UNIVERSITÉ DU QUÉBEC

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

COMME EXIGENCE PARTIELLE
DE LA MAÎTRISE EN MATHÉMATIQUES ET INFORMATIQUE APPLIQUÉES

PAR
ABDALLAH BELKAALOUL

DÉVELOPPEMENT D'UNE INFRASTRUCTURE À CLÉS PUBLIQUES POUR LES RÉSEAUX V2G

Aout 2021

Université du Québec à Trois-Rivières

Service de la bibliothèque

Avertissement

L'auteur de ce mémoire ou de cette thèse a autorisé l'Université du Québec à Trois-Rivières à diffuser, à des fins non lucratives, une copie de son mémoire ou de sa thèse.

Cette diffusion n'entraîne pas une renonciation de la part de l'auteur à ses droits de propriété intellectuelle, incluant le droit d'auteur, sur ce mémoire ou cette thèse. Notamment, la reproduction ou la publication de la totalité ou d'une partie importante de ce mémoire ou de cette thèse requiert son autorisation.

Résumé

La multiplication rapide des véhicules électriques nécessite la mise en place d'une nouvelle infrastructure et d'une nouvelle logistique pour soutenir leur fonctionnement. Par exemple, la recharge des batteries de ces véhicules nécessite une connexion physique qui permet le transfert d'électricité et les échanges de communication entre le véhicule et l'infrastructure. Ces échanges sont gérés par un réseau appelé réseau véhiculaire électrique, plus connu sous l'abréviation V2G (Vehicle To Grid). Ce réseau est régi par la norme ISO 15118 qui définit à la fois les exigences et les caractéristiques des réseaux V2G, y compris la définition des modes de communication.

La norme ISO 15118 recommande l'utilisation de l'infrastructure hiérarchique à clés publiques X.509 (Public key Infrastructure ou PKI) pour protéger les communications du réseau contre les cyberattaques. Bien que plusieurs auteurs aient identifié et critiqué les lacunes de cette proposition, ils n'ont pas réussi à proposer une solution robuste et efficace pour palier à ces lacunes. Le présent mémoire propose un protocole efficace qui comble ces lacunes tout en respectant les principaux concepts de la norme ISO 15118. En outre, il répond aux exigences les plus importantes en matière de sécurité informatique, à savoir la confidentialité, l'anonymat, l'intégrité et la non-répudiation.

La validité et l'efficacité du protocole proposé ont été confirmées à l'aide de l'outil de modélisation formelle Tamarin Prover et à l'aide du simulateur RISE-V2G. Les

résultats de la modélisation et de la simulation ont montré que notre protocole répond aux exigences de base de la sécurité informatique et qu'il est plus efficace que le protocole proposé dans la norme ISO 15118.

Abdallah Belkaaloul

Boucif Amar Bensaber

Abstract

The rapid multiplication of electric vehicles requires the implementation of a new infrastructure and logistics to sustain their operations. For instance, charging these vehicles batteries necessitates a physical connection that allows electricity transfer and communication exchanges between vehicle and infrastructure. These exchanges are managed by a network called V2G (vehicle to grid), which is governed by the ISO 15118 standard. Both the requirements and the characteristics of the V2G networks, including the definition of communication modes are defined in the standard.

The ISO 15118 standard recommends the use of X.509 hierarchical PKI (Public Key Infrastructure) to protect the network communications against cyber-attacks. Although several authors have identified and criticized the shortcomings of this proposal, they all fell short of providing a robust and effective remedial solution to alleviate them. This paper proposes an efficient protocol that addresses these shortcomings while respecting the main concepts of the ISO 15118 standard. Moreover, it fulfills the most important IT security requirements i.e. confidentiality, anonymity, integrity and non-repudiation.

The validity and effectiveness of the proposed protocol were confirmed using the formal modeling tool Tamarin Prover and the RISE-V2G simulator. The modeling and simulation results proved that our protocol meets the basic IT Security requirements and is more effective than the protocol proposed in the ISO 15118 standard.

Remerciements

On remercie Dieu le Tout-Puissant de nous avoir donné la santé et la volonté d'entamer et de terminer ce travail.

Je tiens à exprimer mes sincères gratitudes et mon appréciation à mon directeur de recherche Boucif Amar Bensaber pour ses conseils inestimables, son aide illimitées et ses encouragements constants pendant mes études de maitrise. Je serai toujours honoré et reconnaissant d'avoir travaillé avec lui.

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

Je tiens à remercier mes collègues du laboratoire LAMIA pour les précieux échanges que nous avons eu durant la réalisation de nos projets de recherches.

Je remercie, par ailleurs, tous ceux qui, de près ou de loin, m'ont soutenue et encouragée pour réussir mes études.

Enfin et surtout, je tiens à remercier mes parents, ma famille pour leurs soutiens, encouragements et aide pendant mes études.

Table des matières

Liste des tableaux

Table des figures

LISTE DES ABRÉVIATIONS

V2G	Vehicle To Grid
EVCC	Electric Vehicle Communication Controler
SECC	Electric Vehicle Communication Controller
EV	Electric Vehicle
EMSP	Electric mobility service provider
OEM	Original Equipment Manufacturer
PnC	plug and change
EIM	External Identification Means
PKI	Public Key Infrastructure
ECDSA	Elliptic Curve Digital Signature Algorithm
DES	Data Encryption Standard
AES	(Advanced Encryption Standard)
SHA	(Secure Hash Algorithm)
MD	(Message digest)
CA	Certification authority

Chapitre 1

Introduction

Le développement technologique a impacté toutes nos activités aussi bien sociales, qu'économiques, le secteur des transports étant un des domaines les plus impactés par le développement technologique. Grâce à l'intégration des technologies de l'information et de la communication, le réseau routier est devenu plus performant et plus sécuritaire. L'utilisation en temps réel des données de trafic et des données météorologiques autorise une meilleure planification des travaux (la gestion intelligente du trafic routier et le déglaçage ciblé par exemples) tout en assurant des niveaux de circulation plus élevés.

Cependant, si ce développement permet de gérer un plus grand nombre de voitures et optimiser les ressources d'entretien, il mène à des conséquences négatives sur le climat, à cause de l'augmentation des émissions de CO2 et des gaz à effet de serre. Un rapport de l'agence internationale de l 'énergie a indiqué que 56% du pétrole raffiné sera destiné au secteur du transport d'ici 2040 [8].

Pour répondre au changement climatique, les pays industrialisés ont pris des engagements pour réduire les émissions des gaz à effet de serre en s'orientant vers

des énergies propres et en s'éloignant des matières fossiles (charbon et pétrole surtout). Dans le secteur du transport, l'élimination progressive des véhicules à combustion interne et leur remplacement par les véhicules électriques est une des solutions considérées. En effet, une étude a indiqué que l'utilisation des véhicules électriques peut réduire les émissions de CO2 de 70% [9].

L'utilisation des véhicules électriques peut non seulement contribuer à la diminution de l'émission des gaz à effet de serre mais peut aussi contribuer à la réduction des prix des énergies renouvelables. D'autre part, ces véhicules peuvent être utilisés comme dispositifs de stockage d'énergie électrique au besoin, et vont donc rendre l'énergie éolienne ou solaire encore plus attrayantes. Des études ont mentionné que d'ici 2025, le marché automobile prévoit que le nombre de véhicules électriques dépassera 6,5 millions de véhicules par an dans le monde [10]. Au Québec, il y a présentement plus de 102 000 véhicules électriques sur les routes et ce nombre atteindra les 600 000 d'ici 2026 [11].

L'introduction de nombreux véhicules risque d'être difficile à gérer et pourrait entrainer des problèmes de capacité des infrastructures. Des communications fiables entre les véhicules et les infrastructures sont un des moyens indispensables pour remédier à une partie des problèmes qui peuvent émerger. Les développeurs des véhicules électriques ont proposé le réseau véhiculaire électrique (V2G) pour l'échange des informations et de l'énergie entre les véhicules et les infrastructures à travers les bornes de recharge. Le réseau V2G utilise les technologies de l'information et de la communication pour améliorer les performances globales des véhicules électriques et des bornes de recharge [12]. Cela permet d'échanger, entre autres, la quantité d'électricité nécessaire, les tarifs, les informations de véhicules et la disponibilité de l'électricité.

Ainsi, sous le processus d'échange d'énergie entre le véhicule et la borne, plusieurs informations personnelles sensibles doivent être échangées entre le véhicule et

la borne. Ces informations peuvent englober des données telles que l'identité du propriétaire, l'immatriculation du véhicule, la capacité énergétique, les informations des cartes bancaires et les contrats entre le gestionnaire de l'infrastructure électrique et le véhicule. Ces informations sont sujettes aux risques de cybercriminalité. Pour protéger ces informations, plusieurs systèmes ont été proposés pour combattre les attaques en assurant la confidentialité, l'intégrité et la non-répudiation des informations échangées entre les véhicules et les bornes de recharges et l'anonymat des entités.

De même, l'authentification a une importance considérable dans les échanges V2G. Son but est d'empêcher les utilisateurs illégaux d'accéder au réseau et de se faire passer pour des utilisateurs légaux. Dans le processus d'authentification par nom réel, les données privées des véhicules seront divulguées si certaines informations sensibles (par exemple, l'identité du véhicule) sont envoyées à la borne en texte clair. Les véhicules peuvent même être suivis illégalement en utilisant les informations extraites illicitement. La technologie d'authentification anonyme de l'identité peut permettre de vérifier l'identité légale des utilisateurs sans révéler d'information sensible. De ce fait, l'authentification anonyme occupe une place critique dans le sécurité informatique et est devenue l'une des principales orientations des chercheurs.

La norme ISO 15118 [13], qui est le standard officiel du réseau V2G, a recommandé l'utilisation de la PKI X.509 [14] pour la sécurité des informations transmises au sein de ce réseau. Le modèle de PKI proposé dans la norme ISO 15118 présente plusieurs lacunes telles que l'interopérabilité, la longueur du chemin de certification et le type de certificat utilisé [15]. De plus, l'authentification anonyme n'est pas requise selon la norme ISO 15118. Pour remédier à ces lacunes, nous allons présenter un protocole efficace basé sur l'anonymat et qui améliore la norme ISO-15118 tout en respectant les caractéristiques de base du réseau.

Notre protocole fournit une authentification anonyme entre les différentes entités du réseau V2G. Il assure la confidentialité, la non-répudiation et l'intégrité et résout le

problème d'interopérabilité en divisant le réseau V2G en plusieurs domaines ; chaque domaine est autonome, avec la possibilité d'échanges entre domaines à travers les autorités de certification racines.

Dans notre protocole, l'entité initiatrice génère sa pseudo-entité et son certificat, à travers une clé générée par l'autorité de certification. Les autres entités impliquées dans la communication vérifient la validité de la pseudo-entité et des certificats à travers une clé diffusée par l'autorité de certification. Pour prouver l'efficacité du protocole proposé, le mémoire inclut une modélisation formelle par l'outil de modélisation Tamarin Prover. Par ailleurs, des simulations effectuées en utilisant le simulateur Rise V2G et leurs résultats y sont présentés.

Le reste de ce mémoire est organisé comme suit : le deuxième chapitre porte sur le réseau V2G et la sécurité informatique. Le troisième chapitre présente un aperçu de la littérature sur les PKI dans les réseaux ad hoc véhiculaires (VANET) et les réseaux V2G. Le chapitre 4 présente l'article scientifique, décrivant notre protocole, qui a été soumis et accepté à la conférence IEEE International Symposium on Computer and Communication 2021. Le chapitre 5 présente le simulateur utilisé, les scénarios de simulation considérés et les résultats de l'analyse comparative. Le dernier chapitre comporte nos conclusions et les perspectives de recherche sur le sujet.

Chapitre 2

Concepts de base du réseau V2G et de la sécurité informatique

Le réseaux véhiculaire électrique V2G constitue un nouveau type de réseau qui s'est développé suite à l'émergence des véhicules électriques. Il est issu des réseaux véhiculaires VANET. Il se démarque de ces réseaux par ses composants et ses caractéristiques notamment la mobilité. Ce réseau permet aux véhicules électriques d'établir des communications nécessaires pour le processus de recharge.

La norme ISO 15118 [13] est le standard s'appliquant excluisvement au réseau V2G. Elle spécifie les communications entre les véhicules électriques et les bornes de recharge. Cette norme, publiée initialement en 2013, a été modifiée et enrichie a plusieurs reprises par la suite. Elle est divisée en 8 parties, listées plus bas selon leur date de publication :

Partie 1 : Concepts de base du réseau V2G et cas d'utilisation (avril 2013).

Partie 2 : Exigences de base des couches 3 et 7 du modèle OSI (mars 2014).

