1 et 15118-2, la proposition de la centralisation dans le réseau des VANETs (Vehicle Adhoc Network) et de cryptographie, et le reste des travaux, nous ont inspiré, afin de résoudre plusieurs problèmes de sécurité dans le réseau véhiculaire électrique (V2G), avec une architecture centralisée utilisant des certificats à clé publique (PKI) cryptées par SCS basés sur ECC en utilisant un schéma de certificat implicite. Dans ce chapitre nous allons, ainsi, détailler les caractéristiques de notre implémentation.

4.2 Méthodologie de recherche

Le modèle CA Bridgé mentionné dans [23], ainsi que d'autres architectures dans le réseau V2G, manquent d'évolutivité et/ou des frontières virtuelles, ce qui mène aux problèmes de haute disponibilité (single point of failure). Nos recherches dans la littérature nous ont orienté vers la décentralisation des données et des tâches avec l'architecture PKI cryptée avec ECC.

Cette architecture permet d'alléger les éléments du réseau V2G (Véhicule électrique et borne de recharge) en termes d'espace de stockage et du temps d'exécution de tâches puisque la grande partie de charge de travail se fait sur le Cloud (où un simple système où les entités sont liées au réseau), tandis qu'elle assure d'autres points sécuritaires au cours de ses processus. Nous avons assigné à chaque véhicule participant, un bit qui enregistre son état de connexion, et avons assigné un horodatage aux messages échangés afin de protéger l'identité du véhicule électrique, sa confidentialité, son anonymat ainsi ceux des messages et permettre l'évolutivité du réseau V2G.

4.3 Proposition d'une infrastructure Cloud

L'architecture, que nous proposons, est basée sur la partie principale de la décentralisation des données et des tâches, où tout élément du réseau V2G doit s'inscrire auprès de l'infrastructure Cloud, le CA racine peut-être la racine du Cloud, comme on peut laisser la responsabilité de fournir les certificats par une centrale de certification (CA) inscrite à l'infrastructure. La figure 6 et 7 montrent l'architecture proposée.

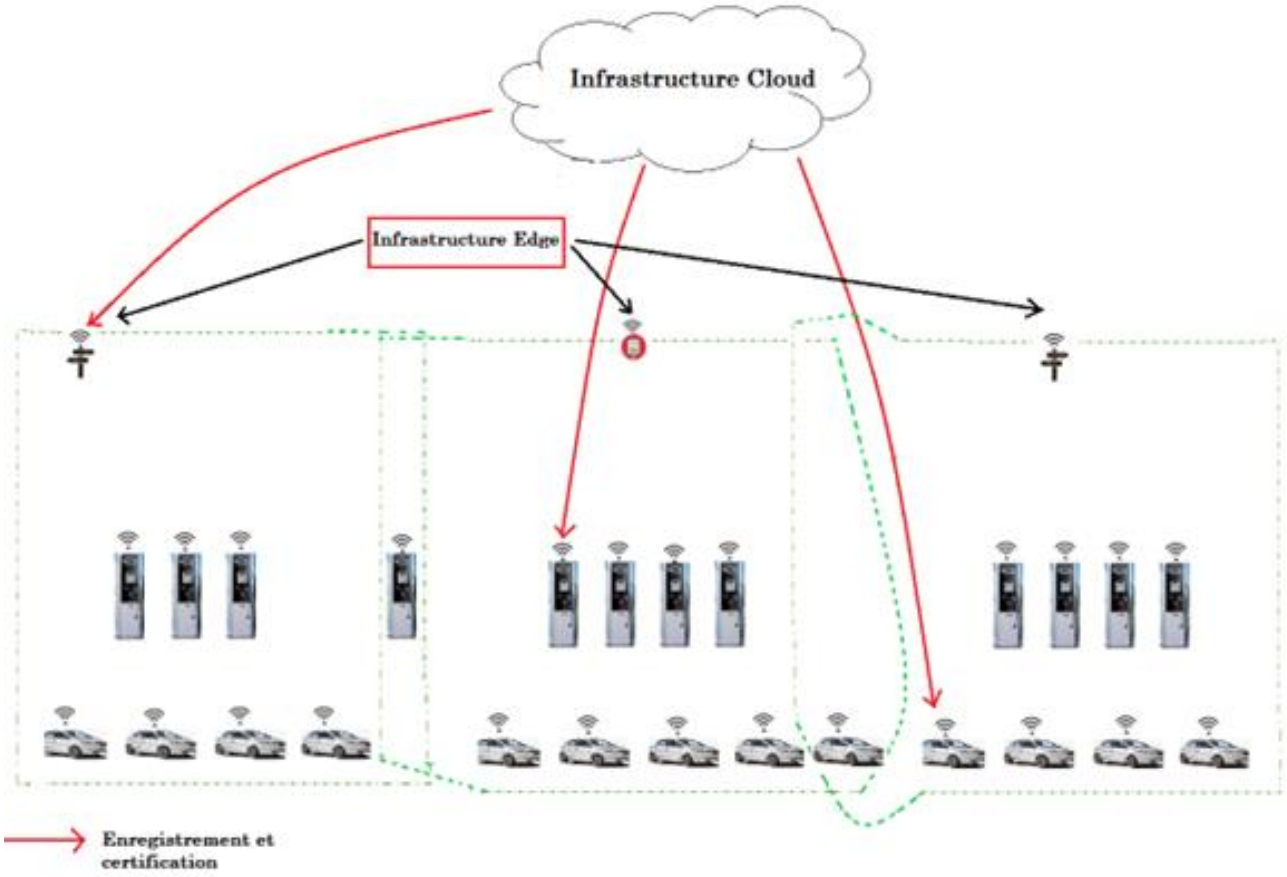


Figure 7 : Infrastructure.

