République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université A. Mira de Béjaïa
Faculté des Sciences Exactes
Département d'Informatique

Mémoire de Fin de Cycle

En vue de l'obtention du diplôme de Master Recherche en Informatique

Option : Réseaux et Systémes Distribués

Thème

Authentification biométrique d'un conducteur dans les STIs

Réalisé par

M^{lle} BOURKEB Lina
M^{lle} ZIZI Kahina

Devant le jury composé de

Président :	M. MOHAMMEDI Mohamed	M.C.B	Université de Béjaïa
Examinateur :	M. KACIMI Farid	M.A.B	Université de Béjaïa
Examinateur :	M. BELHOCINE Sid Ali	Doctorant	Université de Béjaïa
Encadrant :	M. AISSANI Sofiane	M.C.A	Université de Béjaïa
Co-Encadrante :	M^{lle} ZAMOUCHE Djamila	Doctorante	Université de Béjaïa

Remerciements

Au terme de ce travail, nous tenons à exprimer notre profonde gratitude et nos sincères remerciements.

Nous remercions le dieu le tout puissant de nous avoir donné la force, la volonté de donner le meilleur de nous-même et le courage de mener ce travail.

Nous tenons en premier lieu à exprimer notre profonde reconnaissance à notre encadreur **M. AISSANI Sofiane**, pour son encadrement au sens propre du terme, puis pour nous avoir fait confiance et pour nous avoir accompagné, encouragé et conseillé au cours de notre cursus .
Nous tenons à remercier très chaleureusement notre Co-ecadrante Mme **ZAMOUCHE Djamila** pour sa collaboration importante pendant la rédaction de ce mémoire, ses encouragements et ses conseilles.
Nous tenons également à remercier les membres du jury d'avoir consacré leurs temps à la lecture et à la correction de ce mémoire .
Nous remerciements les plus vifs vont tout particulièrement à nos parents, en qui nous avons puisé tout le courage, la volonté et la confiance, nous leur serons éternellement reconnaissants.
Enfin, Nous n'omettrons jamais d'exprimer toute notre gratitude à tous les membres du département d'Informatique de l'Université de Béjaia, que ce soit enseignants ou cadres administratifs, qui de près ou de loin n'ont épargné aucun effort pour que notre formation et nos travaux se terminent dans de bonnes conditions.

Dédicaces

Je dédie ce mémoire

A mes chers parents que nulle dédicace ne puisse exprimer mes sincères sentiments et mon éternelle gratitude, pour leur patience illimitée, leurs encouragements continus, leur aide, en témoignage de mon profond amour et respect pour leurs grands sacrifices

A ma sœurs : Amel

A mes frères : Fayssel et Lyes

Ma belle-sœur : Katia et mon beaux-frères : Djamel pour leur soutien, compréhension et qui n'ont cessé d'être présents pour moi.

Sans oublier **mes chers grands parents** et **mes oncles** A **mes amies et amis exceptionnellement :Fatah, Tinhinane, Milane, Lina, Nina, Dyhia, litissia Kayssa** ,

A mon encadreur M. AISSANI Sofiane

et à **ma Co-encadrante Mme ZAMOUCHE Djamila** et tous ceux qui me connaissent de loin ou de près.

Kahina

Dédicaces

Je dédie ce mémoire

A mes chers parents que nulle dédicace ne puisse exprimer mes sincères sentiments et mon éternelle gratitude, pour leur patience illimitée, leur encouragement continu, leur aide, en témoignage de mon profond amour et respect pour leurs grands sacrifices.

A mon frère : Youba

pour son soutien, compréhension et qui n'a cessé d'être présent pour moi.

A **mes chers grands parents** et **A toute ma famille.**

A **mes amis et amies exceptionnellement :Yacine, Kahina,Tinhinane,Lylia,Célia**,

A mon encadreur M. AISSANI Sofiane

et **ma Co-encadrante Mme ZAMOUCHE Djamila** et à tous ceux qui me connaissent de loin ou de près.

