Stratégies de sécurité contextuelle sous contrainte énergétique pour le réseau intra Véhicule Electrique

Yosra Fraiji

Normandie Université

THÈSE

Pour obtenir le diplôme de doctorat

Spécialité informatique

Préparée au sein de l'Université de Rouen Normandie

Stratégies de Sécurité contextuelle sous contrainte énergétique pour le réseau intra Véhicule Electrique Connecté

Présentée et soutenue par
Yosra FRAIJI

Thèse soutenue publiquement le (date de soutenance) devant le jury composé de		
M. / Sidi Mohammed SENOUCI	Professeur, Université de Bourgogne	Rapporteur
M. / Sofiane OUNI	Professeur à l'INSAT, Tunisie	Rapporteur
M. / Dimitri LEFEBVRE	Professeur à Normandie Université, Université du Havre	Examinateur
Mme / Sihem GUEMARA EL FATIMI	Professeur, Sup'Com, Tunisie	Examinatrice
M. / Leila AZOUZ SAIDANE	Professeur à ENSI, Tunisie	Codirecteur de thèse
M. / Ghaleb HOBLOS	EC-HDR à l'ESIGELEC, Rouen	Directeur de thèse

Thèse dirigée par M. Ghaleb HOBLOS, laboratoire IRSEEM
et codirigée par Mme Leila AZOUZ SAIDANE, laboratoire CRISTAL, pôle RAMSIS

UNIVERSITÉ DE ROUEN NORMANDIE

MIIS

irseem

Remerciements

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

Je tiens tout d'abord à remercier mes directeurs de recherche, **Moniseur Ghaleb HOBLOS**, Professeur à l'École Supérieure d'Ingénieurs en Génie Électrique (l'ESIGELEC et **Madame Leila AZOUZ SAIDANE**, Professeur à l'École Nationale des Sciences de l'Informatique (ENSI), pour leurs encouragements, leur disponibilité et leurs précieux conseils qui m'ont aiguillés dans mes recherches et dans la rédaction de ce manuscrit.

Je tiens également à exprimer ma grande gratitude envers mes co-encadrants, **Madame Lamia ben AZZOUZ**, Maitre Assistant à l'ENSI, et **Monsieur Wassim TROJET**, Maitre Assistant à l'ESIGELEC, pour m'avoir conseillé et fait bénéficié de leurs expériences lors de ces années. J'ai pris plaisir à apprendre à vos côtés.

Mes remerciements les plus sincères vont tout particulièrement à **Mr Sidi Mohammed SENOUCI**, Professeur à l'université de Bourgogne et à **Mr Sofiane OUNI**,Professeur à l'INSAT, d'avoir accepté d'être rapporteurs de cette thèse et d'avoir consacré une partie de leur temps à la lecture de mon manuscrit.

Mes remerciements s'adressent aussi à **Mr Dimitri LEFEBVRE**, Professeur à Université du Havre et à **Mme Sihem Guemara**, Professeur à Sup'Com, d'avoir accepté d'examiner ce travail et de participer au jury de cette thèse.

Je tiens aussi à remercier tous les membres du projet PUVEC avec qui j'ai eu la chance de pouvoir travailler et passé des moments agréables. Je remercie également tous les membres du pôle RAMSIS, laboratoire CRISTAL et les membres du laboratoire IRSEEM pour la bonne ambiance de travail et également pour leurs collaborations.

Mes vifs remerciements vont à **Mr Mohamed HAMDI**, professeur à sup'Com, pour m'avoir fait l'honneur d'accepter de participer aux comités de suivi de thèse.

Résumé

Dans cette thèse, nous nous intéressons à la problématique de la sécurité des communications du réseau de capteurs intra véhicule électrique connecté. En effet, Plusieurs travaux et expérimentations ont montré que différentes attaques peuvent être menées sur ce réseau telles que l'activation des freins et la prise de contrôle du véhicule à distance, les attaques d'écoute, les attaques DoS sur les ECU (Electronic Control Unit), etc. Des solutions de sécurisation du réseau intra véhiculaire existent dont la plus connue est EVITA (E-safety vehicle intrusion protected applications), proposée dans le cadre du septième programme de recherche et développement technologique. Cependant, ces solutions de sécurité sont énergivores (elles utilisent les mécanismes de sécurité les plus robustes) et sont mal adaptées dans un contexte de contrainte énergétique (Véhicule Electrique). Pour cette raison, nous avons proposé, pour le réseau intra-véhicule électrique, une solution de sécurité basée sur le contexte. Le contexte s'adapte à l'écosystème du véhicule électrique et est composé de l'état de charge (SOC State Of Charge), la distance à la station de recharge, les conditions de trafic, le type de capteur et la capacité en mémoire et traitement des capteurs. Dans CASIEV (Context Aware Security for the Intra Electric Vehicle), le capteur passe toujours au niveau de sécurité le plus élevé selon le contexte. Ainsi, la sécurité des communications peut être assurée lorsque le niveau de la batterie est critique mais que le trafic est faible/moyen et l'énergie restante permet d'atteindre la station de recharge disponible la plus proche. La simulation a montré que CASIEV permet d'augmenter le temps d'activation de la sécurité par rapport aux solutions existantes (statiques). De plus, nous avons remarqué un gaspillage de ressources (énergie, mémoire et traitement) dans le cas où le niveau de risque d'attaques est faible. Pour cette raison, nous avons apportée des améliorations à CASIEV en tenant compte du niveau de risque et de la confiance en ce risque. RICAV (RIsk based Context-Aware security solution for the intra electric Vehicle network) a permis d'augmenter le temps d'activation du système de sécurité et de diminuer la consommation d'énergie tout en assurant la sécurité du conducteur.

Mots clés : IoEV, réseau intra-véhiculaire, sécurité contextuelle, risque, trust, énergie, station de recharge.

Abstract

In this thesis, we were interested in investigating the security issues of the intra electric vehicle network. Indeed, several works and experiments have shown that various attacks can be performed on this network such as brakes activation and vehicle remote control, eavesdropping attacks, DoS on ECUs (Electronic Control Unit), etc. Many solutions exist to secure the intra vehicle network. The most popular one is EVITA (E-safety Vehicle Intrusion Protected Applications). However, these security solutions are energy intensive (they use the most robust security mechanisms) and are not well adapted in a context of energy constraints (Electric Vehicle). Hence, we proposed a context-Aware Security solution for the Intra-Electric Vehicle network (CASIEV) that considers as a context ; the sensors memory and processing capacity, the available energy, the nearest charging station, the state of traffic to represent the specific Electric Vehicle ecosystem. In CASIEV, a sensor always switches to the highest security level depending on the context. Security is also provided when the battery level is critical, the traffic is low/medium, and the remaining energy allows to reach the nearest charging station. Simulations showed that the total activation security time provided by CASIEV is higher than the time resulting from static approaches. In addition, we noticed a waste of resources (energy, memory and processing) when the risk level of attacks is low. Hence, we improved CASIEV by considering the risk and the trust in this risk. The basic idea of RICAV (RIsk based Context-Aware security) is to reduce the security level if the risk is low improving this way the vehicle batterie autonomy. Simulations showed that RICAV has increased the activation time of the security system and reduced the energy consumption while providing the safety of the driver.

Keywords : IoEV, intra-vehicle network, context-aware security, risk, trust, energy, charging station.

Table des matières

Table des figures

Liste des tableaux

Liste des sigles et acronymes

ASIL	*Automotive Safety Integrity Level*
C-V2X	*Cellular Vehicle-to-everything*
CAN	*Controller Area Network*
CASIEV	*Context-Aware Security for the Intra-Electric Vehicle network*
CVs	*Connected Vehicles*
D2D	*Device to Device*
EVITA	*E-safety Vehicle Intrusion Protected Applications*
ECU	*Electronic Control Unit*
HSM	*Hardware Security Module*
HMAC	*Hash-based Message Authentication Code*
IoT	*Internet of Things*
IVSN	*Intra Vehicle Sensor Network*
LIN	*Local Interconnect Network*
MAC	*Message Authentication Code*
MOST	*Media Oriented Systems Transport*
RICAV	*RIsk based Context-Aware security for the intra- electric Vehicle network*
SOC	*State Of Charge*
VE	*Véhicules Electriques*

Introduction générale

Au cours des dernières années, la fabrication des véhicules a considérablement changé : les véhicules sont passés d'un système essentiellement électromécanique à un système électrique et électronique (E/E). Cela se traduit par l'utilisation accrue de systèmes et de logiciels embarqués dans les véhicules [8]. D'autre part, selon l'agence européenne pour l'environnement, le secteur des transports est devenu le principal émetteur de carbone en Europe au cours des dix dernières années. Plus de 70 % de ces émissions proviennent des voitures particulières [9]. Pour des raisons écologiques et en raison du coût élevé du carburant, les Véhicules Electriques (VE) font aujourd'hui l'objet d'une grande attention de la part des constructeurs automobiles, des clients, des agences environnementales, etc. Cependant, l'écosystème des véhicules électriques souffre toujours des capacités limitées de batteries, du temps de recharge élevé et de l'absence d'un large déploiement de stations de recharge publiques [10, 11].

De nombreuses technologies ont été intégrées aux véhicules modernes afin de leur donner la capacité d'interagir avec le monde extérieur [12]. On parle aujourd'hui du véhicule intelligent et connecté. D'après l'Union Européenne, d'ici 2023, plus de 1.1 millions de nouvelles voitures seront équipées de systèmes d'infodivertissement et de communication permettant de communiquer avec les autres véhicules et les infrastructures routières. Garantir la sécurité routière est la principale motivation de l'introduction de ces technologies. La plupart des accidents de la route sont causés par des erreurs humaines (par exemple, 70 % des accidents de la route en Europe en 2015 étaient le résultat d'erreurs humaines) [13]. En outre, l'amélioration du confort des conducteurs et des passagers représente un autre avantage de ces technologies. Les véhicules intelligents sont équipés de nombreux capteurs afin de fournir aux conducteurs et aux passagers les services d'un transport intelligent. L'IoV (Internet of Vehicle) permet aux véhicules de communiquer avec des capteurs intelligents (environnement interne) et avec d'autres entités telles que des véhicules, des serveurs, des piétons, des stations de recharge (environnement externe).

Une voiture moderne contient de 70 à 100 calculateurs (ECUs Electronic Control Unit)) en moyenne [14]. Chaque ECU s'appuie sur un ensemble de capteurs et d'actionneurs pour desservir un ou plusieurs des systèmes ou sous-systèmes du véhicule, qui vont des applications les plus simples, comme la commande des feux de courtoisie, aux applications les plus critiques, comme la commande du moteur. Ces calculateurs sont regroupés

en plusieurs sous-réseaux en fonction de leurs fonctions. Les sous-réseaux sont interconnectés par une passerelle centrale, et les ECU de chaque sous-réseau communiquent via différents systèmes de bus. Cependant, la croissance rapide du nombre de capteurs introduit un poids (câbles de réseau) et des coûts (installation, maintenance et remplacement) supplémentaires [15, 16]. Par conséquent, les communications sans fil intra-véhiculaires (réseau de capteurs sans fil intra-véhicule) sont également envisagées pour améliorer le déploiement des nœuds de capteurs [16]. Aujourd'hui, le réseau intra-véhiculaire consiste en un réseau de capteurs hybride (filaire et sans fil).

Le réseau de capteurs intra-véhiculaire (IVSN Intra Vehicle Sensor Network) est la cible des pirates informatiques en raison des informations stockées et accessibles via les capteurs embarqués dans les véhicules telles que la combinaison de verrouillage des portes du système d'entrée, les numéros de cartes de crédit, etc. L'adoption des technologies sans fil pour le réseau intra-véhiculaire a augmenté le champ des attaques. Notre première contribution, dans le cadre de cette thèse, a consisté en un état de l'art des attaques qui peuvent être menées sur l'IVSN [12]. En effet, dans la littérature, les auteurs [17–21] ont présenté différentes manières de pirater les fonctions d'une voiture comme le redémarrage du logiciel de gestion du moteur, l'activation du verrouillage des portes, le démarrage de la voiture, l'activation des ADAS (Advanced Driver Assistance Systems), le piratage du système d'injection électrique [22].

Pour éviter ces attaques, de nombreux travaux [4, 23–26], dans la littérature, ont proposé des solutions de sécurité statiques pour l'IVSN. La plus populaire est EVITA [4, 27] (E-safety Vehicle Intrusion Protected Applications) un projet financé par l'Union européenne dans le cadre du septième programme de recherche et développement technologique. L'objectif principal d'EVITA est de fournir une architecture de sécurité matérielle pour le réseau embarqué des automobiles. Aujourd'hui, EVITA est en train de devenir une norme de facto pour les fabricants de microcontrôleurs [27]. Les solutions existantes sont basées sur les mécanismes de sécurité les plus robustes tels que l'authentification forte et le cryptage, qui consomment beaucoup d'énergie [28–31]. Ainsi, malgré leur importance, ces travaux n'ont pas pris en compte la contrainte énergétique des véhicules électriques lors de la conception des solutions de sécurité. Dans [31], nous avons montré que les solutions de sécurité statiques consomment environ 15 % de la batterie pendant

un trajet de deux heures. Ces solutions peuvent épuiser la batterie lorsque sa charge est faible et qu'il n'y a pas de stations de recharge disponibles à proximité, en particulier dans les zones rurales ou les zones isolées peu peuplées. Cette situation peut donc rendre les déplacements dangereux pour les conducteurs, en particulier la nuit.

Notre deuxième contribution a consisté à proposer une solution de sécurité, appelée CASIEV (Context-Aware Security for the Intra-Electric Vehicle network) [31, 32], qui diffère des solutions de sécurité proposées pour le réseau intra-véhiculaire (solutions statiques) par l'utilisation du contexte du véhicule pour fournir un compromis entre la sécurité et la consommation d'énergie . Le contexte prend en compte l'état de charge (SOC State Of Charge), la distance à la station de recharge, les conditions de trafic, etc. De même, CASIEV définit des niveaux de sécurité selon leur consommation d'énergie et leur robustesse. Dans la solution proposée, même si la batterie est faible, le système tient compte de la distance jusqu'à la station de recharge et de l'état du trafic pour évaluer le niveau de sécurité approprié. Le niveau de sécurité tient toujours compte de la sécurité du conducteur (ne pas dépasser une valeur seuil de la batterie) . L'évaluation de la solution proposée a montré que CASIEV permet une activation plus longue du système de sécurité que les solutions existantes (statiques) et une optimisation de la consommation d'énergie .

Afin d'améliorer le temps d'activation du système de sécurité, nous avons apportée des améliorations à CASIEV en tenant compte du niveau de risque et de la confiance en ce risque. Le risque est défini comme le produit de la probabilité de menace par l'impact [7]. La probabilité de menace estime la faisabilité de l'attaque. L'impact (également appelé sévérité) indique l'évaluation du niveau et de l'intensité du risque. De nombreux travaux dans la littérature [33–36] ont étudié l'évaluation des risques. De plus, certains travaux [37–41] ont conçu des solutions de sécurité basées sur le risque. En effet, les auteurs adaptent le niveau de sécurité à la valeur du risque d'intrusion dans le réseau. Cependant, à notre connaissance, aucune solution de sécurité basée sur le risque n'a été proposée pour le réseau intra-véhiculaire. RICAV (RIsk based Context-Aware security for the intra- electric Vehicle network) [42], notre troisième contribution dans ce travail , est une solution de sécurité contextuelle basée sur le risque et la confiance qui permet d'augmenter le temps d'activation du système de sécurité tout en assurant la sécurité du conducteur.

En effet, si le risque est faible (resp. élevé) et la confiance en ce risque élevée (resp. faible), il est inutile de demander un niveau de sécurité énergivore.

Cette thèse est organisée comme suit (voir figure 1) :

- Dans le premier chapitre, nous présentons le réseau de véhicules connectés. Ainsi„ nous détaillons l'architecture du réseau et nous déterminons les différents types de communication envisagés pour ce réseau. De même, nous identifions les attaques qui peuvent être menées sur ces communications et plus précisément, sur le réseau intra-véhiculaire.

- Dans le deuxième chapitre, nous présentons un état de l'art des solutions existantes pour la sécurisation du réseau intra-véhiculaire. De plus, nous élaborons une analyse énergétique pour différentes configurations de sécurité afin de prouver que le choix des mécanismes de sécurité a un impact sur la consommation énergétique. De même, nous présentons un état de l'art des solutions de sécurité adaptatives, qui permettent d'offrir les services de sécurité en se basant sur un contexte donné.

- Dans le troisième chapitre, nous présentons la solution CASIEV, qui s'adapte à l'écosystème du véhicule électrique, pour offrir un compromis entre la sécurité des communications du réseau IVSN et la consommation d'énergie. De même, nous procédons, e à des simulations, pour évaluer la consommation d'énergie, le temps d'activation de la sécurité et le temps de latence de CASIEV.

- Dans le quatrième chapitre, nous décrivons la solution RICAV, qui est une amélioration de CASIEV et qui prend en compte le risque et la confiance en ce risque. De plus, nous comparons les performances de CASIEV et RICAV en termes de consommation d'énergie et de temps d'activation de la sécurité.

Enfin, nous présentons la conclusion et les perspectives.

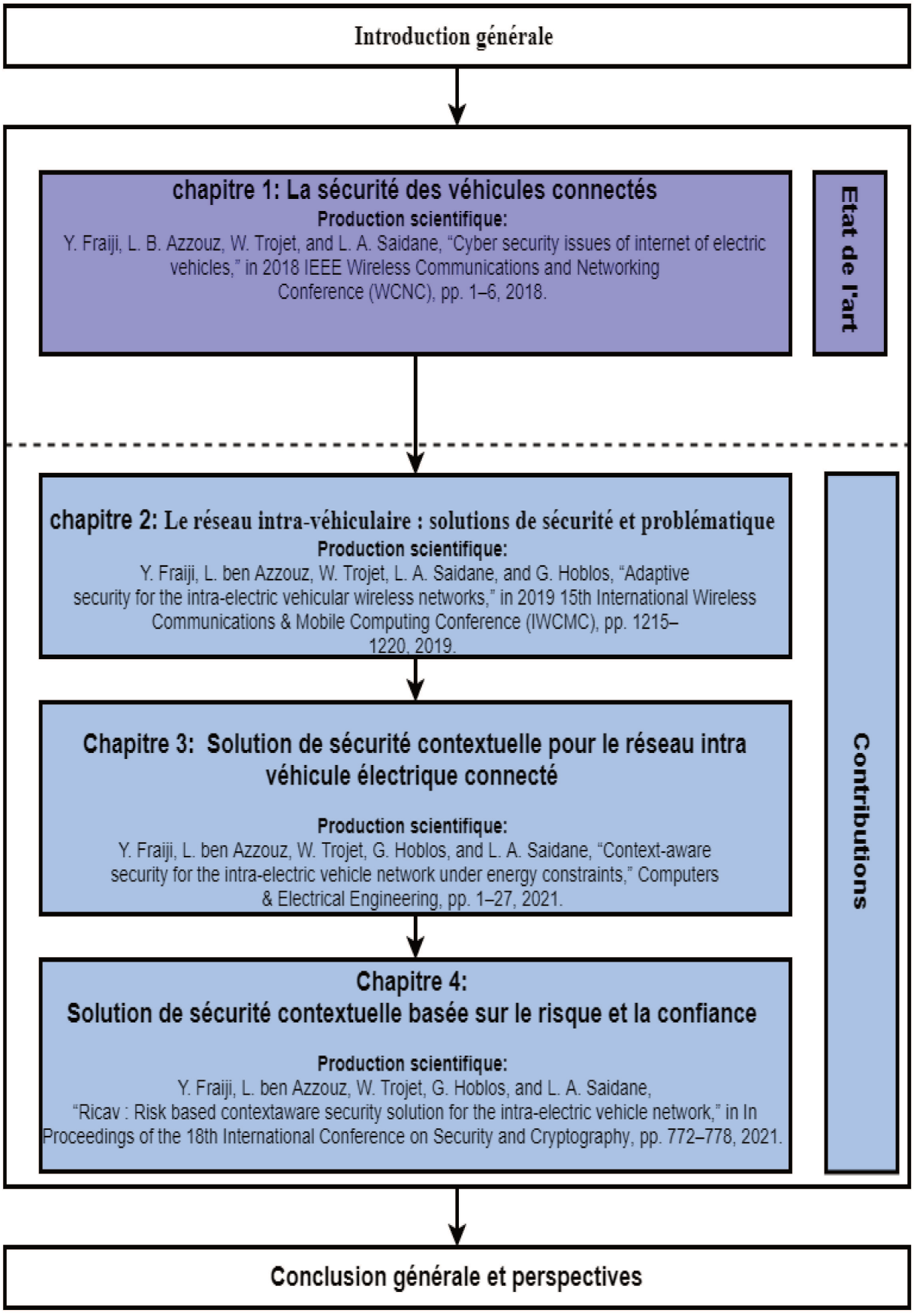


Fig. 1 : Plan de la thèse

Chapitre 1

La sécurité des véhicules connectés

1.1 Introduction

Le réseau de véhicules connectées (connected vehicles (CVs)) (nommé aussi L'Internet of Vehicules (IoV)) [43, 44] est un système distribué à grande échelle pour l'échange d'information entre les véhicules et leurs environnement (Vehicule-to-X(V2X)), selon des protocoles de communication sans fil (802.11p WAVE standard, des technologies cellulaires, etc) [43, 44]. Il est formé de multiples entités telles que des véhicules, des panneaux de signalisation, des capteurs, des piétons, etc. Ces entités peuvent communiquer et interagir ensemble pour collecter et diffuser des informations relatives aux véhicules et à l'environnement.

Ces dernières années, les organismes gouvernementaux ont augmenté leurs investissements pour améliorer la gestion du trafic, la sécurité routière et la communication véhiculaire. Le trafic mobile devrait être multiplié par trois entre 2016 et 2021, poussant le nombre d'appareils mobiles à l'extrême, avec 107 appareils par km2 et plus de 125 milliards d'appareils dans le monde d'ici 2030, une grande partie d'eux sont des véhicules [45, 46]. De même, pour des raisons écologiques et de coût élevé du carburant, on assiste, ces dernières années, à un intérêt grandissant envers la voitures électrique (Electric Vehicles EVs). Cependant, ces véhicules souffrent encore du problème d'autonomie de batterie, de déploiement à large échelle des stations de recharge et du temps de recharge.

Les véhicules intelligents sont aujourd'hui devenus une plate-forme multi-capteurs, qui génèrent chaque jour environ 4000 Go de données [47]. Ainsi, Le flux de données généré par ces capteurs (lidar, caméra, GPS, radar, l'unité de contrôle du moteur, etc) sont non seulement volumineux et de types variés, mais possèdent également une fréquence d'envoi élevée de données en raison de la nature hautement dynamique des réseaux véhiculaires. Ainsi, le réseau de véhicules connectés doit faire face à plusieurs challenges tels que la sécurité des communications, le big data, la gestion de réseaux hétérogènes, l'efficacité énergétique, etc.

Dans ce chapitre, nous présentons le véhicule électrique et son écosystème. Ensuite nous décrivons l'architecture du réseau de véhicules connectés. Enfin, nous nous intéressons à la sécurité du réseau véhiculaire d'une manière globale et à la sécurité du réseau interne du véhicule de manière plus particulière.

1.2 Le véhicule électrique

La tendance mondiale à l'énergie durable a considérablement révolutionné plusieurs secteurs, notamment la construction automobile. La plupart des grands constructeurs automobiles proposent des modèles qui fonctionnent entièrement avec des batteries électriques. Dans les prochaines années, les véhicules électriques (VE) devraient représenter une grande partie de la production automobile totale [48].

Bien que les VE présentent plusieurs défis (moteurs, capteurs, etc.), l'un de leurs principaux obstacles est la batterie [49]. Le développement des véhicules électriques est freiné par l'autonomie de ces véhicules, le nombre de bornes de recharge déployées et le temps de recharge (au minimum entre 20 et 30 minutes pour les recharges rapides) [50, 51]. En effet le souci majeur pour les futurs acquéreurs de véhicules électriques est l'autonomie. Pour la plupart d'entre eux la peur de tomber en panne sèche est un sujet qui revient le plus souvent. Pour la majorité des VE existants sur le marché, leur autonomie moyenne se situe entre 100 et 150 km [52].

Cette autonomie limitée provient de la capacité des batteries de type, lithium-ion, installées sur la plupart des VE. Bien qu'elles soient développées en utilisant les dernières technologies, ces batteries ne sont pas encore suffisamment performantes pour effectuer des centaines de kilomètres. Idéalement, les batteries des VE devraient avoir une autonomie comparable à celle des réservoirs à essence. La batterie devrait également pouvoir être chargée rapidement et rester en bon état après des milliers de cycles de charge. En outre, elle devrait être abordable et enfin, être respectueuse de l'environnement. Toutefois, les batteries actuelles des VE présentent quelques inconvénients importants qu'il faut prendre en compte [51, 53, 54]. Par exemple, les batteries de grande capacité, qui sont optimisées pour la distance de conduite, sont coûteuses à fabriquer, lentes à charger et peu respectueuses de l'environnement. D'autre part, les batteries de petite capacité sont plus abordables mais nécessitent des recharges plus fréquentes.

1.3 Architecture du réseau des véhicules connectés

Le réseau des véhicules connectés (voir figure 1.1) utilise des technologies de traitement des données, de communication entre les véhicules, les unités d'infrastructure et usagers de la route afin d'accroître la sécurité et l'efficacité du système de transport.

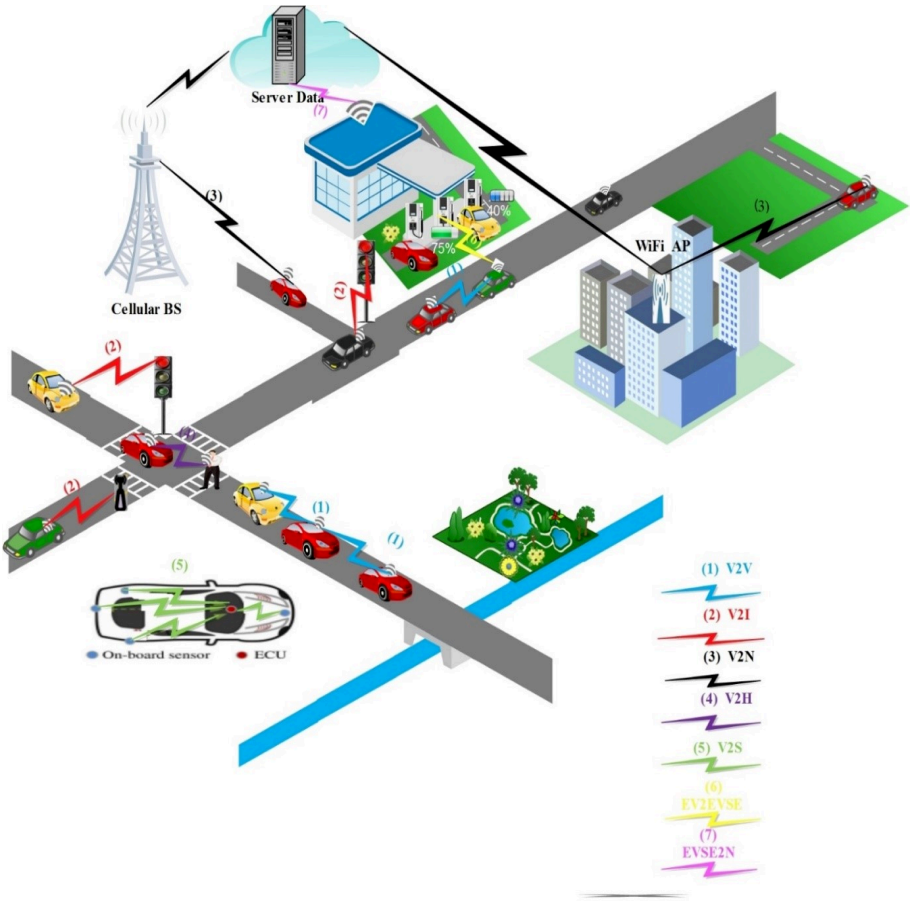


FIG. 1.1 : Architecture du réseau des véhicules connectés

Le réseau véhiculaire se compose de deux sous-réseaux principaux : le réseau intra-véhiculaire et le réseau inter-véhiculaire.

1.3.1 Le réseau intra-véhiculaire

Le réseau intra-véhiculaire supporte le type de communication V2S (Vehicle to Sensor) et vise à interconnecter les différents composants embarqués au sein du véhicule. Le réseau intra-véhiculaire est composé d'un OBU (Onbord Unit) /ECU (Electronic Control Unit) avec des capacités de mémoire et de traitement importantes et d'un ensemble de

ECUs/capteurs (voir figure 1.2). L'ECU centrale (OBU) sert à échanger les données entre les différents sous-réseaux du réseau interne et à communiquer avec le monde extérieur (voiture, piéton, serveurs, infrastructure routière, etc.). Un véhicule peut contenir plus de 100 ECU/ capteurs intelligents [55]. Chaque ECU s'appuie sur un ensemble de capteurs et d'actionneurs pour commander un ou plusieurs des systèmes d'un véhicule. Différentes technologies de communication sont utilisées entre les ECU distribués à l'intérieur du véhicule. Dans cette section, nous allons présenter l'ECU, le type de logiciel qu'elle utilise et les types de communications utilisés.

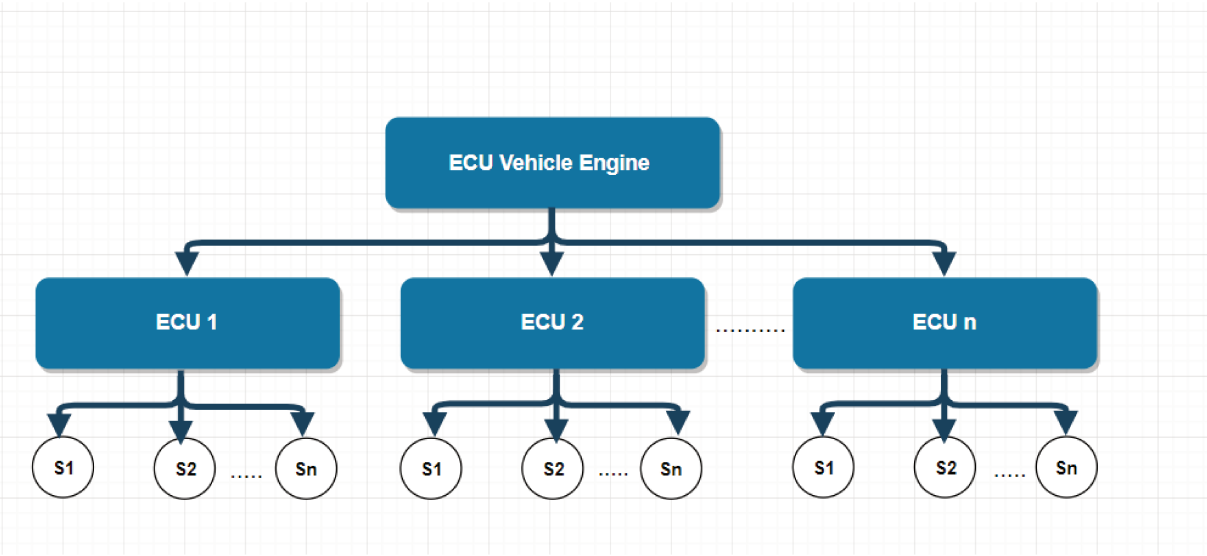


FIG. 1.2 : Architecture du réseau intra-véhiculaire

ECU (Electronic Control Unit) /capteur intelligent

Sur la base des capteurs qu'ils gèrent et des logiciels qu'ils exécutent, les ECUs peuvent être classés en différentes catégories, allant de ceux qui sont critiques pour la sécurité du conducteur, comme le calculateur de contrôle des émissions, à ceux qui ne le sont pas, comme le calculateur d'infotainment [56]. Les propriétés matérielles des ECU varient également d'une ECU à l'autre. En général, les ECU ont des ressources limitées en ce qui concerne la puissance de calcul et la taille de la mémoire. La plupart de ces ECU sont capables de gérer une seule fonctionnalité du véhicule. De nos jours, les chercheurs et les industriels cherchent à fusionner plusieurs calculateurs en des calculateurs avec des processeurs multicœurs plus puissants, une mémoire suffisante et la capacité de servir de nombreuses fonctionnalités ensemble, pour remédier à la complexité exponentielle du

système intra-véhiculaire [57, 58].

Composants logiciels

Aujourd'hui, un grand nombre de composants logiciels fonctionne sur les ECUs dans le but d'améliorer la sécurité, l'efficacité et le confort des véhicules modernes. Dans les voitures de luxe, on peut trouver jusqu'à 2000 fonctions logicielles [59]. Ces composants logiciels comprennent des applications automobiles courantes ainsi que le micrologiciel qui supporte ces applications. Ces dernières peuvent être regroupées en deux catégories principales :

- **Applications critiques pour la sureté de fonctionnement (safety critical applications)** : Elles sont utilisées pour contrôler les fonctions critiques du véhicule. La défaillance de ces applications peut avoir des conséquences catastrophiques sur la sécurité des usagers de la route (conducteurs, passagers, etc.). Ils ont une certaine exigence en termes de latence, de probabilité d'erreur et de niveau de sécurité et de disponibilité strictes. On peut citer comme exemple : le système d'avertissement de collision frontale, le système de régulation de vitesse adaptative (ACC) et le système d'avertissement de perte de contrôle.
- **Applications non critiques pour la sureté de fonctionnement (non-safety critical applications)** : elles peuvent être classées en deux sous catégories :
  - *Applications semi critiques* : ce sont les applications de contrôle des fonctions non critiques pour le véhicule. Le dysfonctionnement de ces applications peut avoir un impact majeur sur le bon fonctionnement d'un système au niveau ou en dehors du véhicule.
  - *Applications de confort* : les applications de cette catégorie visent à améliorer le confort du conducteur et à renforcer l'efficacité du trafic, comme les applications multimédia et télématiques. Ces applications ont généralement des exigences plus souples par rapport aux applications critiques pour la sécurité.

Les composants logiciels doivent être développés en tenant compte des exigences de sécurité, indépendamment du type de l'application. Cette catégorisation va nous servir au

niveau du développement de notre solution de sécurité adaptative pour protéger en priorité les applications hautement critiques. Le micrologiciel (firmware en anglais) : est une catégorie spéciale de composants logiciels qui sont utilisés pour contrôler les différents dispositifs matériels des systèmes embarqués (ECU/capteur intelligent) et pour fournir une couche de base pour l'exécution des applications automobiles. Les microprogrammes pour les appareils embarqués sont comme le système d'exploitation (OS) des ordinateurs correspondant à un micrologiciel temps réel.

Nous pouvons citer comme exemple AUTOSAR (AUTomotive Open Systems Architecture) [60] qui est une architecture logicielle largement utilisée, ouverte et standardisée pour le domaine automobile. Elle vise à soutenir le développement indépendant de l'application automobile en faisant abstraction du matériel de l'ECU sous-jacent. AUTOSAR (voir figure 1.3) déploie trois couches comprenant : la couche application où les applications automobiles peuvent s'exécuter, la couche Run-Time Environment (RTE) qui fournit des services de communication pour toutes les applications afin d'échanger des données dans la même ECU ou avec d'autres applications reliées à une autre ECU et la couche logicielle de base (BSW), contenant le système d'exploitation AUTOSAR.

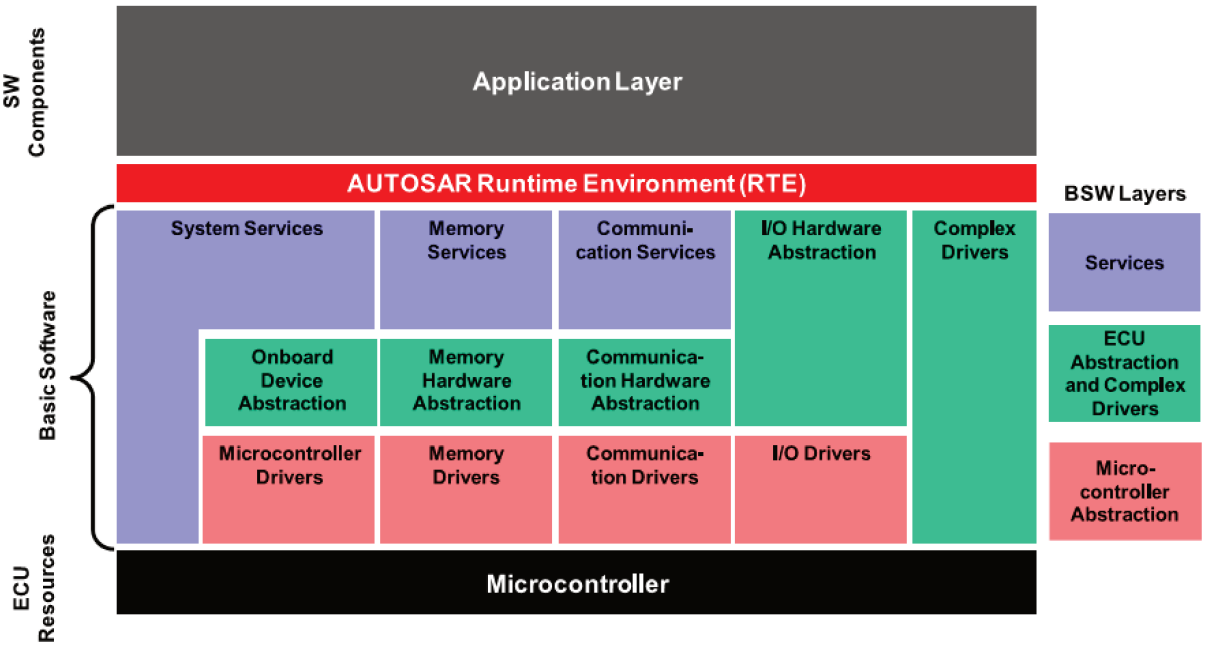


Fig. 1.3 : Architecture AUTOSAR [1]

Les technologies de communications

Plusieurs technologies de communications peuvent être utilisés au niveau du réseau intra-véhiculaire [61–65]. Nous pouvons citer :

- **CAN (Controller Area Network)** : Le CAN est un système de bus peu coûteux et fiable, mais il fournit une faible bande passante (jusqu'à 1 Mbit/s). Il a été introduit au début des années 80 et il est utilisé pour la connexion des systèmes groupe motopropulseur, châssis et carrosserie ainsi que pour les applications temps réel.

- **Local Interconnect Network (LIN)** : il a été développé à la fin des années 90 et est caractérisé par une communication série à faible coût entre les ECU et les actionneurs avec des débits de données allant jusqu'à 20 Kbit/s. Le LIN est utilisé pour les systèmes électronique de la carrosserie tels que les rétroviseurs, le moteur des sièges, les verrous de portes et les capteurs climatiques.

- **FlexRay** : Il a été introduit en 2004 et adopté plus tard comme norme ISO 17458. Le FlexRay assure une communication plus rapide que le CAN et le LIN (bande passante jusqu'à 10 Mbit/s). Il est utilisé pour connecter des applications critiques qui nécessitent une prévisibilité et une tolérance aux pannes. Il est utilisé au niveau des systèmes powertrain et sureté tels que le système régulateur de vitesse automatique.

- **Media Oriented Systems Transport (MOST)** : MOST est un système de bus à grande vitesse qui a été développé pour les applications multimédia et d'infodivertissement dans les véhicules qui nécessitent la transmission d'une grande quantité de données. La largeur de bande passante du MOST150 est de 150 Mbit/s. Il est uniquement utilisé pour les connexions de caméras ou de vidéos.

- Ethernet : Ethernet permet des transmissions de données avec une bande passante plus large que les autres types de bus.

- **Technologie sans fil (wireless technology)** : En raison du nombre croissant d'applications et de capteurs dans les véhicules (ECU, capteurs, etc), une connexion

filaire peut être de moins en moins adaptée puisqu'elle implique : (1) un poids supplémentaire au véhicule et une consommation plus importante de carburant ; (2) un problème de flexibilité de déploiement des capteurs ; (3) un coût supplémentaire (installation, maintenance, remplacement) [15, 16]. Jiun-Ren Lin et all [66] ont montré que les communications sans fil peuvent être la solution la plus appropriée pour les communications intra-véhicule, principalement en raison de leur moindre complexité et de leur faible coût. Plusieurs technologies sans fil peuvent être utilisées telles que : Bluetooth, zigbee, WiFi, etc. Par exemple, le système de sécurité appelé TPMS (Tire Pressure Monitoring System) qui est utilisé pour surveiller et afficher la pression d'air à l'intérieur des pneus du véhicule [67], dépend d'une communication sans fil à courte portée (short-range Wireless communication) pour recevoir la lecture de la pression des pneus par le capteur. Bluetooth est aussi une technologie sans fil qui est déjà utilisée dans le véhicule pour prendre en charge certaines applications de confort telles que les appels téléphoniques, l'affichage des messages sur le tableau de bord, etc [68, 69]. Enfin, le WiFi est utilisé pour connecter les appareils des utilisateurs tels que les téléphones et les tablettes au véhicule [69].