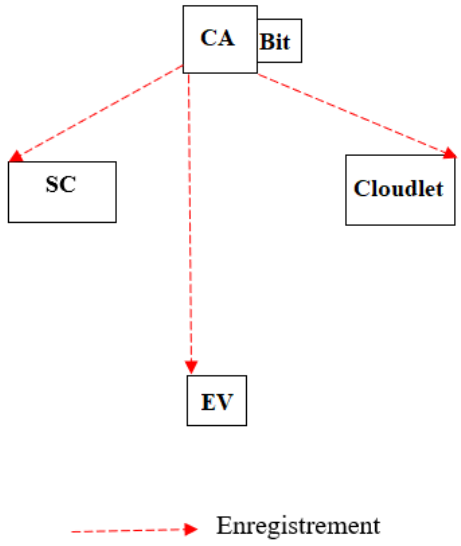


Figure 8 : Architecture proposée

Les messages entre les différentes entités (comme les véhicules électriques) sont vérifiés avant d'être transmis, et par la suite, relayés par les infrastructures de périphéries dépendamment de leurs localisations. L'enregistrement de chaque véhicule participant se fait auprès de la centrale de certification (CA) dans sa région. La communication V2G est prise en charge par les bords alternatifs avec une latence minimale de messages et dans les délais autorisés. Elle utilise la cryptographie SCS basée sur ECC avec un nombre de paquets minimal et un faible taux d'erreur. Chaque cloudlet aura une portée géographique, où les véhicules sont associés à la périphérie. L'anonymat des messages est assuré vu que les certificats sont supprimés avant d'être envoyés. La bande passante est économisée en vérifiant le contenu des messages par le cloudlet avant d'être transmis, ce qui élimine beaucoup de messages non utiles dans le réseau.

4.3.1 Présentation de cas d'utilisation

Avant de détailler les cas d'utilisation ordinaires, on suppose que les véhicules et les infrastructures intelligentes ont déjà été enregistrés au niveau du cloud central.

Dans [6], une définition de la confidentialité nous a poussé à introduire une nouvelle idée sur notre architecture. L'idée est pour assurer la confidentialité et l'anonymat : il faut qu'en un intervalle de temps donné, une seule session soit ouverte par l'utilisateur i (avec une identité ID_i).

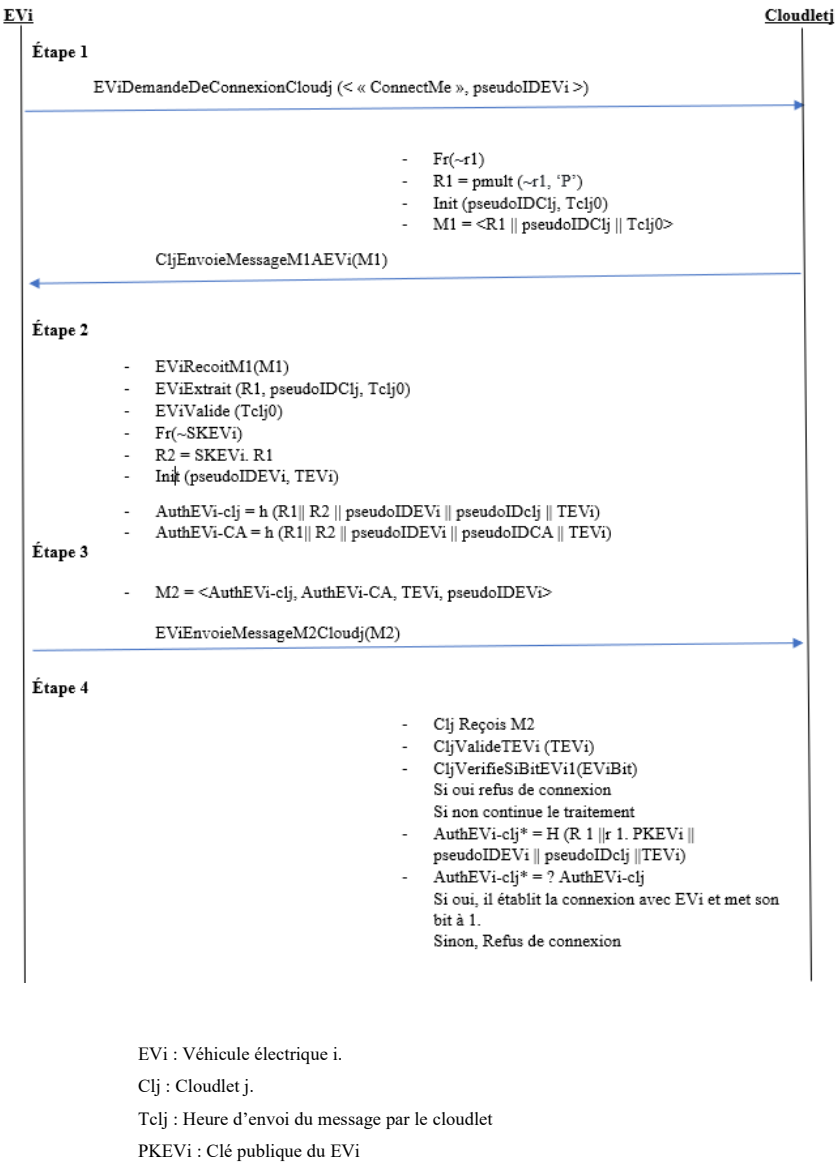
Nous proposons dans notre architecture, d'allouer un bit pour le véhicule électrique (VE) chez le contrôleur et les cloudlet (à l'enregistrement). Si le VE est connecté et/ou en traitement, le contrôleur le met à 1 sinon il le met à 0. Tant que le bit est à 1, aucun élément du réseau (contrôleur, cloudlet, SC, ...) n'accepterait une demande de connexion ou un échange avec un porteur de l'ID et/ou des informations du véhicule. Son pseudoID actuel expire avec la remise à 0 du bit.