Lina

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

ACP	Algebra of Communicating Processes.
BPA	Basic Process Algébra.
CCS	Calculus of Communicating Systems.
CSP	Communicating Sequential Processes.
DSRC	Dedicated Short-Range Communications.
ECG	ÉlectroCardioGramme
FAR	False Acceptance Rate
FRR	False Rejection Rate
FRS	Face Recognition System.
GMM	Gaussian mixture model.
GPS	Global Positioning System.
GSM	Global System for Mobile.
IDE	Integrated Development Environment
JDK	Java développement Kit
LCD	Liquid Crystal Display
LOTOS	Language Of Temporal Ordering Specification.
OBD	On BoarD unit
PA	Process Algebra.
PID	Proportionnel Intégral Dérivé
SGB	Système de Gestion de Bases de Donnée
SMS	Short Message Service.
STI	Systéme de Transport Intelligent.
SVM	Support Vector Machine

Introduction générale

De nos jours, se déplacer est devenu un aspect essentiel de la vie quotidienne, qu'il s'agisse de transports en commun ou de véhicules personnels. Le transport est devenue l'une des principales pierres angulaires de la civilisation humaine qui facilite le mouvement des personnes et des marchandises d'un endroit à un autre. Les gens utilisent régulièrement plusieurs modes de transport, comme le transport routier, aérien, férroviaire et maritime pour leurs activités quotidiennes. L'augmentation de la population mondiale et l'urbanisation dans le monde poussent les systèmes de transport à devenir intelligents en lui intégarant de nouvelle fonctionalité. Cependant, une telle intégration impose des défis majeurs dans la surveillance, le contrôle et la sécurité. L'idée de l'intégration des technologies virtuelles est une innovation dans le domaine des transports et elle joue un rôle vital pour surmonter les problèmes du monde global.

Les systèmes de transport intelligents ont un potentiel important pour l'amélioration de la vie quotidienne, mais malheureusement ces systémes souffent d'un nombre important de problémes de sécurité. Le majeur probléme est l'authentification. De nombreuses technologies ont été développées pour améliorer la sécurité des véhicules ainsi que leurs conducteurs. Ces problémes ont attiré de nombreux chercheurs à investir beaucoup d'efforts afin de développer des systémes de sécurité basés sur des différentes techniques qui permettent de résoudre ces problèmes. La reconnaissance biométrique a été une des solutions les plus appropriées pour les applications nécessitant une haute sécurité

Les technologies biométriques couvrent un large ensemble de techniques permettant d'identifier les personnes et d'automatiser l'authentification de leur identité en utilisant les caractéristiques physiques qui se basent sur de mesures directs du corps humains ou des caractéristiques comportementales qui se basent sur des données dérivées d'une action et mesurent donc indirectement les caractéristiques du corps humain des personnes concernées. L'un des buts de la biométrie est la protection des personnes contre la fraude ou le vol. L'avantage de cette identification est l'unicité des caractéristiques utilisées, en effet chaque personne a ses propres traits biométriques qui ne peuvent être changées, perdues ou volées.

Le travail de ce mémoire s'inscrit dans le contexte d'authentification d'un conducteur, tout en

se basant sur la biométrie comportementale. Nous nous intéressons à l'utilisation d'une méthode mathématique qui est l'algébre de processus pour la modélisation d'un comportement sous forme d'un processus. Un état de l'art sur ce contexte a été élaboré ce qui nous a mené à concevoir notre nouvelle solution. Notre proposition consiste à construire un modéle pour chaque conducteur sous forme de processus qui sera comparé à un modéle de référence. L'evaluation de performances de la méthode proposée est réalisée par des simulation, les résultats de cette simulation ont prouvé l'efficacité de notre approche.