Partie 3 : Exigences de base de la couche physique et de la couche liaison de données du modèle OSI (mai 2015).

Partie 4 : Tests de conformité des protocoles réseau et application (mai 2018).

Partie 5 : Tests de conformité de la couche physique et de la couche liaison de données du modèle OSI (mai 2018).

Partie 8 : Exigences des couches physiques et accès aux donnés pour la communication sans fil (mai 2018).

Partie 20 : Deuxième génération de la partie exigences relative aux réseaux et aux protocoles d'application (2020).

Partie 9 : Tests de conformité de la couche physique Wifi et d'accès au donnés (prévue à la fin de 2021).

Dans la suite de ce chapitre, nous présentons les différents composants du réseau V2G. Nous y décrivons également les exigences de la sécurité informatique définies dans la norme et les mécanismes proposés pour les réaliser.

2.1 Composants du réseau V2G

Selon la norme ISO 15118, le réseau V2G comprend plusieurs entités (acteurs) divisées en deux groupes, des acteurs principaux et des acteurs secondaires. Les acteurs principaux sont les véhicules électriques (Electric vehicle) et les bornes de recharge (Grid), tandis que les acteurs secondaires sont les autorités de certification, l'OEM (Original Equipment Manufacturer), l'opérateur de mobilité électronique et

l'opérateur de flotte.

2.1.1 Acteurs Principaux

Les acteurs principaux sont des entités impliquées directement dans l'opération d'échange de l'électricité.

Véhicule électrique (VE)

C'est un véhicule propulsé par un moteur électrique tirant son énergie d'une ou plusieurs batteries. Pour charger ses batteries, le véhicule électrique est muni d'un système appelé EVCC (Contrôleur de communication pour véhicules électriques) qui lui permet de communiquer avec la borne de recharge.

Borne de recharge

La borne de recharge, dite équipement d'alimentation des véhicules électriques (EVSE), est l'équipement qui fournit l'énergie électrique aux véhicules électriques. La borne est utilisée pour facturer les frais de recharge des véhicules électriques. Elle est munie d'un adaptateur appelé contrôleur de communication de l'équipement d'alimentation (SECC) qui lui permet de communiquer avec le véhicule.

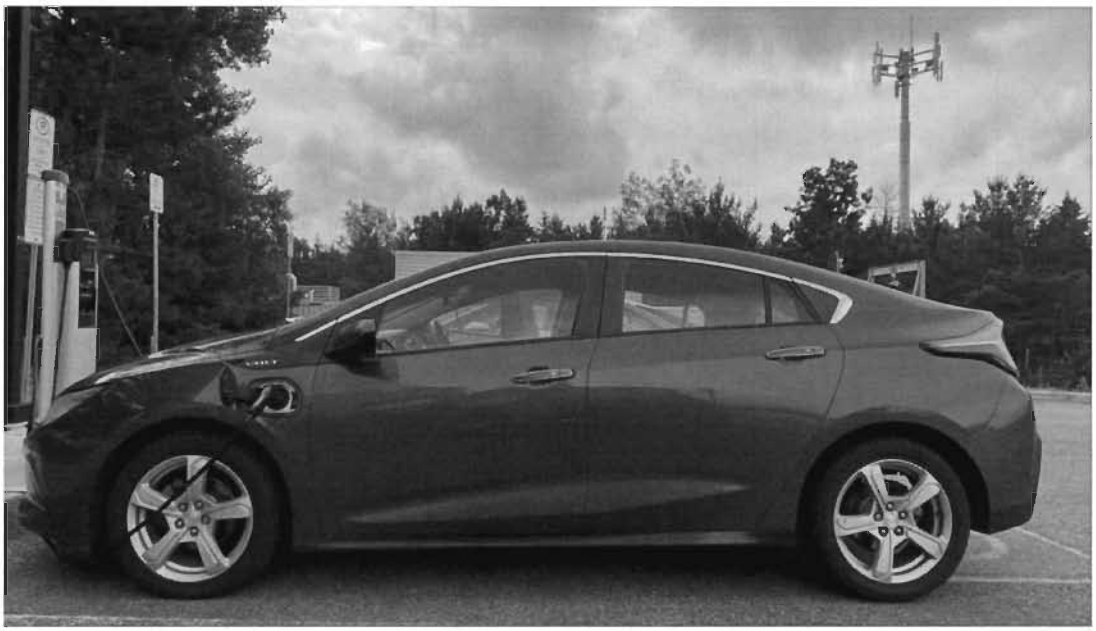

FIGURE 2.1 – Vue globale des acteurs principaux dans le réseau électrique de l'UQTR.

2.1.2 Acteurs secondaires

Les acteurs secondaires sont des entités qui jouent un rôle indirect dans l'opération de charge et de décharge. Parmi ces entités, on trouve :

Fournisseur de services

C'est une entité impliquée indirectement dans l'opération de recharge en offrant des services à valeur ajoutée tout au long du parcours de recharge à travers l'EVSE.

OEM

l'OEM est la compagnie qui a originalement fabriqué les véhicules électriques et les bornes de recharge.

Opérateur de mobilité électronique

C'est l'entité qui offre tous les services de recharge avec un contrat au véhicule. Elle comprend les fournisseurs de l'électricité et les gestionnaires de réseaux (par exemple Hydro-Québec).

Opérateur de flotte

L'opérateur de flotte, c'est une personne physique ou morale qui détient plusieurs véhicules électriques. Cette personne peut avoir plusieurs contrats de service avec l'opérateur de mobilité électronique.

2.1.3 Opérations du réseau V2G

Dans le réseau V2G, on distingue plusieurs opérations permettant d'assurer l'approvisionnement de l'énergie. Certaines de ces opérations, dont le rôle est fondamental lors du chargement des véhicules électriques, sont énumérées ci-dessous :

Autorisation

C'est l'opération qui permet à la borne de recharge de vérifier si le véhicule électrique est autorisé à être chargé.

La charge

C'est l'opération qui permet au véhicule d'obtenir l'énergie électrique auprès de la borne de recharge à travers une connexion physique.

Le paiement

Cette opération est nécessaire avant chaque recharge. Elle peut se réaliser directement, par carte Hi-Pass ou travers un contrat entre le fournisseur de service et le client.

Identification

C'est la procédure qui permet au véhicule électrique de fournir ses informations d'identification telles qu'un carte de paiement ou un certificat de contrat.

Plug and charge

Est un mode d'identification basé sur un contrat, dans ce mode le véhicule électrique obtient un contrat qui lui permet de procéder à l'opération de recharge automatique-

ment sans l'intervention de l'utilisateur [16].

External Identification Means

Est un mode d'identification basé sur des moyens externes. Pour procéder à l'opération de recharge dans ce mode, des moyens externes sont nécessaires tel que Carte Hi-Pass, Carte de crédit etc [16].

2.2 Sécurité informatique des réseaux V2G

Pour aborder les problèmes liés à la sécurité des communications V2G, il est primordial de définir les exigences de la sécurité informatique et le matériel nécessaires pour réaliser ces exigences. Les principales exigences définies dans la norme ISO 15118 se résument juste seulement à la confidentialité, l'intégrité, la non-répudiation et l'authenticité.

Dans ce qui suit, nous aborderons en détail ces exigences et les mécanismes de sécurité définis dans la norme ISO 15118 afin d'assurer la sécurité des informations échangées au sein du réseau V2G.

2.2.1 Exigences de la sécurité informatique dans les réseaux V2G

Les exigences de la sécurité informatique dans le réseau V2G dépassent celles définies dans la norme ISO 15118. Dans ce qui suit, nous résumons ces exigences.

Confidentialité

La confidentialité est la protection des informations échangées entre les véhicules électriques et les bornes de recharge, c'est-à-dire ces informations ne sont pas interceptées par un tiers et ne sont pas divulguées. Ceci peut être réalisé grâce au cryptage des informations par algorithmes de cryptage symétrique et asymétrique. La norme ISO 15118 recommande l'utilisation des algorithmes cryptographiques Elliptic Curve Digital Signature Algorithm (ECDSA) pour la cryptographie asymétrique, dans ce mécanisme chaque entité a une paire de clés publiques / privées. Pour la cryptographie symétrique, la norme recommande les algorithmes AES128.

Intégrité

L'intégrité permet de vérifier que les informations transmises au sein du réseau V2G n'ont été ni modifiées ni altérées ni détruites durant la transmission, car l'information reçue doit correspondre à l'information envoyée. Le destinataire pourra alors corroborer l'identité de l'expéditeur lors de la transaction. Pour atteindre cet objectif, la norme ISO 15118 recommande l'utilisation de la signature numérique pour assurer que les informations n'ont pas été altérées durant la transmission. À l'arrivée du message, la signature doit être vérifiée pour la valider l'intégrité des informations.

Non-répudiation

La non-répudiation consiste à assurer qu'une donnée a été réellement envoyée par son expéditeur et reçu par l'entité destinatrice, elle empêche le destinateur de nier l'envoi d'un message. En d'autres termes, la non-répudiation fournit au destinataire la preuve que l'expéditeur est responsable des messages qu'il a générés. Aussi, elle

vise à résoudre les litiges concernant la survenance d'une action en collectant, conservant, mettant en disposition et validant des preuves solides concernant l'action. En fournissant ces preuves, les contrevenants ou les utilisateurs qui se comportent mal ne peuvent pas nier leurs actions. Pour atteindre cet objectif dans le réseau V2G, la norme ISO 15118 recommande l'utilisation de la signature numérique.

Authentification

L'authentification est considérée comme l'exigence la plus importante de tous les systèmes. Elle permet aux entités impliquées dans la communication d'assurer la bonne identité des entités communicantes. L'authentification permet aussi aux entités du réseau de se fier aux informations diffusées. Par exemple, l'authentification permet d'éviter les attaques Sybil en attribuant un identifiant spécifique à chaque entité et de contrôler le niveau d'autorisation de chacune. Il existe deux types d'authentification : authentification des messages qui permet de vérifier la source du message et l'authentification des entités qui permet d'identifier l'identité émettrice. Dans la pratique, l'authentification peut être réalisée par la vérification de la signature numérique ou par la vérification des certificats électroniques.

Anonymat

L'anonymat est la propriété qui garantit qu'un utilisateur peut communiquer avec les autres entités sans divulguer sa vraie identité. Plutôt, l'anonymat permet d'assurer que la vraie identité du véhicule ou de la borne reste inconnue. La divulgation de la vraie identité du véhicule électrique entraine des conséquences catastrophiques dans la sécurité des acteurs du réseau V2G. Elle permet aux attaquants de retracer toutes les informations de l'entité émettrice. Malheureusement cet objectif n'est pas pris en considération dans la norme ISO 15118.

2.2.2 Mécanismes de la sécurité informatique

Pour assurer la sécurité des informations échangées, plusieurs mécanismes ont été proposés et mises en place dans les différents réseaux. Dans ce qui suit, nous résumons ces mécanismes.

Cryptographie

La cryptographie est l'ensemble des techniques qui permettent de transformer des messages en des messages codés afin d'assurer la confidentialité des informations échangées. La cryptographie ou le chiffrement est réalisé par des algorithmes de chiffrement. Dans ce mécanisme, on distingue deux mécanismes de cryptographie : la cryptographie symétrique et la cryptographie asymétrique.

Cryptographie symétrique

La cryptographie symétrique est considérée comme la plus ancienne technique de cryptographie. Elle consiste à chiffrer et à déchiffrer les informations en utilisant la même clé. Les algorithmes les plus connus et les plus utilisés dans ce type de chiffrement sont les algorithmes DES (Data Encryption Standard) et les algorithmes AES (Advanced Encryption Standard).

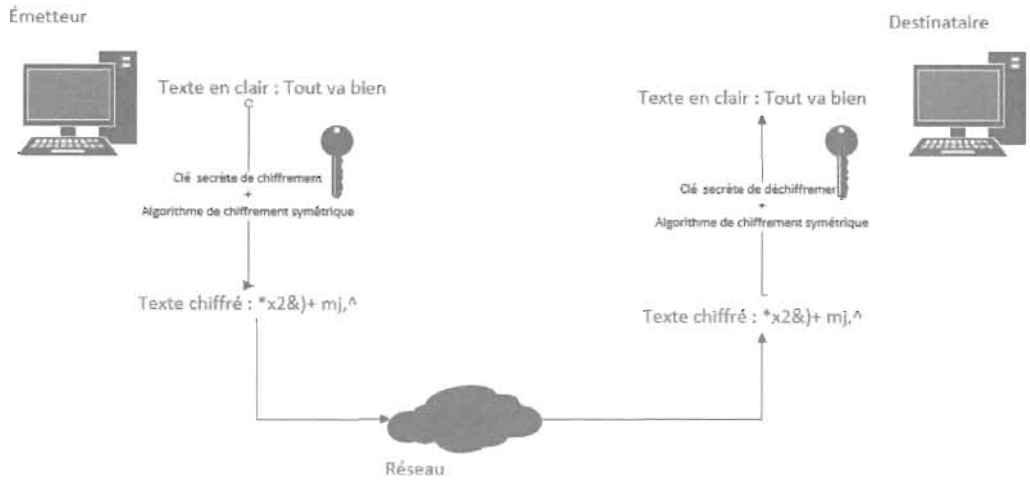

FIGURE 2.2 – Cryptographie symétrique.