Voici les différentes étapes du déroulement de l'échange :

1 – Initialisation du système : Le contrôleur initialise le système en générant les variables nécessaires pour la cryptographie ECC. Il publie les paramètres publics comme la clé publique PK, le point de base P, un grand nombre premier n et la fonction de hachage H(.) dans le réseau. Nous proposons une réplication du contrôleur sur le cloud pour éviter le point de défaillance.

2 – Enregistrement : Le véhicule électrique (VE) choisi le laps de temps Tev, demande l'inscription auprès du contrôleur en utilisant ses informations qui lui ont été fournies par le fournisseur à l'achat et ses cordonnées GPS (Global Positioning System). Le contrôleur vérifie son identité, s'il n'est pas dans la liste des révocations, il met le bit du VE à 1, lui fournit son nouvel ID de session, la liste des cloudlets dans sa zone, et il envoie aux cloudlets listés le ID du VE et à la fin de la connexion, il remet le bit à 0.

3 – Authentification mutuelle avec le cloudlet : Le véhicule électrique (VE) choisit le cloudlet dans sa zone et lui envoie une demande d'inscription. Le cloudlet vérifie l'identité du VE reçu de la part du contrôleur si le bit est à 0 et identifie le VE, sinon il avertit le contrôleur du VE non autorisé pour vérifier et mettre à jour la liste des révocations si nécessaire. Le VE vérifie aussi l'identité du cloudlet, s'y inscrit dépendamment de son GPS. La figure 8 ci-après illustre les séquences :



EVi : Véhicule électrique i.

Clj : Cloudlet j.

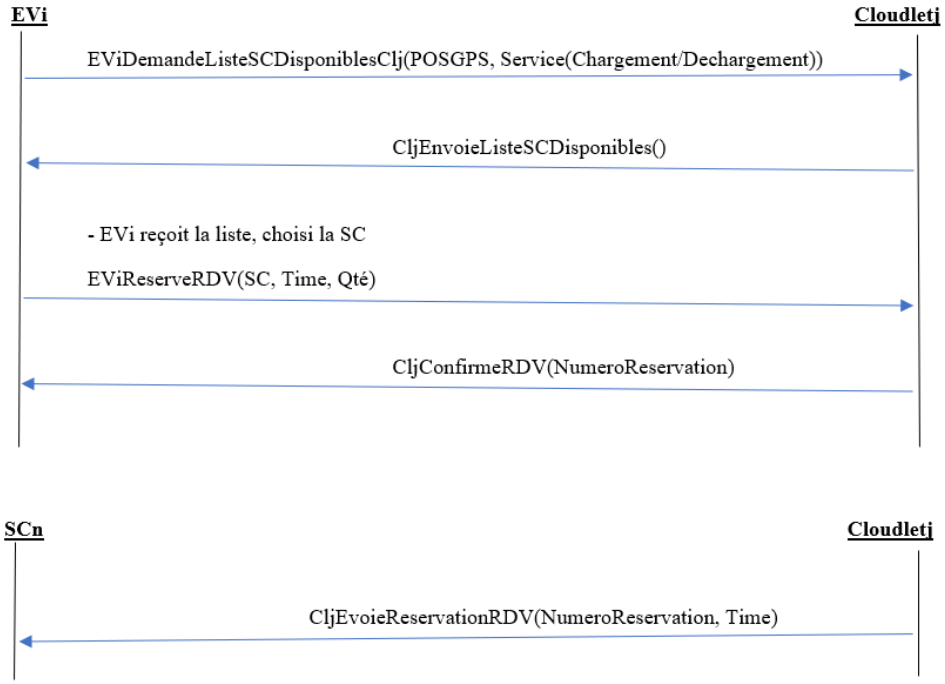
Tclj : Heure d'envoi du message par le cloudlet

PKEVi : Clé publique du EVi

Figure 9: Authentification mutuelle avec le cloudlet

4 – Demande de service : Le véhicule électrique (VE) envoie au cloudlet une requête demandant - pour un chargement ou un déchargement- à la borne la plus proche, disponible, apte à le recevoir, la tarification, et si possible, il fait une réservation (économie du temps et meilleure organisation). S'il n'y a pas de borne (SC) disponible, il envoie la requête (précédente) au prochain cloudlet le plus proche pour ne pas charger le contrôleur. Admettons que la gestion des rendez-vous de la SC se fait au niveau du cloudlet, une station ne peut pas refuser un VE après réservation si ce dernier respecte les modalités. En cas de

réservation, le cloudlet ne transmet pas le ID du VE aux SC, s'il n'y a pas de réservation, il ne saura même pas quelle SC va être choisie par le VE. Ce dernier utilise son numéro de réservation pour s'authentifier à la SC (choisie parmi les SCs disponibles). La figure 9 ci-après illustre les séquences de la demande de service.



Clj : Cloudlet j. EVi : Véhicule électrique i.
POSGPS : Position GPS
Qté : quantité d'énergie. RDV : Rendez-vous.