Ce mémoire est organisé en trois chapitres. Le premier chapitre portera sur des généralités des systèmes de Transport Intelligents, la biométrie ainsi que sur les concepts de l'algèbre de processus. Le deuxiéme chapitre présente un état de l'art sur les systémes d'authentification ainsi qu'une comparaison sur ses différents systémes selon des critéres fixés. Le troisième chapitre est composé de deux parties, dans la premiére partie nous présenterons en détail les différentes phases de notre proposition. Afin de prouver l'efficacité de notre proposition, nous présenterons dans la deuxiéme partie notre éxpérimentation et les résultats de notre simulation. Une conclusion suivie de perspectives clôtureront notre mémoire.

Chapitre 1

Pré-requis théoriques

1.1 Introduction

Traditionnellement, l'utilisation des caractéristiques personnelles comme les marques traditionnelle (mot de passe) utilisés pour valider l'identité d'une personne n'est pas une solution d'authentification fiable. Les limites de ces approches traditionnelles ne conviennent pas à l'authentification personnelle dans le monde moderne. Il est donc recommandé de développer des méthodes d'authentification personnelle plus cohérentes pour contrôler la criminalisation et la fraude quotidienne. Afin de surmonter la difficulté de la gestion de ces marque et d'améliorer la convivialité des systèmes d'authentification traditionelle, la biométrie rentre dans le domaine technologique qui permet de traiter la vérification d'identité des personnes à l'aide de leurs caractéristiques individuelles. L'authentification biométrique a été largement étudiée et a attiré une attention particulière dans le monde universitaire que dans l'industrie, elle constitue un lien fort et permanent entre une personne physique et son identité. De nombreux systèmes d'authentification biométriques ont été étudiés, développés et mise en oeuvre à l'aide de différentes techniques et méthodes, en particuliers pour les systèmes de transport intelligents qui sont devenus une technologie prometteuse qui pourrait tôt ou tard révolutionner notre vie.

Dans ce chapitre nous introduirons quelques notions et définitions de base qu'on aura besoin durant notre travail ce dérnier est décomposé en trois partie, on commencera par l'introduction sur la biométrie, puis présenter les Systémes de Transport Intelligent (STI) et on finira par la présentation d'une méthode formelle qui est l'Algébre de processus.

1.2 Systéme de transport intélligent (STIs)

1.2.1 Définition des STIs

Systéme de transport intélligent (STI) est un système complet de gestion des services de transport, il est dit intelligent car il se base sur des fonctions liées à l'intelligence comme le traitement de l'information, il permet ainsi de traiter, d'analyser et de communiquer des informations relatives à ce service. La gamme des technologies considérées comprend toutes les applications de la télématique au domaine du transport, utilisant notamment l'électronique embarquée ou fixe (ex : capteurs, moyens de calcul), les télécommunications, les bases de données et d'information, les systèmes de régulation, les paiements électroniques [1].

Tous les modes de transport routier, ferroviaire, aérien, maritime sont visés par ces applications, tant pour la sécurité ou la régulation des flux de la circulation que pour l'information des usagers des transports en commun ou des usagers du transport des marchandises. Notre étude se consacre pour les systèmes de transports routiers [1].

1.2.2 Problémes liés aux STIs

En raison du nombre croissant de véhicules, la route devient saturée. À mesure que la situation s'agrave, de plus en plus de problèmes sont exposés. Certains problèmes sont anciens, comme la congestion, tandis que d'autres sont nouveaux comme les impacts environnementaux. Parmi les problèmes de transport les plus notables figurent [1] :

- Congestion du trafic.
- Impacts environnementaux.
- Consommation d'énergie.
- Accidents et sécurité.
- Coûts de maintenance élevés.
- Vol.

1.2.3 Objectifs des STIs

Les STIs ont pour objectif de répondre à des problèmes de société ciblés sur l'utilisation des transports. Ils sont donc ancrés dans un contexte d'amélioration des systèmes autant pour les usagers, que pour les conducteurs et les gestionnaires.
Les STIs sont présents principalement dans la gestion de congestion du trafic routier et dans le développement de nouvelles technologies de l'information embarquées dans les véhicules.