1.3.2 Le réseau inter-véhicule

Le réseau inter-véhicule couvre la communication entre le véhicule et les dispositifs environnants. Selon l'ETSI (European Telecommunications Standards Institute), il est composé de quatre entités, comme suit [70] :

- **Vehicle ITS Station** : représente les véhicules en mouvement tels que des voitures, des camions, des bus. Chaque véhicule connecté est équipé d'un ECU qui fait office de passerelle V2X et qui gère la communication radio ainsi que le codage et le décodage des messages V2X.
- **Central ITS Station** : comprend les serveurs des opérateurs de trafic, des opérateurs routiers, des fournisseurs de services, des fournisseurs de contenu.
- **Le "Roadside"** regroupe les infrastructures routières connectées telles que l'unité Roadside (RSU), les feux de circulation intelligents, le péage intelligent, les stations de recharge.

- **Le "personnel"** regroupe les dispositifs personnels et nomades (par exemple, les drones ou les téléphones portables).

Les types de communication

Le réseau inter-véhicule supporte cinq types de communications avec différentes portées [12].

- **V2V (Vehicle to Vehicle)** : Ce type de communication permet aux véhicules de communiquer et d'interagir ensemble.
- **V2I (Vehicle to Infrastructure) ou V2R (Vehicle-to-Roadside)** : Le V2I/V2R relie les véhicules à l'infrastructure tels que les RSUs, les panneaux de signalisation et les capteurs (les véhicules peuvent interagir avec des capteurs dispersés le long de la route afin de contribuer à la surveillance du trafic et des conditions routières).
- **V2N (Vehicle to Network) ou V2I (Vehicle-to-Internet)** : Il permet une communication directe entre les véhicules et l'Internet (serveurs, etc).
- **V2P (Vehicle to Pedestrian) ou V2H (Vehicle-to-Human)** : Ce type de communication relie à la fois les véhicules et les personnes (passagers, conducteurs, etc.) par le biais de dispositifs intelligents (smartphone, tablette, montre intelligente, etc.) en utilisant le CarPlay d'Apple ou le système Android d'OAA ou le Near Field Communication (NFC) [71, 72].
- **V2G (Vehicle to Grid)** : Ce type de communication relie les véhicules et le réseau électrique (station de recharge électrique) pour charger les véhicules électriques. La norme CEI 61851-24 définit les communications numériques entre les EV et la station de recharge électrique [73].

Les technologies de communication

Les technologies de communications inter-véhicules sont :

- **ITS-G5/ 802.11p** : L'objectif principal de l'IEEE 802.11p est de fournir une communication ad hoc entre les véhicules (Vehicle to Vehicle V2V) et les RSU (Vehicle

to Infrastructure V2I). Elle a été mise en œuvre pour soutenir la communication entre les nœuds mobiles en présence d'obstacles, de topologie fortement dynamique et de connexion discontinue. L'IEEE 802.11p peut être facilement déployé à moindre coût, mais elle fait face à plusieurs défis tels que des latences réduites et la qualité de service. En outre, elle ne peut offrir qu'une connectivité V2I intermittente en raison de la courte portée radio (short radio range) [74].

- Cellular Vehicle-to-everything (C-V2X) : a été introduite par le 3GPP dans la version 14. Les messages C-V2X sont envoyés en utilisant deux types de liens (voir figure 4) :
  - **La communication cellulaire** : couvre la communication bidirectionnelle entre l'UE (User Equipment) et l'eNB (eNodeB) via l'interface Uu [75]. La communication entre l'UE et l'eNB est appelée liaison uplink/ downlink. Elle est utilisée par le serveur d'application V2X pour diffuser des messages aux véhicules, ou les envoyer à l'UE via une connexion unicast. En plus des communications unidirectionnelles entre l'eNB et l'UE, l'eNB prend en charge les communications un à plusieurs (one to many) via la liaison downlink. L'eNB utilise un service single-cell point-to-multipoint pour les transmissions sur une seule cellule et un service de diffusion Multimedia Broadcast Multicast pour les communications sur plusieurs cellules.
  - **Device to device (D2D)** : Le D2D permet à deux dispositifs de communiquer entre eux dans la bande passante cellulaire autorisée sans avoir recours à une station de base (BS) impliquée ou avec une participation limitée de la BS [76–78]. Le D2D est une technologie clé pour les réseaux 5G. Il prend en charge les communications multi-hop entre les entités du réseau pour améliorer la connectivité de bout en bout. Il permet également une communication à courte portée et un faible temps de latence pour les messages de sécurité routière. Dans la communication D2D, l'UE envoie le message aux UEs voisines par le biais de l'interface PC5 [79]. D2D (nommé aussi Proximity Services (ProSe) [80]) se devise en deux catégories : In-band et Out-band D2D [81] :
    - In-band : La communication D2D utilise des bandes cellulaires autorisées.
    - Out-band : Les liens D2D utilisent une bande sans licence telle que le WiFi

Direct, ZigBee, bluetooth. etc.

Le mobile Femtocell (Mfemtocell) ou mobile small cell a été introduit pour répondre à la grande mobilité des systèmes de transport intelligents (ITS) [82, 83]. Le MFemtocell combine à la fois les technologies de relais mobile et de femtocell [82, 84]. Le but de cette technologie est d'accélérer l'accès à l'internet. Les MFemtocells peuvent être définies comme de petites cellules (small cells) qui sont intégrées à l'intérieur des véhicules pour communiquer avec les utilisateurs à l'intérieur du véhicule, tandis que les grands réseaux d'antennes sont situés à l'extérieur du véhicule pour communiquer avec la station de base [82, 85]. L'utilisation des MFemtocells est essentielle pour l'établissement d'une connexion entre le véhicule et internet.

1.4 Les vulnérabilités du réseau des véhicules connectés

Le véhicule connecté peut être utilisé comme cible car il présente un intérêt tant en termes de puissance de traitement (exemple d'attaque botnets) qu'en terme de valeur économique (ransomware). De nombreux travaux de recherche [12, 86, 87] ont identifié les attaques qui pourraient être menées sur le réseau CVs. Etant donné la complexité de l'architecture, une classification des attaques est nécessaire. Plusieurs travaux dans la littérature ont proposé des classifications basées sur les services de sécurité [88]. Dans cette section, nous présentons les vulnérabilités du réseau CV en se basant sur le type de communication (intra-véhiculaire ou inter-véhicules). De même, nous mettrons en valeur leurs impacts sur les véhicules électriques, à l'exception des communications avec l'infrastructure de recharge.

1.4.1 Les vulnérabilités du réseau intra-véhiculaire

La sécurité des communications V2S a été étudiée de manière approfondie dans la littérature [12]. Un nœud malveillant peut perturber le fonctionnement du véhicule en lançant de nombreuses attaques sur le réseau de capteurs. Les attaques peuvent concerner chaque composant du système automobile (l'ECU, les logiciels et le réseau). Le danger

d'exploiter l'une de ces vulnérabilités ne se limite pas aux composants dans lesquels la vulnérabilité existe mais peut s'étendre à d'autres composants et pourrait exposer l'ensemble du système au risque qu'un pirate puisse contrôler l'ensemble du véhicule. Pour présenter les vulnérabilités du réseau intra-véhiculaire, nous commencerons par décrire les attaques sur les ECUs et appareils connectés. Ensuite, nous aborderons les vulnérabilités du logiciel et des technologies de communications.

Les ECUs et les appareils connectés

Les ECUs sont des dispositifs programmables qui comprennent des ports et consoles série pour aider le développeur à accéder et à maintenir le micrologiciel et les logiciels associés à ce calculateur. Ces mêmes ports et consoles peuvent permettre aux attaquants de compromettre le fonctionnement de l'ECU avec un micrologiciel malveillant [89].

En 2015, Miller et Valasek [90] ont réussi à faire **flasher** l'une des puces de l'unité principale de la Jeep Cherokee avec un micrologiciel modifié (Chip tuning attack [91]). Plus tard, ils ont utilisé le micrologiciel malveillant pour envoyer des commandes via le réseau embarqué afin d'effectuer des actions malveillantes telles que la désactivation des freins, la prise de contrôle du volant, et même l'arrêt du moteur. De même, l'ECU peut être susceptible au **side channel attack**. En effet, L'attaquant peut recueillir des informations pendant l'exécution du système de cryptage intégré et utiliser les informations recueillies pour extraire des informations critiques sécurisées telles que les clés de cryptage [92].

Les ECU ne sont pas les seuls composants matériels qui sont être visés par les attaquants. D'autres dispositifs connectés au véhicule, tels que les téléphones, les tablettes, les dispositifs de diagnostic connectés via ODB-II, etc. peuvent être utilisés comme une passerelle pour attaquer un véhicule s'ils contiennent une faille de sécurité.

Woo et al [89] ont démontré la possibilité d'attaquer un véhicule à distance en utilisant une **application malveillante** installée sur un smartphone connecté au véhicule de la victime. De même, les auteurs dans [93] ont connecté un outil d'interface avec le port OBD-II. Ils ont observé que tous les paquets contiennent la même clé SSH. Ils ont pu envoyer une **mise à jour aux TCU (Toll Collection Unit) par SMS**, ce qui leur a permis de **lancer un shell à distance** puis l'utiliser afin d'injecter des messages. Ils ont

pu activer le capteur de freinage dans une voiture de sport.

Composants Logiciels

Les composants logiciels critiques et non critiques à l'intérieur de chaque véhicule ouvrent le champ à un certain nombre d'attaques. Bien que les applications critiques et non critiques doivent tenir compte de la sécurité pendant leur développement, ce n'est pas toujours le cas dans la réalité. L'intégration de différents composants avec une qualité de code très variable dans le même ECU peut laisser l'ensemble du système du véhicule dans un état non sécurisé [94, 95]. En outre, l'utilisation de langages de programmation bas niveau (exemple : le langage de programmation C a conduit à l'introduction de nombreuses vulnérabilités telles que le débordement de la mémoire tampon, les pointeurs pendouillant, etc). Ces vulnérabilités ont été le point de départ de nombreuses attaques réussies. Plusieurs marques de véhicules ont souffert de faiblesses de sécurité dans un ou plusieurs de leurs composants logiciels (exemple : le logiciel Uconnect de Chrysler, le système SmartGate de Skoda, ConnectedDrive de BMW, le point d'accès WIFI du véhicule électrique hybride rechargeable (PHEV) Mitsubishi Outlanderetc) [96].

Ces vulnérabilités ont permis aux attaquants de réaliser de nombreuses attaques et de nombreuses actions malveillantes telles que l'**activation/désactivation de la climatisation, du chauffage et de l'éclairage, la désactivation de l'alarme anti-vol**, etc. Elles ont également provoqué le rappel de millions de voitures. Une attaque peut consister à **rafraîchir le logiciel de gestion du moteur** afin d'augmenter sa puissance. Non seulement les applications automobiles mais aussi les microprogrammes eux-mêmes peuvent contenir de nombreuses vulnérabilités ou des services inutiles qui pourraient être exploités par un attaquant. Par exemple, Tesla S utilisait un système d'exploitation basé sur Ubuntu avec des ports ouverts tel que le telnet qui étaient utilisées par les utilisateurs pour se connecter au système du véhicule [97]. De plus, une mise à jour malveillante ou erronée peut finir par poser un énorme problème, comme dans le cas du système Land Cruiser Enform de la Toyota 2016, dont une ECU **redémarrait continuellement** à cause d'une nouvelle mise à jour contenant des données erronées [98].

Les technologies de communication

Les nouvelles technologies qui permettent à la voiture de se connecter au monde extérieur ont fait disparaître l'isolement physique du réseau interne du véhicule. On peut attaquer le réseau intra-véhiculaire en utilisant les interfaces filaires et/ou les interfaces sans fils.

Interfaces filaires

Les ports ODB-II (On-Board Bebug) sont les interfaces les plus connues pour donner à l'attaquant un accès direct au réseau intra-véhiculaire. D'autres interfaces telles que les ports USB (qui sont utilisés pour connecter les smartphones des conducteurs) sont également utilisées aujourd'hui pour se connecter au réseau intra-véhiculaire. De nombreuses attaques ont été réalisées en se connectant au système OBD embarqué dans le véhicule. Dans [99], les auteurs ont réalisé une attaque via l'OBD qui consistait à **écouter** les paquets du bus CAN, puis à **injecter** de fausses données. Ils ont pu **modifier** le code logiciel des ECUs et **effacer** toute trace d'attaque. Woo [100] a montré que l'utilisation d'un smartphone connecté via Bluetooth sur un "outil de balayage OBD-II" inséré dans le véhicule permettait d'**injecter** à distance des paquets CAN malveillants. Aujourd'hui, les attaquants sont capables d'exploiter diverses vulnérabilités du système automobile, et de pirater et contrôler le véhicule à distance.

Traditionnellement, les systèmes de bus internes aux véhicules ont été développés pour assurer la sûreté et la réduction du coût mais sans tenir compte des risques de sécurité. Les messages CAN sont diffusés et transmis en texte clair sans aucune preuve d'intégrité ou d'authenticité des données [101]. Par conséquent, toute ECU malveillante peut se faire passer pour une autre ECU légitime, intercepter tous les messages échangés entre les différentes ECU , manipuler les données transmises ou retarder ou rejouer de manière frauduleuse les messages précédents. En outre, le composant malveillant peut bombarder le bus de faux messages de haute priorité pour perturber d'autres communication.

Néanmoins, ces problèmes ne sont pas limités au bus CAN. D'autres systèmes de bus (par exemple, Ethernet, FlexRay, LIN) souffrent de défaillances similaires qui ont également fait la cible de nombreuses attaques [102].

Interfaces sans fils

Le réseau sans fil, qui est utilisé par de multiples applications dans le véhicule, est la cible de plusieurs attaques. Les communications sans fils sont exposées aux mêmes vulnérabilités que les interfaces filaires. Par exemple, Roulf et al [103] , ont montré que des attaquants sur le bord de la route (jusqu'à 40 mètres de distance) ou conduisant un autre véhicule peuvent **écouter, intercepter et injecter des messages falsifiés** puisque les capteurs transmettent des messages sans aucune protection de sécurité.

Dans le cas des véhicules électriques, une fausse information sur l'état de la batterie et la température peut influencer la décision du conducteur (continuer vers la destination finale ou chercher une borne de recharge). De même, l'attaquant peut fournir à un véhicule de fausses informations sur sa position et d'autres informations GPS (GPS deception) [104, 105]. Une fausse information sur l'itinéraire (exemple plus court chemin) peut avoir des conséquences graves sur le conducteur. En effet, elle peut avoir un impact sur l'identification de l'itinéraire le plus fiable en termes de consommation d'énergie (pour les véhicules électriques). Cette attaque peut avoir des conséquences plus importantes surtout dans les zones rurales où le nombre des stations de recharge est limité. [103], les auteurs ont montré comment **récupérer** l'ID unique d'un capteur de pression des pneus et **envoyer de faux paquets** pour générer des alertes et amenant ainsi un conducteur à freiner. Dans [21], l'équipe Tencent a exécuté une attaque à distance sur la tesla modèle S en compromettant de nombreux systèmes embarqués (Integrated Circuit (IC), Central Information Display (CID), Gateway, etc.), et injectant de faux messages au niveau du bus CAN.

Des attaques de **bouillage** peuvent être aussi menées sur le réseau intra-véhiculaire sans fils empêchant les capteurs d'envoyer l'état du système. Par conséquent, le conducteur ne pourra pas estimer l'état du véhicule. D'autres travaux ont montré que les attaquants peuvent ouvrir des véhicules sans la clé [106] en rejouant les messages transmis sur le réseau sans fil entre la voiture et la clé intelligente.

1.4.2 Les vulnérabilités du réseau inter-véhicules

Les vulnérabilités du réseau inter-véhicule sont présentées en se basant sur le type de communication.

La sécurité des communications V2V

V2V a fait l'objet d'une multitude de travaux dans le contexte des VANET (Vehicular Ad-Hoc Networks) [104, 105, 107–109]. Un véhicule connecté peut **refuser de coopérer** avec les véhicules voisins (attaque d'**égoïsme**) pour relayer des informations dans le but d'économiser ses ressources (bande passante, ressources de calcul, batterie pour le VE, etc.). De même, un attaquant peut **altérer ou modifier** une partie du paquet qui transite par lui. Exemple : Modification du nombre de sauts d'un message de découverte de route. De plus, un véhicule malveillant peut créer un grand nombre de nœuds de fausses identités avec des ID et positions différentes (**sybil attack**). À partir de ce grand nombre de faux noeuds, l'attaquant peut compromettre plus facilement le fonctionnement général des ITS. L'attaquant peut exploiter cette attaque afin de réaliser une attaque d'**injection de faux messages**. En outre, l'attaquant peut utiliser ce grand nombre de nœuds malveillants pour envoyer un message, par exemple, d'alerte de congestion d'une route pour empêcher les autres véhicules de passer par cette route et ainsi, empêcher le système des CVs de recevoir des données en temps réel sur un chemin donné. De même, l'attaque **Sybi**l peut amener le système des CVs à avoir une mauvaise perception de la file d'attente des stations de recharge (pour les EVs), ce qui peut avoir un impact sur la prise de décision des conducteurs. Cette attaque peut avoir des conséquences graves, dans le cas où la charge ne permet pas au conducteur d'atteindre la prochaine station de recharge. Encore, le réseau V2V peut être susceptible au attaque d'**écoute**, **attaques de routage (Black Hole attack , Gray Hole attack (selective forwarding attacks) et l'attaque du trou de ver (Wormhole Attack))**.

Les communications V2I

V2I peuvent être sujettes à plusieurs types d'attaques tels que l'**injection** de faux messages d'annonce de RSU, les attaques **DoS**, les attaques sur **la vie privée** et le **rejeu**

[12, 110–113]. Par exemple l'**injection de faux messages** d'annonce de RSU permet à un véhicule malveillant de prendre le rôle d'un RSU dans une zone géographique bien déterminée pour envoyer les paramètres permettant l'auto-configuration des véhicules (Préfix IPv6). Pour atteindre cet objectif, le véhicule malveillant diffuse un faux message d'annonce de RSU dans sa zone géographique. Dans ce type d'attaque, nous distinguons deux cas. Dans le premier cas, comme le montre la figure, le message erroné contient un préfixe valide mais le champ adresse source contient l'adresse IPv6 de l'attaquant au lieu de l'adresse IPv6 du RSU. Les véhicules ne peuvent rejoindre ni le RSU légitime ni le serveur, comme le montre la figure suivante. Cependant, l'attaquant peut faire une attaque **MiTM** et **relayer** le Traffic vers l'RSU légitime (voir figure 1.4).

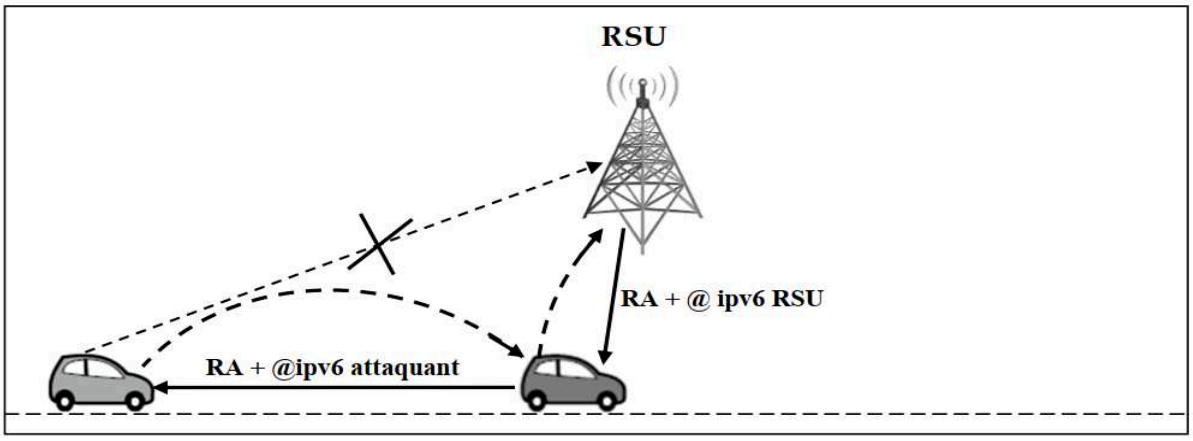


Fig. 1.4 : Attaque d'injection de faux messages d'annonce de RSU

Une autre forme de cette attaque est d'envoyer un préfixe invalide dans le message d'annonce de RSU. Cette attaque a les mêmes effets que celle décrite ci-dessus mais elle a également un effet sur la mobilité. Un véhicule envoie périodiquement à l'agent mère un message de mise à jour (PBU) qui contient le préfixe IPv6 (MNP) permanent et son adresse temporaire (temporary address (CoA)). L'agent mère sauvegarde alors cette association (adresse temporaire / adresse mère). Ainsi, lorsque le préfixe n'est pas valide, l'agent mère associe à l'adresse permanente une adresse temporaire CoA non valide. Lorsqu'un noeud correspondant sur Internet (par exemple serveur) envoie un trafic vers un véhicule, ce trafic ne peut pas atteindre la destination (voir figure 1.5). De même, supposant que le préfixe envoyé par le RSU dans le message RA reste inchangé pendant une longue période et que ce préfixe est associé à une zone géographique, un nœud malveillant sur Internet peut créer une carte (cartographie) basée sur cette association. Il pourrait facilement suivre un

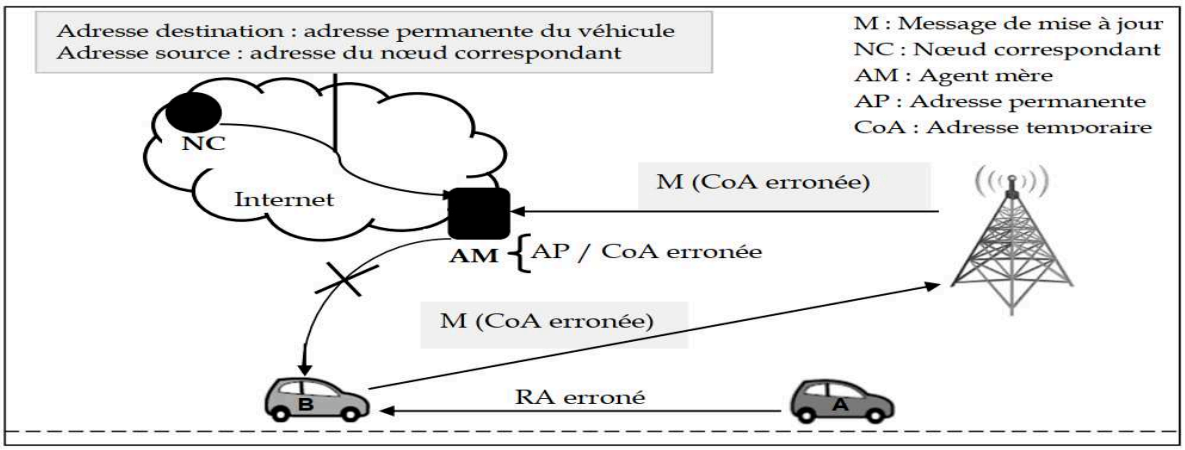


FIG. 1.5 : Impact de l'attaque d'injection de faux messages d'annonce de RSU

véhicule en se basant sur son adresse temporaire (attaque sur la vie privée). Cependant, cela n'est pas possible quand on utilise un Nemo BS puisque le nœud correspondant ne reçoit pas le message avec l'adresse temporaire (CoA). Mais, l'agent mère peut effectuer cette attaque et donc créer une carte pour un véhicule qui appartient à son réseau local.

Les communications V2N

V2N peuvent être vulnérable à plusieurs types d'attaques. Le mobile subscriber est caractérisé par une IMSI (International Mobile Subscriber Identity) et une TMSI (Temporary Mobile Subscriber Identity). La TMSI est envoyée par le véhicule à la station de base (BS) dans un message en clair. Selon la norme 3GPP, le véhicule envoie la TMSI à la BS afin d'être authentifié. Si la station de base ne peut pas authentifier le nœud (véhicule) après trois demandes, le véhicule envoie son Permanent-ID message [2]. Un attaquant peut lancer une attaque de type **MiTM, il peut se présenter sous forme d'un BS malveillant. Ensuite, il pourrait rejeter** le TMSI envoyé afin de forcer le véhicule à envoyer son IMSI. Cette attaque peut conduire à une atteinte à **la vie privée**. L'attaquant pourrait facilement suivre le véhicule en se basant sur son IMSI. De plus, il peut **usurper l'identité** du véhicule et **injecter** des informations malveillantes dans le réseau. Cette attaque est décrite dans la figure 1.6.

Les communications D2D sont exposés aux mêmes vulnérabilités des réseaux ad hoc. Le mmWave peut être soumis à l'attaque d'**écoute**. Cette attaque peut être lancée en installant des récepteurs sur les routes, ce qui peut entraîner une atteinte à la vie privée).

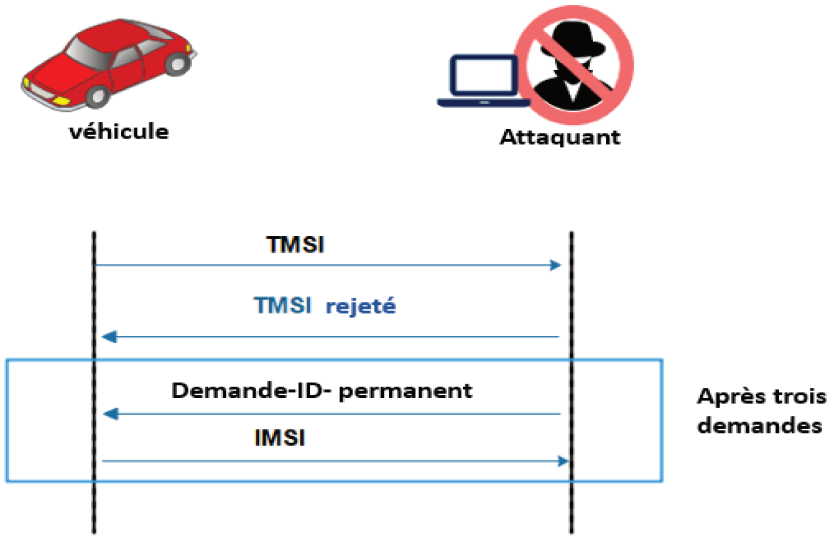


FIG. 1.6 : Attaque IMSI-Catcher [2]

Les attaquants visent à identifier la source des paquets transmis et à suivre le véhicule . Les stations de base femto, pico et micro sont moins sécurisées que les macro BS. L'utilisation des ondes millimétriques comme technologie de communication dans la 5G encourage l'utilisation des femto, pico et micro stations de base ce qui augmentera les vulnérabilités de la 5G . De même, La 5G est vulnérable aux attaques **DDoS**. Les auteurs de ont expliqué qu'il est possible d'utiliser un botnet (logiciel malveillant) pour signaler l'amplification et la saturation du HSS (Home Subscriber Server saturation) [114] . Cette attaque peut conduire à contrôler un grand nombre de véhicules infectés. En outre, la 5G est susceptible à l'attaque de brouillage car il s'agit d'un réseau ultra-dense (ultra-dense networks (UDN)) [12] .

Le protocole DIAMETER est utilisé au niveau du 5G pour assurer les services de mobilité, la gestion des politiques, la comptabilité et la facturation [115]. Il peut être sujet à des attaques d'**usurpation d'identité** et **relpay**, ces attaques peuvent avoir un impact sur la sécurité des couches IP (réseau) et transport.

Un attaquant peut modifier l'adresse IP de destination du message afin de le rediriger vers une autre destination malveillante (attaque ALTER) (voir figure 1.7). Cette attaque peut être définie comme une attaque DNS de redirection [3].

Le mobile femtocell peut faire l'objet d'attaques physiques (le pirate peut modifier

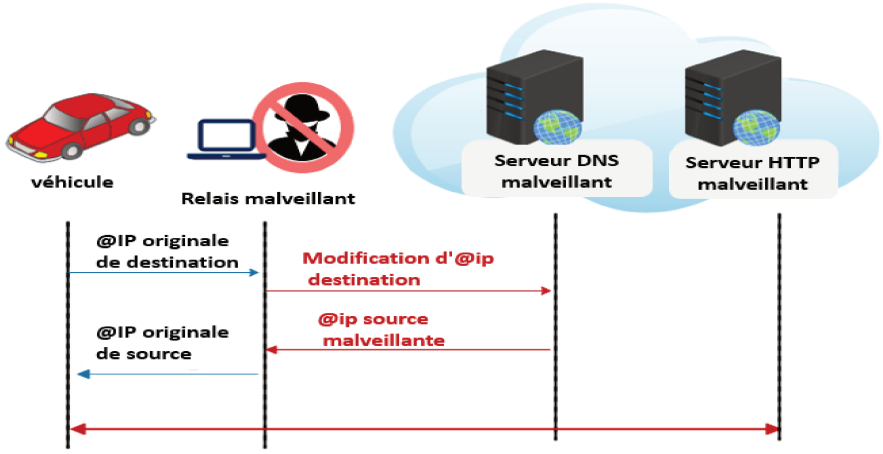


FIG. 1.7 : Attaque alter [3]

ou remplacer les composants du HeNB (Home eNodeB)), d'attaques de **configuration** (mauvaise configuration de la liste de contrôle d'accès (ACL) du HeNB ciblé), d'**attaques de protocole** (y compris les attaques de type MiTM sur le HeNB), de **déni de service**, d'attaques d'**écoute** et de **falsification** de la gestion des ressources radio (le HeNB fournit des informations incorrectes sur les ressources radio), etc. [114]. L'attaquant peut profiter de ces vulnérabilités pour perturber le fonctionnement du système.

MOBIKE (MOBility extension to Internet Key Exchange) est le protocole de sécurité le plus important utilisé par le mobile femtocell [116]. Il s'agit d'une extension de la version 2 d'Internet Key Exchange (IKEv2). Il permet l'échange de clés entre le mobile femtocell, le réseau central et le IP multihoming sans avoir à rétablir tous les SA (Security Association) et les tunnels IPsec [117]. Les auteurs de [116] ont montré que de nombreuses attaques peuvent être effectuées sur MOBIKE, telles que les attaques de type **DoS, MiTM** et les attaques de type **usurpation d'identité** [116]. Les attaques peuvent avoir un impact sur l'échange d'informations avec un serveur puisque le véhicule doit être configuré avec une adresse IP.

La figure 1.8 présente les vulnérabilités du réseau des véhicules connectés.

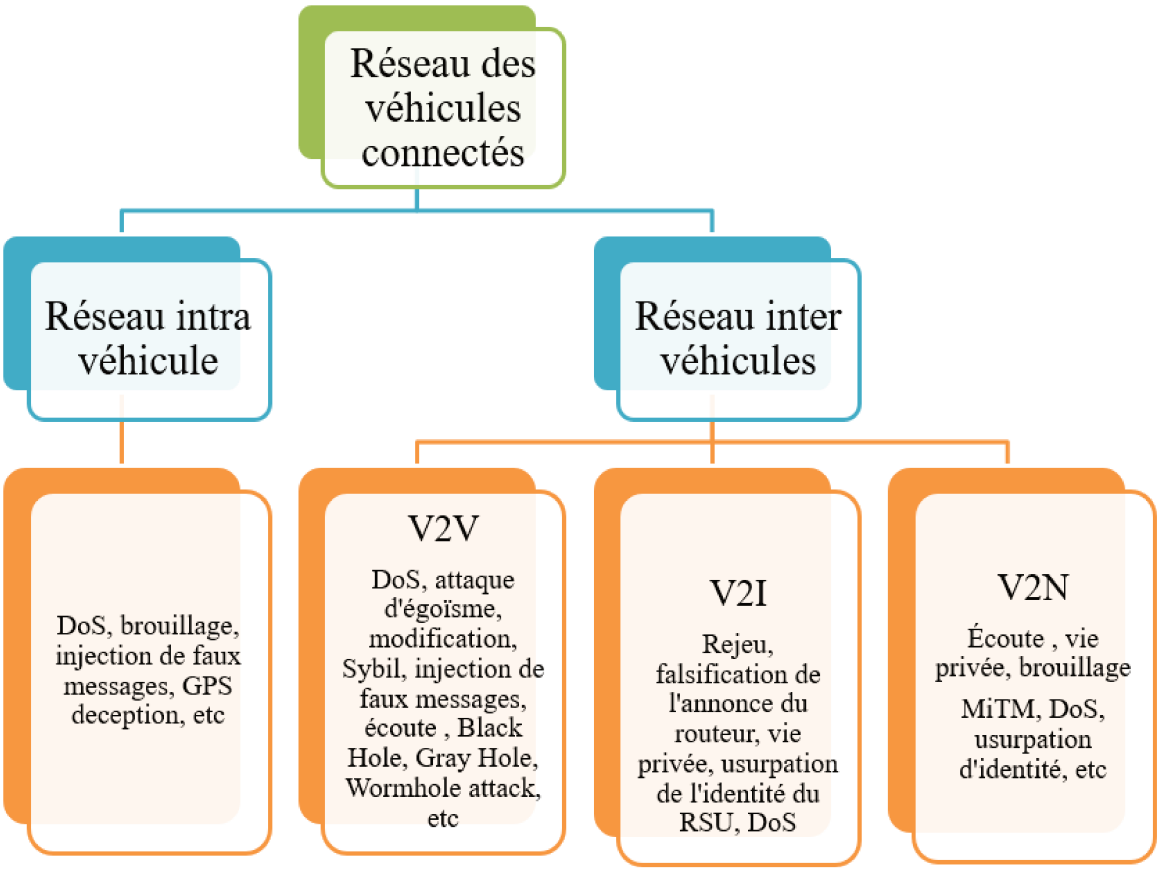


FIG. 1.8 : Les vulnérabilités du réseau des véhicules connectés

1.5 Le réseau intra-véhiculaire : importance et problématique

Jusqu'à présent, le réseau intra-véhiculaire a été conçu sans tenir compte des exigences de sécurité. La plupart des communications sont échangées soit en texte clair, soit sur une liaison faiblement sécurisée, ce qui signifie que des tiers malveillants peuvent écouter ou même injecter de fausses données ou commandes dans le canal de communication. L'interaction illimitée entre des composants de criticité mixte, qui peuvent être hébergés dans différents calculateurs et affectés à différents sous-réseaux, peut également créer des vulnérabilités du point de vue de la sécurité [118]. L'attaquant qui peut pirater un ECU peut apparemment pirater d'autres ECU, puisqu'ils partagent le même réseau.

L'hypothèse était qu'une attaque sur le réseau embarqué impliquait l'accès au véhi-

cule, de sorte que les mesures de sécurité physique réduisaient le risque d'une telle attaque. Cette hypothèse est de plus en plus éloignée de la réalité en raison des différentes technologies désormais intégrées dans le véhicule pour permettre l'interaction avec l'environnement extérieur (par exemple, GPS, wifi, 5G, Bluetooth, etc.). Ces technologies ont laissé les réseaux internes, dont les mécanismes de sécurité sont faibles ou inexistants, face à de nouvelles menaces d'attaques à grande échelle. Les attaquants ont été en mesure d'utiliser les faiblesses de sécurité existantes dans ces technologies pour intercepter la connexion entre différents calculateurs, usurper les données transférées et émettre de fausses données [99]. Dans certaines circonstances, les attaquants ont également pu participer à la communication en utilisant frauduleusement l'identité d'une ECU légitime [118]. Toutes ces attaques ont eu lieu à distance sans qu'il soit nécessaire d'accéder physiquement au véhicule ciblé.

Par conséquent, la sécurisation des communications à bord des véhicules est devenue une exigence fondamentale. Cependant, l'ajout de la sécurité aux protocoles de communication existants dans le véhicule n'est pas simple en raison des contraintes de ressources des ECU, qui peuvent empêcher l'utilisation de tels mécanismes. Par conséquent, l'introduction de la sécurité dans ces protocoles entraîne des surcharges de performance et augmente la taille des paquets, ce qui va à l'encontre des objectifs initiaux de la conception du protocole (par exemple, le protocole CAN, Controller Area Network).

1.6 Conclusion

Le réseau de véhicules connectés CVs est une architecture complexe qui couvre plusieurs types de communications (V2S, V2V, V2P, V2I, V2N, etc.) pour échanger des données entre les différentes entités du réseau véhiculaire. Dans ce chapitre nous avons présenté l'architecture et les cybers attaques sur le réseau CVs en mettant l'accent à chaque fois sur l'impact sur le véhicule électrique.

Les communications intra-véhiculaires (Vehicle to sensor (V2S)) représentent une innovation majeure pour l'industrie automobile. Dans le chapitre suivant, nous allons discuter les solutions qui ont été proposées pour sécuriser le réseau intra-véhiculaires.

Chapitre 2

Le réseau intra-véhiculaire : solutions de sécurité et problématique

2.1 Introduction

La sécurité est un facteur essentiel pour le succès et le déploiement du réseau intra-véhiculaire. En effet, ce dernier introduit de nouveaux défis de sécurité en raison des caractéristiques de l'architecture qui implique plusieurs composants avec des logiciels variés et de la nature critique des applications en termes de délai et de données sensibles et personnelles échangées.

Dans ce chapitre, nous identifions les besoins de sécurité du réseau intra-véhiculaire et nous présentons les solutions de sécurité définies pour ce type de réseau. Nous analysons la consommation énergétique des mécanismes de sécurité afin de montrer que ces solutions peuvent être énergivores dans un contexte de contrainte d'énergie. Enfin, nous présentons les solutions de sécurité adaptatives proposées dans des contextes autres que le réseau véhiculaire mais dont on pourrait s'inspirer pour répondre à la problématique soulevée.

2.2 Notions sur la sécurité des réseaux

La sécurité d'un réseau couvre trois aspects fondamentaux : les attaques, les services de sécurité et les mécanismes. Les attaques sur un réseau sont les méthodes qui peuvent être utilisées pour perturber le fonctionnement d'un service. Ainsi, la sécurisation des communications d'un réseau exige l'utilisation de services et de mécanismes de sécurité pour contrer les attaques qui peuvent être menées sur un réseau. Dans cette partie, nous introduisons les notions de services et de mécanismes de sécurité.

2.2.1 Les services de sécurité

Les services de sécurité peuvent être résumés comme suit :

- **L'authentification** : ce service permet aux membres du réseau de s'assurer de la bonne identité des membres avec lesquels ils communiquent.
- **La confidentialité** : elle garantit que seules les parties autorisées peuvent accéder aux données transmises à travers le réseau

- **L'intégrité** : ce service permet de s'assurer que les données échangées ne sont pas modifiées lors de la transmission des messages.
- **La non-répudiation** : ce service permet de s'assurer qu'un émetteur ne peut nier d'être à l'origine d'un message ou qu'un destinataire ne peut pas nier l'avoir reçu.
- **La disponibilité** : elle vise à garantir aux entités autorisées d'accéder aux ressources du réseau avec une qualité de service adéquate.
- **La protection de la vie privée** : elle garantit que les nœuds malveillants ne peuvent pas accéder ou collecter les données personnelles des utilisateurs et porter atteinte à la vie privée.

2.2.2 Les mécanismes de sécurité

Dans cette section, nous présentons les mécanismes de sécurité qui ont été abordés dans le cadre de ce travail à savoir le chiffrement symétrique, les fonctions de hachage, le mécanisme d'authentification MAC (Message Authentication Code) et de construction de clé.

Le chiffrement

Le chiffrement est utilisé pour assurer la confidentialité [119]. Il permet de chiffrer et déchiffrer un message en utilisant le même algorithme de chiffrement et la même clé ou deux clés différentes. On distingue trois types de chiffrement : le chiffrement symétrique, le chiffrement asymétrique et hybride. Dans cette section, nous allons nous limiter au chiffrement symétrique puisque c'est le type de chiffrement le mieux adapté aux caractéristiques du réseau intra-véhiculaire [31]. En effet, ce réseau est caractérisé par des ressources limités en termes de mémoire et de traitement. Pour cette raison, la cryptographie symétrique et l'authentification par clé partagée sont généralement envisagées.

Le chiffrement symétrique (ou le chiffrement à clé secrète) regroupe les algorithmes qui utilisent la même clé pour chiffrer et déchiffrer un message. Les algorithmes de chiffrement symétrique sont rapides mais nécessitent un partage de clés sécurisé. Dans ce type de

chiffrement, la phase de la distribution des clés secrètes est critique. Le chiffrement par block (block ciphers) est léger et plus adapté à l'IoT en comparaison avec les autres types de chiffrement (exemple : chiffrement par flux (stream ciphers). Nous citons, dans ce qui suit, quelques algorithmes de chiffrement par bloc [31, 120, 121].

- **L'Advanced Encryption Standard (AES)** : désigne un algorithme cryptographique approuvé par la FIPS (Federal Information Processing Standards) qui peut être utilisé pour protéger les données. L'algorithme AES est un chiffrement symétrique par blocs qui 'utilise des clés cryptographiques de 128, 192 et 256 bits. Il est couramment utilisé dans le cadre de l'IoT [28, 122].

- **Triple Digital Encryption Standard (3DES)** : est une version améliorée de DES qui crypte les données en blocs de 64 bits à l'aide d'une clé de 56 bits. L'algorithme transforme, à travers une série d'étapes, une entrée de 64 bits en une sortie de 64 bits. 3DES utilise une taille de clé plus grande que celle de DES (c'est-à-dire 168 bits ou 112 bits). Les opérations DES sont exécutées 3 fois dans 3DES avec 2 ou 3 clés différentes [24]. 3DES offre un niveau de sécurité élevé par rapport à DES. Il est toujours utilisé par le gouvernement américain. En raison de sa popularité et de sa simplicité, l'algorithme 3DES a été largement utilisé pour les transactions sécurisées dans les implémentations IoT [28].