Figure 10 : Demande de service

5 – Authentification mutuelle avec la borne lors du chargement/déchargement : Avant d'arriver à la borne (CS), le véhicule électrique (VE) demande à son cloudlet de maintenir le bit à 1 si le conducteur a l'intention de poursuivre son but de chargement/déchargement et il incrémente le laps du temps (Tev) et le cloudlet informe le contrôleur. En cas de réservation, le VE utilise son numéro de réservation pour s'authentifier à la SC. Cette dernière vérifie le numéro reçu de la part du cloudlet. Ni la SC, ni le cloudlet ne sont responsables de la perte ou du vol de la réservation du VE. Ce dernier vérifie l'identité de la SC et sélectionne la quantité d'électricité voulue. La SC envoie au cloudlet la quantité sélectionnée avec le numéro de réservation pour débiter/alimenter le compte du client, et

commencer le chargement/déchargement. Le cloudlet envoie la facture au VE. La négociation de la méthode du payement (RFID, crédit, ..) se fait lors du choix du service et de la SC. À la fin du service, le VE envoie une requête au cloudlet pour mettre le bit à 0 et bloquer le ID et le cloudlet notifie le contrôleur. Les échanges entre la SC et le cloudlet se font selon l'authentification mutuelle comme avec le VE. La figure 10 ci-après montre les séquences de l'authentification et la fin de la session.

Si le véhicule n'a pas réservé, il s'authentifie à la SC de la même façon qu'avec le cloudlet.

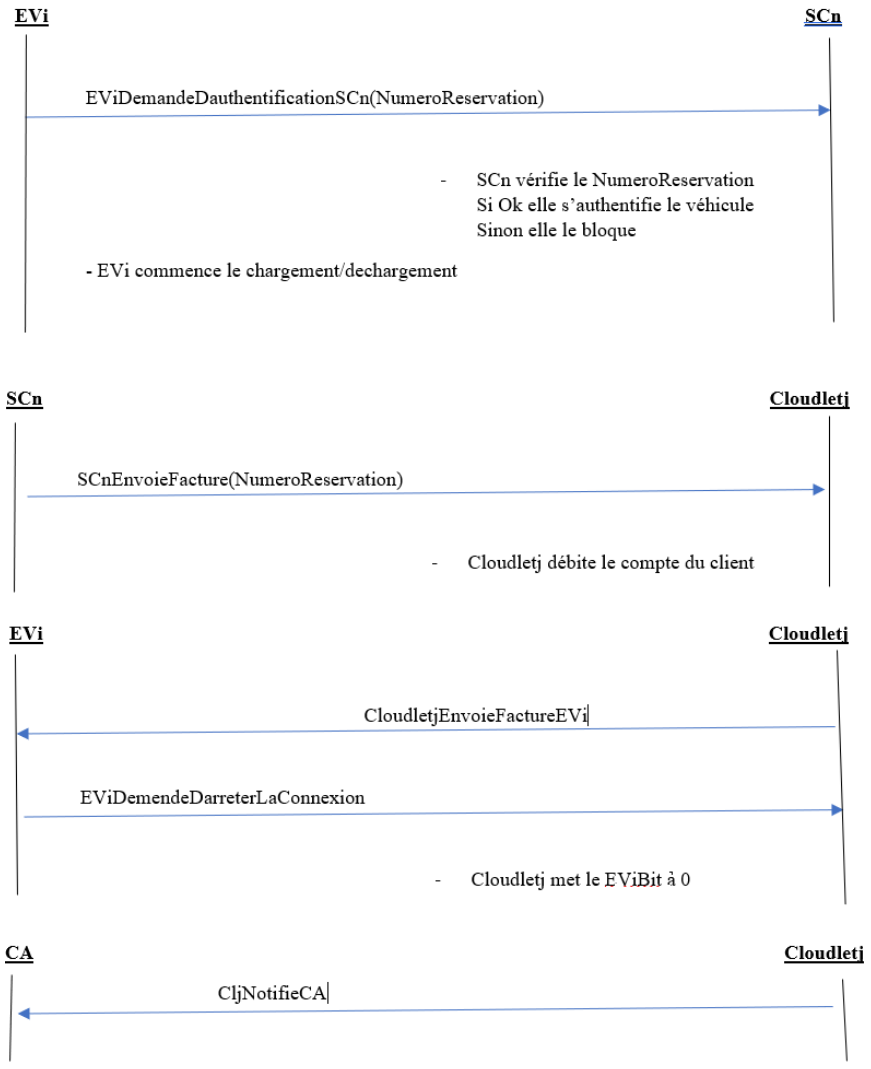


Figure 11 : Authentification mutuelle avec la SC lors du chargement/déchargement

Depuis l'initialisation du système, le véhicule électrique (VE) passe par différentes étapes. L'utilisation de la cryptographie ECC renforce la sécurité. L'allocation d'un bit pour sauvegarder l'état de connexion du VE ainsi que l'utilisation de l'horodatage protègent l'identité et les messages échangés dans les différentes étapes de l'échange depuis l'initialisation, au cours de l'enregistrement, les différentes authentifications et la demande de service. Cela nous a permis de cibler plusieurs aspects de sécurité comme l'attaque de relecture et l'attaque de désynchronisation qui n'ont pas été abordées dans le travail [13] et qui vont être abordées en détail dans le chapitre suivant.

4.4 Conclusion

Dans ce chapitre, nous avons présenté notre méthodologie de recherche et notre proposition d'architecture pour le réseau V2G avec les cas d'utilisation que nous avons détaillés. Nous allons présenter dans le prochain chapitre la modélisation de notre proposition avec le logiciel Tamarin Prover et les résultats de l'analyse de sécurité de notre protocole.