Cryptographie asymétrique

La cryptographie asymétrique est un type de cryptographie qui intègre deux clés de chiffrement, une clé privée et une clé publique. La clé publique est utilisée pour crypter les informations et la clé privée est utilisée pour décrypter les informations. La clé publique est connue de toutes les entités du réseau tandis que la clé privée est dans la possession du destinataire uniquement. La norme ISO 15118 a recommandé l'utilisation des algorithmes de signature numérique à clés publiques (ECDSA) pour crypter les informations.

FIGURE 2.3 – Cryptographie asymétrique.

Hachage

Le hachage est la technique qui permet d'extraire un condensat d'un message de longueur arbitraire pour vérifier l'intégrité des données. Parmi les fonctions de hachage les plus connues, on trouve MD2 (Message digest 2), Md 4 (Message digest 4) et SHA-1 (Secure Hash Algorithm). La norme ISO 15118 recommande l'utilisation des fonctions de hachage SHA-256.

Signature numérique

La signature numérique est la technique qui permet de vérifier l'authenticité et l'intégrité des informations, elle sert à fournir la preuve de l'origine de l'identité et du statut de l'information transmise. La signature numérique repose sur la cryptographie asymétrique. Pour créer une signature, l'expéditeur extrait un condensat de l'information à l'aide d'une fonction de hachage, puis il la crypte en utilisant sa clé

privée. À la réception de l'information, le destinataire décrypte la signature à l'aide de la clé publique de l'expéditeur et extrait un condensat de l'information, ensuite il vérifie l'intégrité et l'authenticité de l'information reçue.

Certificats numériques

Le certificat numérique est une structure de données délivrée par un tiers de confiance appelé autorité de certification, elle permet de renforcer la sécurité dans le réseau V2G en attestant l'authenticité de la paire de clés publiques/privées et en identifiant les entités V2G d'une façon unique. Le certificat contient les informations suivantes :

- Numéro de série du certificat,
- Durée de validité,
- Nom de l'entité qui possède la clé publique,
- Clé publique qui est liée à l'entité,
- Algorithme de chiffrement,
- Nom de l'autorité de certification qui l'a publiée,
- Restrictions d'utilisation de la clé publique.

La Gestion et la délivrance des certificats nécessitent toute une infrastructure composée de plusieurs entités appelée l'infrastructure à clés publiques (PKI). Dans la suite de ce chapitre, nous détaillerons les notions de base d'une infrastructure à clés publiques (PKI).

2.2.3 Infrastructures à clés publiques

L'infrastructure à clés publiques consiste en un ensemble de services basés sur la cryptographie asymétrique et permet la gestion du cycle de vie des certificats numériques. La PKI à plusieurs tâches notamment la génération, la distribution, le stockage, la révocation et l'archivage des clés et des certificats. La PKI est composée principalement des éléments suivants :

Autorité de certification

L'autorité de certification est l'entité la plus importante dans l'infrastructure, parce qu'elle est l'entité responsable de la génération des certificats. Ce dernier contient plusieurs informations telles que, la clé publique, la durée de validité et les restrictions d'utilisation de la clé publique. Ce certificat est signé avec la clé privée de l'autorité de certification. Pour vérifier la validité du certificat, il faut envoyer une requête à l'autorité de certification afin de vérifier s'il est valide ou s'il a été révoqué.

Autorité d'enregistrement

L'autorité d'enregistrement est l'entité qui vérifie les demandes d'enregistrement d'un nouvel utilisateur dans l'infrastructure. Elle peut être contenue au sein de l'autorité de certification, cette répartition a pour but de séparer les charges de chaque entité. En effet, si l'autorité d'enregistrement valide la requête d'enregistrement, la demande de certificat passera directement à l'autorité de certification.

Annuaires

Pour que les utilisateurs puissent échanger leurs clés publiques, les certificats doivent être disponibles au public. Pour cela, les certificats sont publiés dans un annuaire d'accès libre. Aussi, l'annuaire peut stocker les certificats révoqués afin d'avoir un accès rapide à ces certificats.

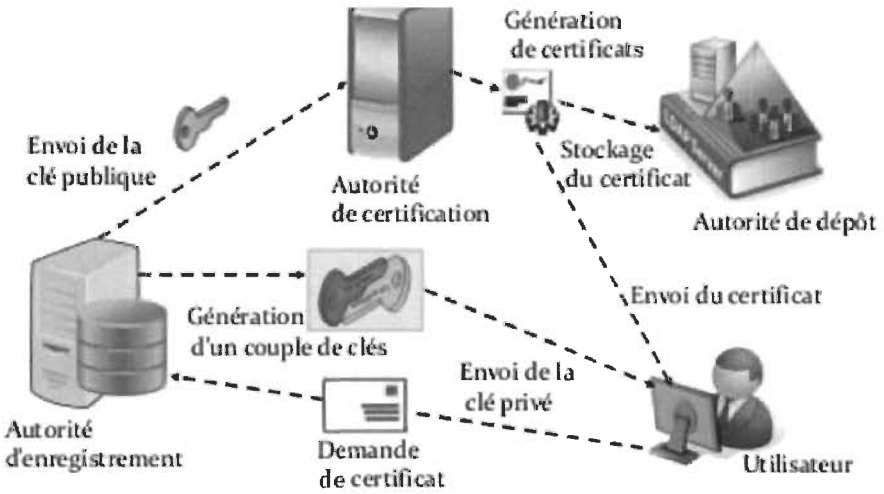

FIGURE 2.4 – Vue globale de la PKI [17].

2.2.4 Architectures de l'infrastructure à clés publiques

Modèle hiérarchique : Le modèle hiérarchique est basé sur une approche à multiniveaux avec plusieurs niveaux d'autorités de certification. Dans ce modèle, l'autorité de certification racine est placée au sommet de la hiérarchie et possède un certificat autosigné. Aussi, dans cette architecture l'autorité de certification ne délivre pas les certificats aux entités finales, elle délègue cette procédure aux autorités de certifications intermédiaires.

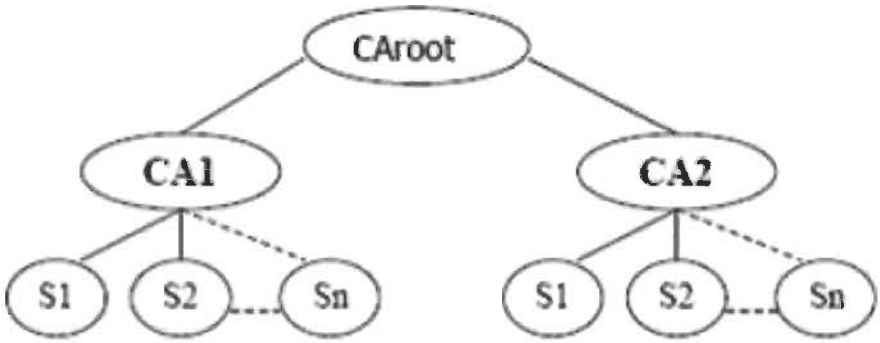

FIGURE 2.5 – PKI hiérarchique [18] .

Modèle Peer-to-peer : Contrairement à l'architecture hiérarchique, dans cette architecture les autorités de certifications ont le même niveau, c'est-à-dire les autorités de certification certifient l'une l'autre, ce qui crée une confiance bidirectionnelle. En effet, dans cette architecture les certificats sont co-signés. Elle se caractérise par la flexibilité en rendant l'extension du domaine de confiance plus pratique, mais le problème de cette architecture est dans la génération des certificats pour les autorités de certification du même niveau, ou chaque autorité de certification doit échanger ses clés publiques pour pouvoir générer des certificats, ce qui rend la gestion du système plus difficile.

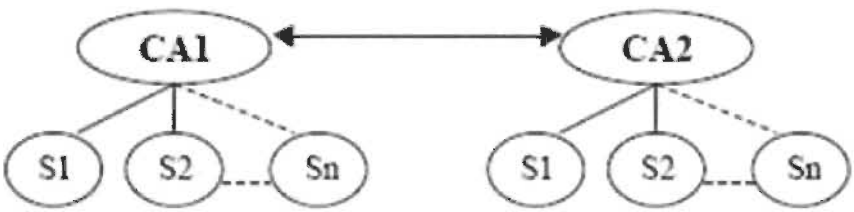

FIGURE 2.6 – PKI Peer-to-peer [19].

Modèle bridge : Pour résoudre le problème de la complexité du processus du chemin de certification des modèles hiérarchiques et Peer-to-Peer, on peut faire appel

au modèle bridge (pont). Ce modèle est une architecture qui combine les architectures hiérarchiques et Peer-to-Peer. Le modèle consiste à établir des connexions entre les autorités de certification racine à travers une autorité de certification (autorité du pont) en émettant des certificats croisés. Ceci permet d'avoir une architecture stable et de limiter le nombre d'échanges entre les autorités de certification, car il n'est pas nécessaire d'échanger la clé publique avec toutes les autres autorités, mais uniquement avec l'autorité du pont.

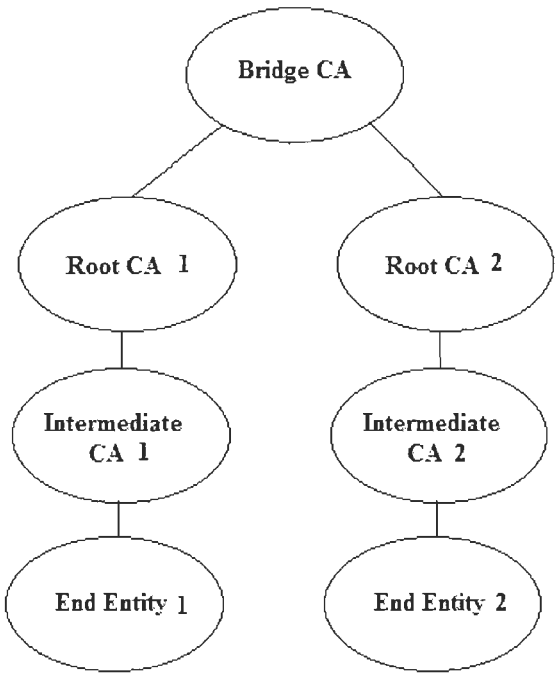

FIGURE 2.7 – PKI bridge [19].

2.2.5 Utilisation de l'infrastructure à clés publiques dans la norme ISO 15118

Dans la norme ISO 15118, la sécurité des informations échangées a une énorme importance. Pour assurer la sécurité des informations, la norme a recommandé l'uti-

lisation de l'infrastructure à clés publiques (PKI) hiérarchique X.509, cette PKI est composée d'une autorité de certification racine et plusieurs sous-autorités de certification. Dans cette architecture, l'autorité de certification racine est dans niveau le plus élevé de la PKI. Les certificats racine V2G sont considérés comme l'ancre de confiance mondiale, elles sont utilisées pour vérifier l'authenticité des certificats de contrats et des certificats SECC (voir figure 2.8). Pour le mode d'identification plug and change (PnG), le véhicule électrique obtient un certificat de contrat auprès de l'EMSP. De l'autre côté, L'EVSE obtiendra son certificat EVSE auprès de l'opérateur EVSE. Ces deux derniers certificats sont dérivées du certificat Racine V2G. La clé de vérification publique de l'AC Racine est utilisée par toutes les entités V2G pour authentifier toutes les autres entités V2G. Les autorités de certifications subordonnées ont pour but de délivrer les certificats aux entités finales. Dans ce qui suit, nous détaillerons les différents types de certificats proposés dans la norme ISO 15118.