- **SKIPJACK** : est un chiffrement par blocs développé par l'Agence nationale de sécurité américaine (US National Security Agency (NSA)). Skipjack a une taille de clé de 80 bits et résiste aux attaques les plus courantes (en raison de la taille de la clé). Skipjack est actuellement utilisée dans les plateformes des capteurs tel que TinySec et SenSec [123].

- **XXTEA** : également appelé Corrected Block TEA, est le successeur de XTEA et a été conçu pour corriger les défauts du Block TEA original (Tiny Encryption Algorithm). XXTEA nécessite peu de mémoire, ce qui permet de l'utiliser dans des environnements où les ressources sont limitées, comme les systèmes embarqués [28]. La taille de la clé de XXTEA est de 128 bits.

Fonction de hachage

Les fonctions de hachage sont utilisées pour garantir l'intégrité des données [124]. En cryptographie symétrique, elles sont également souvent utilisées pour construire les codes d'authentification de messages [125]. Les fonctions de hachage ne font pas appel à une clé secrète et compriment des données d'entrée de taille arbitraire (M) mais finie en une sortie de taille fixe (H). Cette dernière peut être considérée comme l'empreinte digitale. Ces primitives appartiennent à la famille des fonctions dites à sens unique ce qui signifie qu'elles sont considérées comme pratiquement « impossible » à inverser. Leur champ d'application inclut, sans s'y limiter, les contrôles d'intégrité des données, la vérification des mots de passe, la génération de nombres pseudo-aléatoires et l'authentification des messages. On peut citer comme exemple : MD5, SHA1, SHA2, SHA3. La définition formelle d'une fonction de hachage est la suivante (2.1). Soit $n \geq 1$

$$\eta : \mathbb{F}_2^* \longmapsto \mathbb{F}_2^n, M \longmapsto H \tag{2.1}$$

Méthode d'authentification : code d'authentification de message (Message Authentication Code (MAC))

Les fonctions de hachage qui prennent une clé secrète comme entrée supplémentaire sont mieux connues sous le nom de codes d'authentification de message. Ces primitives ne fournissent pas seulement l'intégrité des données mais permettent également de vérifier l'authenticité d'un message. Cela signifie que le récepteur d'un message peut vérifier qu'il provient d'un expéditeur valide, notamment de celui avec lequel le récepteur a échangé la clé secrète avant la réception du message [125, 126].

Concrètement, un MAC est un couple (T ; V) constitué d'une fonction de génération d'étiquettes (tag en anglais) T et d'une fonction de vérification d'étiquettes V. La fonction de génération d'étiquettes est spécifiée par (2.2)

$$\Gamma : \mathbb{F}_2^K \times \mathbb{F}_2^* \longmapsto \mathbb{F}_2^t, (K, M) \longmapsto T \tag{2.2}$$

Elle prend en entrée une clé secrète K et un message arbitraire M qu'elle compresse en une étiquette d'authentification de taille fixe T de longueur t. La fonction de vérification de l'étiquette est spécifiée par la formule suivante (2.3) :

$$\nu : \mathbb{F}_2 \times \mathbb{F}_2^t \longmapsto \{\perp, \top\}, \left(T, T^{'}\right) \longmapsto \begin{cases} \top \text{ if } T = T^{'} \\ \perp \text{ if } T \neq T^{'} \end{cases} \tag{2.3}$$

Elle vérifie si l'étiquette reçue T correspond à l'étiquette calculée $T^{'}$. Il existe de nombreuses façons de construire des MAC. Une approche courante consiste à prendre une fonction de hachage cryptographique et à l'utiliser dans le mode HMAC. les auteurs de [126] ont montré que le calcul du HMAC consomme moins d'énergie en comparaison avec d'autres méthodes telles que le CMAC, XMAC et occupe moins de RAM.

Diffie-Hellman

Diffie-Hellman [127] permet à deux hôtes d'échanger une clé de manière sécurisée . Soit A et B deux entités désirant posséder une clé de session afin de chiffrer leur communication. A et B se mettent tout d'abord d'accord sur une base g et un modulo n (un nombre premier suffisamment grand, dont la taille doit être supérieure à 1024 bits). La table 2.1 décrit un échange Diffie et Hellman. Comme $K = K^{'}$, A et B possèdent maintenant une clé de session qu'ils sont les seuls à connaître.

Tab. 2.1 : Diffie Hellman

1	paramètres : p,g
2	A =random(), $a = g^A (mod\ p)$ B=random(), b=g$^B (mod\ p)$
3	a$\longrightarrow$ $b \longleftarrow$
4	K=g$^{BA} (mod\ p) = b^A (mod\ p)$ K=g$^{AB} (mod\ p) = a^B (mod\ p)$
5	$\longleftarrow E_K(data) \longrightarrow$

2.3 Etat de l'art des solutions de sécurité pour le réseau intra-véhiculaire

De nombreux chercheurs et industriels [4, 27, 128–131] ont proposé des solutions de sécurité pour le réseau intra véhiculaire. Dans cette section, nous classifions les solutions en solution matérielle, solution à base firewall, solution à base d'IDS, solution logicielle.

2.3.1 Solutions matérielles

EVITA [4, 27] (E-safety vehicle intrusion protected applications) est un projet financé par l'Union européenne dans le cadre du septième programme de recherche et développement technologique. EVITA a développé une architecture de sécurité pour les réseaux automobiles embarqués qui protège le trafic contre les intrusions. Cette solution consiste en l'ajout d'un module de sécurité au niveau des ECUs, appelé HSM (Hardware Security Module). Le HSM consiste en un processeur et une mémoire embarquée sur la même puce afin de prévenir les écoutes et les fausses attaques par injection de données. De même, un autre objectif de l'utilisation de solutions de sécurité basées sur le matériel est de détecter et d'atténuer l'infection du code d'amorçage (code de démarrage). Ainsi, le HSM peut être utilisé comme une racine de confiance pour authentifier le code d'amorçage avant qu'il ne soit exécuté ainsi que, les microprogrammes et d'autres applications critiques [132].

Il existe trois types de HSM (voir figure 2.1) : le HSM léger (EVITA small), HSM moyen (EVITA medium), HSM complet (EVITA full). Ces trois type HSM sont conçus en fonction des exigences de sécurité de la communication du réseau embarqué. Par exemple, le HSM léger (EVITA small) peut être utilisé pour la communication entre les capteurs et les actionneurs, le HSM moyen (EVITA medium) pour la communication entre les ECUs, et le HSM complet (EVITA full) est généralement utilisé pour les communications avec l'environnement extérieure. Ce projet a été considéré comme un standard de facto pour les solutions commercialisées [27].

D'autres solutions telles que les Intel Software Guard Extensions (SGX) [133] ont été introduites pour garantir l'intégrité du code d'une application qui s'exécute sur une plateforme où tous les logiciels privilégiés sont potentiellement malveillants. Dans [128], les

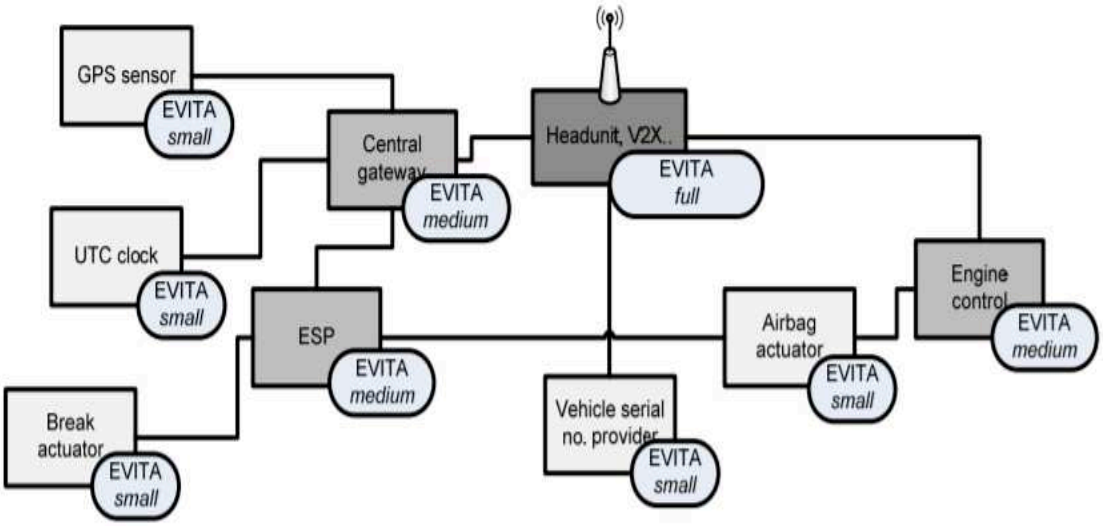


FIG. 2.1 : Architecture EVITA [4]

auteurs ont créé un module matériel sécurisé. Il préserve la sécurité des communications au niveau du bus CAN. Ce module est responsable de la distribution et de la gestion des clés, de l'authentification des messages CAN et du blocage des messages malveillants.

Müter et al [129] ont proposé une solution de sécurité de détection d'attaques, basées sur huit capteurs, qui sont utilisés pour observer les anomalies survenant dans le réseau interne du véhicule. Ces capteurs comprennent la formalité, l'emplacement, la portée, la fréquence, la corrélation, le protocole, la plausibilité et la cohérence de chaque message transmis.

2.3.2 Solutions à base de pare-feu (firewall)

Dans [134], les auteurs ont mis en place un pare-feu matériel dans la couche de liaison de données du réseau CAN afin de le protéger contre les attaques de types DoS (voir figure 11). Cette étude propose un mécanisme de renforcement de la sécurité du bus CAN en se basant sur l'identification par saut (ID hopping (IDH-CAN)). Cette solution respecte les contraintes de temps réel et d'ordonnancement. Au niveau du bus CAN, chaque message dispose d'un ID (identifiant) unique. Le mécanisme d'ID-Hopping permet de générer des IDs alternatifs qui conservent les mêmes priorités que les priorités des ID d'origine et qui peuvent être utilisés lorsqu'une attaque DoS aura eu lieu

Une autre solution consiste à utiliser la passerelle centrale comme étant un pare-feu (Gateway Firewalls) pour intercepter les communications échangées entre les différents systèmes de bus [130, 131]. Cette passerelle contient les règles de contrôle d'accès et les clés de sécurité pour crypter les liens entre les différents sous-réseaux. Cependant, elle peut être considérée comme étant une surface d'attaque. De plus, les communications au sein de chaque sous-réseau ne sont pas contrôlées. Pour remédier à ces limitations, une autre solution a été introduite pour utiliser le pare-feu afin de sécuriser chaque passerelle du sous-réseau (ces passerelles sont connectées à la passerelle centrale) [135]. Cependant, elle reste très coûteuse.

2.3.3 Solutions à base d'IDS (Intrusion Detection System)

La majorité des solutions IDS sont proposées pour le système de bus CAN (voir figure 2.2).

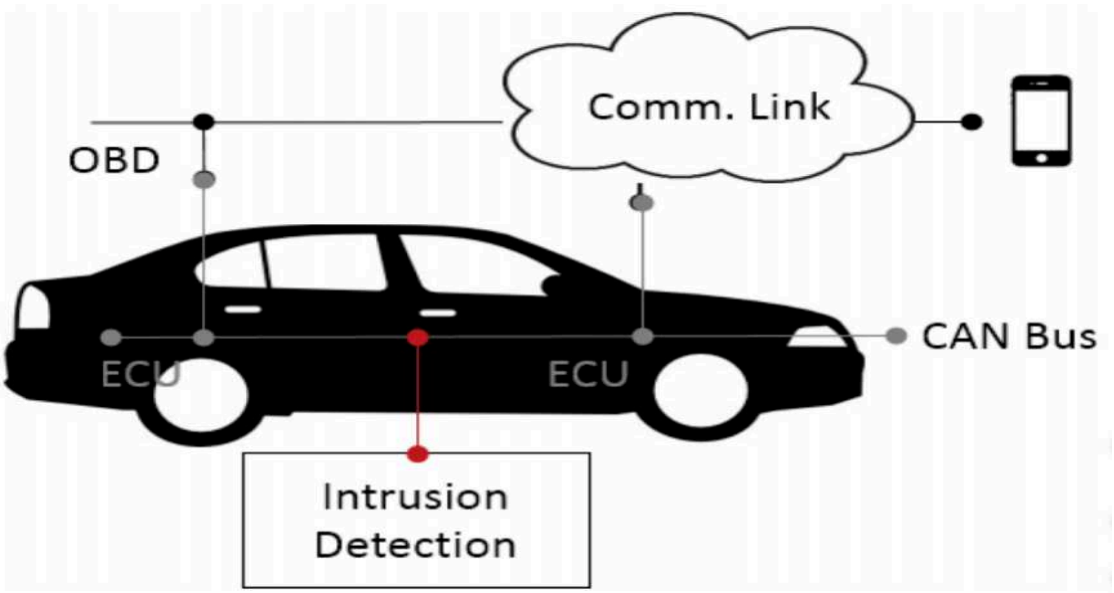


FIG. 2.2 : IDS pour sécuriser le réseau intra-véhiculaire [5]

L'accent est mis sur le bus CAN car il est utilisé de nos jours pour contrôler les composants les plus critiques du véhicule tels que le système de freinage et la commande du moteur qui doivent être particulièrement bien protégé. Dans [136], les auteurs ont présenté un système de détection d'intrusion à faible latence, pour le réseau CAN, basé sur l'entropie de l'information avec un nombre fixe de messages comme fenêtre glissante.

Le travail décrit dans [137] a proposé la mise en place d'un IDS pour surveiller le comportement des composants logiciels. Les auteurs ont créé une table de recherche comprenant toutes les relations prédécesseur/successeur des exécutables surveillés. Ils ont, ensuite, utilisé cette table pour comparer la séquence d'exécution réelle avec celle prédéfinie.

Plusieurs travaux [138, 139] ont proposé des solution d'IDS basés sur un seuil temporel pour détecter les attaques d'injection de faux message sur le bus CAN. La plupart des messages CAN sont transmis de manière planifiée à intervalles fixes. Les solutions IDS utilisent la fréquence de chaque message (chaque message a un ID unique) pour modéliser son comportement nominal [138, 139]. Pendant le fonctionnement du véhicule, tout message malveillant injecté sera remarqué car il aura un intervalle de temps plus court par rapport au seuil de référence défini par le calcul. Un court intervalle détecté indique une attaque par injection de faux message sur le bus CAN. De plus, les auteurs de, [139] utilisent la fréquence des messages pour détecter les attaques par déni de service. Dans leur proposition d'IDS, si ce court intervalle continue d'apparaître fréquemment plus qu'un score seuil prédéfini, le modèle considère que le système est en train de subir une attaque DoS.

Dans le cas où un ECU besoins des données fournit par un autre ECU. Il diffuse une requête (appelée remote frame) avec une identification particulière et reçoit une réponse (data frame) qui contient les données demandées. Lee et al. [140] ont proposé un mécanisme pour détecter une attaque d'injection de faux message basé sur le calcul de l'intervalle de temps entre les trames de demande et de réponse. Le mécanisme utilise cet intervalle de temps calculé pour le comparer avec celui qui a été détecté pendant l'exécution. Si le temps détecté est différent du temps calculé, les auteurs considèrent cela comme intrusion. Dans [5], les auteurs ont utilisé Deep Neural Network (DNN) pour concevoir un système de détection d'intrusion pour le réseau embarqué. L'IDS proposé est composé de deux phases : une phase de formation hors ligne et une phase de détection. Dans la phase de formation, les auteurs extraient un comportement statistique du réseau. Dans la phase de détection, le DNN calcule la probabilité d'un paquet CAN et décide si le paquet est normal ou s'il est contaminé.

Larson et ses collaborateurs [141] ont proposées une approche pour détecter les com-

portements indésirables au sein de chaque ECU. Cette approche consiste à examiner son comportement de communication. Les auteurs ont proposé de construire un modèle représentant les spécifications de comportement nominal pour chaque ECU. Ces spécifications contiennent l'ensemble des types et de fréquence d'envoi de messages sortants/entrants autorisés. De même, les auteurs de [142] ont proposé de créer une liste de tous les IDs des messages CAN légitimes que chaque ECU est autorisé à envoyer et recevoir. Ensuite, cette liste sera utilisée pour détecter les messages qui ne sont pas prédéfinis et les traiter comme des attaques d'injection de faux message.

2.3.4 Solutions logicielles

Les travaux [143, 144] ont proposé des solutions de sécurité à base d'algorithmes de chiffrement symétrique pour assurer la confidentialité des communications intra-véhiculaire sur le bus CAN. Dans d'autres cas, par exemple [145], un algorithme asymétrique est utilisé pour chiffrer la clé partagée qui sera utilisée ultérieurement par l'algorithme symétrique pour chiffrer les messages échangés. Le code d'authentification de message (MAC) est fréquemment adopté pour assurer l'intégrité et l'authenticité des communications à bord des véhicules [145]

Dans [146], les auteurs ont utilisé les algorithmes CMAC pour se protéger contre les attaques de mascarade sur le bus CAN, tandis que [6, 147] ont utilisé le HMAC dans le même but et les auteurs de [148] ont utilisé le keyed-hash MAC (32- bit truncated MAC)). Les auteurs de [6] ont créé une approche de sécurité basée sur ISO 26262 (Automotive Safety Integrity Level (ASIL)) . L'ASIL est composé de quatre niveaux (A, B, C et D) trié par degré de gravité, où A représenté le niveau de sécurité le plus bas (pas de mécanismes de sécurité) et D le niveau de sécurité le plus élevé (confidentialité, authentification et contrôle d'accès). Exemple : les auteurs ont attribué le niveau D au module TCM (Transmission Control Module) puisqu'il est responsable de la gestion de plusieurs fonctionnalité critique telles que le temps optimal pour le changement de la vitesse, le contrôle de l'économie de carburant et des émissions, ainsi que la qualité du changement de vitesse. La figure 2.3 présente un exemple de spécification de [6].

L'un des principaux problèmes dont souffre le MAC est celui de la non-répudiation. Pour cette raison, plusieurs auteurs [130, 149] ont proposé des solutions basées sur l'utilisa-

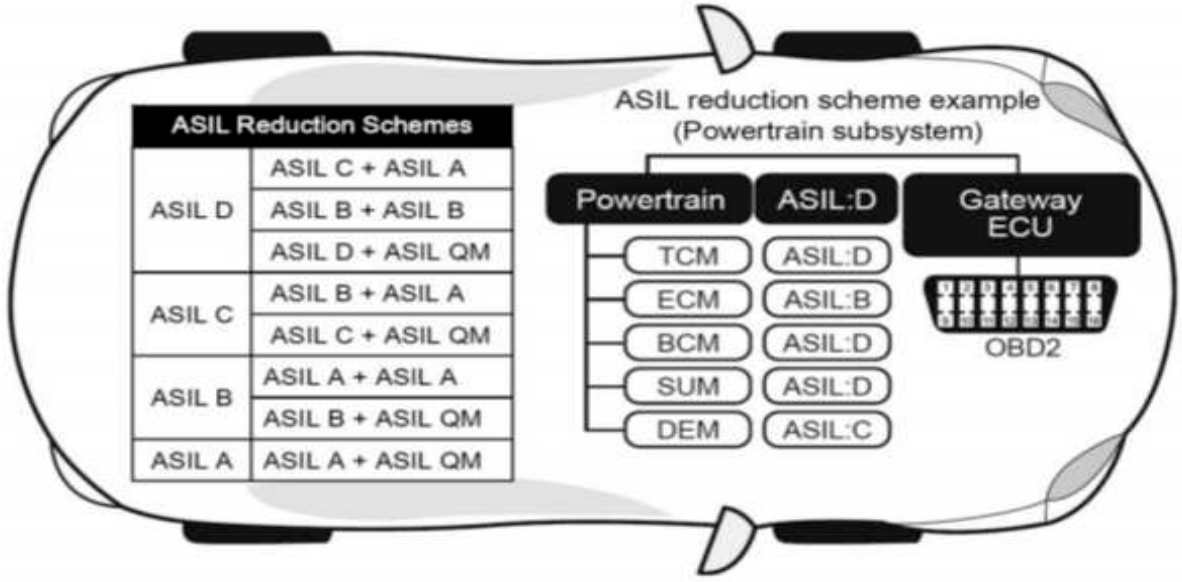


Fig. 2.3 : Couple (ECU, ASIL) [6]

tion d'une signature numérique pour assurer l'intégrité des messages et l'authentification de l'expéditeur dans le réseau intra-véhicule.

In [150], les auteurs ont proposé l'utilisation de IPsec pour le bus Ethernet. Avec l'intégration des technologies de communications sans fils, la mise en place des services de sécurité (confidentialité, authentification, intégrité, disponibilité, etc) devient une nécessité primordiale pour préserver la sécurité du réseau intra-véhicule.

2.4 Analyse énergétique des solutions de sécurité proposées

Les solutions proposées sont basées sur les mécanismes de sécurité les plus robustes. En outre, plus la solution de sécurité est solide, plus sa consommation d'énergie est élevée [28–31]. Nous allons évaluer la consommation énergétique d'un IVWSN (Intra-Vehicle Wireless Sensor Network) embarqué dans un véhicule. Ce scénario consiste à utiliser un IVWSN de 100 capteurs (deux caméras (450000 b/s), deux lidars (vlp32 (600000 points/s), vlp16 (300000 points/s)) et d'autres capteurs (100 b/s)) embarqués dans une Renault Zoe ZE (2015) avec différentes solutions de sécurité pendant un trajet de deux heures. Le fichier de l'énergie consommé par le véhicule est issu d'une étude expérimentale réel qui a eu lieu

à Rouen, France.

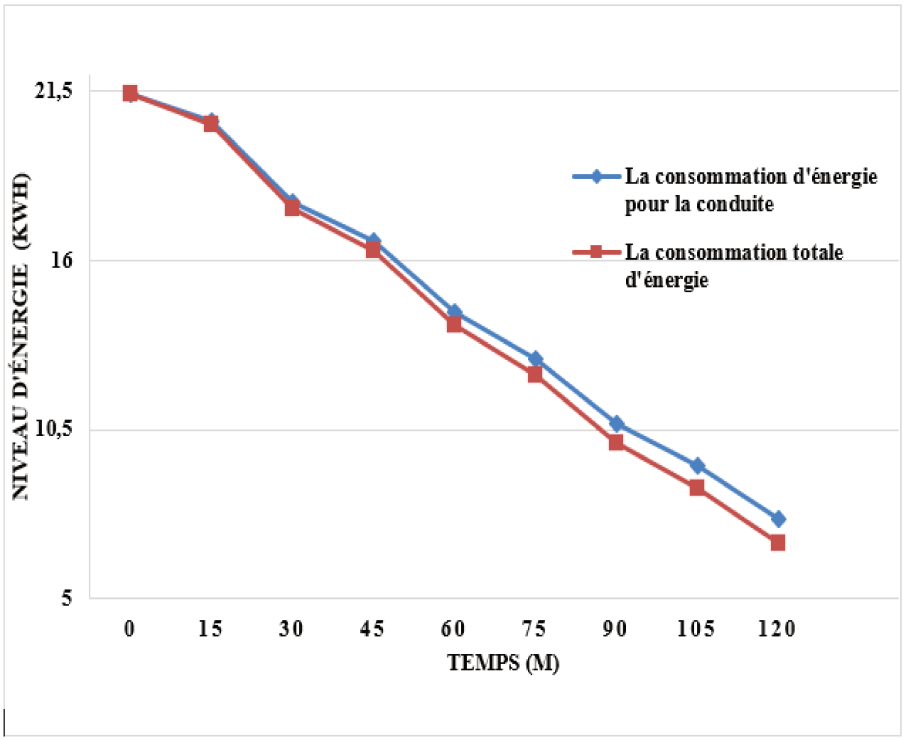


FIG. 2.4 : Consommation d'énergie utilisée pour la conduite et consommation totale d'énergie

La figure 2.4 montre la différence entre la consommation d'énergie utilisée pour la conduite et la consommation totale d'énergie du véhicule (y compris la génération des clés et l'échange d'un trafic sécurisé entre les capteurs) avec une périodicité de 15 minutes. Il y a une augmentation d'énergie en certains points de la courbe qui est due à la récupération d'énergie lors des freinages dans le scénario considéré.

Dans la figure 2.5, nous évaluons la consommation totale d'énergie des véhicules pour multiples mécanismes de sécurité (algorithmes de cryptage, fonctions de hachage). Dans le but d'éclaircir les résultats, dans la figure 16 nous se focalisons sur un laps de temps. La figure 2.5 et 2.6 montres que l'énergie consommée par les modules de sécurité augmente de manière significative en fonction de la robustesse des algorithmes cryptographiques et des services de sécurité. Par exemple, la consommation d'énergie d'un véhicule utilisant une solution de sécurité de haut niveau basée sur l'algorithme de cryptage AES_256 (Advanced Encryption Standard) et le Hash-based message authentication code (HMAC) consomme 92,3% de la capacité de la batterie. Cependant, en préservant le même cadre d'expérimentation, avec une solution de sécurité de bas niveau basée sur SKIPJACK et

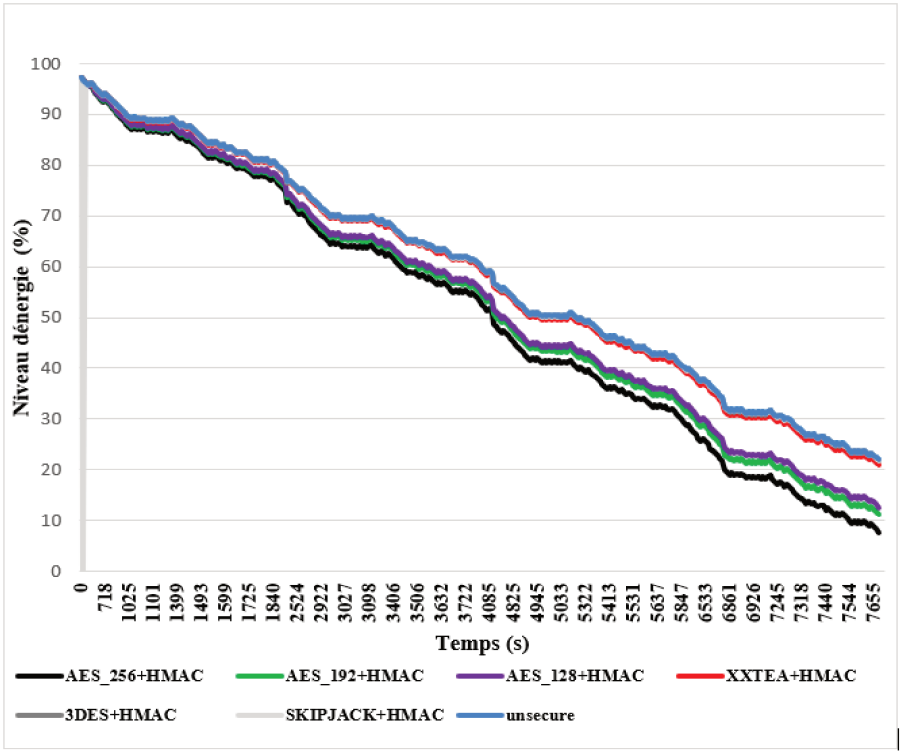


FIG. 2.5 : Consommation énergétique de configurations de sécurité

HMAC, la consommation d'énergie du véhicule est inférieure à 77% de la capacité de la batterie. La différence entre la consommation d'énergie des deux scénarios est d'environ 15 % de la capacité de la batterie. Les solutions proposées n'ont pas pris en compte les critères

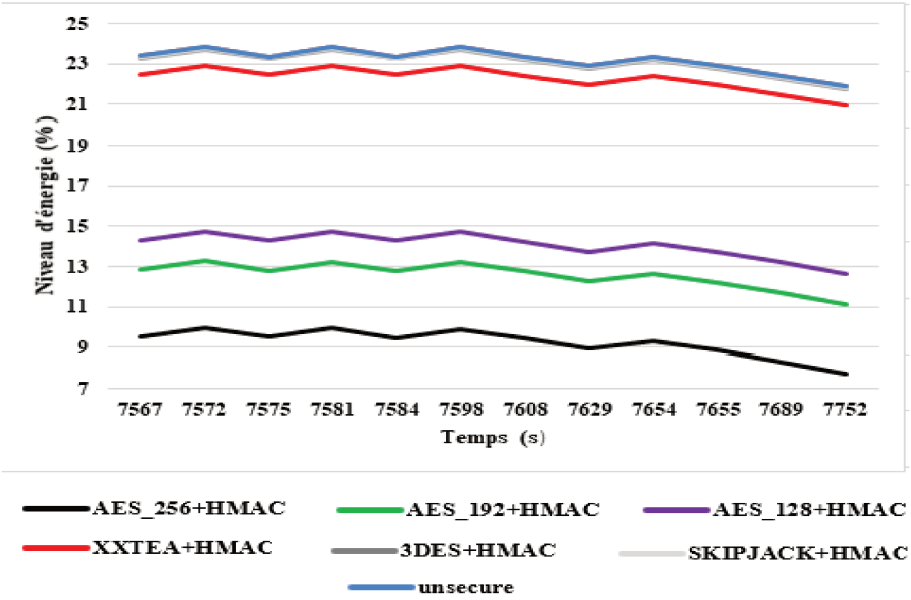


FIG. 2.6 : Consommation énergétique dans un intervalle de temps limité

de contrainte énergétique car les véhicules traditionnels (à carburant ou hybrides) n'ont

pas de contrainte énergétique. Cependant, on peut conclure que suivant les mécanismes de sécurité utilisés, il est possible d'augmenter le temps d'activation de la solution sur des véhicules qui présentent une contrainte d'énergie. La différence considérable en matière de consommation d'énergie pour les différentes politiques de sécurité est due au chiffrement. En effet, la différence entre la consommation énergétique des différentes fonctions de hachage est négligeable (voir figure 2.7).

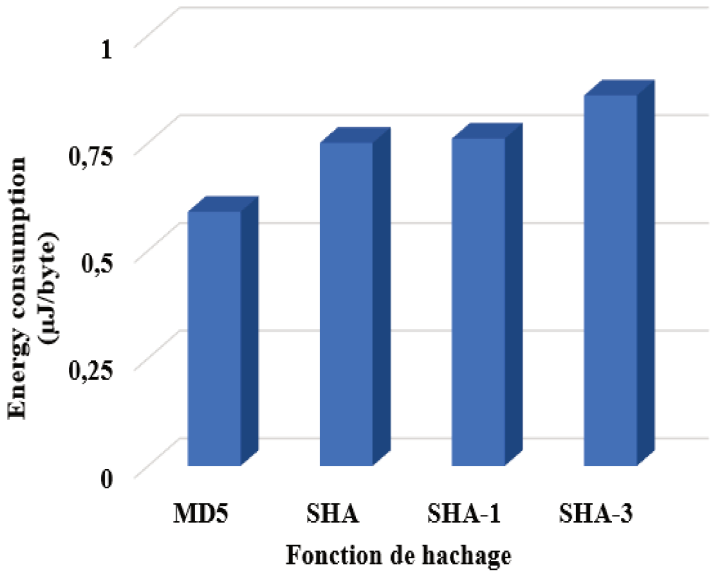


FIG. 2.7 : Consommation énergétique des fonctions de hachages

2.5 Solutions de sécurité basées sur le contexte (sécurité adaptative)

La sécurité contextuelle est généralement considérée comme une solution/protocole de sécurité qui détecte et s'adapte aux changements de l'environnement, la capacité des appareils et les variations des services du réseau. Elle s'adapte donc à l'évolution du contexte [31, 151, 152]. Par conséquent, une solution de sécurité contextuelle est bien adaptée aux communications à l'intérieur du véhicule électrique.

Dans cette section, nous allons définir le contexte et présenter les solutions de sécurité adaptative pour les réseaux WSNs. En effet, étant donné qu'il n'existe pas, à notre connaissance, de solutions de sécurité adaptatives pour le IVWSN proposées dans la lit-

térature, les réseaux de capteurs sont ceux qui s'y rapprochent le plus. De même, nous allons présenter les méthodes de modélisation de la sécurité adaptative.

2.5.1 Le contexte

Le contexte est défini comme étant toute information qui peut être utilisée pour caractériser la situation d'une entité. Une entité est une personne, un lieu ou un objet qui est considéré comme pertinent pour l'interaction entre un utilisateur et une application, y compris l'utilisateur et les applications elles-mêmes [151, 152]. Un système est dit contextuel s'il utilise le contexte pour fournir des informations et/ou des services pertinents à l'utilisateur [152]. En général, le développement de toute système

application contextuelle comprend les trois notions principales suivantes [152] :

- Acquisition du contexte : l'utilisation des capteurs pour la collecte d'informations contextuelles.
- Traitement : utilisation des techniques de raisonnement afin d'obtenir des informations contextuelles de haut niveau.
- Action : fournir des services à l'utilisateur en fonction de sa situation actuelle.

De nombreux travaux dans la littérature [153–155] se sont intéressés à la définition et à la caractérisation du contexte. Dans [155], les auteurs se réfèrent au contexte en tant qu'environnement (temps, lieu, température et paramètres d'identité). Schilit et al. [154] ont pris en compte les ressources proches (personnes, hôtes et dispositifs accessibles). Dans [153], Abowd et Dey ont considéré l'identité et l'activité (ce qui se passe dans la situation). Le réseau des véhicules connectés est un système basé sur le contexte car il fournit des services adaptés à l'utilisateur en fonction des informations variables du contexte de conduite : informations sur le véhicule (vitesse, position, niveau de batterie, etc.), trafic routier, conditions de route, etc. Les informations sur le contexte de conduite sont généralement composées de toute information décrivant la situation de conduite [152].

Les auteurs, dans [156], ont considéré la criticité du message comme étant un contexte. Ces messages sont classés en quatre types : normal, critique, très critique (signaux d'alerte)

et extrêmement critique (messages d'alerte, d'assistance). Dans [157], le contexte est composé de la sensibilité des messages V2X et de la sécurité des véhicules. Les auteurs, dans [158], ont considéré la priorité des messages et la force du signal. Les chercheurs, dans [159], ont présenté le contexte comme étant la signature du message, le nombre de saut du message (messages à saut unique (single hop messages), messages à sauts multiples (multi-hop messages)), la densité du trafic et le trajet.

2.5.2 Les solutions de sécurité contextuelle pour les WSNs

De nombreuses travaux de recherche [37, 38, 40, 41, 160] se sont intéressées au compromis entre l'efficacité énergétique et la sécurité des communications dans les WSNs. Dans ces travaux, pour remédier aux problèmes énergétiques dans les réseaux WSNs, la sécurité est adaptée en fonction des informations contextuelles. Dans [37, 160], les auteurs ont défini des niveaux de sécurité en fonction des caractéristiques des mécanismes de sécurité (taille des clés, type de chiffrement (symétrique, asymétrique)). Dans [160], les auteurs ont défini deux niveaux de sécurité basés sur la taille des clés (AES-CBC-128, AES-CBC-256). Cependant dans [37], les niveaux de sécurité sont basés sur le type de cryptage (symétrique (mode d'économie d'énergie), asymétrique (mode consommateur d'énergie)).

Dans [160], le contexte est composé du type de données, de l'emplacement du dispositif et du niveau du risque. Dans [37], le contexte est défini comme étant l'énergie restante (seuil). Dans [160], la dépendance totale de l'identification du niveau de risque à l'IPS (Intrusion Prevention System) a un impact sur la sécurité du système, puisqu'il est susceptible d'identifier des valeurs de risque faux positifs et faux négatifs. Pour ces deux travaux, les auteurs devraient considérer autant d'algorithmes de cryptage que possible, tels que DES, 3DES, skipjack qui sont plus efficaces en termes de consommation énergétique que l'AES [28].

Dans [38, 40, 41], les auteurs ont défini des niveaux de sécurité en fonction des services de sécurité (authentification, confidentialité, etc.). Dans [38, 41], les auteurs ont défini les niveaux de sécurité en fonction de l'authentification et de la confidentialité, tandis que dans [40], les niveaux de sécurité sont basés uniquement sur le service d'authentification. Dans [38], le contexte est constitué de la sensibilité des données transmises (sensibles

et non sensibles) et de l'énergie disponible. L'une des faiblesses de cette solution est de choisir l'algorithme de cryptage symétrique (skipjack) le moins robuste pour le plus haut niveau de sécurité.

Dans [41], Gheorghe et al. ont présenté un cadre de sécurité adaptative pour les WSNs, basé sur des informations contextuelles telles que les menaces détectées et les ressources disponibles des capteurs (énergie et mémoire). Plusieurs configurations de sécurité existent et sont choisies en fonction du contexte. Cette solution nécessite beaucoup de mémoire disponible pour s'adapter à toutes les configurations. De plus, les auteurs ont utilisé un cryptage asymétrique (comme niveau de sécurité supérieur) qui consomme beaucoup d'énergie et de mémoire dans le contexte des WSNs.

Dans [40], Arfaoui et al. ont développé un protocole d'authentification en fonction du contexte pour les applications de santé en ligne. Pendant la phase d'authentification, les auteurs ont sélectionné de manière adaptative un nœud de relais en fonction du niveau d'énergie, du canal de communication, de la mémoire et de la mobilité du WBAN (Wireless Body Area Network). Néanmoins, la solution de sécurité adaptative doit également prendre en compte le cryptage afin de préserver la vie privée des patients.

Dans les travaux de [161], les auteurs ont développé un jeu non coopératif, pour les WSNs cognitifs, permettant une sécurité adaptative pour la couche physique (adaptive physical layer security) et offrant un compromis entre la sécurité et la consommation d'énergie. La solution proposée génère du bruit artificiel adaptatif pour protéger les réseaux des attaques contre la vie privée. La décision de générer du bruit artificiel dépend du contexte qui est formé de l'état de charge du capteur et de la décision des autres joueurs. Les avantages et les inconvénients de chaque approche sont présentés dans le tableau 2.2.

Ces solutions considèrent essentiellement l'énergie et la mémoire comme étant le contexte. En effet, les WSNs traditionnels sont caractérisés par une batterie limitée, difficile à remplacer ou à recharger. Dans l'IVSN, ces paramètres doivent aussi être pris en considération, cependant, l'énergie à considérer sera celle de la batterie du véhicule plutôt que celle du capteur.

Tab. 2.2 : Avantages et inconvénients des solutions proposées

Travaux	Les paramètres d'adaptation	Avantages	Inconvénients
(Gheorghe et al., 2012) [41]	- L'énergie disponible - Le risque détecté, la mémoire Les exigences de sécurité	- Modularité -Extensibilité	Gourmand en mémoire
(Di Mauro et al., 2015) [38]	- Niveau d'énergie - Type de données (sensibles, non sensibles)	Économie d'énergie	Manque de robustesse de la stratégie de sécurité la plus élevée
(Ferrera et al. , 2016) [160]	-Type de données - Localisation du dispositif - Niveau de risque	Amélioration de la durée de vie de la batterie	- Dépendance totale à IPS - Fausses positives et vraies négatives.
(Kim et all, 2016)[37]	L'énergie restante provenant de la récupération de l'énergie	- Réduction du blocage - Efficacité énergétique	L'AES-128 est utilisé comme étant le mode le plus économe en énergie.
(Arfaoui et al., 2019) [40]	- Énergie, Mémoire , Mobilité - Modèle de communication - Scénario d'application (Normal / Urgent)	- Efficacité des communications -Efficacité énergétique	Devrait considérer le cryptage
(Romero et all, 2019) [161]	La décision des autres joueurs Ressources énergétiques	Économie d'énergie	Devrait considérer le cryptage

En effet, les capteurs sont alimentés par la batterie de l'EV qui peut être rechargée tout au long du trajet. De même, l'état du trafic est un facteur déterminant pour atteindre la station de recharge. Par conséquent, le contexte de la solution que nous proposons va au-delà du contexte WSNs en considérant à la fois la distance aux stations de recharge et l'état du trafic. Ainsi, la mémoire et la capacité de traitement des capteurs, l'énergie disponible, la station de recharge la plus proche, l'état du trafic et le type de capteur (critique, semi-critique ou de confort) font partie du contexte pour représenter l'écosystème spécifique des VE. De plus, dans la solution que nous proposons, les niveaux de sécurité seront basés à la fois sur la robustesse des mécanismes cryptographiques et sur les services de sécurité. Nous avons également ajouté la consommation d'énergie des mécanismes cryptographiques comme critère puisque notre objectif principal est de réduire la consommation énergétique d'énergie.

2.6 Conclusion

Dans ce chapitre, nous avons présenté les solutions proposées pour la sécurisation des réseaux intra-véhiculaires. Ces solutions sont classées en solutions matérielles, à base de firewalls, d'IDS et logicielles. Cependant, ces solutions ne sont pas adaptées telles qu'elles sont (statiques) pour le réseau interne des véhicules électriques qui présentent des contraintes d'énergie. Les solutions de sécurité adaptatives permettent de mieux répondre aux exigences des réseaux intra-véhiculaires en termes de compromis entre la sécurité et la consommation d'énergie. Ainsi, nous avons étudié les solutions de sécurité adaptées au contexte et proposées pour les WSNs en tant que réseaux qui se rapprochent le plus des réseaux intra-véhiculaires. Dans le chapitre suivant, nous allons présenter la solution de sécurité que nous proposons pour le réseau intra-véhiculaire et que nous désignons par CASIEV.