Chapitre 5 : Analyse des résultats

5.1 Introduction

Après avoir présenté dans le chapitre précédent notre proposition d'architecture et les cas d'utilisation, nous allons présenter dans ce chapitre l'environnement de modélisation de notre modèle avec l'outil Tamarin Prover qui est mieux adapté au réseau V2G. Nous allons donner deux exemples d'envoie et de réception d'un message de notre protocole ainsi que leurs résultats, vue que les messages échangés sont soit, de type « envoie » ou de type « réception ». Ensuite, nous allons faire une analyse de sécurité de notre protocole en décrivant les différents points sécuritaires et attaques assurés par notre protocole. A la fin, nous présenterons une analyse comparative entre le protocole présenté dans [13] et notre protocole en montrant notre valeur ajoutée et on termine le chapitre par une conclusion.

5.2 Modélisation du protocole

Tamarin Prover est un outil puissant pour la modélisation symbolique, l'analyse des protocoles de sécurité [34] et leur vérification. Il prend en charge à la fois la falsification et la vérification illimitée dans le modèle symbolique [35]. Les protocoles et les adversaires sont spécifiés à l'aide d'un langage expressif basé sur des règles de réécriture multiensembles. Ces règles définissent un système de transition étiqueté dont l'état consiste en une représentation symbolique des connaissances de l'adversaire, des messages sur le réseau, des informations sur les valeurs fraîchement générées et de l'état du protocole. L'adversaire et le protocole interagissent en mettant à jour les messages du réseau et en générant de nouveaux messages [34].

Lors de la modélisation de notre protocole, nous avons pu prouver qu'il est fonctionnel, de plus, il atteint les objectifs de la sécurité informatique : la confidentialité, l'intégralité et la non-répudiation des informations transmises lors des différentes communications entre les éléments du réseau V2G, comme le montre le code suivant (figures 12 et 13).

```
//Cloudletj envoie le message M1 au EVi

rule CljEnvoieMessageM1AEVi:

   let
        R1 = pmult(~r1,'P')
        M1 = <h(R1, ~pseudoIDClj, ~Tclj0)>

    in

  [CloudState(~pseudoIDClj, ~Tclj0, 'NOTCONNECTEDTOEVI'),
  Fr(~r1),
  Fr(~SKClj)]

  --[CljEnvoieLeMessageM1AEVi(~pseudoIDClj, M1)]->

  [Out(<MAC(~SKClj, <~Tclj0, h(R1, ~pseudoIDClj, ~Tclj0)>)>),
   CloudState(~pseudoIDClj, ~Tclj0, 'SENTMSGM1')]


//Etape 2 : Reception de M1 de la part du vehicule

rule EViReceptionM1Cloudletj:

    let
        M1 = <h(R1, ~pseudoIDClj, ~Tclj0)>
    in


  [In(<MAC(~SKClj, <~Tclj0, h(R1, ~pseudoIDClj, ~Tclj0)>)>),
   EViState(~pseudoIDEVi, TEVi0, 'NOTCONNECTEDTOCLOUDLET', ~pseudoIDEVi)]

  --[EViRecoitM1deClj(~pseudoIDEVi, M1)  ]->

  [EViState(~pseudoIDEVi, TEVi0, 'MSG1RECEIVED', ~pseudoIDEVi)

  ]
```

Figure 12 : Modélisation du protocole pour l'envoie et la réception d'un message

```
lemma EnvoieEtReceptionMessageM1:
  exists-trace
  "∃ Clj EVi msg #i #j.
         (CljEnvoieLeMessageM1AEVi( Clj, msg ) @ #i)
∧
         (EViRecoitM1deClj( EVi, msg ) @ #j)"
simplify
solve( CloudState( ~pseudoIDClj, ~Tclj0,
                   'NOTCONNECTEDTOEVI'
       ) ▶₀ #i )
  case Init
  solve( EViState( ~pseudoIDEVi, TEVi0,
                   'NOTCONNECTEDTOCLOUDLET',
~pseudoIDEVi
         ) ▶₁ #j )
    case Init
    solve( !KU( MAC(~SKClj.1,
                    <~Tclj0,
                     h(<pmult(~r1, 'P'),
~pseudoIDClj, ~Tclj0>)>)
           ) @ #vk )
      case CljEnvoieMessageM1AEVi
      SOLVED // trace found
    qed
  qed
qed
```

Figure 13 : Résultats de la modélisation du protocole pour l'envoie et la réception d'un message

Dans la figure 12, le cloudlet (Clj) a envoyé le message M1 au véhicule électrique (EVi) à l'instant TClj0 comme montré à l'étape 1 du cas d'utilisation 3 : Authentification mutuelle avec le cloudlet (figure 9). La règle CljEnvoieM1AEVi a été appliquée où les variables (R1 et M1) ont été calculées et le message M1 a été horodaté, crypté et envoyé.

Le message M1 a été reçu par le véhicule électrique (EVi) comme montré à l'étape 2 du cas d'utilisation 3 : Authentification mutuelle avec le cloudlet (figure 9). La règle EViReceptionM1Cloudletj a été appliquée où le message M1 a été décrypté et vérifié.

La figure 13 montre l'exécution du lemma EnvoiEtReceptionDuMessageM1aplliqué sur les deux règles, mentionnées dans la figure 12, sur Tamarin Prover avec succès.