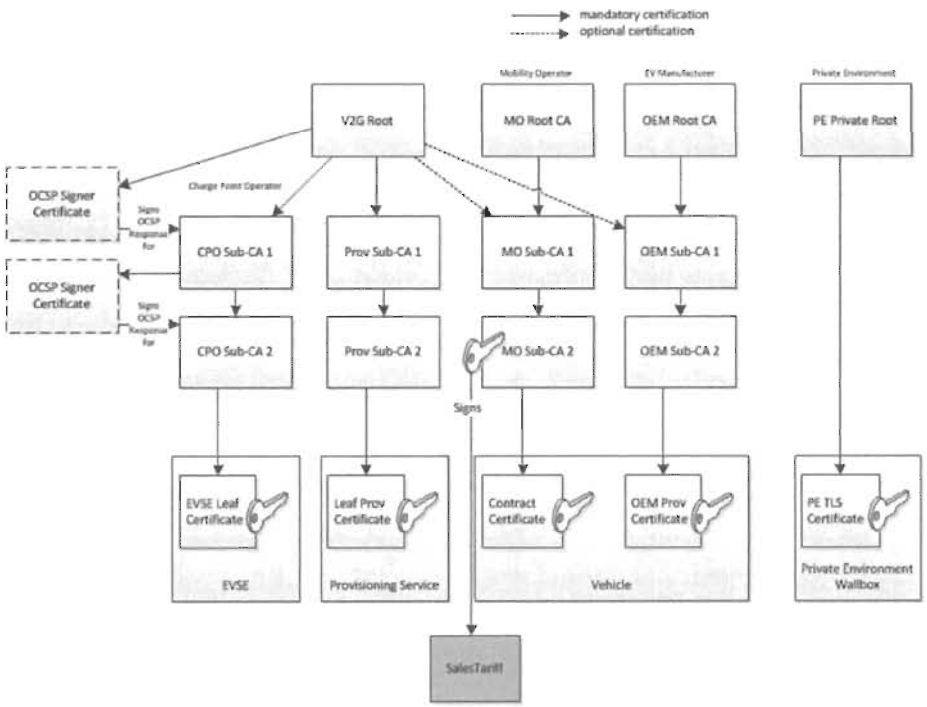

FIGURE 2.8 – PKI proposée dans la norme ISO 15118.

[13]

Types de certificats recommandés par la norme ISO 155118

Certificat Racine V2G : est un certificat du premier niveau, il est utilisé par les entités V2G pour la validation des autres certificats.

Certificat racine d'opérateur de mobilité : Ce type de certificat est utilisé pour signer des certificats de contrat.

Certificats de contrat : Ce certificat est dérivé d'un certificat racine d'opérateur de mobilité. Il est utilisé dans le mode d'identification plug and change pour représenter un contrat entre le véhicule et l'acteur secondaire.

Certificat SECC : ce certificat est utilisé par la borne de recharge pour s'authentifier auprès du véhicule. La clé privée correspondante est en possession de la borne de recharge.

Certificat racine d'opérateur privé : Ce certificat sert à faciliter la mise en place d'une infrastructure de recharge privée pour les véhicules sous le contrôle immédiat de propriétaire de l'infrastructure.

Certificat d'approvisionnement OEM : ce certificat est utilisé pour vérifier l'identité du véhicule au début du processus d'approvisionnement, il est individuel à chaque véhicule.

Certificat Racine OEM : Ce certificat est utilisé pour signer les certificats d'approvisionnement OEM, il ne fait pas partie de la PKI V2G globale. C'est-à-dire, il n'est pas nécessaire d'être signé par le certificat racine V2G.

2.3 Conclusion

La sécurité des informations a une grande importance dans tous les réseaux, notamment dans les réseaux V2G. Dans ce réseau, plusieurs informations sont échangées telles que les informations personnelles, les données privées, etc. Ces informations sont sujets aux risques des cyberattaques, pour cela la norme ISO 15118 a recommandé l'utilisation d'une infrastructure à clés publiques pour les réseaux V2G. Dans ce chapitre, nous avons présenté les concepts de base des réseaux V2G et les mécanismes recommandés dans la norme ISO 15118 pour assurer la sécurité des informations échangées au sein de ce réseau. Le modèle d'infrastructure à clés publiques recommandé dans la norme ISO 15118 peut offrir la confidentialité, l'intégrité et la non-répudiation des informations échangées au sein de ce réseau. Dans le chapitre suivant, nous allons revenir sur la littérature des PKI dans les réseaux V2G, les réseaux VANET en discutant les points forts et faibles de chaque modèle proposé.

Chapitre 3

Revue de la littérature

Ces dernières années, de nombreux protocoles et schémas ont été proposés pour garantir la sécurité des communications dans les différents réseaux. Dans la littérature, on trouve de nombreux travaux proposant différents systèmes de détection d'intrusion et d'autres travaux proposant de nouveaux mécanismes cryptographiques et de nouveaux modèles de PKI dans différents réseaux.

Dans la mesure où les réseaux VANET et V2G partagent certaines caractéristiques telles que la mobilité, la limitation des ressources de calcul et de mémoire, nous présentons dans cette section quelques travaux proposant des modèles de PKI pour les VANET en général et des modèles de PKI pour les V2G en particulier.

3.1 VANETs

Dans le but d'avoir des connaissances sur les caractéristiques des réseaux VANETs et d'identifier les lacunes et les avantages des protocoles proposés pour sécuriser les

réseaux VANETs, nous présentons dans ce qui suit une analyse de quelques travaux proposant des modèles de PKI pour les VANETs.

Dans le but d'assurer la sécurité et la confidentialité dans les VANETs, les auteurs dans [1] ont proposé un schéma d'authentification d'identité asymétrique anonyme utilisant le problème de la courbe elliptique discrète et la technique de chaine de blocs. Le protocole assure la sécurité, la confidentialité et garantit la mise à jour hors ligne, mais il ne préserve pas l'intégrité des informations échangées.

Dans [2], Han, M., et al, ont proposé un schéma d'authentification anonyme utilisant un brouillard informatique. Ce dernier est conçu pour les problèmes de congestion du réseau liés aux communications entre les véhicules et l'autorité de certification lors de l'échange de pseudonymes. L'utilisation d'un brouillard informatique pour la mise à jour et le suivi des pseudonymes permet d'assurer une communication en temps réel et de réduire les instances de réauthentification ; de plus, ce protocole garantit les exigences de sécurité des réseaux informatiques, mais avec un taux de perte de paquets assez élevé.

Dans [3], les auteurs ont proposé une PKI décentralisée construite sur un système de certificats basé sur les automates d'apprentissage et le jeu de coalition bayésien. L'authentification et la confidentialité des messages dans cette PKI sont préservées par la construction d'un arbre de Merkel basé sur une chaine de hachage. La PKI proposée garantit l'authentification, la confidentialité et l'intégrité des messages, mais ne prend pas en compte la non-répudiation et l'anonymat, ce qui peut conduire à la divulgation d'informations sur la vie privée des véhicules.

Kim, Y. et J. Lee, ont proposé dans [4] un système de sécurité et d'authentification pour les véhicules basé sur une identification utilisant une carte hi-pass et un numéro d'immatriculation. Le schéma est construit à l'aide d'un algorithme codé et d'un nombre aléatoire temporel pour l'authentification mutuelle en utilisant des réseaux de

pétris. Ce protocole garantit l'authentification et la confidentialité, mais ne garantit pas la non-répudiation, l'anonymat et l'intégrité des données.

Dans le but d'authentifier les messages transmis dans VANET, Wu, H.-T. et W.-S. Hsieh, ont proposé dans [5] un schéma pour authentifier les messages dans les plages intra et inter RSU (Road Side Unit) et le transfert entre différents RSU. Ce dernier utilise le protocole d'établissement Diffie Hellman et un code d'authentification des messages basé sur le hachage (HMAC). Ce protocole assure l'authentification, la non-répudiation et l'intégrité des informations transmises entre les différentes RSU, cependant, il ne prend pas en considération la confidentialité.

Dans [6], Fraiji, Y. et al. ont introduit les vulnérabilités de sécurité et les attaques qui peuvent être réalisées dans l'IOEV (Internet of Vehicles based only on Electric Vehicles). Dans cet article, les auteurs ont présenté l'architecture du projet PUVEC (Plateforme Urbaine pour Véhicules Électriques Connectés) qui consiste à intégrer les technologies de communication et d'informations dans le domaine des véhicules électriques afin d'améliorer les problèmes des véhicules électriques tels que le manque de station de recharge et le temps de recharge. Ensuite, ils ont identifié les vulnérabilités de sécurité du réseau IOEV en divisant les communications de véhicule à tout (V2X) en quatre groupes : V2S (véhicule à capteur embarqué), V2V (véhicule à véhicule), V2R (véhicule à infrastructure routière), V2I (véhicule à infrastructure). Pour chaque groupe, ils ont cité différentes attaques possibles. Malheurseument, les auteurs n'ont pas proposé des solutions aux vulnérabilités identifiées.

Adigun, A., B.A. Bensaber, et I. Biskri, ont proposé dans [7] un protocole de sécurité basé sur un changement périodique de pseudonymes. L'idée est d'éviter le suivi illégal des véhicules pendant leurs communications et de préserver leur vie privée et leurs informations confidentielles. Ils ont proposé deux approches différentes. La première approche consiste à demander à l'autorité de certification racine un nouveau pseudonyme et un certificat pour la communication après un temps t. Dans la

deuxième approche, chaque véhicule génère lui-même après un temps t, un nouveau pseudonyme pour la communication et un certificat en utilisant une clé générée par l'autorité de certification. Dans ce travail, ils ont évalué la bande passante utilisée en considérant la vitesse des véhicules dans chaque approche. L'échange d'informations est basé sur un schéma cryptographique asymétrique et symétrique et utilise la fonction de hachage. Cette dernière assure non seulement l'authentification, mais aussi la non-répudiation et la confidentialité. Les auteurs ont prouvé l'efficacité de leurs protocoles en utilisant le simulateur OMNET++.

3.2 V2G

Dans le but de comprendre les enjeux sécuritaires des réseaux V2G et d'identifier les lacunes des travaux proposés dans la littérature V2G, nous présentons dans ce qui suit une étude sur les protocoles déployés et proposés pour la sécurité des informations échangées au sein du réseau V2G.

Dans le but de protéger les transmissions entre la borne et le véhicule électrique, Shuaib, K., et al. ont proposé dans [9] un protocole de chargement et de paiement sécurisé (SCPP) pour les véhicules électriques rechargeables itinérants. Ce protocole assure la confidentialité des utilisateurs en utilisant une double signature. De plus, il protège l'identité des utilisateurs et des fournisseurs par l'anonymat. Ce protocole assure la sécurité des transactions de paiement et la confidentialité des utilisateurs pendant le processus de paiement ; cependant, il ne prend pas en compte la non-répudiation.

Dans [15], Vaidya, B., D. Makrakis, et H. Mouftah, ont proposé une PKI pour les réseaux V2G basée sur la cryptographie à courbe elliptique (ECC) et une technique de clé publique autocertifiée avec un certificat implicite pour la réduction du temps de

vérification. Ils ont utilisé un algorithme de programmation de chargement intelligent (SCSA). La PKI proposée comprend un ensemble d'autorités de certification racine globales V2G qui peuvent générer plus de cinq certificats autosignés. Pour prouver l'efficacité de leur système, ils l'ont comparé avec le modèle PKI proposé dans la norme ISO 15118 et ils ont démontré que le temps de traitement des certificats dans leur système est plus petit que le temps de traitement du système proposé dans la norme.

Les auteurs dans [16], ont proposé une autre architecture de distribution de PKI, où le réseau V2G est divisé en plusieurs domaines. Chaque domaine est autonome et est composé d'une autorité de certification et d'autres entités telles que les véhicules et les bornes de recharge. Dans ce modèle, le certificat racine est accessible au public. Pour les scénarios inter-domaines, ils ont défini des certificats implicites croisés Peer to Peer (P2P). Ces certificats croisés établissent les contraintes et les politiques définies par l'accord entre deux autorités de certification homologues. L'objectif principal du modèle PKI P2P proposé est d'établir une relation de confiance Peer to Peer entre deux régimes administratifs pour la communication V2G interdomaine. L'efficacité des protocoles proposés dans [15] et [16] n'a pas prouvée par la modélisation formelle ou la simulation et ils n'ont pas comparé leurs propositions avec d'autres protocoles. En outre, ces deux derniers protocoles ne préservent pas l'anonymat.

Dans le but de dériver le matériel de sécurité nécessaire à l'authentification et afin de réduire le taux de calcul, Braeken, A. et A. Touhafi, ont proposé dans [20] deux versions de protocoles d'authentification appelés AAA1 (Autonomous, Anonymous, and Authentication 1) et AAA2 (Autonomous, Anonymous, and Authentication 2). Le premier est utilisé pour la surveillance sécurisée et le deuxième permet la charge et la décharge des véhicules électriques dans un réseau intelligent. Ces deux protocoles sont efficaces en termes de sécurité, mais ils ne prennent pas en compte les exigences de base du réseau V2G.