Chapitre 3

Solution de sécurité contextuelle pour le réseau intra véhicule électrique connecté

3.1 Introduction

Le réseau de capteurs embarqués dans les véhicules (Intra-Vehicle Sensors Network (IVSN)) est une cible des pirates informatiques puisqu'il constitue une source d'informations critiques stockées et échangées via les capteurs embarqués dans les véhicules, telles que la combinaison porte-verrouillage du véhicule, les numéros de cartes de crédit, les informations pour les applications intelligentes, etc.

Pour éviter ces attaques, plusieurs travaux [4, 23–26], dans la littérature, ont proposé des solutions de sécurité statique pour l'IVSN. Ces solutions statiques sont basées sur les mécanismes de sécurité les plus robustes, tels que l'authentification forte et le chiffrement, qui ont un impact sur la consommation d'énergie [31]. Ainsi, malgré leur importance, ces travaux n'ont pas pris en compte la contrainte énergétique des véhicules électriques lors de la conception des solutions de sécurité.

Pour répondre à ces contraintes et sécuriser l'IVSN, nous proposons, dans ce chapitre, une solution de sécurité basée sur le contexte (adaptative) que nous désignons par CASIEV (Context Aware Adaptive security for the Intra-Electric Vehicle network). De même, nous évaluons ses performances en termes de niveau de sécurité, temps d'activation de la sécurité et temps de latence. Enfin, nous comparons la solution proposée avec une solution statique de sécurité.

3.2 Méthodes de modélisation pour la sécurité adaptative

Dans la littérature, certaines méthodes de modélisation sont couramment utilisées pour la sécurité adaptative telles que la méthode à base de scénario [162], la théorie des jeux [163] et l'ontologie [164].

- Modélisation à base de scénario : La méthode à base de scénario [162, 165] décrit les hypothèses de base et le modèle de processus, spécifie les scénarios, la méthode par laquelle les scénarios sont formés, y compris les techniques de modélisation et les sources de données . Ce type de modélisation est très adapté pour les solutions basées

sur le contexte. La plupart des solutions de sécurité contextuelle, pour les réseaux de capteurs, décrites dans le chapitre 2 sont modélisées à travers cette méthode. CASIEV va être modélisé suivant cette méthode.

- La théorie des jeux La théorie des jeux traite des problèmes dans lesquels plusieurs joueurs ayant des motivations ou des objectifs contradictoires sont en concurrence les uns avec les autres [163]. Elle a la capacité de modéliser un grand nombre de scénarios avant de prendre la meilleure action. La théorie des jeux est également utilisée dans la sécurité des réseaux qui étudie l'interaction entre les pirates et les défenseurs [166] . De nombreux auteurs [167, 168] ont adopté l'approche de la théorie des jeux pour modéliser des solutions de sécurité adaptative.

- Ontologie L'ontologie est une spécification formelle explicite qui vise à identifier les propriétés d'un domaine et les relations existant entre elles. Elle fournit une signification sémantique en définissant les relations entre les concepts liés au domaine [164, 169]. Dans la littérature, plusieurs travaux ont proposé une sécurité adaptative basée sur les événements dans le cadre de IoT.

3.3 Solution de sécurité contextuelle pour le réseau intra véhicule électrique connecté : CASIEV

Dans cette partie, nous présentons la solution CASIEV qui est une solution de sécurité basé sur le contexte [170]. CASIEV adapte les niveaux de sécurité en fonction des informations contextuelles du véhicule électrique. Nous identifions, tout d'abord, les paramètres du contexte du véhicule électrique. Ensuite, nous présentons la solution CASIEV.

3.3.1 Le contexte dynamique du véhicule électrique

Nous considérons cinq paramètres de base pour représenter le Contexte des VEs (CVE). CVE= {SoC, m&p, tc, tr, dcs} où SOC désigne l'état de charge de la batterie, m&p : les ressources en termes de mémoire et de traitement, tc : le type de capteurs, tr : le modèle de trafic et dcs : la distance par rapport à la station de charge.

État de charge de la batterie « Battery State Of Charge (SOC) »

Dans [171], les auteurs ont proposé un modèle de consommation d'énergie instantanée pour les VE en introduisant, comme entrées, la vitesse du véhicule, l'accélération et la pente de la route. Le modèle proposé estime la consommation d'énergie avec une erreur moyenne de 5,9 %, par rapport aux données empiriques. Il prend également en compte la récupération instantanée de l'énergie de freinage en fonction de la décélération. En appliquant un tel modèle, les véhicules électriques récupèrent plus d'énergie dans une zone urbaine que sur les autoroutes à grande vitesse. L'impact des auxiliaires sur la consommation d'énergie a été identifié dans [171]. Ce résultat a été confirmé dans [172]. D'après [33], le SOC (State Of Charge) devrait se situer entre 20 et 95% pour garantir la sécurité du système de batterie. L'état de charge de la batterie peut être représenté comme suit [171] :

$$SOC = SOC_0 - \frac{1}{C_N}\eta \int_0^t I dr \tag{3.1}$$

Où C_N est la puissance de la batterie ; I désigne le courant de la batterie ; η correspond à l'efficacité d'une charge et d'une décharge non constante (dépendant de plusieurs facteurs tels que la température, le comportement du conducteur, etc.) et SOC_0 désigne le niveau de charge initial.

Ressources en termes de Mémoire et de Traitement

La puissance de calcul, la mémoire et la capacité de communication limitée des dispositifs électroniques d'un véhicule sont les principales limites à l'application des mécanismes de sécurité conventionnels pour protéger les réseaux embarqués [173, 174]. Dans l'obligation de la mise en place d'une solution de sécurité au niveau du réseau intra-véhicule, il est primordial de prendre en considération principalement les deux critères mémoires et traitement lors du choix des mécanismes de sécurité.

Type de capteurs

Plusieurs travaux dans la littérature [175–177] se sont intéressés à la catégorisation des capteurs dans l'intra-véhicule. Dans [175], les capteurs ont été classés en trois catégories

en fonction de leur déploiement dans le véhicule châssis, groupe motopropulseur et carrosserie. Sherin et al. [176] ont considéré le type d'application comme critère de classification et ont classé les capteurs en quatre catégories : sécurité, diagnostic, confort et surveillance de l'environnement. Les capteurs de sécurité sont classés en plusieurs types : capteurs de distance (radars, scanners laser – appelés LIDAR (pour Light Radars), capteurs à ultrasons, etc), Capteurs de vision nocturne (Caméra Vision Nocturne Infrarouge), capteurs de vitesse, Capteurs inertiels de vitesse angulaire/accélération linéaire, Capteurs passifs de soutien à la sécurité (capteurs de poids, les capteurs de position des sièges, etc), Systèmes de positionnement/navigation (Global Positioning System (GPS)). Les capteurs de diagnostics sont utilisés pour fournir aux conducteurs des services de diagnostic embarqués afin de détecter les dysfonctionnements des composants et d'éviter tout dommage supplémentaire qui pourrait entraîner une panne. Cette catégorie de capteurs contient : les capteurs pour le diagnostic des groupes motopropulseurs, Capteurs pour le diagnostic du châssis (capteur de vitesse, capteur de pression), Capteurs pour le diagnostic de la carrosserie (le capteur utilisé pour diagnostiquer le dysfonctionnement des airbags).

Les capteurs de confort sont classés en deux catégories : capteurs de confort dans la cabine (capteurs d'humidité et de température) et capteurs de confort de conduite (capteurs d'image, capteurs de prévention de la buée, capteur de position). Les capteurs pour la surveillance de l'environnement sont chargés de surveiller le milieu environnant et ses conditions. Ils visent à fournir des services ITS sous la forme d'alertes concernant les dangers sur les routes ou d'informations sur le trafic (capteur de distance), les conditions routières et météorologiques (un capteur de pression, les capteurs de température). Dans [177], Juan et al. ont ajouté deux nouvelles catégories : surveillance de la conduite (les capteurs radar, les caméras, les boucles inductives et les capteurs de profondeur) et surveillance du trafic (caméras, capteurs de profondeur, radars, ultrasons).

Ces classifications n'ont pas pris en compte la criticité et la consommation énergétique du capteur. En effet, on remarque que les classifications proposées sont basées sur le type d'applications, alors qu'un capteur peut appartenir à plusieurs catégories d'applications. En outre, ces travaux ne traitent pas le degré d'impact des capteurs sur la sureté de fonctionnement du véhicule. De même, comme nous considérons les véhicules électriques dans ce travail, les capteurs multimédias peuvent avoir un impact sur la consommation éner-

gétique du véhicule. Pour toutes ces raisons, nous proposons, une nouvelle classification des capteurs basée sur leur criticité et consommation énergétique.

- ***Criticité*** :Les capteurs peuvent être classés en trois types selon la sécurité du conducteur et le type d'application (e-safety, etc.) : les capteurs critiques, les capteurs semi-critiques et les capteurs de confort.
  - Un capteur **critique** est un capteur qui envoie des informations essentielles pour la sécurité du conducteur. Dans [176, 177], les auteurs ont énuméré les capteurs critiques tels que le radar, le laser, le lidar, la vision par caméra, les ultrasons, la vitesse, le GPS et le niveau de charge de la batterie.
  - Un capteur **semi-critique** est un capteur qui envoie des informations essentielles pour une application spécifique mais qui n'a pas d'impact sur la sécurité du conducteur.
  - Les capteurs de **confort** tels que le chauffage et la climatisation, sont ceux qui rendent le véhicule plus confortable.
- ***Consommation d'énergie*** : Selon ce critère, les capteurs peuvent être classés en deux types :
  - Capteurs **économes** en termes de consommation énergétique.
  - Capteurs **gourmands** en termes de consommation d'énergie (énergivore) tels que les caméras et les lidars.

  Ce critère de classification n'est pas pris en compte pour les capteurs critiques.

Ainsi, le type de capteur (tc) est défini comme suit :

$$tc \in \{C_c, C_{SC-E}, C_{SC-G}, C_{CO-E}, C_{CO-G}\}$$

où C_c : pour critique (peu importe la consommation d'énergie) ; C_{SC-E} : pour sous-critique - économique ; C_{SC-G} : pour semi-critique -gourmand en énergie ; C_{CO-E} : pour confort – économes en énergie ; C_{CO-G} : pour confort – gourmand en énergie.

La figure 3.1 présente les catégories de capteurs intra-véhicule.

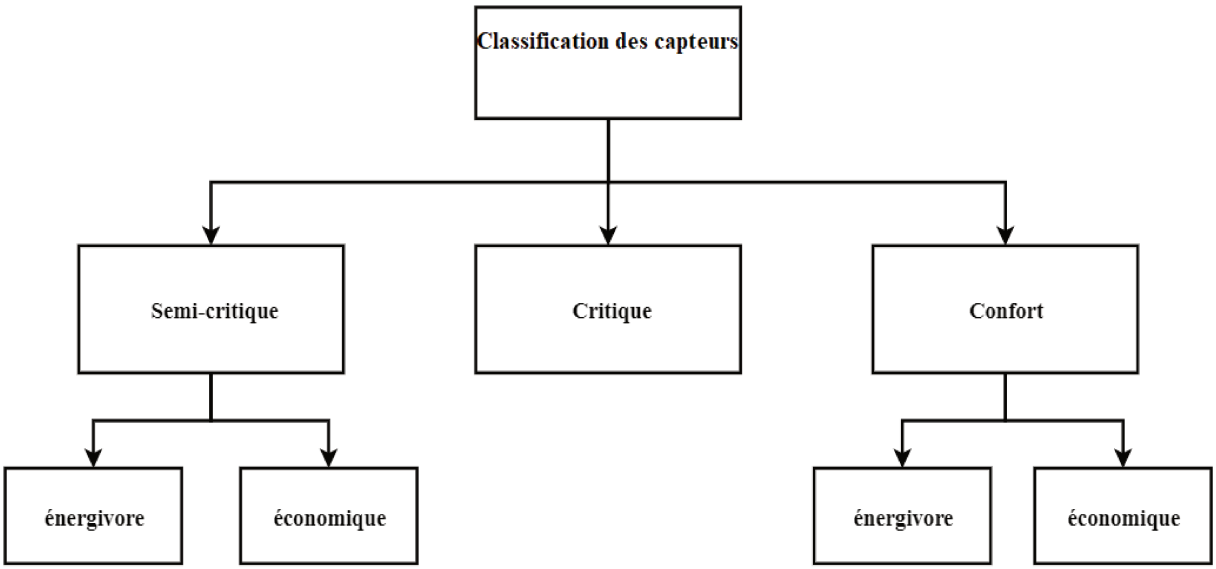


FIG. 3.1 : Type de capteurs

Le Modèle de trafic

Le trafic est un facteur important pour les réseaux véhiculaires [178]. Il affecte la consommation d'énergie des VE de diverses manières. En effet, l'augmentation du trafic routier entraîne une augmentation de la consommation d'énergie des VE [179]. L'état du trafic routier peut être identifié grâce à la vitesse du véhicule tel que représenté dans (3.2).

$$V_t = \alpha \times S_t + (1 - \alpha) \times V_{t-1} \tag{3.2}$$

V_t : vitesse moyenne (km/h) calculée au temps t sur une fenêtre glissante W de taille T telle que W= [t-T+1, t] ; S_t : vitesse instantanée au temps t et V_{t-1} : vitesse moyenne précédente ; $\alpha \in [0..1]$. Le trafic peut être faible, moyen ou élevé comme suit (3.3).

$$Trafic = \begin{cases} faible, & V_t \geq \beta \\ moyen, & \gamma \leq V_t < \beta \\ \text{élevé}, & V_t < \gamma \end{cases} \tag{3.3}$$

avec, $\beta > \gamma$

Les perturbations de la circulation (traffic oscillations) désignent les conditions de conduite discontinu « stop-and-go » dans un trafic congestionné. Ces derniers forment généralement des bouchons dans les infrastructures de transport et ont un impact très important sur la consommation énergétique du véhicule électrique [179]. Pour cette raison, nous allons considérer ce paramètre lors de la conception de la solution de sécurité.

Distance à la station de recharge

Les Stations de Recharge (SR) constituent un élément clé de l'écosystème des VE [180]. La distance jusqu'à la station de recharge DSR est le chemin entre les deux positions (x_{SR}, y_{SR}) et (x_{VE}, y_{VE}), où (x_{SR}, y_{SR}) est la position de la station de recharge la plus proche disponible et (x_{VE}, y_{VE}) désigne la position du VE.

En pratique, on pourra utiliser l'algorithme de Dijkstra pour déterminer le plus court chemin entre le VE et le SR.

3.3.2 La sécurité adaptative pour le réseau intra-véhiculaire

Pour répondre aux problèmes de sécurité du réseau interne des véhicules électriques, nous proposons une stratégie de sécurité qui s'adapte au contexte et qui fournit des services de sécurité (authentification, confidentialité, intégrité, etc.) même si l'énergie est faible.

Hypothèses

Nous supposons que :

- E_s : est le niveau d'énergie critique pour assurer la sécurité du conducteur.
- E_{th} est le seuil d'adaptation de la sécurité par rapport à l'environnement, avec $E_{th} > E_s$. Nous attribuons trois seuils selon le type de capteur (critique, semi-critique et de confort) tels que : $E_{th\_c} < E_{th\_sc} < E_{th\_co}$, avec E_{th_c} : le seuil d'adaptation du capteur critique, E_{th_sc} : le seuil d'adaptation du capteur semi-critique, E_{th_co} : le seuil d'adaptation énergétique du capteur de confort.
- $L = \{l_0 ...., l_n\}$ l'ensemble des niveaux de sécurité.

- Chaque capteur est capable d'estimer la consommation énergétique des autres capteurs.
- Les capteurs sont authentifiés en appliquant une authentification par clé partagée.
- Les capteurs peuvent offrir des services de confidentialité, d'intégrité et d'authentification.
- Nous considérons trois zones (voir figure 3.2) :
  - Une zone verte où la sécurité est maximale tant que l'énergie est disponible ($e \geq E_{th}$).
  - Une zone orange où on adapte la sécurité à l'énergie ($e \geq E_{th}$), le trafic et la distance à la stations de recharge($E_s < e < E_{th}$).
  - Une zone rouge où la sécurité ne sera pas assuré pour ne pas mettre en danger le conducteur (sécurité du conducteur) puisque l'énergie a atteint un seuil critique ($e < E_s$).

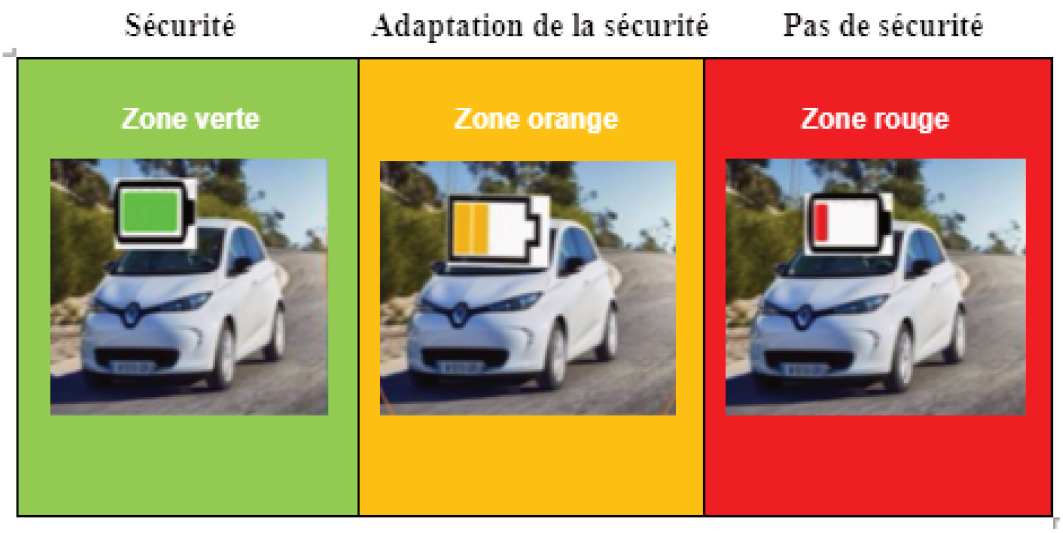


FIG. 3.2 : Zone d'adaptation de la sécurité

Approche de sécurité adaptative monocritère

Nous présentons la stratégie de sécurité adaptative mono critère pour chaque capteur (zone orange). Pour cela, nous considérons les stratégies suivantes :

Adaptation à l'énergie

L'adaptation en fonction de l'énergie est présentée dans (3.4).L_e est l'ensemble des niveaux de sécurité qui peuvent être atteints en fonction de l'énergie restante.

$$L_e = \{l_i, \forall \;\; 0 \leq i \leq n; \;\; e - e\_cons(l_i) \geq E_{th}\} \tag{3.4}$$

Avec e représente l'énergie disponible en tenant compte de la consommation des autres capteurs et du SOC du véhicule. Eth $\in \{E_{th\_c}, E_{th\_sc}, E_{th\_co}\}$ suivant le type de capteurs. $e_cons(l_i)$ Consommation d'énergie du capteur mettant en œuvre le niveau de sécurité (l_i). Pour chaque capteur :
$e\_cons(l_i) = e_{transmission} + e_{reception} + e_{processing}(l_i)$,
$e_{transmission}$: l'énergie utilisée pour la transmission, $e_{reception}$: l'énergie utilisée pour la réception, $e_{processing}(l_i)$: l'énergie utilisée pour le traitement du niveau de sécurité (l_i).

Adaptation par rapport à la distance à la station de recharge

L'adaptation du niveau de sécurité en fonction de la distance à la station de recharge la plus proche est présentée dans (3.5).$L_{dcs,e}$ est l'ensemble des niveaux de sécurité dont la consommation d'énergie permet d'atteindre la station de recharge. Ainsi, ces niveaux doivent satisfaire la contrainte ($e - e\_cons(l_i) > E_s$) afin de préserver la sureté de fonctionnement du véhicule et la sécurité des passagers.

$$L_{dcs,e} = \{l_i, \forall \;\; 0 \leq i \leq n; (d(e) \geq dcs) \wedge (e - e\_cons(l_i) > E_s)\} \tag{3.5}$$

Avec : dcs : la distance jusqu'à la station de recharge disponible la plus proche. $d(e, l_i)$: la distance qui peut être parcourue par l'énergie restante en utilisant le niveau de sécurité (l_i). E_s : le seuil du niveau d'énergie critique

Adaptation au trafic

L'adaptation du niveau de sécurité en fonction du trafic est présentée dans (3.6). L_{tr} représente l'ensemble des niveaux de sécurité qui peuvent être mis en œuvre en fonction du trafic.itr est l'indice du niveau de sécurité le plus élevé possible autorisé par le trafic (tr).

$$L_{tr} = \{l_i, 0 \leq i \leq itr, tr \in \{low, medium, high\}; (l_i \leq l_{itr})\} \tag{3.6}$$

Pour le même type de trafic, itr peut différer d'un type de capteur à un autre. Nous définissons les valeurs suivantes pour itr (voir table 3.1). On peut remarquer que même

TAB. 3.1 : Niveau de sécurité pour le couple (type de trafic, type de capteur)

Type de trafic	type de capteur	itr
Faible	critique	4
	Semi-critique	3
	confort	2
moyen	critique	3
	Semi-critique	3
	confort	1
élevé	critique	2
	Semi-critique	1
	confort	0

pour un trafic fluide (faible), seuls les capteurs critiques sont autorisés à appliquer le plus haut niveau de sécurité. Cette décision a été prise pour répondre à la contrainte énergétique du véhicule électrique.

Approche de sécurité adaptative multicritères

La figure 3.3 décrit l'approche d'adaptation de la sécurité en fonction du contexte global. CASIEV prend en entrée le contexte (énergie, trafic, distance à la borne de recharge, mémoire et traitement, type de capteur) et l'ensemble des niveaux de sécurité. Les niveaux de sécurité ont été choisis en fonction du paramètre de contexte « capacité de mémoire et traitement » ainsi que leurs consommations d'énergie. Dans la stratégie actuelle, on applique le niveau de sécurité le plus haut. C'est ce que l'on désigne par zone verte (L_n). Dans le cas contraire ou l'énergie disponible ne permet pas d'appliquer le niveau de sécurité le plus robuste ($e - econs(l_n) < e_{th}$) , l'adaptation de la sécurité est déclenchée par les facteurs suivants : l'énergie (L_e), la distance à la station de recharge et le trafic (L_{dcs-tr}). C'est ce que l'on désigne par zone orange. La distance à la station de recharge et le trafic sont étroitement liés puisque le type du trafic peut avoir un impact sur l'énergie restante et conditionner le fait d'atteindre ou pas la station de recharge.

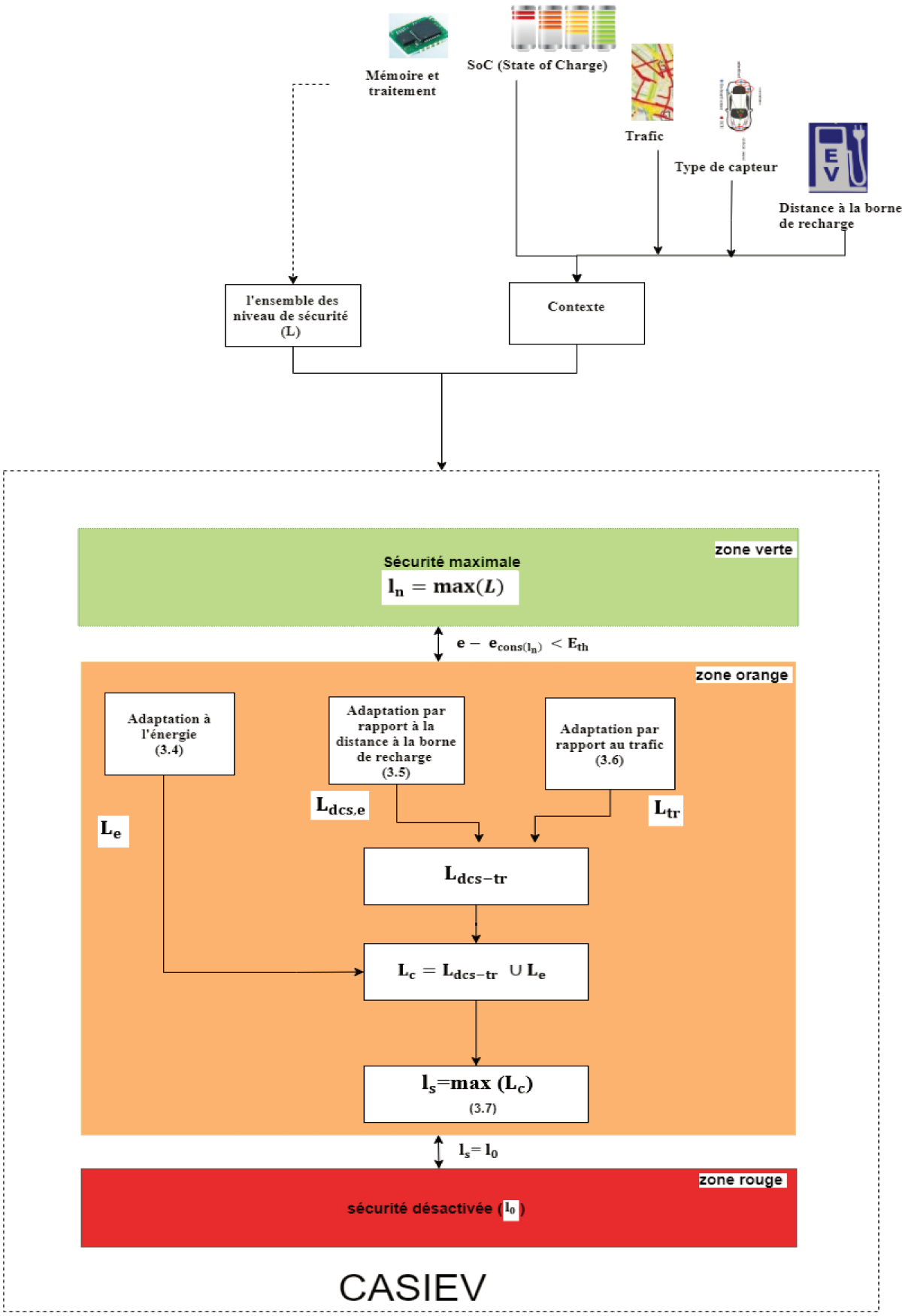


FIG. 3.3 : Architecture de CASIEV

Ainsi, on considère l'intersection des deux ensembles (L_{dcs-tr}) résultant de l'adaptation par rapport à la distance qui sépare le véhicule de la station de recharge ($L_{dcs,e}$) et l'adaptation par rapport au trafic(L_{tr}). Enfin, nous déterminons le niveau de sécurité maximal entre (L_{dcs-tr}, L_e).

L'adaptation au contexte global (type de capteur, énergie, trafic, distance à la station de recharge disponible la plus proche) est présentée dans (3.7). $l_s(tc, e, tr, dcs)$ détermine le niveau de sécurité le plus robuste qui peut être atteint en fonction du contexte global.

$$l_s(e, ts, tr, dcs) = max_{(e,ts,tr,dcs)}\{l_i, \forall \ \ 0 \leq i \leq n; \ \ L_e \cup (L_{dcs,e} \cap L_{tr}) \ \} \tag{3.7}$$

La figure 3.4 présente le diagramme d'état de la solution CASIEV et les transitions entre les états.CASIEV passe de l'état attente à l'état zone de confort si l'énergie est disponible ($Econs(l_n) < E - E_{th}$).

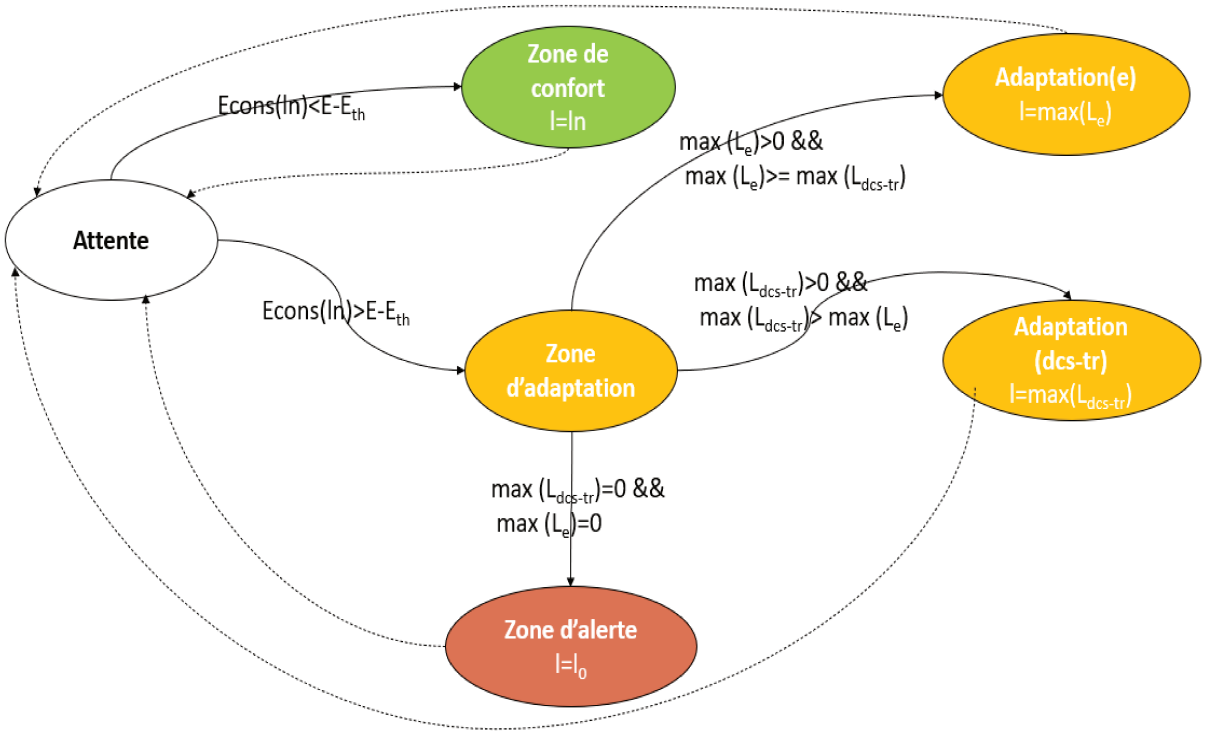


FIG. 3.4 : Diagramme d'état de la solution CASIEV

Dans le cas contraire (Econs (l_n) > $E - E_{th}$), il passe à l'état zone d'adaptation afin d'adapter la sécurité suivant l'énergie, la distance à la borne de recharge et le trafic. L'état zone d'adaptation conduit aux états adaptation (e) ou adaptation (dcs-tr). Le système adapte la sécurité en fonction de l'energie si max (L_e)>0 && max (L_e)> max

(L_{dcs-tr}). Cependant, il adapte la sécurité on fonction de la distance à la station de recharge et le traffic si max (L_{dcs-tr}>0 && $maxL_{dcs-tr} > maxL_e$). Dans le cas ou max ($L_{dcs-tr} = 0$ && $max(L_e) = 0$), CASIEV passe à l'état zone rouge.

3.3.3 Complexité et surcharge de la mémoire

Dans cette section, nous allons calculer la complexité et la surcharge de la mémoire associées à l'algorithme proposé.

Analyse de la complexité de la solution CASIEV

L'algorithme proposé consiste en deux tâches (3.8) : identifier le bon niveau de sécurité et appliquer les mécanismes de sécurité.

$$\begin{aligned} \textit{Complexité de l'algorithme} \;=\; & \textit{complexité de la sélection du niveau de sécurité } (SLS)+ \\ & \textit{complexité des mécanismes de sécurité} \end{aligned} \tag{3.8}$$

L'algorithme SLS se compose de trois algorithmes (adaptation à l'énergie, adaptation à la distance à la station de recharge, adaptation au trafic). Chaque algorithme prend O(n), où n est le nombre de niveaux de sécurité disponibles au choix. Les opérations prennent un temps constant. La complexité des mécanismes de sécurité peut être calculée comme la complexité des algorithmes de cryptographie O(m)+ la complexité des mécanismes d'authentification O(HMAC), où m est la taille du message en termes de nombre de blocs de données à chiffrer. Ainsi, la complexité temporelle globale de cet algorithme est calculée en (3.9).

$$3 \times O(n) + O(1) + O(m) + O(HMAC) = O(n) + O(m) \tag{3.9}$$

Surcharge de la mémoire

Considérons les caractéristiques du TelosB : CPU à 8 MHz, 10 Ko de RAM, 48 Ko de ROM, 1 Mo de mémoire flash [181, 182]. Les capteurs TelosB sont bien adaptés aux véhicules électriques car ils sont efficaces en termes de consommation d'énergie du CPU, à la fois à l'état actif et en veille comparé à d'autres types de capteurs. Considérons aussi que

la communication est permise par la technologie ZigBee. Le coût supplémentaire généré par la solution proposée est décrit par (3.10) :

$$\begin{aligned} Surcharge\ de\ l'algorithme\ =\ & surcharge\ du\ contexte\ + surcharge\ du\ SLS\ + \\ & surcharge\ application\ du\ niveau\ de\ sécurité \end{aligned} \tag{3.10}$$

Le contexte consomme 406 octets (47 octets (position du véhicule) + 4 octets (SOC) + 47 octets (position de la station de recharge), 4 octets (vitesse du véhicule) + 4 × (28 octets (en-tête ZigBee) + 40 (en-tête IPv6) + 8 (en-tête UDP)), soit environ 4 % de la mémoire vive disponible. En outre, l'algorithme de sélection du niveau de sécurité nécessite 24,5 octets de mémoire vive, soit environ 0,2 % de la mémoire disponible. Le surcroît de mémoire le plus important est généré par les mécanismes de sécurité (cryptographie, authentification). Le cryptage avec AES consomme environ 1,8 koctets de mémoire de données, soit 18 % de la RAM, et 9 koctets de mémoire de code, soit environ 19 % de la ROM disponible. L'authentification au moyen de la fonction HMAC nécessite 0,1 koctets, soit 1 % de la mémoire RAM disponible, et 11 koctets, soit environ 23 % de la mémoire ROM disponible. La consommation totale de mémoire de l'algorithme proposé est de 2,32 koctets de RAM et de 20 koctets de ROM, soit 22,3 % et 41,66 % de la mémoire disponible.

3.4 Validation formelle de CASIEV

Dans cette section, nous modélisons la solution CASIEV en utilisant l'outil AVISPA (Automated Validation of Internet Security Protocols and Applications) [183] et SPAN (Security Protocol Animator for AVISPA) [184] pour valider formellement les propriétés de sécurité. Dans ce paragraphe, nous allons présenter les outils AVISPA et procéder à la vérification formelle de CASIEV.

3.4.1 Les outils AVISPA

Dans la littérature, plusieurs outils sont utilisés pour la modélisation et la vérification formelle des systèmes et des protocoles de communication [183] tels que : Specification and Description Language (SDL), PROMELA/SPIN, AVISPA et SPAN. Automated Validation of Internet Security Protocols and Applications (AVISPA) est un outil de validation

et d'analyse automatique des protocoles de sécurité. Il permet de modéliser des protocoles à petite et moyenne échelle, ainsi que des protocoles de sécurité Internet à grande échelle. Le protocole de sécurité à analyser avec AVISPA est spécifié dans un langage appelé High Level Protocol Specification Language (HLPSL). C'est un langage de spécification modulaire basé sur la notion de rôles (participants) et de rôles composés (sessions, instances). Un rôle simple sert à décrire les actions d'un agent lors de l'exécution du protocole. Un rôle composé permet d'instancier plusieurs rôles simples afin de modéliser l'exécution du protocole entier.

Security animator for AVISPA (SPAN) est un outil graphique qui permet d'aider à la vérification et représentation graphique des spécifications HLPSL.

3.4.2 Vérification formelle de CASIEV

Pour la vérification du protocole de sécurité CASIEV, nous avons utilisé le back-end On-the-Fly Model Checker (OFMC) intégré à AVISPA. Ce back-end permet de vérifier si les agents légitimes peuvent exécuter le protocole spécifié en introduisant un intrus [184] . Dans notre travail, nous avons vérifié les propriétés de sécurité exigées pour CASIEV qui sont l'authentification et la confidentialité.

Spécification formelle

La spécification formelle définie deux rôles (roles) : ECU (Electric Control Unit) et S (Sensor). Ces deux rôles sont instanciés afin de spécifier CASIEV.

Les propriétés de sécurité validées pour la solution CASIEV sont : l'authentification et la confidentialité. L'authentification est spécifiée dans la partie buts (goals) de la spécification formelle pour assurer l'authentification des deux côtés de la communication (ECU et S). La confidentialité est décrite pour assurer la sécurité de l'échange et la construction de la clé. La figure 3.5 décrit la spécification.

Vérification Formelle Pour la vérification formelle de CASIEV, nous envisageons deux scénarios d'attaques. Le premier scénario représente une attaque d'écoute et le deuxième une attaque de Man In the Middle.

```
role session(ECU:agent,S:agent,SK:symmetric_key ,H: function)
def=
        local
                SND2,RCV2,SND1,RCV1:channel(dy)
        composition
                role_ECU(ECU,S,SK,H,SND2,RCV2) /\ role_A(ECU,S,SK,H,SND1,RCV1)
end role
goal
        authentication_on ECU
        authentication_on S
        secrecy_of SK


end goal
```

FIG. 3.5 : Spécification formelle de CASIEV

Scénario 1 : Attaque d'écoute

Le résultat de la vérification formelle de la solution de sécurité CASIEV, pour le cas où le niveau de sécurité est maximal (confidentialité et authentification), est représenté dans la figure 3.6 et montre que le système résiste à l'attaque d'écoute.

```
SUMMARY
 SAFE
DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
 /home/span/span/testsuite/results/CASIEV.if
GOAL
 as_specified
BACKEND
 OFMC
```

FIG. 3.6 : Résultats de la validation de CASIEV pour les niveaux de sécurité élevés

La figure 3.7 montre que le système est non sécurisé lorsqu'on envisage un niveau de sécurité bas (uniquement authentification) ou pas de sécurité du tout (détection d'une attaque d'écoute). En effet, dans les deux cas, le service de confidentialité n'est pas assuré.

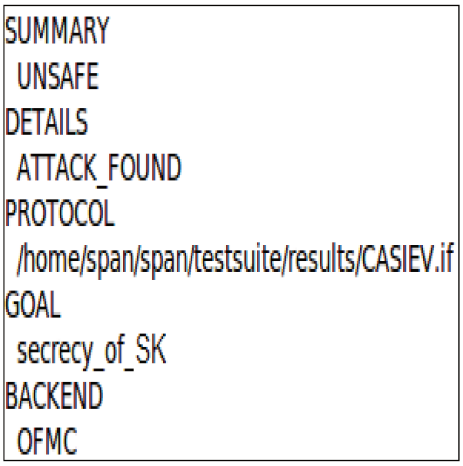


FIG. 3.7 : Résultats de la validation de CASIEV pour un niveau de sécurité bas ou pas de sécurité

Scenario 2: Attaque Man In the Middle

De même, nous analysons la résistance de la solution CASIEV à une attaque de type Man In The Middle. Nous introduisons un intrus actif jouant les rôles des agents ECU et Sensor (S). La description du rôle de l'environnement est donnée dans la figure 3.8 et permet de détecter l'attaque Man In the Middle quand elle existe. Un attaquant peut prendre le rôle d'un ECU ou d'un capteur (S).

```
role enviroment()
def=
   const ECU,S,i:agent,
   sk:secret_key
   h: function

        intruder_knowledge={ECU,i,S,sk,h}

        composition
                session(ECU,S,sk,h)
                /\ session(ECU,i,sk,h) intruder playing role of S
                /\ session(i,S,sk,h)intruder playing role of ECU
end role
```

FIG. 3.8 : Scénario d'une attaque Man In the Middle

Dans le cas où l'on utilise un niveau de sécurité élevé (authentification et confidentialité) ou bas (authentification uniquement), la figure 3.9 montre que CASIEV permet d'éviter l'attaque de type Man In the Middle. Cependant, pour un niveau de sécurité égal à zéro, le système n'est plus sécurisé.

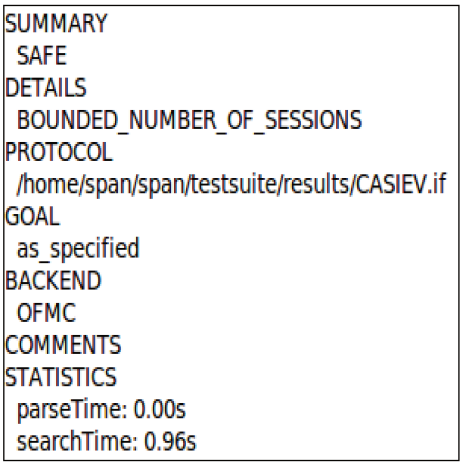


FIG. 3.9 : Résultats de l'analyse de l'attaque Man In the Middle pour les niveaux de sécurité supérieurs à zéro (scénarios 1 et 2)

3.5 Simulation

Nous avons mené des simulations pour évaluer les performances de l'architecture CASIEV en utilisant le simulateur OMNET++ [185] et la plate-forme INET qui fournit les couches TCP/IP [186]. OMNeT++ (Objective Modular Network Testbed in C++) est un simulateur à événements discrets basé sur le langage C++. Il est totalement programmable, paramétrable et modulaire. INET a ajouté une bibliothèque complète de normes utilisées dans un réseau Internet. Ce projet a été développé afin d'avoir une simulation réaliste. En outre, nous avons intégré la bibliothèque MiXim [102] qui implémente le protocole ZigBee sur le simulateur OMNET++.