5.2.1 Analyse de la sécurité

Dans le cadre de notre travail de recherche, notre proposition d'architecture assure plusieurs points sécuritaires dans le réseau V2G, qui sont les suivants :

- **Disponibilité**

Le modèle assure que le véhicule électrique se charge/décharge dans un temps de disponibilité réduit pour les bornes de recharge en choisissant celle qui est la plus proche et disponible. Il règle aussi le problème de la haute disponibilité et des opérations à temps réel du modèle CA Bridgé par la redondance qui a été abordé dans le chapitre précédent par Todd Baumeister [23]. La redondance et d'autres caractéristiques seront faciles à gérer sur le Cloud.

- **Authentification**

Les bornes reçoivent continuellement après chaque traitement une mise à jour de la liste des véhicules enregistrés dans la zone, ce qui minimise le risque d'être usurpé que ce soit la borne ou le véhicule. L'utilisation de la clé publique assure l'identité des éléments du réseau V2G.

- **Confidentialité et intégrité**

Le cryptage SCS basé sur ECC assure le chiffrement des certificats à clé publique et des messages échangés ainsi qu'un autre gain du temps et d'espace de stockage vu sa rapidité et une double vérification de l'identité qui est aussi assurée par l'attribution d'un bit mentionnant que le véhicule est connecté ou non.

- **Anonymat**

Il est assuré par le contrôleur qui vérifie l'identité et n'envoie que le message à la bonne entité en implémentant le processus de [13]. Ceci empêche, en cas de violation de données, de faire le lien entre le message et son propriétaire, un double anonymat assuré aussi par l'utilisation de l'infrastructure PKI.

Il existe plusieurs types d'attaque de sécurité, les suivantes ont été abordées dans [31], notre proposition les assure aussi, nous les avons introduites dans notre proposition d'architecture.

- **Révocabilité**

Avec la liste de révocation, le véhicule électrique (VE) malveillant révoqué ne pourra plus envoyer de rapport de message aux cloudlets, ni aux autres éléments du réseau électrique parce qu'il est affiché dans toutes les listes de révocation de tous les éléments participants dans le réseau électrique.

- **Traçabilité**

Pour chaque véhicule électrique (VE) qui envoie des messages malveillants, la centrale de certification (CA) peut retracer sa véritable identité puisqu'il est déjà dans la liste des révocations.

- **Non-répudiation**

Un attaquant qui est révélé par la centrale de certification (CA) ne peut pas nier son comportement d'attaque puisqu'il est déjà dans la liste des révocations et il y a une traçabilité sur les fichiers journaux du CA sur le cloud.

- **Attaque d'usurpation d'identité**

L'adversaire doit connaitre le mot de passe de connexion du véhicule électrique en temps polynomial, ce qui est impossible surtout avec l'implémentation de la cryptographie ECC.

- **Homme du milieu**

L'adversaire doit passer par le contrôleur et le cloudlet pour être authentifié comme entité légitime, ce qui est impossible, car les deux se coordonnent au moment de l'authentification du véhicule, et le cloudlet a sa propre clé sécrète que l'adversaire ne peut pas avoir, donc l'attaque de l'homme du milieu ne peut pas être implémentée.

- **Attaque de désynchronisation**

Un adversaire qui essaie de modifier le message échangé entre la centrale de certification (CA) et le cloudlet ou entre ce dernier et le véhicule électrique (VE), ne pourra pas le faire, parce que les messages sont mutuellement authentifiés, même si les deux parties sont désynchronisées.

- **Attaque de relecture**

Un système d'horodatage est utilisé à chaque envoie de message et chaque récepteur vérifie la fraîcheur du message par rapport à son horodatage. Même si le message est volé, il ne pourra pas passer la vérification du temps.

- **Attaque d'initié privilégié**

Le mot de passe de l'utilisateur n'est enregistré sur aucune table, et n'est jamais transmis en texte brut. Ainsi personne d'autre dans le système ne pourra le deviner.

- **Attaque de contre identification du mot de passe hors ligne**

Si la carte intelligente du véhicule est volée, l'adversaire ne peut pas extraire le mot de passe, car il est stocké d'une façon sécuritaire avec du XOR, il ne pourra pas le découvrir en un temps polynomial.

- **Attaque de Carte intelligente volée**

Comme dit précédemment, l'adversaire ne pourra pas récupérer les informations sur la carte volée, et ne peut rien faire avec, parce qu'il n'a pas le mot de passe de l'utilisateur.

5.3 Analyse comparative

L'architecture proposée dans [13] est destinée pour les réseaux VANETs (Vehicle Adhoc Network), où le débit de la communication est trop élevé par rapport au réseau V2G, ainsi que les entités participantes. Elle a optimisé la communication, le débit et a amélioré la sécurité au sein des réseaux VANETS. Les réseaux V2G peuvent bénéficier des applications embarquées de cette proposition pour filtrer les messages échangés et assurer un certain degré d'anonymat, de fiabilité et de confidentialité. Notre proposition, avec le bit assigné au véhicule électrique et l'utilisation de l'horodatage pendant la communication, renforce l'anonymat dans les réseaux V2G ainsi que la confidentialité et la fiabilité. Nous avons prouvé ainsi, avec l'outil Tamarin Prover, que notre proposition résiste aux différentes attaques de sécurité comme l'attaque d'usurpation d'identité, de relecture, d'initié privilégié, de contre identification du mot de passe hors ligne, et de carte intelligente volée qui n'ont pas été traités dans [13].