Pour assurer l'authentification et la confidentialité des informations transmises

au sein du réseau V2G, Saxena, N. et B.J. Choi, ont proposé dans [21] un schéma d'authentification pour la charge et la décharge des véhicules électriques. Ce dernier est basé sur une technique de jumelage bilinéaire avec un accumulateur effectuant une vérification par lot. Ce schéma manipule l'authentification mutuelle entre les véhicules électriques (EV) et les autorités de certification à domicile, dans les réseaux de visiteurs et dans les réseaux centralisés ; ce qui permet de préserver la confidentialité des informations et de réduire les frais généraux de communication.

Dans [22], Liu, H., et al. Ont proposé un schéma d'authentification visant à préserver la confidentialité dans le réseau V2G. Ce schéma est applicable pendant la demande, la fourniture et le stockage d'énergie. Pour réaliser une authentification anonyme, les auteurs ont appliqué des primitives cryptographiques hybrides telles que la signature en anneau, la signature aveugle et le cryptage par procuration. Ce protocole garantit la confidentialité, l'intégrité et l'anonymat, mais il ne garantit pas la non-répudiation.

Dans [23], Guo, H., et al ont proposé un protocole unique d'authentification par lot pour les communications V2G. Dans ce protocole, l'agrégateur attend un intervalle de temps pour recevoir plusieurs réponses par lot et à la réception du lot, il le vérifie, en utilisant une signature, puis diffuse un paquet d'informations signé pour informer le lot de véhicules avec une seule signature. Ce protocole garantit l'intégrité, la confidentialité des informations échangées et réduit le temps d'authentification, mais il ne préserve pas l'anonymat des entités.

Shuaib, K., et al. ont proposé dans [24] un protocole de facturation de bout en bout, qui utilise des signatures imbriquées pour assurer la confidentialité. Ce protocole prend en charge l'authentification anonyme des utilisateurs ainsi que le paiement anonyme. Dans l'approche proposée, les auteurs ont classé les méthodes de paiement en quatre groupes : facturation de l'utilisateur privé, privilège, invité et frais d'itinérance interne-externe. Les performances du protocole ont été formellement évaluées à l'aide de l'outil

AVISPA. Les résultats de la modélisation montrent que le protocole peut répondre aux objectifs de la sécurité informatique ; cependant, aucune simulation n'a été effectuée pour une validation adéquate.

Dans le but de protéger les informations de facturation dans le réseau V2G, les auteurs dans [25] ont proposé un système de protection de la vie privée basé sur le protocole Diffie-Hellman pour générer dynamiquement des clés de session et réaliser une authentification sécurisée. Ils ont adopté une stratégie de transmission de données anonymes pour garantir l'anonymat et ont supprimé l'autorité de certification du processus de communication entre les entités du réseau V2G pour améliorer le temps de calcul. Ce protocole préserve l'anonymat et la confidentialité des données dans le réseau V2G sans avoir recours à un tiers de confiance, cependant il ne préserve pas l'intégrité des données et son efficacité n'a pas été prouvée par la simulation.

Dans [26], Roman, L.F., Gondim, P.R. et J. Lloret, ont proposé un protocole d'authentification de groupe pour l'administration et la distribution de clés dans les réseaux V2G. Ce protocole est basé sur une gestion de clé secrète de groupe, une courbe elliptique - Diffie Hellman (ECDH), une correspondance bilinéaire pour le partage de secret, l'authentification simultanée et la génération de clé de session. Cependant, l'architecture proposée est composée des véhicules électriques qui se réfèrent à toute entité mobile, la station de recharge, les agrégateurs, le serveur d'authentification et le centre de contrôle. Les performances du protocole ont été formellement évaluées à l'aide des outils AVISPA. Les résultats de la modélisation montrent que le protocole peut répondre aux objectifs de sécurité informatique ; cependant, aucune simulation n'a été effectuée pour une validation adéquate.

Pour garantir la confidentialité de la localisation des véhicules électriques, les auteurs ont proposé dans [27] un mécanisme de paiement qui améliore la confidentialité de la localisation des véhicules électriques. Ce mécanisme est basé sur plusieurs techniques cryptographiques telles que la correspondance bilinéaire, l'hypothèse de

décision DiffieHellman et la preuve de connaissance nulle. Ce système garantit non seulement la confidentialité de la localisation, mais aussi l'anonymat. Dans les cas où la traçabilité est requise (par exemple en cas de vol), le système peut fournir la localisation des véhicules ; malheureusement, ce protocole ne prend pas en considération l'intégrité des informations et la non-répudiation.

Dans [28], Xia, Z., et al. ont proposé un protocole d'authentification basé sur la signature de groupe et le fog computing pour minimiser la latence. Ce protocole est divisé en quatre étapes d'interaction entre les utilisateurs de véhicules et d'autres entités dans le réseau V2G. La première étape est l'enregistrement, la deuxième étape est la charge de l'interaction des véhicules électriques, la troisième étape est la conservation des informations de charge et la dernière étape est l'audit de l'électricité. Le protocole est prouvé par un modèle formel sous forme de ROR (Ruby on Rails). Ce protocole assure la confidentialité et l'authentification des utilisateurs de véhicules électriques et réduit les interactions entre les utilisateurs de véhicules électriques et le serveur dans l'infonuagique (cloud), mais il ne préserve pas la confidentialité des véhicules électriques ou des bornes et il n'assure pas la non-répudiation.

Dans [29], Tseng, H.-R, a proposé un protocole de communication sécurisé et préservant la vie privée pour les réseaux V2G. Ce protocole utilise une signature restrictive partiellement aveugle pour la protection des identités des propriétaires de véhicules électriques. Pour simplifier la gestion des certificats et surmonter le problème de la résolution des clés, l'auteur a choisi d'utiliser un modèle cryptographique à clé publique sans certificat. Ce protocole assure la confidentialité et l'intégrité, mais il n'assure pas l'anonymat et la non-répudiation, de plus l'efficacité de ce protocole n'a pas été prouvée ni par modélisation ni par simulation.

Dans [30], He, M., K. Zhang et X.S. Shen ont proposé un schéma d'évaluation d'attributs préservant la confidentialité pour les véhicules électriques en vue d'une recharge de qualité multiple. Le modèle de schéma est composé des entités suivantes : le véhicule

électrique d'administration (EVA), l'agrégateur (AGG) et le véhicule électrique (EV). L'EVA est responsable de l'administration des véhicules électriques dans une zone géographique telle une province. L'AGG fournit des services de recharge à tarifs multiples aux véhicules électriques et il existe un flux unidirectionnel d'électricité de l'AGG vers les VE. Pour préserver la confidentialité, les informations relatives aux VE ne sont pas accessibles à l'agrégateur pendant les évaluations d'attributs et l'EVA est la seule entité de confiance. Ce schéma garantit la confidentialité, l'anonymat et l'intégrité, mais il ne garantit pas la non-répudiation.

Dans [31], Schwerdt, R. et al. ont proposé un système de paiement et de récompense V2G sécurisé basé sur le système P4TC (Provably-Secure yet Practical Privacy-Preserving Toll Collection). Le système proposé facilite les transactions bidirectionnelles dans un cadre semi-en ligne et post-paiement. En outre, il assure la confidentialité, l'intégrité et l'anonymat, mais ne garantit pas la non-répudiation. Ce système ne traite que les transactions de paiement alors que dans les communications. V2G, il existe plusieurs types d'échanges, notamment les négociations sur le mode de facturation, les échanges d'authentification et l'enregistrement du véhicule.

Shen, G., Y. Su, et M. Zhang, ont proposé dans [32] un schéma de partage de données sécurisé. Ce schéma utilise un mécanisme de chiffrement basé sur les attributs de la politique de chiffrement en ligne et hors ligne combinés au cloud computing. Le schéma préserve la confidentialité des données et réduit le temps de calcul en divisant les informations de service en plusieurs parties, mais il ne prend pas en compte l'anonymat des entités et l'intégrité des informations échangées dans le réseau V2G.

Dans [33], Mustafa, M.A. et al. ont proposé un protocole de chargement sécurisé pour les véhicules électriques (VE) itinérants protégeant la sécurité des utilisateurs. Ce protocole comporte quatre phases : l'initialisation du système, l'enregistrement du VE, la précharge du véhicule électrique en itinérance et la postcharge du véhicule

électrique en itinérance. Ce protocole préserve la confidentialité, l'intégrité et la non-répudiation des messages des VE et des utilisateurs de VE, mais il ne garantit pas la confidentialité, l'intégrité et la non-répudiation des messages des stations de recharge.

Dans [34], les auteurs ont proposé un schéma d'authentification basé sur l'état de la batterie pour les réseaux V2G dans les villes intelligentes. Dans ce schéma, un identifiant agrégé est proposé pendant la transition de l'état de la batterie pour garantir que les véhicules électriques peuvent être authentifiés sans révéler leur identité réelle. Ce schéma assure la transition anonyme des données d'alimentation, mais il est inefficace, car il génère une énorme surcharge pendant l'authentification V2G.

L'analyse des protocoles proposés dans la littérature V2G nous a permis d'identifier les avantages et les lacunes de ces protocoles. Aussi, l'analyse des travaux proposés dans la littérature VANETs, nous a permis d'avoir plus de connaissances sur les caractéristiques de ce réseau en même temps qu'elle nous a inspiré et orienté vers des stratégies de solutions propices à une compréhension des démarches qui nous permettent d'envisager plus d'options pour notre recherche.

À notre connaissance, aucun protocole dans la littérature sur les réseaux V2G ne répond à toutes les exigences de sécurité informatique, y compris l'anonymat, et ne prend en considération les exigences de base de la norme ISO 15118.

Dans le chapitre suivant, nous allons présenter notre modèle sous forme d'article scientifique soumis et accepté à la conférence **IEEE International Symposium on Computers and Communications 2021, Athènes, septembre 2021.**.

Chapitre 4

ARTICLE SCIENTIFIQUE

Dans ce chapitre, nous présentons notre article scientifique soumis et accepté à la conférence **IEEE International Symposium on Computers and Communications, Athènes, septembre 2021.**

Résumé de l'article La multiplication rapide des véhicules électriques nécessite la mise en place d'une nouvelle infrastructure pour soutenir leurs opérations de chargement et déchargement. Par exemple, la recharge des batteries de ces véhicules nécessite une connexion permettant l'échange d'informations entre le véhicule et l'infrastructure. Ces échanges sont gérés par un réseau appelé V2G (Vehicle to Grid), qui est régi par la norme ISO 15118. Cette dernière recommande l'utilisation d'une PKI hiérarchique X.509 pour protéger les communications du réseau contre les attaques. Bien que plusieurs auteurs aient indiqué et critiqué les lacunes de cette proposition, aucun n'a proposé de solution robuste et efficace pour y remédier. Notre article propose un protocole efficace qui répond à ces lacunes tout en respectant les concepts de la norme ISO 15118. Il répond aux exigences de la sécurité informatique les plus importantes, à savoir la confidentialité, l'anonymat, l'intégrité et la non-répudiation.

La validité et l'efficacité du protocole proposé ont été confirmées en utilisant l'outil de modélisation formelle Tamarin Prover et le simulateur RISE-V2G.

Mots clé :Vehicle to Grid ; ISO 15118 Standard ; Authentication ; X.509 PKI ; Security requirements ; Attacks

Anonymous Authentication Protocol for Efficient Communications in Vehicle to Grid Networks*

Abdallah Belkaaloul
Laboratoire de Mathematiques et Informatique appliquées (LAMIA)
Department of Mathematics and Computer Science
University of Quebec at Trois-Rivieres
Trois-Rivieres, QC, Canada
Abdallah.Belkaaloul@uqtr.ca

Boucif Amar Bensaber
Laboratoire de Mathematiques et Informatique appliquées (LAMIA)
Department of Mathematics and Computer Science
University of Quebec at Trois-Rivieres
Trois-Rivieres, QC, Canada
Boucif.Amar.Bensaber@uqtr.ca

***Abstract*—Rapid multiplication of electric vehicles requires the implementation of a new infrastructure to sustain their operations. For instance, charging these vehicles batteries necessitates a connection that allows information exchanges between vehicle and infrastructure. These exchanges are managed by a network called V2G (Vehicle to Grid), which is governed by the ISO 15118 standard. This last recommends the use of X.509 hierarchical PKI to protect the network communications against attacks. Although several authors have identified and criticized the shortcomings of this proposal, but no one provides a robust and effective remedial solution to alleviate them. This paper proposes an efficient protocol that addresses these shortcomings while respecting the concepts of the ISO 15118 standard. It fulfills the most important security requirements i.e. confidentiality, anonymity, integrity and non-repudiation. The validity and effectiveness of the proposed protocol were confirmed using the formal modeling tool Tamarin Prover and the RISE-V2G simulator.**

***Index Terms*—Vehicle to Grid; ISO 15118 Standard; Authentication; X.509 PKI; Security requirements; Attacks.**

I. Introduction

Climate change is forcing the major industrial countries to reduce CO2 emissions. The use of clean energy is being promoted in all economical sectors, including the transportation sector, which is a high consumer of fossil fuels. The use of electric vehicles can contribute to the reduction of greenhouse gas emissions and can help reduce the cost of non-renewable energy. Consequently, the replacement of internal combustion (IC) vehicles with electric vehicles will be one of the key priorities to address climate change.