3.5.1 Les critères de performances

Nous avons fixé les critères de performance suivants pour évaluer la solution CASIEV.
- Le temps total d'activation de la sécurité : $TVS = \sum_{i=0}^{n}(T_{sec}[i])$, où $T_{sec}[i]$ représente un intervalle de temps dans lequel le système de sécurité met en œuvre une stratégie de sécurité, avec k le nombre de changement du niveau de sécurité.
-La latence est un critère d'évaluation important puisque certaines applications du réseau IVN sont des applications temps réel. Il est important d'évaluer l'impact du déploiement de la solution CASIEV sur les latences requises par les applications IVN. La latence est calculée comme suit : temps de réception du message - temps d'émission du message.

3.5.2 Paramètres de simulation

Nous avons considéré un réseau de 120 capteurs uniformément répartis sur une zone de 1730*4084*1562 mm. Tous les nœuds sont authentifiés et seules les caméras, les LIDAR, les GPS et les capteurs de niveau de batterie offrent la confidentialité. La table 3.2 présente

TAB. 3.2 : Paramètres de simulation

Paramètres	Valeur
Nombre de capteurs	120
Model de Trafic	Single line
Vitesse	Traffic réel γ =10km/h, β=80km/h
Distance à la station de recharge	20km
capteurs	Capteurs critiques : 40 % including 2 cameras and LIDARs. Capteurs semi critique : 50% Capteurs de conforts : 10%
E_{th}	Capteur critique : 20 $\times$ $SOC/100$ Capteur semi critique : 25 $\times$ $SOC/100$ Capteur de confort : 30 $\times$ $SOC/100$
E_s	10%
Périodicité (Packet interval)	1 s
Taille des données	Lidar1: vlp16 (300000 points/ s) Lidar 2: vlp32 (600000 points/s) Camera : 4Camera axis-f44 (450000 b/s) Autres capteurs : [8..100] bytes/s
Technologies de communication	CAN/zigbee 250 kb/s, WIFI(802.11 ac (1 Gb/s))
SOC (State of Charge)	32%
Taille du HMAC	160 bits= 20 bytes
Application temps réel	Traction Control System (TCS) Latence : 100 ms

les paramètres de simulation.

3.5.3 Niveaux de sécurité

Les mécanismes de sécurité ont été évalués, dans de nombreuses études de recherche [28–30, 187], selon de nombreux critères tels que la consommation d'énergie, la robustesse et l'utilisation de la mémoire. Par exemple, dans [28, 29], seule la consommation d'énergie a été prise en compte. Cependant, dans [187], la consommation de mémoire a également été prise en compte. Dans [30], la mémoire et la robustesse ont été traitées comme des critères d'évaluation des algorithmes de chiffrement. Selon [28, 30], la consommation d'énergie des mécanismes de sécurité est proportionnelle à leur robustesse. Par exemple, AES est plus robuste que DES [30]. Par conséquent, le chiffrement utilisant AES consomme plus d'énergie que DES [28]. Nous considérons les quatre critères mentionnés ci-dessus (robustesse, capacité de mémoire et de traitement ainsi que la consommation d'énergie) pour classer les mécanismes de sécurité en cinq niveaux de sécurité (voir table 3.3).

Tab. 3.3 : Les niveaux de sécurité

Les niveaux de sécurité (l)	0	1	2	3	4
Mécanismes d'authentification	—	HMAC	HMAC	HMAC	HMAC
Mécanismes de chiffrement	—	—	Skipjack	XXTEA	AES_128

La figure 3.10 montre que les quatre niveaux de sécurité varient considérablement en termes de consommation d'énergie.

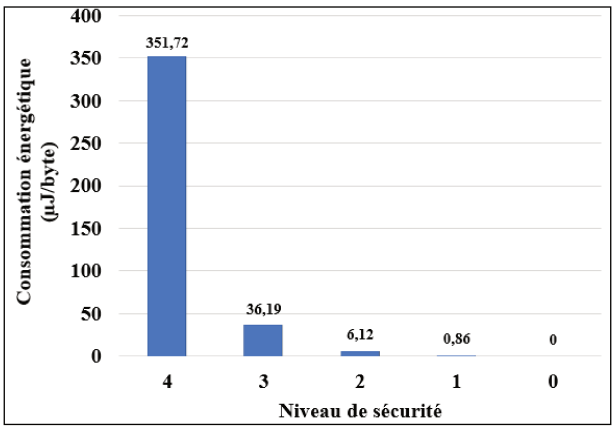


Fig. 3.10 : Consommation énergétique des niveaux de sécurité

3.5.4 Résultats de la simulation

Les relevés des niveaux d'énergie sont issus d'expériences réelles réalisées à Rouen avec un véhicule électrique Renault Zoe. La figure 3.11 montre la consommation d'énergie du module de conduite. A t=0, nous considérons qu'une charge de batterie de 32% donne des résultats pertinents puisque notre solution adapte le niveau de sécurité lorsque le niveau de la batterie est inférieur à E_{th}. Une légère augmentation du niveau de la batterie est observée pendant le trajet, résultant d'événements de récupération d'énergie lors du freinage.

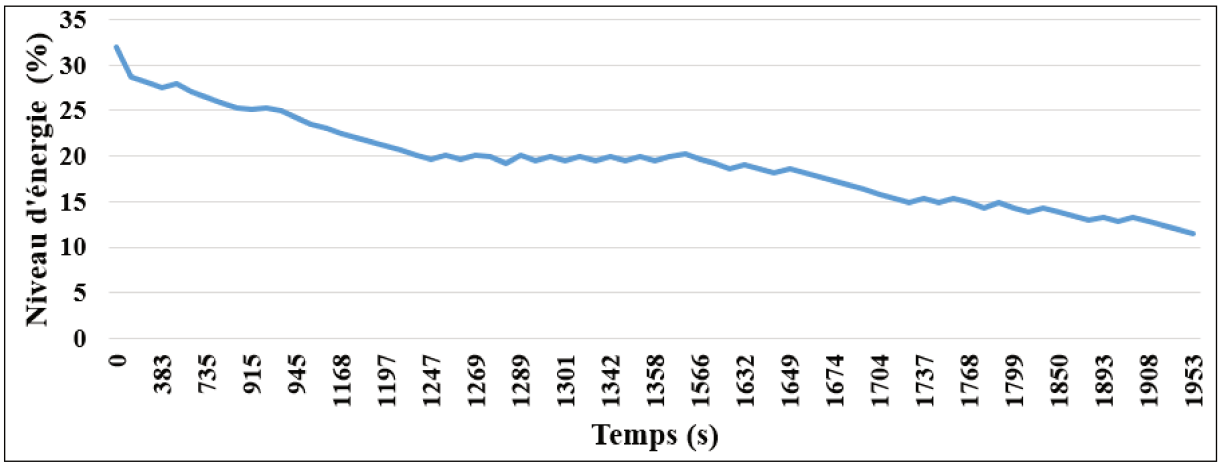


FIG. 3.11 : L'énergie consommée par le module de conduite

La figure 3.12 montre l'adaptation de la sécurité en fonction de l'énergie pour plusieurs types de capteurs (capteurs critiques, semi-critiques et de confort). Le niveau de sécurité pour les capteurs critiques commence au niveau 4 et diminue jusqu'au niveau zéro après 21 minutes (niveau d'énergie< E_{th_c}). Cependant, on peut observer une augmentation de la robustesse de la sécurité (niveau 2) à 1290s lorsque le véhicule récupère de l'énergie (voir figure 3.10). Le même scénario peut être observé dans l'intervalle de temps entre 1370s et 1485s, où le niveau de sécurité augmente pour atteindre le niveau 3 lorsque tous les autres types de capteurs passent en mode non sécurisé (60% des capteurs). Comme le seuil des capteurs semi-critiques est d'environ 25% du SOC, ils commencent l'adaptation de la sécurité avant les capteurs critiques ($E_{th\_c} < E_{th\_sc}$). Cependant, après 15 minutes, aucune augmentation du niveau de sécurité n'est observée car la charge de la batterie n'atteint plus jamais 25% du SoC. Les capteurs de confort commencent au niveau 1 car ils sont seulement authentifiés. Selon la stratégie de sécurité proposée, un capteur de

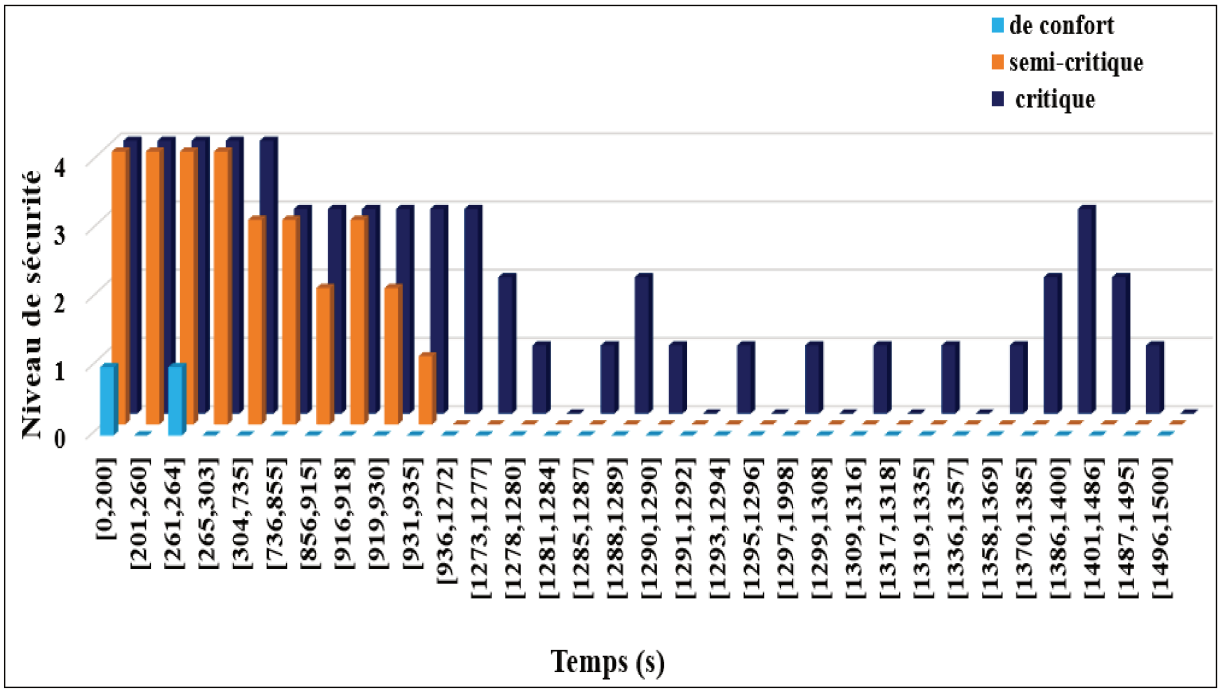


FIG. 3.12 : Adaptation de la sécurité des capteurs par rapport à l'énergie

confort passe en mode non sécurisé bien avant le capteur critique et semi-critique. En effet, leur seuil est le plus élevé ($E_{th\_co} = 30\%$).

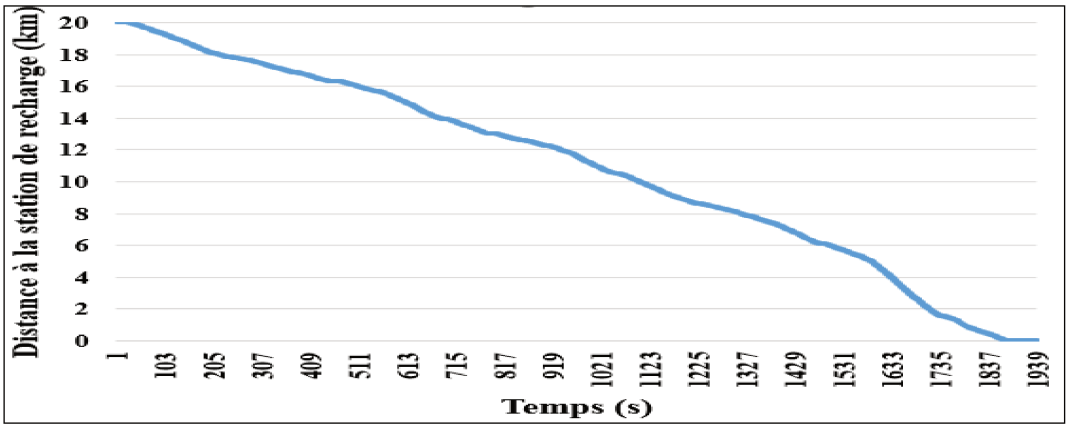


FIG. 3.13 : Distance par rapport à la borne de recharge

Les figures 3.13 et 3.14 présentent la distance jusqu'à la station de recharge ainsi que la vitesse du véhicule.

La figure 3.15 montre l'impact du trafic et de la distance à la station de recharge sur l'adaptation de la sécurité. Nous supposons que l'énergie restante permet au véhicule d'atteindre la station de recharge. Nous observons que le niveau de sécurité passe fréquemment du niveau 3 au niveau 0, pour les deux types de capteurs, car il dépend

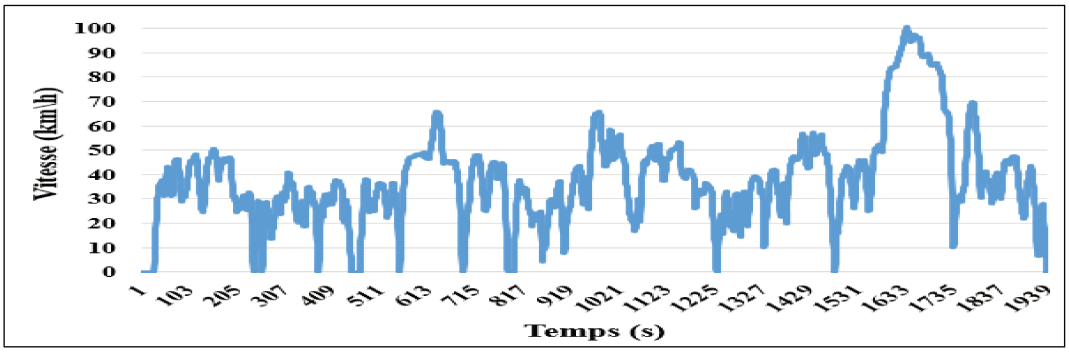


FIG. 3.14 : Vitesse du véhicule

de l'état du trafic. Par exemple, dans l'intervalle [447, 469], on observe que le niveau de sécurité passe à zéro puisque le trafic est élevé (voir figure 3.13).

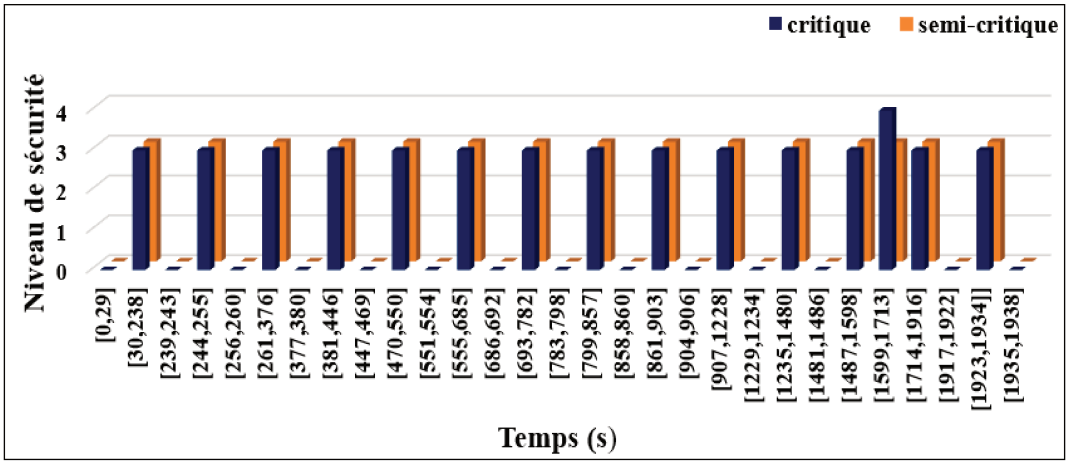


FIG. 3.15 : Adaptation de la sécurité par rapport à la distance à la borne de recharge et le trafic

La figure 3.16 montre l'adaptation de sécurité des capteurs critiques et sous-critiques en fonction du contexte global. Le niveau de sécurité des capteurs critiques diminue jusqu'à zéro pour la première fois après 32 minutes. Nous remarquons qu'un capteur critique adapte le niveau de sécurité en fonction de l'énergie dans l'intervalle de temps [0-1272] et [1481-1486] (voir figures 3.12 et 3.16). Dans les intervalles de temps [1273 - 1480] et [1487-1938], les niveaux de sécurité obtenu sont différents de ceux issus de l'adaptation à l'énergie (voir figure 3.12). Ainsi, le capteur adapte la sécurité en fonction de la distance à la station de recharge et du trafic Dans l'intervalle [1626 -1704] , on observe une augmentation significative du niveau de sécurité (voir figure 3.15) puisque le véhicule a assez de charge pour atteindre la station de charge disponible la plus proche (D>DCS).

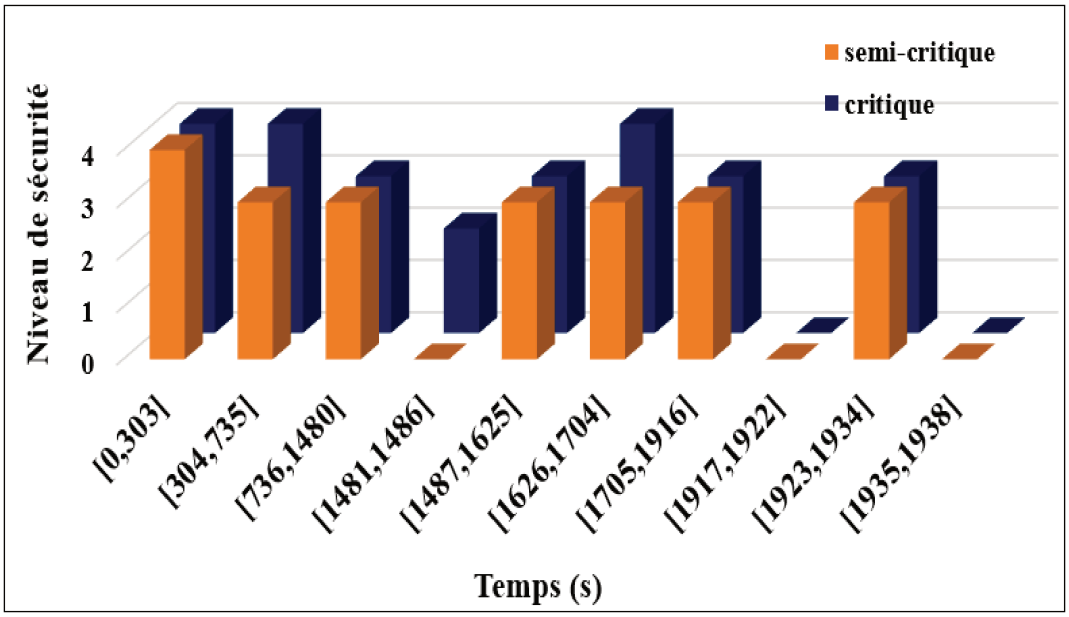


FIG. 3.16 : Adaptation de la sécurité par rapport au contexte global

Pour le capteur semi-critique, le niveau de sécurité diminue à zéro après 25 minutes. Dans les intervalles de temps [0-855] et [916-918], un capteur semi-critique adapte le niveau de sécurité en fonction du SOC (voir figure 3.12). Sinon, il adapte la sécurité en fonction du contexte (voir figure 3.15).

La solution de sécurité adaptée au contexte (CASIEV) est comparée à deux stratégies, à savoir la stratégie de sécurité statique (solution logicielle : voir section 2.3.4) qui met

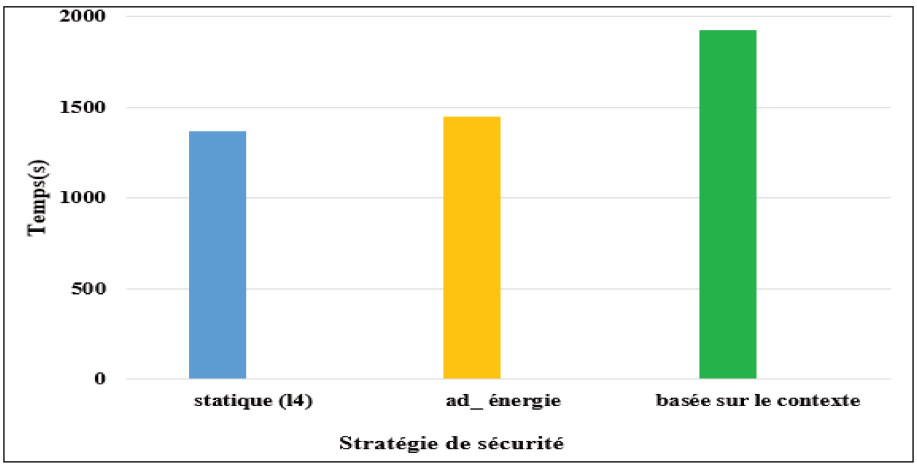


FIG. 3.17 : Temps total d'activation de la sécurité

en œuvre la stratégie de sécurité la plus élevée (l4) tout au long du parcours et la stratégie d'adaptation à l'énergie qui adapte la sécurité uniquement en fonction de l'énergie

restante. Dans la figure 3.17, on remarque que le temps total d'activation de la sécurité de CASIEV est plus important que les deux autres stratégies.

Nous avons effectué une simulation pour évaluer l'impact de CASIEV sur la latence exigée par les applications automobiles temps réel. Nous avons considéré l'application TCS (Traction Control System) [188]. Un TCS peut aider à limiter la rotation des roues et à améliorer la stabilité du véhicule, en particulier sur une route glissante ou dans les virages où la surface est cahoteuse et peu stable, probablement en raison des conditions météorologiques (pluie, glace ou neige). Le TCS est composé de deux unités de commande électrique (ECU) : l'ECU hôte et l'ECU du contrôleur de papillon. L'ECU hôte reçoit des signaux de capteurs tels que les capteurs de vitesse des roues, le capteur d'accélération longitudinale, le capteur de position de la pédale d'accélérateur et le capteur de position du papillon des gaz du moteur. De plus, elle envoie les signaux de commande à une ECU de commande des gaz afin d'éviter le patinage excessif des roues motrices.

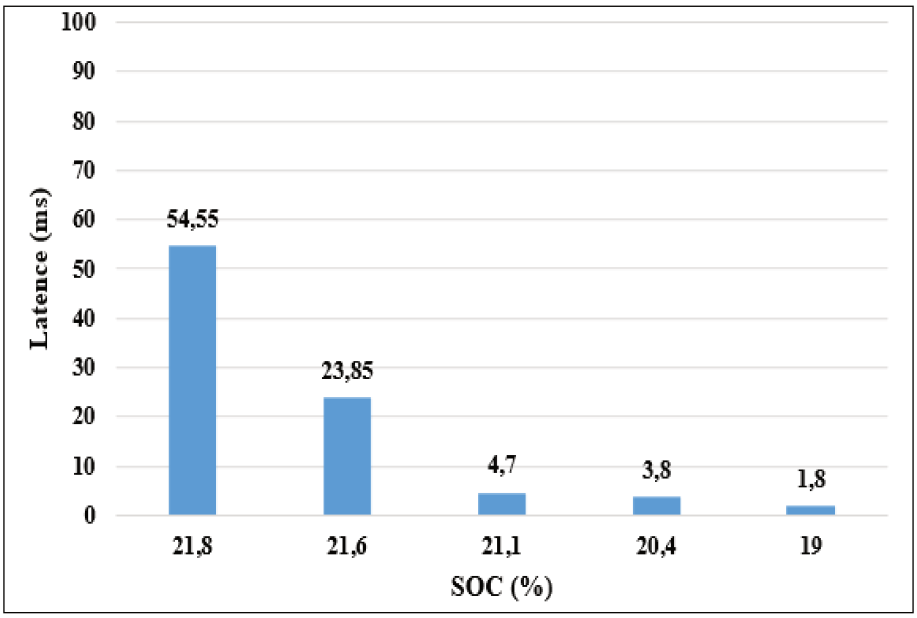


Fig. 3.18 : Latence pour l'application TCS

La figure 3.18 présente la latence en fonction de l'état de charge de la batterie. Dans ce scénario, nous calculons la latence pour la stratégie d'adaptation à l'énergie. La latence de l'application de contrôle de la traction varie entre 54,55 ms et 1,8 ms car l'approche proposée adapte le niveau de sécurité en fonction du SOC. Elle atteint 54,55 ms lorsque le SOC (21,8%) permet d'utiliser le niveau de sécurité maximal niveau 4. De plus, la latence diminue à 4,7 ms lorsque le SOC permet d'utiliser le niveau 2 et décroit à 1,8

ms si aucune sécurité n'est assurée. Par conséquent, la latence augmente en fonction du niveau de sécurité. Ces délais sont bien inférieurs à la latence recommandée (100 ms).

3.6 Conclusion

Dans ce chapitre, nous avons présenté les méthodes de modélisation de la sécurité adaptative et nous avons choisi la modélisation par scénario pour CASIEV. De même, nous avons proposé une stratégie de sécurité ou les capteurs passe d'un niveau de sécurité à autre en fonction du contexte dynamique qui est composé du niveau de la batterie, du type de capteur, de la mémoire et de la capacité de traitement du capteur, de la distance par rapport aux stations de recharge disponibles les plus proches et du trafic. Les niveaux de sécurité sont définis en tenant compte de la robustesse, de l'énergie et de la consommation de mémoire/traitement des mécanismes de sécurité. Dans la stratégie de sécurité proposée, le capteur passe toujours au niveau de sécurité le plus élevé autorisé par le contexte. Les simulations ont montré que la sécurité est assurée lorsque le niveau de la batterie est critique dans le cas où le trafic est faible/moyen et que l'énergie restante permet d'atteindre la station de recharge disponible la plus proche. Dans le cas contraire, les résultats ont montré une diminution progressive des niveaux de sécurité lorsque l'énergie est inférieure à un seuil, que le trafic est intense et que le véhicule ne peut pas atteindre la station de recharge. Cependant, nous remarquant un gaspiage d'énergie lorsque le risque d'attaque est faible. Ainsi, dans le chapitre 4, nous portant des amélioration à CASIEV en tenant compte du niveau de risque.

Chapitre 4

Solution de sécurité contextuelle basée sur le risque et la confiance

4.1 Introduction

Afin d'améliorer le modèle CASIEV, nous allons exploiter les deux concepts risque et confiance dans ce risque, pour proposer le modèle RICAV (Risk-based Context-Aware security for the Intra-Vehicular network). CASIEV vise à utiliser le niveau de sécurité le plus robuste autorisé par le contexte et qui sera consommateur d'énergie. Cependant, le risque d'attaques est variable tout au long du trajet. Il peut être faible, moyen ou élevé. Pour cette raison, RICAV intègre le risque et la confiance afin d'économiser l'énergie tout en augmentant le temps d'activation de la sécurité et la robustesse du système. Ainsi, dans ce chapitre, nous décrivons les deux paradigmes risque et confiance. Ensuite, nous présentons la modélisation de RICAV. Enfin, nous procédons à l'évaluation de RICAV et comparons ses performances avec celles de CASIEV en termes de d'activation de la sécurité et consommation énergétique.

4.2 Risque et confiance

Dans cette section, nous allons présenter les concepts de risque et confiance. De même, nous allons décrire les travaux d'évaluation du risque et de la confiance.

4.2.1 Risque et évaluation

Dans la littérature, l'évaluation du risque, dans le secteur du transport, a attiré l'attention des chercheurs et des organismes de normalisation qui ont publié plusieurs normes. L'Institut national des normes et de la technologie (NIST) [7] a défini le risque comme suit :

$$\text{Risque} = \text{Probabilité de la menace} \times \text{Impact}$$

La probabilité de la menace constitue l'estimation de la faisabilité de l'attaque (probabilité de succès). L'impact (également appelé sévérité) présente l'évaluation du niveau et de l'intensité du risque. Il fournit une mesure des impacts de la menace (vulnérabilité), qu'ils soient directs ou indirects. Selon NIST, le risque peut être très faible, faible, moyen, élevé et très élevé. La méthode d'évaluation des risques du NIST [7] comprend la

caractérisation du système, les sources et les scénarios d'attaques, l'identification des vulnérabilités du système, l'évaluation des contre-mesures de sécurité et la détermination du risque (matrice impact-probabilité de succès). La figure 4.1 décrit l'évaluation du risque proposée par le NIST.

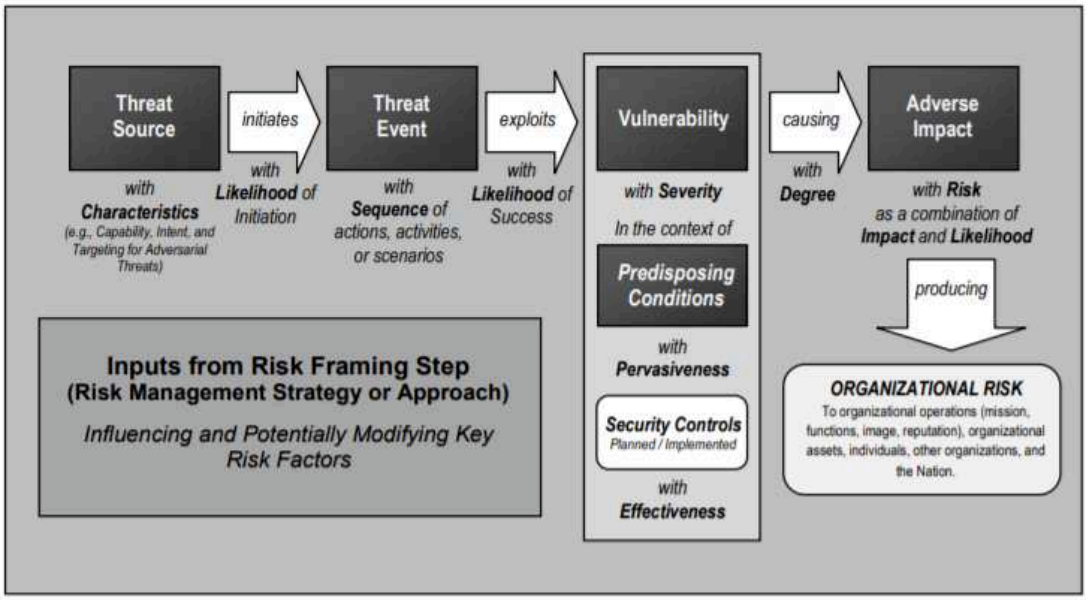


Fig. 4.1 : Modèle de l'évaluation de risque de NIST [7].

L'ETSI TVRA [33] (Threat, Vulnerability and Risk Analysis) étudie le risque dans le contexte du réseau de véhicules. Elle comporte six étapes : identifier les objectifs et les exigences de sécurité, réaliser un inventaire des actifs du système, classer les vulnérabilités et les menaces, quantifier la probabilité et l'impact des attaques, déterminer les risques encourus et spécifier les exigences de sécurité. SecRAM [189] représente la méthode d'évaluation du risque basée sur la norme ISO 27005, Cette norme est développée pour la gestion du trafic aérien. Elle associe une valeur entre 1 et 5 à l'impact de la menace sur les services de sécurité (Disponibilité (Av), Authentification (Au), Confidentialité (C), Intégrité (I) et Non-répudiation (Nr)). En outre, elle considère le service ayant l'impact le plus élevé comme l'impact global de la menace. De nombreux travaux dans la littérature ont étudié l'évaluation des risques dans le contexte du réseau intra-véhicule. Dans [34], les auteurs ont adapté [7] dans le contexte d'un réseau intra-véhiculaire. L'objectif de cette méthodologie est d'explorer les menaces ciblant le réseau intra-véhiculaire et de catégoriser les impacts de ces menaces dans des groupes de risques. Par exemple, ils considèrent la sécurité du conducteur et les impacts comportementaux comme un risque très élevé.

Dans [35], les auteurs se basent sur la définition du risque proposée par le NIST mais utilisent de nouveaux mécanismes pour identifier la probabilité et la valeur de l'impact. La probabilité est basée sur le contexte du véhicule (voie, route, trafic, météo, vitesse et temps) et sur l'attitude du conducteur. L'impact est calculé en fonction du type d'application ((élevé pour les applications de sécurité routière). Le projet EVITA [23, 190] (Esafety Vehicle Intrusion Protected Applications) a proposé une évaluation du risque pour le réseau intra-véhicule. EVITA calcule la gravité de l'attaque en fonction de quatre facteurs : La sécurité, la vie privée des conducteurs, les performances opérationnelles et les pertes financières. La probabilité d'une menace est considérée en termes d'expertise, de connaissance de la cible, de fenêtre d'opportunité (y compris le temps requis). Dans [36], les auteurs ont proposé un modèle de confiance basé sur le chef de groupe dans un réseau VANET. De même, ils ont adopté une méthodologie d'évaluation de risque basé sur le SecRAM [189] et l'ETSI TVRA [33] afin de détecter les problèmes de sécurité du modèle de confiance proposé.

4.2.2 Confiance

Le concept de confiance joue un rôle important dans la définition et l'application des politiques de sécurité, car le fait qu'une entité soit autorisée à accéder à des informations privées ou à les manipuler dépend directement de la confiance que la source d'information lui accorde [191].

Toute approche visant à assurer la sécurité d'un tel système doit donc prendre en compte l'établissement et la mise à jour de la confiance entre les entités du système [192]. Pour appliquer une approche basée sur le risque afin de renforcer la sécurité dans un système décentralisé, il est donc nécessaire que la confiance dans l'entité responsable de la quantification du risque soit prise en compte dans la sécurité.

la confiance est dynamique et évolue dans le temps [193]. Par conséquent, un système qui vise à appliquer des politiques basées sur la confiance doit s'adapter pour gérer les incertitudes qui découlent de la nature dynamique de la confiance. Les changements de la valeur de la confiance entre les entités du système entraînent des changements dans leur sécurité, et donc le système doit adapter ses capacités d'application de la sécurité en conséquence, s'il aspire à appliquer les politiques de sécurité actualisées de ses entités.

Dans notre cas, la dynamicité de la confiance ne constitue pas une contrainte puisque notre système s'adapte à son contexte.

4.3 Etat de l'art des solutions de sécurité basées sur le risque

Plusieurs travaux [194, 195] se sont basés sur le risque pour définir des systèmes de contrôle d'accès. D'autres travaux ont proposé des solutions de sécurité adaptative pour l'IoT.

Il existe une variété de méthodes pour construire un modèle basé sur le risque pour le contrôle d'accès. Ces méthodes présentent certaines caractéristiques communes. La figure 4.2 décrit les principaux éléments et le déroulement d'un modèle basé sur le risque pour le contrôle d'accès.

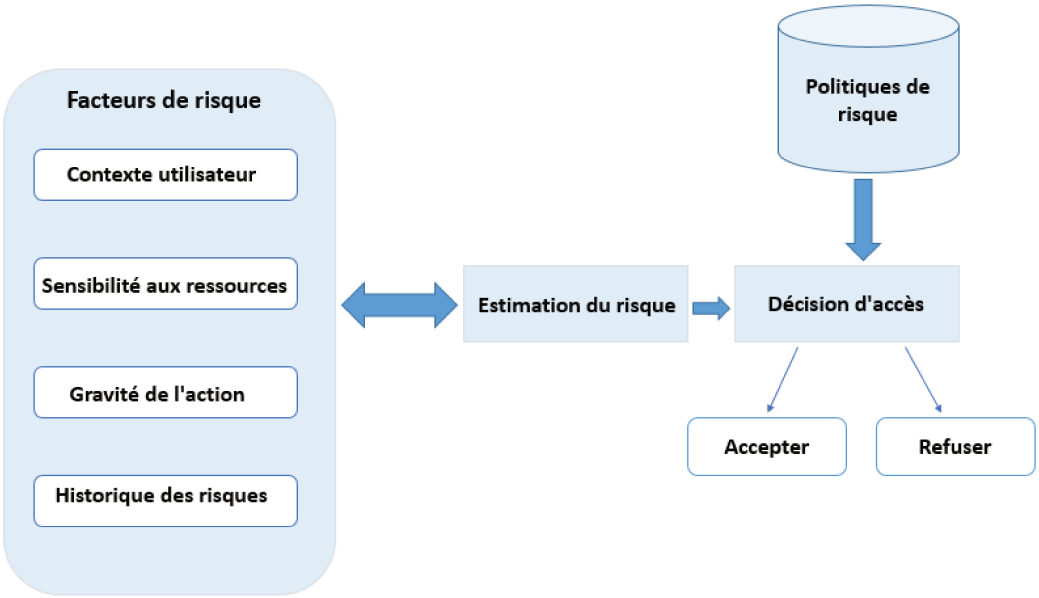


FIG. 4.2 : Modèle d'accès basé sur le risque.

L'utilisateur tente d'accéder aux ressources du système en envoyant une demande d'accès au gestionnaire de contrôle d'accès. La demande d'accès est ensuite traitée, et le module d'estimation du risque utilise les informations disponibles sur les caractéristiques du risque pour mesurer la valeur du risque lié à la demande d'accès. Ensuite, la valeur de risque estimée est comparée aux politiques de risque qui sont spécifiées par les administrateurs du système de sécurité. Si la valeur de risque estimée est inférieure à la valeur

seuil définie au niveau des politiques de risque, l'accès est accordé et l'obligation sera appliquée, sinon, l'accès sera refusé [196]. Dans [197], les auteurs ont proposé un modèle d'accès adaptatif basé sur le risque pour l'IoT. Le modèle comporte quatre entrées : le contexte de l'utilisateur, la sensibilité des ressources, la gravité de l'action et l'historique des risques. Ces facteurs de risque sont utilisés pour estimer le risque associé à chaque demande d'accès. La valeur du risque estimée est ensuite comparée aux politiques de risque pour prendre la décision d'accès. Pour fournir les fonctions adaptatives, le comportement de l'utilisateur sera surveillé pour détecter toute action anormale de sa part pendant la session d'accès. Ce modèle fournira un niveau de sécurité approprié tout en assurant la flexibilité et l'évolutivité du système IoT.

Gupta et al.[198] ont proposé un système d'authentification biométrique multimodal, basé sur le risque, appelé DriverAuth. Ce système exploite le visage, la voix et la lecture optique pour vérifier l'identité des conducteurs enregistrés pour garantir la sûreté et la sécurité des clients utilisant les transports à la demande et le covoiturage. Dans [199], Hintze et al. considèrent la localisation géographique comme un facteur pour évaluer le risque et prendre une décision d'authentification pour les appareils mobiles. Leur méthode utilise le risque basé sur l'emplacement en combinaison avec la biométrie multimodale pour ajuster le niveau d'authentification nécessaire à un risque donné.

De même, plusieurs travaux [200–203] ont proposé des solutions de sécurité adaptatives, basées sur le risque, pour l'IoT. Dans [200], les auteurs ont proposé une solution de sécurité pour le WBAN qui maintient le compromis entre la sécurité et les performances correspondantes. Le choix du modèle de sécurité le plus approprié se fait par une approche de jeu stochastique conçue pour évaluer et calculer les coûts des risques afin de mettre en œuvre la contremesure de sécurité appropriée. Savola et al.[201] ont discuté des besoins en matière de gestion adaptative de la sécurité basée sur des mesures et des solutions initiales pour les applications E-health IoT, en particulier pour le traitement des maladies chroniques et le bien-être des personnes âgées. Ils ont affirmé que la gestion adaptative de la sécurité est nécessaire, notamment pour définir les exigences de sécurité suffisantes et pour appliquer les contrôles de sécurité adéquats face à l'évolution des risques de sécurité et du contexte d'utilisation, et que la prise de décision adaptative éclairée en matière de sécurité repose sur des preuves adéquates de l'efficacité, de l'exactitude et de l'efficience

de la sécurité offertes par les mesures de sécurité.

Dans [202], les auteurs ont présenté un cadre de sécurité adaptatif de haut niveau basé sur le risque pour les applications E-health. Le cadre décrit comment les méthodes et mécanismes de sécurité doivent adapter leurs décisions de sécurité en fonction des estimations et prédictions de risques en intégrant des modèles d'évaluation pratiques et systématiques utilisant des mesures de sécurité pour valider l'adaptation. Dans [203], il ont proposé un nouveau modèle d'authentification adaptatif, basé sur le risque, pour les applications Smart Home. Le modèle utilise un algorithme d'apprentissage automatique Naïve Bayes pour classifier la variation des caractéristiques du canal entre les nœuds de capteurs et leur passerelle. En fonction de la variation observée, le modèle évalue le risque pour déterminer la probabilité que le dispositif en question soit compromis. Sur la base du score de risque obtenu, le modèle sélectionne une décision d'authentification adéquate.

À notre connaissance, il n'existe aucun travail qui considère le risque dans le cadre des réseaux véhiculaires. Dans les travaux [200–203], les auteurs ont proposé des solutions de sécurité basées sur le risque. Cependant, ces travaux n'ont pas pris on compte les critères consommation d'énergie et la confiance en ce risque. RICAV va prendre en considération le risque, la confiance en ce risque et le contexte énergétique du véhicule électrique afin de mettre en place la stratégie de sécurité adéquate.