5.4 Conclusion

Dans ce chapitre, nous avons choisi deux exemples de messages (envoie / réception) échangés dans notre protocole modélisé avec le logiciel Tamarin Prover. Ainsi les résultats obtenus montrent l'efficacité de notre modèle et appuient notre proposition sur les différents points sécuritaires et d'attaques assurés par la solution. Pour montrer les valeurs ajoutées de notre proposition, nous avons comparé nos résultats avec ceux présentés dans l'étude faite dans [13]. Cette dernière a amélioré la sécurité dans les réseaux VANETs ainsi que le débit. Mais cette étude n'a pas abordé les différents types d'attaques dont souffrent les réseaux VANETS et les réseaux V2G. Ce sont des menaces de sécurité qui touchent tout type d'entité dans ces réseaux (VANET et V2G) et qui causent des dommages lourds sur plusieurs plans humains et économiques. Pour cela, nous les avons tous identifiés dans notre étude et nous les avons étudiés et implémentés prudemment dans

notre protocole sur tous type de message échangé entre les différentes entités du réseau V2G décrites dans notre architecture.

Dans le chapitre suivant, nous présenterons une conclusion générale de notre travail en citant quelques perspectives pour un travail ultérieur (futur).

Chapitre 6 : Conclusion générale et perspectives

Plusieurs solutions ont été proposées pour remédier aux problèmes de sécurité qui ont été jugées critiques dans les réseaux V2G. Cependant, plusieurs d'entre elles ont rencontré des obstacles et des limitations, notamment la limitation matérielle et certaines sont encore en cours d'étude.

Par conséquent, pour remédier à ces défis, nous avons proposé dans le cadre de ce mémoire une solution basée sur le cloud, qui comble les problèmes du matériel (stockage, calcul, ..), de la gestion et de la sécurité en même temps et les avantages des applications embarquées proposées dans [13] pour les réseaux VANETs (Vehicle Adhoc Network). Notre proposition est renforcée par l'ajout d'un bit et l'horodatage pour sauvegarder l'état de connexion du véhicule et ainsi bloquer tout attentat d'usurpation d'identité ou d'envoie/renvoie de message à sa place, et d'autres attaques de sécurité. Aussi, la confidentialité et l'anonymat sont assurés et renforcés. Pour montrer la sécurité de notre protocole, nous avons présenté une preuve de validité et de sécurité avec l'outil de modélisation Tamarin Prover. Les résultats ont montré la faisabilité de notre proposition par rapport aux différentes attaques dans le réseau V2G. Il est vrai que sa mise en place sur le terrain est coûteuse mais, les mises à jour du réseau V2G seront par la suite moins coûteuses.

Nous pensons, pour notre prochaine étape, à proposer un routeur virtuel pour le réseau V2G. Les routeurs réseaux se basent principalement sur l'adressage, vu que les véhicules électriques sont des entités en mouvement pouvant appartenir à plusieurs cloudlets en même temps, nous pensons à introduire une nouvelle notion d'identification d'entité réseau sur le routeur V2G sur le cloud. L'adresse du véhicule électrique (VE) ressemblera à IDi.CA1.CA2. .. . CAn, c'est la concaténation du pseudo l'ID du véhicule et l'ajout des CA par niveau, chaque communication ou vérification requise d'un niveau supérieur, le cloudlet ou la centrale de certification (CA) courant ajoute à la fin de l'adresse le ID de la CA suivante, où il n'y aura pas de

limitation du nombre de CA dans le réseau V2G tout en respectant les exigences de la norme ISO 15118. L'adresse du VE sera cryptée et seules les entités concernées pourront la décrypter. Cet adressage va aider à résoudre plusieurs problèmes de sécurité comme la délocalisation d'un VE volé d'un autre continent et la reconnaissance d'un véhicule malveillant d'un autre continent et ainsi bénéficier de la rapidité, de la sécurité et de l'optimisation du routage dans la communication V2G ... etc.

Références bibliographiques

[1] Khosrojerdi, F., et al. *Integration of electric vehicles into a smart power grid: A technical review*. in *2016 IEEE Electrical Power and Energy Conference (EPEC)*. 2016. IEEE.

[2] Ji, B., et al., *Research on secure transmission performance of electric vehicles under Nakagami-m channel.* IEEE Transactions on Intelligent Transportation Systems, 2020. **22**(3): p. 1881-1891.

[3] Québec, G.d. *Véhicule électrique : Rabais pour un véhicule neuf*. 2012-2022 november, 2021]; Available from: https://vehiculeselectriques.gouv.qc.ca/rabais/ve-neuf/programme-rabais-vehicule-neuf.asp.

[4] Liu, L. and J. Zhang. *Definition and Framework Study for Aggregator of PEVs as Controllable Load in V2G Technology*. in *2018 IEEE International Conference on Energy Internet (ICEI)*. 2018. IEEE.

[5] Abbasinezhad-Mood, D., et al., *Provably secure escrow-less Chebyshev chaotic map-based key agreement protocol for vehicle to grid connections with privacy protection.* IEEE Transactions on Industrial Informatics, 2020. **16**(12): p. 7287-7294.

[6] Wang, Q., et al., *Conditional privacy-preserving anonymous authentication scheme with forward security in vehicle-to-grid networks.* IEEE Access, 2020. **8**: p. 217592-217602.

[7] Zhang, D., et al., *A Public-key Encryption with Multi-keyword Search Scheme for Cloud-based Smart Grids.* IEEE Conference on Dependable and Secure Computing (DSC), 2021.

[8] Kawoosa, A.I. and D. Prashar, *A Review of Cyber Securities in Smart Grid Technology.* 2nd International Conference on Computation, Automation and Knowledge Management (ICCAKM), 2021.