By 2025, the automotive market demand for electric vehicles is expected to exceed 6.5 million units per year worldwide [1].

The rapid deployment of a high number of vehicles requires the development of a massive infrastructure to allow the full success of the transition to electricity. In order to ensure safe and efficient charging and discharging operations, reliable communications between vehicles and infrastructure are necessary. Through these communications, the vehicles exchange technical data related to charging but also other critical privileged information. These communications, exchanged through the Vehicle to Grid (V2G) network, are governed by the ISO 15118 standard.

The protection of the communications against cyber-attacks is safeguarded by the use of X.509 hierarchical public key infrastructure as recommended by the ISO 15118 standard. However, this proposed model that has been criticized by several authors, who cite some shortcomings such as interoperability, length of the certification path and type of certificate used [2]. In addition, the standard does not address the issue of anonymity and does not make mutual authentication mandatory even though anonymous identity authentication technology can enable verification of users' legal identity without revealing sensitive information.

To overcome these shortcomings and improve the PKI proposed in the ISO 15118 standard, we present an efficient protocol for V2G communication. This protocol guarantees confidentiality, anonymity, integrity and non-repudiation at the same time it takes into consideration the basic requirements of the ISO 15118 standard and respects the basic characteristics of this network.

The rest of the paper is organized as follows. In the second section an overview of the literature on using PKI in V2G networks is presented. In section 3, we will present our model. In section 4, we present a detailed description of our protocol. In section 5, we present an analysis of our protocol using the Tamarin Prover modeling tool. The effectiveness of our proposed protocol and its comparison to protocol proposed in the ISO 15118 standard using the Rise V2G simulator will be presented in section 6.

II. STATE OF THE ART

In recent years, many protocols and schemes have been proposed to guarantee the security of communications in V2G networks. In the literature, there are many works proposing new cryptographic mechanisms and new models of PKI. In

978-1-6654-2744-9/21/$31.00 ©2021 IEEE

this section, we present a short overview of the literature on PKI in V2G networks.

In [3], Vaidya, B., et al., proposed a PKI architecture based on elliptic curve cryptography (ECC) and a self-certified public key technique with an implicit certificate for the reduction of verification time. They used an ECC based on a Smart Charging Scheduling Algorithm (SCSA). This PKI includes a set of V2G global root certification authority (CAs) that can generate more the five self-signed certificates. The proposed protocol was compared with the PKI model proposed in ISO 15118 but was not compared to other protocols. They have indicated that the certificate processing time in their system is smaller than the processing time of the system proposed in the standard. This protocol does not preserve anonymity and its effectiveness has not been proven by either formal modeling or simulation.

In [4], Liu, H., et al., proposed an authentication scheme to preserve privacy. This scheme is applicable during energy demand, supply and storage. To achieve anonymous authentication the authors applied hybrid cryptographic primitives such as ring signature, blind signature and proxy encryption. This protocol ensures confidentiality, integrity and anonymity but it does not ensure non-repudiation.

In [5], Guo, H., et al proposed a unique batch authentication protocol. In this protocol, the aggregator waits for a time interval to receive multiple batch responses, verifies them, using a signature and then broadcasts a signed information packet to inform the batch of vehicles with a single signature. This protocol ensures the integrity and confidentiality of the information exchanged and reduces the authentication time, but it does not ensure the anonymity of the entities.

In order to ensure the security of information transmitted within the V2G network, Shuaib, K., et al., have proposed in [6] an end to-end charging protocol, which uses nested signatures to ensure confidentiality. This protocol supports anonymous user authentication as well as anonymous payment. In the proposed approach, the authors classified the payment methods into four groups, billing the private user, privilege, guest, and internal-external roaming charge. The performance of the protocol has been formally evaluated using the AVISPA tools. Modeling results show that the protocol can meet the objectives of IT security; however, no simulation was performed for adequate validation.

In [7], et al., have proposed a group authentication protocol for the administration and distribution of keys. This protocol is based on a group secret key management, Elliptic Curve - Diffie Hellman (ECDH) and bilinear matching for secret sharing, simultaneous authentication and session key generation. However, the proposed architecture is composed of EVs which refers to any mobile entity, the charging station, the aggregators, the authentication server and the control center. The performance of the protocol has been formally evaluated using AVISPA tools. Modeling results show that the protocol can meet IT security objectives; however, no simulation was performed for adequate validation.

In [8], Xia, Z., et al., have proposed an authentication protocol based on group signature and fog computing for latency minimization. This protocol is divided into four steps of interaction between vehicle users and other entities in the V2G network. The first step is the registration, the second step is charging the interaction of electric vehicles, the third step is charging information preservation and the last step is the electricity audit. The protocol is proved by a formal model in POR form. This protocol ensures the privacy of EV users, authentication of EV users and reduces interactions between EV users and the cloud server but it does not preserve the privacy of EVs or grids and it does not ensure non-repudiation.

In [9], authors proposed a battery status-based authentication scheme for V2G networks in smart cities. In this scheme an aggregated identifier is proposed during the battery state transition to ensure that electric vehicles can be authenticated without revealing their real identities. This scheme ensures the anonymous transition of power data, but it is inefficient because it generates a huge overhead during V2G authentication.

The communication protocols for V2G networks proposed in literature do not meet some important computer security requirements, such anonymity and non-repudiation. Even though [6], [7] protocols address anonymity, they do not take into consideration the basic concepts announced in the official V2G network standard such as the use of certificates in communications. The analysis of these protocols has allowed us to identify their advantages and shortcomings.

To address the shortcomings identified in the V2G literature and to improve the protocol suggested in the ISO 15118 standard, we are proposing a robust scheme that exceeds the basic requirements of the ISO 15118 standard. It is based on anonymity and includes a mandatory mutual authentication. In this scheme, we will divide the V2G network into several domains, where each domain is autonomous with the possibility of exchanges between domains through a root certification authority. The efficiency of this protocol has been proven by using the formal modeling tool Tamarin Prover and the V2G network specific simulator Rise V2G.

III. PROPOSED SCHEME FOR THE V2G NETWORK:

In our model, the V2G network is divided into several domains (see Figure 1), each of them being autonomous and having its own root certification authority and sub-certification authorities and several other entities (electric vehicles and charging stations). The exchanges between the different domains are done through the root certification authorities. The division of the V2G network into several domains allows us to overcome the problem of interoperability and facilitates the management of the V2G network.

Before each communication establishment, the vehicles and the grid exchange their information (ID) with the certification authorities in order to have keys and pseudo entities. Several types of certificates are used, the cross implicit certificates

are used for inter-domain scenarios [2] while explicit X.509 certificates are used for local communication scenarios.

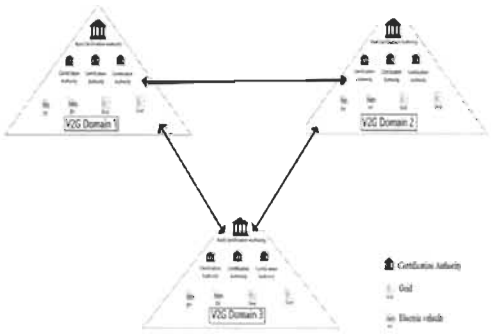

Fig. 1. Proposed PKI model for the V2G network

For cryptographic operations, a hybrid model is used. It combines symmetric and asymmetric cryptography. The latter is for the exchange of pseudo-entities and the establishment of communication sessions, while symmetric cryptography is for the exchange of information. We decided to use the RSA algorithm for the asymmetric cryptography and the AES 256 algorithm for the symmetrical cryptography. SHA-256 algorithm is used for the authentication and the integrity of the messages.

TABLE I
SYMBOLS USED IN THE PROPOSED PROTOCOL

Symbol	Description
Vs	Random key generated by the vehicle
IDv	The Original identity of the vehicle
Kpac	Public key of the certification authority
PrCa	Private key of the certification authority
PPv	The generation key of pseudo-entities and certificates for the vehicle
KVv	The verification key of the pseudo entity and generated certificates for the vehicle
KBv	The verification key of the pseudo entity and generated certificates for the grid
($\Delta 1$, $\Delta 2$)	Vehicle Key pair for asymmetric cryptography
($\Delta b1$, $\Delta b2$)	Grid Key pair for asymmetric cryptography
Bs	Random key generated by the grid
IDb	Original identity of the grid
PPb	The generation key of pseudo-entities and certificates for the grid
Fb	Pseudo-entities of the grid
Fv	Pseudo-entities of the Vehicle
Lv	Certificates generated by the vehicle
Lb	Certificate generated by the grid

IV. DETAILS OF THE PROPOSED PROTOCOL

Before starting the communication, each V2G entity generates a random key, then it sends its identity information and the generated key, to the Certification Authority (CA). The information is being encrypted by the public key of the CA. Upon receipt of the packet, the CA decrypts the packet and generates a key pair and two random keys, one for the pseudo-entity and certificate generation and the other one for the entity validation. This packet is signed by the private key of the CA and then sent to the other entity. At the same time, the CA sends the validation key to the other entities involved in the communication (see Table 1 for the symbols used in the proposed PKI model).

The protocol consists of 9 steps detailing the exchanges between the entities. A summary of all the exchanges is presented on Figure 2.

A. Electric vehicle authentication

Before starting a communication, the electric vehicle retrieves the CA public key (Kpac), then it generates a random key (Vs) and sends it to the CA with its real identity (IDv) encrypted by the public key of the certification authority (Kpac).

Upon receipt of the packet, the CA decrypts the packet and recovers Vs. Using Vs, the CA generates a key pair($\Delta 1$, $\Delta 2$) and two random keys, one for the pseudo-entity generation and certificate (PPv) and other one for the pseudo-entity and certificate validation (KVv). Then, the CA puts the key pair and the PPv key into a packet signed by the CA's private key (PrCa) and sends the packet to the EV encrypted by Vs. It finally broadcasts the verification key (KVv) to the domain grid.

B. Authentication of the grid

Before starting the communication, the grid retrieves the CA public key (Kpac), generates a random key (Bs) and then sends it to the CA with its real identity (IDb) encrypted by the Kpac.

Upon receipt of the packet, the CA decrypts the packet and recovers the random key Bs. Using Bs, the CA generates a key pair ($\Delta b1$, $\Delta b2$) and two random keys, one for pseudo-entity and certificate generation (PPb) and the other one for pseudo-entity and certificate validation (KBv). The CA puts the key pair and the generation key of pseudo-entities and certificates (PPb) into a packet signed by the CA's private key (PrCa) and then sends it to the grid encrypted by the random key generated by the grid (Bs). It finally broadcasts the verification key (KBv) to vehicles driving within the domain of the grid.

C. Establishing a communication session

Upon receipt of the packet from the certification authority, the electric vehicle decrypts the packet, generates a condensate and decrypts the signature. If the packet is falsified during transmission, it ignores it and informs the certification authority. Else, it recovers its public key and generates a pseudo-entity (Fv) and certificate (Lv) using the pseudo-entity generation and certificate (PPv), then it sends its pseudo-entity and its certificate to the grid encrypted by the grid's public key.

On the other side, the grid decrypts the packet received from the electric vehicle and verifies the authenticity and the validity of the pseudo-entity and certificate using the verification key

(KVv) received from the CA. If it is valid, it sends its pseudo-entity (Fb) and certificate (Lb) to the vehicle, encrypted by the public key of the electric vehicle. The latter decrypts the packets using its private key, then it verifies the authenticity and the validity of the grid's pseudo-entity and certificate using the key KBv received from the certification authority.

After validation of the pseudo-entities, the grid and the vehicle negotiate a session key based on Vs and Bs, then start the session.

In V2G, we distinguish two payment modes, contract-based payment (plus and charge), and external payment (payment based on the use of cards (credit card, RFID...etc.). At the beginning of the communication, the entities negotiate the payment method. In the plug and charge mode, the vehicle sends the contract certificate encrypted by the session key. Then, they define the charging mode (CA or DC). At the end of the charging session, the entities send their pseudo-Id and certificate to the Certification Authority for revocation.