4.4 Solution de sécurité basée sur le contexte et le risque pour le réseau Intra-véhiculaire : RICAV

Le réseau intra-véhiculaire est un réseau complexe, composé de capteurs, calculateurs et micrologiciels, qui peut être vulnérable à de nombreux types d'attaques. Le système RICAV, que nous proposons, se base sur trois facteurs (contexte, risque et confiance) afin de minimiser la consommation d'énergie de la solution de sécurité tout en assurant la sécurité des communications du réseau intra-véhiculaire le plus longtemps possible pendant la mission. Dans ce paragraphe, nous présentons l'architecture de RICAV et sa modélisation en utilisant la théorie des jeux.

4.4.1 Architecture de RICAV

La figure 4.3 présente l'architecture de RICAV. Elle est composée de deux systèmes : CASIEV (Context-Aware Security for the Intra-Electric Vehicle) [31] et ASR (Adaptive Security based on the Risk). CASIEV adapte la sécurité du réseau interne de capteurs du véhicule en fonction du contexte dynamique du véhicule électrique. Nous avons défini le contexte comme étant l'état de charge (SoC), la station de recharge disponible la plus proche, les ressources des capteurs (mémoire et traitement) et les conditions de circulation. CASIEV applique le niveau de sécurité élevé autorisé par le contexte sans tenir compte de la probabilité du risque. Le module ASR choisit le niveau de sécurité adéquat en fonction du risque afin d'améliorer le processus d'économie d'énergie. Si le risque est faible, il n'est pas nécessaire de demander un niveau de sécurité élevé qui sont énergivore.

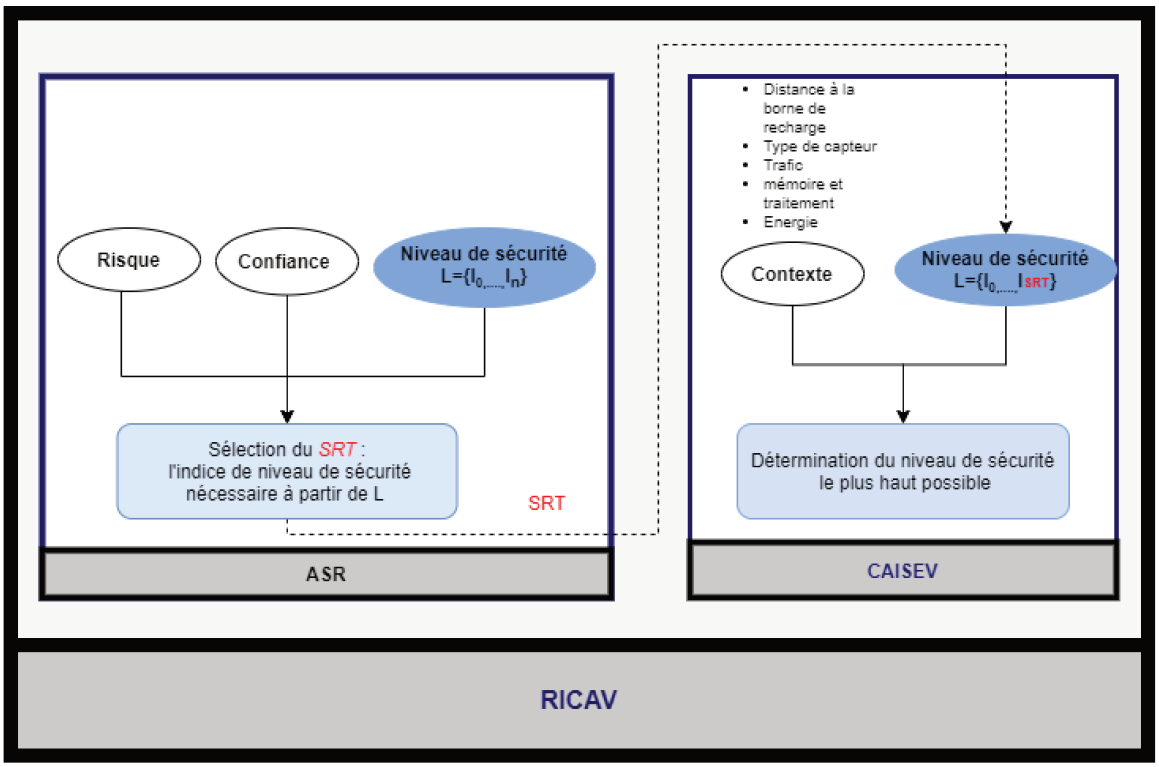


FIG. 4.3 : Architecture de RICAV

4.4.2 Quelle modélisation pour RICAV ?

Dans cette section, nous allons présenter le modèle utilisé pour modéliser RICAV.

Choix du modèle

Dans RICAV, nous sommes confrontés à un problème d'optimisation multi-objectifs puisque nous devons veiller à l'optimisation simultanée de plusieurs fonctions objectives (préservation de la sécurité et optimisation de l'énergie). Dans la littérature, de nombreuses techniques peuvent être utilisées pour résoudre ce problème, telles que la méthode de la somme pondérée (Weighted-sum method), la méthode des contraintes (e-constraints Method), la programmation multi-niveaux (Multi-level Programming), la programmation par objectifs (Goal Programming), l'algorithme évolutif (Evolutionary Algorithm (Genetic Algorithm, Differential Evolution)) et la théorie des jeux (game theory) [204]. Dans [205], les auteurs ont montré que la théorie des jeux surpasse de nombreux algorithmes multi-objectifs et métaheuristiques bien connus en termes de qualité, de stabilité, de vitesse de convergence et de durée d'exécution. Dans [163, 206], les auteurs montrent que la théorie des jeux permet le compromis entre des objectifs contradictoires. En outre, la théorie des jeux permet d'analyser de nombreux scénarios avant de définir les actions appropriées. Elle peut modéliser des scénarios dans lesquels il n'y a pas d'entité centralisée ayant une image complète des conditions du réseau ce qui représente notre cas [52]). En effet, le système de sécurité ne dispose d'aucune information sur le SoC (State of Charge) de la batterie et vice versa.

Dans [207], les auteurs ont proposé un modèle de théorie des jeux pour une sécurité adaptative de e-Health préservant l'authentification des entités intelligentes. Les auteurs ont fourni un modèle mathématique, s'appuyant sur la théorie des jeux de Markov, pour présenter l'e-Health dans un contexte dynamique. Ce modèle est basé sur un ensemble de stratégies pour concevoir le modèle du jeu et utilise quatre paramètres de base pour représenter le contexte (mémoire, canal de communication, modèle d'épuisement de l'énergie et modèle de menace). Dans [208], les auteurs ont développé un modèle de sécurité adaptative s'appuyant sur la chaîne de Markov pour systèmes d'information en réseau. Ce travail est basé sur deux chaînes de Markov. La première chaîne a été utilisée pour modéliser la propagation des menaces dans le réseau et le risque quantifié. La seconde a permis d'adapter la sécurité du système en fonction du risque quantifié.

Théorie des jeux

Dans la théorie des jeux, les quatre notions suivantes sont des éléments de base pour la description d'un jeu [204, 206] :

- Les joueurs : Les entités impliquées dans un jeu.
- Actions : À chaque mouvement d'un joueur, celui-ci effectue une action.
- Gain : Après que tous les joueurs aient effectué des actions dans le jeu, chacun d'entre eux obtiendra un revenu négatif ou positif. Le rendement de chaque joueur correspond à son gain.
- Stratégies : La stratégie d'un joueur est son plan d'action qui spécifie l'action à entreprendre en fonction de sa connaissance de l'historique des actions. Les stratégies peuvent être pures ou mixtes.

En partant de l'hypothèse que les joueurs sont rationnels dans la théorie des jeux, les joueurs choisiront des stratégies visant à maximiser leurs gains lorsqu'ils réagissent aux stratégies des autres joueurs. Cette hypothèse conduit au concept d'équilibre dans un jeu, qui peut être considéré comme la solution d'un jeu.

Un équilibre dans un jeu est une combinaison des stratégies des joueurs de sorte que la stratégie de chaque joueur soit la meilleure réponse aux stratégies des autres joueurs. "Meilleure" signifie que la stratégie conduit à un gain maximal compte tenu des stratégies des autres joueurs. Un équilibre de Nash [204, 206] est un type d'équilibre qui peut être appliqué pour résoudre la solution d'un jeu.

On distingue deux types de jeux : coopératifs et non coopératifs. Dans les jeux non coopératifs, chaque joueur choisit des stratégies sans coordination avec les autres. Les entités interagissent de manière compétitive. En revanche, dans un jeu coopératif, les joueurs tentent de parvenir à un accord de manière coopérative, et les joueurs ont le choix de négocier entre eux afin d'obtenir un bénéfice maximal, supérieur à celui qu'ils auraient pu obtenir en jouant le jeu sans coopération [204, 206] . Les entités interagissent de manière coopérative. De même, ces deux types de jeux peuvent être classé suivant trois aspects. La première méthode de classification consiste à déterminer si le jeu comporte une ou plusieurs étapes.

Le jeu statique est un jeu à une étape dans lequel les joueurs effectuent des actions en même temps. Un jeu dynamique est un jeu composé de plusieurs étapes ou mouvements. Le nombre d'étapes peut être fini ou infini [206] . La deuxième façon de classer les jeux est basée sur la présence ou non d'une information parfaite. Dans un jeu à information parfaite, chaque joueur connaît toutes les actions précédentes des joueurs lorsqu'il joue son coup. Un exemple de ce type de jeu est le jeu d'échecs. Dans un jeu à information imparfaite, au moins un joueur ne connaît pas toutes les actions précédentes lorsqu'il joue son coup. La troisième façon de classer les jeux est basée sur le fait de savoir si le jeu est à information complète ou non. Dans un jeu à information complète, chaque joueur du jeu connaît les fonctions de gain de tous les joueurs. Dans un jeu à information incomplète, au moins un des joueurs ne connaît pas les fonctions de gain de tous les joueurs.

4.4.3 Modélisation de RICAV en se basant sur la théorie des Jeux

Dans RICAV, les joueurs sont en concurrence pour les ressources limitées du réseau (dans notre cas : l'énergie). Dans cette section, nous présenterons les hypothèses, la spécification du jeu, l'arbre de jeu, l'équilibre de Nash et le modèle comportemental du système.

Hypothèses

Nous supposons que :

- Le jeu proposé est un jeu dynamique non coopératif avec des informations incomplètes dans lequel deux joueurs sont en compétition l'un avec l'autre. Le jeu est dynamique car nous considérons un contexte véhiculaire dynamique (contexte énergétique dynamique, risque et confiance). Les joueurs n'ont pas d'informations les uns par rapport aux autres mais ils doivent identifier leurs choix et donc, prévoir leurs comportements.
- Le jeu est séquentiel dans lequel les joueurs alternent les tours. Le système de sécurité joue sa stratégie et le système énergétique réagit à son tour.

Nous considérons un risque faible (regroupe le risque faible et très faible), moyen et élevé (regroupe le risque élevé et très élevé).

Spécification du jeu

Le jeu G est défini comme un triplet (P, S, U), où P est l'ensemble des joueurs, S est l'ensemble des stratégies et U est l'ensemble des fonctions de gain [206]. Dans la stratégie proposée, nous considérons deux joueurs : le système de sécurité (joueur 1) et le système de gestion de l'énergie (joueur 2). Le système de gestion de l'énergie représente le joueur clé du jeu. Pour chaque joueur, nous allons décrire ses stratégies, sa fonction d'utilité et ses gains. Le système de sécurité adapte le niveau de sécurité des capteurs en fonction du risque identifié et de la confiance en ce risque. Le système de gestion de l'énergie vise à optimiser la consommation d'énergie du réseau intra-véhiculaire en fonction du contexte. Dans cette section, nous commençons par décrire le jeu du joueur 1. Ensuite, nous décrivons le jeu du joueur 2.
Les joueurs : P= {système de sécurité, système de gestion de l'énergie}.

Le table 4.1 présente les paramètres du jeu et les variables de décision qui seront utilisés par la suite.

Le joueur système de sécurité

Le niveau de sécurité dépend du niveau de risque et de sa valeur de la confiance.La valeur de la confiance varie entre 1 et 10, ou une confiance égal à 1 représente la confiance la plus faible et une confiance égal à 10 représente la confiance la plus élevé.

Soit $S_{systéme\ de\ sécurité} = \mathrm{l}_i$, $0 \preceq i \preceq N$ l'ensemble des stratégies du système de sécurité.

Utilité du joueur 1 : maximiser la robustesse du système de sécurité tout en minimisant les frais généraux (traitement, mémoire, délai). La robustesse d'un réseau est évaluée en fonction du niveau de résistance aux attaques pour la stratégie de sécurité. Le système de sécurité adapte le niveau de sécurité en fonction de la valeur du risque r et de la confiance T.

$$S_{systéme\ de\ sécurité} = G(p_l)$$

TAB. 4.1 : Paramètres du jeu.

Variable	Rôle
$U(p_{lr})$	L'objectif du jeu
$L(p_e)$	Fonction de perte (consommation d'énergie)
$G(p_l)$	Fonction de gain (robustesse)
r_j	Niveau de risque avec R= r_0, r_1 , .., r_n être l'ensemble des niveaux de risque r_j , avec $0 \preceq j \preceq n$,
rt	la confiance en ce risque
g_l	r*tr
g_e	L'état énergétique du système
p_l	La probabilité d'utiliser le niveau de sécurité adéquat
p_e	La probabilité de fournir la consommation d'énergie requise
eq	La solution du jeu

La fonction de gain est modélisée par une fonction sigmoïde, est défini . La valeur du sigmoïde est comprise entre [0, 1]. Cette fonction est classée comme une fonction non linéaire, rapidement croissante et simple qui peut répondre à l'exigence de calculer le gain (robustesse) dans un délai raisonnable. La fonction de gain $G(p_l)$ est définie comme suivant.

$$G(p_l) = \begin{cases} \frac{1}{1+\exp(-g_l*(p_l-h_l))} & , g_l\text{=rt*r } \forall r > 0 \\ \frac{1}{1+\exp(-g_l*(p_l))} & , \text{ r}\approx 0, \text{ g}_l\text{=rt , rt=élevé} \\ \frac{1}{1+\exp(-g_l*(1-p_l))} & , \text{ r}\approx 0, \text{ g}_l\text{=-rt , rt=faible} \end{cases}$$

Avec g_l : la pente de la fonction sigmoîde, h_l : le centre de la fonction sigmoîde, p_l est la probabilité d'utiliser le niveau de sécurité requis l_i.

lorsque le risque est supérieur à zéro (r>0) , g_l est le produit du risque et de la confiance car les deux paramètres ont un impact sur la fonction de gain.

Si le risque est élevé et la confiance est faible, le système reste robuste (le gain du joueur 1 est élevé)) même si le niveau de sécurité demandé n'est pas permis en raison de la sur-quantification du risque. Néanmoins, si le risque et la confiance sont élevés, le

niveau de sécurité demandé n'est pas disponible, la robustesse du système sera faible (gain du joueur système de sécurité est faible). Dans le cas où le risque est quasiment nulle (r $\simeq$ 0), g_l dépend uniquement de la valeur de la confiance (rt).

Le joueur système de gestion de l'énergie

Soit $S_{systéme\ de\ gestion\ de\ l'énergie} = \{on, off\}$ l'ensemble de la stratégie du joueur système de gestion de l'énergie.
Le système de gestion de l'énergie est en mode "on" s'il accepte de fournir l'énergie requise et en mode "off" dans le cas contraire.

Fonction d'utilité du joueur 2 : Le système de gestion de l'énergie garantit le bon fonctionnement du réseau intra-véhiculaire avec un coût minimal (en minimisant la consommation d'énergie). Nous considérons, pour le joueur 2, une fonction de minimisation de la perte (loss function) puisque le système de gestion énergétique vise à donner de l'énergie.

$$U_{systéme\ de\ gestion\ de\ l'énergie} = L(p_e)$$
$$L(p_e) = \frac{1}{1+\exp(-g_e*(p_e-h_e))}$$

avec g_e : la pente de la fonction sigmoîde, h_e : le centre de la fonction sigmoïde. En pratique, g_e reflètent l'état du système. Nous considérons trois zones (verte, orange, rouge) pour caractériser l'état du système énergétique (voir table 4.2). g_e est égal à 0,05 si le système est en zone verte (disponibilité de l'énergie), 0,5 si le système est en zone orange (zone d'adaptation), 1 si le système est en zone rouge. p_e est la probabilité de fournir l'énergie requise.

Tab. 4.2 : Etats du système de gestion d'énergie.

État du système	Description
Zone verte (g_e= 0.05)	Le système de gestion de l'énergie accepte de délivrer l'énergie.
Zone orange(g_e= 0.5)	Le système de gestion de l'énergie peut accepter ou refuser de fournir de l'énergie. Cette décision est basée sur les paramètres du contexte (station de recharge et trafic).
Zone rouge (g_e= 1)	Le système de gestion de l'énergie refuse de fournir de l'énergie.

Fonction de l'objectif général

Les deux paramètres probabilités p_l et p_e sont définis indépendamment. Toutefois, dans le présent modèle, le seul contexte dans lequel le système de sécurité applique la stratégie de sécurité voulue est celui où il dispose de l'énergie nécessaire. Nous pouvons conclure que les deux événements sont identiques et que leurs probabilités coïncident. Dans cette optique, nous pouvons définir $p_{lr} := p_l = p_e$. L'objectif du jeu est de maximiser la fonction définie dans $U(p_{lr})$. La maximisation de la fonction U consiste à maximiser $G(p_{lr})$(donc le gain du joueur 1) et à minimiser de la fonction $L(p_{lr})$) (donc la perte du joueur 2) . Elle est continue, ce qui est facile à prouver dans notre cas.

$$U(p_{lr}) = (G(p_{lr}) * (1 - L(p_{lr})))$$

La solution d'équilibre

Les fonctions d'utilité définies ci-dessus expriment un compromis entre (l'énergie et la sécurité) :

- L'application de la politique de sécurité (au risque d'épuiser la batterie)
- Minimiser la consommation d'énergie (au risque de violer la sécurité).

L'équilibre du jeu est indiqué par (eq^*) et est obtenu en résolvant le problème d'optimisation suivant :

$$\text{eq= argmax } \{ \ U(p_{lr}), \ p_{lr} \in [0..1] \ \}$$

eq est la valeur maximisant $U(p_{lr})$ où p_{lr} la probabilité optimale d'obtenir du niveau de sécurité requis. Dans le cas particulier, nous pouvons récupérer la valeur optimale de eq explicitement g_e= g_l et $h_l > h_e$. Dans le cas général, la valeur de eq est calculée numériquement (voir la section sur la simulation).

L'arbre du jeu (Game tree)

L'arbre de jeu fournit de nombreuses informations sur le jeu, telles que les joueurs, les gains et les stratégies. Il est composé de nœuds (joueurs) et du processus décisionnel

des joueurs. Les nœuds sont reliés par des arêtes qui représentent l'action choisie par les joueurs. Pour le joueur système de sécurité, il existe n actions (stratégies) possibles, $S_{systéme\ de\ sécurité} = l_i$, i = 1, ..., n. Le système de sécurité choisit le niveau de sécurité des capteurs en fonction de la valeur de risque identifiée. Cependant, le système de gestion de l'énergie (Energy management system) peut choisir une stratégie parmi les stratégies $S_{systéme\ de\ géstion\ d'énergie}$ en fonction de la stratégie du système de sécurité et du contexte énergétique. Il peut accepter de fournir l'énergie nécessaire pour implémenter $l_i(stratégie\ on)$ ou refuser de fournir l'énergie nécessaire (stratégie off). La figure 4.4 donne une représentation du jeu à une étape.

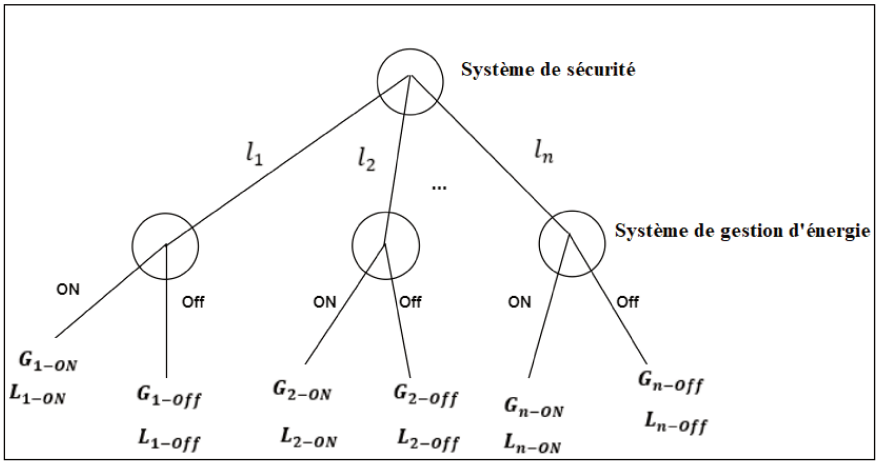


FIG. 4.4 : Arbre du jeu

4.4.4 Le modèle comportemental de RICAV

Nous avons choisi de formaliser le comportement de RICAV en utilisant le formalisme DEVS. DEVS (Discrete Event System Specification) [209] est un formalisme dynamique hiérarchique et modulaire permettant de concevoir, d'analyser et de contrôler des systèmes à événements continus ou discrets. Nous allons commencer par présenter le modèle atomique du système de sécurité. Ensuite, nous aborderons le système de gestion d'énergie et donnerons une description du modèle couplé RICAV. La figure 4.5 représente le diagramme DEVS du système de sécurité qui est composé de quatre états. $S = \{Wait, Risk\_Eval, Wait\_energy, Switch\_level, Decrease\_l\}$

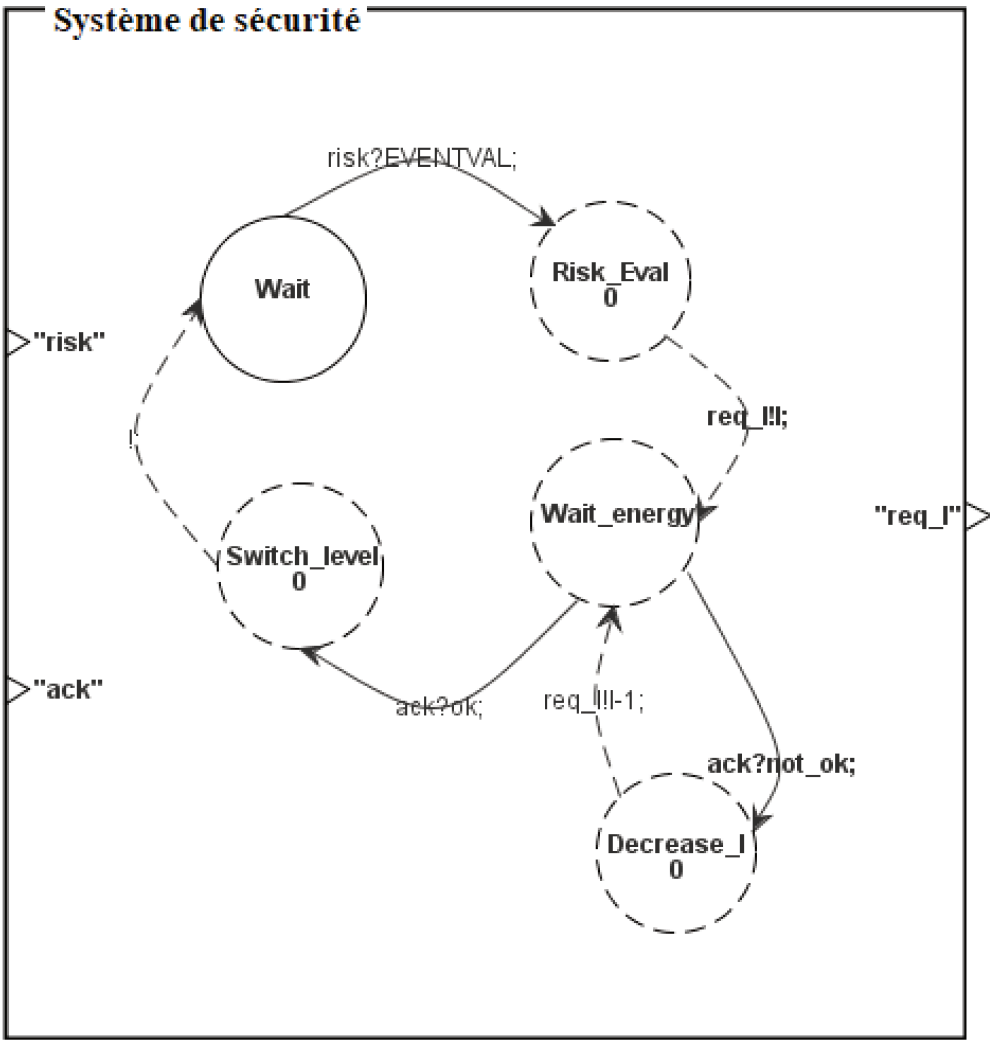


Fig. 4.5 : Modèle atomique de système de sécurité

Le système de sécurité prend en entrée le risque (avec sa valteur de confiance) et la réponse du du système gestion d'énergie. L'état Wait représente l'état dans lequel le système attend une nouvelle évaluation du risque. L'état Risk_Eval (évaluation du risque) représente l'état dans lequel le système identifie le niveau de sécurité requis. L'état Wait_energy représente l'état d'attente de la décision du système de gestion de l'énergie. Si le système de gestion de l'énergie accepte de fournir de l'énergie (ack=ok), le système passe à l'état Switch_level et revient à l'état Wait. Sinon, le système réduit le niveau de sécurité requis (l - -) jusqu'à la mise en place d'un niveau de sécurité. La figure 4.6 présente le diagramme DEVS du système de gestion énergétique qui est composé d'états en forme d'arbre. Le système énergétique prend entrée le contexte c et la requête du système de sécurité (red_l).

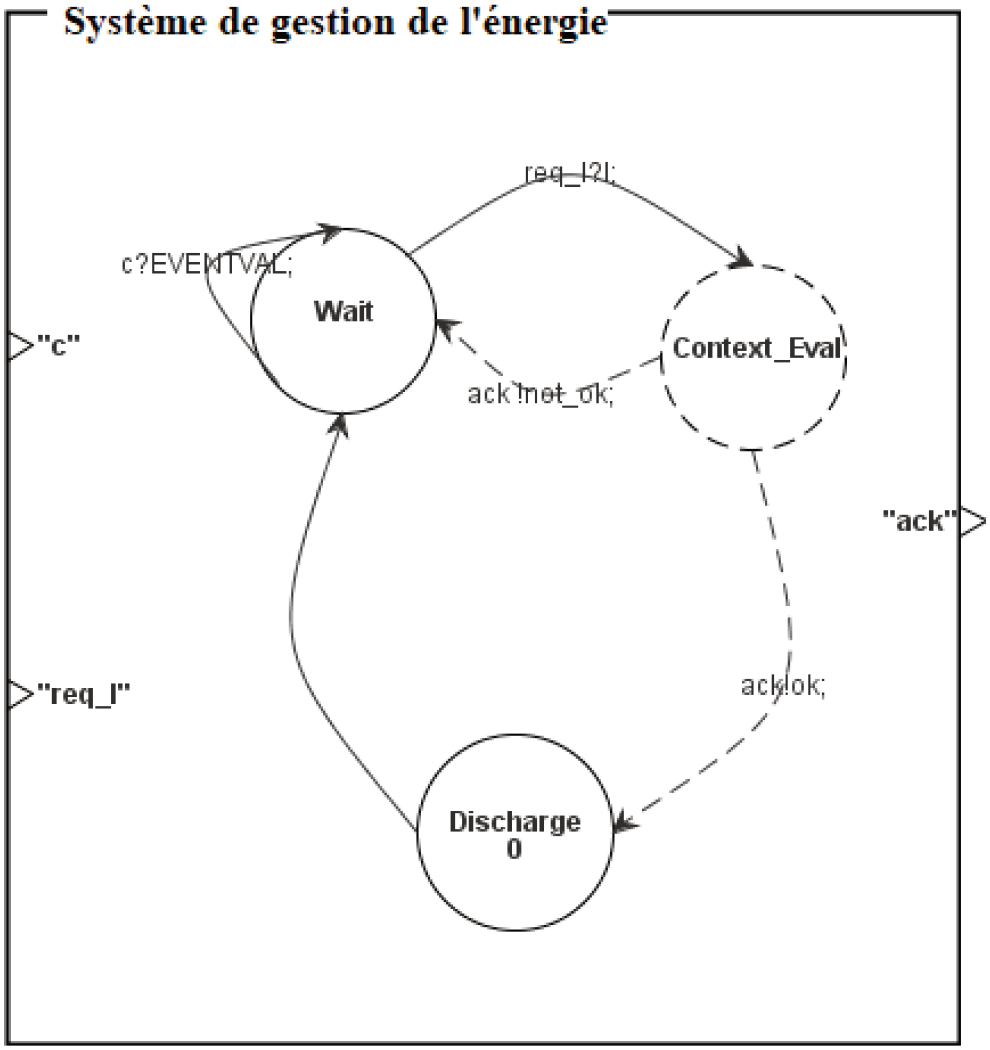


FIG. 4.6 : Modèle atomique du système de gestion d'énergie

S= { Wait, Context_Eval, Discharge }, où l'état Wait représente l'état dans lequel le système actualise le contexte (c). L'état Context_Eval représente l'état où le système évalue le contexte et prend une décision (fournir de l'énergie ou non). Si le contexte permet de délivrer de l'énergie, le système passe à l'état Discharge et retourne à l'état Wait. Sinon, le système retourne à l'état Wait. La figure 4.7 montre le modèle RICAV couplé qui est composé des deux modèles atomiques décrits précédemment.

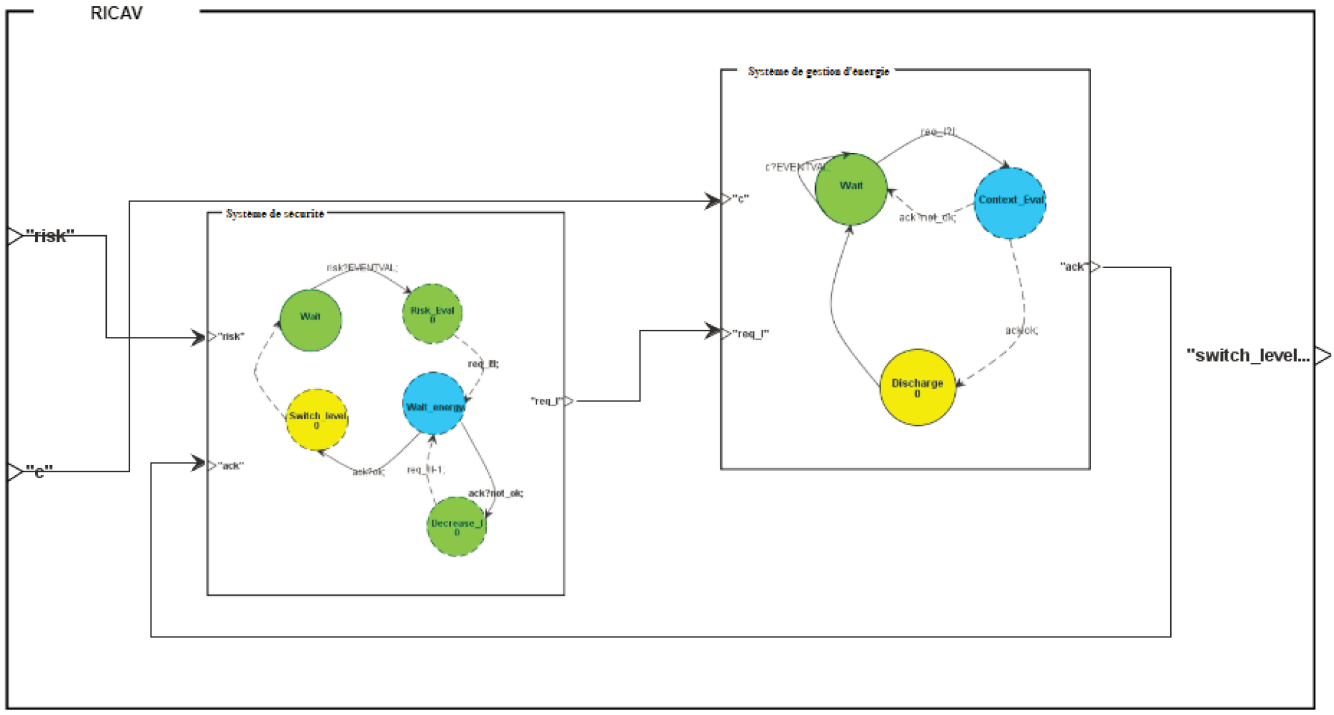


FIG. 4.7 : Modèle couplé RICAV

4.5 Simulation

Nous déterminons numériquement l'équilibre du jeu pour différentes situations. Pour cela, nous représentons la fonction de gain $\boldsymbol{G(p_l)}$, la fonction de perte $\boldsymbol{L(p_e)}$, calculons leur produit, trouvons leur point maximum et obtenons l'état d'équilibre correspondant. Nous envisageons différents scénarios en faisons varier la valeur du risque, de la confiance et du niveau d'énergie.

Scénario 1 : nous considérons une confiance élevée (rt=10) et nous faisons varier le risque et le niveau d'énergie e.

Les figures 4.8a, 4.8b, 4.8c présentent les résultats pour un scénario où l'énergie est disponible (g_e=0.005 zone verte) et la valeur du risque varie. Nous remarquons dans les figures 4.8a, 4.8b, 4.8c un équilibre de Nash. En effet, les deux joueurs sont gagnants ; l'énergie étant disponible, a perte du joueur 2 sera toujours modérée. La figure 4.8a montre que le gain du système de sécurité (robustesse) est très faible (égale à 0) si la probabilité d'obtenir le niveau de sécurité requis est faible et il peut atteindre 1 dans le

cas contraire. Dans un tel scénario, le risque étant très élevé, le gain du joueur 1 est élevé que s'il obtient le niveau de sécurité requis. RICAV privilège la sécurité à la consommation d'énergie. Dans la figure 4.8b, puisque le risque est égal à 0,5, le gain du système de sécurité est plus important que dans le cas précédent, même pour une faible probabilité. Dans la figure 4.8c, nous avons considéré un risque égal à 0,05. Nous remarquons que la robustesse du système est élevée ($G(p_l)$=0.5) même si le niveau de sécurité n'est pas du tout assuré puisque le risque d'attaque est quasi inexistant. En effet, la diminution du risque entraîne une augmentation de la robustesse du système. Dans ce cas, RICAV peut demander un faible niveau de sécurité (ou pas de sécurité du tout) même si l'énergie est disponible.

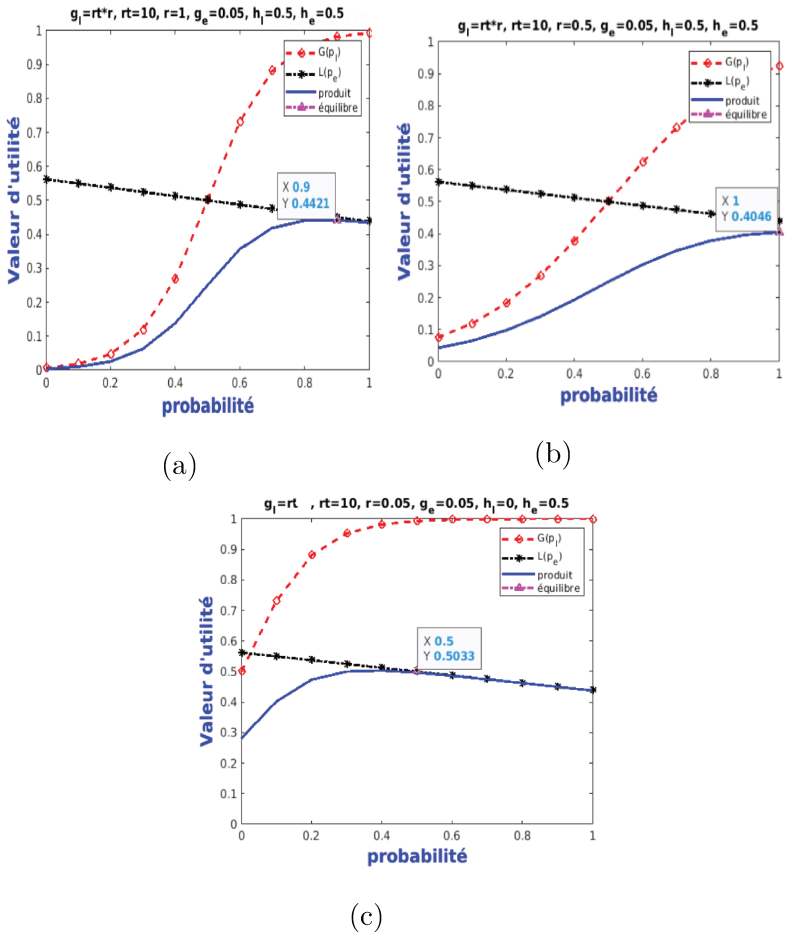
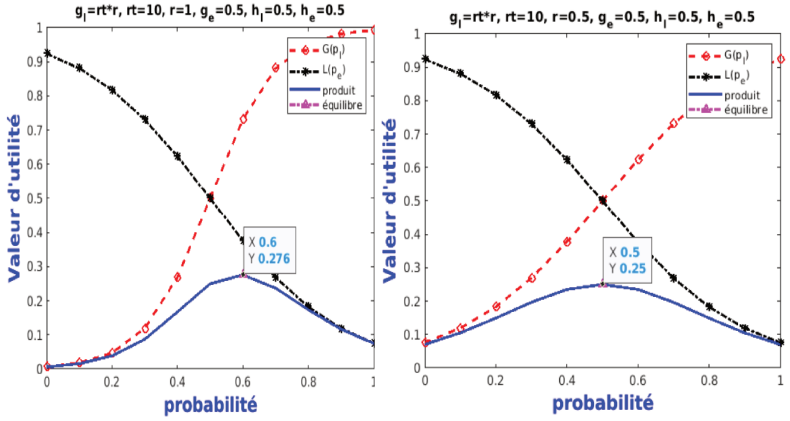


FIG. 4.8 : Equilibre de Nash pour confiance=10 et batterie en zone verte

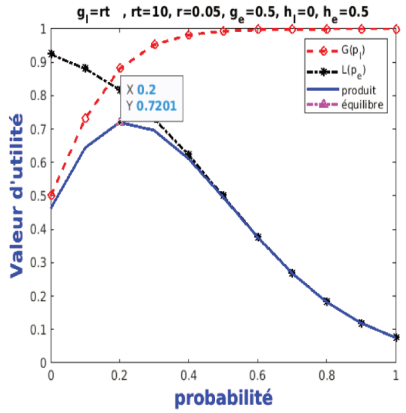
Les figures 4.9a, 4.9b, 4.9c présentent les résultats pour un scénario où l'énergie est devenue critique (g_e == 0.5 zone orange) et la valeur du risque varie. Dans ce cas, on obtient un équilibre de Nash uniquement dans le cas où le risque est très faible (r=0,05). En effet, puisque la batterie peut délivrer ou non de l'énergie, il y a toujours un gagnant et

un perdant. Dans ce scénario, RICAV propose un compromis entre l'énergie et la sécurité. Il donne la priorité à la sécurité si le risque est élevé/moyen et à l'économie d'énergie si le risque est faible.



(a)

(b)



(c)

FIG. 4.9 : Equilibre de Nash pour confiance=10 et batterie en zone orange

Les figures 4.10a, 4.10b, 4.10c présentent l'état énergétique rouge. Dans ce scénario, nous considérons une batterie dans la zone rouge où l'énergie devient très critique. Dans ce cas, nous obtenons un équilibre de Nash uniquement dans le cas où le risque est très faible (r=0,05) puisque le système énergétique n'est pas autorisé à fournir de l'énergie dans cette zone. Ainsi, le système est robuste même s'il n'obtient pas le niveau de sécurité demandé pour un risque faible. Dans ce scénario, RICAV donne la priorité à l'économies d'énergie au risque de rendre le système vulnérable pour le cas risque élevé/ moyen.