[9] Wenlin Han, Y.X., *Privacy preservation for V2G networks in smart grid: A survey.* The International Journal for the Computer and Telecommunications Industry, 2016: p. 12.

[10] Linghui Chen, J.Z., Ying Chen, Zhenfu Cao, Xiaolei Dong Kim-Kwang Raymond Choo, *PADP: Efficient Privacy-preserving Data Aggregation and Dynamic Pricing for Vehicle to Grid Networks* IEEE Internet of Things 2020: p. 11.

[11] QINGLONG WANG, M.O., YUN YANG , AND ZONGTAO DUAN, *Conditional Privacy-Preserving Anonymous Authentication Scheme With Forward Security in Vehicle-to-Grid Networks.* IEEE Access 2020: p. 11.

[12] Gupta, M., et al., *Secure V2V and V2I Communication in Intelligent Transportation ising Cloudlets.* IEEE Transaction on Services Computing 2020.

[13] Gupta, M., et al., *Secure V2V and V2I communication in intelligent transportation using cloudlets.* IEEE Transactions on Services Computing, 2020.

[14] Amazon Web Services, I.o.s.a. *AWS IoT Greengrass*. 2020 March, 2021]; Available from: https://docs.aws.amazon.com/fr_fr/greengrass/v1/developerguide/what-is-gg.html.

[15] Amazon Web Services, I.o.s.a. *GreenGrass Policies*. 2020 March, 2021]; Available from: https://docs.aws.amazon.com/fr_fr/greengrass/v1/developerguide/security_iam_id-based-policy-examples.html.

[16] AWS, *AWS Lambda*, in *AWS Lambda Guide du développeur*, I.o.s.a. Amazon Web Services, Editor. 2021, AWS: AWS web site. p. 1-2.

[17] Vaidya, B., D. Makrakis, and H. Mouftah. *Effective public key infrastructure for vehicle-to-grid network*. in *Proceedings of the fourth ACM international symposium on Development and analysis of intelligent vehicular networks and applications*. 2014.

[18] Kawoosa, A.I. and D. Prashar. *A Review of Cyber Securities in Smart Grid Technology*. in *2021 2nd International Conference on Computation, Automation and Knowledge Management (ICCAKM)*. 2021. IEEE.

[19] Mültin, M. *What is ISO 15118?* 2019 July 6, 2021; Available from: https://v2g-clarity.com/knowledgebase/what-is-iso-15118/

[20] Han, W. and Y. Xiao, *Privacy preservation for V2G networks in smart grid: A survey.* Computer Communications, 2016. **91**: p. 17-28.

[21] Zhang, L., S. Tang, and H. Luo, *Elliptic curve cryptography-based authentication with identity protection for smart grids.* PloS one, 2016. **11**(3): p. e0151253.

[22] He, D., et al., *An enhanced public key infrastructure to secure smart grid wireless communication networks.* IEEE Network, 2014. **28**(1): p. 10-16.

[23] Baumeister, T. *Adapting PKI for the smart grid*. in *2011 IEEE International Conference on Smart Grid Communications (SmartGridComm)*. 2011. IEEE.

[24] Kaur, K., et al. *A secure, lightweight, and privacy-preserving authentication scheme for V2G connections in smart grid*. in *IEEE INFOCOM 2019-IEEE conference on computer communications workshops (INFOCOM WKSHPS)*. 2019. IEEE.

[25] Javaid, U. and B. Sikdar. *A Lightweight and Secure Energy Trading Framework for Electric Vehicles*. in *2021 International Conference on Sustainable Energy and Future Electric Transportation (SEFET)*. 2021. IEEE.

[26] Garg, S., et al. *An efficient blockchain-based hierarchical authentication mechanism for energy trading in V2G environment*. in *2019 IEEE International Conference on Communications Workshops (ICC Workshops)*. 2019. IEEE.

[27] Kalogridis, G., et al. *Privacy for smart meters: Towards undetectable appliance load signatures*. in *2010 First IEEE International Conference on Smart Grid Communications*. 2010. IEEE.

[28] Kalogridis, G., et al., *Elecprivacy: Evaluating the privacy protection of electricity management algorithms.* IEEE Transactions on Smart Grid, 2011. **2**(4): p. 750-758.

[29] Chen, L., et al., *PADP: efficient privacy-preserving data aggregation and dynamic pricing for vehicle-to-grid networks.* IEEE Internet of Things Journal, 2020. **8**(10): p. 7863-7873.

[30] Luo, J., et al., *A Secure and Anonymous Communication Scheme for Charging Information in Vehicle-to-Grid.* IEEE Access, 2020. **8**: p. 126733-126742.

[31] Ahmed, S., et al., *Anonymous key-agreement protocol for v2g environment within social internet of vehicles.* IEEE Access, 2020. **8**: p. 119829-119839.

[32] Niddodi, C., et al. *Secure integration of electric vehicles with the power grid*. in *2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. 2019. IEEE.

[33] Li, M., et al. *A new modified bridge certification authority PKI trust model*. in *2006 First International Symposium on Pervasive Computing and Applications*. 2006. IEEE.

[34] Team, T.T. *Tamarin Prover Manual Security Protocol Analysis in the Symbolic Model*. 2021 January, 2022]; Available from: https://tamarin-prover.github.io/manual/book/001_introduction.html.

[35] David Basin, C.C., Jannik Dreier, Simon Meier, Ralf Sasse, Benedikt Schmidt *Tamarin Prover*. January, 2022]; Available from: https://tamarin-prover.github.io/.