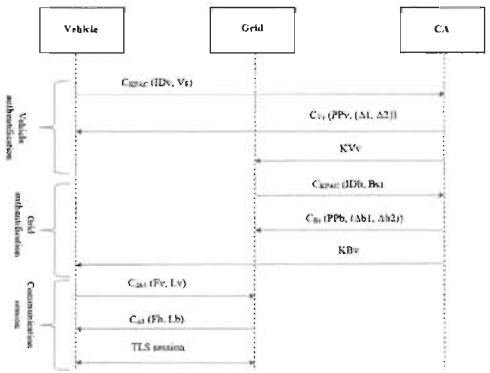

Fig. 2. Proposed PKI model for the V2G network

By using cryptography, pseudo-entities, certificate and digital signature, our protocol should ensure confidentiality, anonymity, non-repudiation and integrity. The formal analysis of our protocol will be presented in the next section.

V. PROTOCOL ANALYSIS

We present an analysis of our protocol using the formal modeling tool Tamarin Prover [10] which provides general support for modeling and reasoning about security protocols. This modeling will allow us to confirm the functioning and the efficiency of our protocol in front of Man in The Middle attacks. With this tool, the protocol and the adversary are specified using expressive language based on multisets writing rules. Thus, the adversary model integrated in Tamarin Prover controls the network. It can inject, modify and delete packets exchanged in the network. This adversary model is known as Dolev-Yao. The objectives of computer security in this tool are modeled by lemmas [10].

For the modelisation of our protocol (see Figure 3), we have defined several Rules, Random Key Generation Rules, Asymmetric Key Generation and Diffusion Rules. For the verification of the security properties, several lemmas have been defined, for checking the functioning of the protocol and for identifying the expected attacks.

```
148 rule vehicle_communication_with_server:
149
150 [ Fr(nes),
151 !Ltk($vehicle, privkeyvehicle)
152 ,!Pk($Grid, pubkeygrid)]
153
154 --[Send($vehicle, aenc(<$vehicle, nes>, pubkeygrid)), Secret(nes), Honest($vehicle), Honest($Grid), Role('vehicle')]->
155 [!F_vehicle($vehicle, privkeyvehicle, pubkeygrid, $Grid, nes),
156 Out(aenc(<$vehicle,nes>,pubkeygrid))]
157
158 rule gridreceivem:
159 [!Ltk($Grid, privkeygrid)
160 ,In(aenc(<$vehicle, nes>, privkeygrid))]
161
162 --[Recv($Grid, aenc(<$vehicle, nes>,pk(privkeygrid)))]
163 ,Secret(nes), Honest($Grid), Honest($vehicle), Role('Grid')]->
164 [!Fr_Grid($Grid, privkeygrid, $vehicle, nes)]
165 lemma executable1:
166 exists-trace
167 "Ex vehicle AC nv #i #j. Send(vehicle,nv)@i & Recv(AC,nv) @j"
168
169 lemma message_authentication:
170     "All Grid n #i. authentic(Grid,n) @i
171     ==> (Ex #j. Send(Grid,n) @j & j<i)"
172 lemma fact2:
173 exists-trace
174 "Ex vehicle Grid nes #i #j.
175 Send(vehicle, nes) @i
176 & Recv(Grid, nes) @j "
177 lemma executable2:
178 exists-trace
179 "Ex Grid AC ng #i #j. Send(Grid,ng)@i & Recv(AC,ng) @j"
180 lemma secret_N:
181 all-traces
182 "All nv #i. Secret(nv) @i & Role('vehicle') @i ==> (not (Ex #j. K(nv)@j)) | (Ex AC #j. Reveal(AC)@j & Honest(AC)@i)"
183
```

Fig. 3. The lemma and the rules used in the modeling of our protocols

The verification of our protocol has allowed us not only to verify the operability of our protocol but has also allowed us to verify that our protocol achieves the objectives of basic computer security. Given the adversary model integrated in this tool and Man in The Middle attacks target the same computer security requirements. Our protocol ensures the confidentiality, integrity and non-repudiation of the information transmitted between V2G network entities (Vehicles, Grids, Certificate Authority). Since the entities communicate using pseudo-entities our protocol ensures also the anonymity.

To assess the performance of our protocol in a V2G environment, we present in the next section, the simulation of the protocol proposed in the ISO 15118 standard and our protocol using the Rise V2G simulator.

VI. PERFORMANCE ANALYSIS

We have evaluated the effectiveness of our model against attacks that target confidentiality, non-repudiation and data integrity using simulation. We used the Rise V2G simulator which is a simulator in the form of source code to define the various components of the V2G network. It allows the simulation of various communications exchanged in the V2G networks. In our simulation, we consider a model using the ISO 15118 protocol and then a model using our proposed protocol. Using Ettercaps tool, several Man in the Middle attacks were launched to evaluate each protection protocol.

A. Simulation results

Figure 4 illustrates the difference in packets intercepted by the third party in the two models in the case of Man in the Middle attacks. The slopes of the curves represent the

interception rate. The number of intercepted packets decreases drastically when our proposed protocol is applied, compared to the PKI model proposed in the ISO 15518 standard.

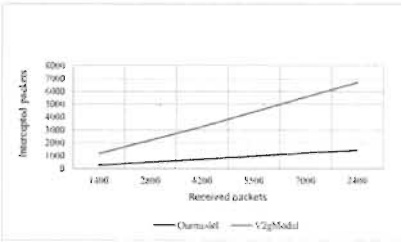

Fig. 4. Comparison of intercepted packets between V2G model and our model

The interception rate drops from 89 % to 14 %. These results demonstrate that our protocol ensures the confidentiality, integrity and non-repudiation given that Man in The Middle attack target mainly these three computer security requirements. The model ensures also anonymity since its entities generate their pseudo entities and their certificates through a key generated by the certification authority. In addition, the proposed protocol uses mutual authentication and message verification with digital signature while the ISO 15118 protocol is more lenient in this area.

VII. Conclusion

In this paper, we have presented an overview of the literature on communication protocols in V2G networks. The analysis of these protocols has allowed us to identify their advantages and shortcomings. To overcome their shortcomings, we have proposed an efficient communication protocol for the V2G network improving the basic concepts of the ISO 15118 standard. To our knowledge, our proposed protocol offers a complete solution that no other protocol in the literature offers. It handles the requirements of computer security such as confidentiality, anonymity, integrity, non-repudiation and make mutual authentication mandatory. Furthermore, it respects the basic requirements of the ISO 15118 standard. The effectiveness of our protocol has been validated using the formal modeling tool Tamarin Prover and Rise V2G simulator. The simulation results showed that our protocol is more efficient than the protocol proposed in the ISO 15118 standard in terms of interception rate and less vulnerable to attacks that target confidentiality, non-repudiation and data integrity.

References

[1] Doe,Benjamin Cuq, " Electric vehicles number prediction," January, 2020. https://www.capital.fr/auto/ventes-autonomie-la-voiture-electrique-passe-a-la-vitesse-superieure-136022.

[2] Vaidya, Binod and Makrakis, Dimitrios and Mouftah, Hussein T.Multi-domain Public key infrastructure for Vehicle-to-Grid network,IEEE Military Communications Conference, MILCOM, IEEE (2015), pp. 1572-1577.

[3] B. Vaidya, D. Makrakis and H. Mouftah, "Effective public key infrastructure for vehicle-to-grid network", Proc. 4th ACM Int. Symp. Develop. Anal. Intell. Veh. Netw. Appl., pp. 95-101, 2014.

[4] Liu, H., et al., Role-dependent privacy preservation for secure V2G networks in the smart grid. IEEE Transactions on Information Forensics and Security, 2013. 9(2): p. 208-220.

[5] Guo, H., et al., UBAPV2G: A unique batch authentication protocol for vehicle-to-grid communications. IEEE Transactions on Smart Grid, 2011. 2(4): p. 707-714.

[6] Shuaib, K., et al., Secure plug-in electric vehicle (PEV) charging in a smart grid network. Energies, 2017. 10(7): p. 1024.

[7] Roman, L.F., P.R. Gondim, and J. Lloret, Pairing-based authentication protocol for V2G networks in smart grid. Ad Hoc Networks, 2019. 90: p. 101745.

[8] Xia, Z., et al., Effective charging identity authentication scheme based on fog computing in V2G networks. Journal of Information Security and Applications, 2021. 58: p. 102649.

[9] Liu, H., et al., Battery status-aware authentication scheme for V2G networks in smart grid. IEEE Transactions on Smart Grid, 2013. 4(1): p. 99-110.

[10] Team, T., Tamarin-Prover Manual–Security Protocol Analysis in the Symbolic Model. 2016, Tech. rep. Version of 2018-11-27. https://tamarin-prover. github. io/manual ....

Chapitre 5

Analyse des résultats

Dans ce chapitre, nous résumons les principaux résultats obtenus lors de la modélisation et de la simulation de notre protocole. Nous avons réalisé nos modélisations et simulations respectivement avec les outils Tamarin Prover et le simulateur Rise V2G car leurs caractéristiques sont bien adaptées aux réseaux V2G.

5.1 Modélisation du protocole

Tamarin Prover [35] est un outil de modélisation formelle qui fournit un support général pour la modélisation et le raisonnement sur les protocoles de sécurité. Les objectifs de la sécurité informatique y sont modélisés par des lemmas. Y ce protocole et l'adversaire sont spécifiés à l'aide d'un langage expressif basé sur des règles d'écriture multi-set. Ainsi, le modèle d'adversaire intégré dans Tamarin Prover [35] contrôle le réseau et peut injecter, modifier et supprimer les paquets.

Les résultats obtenus lors de la vérification de notre protocole nous ont permis, non

seulement de vérifier l'opérabilité de notre protocole, mais aussi d'assurer que notre protocole atteint les objectifs de la sécurité informatique de base. À partir des lemmes proposés, nous pouvons dire que notre protocole assure la confidentialité, l'intégrité et la non-répudiation des informations transmises entre les entités du réseau V2G (voir figure 5.1).

```
lemma communicationbetweengridandvehicle:
  exists-trace
  "∃ Vehicle Grid mes #i #j.
        (Send( Vehicle, mes ) @ #i) ∧ (Recv( Grid,
mes ) @ #j)"
simplify
solve( Send( Vehicle, mes ) @ #i )
  case vehicle_communication_with_borne
  solve( !Ltk( $Vehicle, privkeyvehicle ) ▶₁ #i )
    case Register_pk
    solve( !Pk( $Grid, pubkeygrid ) ▶₂ #i )
      case Register_pk
      solve( Recv( Grid.1, aenc(<$Vehicle, ~n>,
pk(~ltkX.1))
             ) @ #j )
        case ReceiveNonceGridByAc
        solve( !Atk( $Vehicle, ltkAC ) ▶₀ #j )
          case Register_pk2
          solve( !KU( aenc(<$Vehicle, ~n>,
pk(~ltkX.1)) ) @ #vk )
            case vehicle_communication_with_borne
            SOLVED // trace found
          qed
        qed
      qed
    qed
  qed
qed
```

FIGURE 5.1 – Modélisation du protocole.

5.2 Simulation du protocole

La simulation permet d'évaluer la performance de notre protocole dans un environnement V2G. Pour cela nous avons utilisé le simulateur Rise V2G [36] qui est un simulateur sous forme de code source pour définir les différents composants du réseau V2G. Il permet également de simuler les échanges des différentes communications dans les réseaux V2G.

Pour prouver l'efficacité de notre protocole, nous avons étudié le nombre de paquets interceptés dans le cas où plusieurs attaques de type « Man in the Middle » sont lancées. Pour cela, nous avons considéré deux scénarios. Le premier scénario consiste à étudier l'efficacité du protocole proposé dans la norme ISO 15118 face à des attaques de type « Man in the Middle » ; alors que le deuxième scénario consiste à examiner l'impact et la valeur ajoutée de notre modèle sur les performances du réseau V2G contre ces mêmes attaques.

Dans les deux scénarios, le modèle comprend six groupes. Chaque groupe contient 5 véhicules et une borne où chaque véhicule électrique échange 250 paquets avec la borne, soit un total de 1250 paquets par groupe. Dans le premier scénario, où le protocole proposé dans la norme ISO 15118 est appliqué, le taux d'interception dépasse 86 %, alors que dans le deuxième scénario, où notre protocole est appliqué, le taux d'interception est inférieur à 14% (voir figure 5.2). Nous avons aussi évalué le nombre de paquets perdus (nombre de paquets envoyés moins le nombre de paquets reçus). Les résultats montrent que le nombre de paquets perdus lors de l'application de notre protocole est négligeable, alors que dans le scénario où le protocole de la norme ISO 15118 est appliqué, le taux de perte dépasse 6 % pour certains cas.