Les STI connaissent de nombreuses applications dont [1] :

— L'amélioration de la sécurité du réseau de transports.
— La réduction de l'encombrement et l'amélioration de la mobilité.
— L'accroissement de la productivité économique.
— La réduction du temps de déplacement et des coûts pour le gouvernement, le voyageur et l'exploitant.
— L'amélioration de l'efficacité énergétique et la réduction des effets sur l'environnement.
— L'amélioration de l'exploitation du système de transport par divers moyens.
— La Réduction de la pollution engendrée par les véhicules.
— L'amélioration du confort et de la sécurité des biens et des personnes et l'optimisation de la gestion des infrastructures.
— Minimisation des menaces relatives à la sûreté et à la sécurité des déplacements.

1.2.4 Techniques utilisées par les STIs

Le système de transport intelligent (STI) est un système de transport qui permet aux véhicules de fonctionner en douceur pendant son trajet et offre la sécurité et le confort à un véhicule individuel ou à un réseau de véhicules en utilisant des techniques avancées qui peuvent être appliquées pour chaque mode de transport, à savoir, routes, chemins de fer, eau ou air, telles que [2] :

— Le système de positionnement mondial (GPS).
— Le système mondial de navigation par satellite (GNSS).
— Le système coopératif de transport intelligent (C-ITS).
— Communications dédiées à courte portée (DSRC).
— Les réseaux sans fil qui sont accessibles aux communications entre les véhicules et la route.
— Les réseaux téléphoniques de troisième ou quatrième génération (3G ou 4G).
— Balises hyperfréquences ou infrarouges pour transmettre le trafic en temps réel.
— La reconnaissance d'image.

1.3 Biométrie et Sécurité

1.3.1 Définition de la biométrie

Le terme biométrique vient des mots grecs bios (vie) et metrikos (mesure) [3], la biométrie est définie comme étant un ensemble des techniques informatiques visant à reconnaître automatiquement un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales. Ces caractéristiques sont utilisés pour identifier et authenifier chaque être humain. Les données biométriques sont des données à caractère personnel. Elles ont, pour la plupart, la particularité

d'être uniques et permanentes, elles se rapprochent ainsi de ce qui pourrait être défini comme un « identificateur unique universel » [4].

1.3.2 Modalités biométriques

On peut classer les techniques biométriques en trois catégories (voir la Figure 1.1) :

1. **Biométrie physiologique :** elle se base sur les traits physiques particuliers qui pour toutes personnes, sont permanents et uniques (empreinte digitale, visage, forme de la main, etc.) [5] .

2. **Biométrie comportementale :** Cette categorie se base sur l'analys edu comportement d'un individu [6] comme la dynamique de signature, sa demarche, sa facon de taper au clavier et sa voix [7].

3. **Analyse des traces biologiques :** Cette categorie s'appuie sur l'analyse de caracteristiques biologiques de l'individu (salive, ADN, etc.) [5].
   Cette modalité n'est pas beaucoup utilisée pour du contole d'accèes logique et physique. Nous ne détaillons pas plus sur ce type.