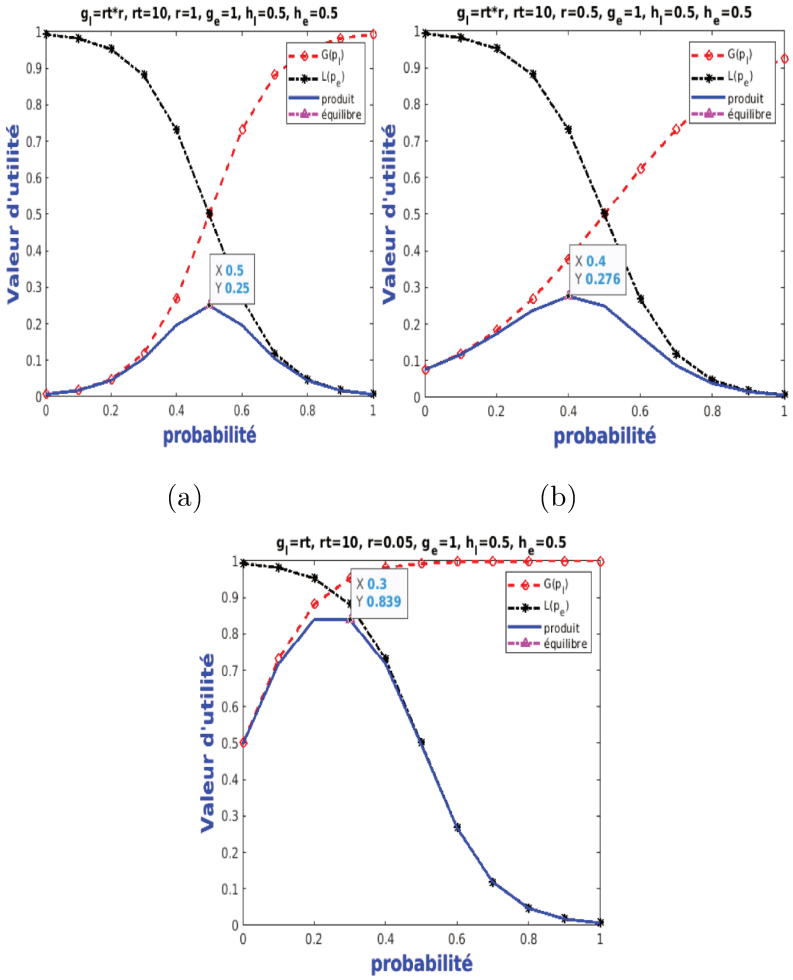


FIG. 4.10 : Equilibre de Nash pour confiance=10 et batterie en zone rouge

Scénario 2 : nous considérons une confiance non fiable (rt=1) et nous faisons varier le risque r et le niveau d'énergie e.

La figure 4.11a, 4.11b, 4.11c montre que la robustesse du système augmente lorsque le risque est élevé et que la confiance en ce risque est très faible. Lorsque $p_l = 0$, on peut observer que la fonction d'utilité du joueur système de sécurité est égal à 0 si r=0.05 et à 0,43 si r=1. Lorsque le risque est élevé à modéré et que la probabilité de fournir l'énergie requise est faible, on peut observer que le système est robuste ($g(p_l)$=0.43). Cependant, nous pouvons observer que la robustesse du système diminue lorsque le risque est sous quantifié. Ainsi, dans ce cas de figure, RICAV doit privilégier l'économie d'énergie dans le cas où le risque est élevé à modéré (ne pas délivrer l'énergie) et privilégier la sécurité dans le cas où le risque est faible ce qui ne constitue pas un problème puisque l'énergie

est disponible.

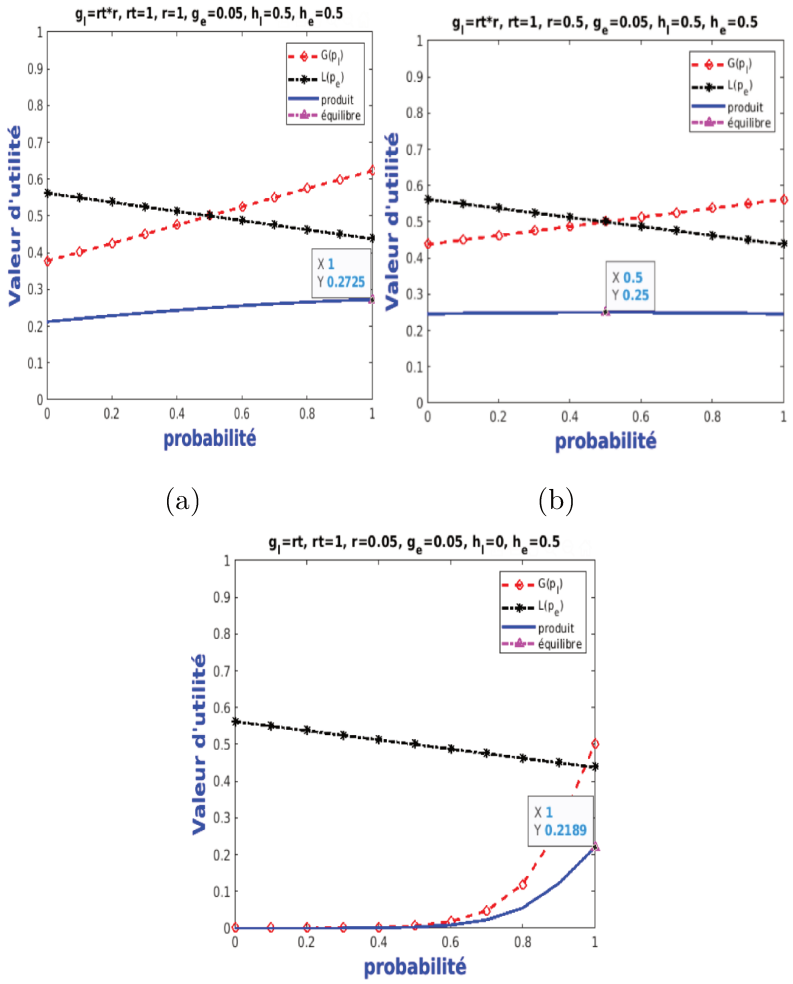


FIG. 4.11 : Equilibre de Nash pour confiance=1 et batterie en zone verte

Un scénario où la batterie est zone orange montre des résultats similaires au cas précédent sauf dans le cas d'un risque faible où RICAV privilégie la sécurité à la consommation d'énergie ce qui peut faire basculer le système énergétique en zone rouge (voir figure A.1). Lorsque la batterie est en zone rouge, la figure 4.12 montre que le système reste sécurisé, même s'il n'obtient pas l'énergie, dans le cas où le risque est élevé à modéré. Cependant, dans le cas où le risque est faible, nous assistons à un système non sécurisé puisque RICAV privilégie la consommation d'énergie à la sécurité.

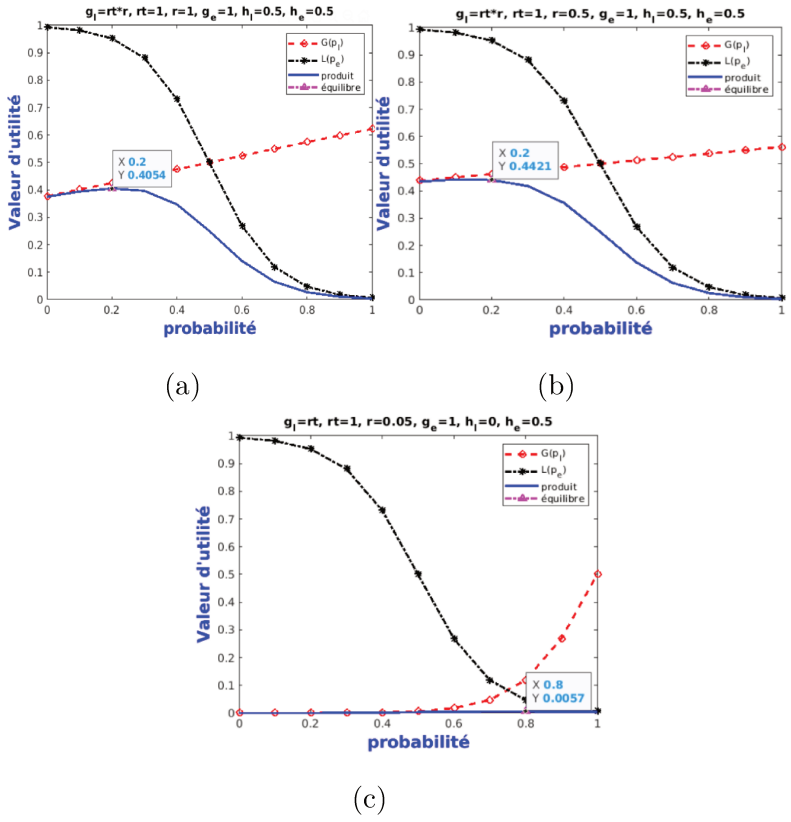


FIG. 4.12 : Equilibre de Nash pour confiance=1 et batterie en zone rouge

Synthèse

A partir des résultats obtenus, nous pouvons récapituler le comportement de RICAV de la manière suivante : (voir table 4.3) :

TAB. 4.3 : Synthèse

Risqueconfiance	Elevé/moyen	Faible
Faible	Un niveau de sécurité économe en termes d'énergie (energy-save)	Le niveau de sécurité le plus haut (le plus robuste)
Moyen/ élevé	Le niveau de sécurité le plus haut (le plus robuste)	Un niveau de sécurité économe en termes d'énergie (energy-save)

4.6 Comparaison de RICAV à CASIEV

Dans cette section, nous allons comparer les performances de CASIEV avec celles de RICAV. La comparaison porte sur les critères suivants :

- La consommation énergétique
- Le temps d'activation de la sécurité

TAB. 4.4 : Paramètres de simulation.

Paramètres	**Valeur**
Nombre de capteurs	120
Vitesse	Traffic réel
Distance à la station de recharge	20km
E_{th}	E_{th_c} : 20 × SOC /100 E_{th_sc} : 25 × SOC /100 E_{th_co} : 30 × SOC /100
E_s	10%
Périodicité (Packet interval)	1 s
Taille des données	Lidar1: 1 vlp16 (300000 points/ s) Lidar 2: 1 vlp32 (600000 points/s) Camera : 4* Camera axis-f44 (450000 b/s) Autre capteur : [8..100] bytes/s
SOC	32%
Risque	Faible, élevée/moyen, variable
confiance	Élevé (confiance= 10), faible (confiance =1)
Technologies de communication	ZigBee 250 kb/s, CAN 250 kb/s WI-FI 802.11 ac (1 GB/s)

Nous avons considéré les mêmes paramètres de simulation utilisés dans CASIEV que nous résumons dans la Table 4.4. Comme il existe plusieurs facteurs qui peuvent avoir un impact sur le risque tels que le trafic, le comportement du conducteur, le temps et le lieu [réf]. Par exemple, si le trafic est intense la probabilité d'attaque augmente et vice

versa. Dans ce travail, nous nous sommes basés sur un trafic réel (voir figure 3.14) afin de construire un fichier de risque variable.

Scénario 1 : Dans ce scénario, nous considérons une confiance élevée (confiance=10). De même, nous considérons une zone où le risque est soit faible, élevé/ moyen ou variable.

La figure 4.13 montre l'adaptation de la sécurité par rapport à l'énergie pour les valeurs de risque faible, élevée/moyen. Nous pouvons considérer que le risque élevé correspond à CASIEV puisque, dans ce cas, nous appliquons toujours le plus haut niveau de sécurité disponible. Les capteurs appliquent un niveau de sécurité faible (niveau 2) tout au long du trajet si le risque est faible. En effet, lorsque le risque est faible, le système demande un niveau de sécurité faible et donc économe en termes de consommation énergétique (energy-saving) ce qui augmente le temps d'activation de la sécurité (temps de simulation environ 43 minutes). Dans ce cas, le temps d'activation de la sécurité et le temps d'activation du niveau de sécurité adéquat est le même. En effet, même lorsque le niveau de sécurité diminue dans l'intervalle [2475, 2593], le système reste robuste puisque le risque est faible. Lorsque le risque est élevé/moyen (cas de CASIEV), on remarque que la robustesse du système diminue (passage du niveau 4 au niveau 0) et que le temps d'activation du niveau de sécurité adéquat est limité (environ 12 minutes).

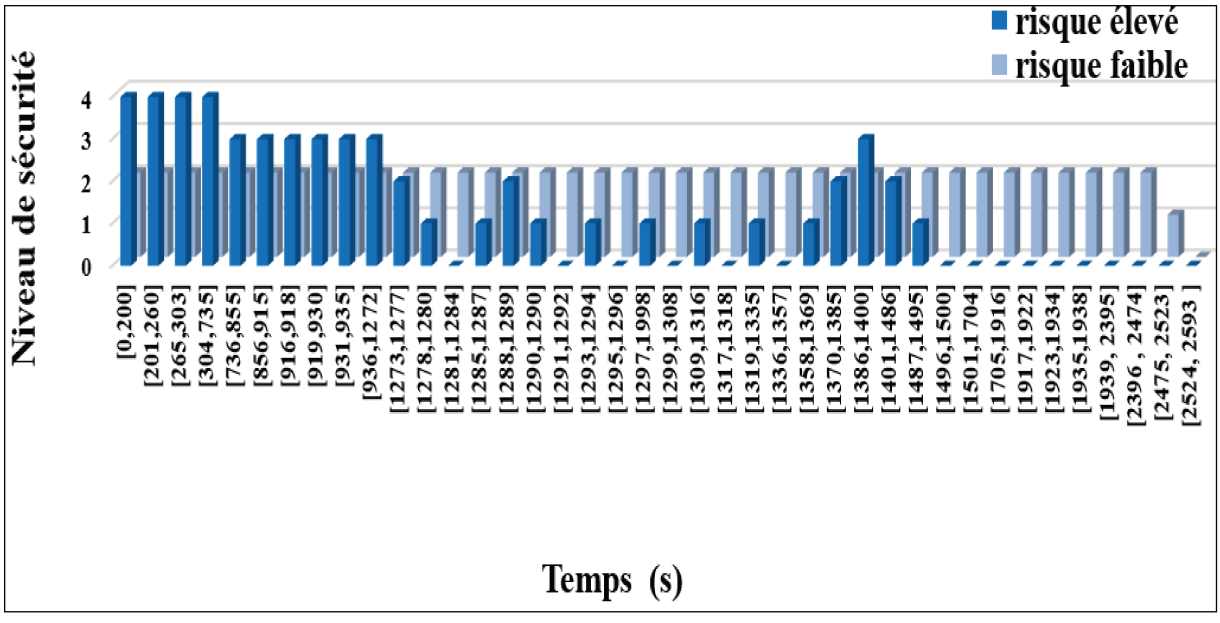


FIG. 4.13 : Adaptation par rapport à l'énergie : confiance élevée.

La figure 4.14 montre l'adaptation de la sécurité par rapport au contexte pour différentes valeurs du risque (faible, élevée/moyen). Si l'on compare avec l'adaptation à l'énergie, on remarque une augmentation de la robustesse et du temps d'activation de la sécurité du système pour les différentes valeurs du risque. Le temps d'activation de la sécurité peut atteindre environ 50 minutes si le risque est faible. De même, le temps total d'activation de la sécurité augmente lorsque le risque élevée (environ 32 mn). Dans le cas, où l'on a un risque faible sur une zone, RICAV optimise de 97,8% l'énergie consommée par CASIEV pour le niveau le plus robuste. Dans le cas où le risque est élevé, les résultats de RICAV sont équivalents à ceux de CASIEV.

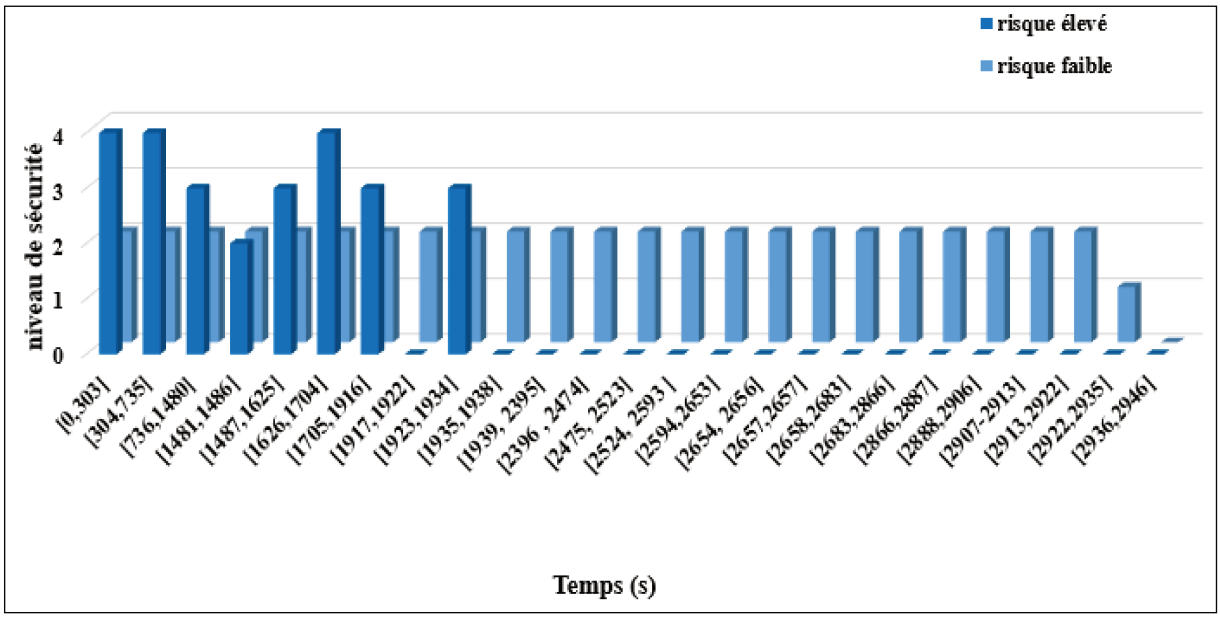


FIG. 4.14 : Adaptation par rapport au contexte : confiance élevé

La figure 4.15 montre l'adaptation de la sécurité par rapport à l'énergie et au contexte pour un risque variable. Nous pouvons constater que lorsque le risque est variable, le temps total d'activation de la sécurité est de 32 minutes pour l'adaptation à l'énergie et est supérieure au temps total d'activation de la sécurité pour CASIEV (environ 24 minutes) soit 33.5% de plus et est inférieur à un risque faible statique sur une zone (43 minutes). De même, le temps total d'activation de la sécurité (environ 43 minutes) pour l'adaptation au contexte est supérieur au temps total d'activation de la sécurité pour CASIEV (environ 34.5% de plus). Cependant, les résultats obtenus pour un risque variable sont inférieurs à un risque faible statique sur une zone (environ 50 minutes). De même, nous pouvons constater que la robustesse du système est améliorée par rapport à CASIEV puisque le

niveau de sécurité n'atteint jamais zéro tout à long du trajet et le temps d'activation du niveau 4 a augmenté pour atteindre 167% de plus (environ 32 minutes) sachant qu'il de 12 mn pour CASIEV. Les passages fréquents entre niveau 4 et niveau 2 correspondent au changement de la valeur du risque. En effet, pour un risque élevé, RICAV applique le niveau 4 lorsque l'énergie est disponible et le niveau 2 pour un risque faible.

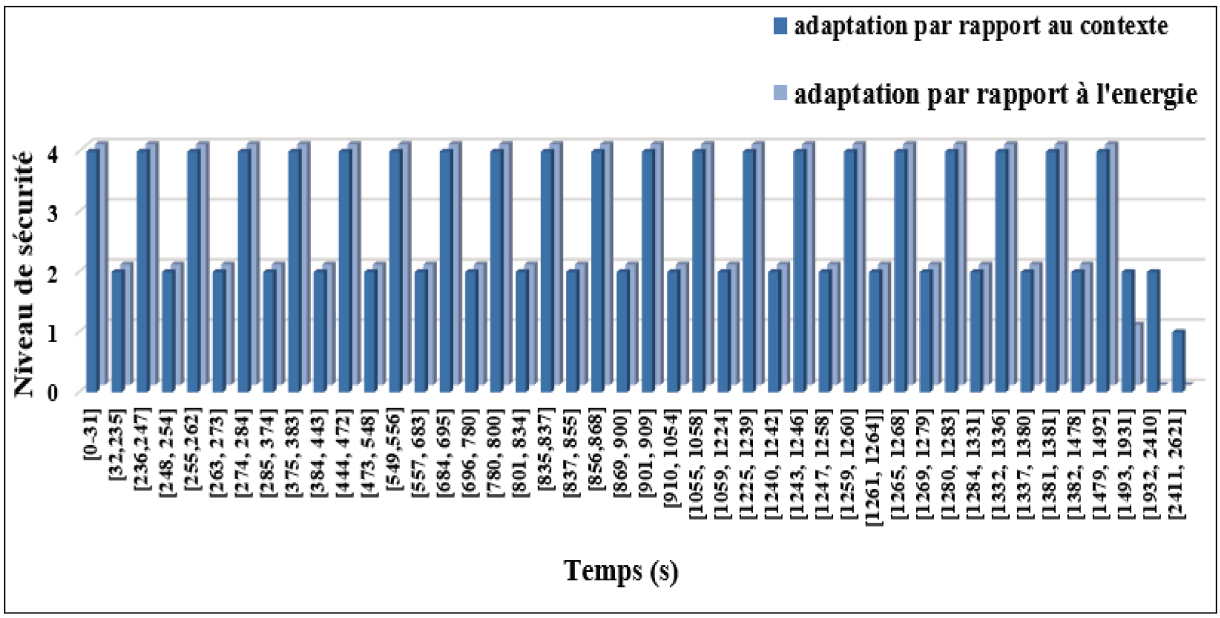


FIG. 4.15 : Adaptation par rapport l'énergie et le contexte : risque variable

Scénario 2

Dans ce scénario, nous considérons une confiance faible (confiance=1). Les résultats pour une confiance faible correspondent exactement à l'inverse de ceux pour une confiance élevée. En effet, lorsque le risque est faible, nous appliquons un niveau de sécurité correspondant à un risque élevé et vice versa. Ainsi, lorsque la confiance est faible, RICAV demande un niveau de sécurité nécessaire pour un risque 1-r (voir figures B.1 et B.2).

4.7 Conclusion

Dans ce chapitre, nous avons proposé un modèle de sécurité pour le réseau intra-véhiculaire basé sur le contexte (énergie, distance à la station de recharge, trafic, etc.), le risque et la confiance. RICAV est composé de deux joueurs : le système de sécurité et le système de gestion de l'énergie. Le système de sécurité choisi le niveau de sécurité adéquat

en fonction du couple risque d'intrusion et confiance. Le système de gestion de l'énergie représente le module CASIEV. Cependant, le niveau choisi par le système de sécurité va être considéré comme étant le niveau le plus haut pour CASIEV. RICAV donne la priorité au processus d'économie d'énergie si le risque est faible. Par contre, Il donne la priorité à la sécurité si l'énergie est disponible et que le risque est élevé ou moyen. Les simulations ont montré que RICAV a permis au système d'augmenter le temps d'activation de la sécurité et la robustesse du système par rapport à CASIEV.

Conclusion générale et perspectives

Conclusion générale

Cette thèse s'intéresse à la sécurité des systèmes véhiculaires électriques et plus particulièrement, au réseau intra véhiculaire. Nous proposons, dans ce travail, une solution de sécurité, basée sur le contexte, qui vise à augmenter le temps d'activation de la sécurité tout en respectant les contraintes énergétiques et la sécurité du conducteur. De même, nous avons apporté des améliorations à cette solution en considérant le risque et la confiance en ce risque.

Pendant très longtemps, le réseau intra-véhiculaire a été considéré comme sécurisé. Cependant, avec l'intégration des technologies sans fil (WiFi, Bluetooth, cellulaire (3g, 4g,5g)) à bord du véhicule moderne, on assiste à l'apparition de nouvelles vulnérabilités. Plusieurs expérimentations et travaux de recherche ont montré que des attaquants pouvaient compromettre la sécurité du réseau intra-véhiculaire. Ainsi, en 2015, les cyberpirates Charlie Miller et Chris Valasek ont manipulé à distance la climatisation, les essuie-glaces, et la radio d'une Jeep Cherokee et ont finalement arrêté le moteur au milieu d'une autoroute [90]. Le point d'entrée était une connexion cellulaire vulnérable dans le véhicule, qui a permis d'atteindre le bus CAN et d'effectuer des actions malveillantes. En 2016, une équipe de hackers prend le contrôle à distance d'une Tesla Model S à 30 km de distance [210]. Les chercheurs ont exploité des vulnérabilités dans le système Wi-Fi du véhicule pour actionner les freins d'un véhicule en mouvement. Même si Tesla a répondu par des mises à jour de sécurité , en 2017 de nouvelles vulnérabilités ont été exploitées dans [21] les chercheurs ont piraté des voitures BMW et ont découvert 14 vulnérabilités [211]. Dans la littérature, plusieurs travaux [4, 23–26] ont proposé des solutions de sécurité pour le réseau intra-véhiculaire. Cependant, ils se sont, à chaque fois, focalisés sur les capacités de mémoire et de traitement des capteurs et n'ont pas envisagé le paramètre de consommation énergétique. Les solutions proposées pour le réseau intra-véhiculaire sont énergivores puisqu'elles sont basées sur les mécanismes de sécurité les plus robustes.

Analyse énergétique : Les mécanismes de sécurité ne disposent pas de la même consommation de ressources et plus spécifiquement la consommation d'énergie. Ainsi, nos mesures ont montré que l'utilisation d'une politique de sécurité implémentant SKIPJACK + HMAC permet d'optimiser d'environ 20% l'énergie par rapport à une politique de sé-

curité utilisant AES + HMAC. Cette différence est due à la consommation énergétique des algorithmes cryptographiques puisque la consommation d'énergie des fonctions de hachage est presque négligeable. Par conséquence, nous avons défini des niveaux de sécurité en se basant sur la consommation énergétique des mécanismes de sécurité, leurs robustesse et leur utilisation en termes de mémoire et traitement.

Sécurité basée sur le contexte (CASIEV) : Pour répondre à la contrainte énergétique des véhicules électriques, nous avons proposé une stratégie de sécurité, basée sur le contexte, pour le réseau de capteurs intra-véhiculaire (CASIEV). Les capteurs passent d'un niveau de sécurité à l'autre en fonction du contexte véhiculaire dynamique. Pour s'adapter à l'écosystème des véhicules électriques, le contexte prend en compte le niveau de la batterie, le type de capteurs, la mémoire et la capacité de traitement des capteurs, la distance aux stations de recharge les plus proches et les conditions de trafic. Dans la solution proposée, afin de préserver la sécurité du système le plus longtemps possible, chaque capteur du réseau intra-véhiculaire implémente toujours le niveau de sécurité le plus élevé autorisé par le contexte. Les simulations ont montré que lorsque l'énergie est supérieure à un seuil (E_{th}), nous assistons à une diminution progressive des niveaux de sécurité pour être toujours dans une zone de confort (niveau de batterie supérieure à Eth). De même, lorsque le niveau de la batterie est (inférieur à E_{th}), que le trafic est faible/moyen et que l'énergie restante permet d'atteindre la station de recharge la plus proche, la sécurité continue à être assurée. Cependant, lorsque l'énergie est inférieure à ce seuil, que le trafic est élevé et/ou que le véhicule ne peut pas atteindre la station de recharge, la sécurité est désactivée. Lorsque le niveau de batterie devient inférieur à seuil critique (E_s), la sécurité est désactivée pour assurer la sécurité du conducteur. Les simulations ont aussi montré que, le temps total d'activation de la sécurité fourni par CASIEV est d'environ 30% plus important que le temps résultant d'une approche statique implémentant le niveau de sécurité le plus haut. De plus, nous avons considéré une application véhiculaire temps réels, appelée système de commande de traction (TCS), et nous avons évalué la latence fournie par CASIEV qui est d'environ 54 ms pour la configuration de sécurité la plus robuste et 1,8 ms pour la configuration de sécurité la plus faible. Ces valeurs sont en dessous de la latence demandée par TCS (traction control system).

Sécurité basée sur le contexte, le risque et le trust (RICAV) : CASIEV

considère que le risque est toujours très élevé (selon NIST qui catégorise le risque en très faible, faible, moyen, élevé ou très élevé). Ainsi, nous avons apporté des améliorations à CASIEV en prenant en compte le risque et la confiance en ce risque (trust) toujours dans un but de compromis entre la sécurité et la consommation d'énergie. RICAV adapte la sécurité en fonction du risque, trust et du contexte véhiculaire. La solution est modélisée en utilisant la théorie des jeux. Le jeu est composé de deux joueurs : le système de sécurité (le module ASR) et le système de gestion de l'énergie (le module CASIEV). Le système de sécurité choisit le niveau de sécurité approprié en fonction du couple risque et trust. Les simulations ont montré que si le trust est moyen/élevé (resp faible), le système demande un niveau de sécurité économe en termes d'énergie pour un risque faible (resp moyen/élevé) et le niveau de sécurité le plus haut pour un risque élevé (resp faible). Le système de gestion de l'énergie considère le niveau de sécurité demandé et fournit la quantité d'énergie requise par le système de sécurité en fonction du contexte véhiculaire. Nous avons comparé les performances de CASIEV à celles de RICAV en termes de temps total d'activation de la sécurité et de robustesse du système (niveaux de sécurité). La simulation a montré que le temps total d'activation de la sécurité a augmenté par rapport à CASIEV. Pour un risque faible et un trust élevé constant sur une zone, le temps total d'activation de la sécurité est supérieur au temps total d'activation de la sécurité pour CASIEV d'environ 56%. Cependant, pour un risque variable, le temps d'activation de la sécurité est d'environ 34,5% de plus par rapport à celui fourni par CASIEV. Pour un risque élevé, RICAV fournit les mêmes valeurs que CASIEV puisqu'il va solliciter à chaque fois le niveau de sécurité le plus élevé.

Perspectives

Nous envisageons de développer une approche plus élaborée d'analyse des risques d'intrusion dans le réseau intra véhiculaire. Cette approche doit prendre en compte le contexte du véhicule et l'historique des tentatives d'intrusion. Pour cela, nous souhaitons combiner des approches existantes (adaptés au contexte véhiculaire) avec des techniques de machine Learning pour rendre le modèle d'estimation plus précis et plus réaliste. De plus, il serait intéressant de solliciter le conducteur dans le modèle RICAV pour traiter le cas élevé toujours dans un but d'amélioration de la consommation énergétique.

Dans ces travaux, nous nous sommes intéressés à la communication intra-véhiculaire (V2S). Cependant, la stratégie de sécurité adaptative peut aussi être appliquée pour les communications à l'extérieur du véhicule (V2V, V2I et V2N). Ce type de communication présente un spectre de menaces complexe en raison de la grande variété des technologies de communication disponibles. Il serait intéressant de considérer les types de technologies disponibles (5G, Wi-Fi, 802.11p, etc.), en fonction de leur consommation d'énergie, leur niveau de sécurité, la qualité du signal, etc, dans le contexte sur lequel s'appuie l'adaptation de la sécurité. Ainsi, l'ECU (Gateway) peut basculer d'une technologie de communication à une autre en fonction du niveau de la batterie et de son contexte.

Bibliographie

[1] R. Warschofsky, "Autosar software architecture," *Hasso-Plattner-Institute für Softwaresystemtechnik : Potsdam, Germany*, pp. 1–12, 2009.

[2] D. Rupprecht, K. Kohls, T. Holz, and C. Pöpper, "Breaking lte on layer two," in *2019 IEEE Symposium on Security and Privacy (SP)*, pp. 1121–1136, 2019.

[3] Y. Li, Y. Yu, W. Susilo, Z. Hong, and M. Guizani, "Security and privacy for edge intelligence in 5g and beyond networks : Challenges and solutions," *IEEE Wireless Communications*, pp. 63–69, 2021.

[4] K. Zeng, E. Wang, W. Xu, and S. Sastry, "Hardware module-based authentication in intra-vehicle networks," June 30 2020. US Patent 10,701,102.

[5] M.-J. Kang and J.-W. Kang, "Intrusion detection system using deep neural network for in-vehicle network security," *PloS one*, pp. 1–11, 2016.

[6] S. Woo, H. J. Jo, I. S. Kim, and D. H. Lee, "A practical security architecture for in-vehicle can-fd," *IEEE Transactions on Intelligent Transportation Systems*, pp. 2248–2261, 2016.

[7] S. NIST, "800-30 revision 1, guide for conducting risk assessments, september 2012," *URL : http ://csrc. nist. gov/publications/nistpubs/800-30-rev1/sp800_30_r1. pdf (accessed : 10.02. 2021).*

[8] R. Bharathi and R. Selvarani, "Software reliability assessment of safety critical system using computational intelligence," *International Journal of Software Science and Computational Intelligence (IJSSCI)*, pp. 1–25, 2019.

[9] E. E. Agency, "A european strategy for low-emission mobility," *[online] Available at : <https ://ec.europa.eu/clima/policies/transport_en>, [Accessed : le 3/05/ 2021].*

[10] M. Ziefle, S. Beul-Leusmann, K. Kasugai, and M. Schwalm, "Public perception and acceptance of electric vehicles : exploring users' perceived benefits and drawbacks,"

in *International conference of design, user experience, and usability*, pp. 628–639, 2014.

[11] A. T. Thorgeirsson, S. Scheubner, S. Fünfgeld, and F. Gauterin, "Probabilistic prediction of energy demand and driving range for electric vehicles with federated learning," *IEEE Open Journal of Vehicular Technology*, pp. 151–161, 2021.

[12] Y. Fraiji, L. B. Azzouz, W. Trojet, and L. A. Saidane, "Cyber security issues of internet of electric vehicles," in *2018 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–6, 2018.

[13] L. Eboli, G. Mazzulla, and G. Pungillo, "Measuring the driver's perception error in the traffic accident risk evaluation," *IET intelligent transport systems*, pp. 659–666, 2017.

[14] F. Kohnhäuser, D. Püllen, and S. Katzenbeisser, "Ensuring the safe and secure operation of electronic control units in road vehicles," in *2019 IEEE Security and Privacy Workshops (SPW)*, pp. 126–131, 2019.

[15] J.-R. Lin, T. Talty, and O. K. Tonguz, "A blind zone alert system based on intra-vehicular wireless sensor networks," *IEEE Transactions on Industrial Informatics*, pp. 476–484, 2015.

[16] R. Liu, S. Herbert, T. H. Loh, and I. J. Wassell, "A study on frequency diversity for intra-vehicular wireless sensor networks (wsns)," in *2011 IEEE Vehicular Technology Conference (VTC Fall)*, pp. 1–5, 2011.

[17] C. Miller and C. Valasek, "Adventures in automotive networks and control units," *Def Con*, pp. 260–264, 2013.

[18] L. Pan, X. Zheng, H. Chen, T. Luan, H. Bootwala, and L. Batten, "Cyber security attacks to modern vehicular systems," *Journal of information security and applications*, pp. 90–100, 2017.

[19] P. Carsten, T. R. Andel, M. Yampolskiy, and J. T. McDonald, "In-vehicle networks : Attacks, vulnerabilities, and proposed solutions," in *2015 Proceedings of the 10th Annual Cyber and Information Security Research Conference*, pp. 1–8, 2015.

[20] S. Woo, H. J. Jo, and D. H. Lee, "A practical wireless attack on the connected car and security protocol for in-vehicle can," *IEEE Transactions on intelligent transportation systems*, pp. 993–1006, 2014.

[21] S. Nie, L. Liu, and Y. Du, "Free-fall : hacking tesla from wireless to can bus," *Briefing, Black Hat USA*, pp. 1–16, 2017.

[22] Y. Zhang, J. Li, D. Zheng, P. Li, and Y. Tian, "Privacy-preserving communication and power injection over vehicle networks and 5g smart grid slice," *Journal of Network and Computer Applications*, pp. 50–60, 2018.

[23] O. Henniger, A. Ruddle, H. Seudié, B. Weyl, M. Wolf, and T. Wollinger, "Securing vehicular on-board it systems : The evita project," in *2009 VDI/VW Automotive Security Conference*, pp. 1–41, 2009.

[24] R. Islam and R. U. D. Refat, "Improving can bus security by assigning dynamic arbitration ids," *Journal of Transportation Security*, pp. 19–31, 2020.

[25] A. Chattopadhyay, K.-Y. Lam, and Y. Tavva, "Autonomous vehicle : Security by design," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–11, 2020.

[26] C. Corbett, M. Brunner, K. Schmidt, R. Schneider, and U. Dannebaum, "Leveraging hardware security to secure connected vehicles," tech. rep., SAE Technical Paper, 2018.

[27] M. La Manna, L. Treccozzi, P. Perazzo, S. Saponara, and G. Dini, "Performance evaluation of attribute-based encryption in automotive embedded platform for secure software over-the-air update," *Sensors*, pp. 515–536, 2021.

[28] J. Lee, K. Kapitanova, and S. H. Son, "The price of security in wireless sensor networks," *Computer Networks*, pp. 2967–2978, 2010.

[29] N. R. Potlapally, S. Ravi, A. Raghunathan, and N. K. Jha, "Analyzing the energy consumption of security protocols," in *Proceedings of the 2003 international symposium on Low power electronics and design*, pp. 30–35, 2003.

[30] S. Mewada, P. Sharma, and S. Gautam, "Classification of efficient symmetric key cryptography algorithms," *International Journal of Computer Science and Information Security*, pp. 1–14, 2016.

[31] Y. Fraiji, L. ben Azzouz, W. Trojet, L. A. Saidane, and G. Hoblos, "Adaptive security for the intra-electric vehicular wireless networks," in *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*, pp. 1215–1220, 2019.

[32] Y. Fraiji, L. ben Azzouz, W. Trojet, G. Hoblos, and L. A. Saidane, "Context-aware security for the intra-electric vehicle network under energy constraints," *Computers & Electrical Engineering*, pp. 1–27, 2021.

[33] I. ETSI, "Intelligent transport systems (its) ; security ; threat, vulnerability and risk analysis (tvra)," tech. rep., Technical report, ETSI TR 102 893, European Telecommunications Standards …, 2010.

[34] K. B. Kelarestaghi, M. Foruhandeh, K. Heaslip, and R. Gerdes, "Intelligent transportation system security : impact-oriented risk assessment of in-vehicle networks," *IEEE Intelligent Transportation Systems Magazine*, pp. 1–1, 2019.

[35] R. A. Shaikh and V. Thayananthan, "Risk-based decision methods for vehicular networks," *Electronics*, pp. 627–635, 2019.

[36] H. Hasrouny, C. Bassil, A. E. Samhat, and A. Laouiti, "Security risk analysis of a trust model for secure group leader-based communication in vanet," in *Vehicular Ad-Hoc Networks for Smart Cities*, pp. 71–83, 2017.

[37] J. M. Kim, H. S. Lee, J. Yi, and M. Park, "Power adaptive data encryption for energy-efficient and secure communication in solar-powered wireless sensor networks," *Journal of Sensors*, pp. 1–10.

[38] A. Di Mauro, X. Fafoutis, and N. Dragoni, "Adaptive security in odmac for multihop energy harvesting wireless sensor networks," *International Journal of Distributed Sensor Networks*, pp. 1–10, 2015.

[39] E. Romero, J. Blesa, and A. Araujo, "An adaptive energy aware strategy based on game theory to add privacy in the physical layer for cognitive wsns," *Ad Hoc Networks*, pp. 1–29, 2019.

[40] A. Arfaoui, A. Kribeche, and S.-M. Senouci, "Context-aware anonymous authentication protocols in the internet of things dedicated to e-health applications," *Computer Networks*, pp. 23–36, 2019.

[41] L. Gheorghe, R. Rughinis, and N. Tapus, "Adaptive security framework for wireless sensor networks," in *2012 Fourth International Conference on Intelligent Networking and Collaborative Systems*, pp. 636–641, 2012.

[42] Y. Fraiji, L. ben Azzouz, W. Trojet, G. Hoblos, and L. A. Saidane, "Ricav : Risk based context-aware security solution for the intra-electric vehicle network," in *In Proceedings of the 18th International Conference on Security and Cryptography*, pp. 772–778, 2021.

[43] N. Lu, N. Cheng, N. Zhang, X. Shen, and J. W. Mark, "Connected vehicles : Solutions and challenges," *IEEE internet of things journal*, pp. 289–299, 2014.

[44] F. Yang, J. Li, T. Lei, and S. Wang, "Architecture and key technologies for internet of vehicles : a survey," pp. 1–17, 2017.

[45] M. Giordani, M. Polese, M. Mezzavilla, S. Rangan, and M. Zorzi, "Toward 6g networks : Use cases and technologies," *IEEE Communications Magazine*, pp. 55–61, 2020.

[46] T. Q. Duong, V.-P. Hoang, and C.-K. Pham, "Convergence of 5g technologies, artificial intelligence and cybersecurity of networked societies for the cities of tomorrow," *Mobile Networks and Applications*, pp. 1–3, 2021.

[47] D. Grewe, M. Wagner, M. Arumaithurai, I. Psaras, and D. Kutscher, "Information-centric mobile edge computing for connected vehicle environments : Challenges and research directions," in *Proceedings of the Workshop on Mobile Edge Communications*, pp. 7–12, 2017.

[48] A. Mohan, S. Sripad, P. Vaishnav, and V. Viswanathan, "Trade-offs between automation and light vehicle electrification," *Nature Energy*, pp. 543–549, 2020.

[49] D. Roszczypala, C. Batard, F. Poitiers, and N. Ginot, "Electric vehicle charging strategies including load demand response to address utility grid constraints : a

real implementation," in *International Conference on Electrical Engineering and Electronics (EEE'20)*, pp. 1–1, 2020.

[50] H. Xiao, Y. Huimei, W. Chen, and L. Hongjun, "A survey of influence of electrics vehicle charging on power grid," in *2014 9th IEEE Conference on Industrial Electronics and Applications*, pp. 121–126, 2014.

[51] Y. Tao, M. Huang, and L. Yang, "Data-driven optimized layout of battery electric vehicle charging infrastructure," *Energy*, pp. 735–744, 2018.

[52] U. Eberle and R. Von Helmolt, "Sustainable transportation based on electric vehicle concepts : a brief overview," *Energy & Environmental Science*, pp. 689–699, 2010.