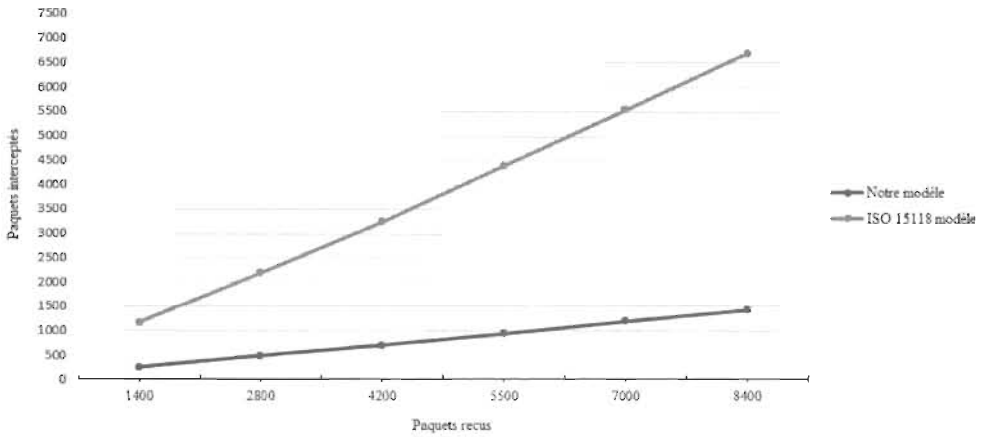

FIGURE 5.2 – Comparaison des paquets interceptés entre le modèle proposé dans la norme ISO 15118 et notre modèle.

Les résultats de la simulation montrent que notre protocole est moins vulnérable face aux attaques « Man in the Middle » et est plus efficace que le protocole proposé dans la norme. Il réalise les objectifs principaux de la sécurité informatique. De plus, on peut affirmer qu'il est très efficace en termes de confidentialité, d'intégrité et de non-répudiation, car les attaques de « Man in the Middle » ciblent essentiellement ces trois critères.

Dans ce qui suit, nous proposons une comparaison de notre protocole avec d'autres protocoles proposés dans la littérature V2G

5.3 Analyse comparative

Notre protocole proposé est conforme à toutes les exigences de sécurité informatique. Dans notre protocole, les entités génèrent leurs pseudo-entités et leurs certificats à travers une clé générée par l'autorité de certification pour assurer l'anonymat,

la confidentialité est assurée par le cryptage des informations par des algorithmes symétriques et asymétriques. L'intégrité et la non-répudiation sont assurées par la vérification de la signature numérique. La plupart des travaux disponibles dans la littérature V2G n'ont pas prouvé l'efficacité de leur modèle par un simulateur V2G. En ce qui concerne les caractéristiques de sécurité, le tableau 5.1 présente une comparaison de notre modèle avec certains protocoles existants dans la littérature.

Protocole	[15]	[16]	[27]	[28]	[31]	[32]	Notre protocole
Authentification mutuelle	Oui	Oui	Oui	Oui	Non	Non	Oui
Confidentialité	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Intégrité	Oui	Oui	Oui	Oui	Oui	Non	Oui
Non-répudiation	Non	Non	Non	Oui	Non	Non	Oui
Anonymat	Non	Non	Non	Non	Oui	Non	Oui
Conformité avec ISO 15118	Oui	Oui	Non	Non	Non	Non	Oui

TABLE 5.1 – Comparaison de notre solution avec certains protocoles existants

Les données du tableau 5.1 montrent que la confidentialité et l'anonymat sont généralement respectés par les différents modèles existants, mais pas les autres exigences de sécurité. En outre, la majorité des protocoles ne sont pas basés sur la norme ISO 15118.

Chapitre 6

Conclusion générale

Dans le but d'assurer la sécurité des informations échangées dans les réseaux V2G et de rendre les utilisateurs de ces véhicules plus confiants en ce qui concerne la sécurité de leurs données, nous avons réalisé dans le cadre de ce mémoire un état d'art sur les protocoles de sécurité des informations échangées dans les réseaux V2G entre un véhicule électrique et une borne de recharge. Ensuite, nous avons proposé un protocole de communication efficace et sécuritaire pour l'échange d'informations entre le véhicule électrique et la borne de recharge.

Notre protocole offre une solution complète qui à notre connaissance, aucun autre protocole n'offre présentement. De plus, notre protocole répond aux exigences de sécurité informatique telles que la confidentialité, l'anonymat, l'intégrité, la non-répudiation, tout en respectant les critères de la norme ISO 15118.

Dans ce protocole, les entités obtiennent leurs clés asymétriques de l'autorité de certification sur la base d'une clé aléatoire puis génèrent elles-mêmes leur pseudo-entité à partir de cette clé. La vérification de la pseudo-entité et des clés est basée sur les clés reçues de l'autorité de certification.

L'efficacité du protocole a été validée en utilisant l'outil de modélisation formelle Tamarin Prover et le simulateur Rise V2G. Les résultats des simulations ont montré que notre protocole est plus efficace que le protocole proposé dans la norme ISO 15118 en termes de taux d'interception et qu'il est moins vulnérable aux attaques qui visent la confidentialité, la non-répudiation et l'intégrité des données que celui proposé par la norme ISO 15118.

Dans nos travaux futurs, nous prévoyons prendre en charge d'autres entités (acteurs secondaires) de la Grid afin de leur intégrer les fonctions de sécurité. Ce travail est plus complexe parce qu'il prend en compte des entités homogènes appartenant à différents opérateurs. L'ajout de ces éléments sera suivi par des modifications au niveau du processus d'échange afin d'adapter le protocole aux caractéristiques (puissance, mémoire...) des entités et aux exigences techniques et à la variété des différents réseaux constituant la Grid.

Bibliographie

[1] Liu, Y., Lv, S., Xie, M., Chen, Z. & Wang, P. Dynamic anonymous identity authentication (DAIA) scheme for VANET. *International Journal Of Communication Systems.* **32**, e3892 (2019)

[2] Han, M., Liu, S., Ma, S. & Wan, A. Anonymous-authentication scheme based on fog computing for VANET. *PLoS One.* **15**, e0228319 (2020)

[3] Kumar, N., Iqbal, R., Misra, S. & Rodrigues, J. An intelligent approach for building a secure decentralized public key infrastructure in VANET. *Journal Of Computer And System Sciences.* **81**, 1042-1058 (2015)

[4] Kim, Y. & Lee, J. A secure analysis of vehicular authentication security scheme of RSUs in VANET. *Journal Of Computer Virology And Hacking Techniques.* **12**, 145-150 (2016)

[5] Wu, H. & Hsieh, W. RSU-based message authentication for vehicular ad-hoc networks. *Multimedia Tools And Applications.* **66**, 215-227 (2013)

[6] Fraiji, Y., Azzouz, L., Trojet, W. & Saidane, L. Cyber security issues of Internet of electric vehicles. *2018 IEEE Wireless Communications And Networking Conference (WCNC).* pp. 1-6 (2018)

[7] Adigun, A., Bensaber, B. & Biskri, I. Protocol of change pseudonyms for VANETs. *38th Annual IEEE Conference On Local Computer Networks-Workshops.* pp. 162-167 (2013)

[8] Bibak, B. & TEK ?NER MO ?ULKOÇ, H. A comprehensive analysis of Vehicle to Grid (V2G) systems and scholarly literature on the application of such. (2021)

[9] Shuaib, K., Barka, E., Abdella, J. & Sallabi, F. Secure charging and payment protocol (SCPP) for roaming plug-in electric vehicles. *2017 4th International Conference On Control, Decision And Information Technologies (CoDIT)*. pp. 0173-0178 (2017)

[10] Benjamin, C., Electric vehicles number prediction @ONLINE. 2020.

[11] Société de l'assurance automobile du Québec (SAAQ).Statistiques SAAQ-AVÉQ sur l'électromobilité au Québec en date du 30 juin 2021 @ONLINE.2021.

[12] Sun, Y., Feng, Z., Hu, Q. & Su, J. An efficient distributed key management scheme for group-signature based anonymous authentication in VANET. *Security And Communication Networks*. **5**, 79-86 (2012)

[13] International Organization for Standardization. Road vehicles — Vehicle to grid communication interface — ISO 15118 :2014 *@ONLINE. Published in Switzerland.*

[14] Tuecke, S., Welch, V., Engert, D., Pearlman, L., Thompson, M. & Others Internet X. 509 public key infrastructure (PKI) proxy certificate profile. (RFC 3820 (Proposed Standard),2004)

[15] Vaidya, B., Makrakis, D. & Mouftah, H. Effective public key infrastructure for vehicle-to-grid network. *Proceedings Of The Fourth ACM International Symposium On Development And Analysis Of Intelligent Vehicular Networks And Applications*. pp. 95-101 (2014)

[16] Vaidya, B., Makrakis, D. & Mouftah, H. Multi-domain Public key infrastructure for Vehicle-to-Grid network. *MILCOM 2015-2015 IEEE Military Communications Conference*. pp. 1572-1577 (2015)

[17] Tan, S., Yau, W. & Lim, B. An implementation of enhanced public key infrastructure. *Multimedia Tools And Applications*. **74**, 6481-6495 (2015)

[18] El Uahhabi, Z. & El Bakkali, H. A comparative study of PKI trust models. *2014 International Conference On Next Generation Networks And Services (NGNS)*. pp. 255-261 (2014)

[19] Diop, S. Une infrastructure à clés publiques (PKI) pour sécuriser les messages dans un réseau V2G. (Université du Québec à Trois-Rivières,2018)

[20] Braeken, A. & Touhafi, A. AAA-autonomous anonymous user authentication and its application in V2G. *Concurrency And Computation : Practice And Experience.* **30**, e4303 (2018)

[21] Saxena, N. & Choi, B. Authentication scheme for flexible charging and discharging of mobile vehicles in the V2G networks. *IEEE Transactions On Information Forensics And Security.* **11**, 1438-1452 (2016)

[22] Liu, H., Ning, H., Zhang, Y., Xiong, Q. & Yang, L. Role-dependent privacy preservation for secure V2G networks in the smart grid. *IEEE Transactions On Information Forensics And Security.* **9**, 208-220 (2013)

[23] Guo, H., Wu, Y., Bao, F., Chen, H. & Ma, M. UBAPV2G : A unique batch authentication protocol for vehicle-to-grid communications. *IEEE Transactions On Smart Grid.* **2**, 707-714 (2011)

[24] Shuaib, K., Barka, E., Abdella, J., Sallabi, F., Abdel-Hafez, M. & Al-Fuqaha, A. Secure plug-in electric vehicle (PEV) charging in a smart grid network. *Energies.* **10**, 1024 (2017)

[25] Luo, J., Yao, S., Zhang, J., Xu, W., He, Y. & Zhang, M. A Secure and Anonymous Communication Scheme for Charging Information in Vehicle-to-Grid. *IEEE Access.* **8** pp. 126733-126742 (2020)

[26] Roman, L., Gondim, P. & Lloret, J. Pairing-based authentication protocol for V2G networks in smart grid. *Ad Hoc Networks.* **90** pp. 101745 (2019)

[27] Au, M., Liu, J., Fang, J., Jiang, Z., Susilo, W. & Zhou, J. A new payment system for enhancing location privacy of electric vehicles. *IEEE Transactions On Vehicular Technology.* **63**, 3-18 (2013)

[28] Xia, Z., Fang, Z., Gu, K., Wang, J., Tan, J. & Wang, G. Effective charging identity authentication scheme based on fog computing in V2G networks. *Journal Of Information Security And Applications.* **58** pp. 102649 (2021)

[29] Tseng, H. A secure and privacy-preserving communication protocol for V2G networks. *2012 IEEE Wireless Communications And Networking Conference (WCNC).* pp. 2706-2711 (2012)

[30] He, M., Zhang, K. & Shen, X. PMQC : A privacy-preserving multi-quality charging scheme in V2G network. *2014 IEEE Global Communications Conference.* pp. 675-680 (2014)

[31] Schwerdt, R., Nagel, M., Fetzer, V., Gräf, T. & Rupp, A. P6V2G : A privacy-preserving V2G scheme for two-way payments and reputation. *Energy Informatics.* **2**, 1-21 (2019)

[32] Shen, G., Su, Y. & Zhang, M. Secure and membership-based data sharing scheme in V2G networks. *IEEE Access.* **6** pp. 58450-58460 (2018)

[33] Mustafa, M., Zhang, N., Kalogridis, G. & Fan, Z. Roaming electric vehicle charging and billing : An anonymous multi-user protocol. *2014 IEEE International Conference On Smart Grid Communications (SmartGridComm).* pp. 939-945 (2014)

[34] Liu, H., Ning, H., Zhang, Y. & Guizani, M. Battery status-aware authentication scheme for V2G networks in smart grid. *IEEE Transactions On Smart Grid.* **4**, 99-110 (2013)

[35] Team, T. Tamarin-Prover Manual–Security Protocol Analysis in the Symbolic Model. (Tech. rep. Version of 2018-11-27. https ://tamarin-prover. github. io/manual . . . ,2016)

[36] V2GClarity. RISE-V2G. https ://github.com/V2GClarity/RISE-V2G.