[53] B. Kloör, M. Monhof, D. Beverungen, and S. Braäer, "Design and evaluation of a model-driven decision support system for repurposing electric vehicle batteries," *European Journal of Information Systems*, pp. 171–188, 2018.

[54] A. Singh, P. Karandikar, and N. Kulkarni, "Mitigation of sulfation in lead acid battery towards life time extension using ultra capacitor in hybrid electric vehicle," *Journal of Energy Storage*, pp. 1–34, 2021.

[55] M. Boehner, "Security for connected vehicles throughout the entire life cycle," *ATZelectronics worldwide*, pp. 16–21, 2019.

[56] S. Jadhav and D. Kshirsagar, "A survey on security in automotive networks," in *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)*, pp. 1–6, 2018.

[57] F. Wuhlegemuth and P. Hofmann, "Automotive system design : today and tomorrow," in *17th DASC. AIAA/IEEE/SAE. Digital Avionics Systems Conference. Proceedings (Cat. No. 98CH36267)*, pp. 1–2, 1998.

[58] P. C. Nissimagoudar, V. Mane, N. C. Iyer, S. Eligar, S. Ramakrishna, M. Kiran, A. Patil, H. Gireesha, K. Shamshuddin, A. Raju, *et al.*, "Educational framework for automotive ecu design : A case study," *Journal of Engineering Education Transformations*, pp. 48–56, 2017.

[59] M. Broy, I. H. Kruger, A. Pretschner, and C. Salzmann, "Engineering automotive software," *Proceedings of the IEEE*, pp. 356–373, 2007.

[60] S. Fürst and M. Bechter, "Autosar for connected and autonomous vehicles : The autosar adaptive platform," in *2016 46th annual IEEE/IFIP international conference on Dependable Systems and Networks Workshop (DSN-W)*, pp. 215–217, 2016.

[61] S. Tuohy, M. Glavin, C. Hughes, E. Jones, M. Trivedi, and L. Kilmartin, "Intra-vehicle networks : A review," *IEEE Transactions on Intelligent Transportation Systems*, pp. 534–545, 2014.

[62] K. Tindell, A. Burns, and A. J. Wellings, "Calculating controller area network (can) message response times," *Control engineering practice*, pp. 1163–1169, 1995.

[63] M. Brandl and K. Kellner, "Performance evaluation of power-line communication systems for lin-bus based data transmission," *Electronics*, pp. 85–94, 2021.

[64] R. Makowitz and C. Temple, "Flexray-a communication network for automotive control systems," in *2006 IEEE International Workshop on Factory Communication Systems*, pp. 207–212, 2006.

[65] B. Fijalkowski, "Media oriented system transport (most) networking," in *Automotive Mechatronics : Operational and Practical Issues*, pp. 73–74, 2011.

[66] J.-R. Lin, T. Talty, and O. K. Tonguz, "On the potential of bluetooth low energy technology for vehicular applications," pp. 267–275, 2015.

[67] Q. Kang, X. Huang, Y. Li, Z. Xie, Y. Liu, and M. Zhou, "Energy-efficient wireless transmissions for battery-less vehicle tire pressure monitoring system," *IEEE Access*, pp. 7687–7699, 2017.

[68] D. Mukhopadhyay, M. Gupta, T. Attar, P. Chavan, and V. Patel, "An attempt to develop an iot based vehicle security system," in *2018 IEEE International Symposium on Smart Electronic Systems (iSES)(Formerly iNiS)*, pp. 195–198, 2018.

[69] Q. Luo and J. Liu, "Wireless telematics systems in emerging intelligent and connected vehicles : Threats and solutions," *IEEE Wireless Communications*, pp. 113–119, 2018.

[70] ETSI, "Intelligent transport systems (its), communications architecture," 2010.

[71] O. Kaiwartya, A. H. Abdullah, Y. Cao, A. Altameem, M. Prasad, C.-T. Lin, and X. Liu, "Internet of vehicles : Motivation, layered architecture, network model, challenges, and future aspects," *IEEE Access*, pp. 5356–5373, 2016.

[72] R. Dev, "Connected cars & iot—emerging trends and predictions," *Auto Tech Review*, pp. 12–13, 2016.

[73] R. Falk and S. Fries, "Electric vehicle charging infrastructure security considerations and approaches," *Proc. of INTERNET*, pp. 58–64, 2012.

[74] S. Cao and V. C. Lee, "An accurate and complete performance modeling of the ieee 802.11 p mac sublayer for vanet," *Computer Communications*, pp. 107–120, 2020.

[75] D. Garcia-Roger, S. Roger, D. Martín-Sacristán, J. F. Monserrat, A. Kousaridas, P. Spapis, and C. Zhou, "5g functional architecture and signaling enhancements to support path management for ev2x," *IEEE Access*, pp. 20484–20498, 2019.

[76] A. Laya, K. Wang, A. A. Widaa, J. Alonso-Zarate, J. Markendahl, and L. Alonso, "Device-to-device communications and small cells : enabling spectrum reuse for dense networks," *IEEE Wireless Communications*, pp. 98–105, 2014.

[77] A. Laya, K. Wang, A. A. Widaa, J. Alonso-Zarate, J. Markendahl, and L. Alonso, "Device-to-device communications and small cells : enabling spectrum reuse for dense networks," *IEEE Wireless Communications*, pp. 98–105, 2014.

[78] M. N. Tehrani, M. Uysal, and H. Yanikomeroglu, "Device-to-device communication in 5g cellular networks : challenges, solutions, and future directions," *IEEE Communications Magazine*, pp. 86–92, 2014.

[79] D. Namiot and M. Sneps-Sneppe, "On one d2d usage model for 5g networks," in *2021 28th Conference of Open Innovations Association (FRUCT)*, pp. 322–327, 2021.

[80] S. Abdellatif, O. Tibermacine, W. Bechkit, and A. Bachir, "Service oriented d2d efficient communication for post-disaster management," in *2020 International Wireless Communications and Mobile Computing (IWCMC)*, pp. 970–975, 2020.

[81] K. M. Malarski, F. Moradi, K. D. Ballal, L. Dittmann, and S. Ruepp, "Internet of reliable things : Toward d2d-enabled nb-iot," in *2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC)*, pp. 196–201, 2020.

[82] C.-X. Wang, F. Haider, X. Gao, X.-H. You, Y. Yang, D. Yuan, H. M. Aggoune, H. Haas, S. Fletcher, and E. Hepsaydir, "Cellular architecture and key technologies for 5g wireless communication networks," *IEEE communications magazine*, pp. 122–130, 2014.

[83] M. H. Qutqut, F. M. Al-Turjman, and H. S. Hassanein, "Hof : A history-based offloading framework for lte networks using mobile small cells and wi-fi," in *38th Annual IEEE Conference on Local Computer Networks-Workshops*, pp. 77–83, 2013.

[84] N. T. Le, M. A. Hossain, A. Islam, D.-y. Kim, Y.-J. Choi, and Y. M. Jang, "Survey of promising technologies for 5g networks," 2016.

[85] F. Haider, C.-X. Wang, H. Haas, D. Yuan, H. Wang, X. Gao, X.-H. You, and E. Hepsaydir, "Spectral efficiency analysis of mobile femtocell based cellular systems," in *2011 IEEE 13th International Conference on Communication Technology*, pp. 347–351, 2011.

[86] G. A. Francia III, "Connected vehicle security," in *International Conference on Cyber Warfare and Security*, pp. 173–181, 2020.

[87] J. Sun, S. Iqbal, N. S. Arabi, and M. Zulkernine, "A classification of attacks to in-vehicle components (ivcs)," *Vehicular Communications*, pp. 1–25, 2020.

[88] A. Samad, S. Alam, S. Mohammed, and M. Bhukhari, "Internet of vehicles (iov) requirements, attacks and countermeasures," in *Proceedings of 12th INDIACom ; INDIACom-2018; 5th international conference on "computing for sustainable global development" IEEE conference, New Delhi*, pp. 1–4, 2018.

[89] S. Woo, H. J. Jo, and D. H. Lee, "A practical wireless attack on the connected car and security protocol for in-vehicle can," *IEEE Transactions on intelligent transportation systems*, pp. 993–1006, 2014.

[90] C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," *Black Hat USA*, no. 1–92, 2015.

[91] A. Wasicek and A. Weimerskirch, "Recognizing manipulated electronic control units," tech. rep., 2015.

[92] T. Eisenbarth, T. Kasper, A. Moradi, C. Paar, M. Salmasizadeh, and M. T. M. Shalmani, "On the power of power analysis in the real world : A complete break of the keeloq code hopping scheme," in *Annual International Cryptology Conference*, pp. 203–220, 2008.

[93] I. Foster, A. Prudhomme, K. Koscher, and S. Savage, "Fast and vulnerable : A story of telematic failures," in *9th {USENIX} Workshop on Offensive Technologies ({WOOT} 15)*, pp. 1–9, 2015.

[94] T. Bécsi, S. Aradi, and P. Gáspár, "Security issues and vulnerabilities in connected car systems," in *2015 International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS)*, pp. 477–482, 2015.

[95] M. Scalas and G. Giacinto, "Automotive cybersecurity : Foundations for next-generation vehicles," in *2019 2nd International Conference on new Trends in Computing Sciences (ICTCS)*, pp. 1–6, 2019.

[96] M. Hamad and V. Prevelakis, "Savta : A hybrid vehicular threat model : Overview and case study," *Information*, pp. 273–284, 2020.

[97] Y. Wang, S. Han, N. Zhang, and P. Hu, "Study on cybersecurity attack-defense visualization method based on intelligent connected vehicle," in *E3S Web of Conferences*, pp. 1–268, 2021.

[98] J. Bogage, "Scary glitch affects luxury cars," *[online] Available at : <https : / / www . bostonglobe . com / lifestyle / 2016 / 06 / 09 / scary - glitch - affects-luxury-cars/kj4wg2lhphlJDC3gATGuPM/story.html>, [Accessed : 05/03/2021].*

[99] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, *et al.*, "Experimental security analysis of a modern automobile," in *The Ethics of Information Technologies*, pp. 119–134, 2020.

[100] S. Woo, H. J. Jo, and D. H. Lee, "A practical wireless attack on the connected car and security protocol for in-vehicle can," *IEEE Transactions on intelligent transportation systems*, pp. 993–1006, 2014.

[101] C.-W. Lin and A. Sangiovanni-Vincentelli, "Cyber-security for the controller area network (can) communication protocol," in *2012 International Conference on Cyber Security*, pp. 1–7, 2012.

[102] N. Khatri, R. Shrestha, and S. Y. Nam, "Security issues with in-vehicle networks, and enhanced countermeasures based on blockchain," *Electronics*, pp. 893–903, 2021.

[103] I. Rouf, R. D. Miller, H. A. Mustafa, T. Taylor, S. Oh, W. Xu, M. Gruteser, W. Trappe, and I. Seskar, "Security and privacy vulnerabilities of in-car wireless networks : A tire pressure monitoring system case study.," in *USENIX Security Symposium*, pp. 1–10, 2010.

[104] Y. Sun, L. Wu, S. Wu, S. Li, T. Zhang, L. Zhang, J. Xu, Y. Xiong, and X. Cui, "Attacks and countermeasures in the internet of vehicles," *Annals of Telecommunications*, pp. 283–295, 2017.

[105] T. Garg, N. Kagalwalla, P. Churi, A. Pawar, and S. Deshmukh, "A survey on security and privacy issues in iov.," *International Journal of Electrical & Computer Engineering*, pp. 1–10, 2020.

[106] S. Čapkun, A. Francillon, and B. Danev, "Relay attacks on passive keyless entry and start systems in modern cars," *System Security Group*, pp. 1–14, 2011.

[107] B. Lipiński, W. Mazurczyk, K. Szczypiorski, and P. Śmietanka, "Towards effective security framework for vehicular ad-hoc networks," *J. Adv. Comput. Netw.*, pp. 134–140, 2015.

[108] A. Rawat, S. Sharma, and R. Sushil, "Vanet : Security attacks and its possible solutions," *Journal of Information and Operations Management*, pp. 301–304, 2012.

[109] A. Y. Dak, S. Yahya, and M. Kassim, "A literature survey on security challenges in vanets," *International Journal of Computer Theory and Engineering*, pp. 1007–1011, 2012.

[110] R. Baldessari, C. J. Bernardos, and M. Calderon, "Geosac-scalable address autoconfiguration for vanet using geographic networking concepts," in *2008 IEEE 19th*

International Symposium on Personal, Indoor and Mobile Radio Communications, pp. 1–7, 2008.

[111] T. Susan and T. Narten, "Rfc 2462 ipv6 stateless address autoconfiguration," *Ietf. org.*

[112] N. A. Sahloul, L. Benazzouz, and I. Aouini, "Towards an ipsec security geonet architecture," in *2012 Third International Conference on The Network of the Future (NOF)*, pp. 1–5, 2012.

[113] M. N. Mariyasagayam, H. Menouar, and M. Lenardi, "Geonet : A project enabling active safety and ipv6 vehicular applications," in *2008 IEEE International Conference on Vehicular Electronics and Safety*, pp. 312–316, 2008.

[114] G. Mantas, N. Komninos, J. Rodriuez, E. Logota, and H. Marques, "Security for 5g communications," *John Wiley Sons*, pp. 207–220, 2015.

[115] H. Kim, "5g core network security issues and attack classification from network protocol perspective," *J. Internet Services Inf. Secur.*, pp. 1–15, 2020.

[116] S. Namal, M. Liyanage, and A. Gurtov, "Realization of mobile femtocells : operational and protocol requirements," *Wireless personal communications*, pp. 339–364, 2013.

[117] M. Liyanage, P. Kumar, M. Ylianttila, and A. Gurtov, "Novel secure vpn architectures for lte backhaul networks," *Security and Communication Networks*, pp. 1198–1215, 2016.

[118] I. Rouf, R. D. Miller, H. A. Mustafa, T. Taylor, S. Oh, W. Xu, M. Gruteser, W. Trappe, and I. Seskar, "Security and privacy vulnerabilities of in-car wireless networks : A tire pressure monitoring system case study.," in *USENIX Security Symposium*, pp. 1–10, 2010.

[119] B. Mandal, S. Chandra, S. S. Alam, and S. S. Patra, "A comparative and analytical study on symmetric key cryptography," in *2014 International Conference on Electronics, Communication and Computational Engineering (ICECCE)*, pp. 131–136, 2014.

[120] C. Labrado, H. Thapliyal, and S. P. Mohanty, "Fortifying vehicular security through low overhead physically unclonable functions," *arXiv preprint arXiv :2106.02976*, pp. 1–19, 2021.

[121] K. Coelho, D. Damião, G. Noubir, A. Borges, M. Nogueira, and J. Nacif, "Cryptographic algorithms in wearable communications : An empirical analysis," *IEEE Communications Letters*, pp. 1931–1934, 2019.

[122] R. Ahmed Ab M, A. Madani, A. Wahdan, and G. M. Selim, "Design, analysis, and implementation of a new lightweight block cipher for protecting iot smart devices," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–18, 2021.

[123] H. Nunoo-Mensah, K. O. Boateng, and J. D. Gadze, "Tamper-aware authentication framework for wireless sensor networks," *IET Wireless Sensor Systems*, pp. 73–81, 2017.

[124] B. Preneel, "Cryptographic hash functions," *European Transactions on Telecommunications*, pp. 431–448, 1994.

[125] M. Bellare, R. Canetti, and H. Krawczyk, "Keying hash functions for message authentication," in *Annual international cryptology conference*, pp. 1–15, 1996.

[126] S. B. Suhaili and T. Watanabe, "High speed implementation of the keyed-hash message authentication code (hmac) based on sha-1 algorithm," *Advanced Science Letters*, pp. 11096–11100, 2017.

[127] A. Othman and D. Maga, "Relation between security and energy consumption in wireless sensor network (wsn)," in *2018 New Trends in Signal Processing (NTSP)*, pp. 1–8, 2018.

[128] E. Wang, W. Xu, S. Sastry, S. Liu, and K. Zeng, "Hardware module-based message authentication in intra-vehicle networks," in *2017 ACM/IEEE 8th International Conference on Cyber-Physical Systems (ICCPS)*, pp. 207–216, 2017.

[129] M. Müter, A. Groll, and F. C. Freiling, "A structured approach to anomaly detection for in-vehicle networks," in *2010 Sixth International Conference on Information Assurance and Security*, pp. 92–98, 2010.

[130] M. Wolf, A. Weimerskirch, and C. Paar, "Security in automotive bus systems," in *Workshop on Embedded Security in Cars*, pp. 1–13, 2004.

[131] N. Semiconductor, "Automotive gateway : A key component to securing the connected car," *[online] Available at : <https ://www.nxp.com/docs/en/ white-paper/AUTOGWDEVWPUS.pdf>, [Accessed : 3/04/ 2021].*

[132] L. Gallo and J. Harri, *Analytic performance comparison of unsupervised LTE D2D and DSRC in a V2X safety context.* PhD thesis, 2014.

[133] V. Costan and S. Devadas, "Intel sgx explained.," *IACR Cryptol. ePrint Arch.*, pp. 1–118, 2016.

[134] W. Wu, R. Kurachi, G. Zeng, Y. Matsubara, H. Takada, R. Li, and K. Li, "Idh-can : A hardware-based id hopping can mechanism with enhanced security for automotive real-time applications," *IEEE Access*, pp. 54607–54623, 2018.

[135] M. S. U. Alam, *Securing vehicle Electronic Control Unit (ECU) communications and stored data.* PhD thesis, Queen's University (Canada), 2018.

[136] W. Wu, Y. Huang, R. Kurachi, G. Zeng, G. Xie, R. Li, and K. Li, "Sliding window optimized information entropy analysis method for intrusion detection on in-vehicle networks," *IEEE Access*, pp. 45233–45245, 2018.

[137] X. Chen, J. Feng, M. Hiller, and V. Lauer, "Application of software watchdog as a dependability software service for automotive safety relevant systems," in *37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN'07)*, pp. 618–624, 2007.

[138] C. Miller and C. Valasek, "A survey of remote automotive attack surfaces," *black hat USA*, vol. 2014, p. 94, 2014.

[139] H. M. Song, H. R. Kim, and H. K. Kim, "Intrusion detection system based on the analysis of time intervals of can messages for in-vehicle network," in *2016 international conference on information networking (ICOIN)*, pp. 63–68, 2016.

[140] H. Lee, S. H. Jeong, and H. K. Kim, "Otids : A novel intrusion detection system for in-vehicle network by using remote frame," in *2017 15th Annual Conference on Privacy, Security and Trust (PST)*, pp. 57–5709, 2017.

[141] U. E. Larson, D. K. Nilsson, and E. Jonsson, "An approach to specification-based attack detection for in-vehicle networks," in *2008 IEEE Intelligent Vehicles Symposium*, pp. 220–225, 2008.

[142] S. Abbott-McCune and L. A. Shay, "Intrusion prevention system of automotive network can bus," in *2016 IEEE International Carnahan Conference on Security Technology (ICCST)*, pp. 1–8, 2016.

[143] S. Woo, H. J. Jo, and D. H. Lee, "A practical wireless attack on the connected car and security protocol for in-vehicle can," *IEEE Transactions on intelligent transportation systems*, pp. 993–1006, 2014.

[144] X. Fang, J. Wills, J. Granacki, J. LaCoss, and J. Choma, "Cmos charge-metering microstimulator for implantable prosthetic device," in *2008 51st Midwest Symposium on Circuits and Systems*, pp. 826–829, 2008.

[145] P. Mundhenk, S. Steinhorst, M. Lukasiewycz, S. A. Fahmy, and S. Chakraborty, "Lightweight authentication for secure automotive networks," in *2015 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pp. 285–288, 2015.

[146] C.-W. Lin, Q. Zhu, C. Phung, and A. Sangiovanni-Vincentelli, "Security-aware mapping for can-based real-time distributed automotive systems," in *2013 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, pp. 115–121, 2013.

[147] H. Ueda, R. Kurachi, H. Takada, T. Mizutani, M. Inoue, and S. Horihata, "Security authentication system for in-vehicle network," *SEI technical review*, pp. 5–9, 2015.

[148] S. Woo, H. J. Jo, and D. H. Lee, "A practical wireless attack on the connected car and security protocol for in-vehicle can," *IEEE Transactions on intelligent transportation systems*, pp. 993–1006, 2014.

[149] M. S. Idrees, H. Schweppe, Y. Roudier, M. Wolf, D. Scheuermann, and O. Henniger, "Secure automotive on-board protocols : A case of over-the-air firmware updates," in *International Workshop on Communication Technologies for Vehicles*, pp. 224–238, 2011.

[150] J. Lastinec and L. Hudec, "A study of securing in-vehicle communication using ipsec protocol," *Journal of Electrical Engineering*, pp. 89–98, 2021.

[151] G. Jagadamba and B. S. Babu, "Adaptive security schemes based on context and trust for ubiquitous computing environment : A comprehensive survey," *Indian J. Sci. Technol*, pp. 1–9, 2017.

[152] H. Vahdat-Nejad, A. Ramazani, T. Mohammadi, and W. Mansoor, "A survey on context-aware vehicular network applications," *Vehicular Communications*, pp. 43–57, 2016.

[153] G. D. Abowd, A. K. Dey, P. J. Brown, N. Davies, M. Smith, and P. Steggles, "Towards a better understanding of context and context-awareness," in *International symposium on handheld and ubiquitous computing*, pp. 304–307, 1999.

[154] B. Schilit, N. Adams, and R. Want, "Context-aware computing applications," in *1994 First Workshop on Mobile Computing Systems and Applications*, pp. 85–90, 1994.

[155] N. S. Ryan, J. Pascoe, and D. R. Morse, "Enhanced reality fieldwork : the context-aware archaeological assistant," in *Computer applications in archaeology*, pp. 1–8, 1998.

[156] A. Smitha, M. M. Pai, N. Ajam, and J. Mouzna, "An optimized adaptive algorithm for authentication of safety critical messages in vanet," in *2013 8th International Conference on Communications and Networking in China (CHINACOM)*, pp. 149–154, 2013.

[157] M. Villarreal-Vasquez, B. Bhargava, and P. Angin, "Adaptable safety and security in v2x systems," in *2017 IEEE International Congress on Internet of Things (ICIOT)*, pp. 17–24, 2017.

[158] E. B. Hamida, M. A. Javed, and W. Znaidi, "Adaptive security provisioning for vehicular safety applications," *International Journal of Space-Based and Situated Computing*, pp. 16–31, 2017.

[159] M. A. Javed, S. Zeadally, M. Usman, and G. A. S. Sidhu, "Faspm : Fuzzy logic-based adaptive security protocol for multihop data dissemination in intelligent transport systems," *Transactions on Emerging Telecommunications Technologies*, pp. 1–28, 2017.

[160] E. Ferrera, R. Rossini, D. Conzon, S. Tassone, and C. Pastrone, "Adaptive security framework for resource-constrained internet-of-things platforms," in *2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, pp. 1–5, 2016.

[161] E. Romero, J. Blesa, and A. Araujo, "An adaptive energy aware strategy based on game theory to add privacy in the physical layer for cognitive wsns," *Ad Hoc Networks*, pp. 1–92, 2019.

[162] L. Liang, "Abnormal detection of electric security data based on scenario modeling," *Procedia computer science*, pp. 578–582, 2018.

[163] X. Liang and Y. Xiao, "Game theory for network security," *IEEE Communications Surveys & Tutorials*, pp. 472–486, 2012.

[164] A. Kayes, W. Rahayu, P. Watters, M. Alazab, T. Dillon, and E. Chang, "Achieving security scalability and flexibility using fog-based context-aware access control," *Future Generation Computer Systems*, pp. 307–323, 2020.

[165] H. Wang and C. Bao, "Scenario modeling of ecological security index using system dynamics in beijing-tianjin-hebei urban agglomeration," *Ecological Indicators*, pp. 1–125, 2021.

[166] H. Saidi, D. Gretete, and A. Addaim, "Game theory for wireless sensor network security," in *Fourth International Congress on Information and Communication Technology*, pp. 259–269, 2020.

[167] W. Li, T. Song, Y. Li, L. Ma, J. Yu, and X. Cheng, "A hierarchical game framework for data privacy preservation in context-aware iot applications," in *2017 IEEE Symposium on Privacy-Aware Computing (PAC)*, pp. 176–177, 2017.

[168] W. Aman and F. Kausar, "Towards a gatewaybased context-aware and self-adaptive security management model for iot-based ehealth systems," *INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS*, pp. 280–287, 2019.

[169] P. Pradeep, S. Krishnamoorthy, and A. V. Vasilakos, "A holistic approach to a context-aware iot ecosystem with adaptive ubiquitous middleware," *Pervasive and Mobile Computing*, pp. 1–72, 2021.

[170] A. Ayyagari, T. M. Aldrich, D. E. Corman, G. M. Gutt, and D. A. Whelan, "Context aware network security monitoring for threat detection," 2015.

[171] C. Fiori, K. Ahn, and H. A. Rakha, "Power-based electric vehicle energy consumption model : Model development and validation," *Applied Energy*, pp. 257–268, 2016.

[172] I. Sagaama, A. Kchiche, W. Trojet, and F. Kamoun, "Improving the accuracy of the energy consumption model for electric vehicle in sumo considering the ambient temperature effects," in *2018 IFIP/IEEE International Conference on Performance Evaluation and Modeling in Wired and Wireless Networks (PEMWN)*, pp. 1–6, 2018.

[173] M. Chen, Y. Tian, G. Fortino, J. Zhang, and I. Humar, "Cognitive internet of vehicles," *Computer Communications*, pp. 58–70, 2018.

[174] A. A. Abd El-Latif, B. Abd-El-Atty, S. E. Venegas-Andraca, H. Elwahsh, M. J. Piran, A. K. Bashir, O.-Y. Song, and W. Mazurczyk, "Providing end-to-end security using quantum walks in iot networks," *IEEE Access*, pp. 92687–92696, 2020.

[175] W. J. Fleming, "New automotive sensors—a review," *IEEE Sensors Journal*, pp. 1900–1921, 2008.

[176] S. Abdelhamid, H. S. Hassanein, and G. Takahara, "Vehicle as a mobile sensor," *Procedia Computer Science*, pp. 286–295, 2014.

[177] J. Guerrero-Ibáñez, S. Zeadally, and J. Contreras-Castillo, "Sensor technologies for intelligent transportation systems," *Sensors*, pp. 1–18, 2018.

[178] H. Vahdat-Nejad, A. Ramazani, T. Mohammadi, and W. Mansoor, "A survey on context-aware vehicular network applications," *Vehicular Communications*, pp. 43–57, 2016.

[179] K. Hu, J. Wu, and T. Schwanen, "Differences in energy consumption in electric vehicles : An exploratory real-world study in beijing," *Journal of Advanced Transportation*, pp. 1–17, 2017.

[180] A. Y. Lam, Y.-W. Leung, and X. Chu, "Electric vehicle charging station placement : Formulation, complexity, and solutions," *IEEE Transactions on Smart Grid*, pp. 2846–2856, 2014.

[181] D. He, S. Chan, and M. Guizani, "Cyber security analysis and protection of wireless sensor networks for smart grid monitoring," *IEEE Wireless Communications*, pp. 98–103, 2017.

[182] S. Bansal and D. Kumar, "Iot ecosystem : A survey on devices, gateways, operating systems, middleware and communication," *International Journal of Wireless Information Networks*, pp. 1–25, 2020.

[183] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuéllar, P. H. Drielsma, P.-C. Héam, O. Kouchnarenko, J. Mantovani, *et al.*, "The avispa tool for the automated validation of internet security protocols and applications," in *International conference on computer aided verification*, pp. 281–285, 2005.

[184] Y. Glouche, T. Genet, O. Heen, and O. Courtay, "A security protocol animator tool for avispa," in *ARTIST2 workshop on security specification and verification of embedded systems, Pisa*, pp. 1–44, 2006.

[185] Omnetpp.org, "Omnet++ discrete event simulator," *[online] Available at : <https ://omnetpp.org/>, [Accessed : le 3/05/ 2021].*

[186] omnet++, "Framework inet," *[online] Available at : <https ://omnetpp.org/download-items/INET.html>, [Accessed : 3/05/ 2021].*

[187] D. D. Hwang, B.-C. C. Lai, and I. Verbauwhede, "Energy-memory-security tradeoffs in distributed sensor networks," in *2004 International Conference on Ad-Hoc Networks and Wireless*, pp. 70–81, 2004.

[188] X. Yang, C. Yang, C. Yang, T. Peng, Z. Chen, Z. Wu, and W. Gui, "Transient fault diagnosis for traction control system based on optimal fractional-order method," *ISA transactions*, pp. 365–375, 2020.

[189] A. Marotta, G. Carrozza, L. Battaglia, P. Montefusco, and V. Manetti, "Applying the secram methodology in a cloud-based atm environment," in *2013 International Conference on Availability, Reliability and Security*, pp. 807–813, 2013.

[190] A. Ruddle, D. Ward, B. Weyl, M. S. Idrees, Y. Roudier, M. Friedewald, T. Leimbach, A. Fuchs, S. Gurgens, O. Henniger, *et al.*, *Security requirements for automotive on-board networks based on dark-side scenarios, Deliverable D2. 3*. PhD thesis, Telecom ParisTech, 2010.

[191] Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy," *IEEE Transactions on Intelligent Transportation Systems*, pp. 760–776, 2018.

[192] D. Huang, X. Hong, and M. Gerla, "Situation-aware trust architecture for vehicular networks," *IEEE Communications Magazine*, pp. 128–135, 2010.

[193] B. Gong, J. Liu, and S. Guo, "A trusted attestation scheme for data source of internet of things in smart city based on dynamic trust classification," *IEEE Internet of Things Journal*, pp. 1–1, 2020.

[194] Y. Liu, M. Xiao, Y. Zhou, D. Zhang, J. Zhang, H. Gacanin, and J. Pan, "An access control mechanism based on risk prediction for the iov," in *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, pp. 1–5, 2020.

[195] H. Atlam, A. Alenezi, R. Walters, G. Wills, *et al.*, "An overview of risk estimation techniques in risk-based access control for the internet of things," pp. 1–8, 2017.

[196] H. F. Atlam and G. B. Wills, "An efficient security risk estimation technique for risk-based access control model for iot," *Internet of Things*, pp. 1–6, 2019.

[197] H. F. Atlam, A. Alenezi, R. K. H. Hussein, and G. Wills, "Validation of an adaptive risk-based access control model for the internet of things," *International Journal of Computer Network and Information Security*, pp. 26–35, 2018.

[198] S. Gupta, A. Buriro, and B. Crispo, "Driverauth : A risk-based multi-modal biometric-based driver authentication scheme for ride-sharing platforms," *Computers & Security*, pp. 122–139, 2019.

[199] D. Hintze, E. Koch, S. Scholz, and R. Mayrhofer, "Location-based risk assessment for mobile authentication," in *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing : Adjunct*, pp. 85–88, 2016.

[200] A. Arfaoui, A. Kribeche, S. M. Senouci, and M. Hamdi, "Game-based adaptive risk management in wireless body area networks," in *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)*, pp. 1087–1093, 2018.

[201] R. M. Savola, H. Abie, and M. Sihvonen, "Towards metrics-driven adaptive security management in e-health iot applications.," in *BODYNETS*, pp. 276–281, 2012.

[202] H. Abie and I. Balasingham, "Risk-based adaptive security for smart iot in ehealth," in *Proceedings of the 7th International Conference on Body Area Networks*, pp. 269–275, 2012.

[203] M. T. Gebrie and H. Abie, "Risk-based adaptive authentication for internet of things in smart home ehealth," in *Proceedings of the 11th European Conference on Software Architecture : Companion Proceedings*, pp. 102–108, 2017.

[204] J. T. Matamalas Llodrà, "Evolutionary game theory in complex interconnected networks," Master's thesis, Universitat Politècnica de Catalunya, 2014.

[205] A. R. Sfar, Y. Challal, P. Moyal, and E. Natalizio, "A game theoretic approach for privacy preserving model in iot-based transportation," *IEEE Transactions on Intelligent Transportation Systems*, pp. 4405–4414, 2019.

[206] S. Rass and S. Schauer, "Game theory for security and risk management," *Springer International Publishing*, pp. 978–988, 2018.

[207] M. Hamdi and H. Abie, "Game-based adaptive security in the internet of things for ehealth," in *2014 IEEE International Conference on Communications (ICC)*, pp. 920–925, 2014.

[208] C. Xiaolin, T. Xiaobin, Z. Yong, and X. Hongsheng, "A markov game theory-based risk assessment model for network information system," in *2008 International Conference on Computer Science and Software Engineering*, pp. 1057–1061, 2008.

[209] H. Vangheluwe, "The discrete event system specification (devs) formalism," *tech. rep*, pp. 1–10, 2001.

[210] N. Ruan and Y. Hori, "Dos attack-tolerant tesla-based broadcast authentication protocol in internet of things," in *2012 International Conference on Selected Topics in Mobile and Wireless Networking*, pp. 60–65, IEEE, 2012.

[211] H.-l. LIU, S.-y. ZHU, Z.-j. LU, Z.-l. LIU, *et al.*, "Practical contactless attacks on hitag2-based immobilizer and rke systems," *DEStech Transactions on Computer Science and Engineering*, no. CCNT, 2018.

Annexe A

Résultats de simulation : Equilibre de Nash

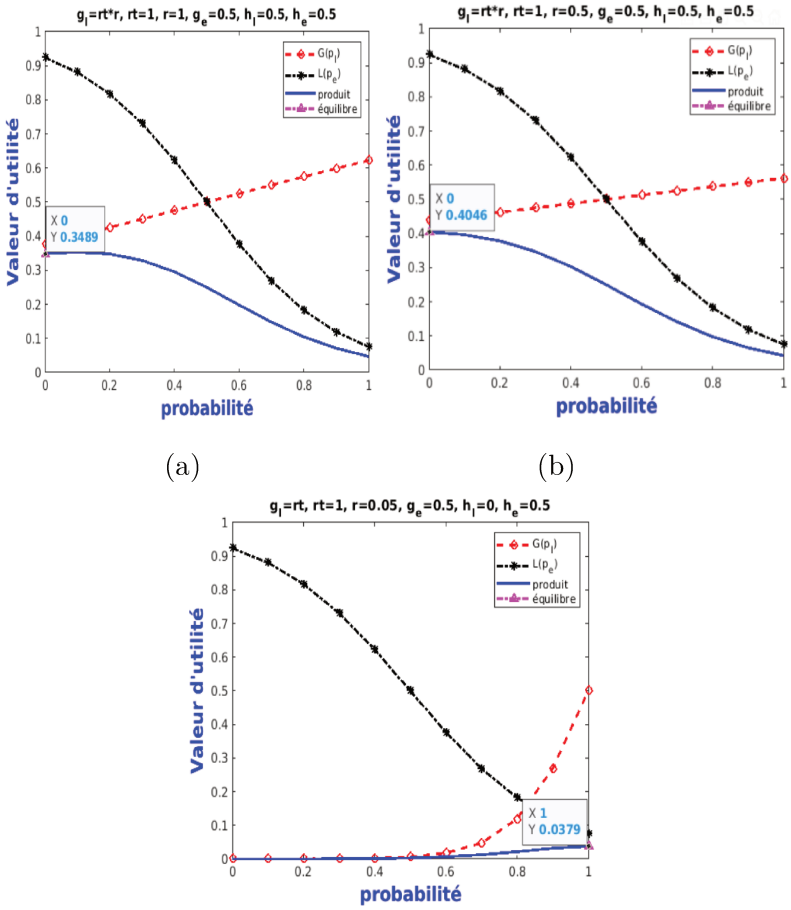


FIG. A.1 : Equilibre de Nash pour confiance=1 et batterie en zone orange

.

Annexe B

Résultats de simulation : confiance faible

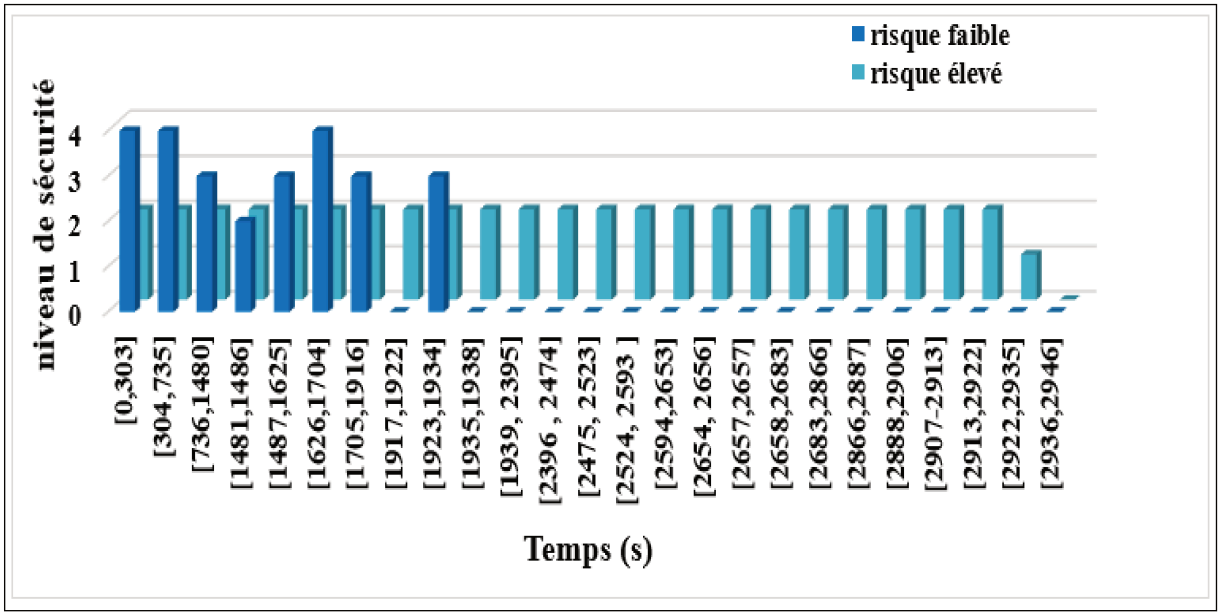


FIG. B.1 : Adaptation par rapport au contexte : confiance faible

Pour un trust faible, on peut conclure que les résultats de RICAV ressemblent aux résultats de CASIEV si le risque est faible tout a long du trajet. Dans le cas contraire, si le risque est élevé/moyen RICAV est plus efficace en termes de consommation énergétique et robustesse.

Dans ce scénario, nous considérons une confiance élevée (confiance=10) et une confiance faible (confiance=1). De même, nous considérons une zone où le risque est soit variable, en se basant sur un trafic routier réelle. La figure 4 montre l'adaptation de la sécurité par rapport au contexte pour un trust élevé est supérieur au temps d'activation avec une confiance faible. De même, le temps d'activation du niveau adéquat au niveau d'un trust élevé est supérieur à celui d'une confiance faible.

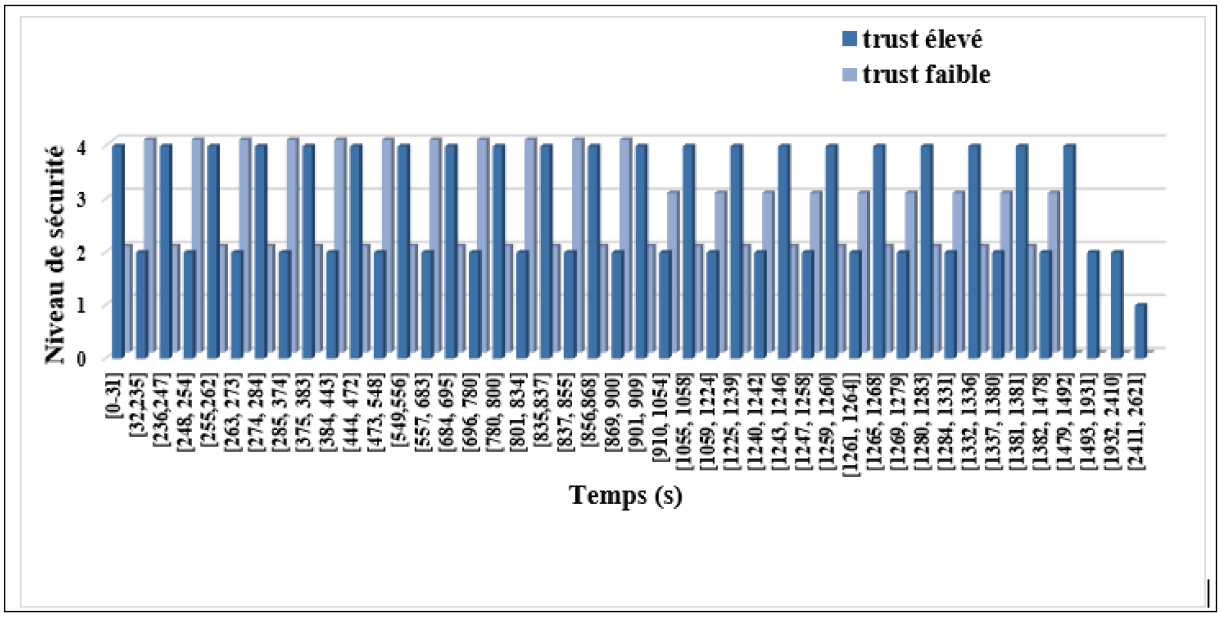


Fig. B.2 : Adaptation par rapport au contexte : confiance faible, elevée et risque variable