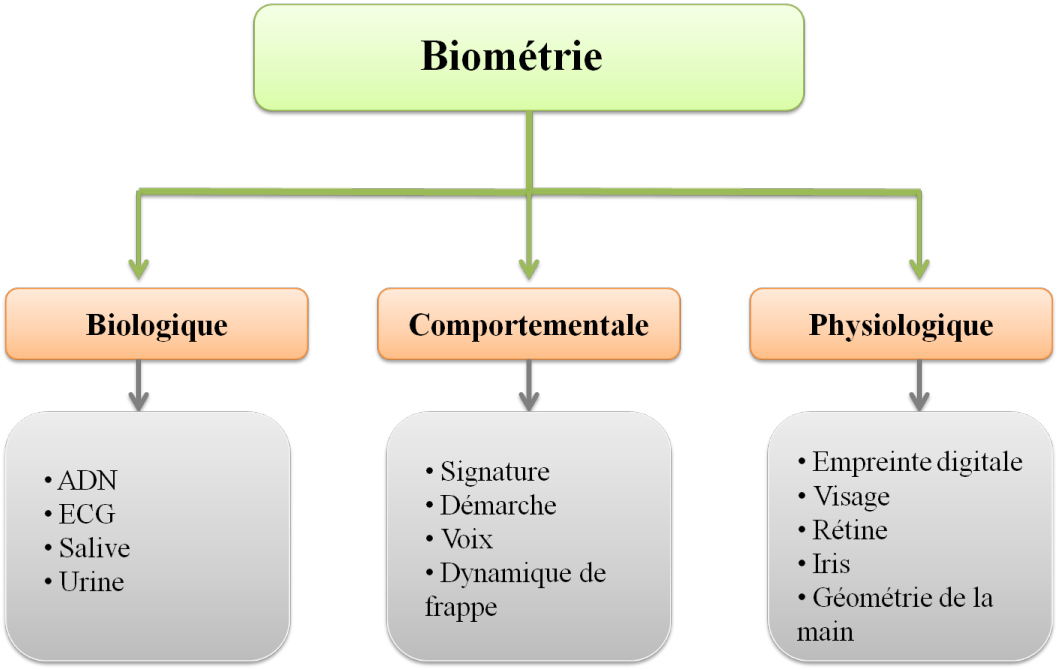

FIGURE 1.1 – Classification des modalités .
[8]

1.3.3 Propriétés souhaitées dans une caractéristique biométrique

En théorie, la plupart des traits physiologiques ou comportementaux humains peuvent être utilisés en tant que modalités biométriques. Quoiqu'il en soit, ces techniques ont en commun la qualité des caractéristiques collectées [5] :

- **Universelles**, elles doivent exister, naturellement, chez tous les individus.
- **Uniques**, permettant ainsi de différencier un individu par rapport à un autre.
- **Permanentes**, autorisant l'évolution dans le temps.
- **Mesurables**, autorisant une comparaison future infalsifiables.
- **Invariance**, les caractéristiques doivent être constantes sur une longue période de temps. Elles ne doivent pas être soumises à des différences significatives liées à l'âge.

1.3.4 Application de la biométrie

1.3.4.1 Contrôle d'accés

Le contrôle d'accès biométrique est une méthode qui consiste à utiliser des données morphologiques ou biologiques pour accorder ou refuser l'accès à des locaux de tous types mais aussi sécuriser l'accès à des stations informatiques et aux dossiers et fichiers présents sur ces dernières [9]. Il existe de nombreux systèmes biométriques pour le contrôle d'accès que nous pouvons séparer en deux grandes familles : avec contact (physique) ou sans contact (virtuel) .

1.3.4.2 Authentification

L'authentification biométrique est un processus de sécurité qui repose sur les caractéristiques biométriques uniques d'un individu pour apporter la preuve de sa propre identité. Les systèmes d'authentification biométrique comparent une capture de données biométriques à des données authentiques confirmées stockées dans une base de données. Si les deux échantillons des données biométriques correspondent, l'authentification est confirmée [10] .

1.3.4.3 Criminologie

La criminologie est l'étude scientifique de la criminalité et des criminels et leurs motivations pour les phénomènes émotionnels ou de personnalité anormaux qui soulignent des symptômes. Plusieurs méthodes ont été utilisées pour identifier les criminels dont l'utilisation de la biométrie qui a été présentée comme une solution miracle pour lutter contre ce phénoméne.

1.3.5 Menaces sur un modéle biométrique

Bien que la biométrie puisse améliorer la sécurité dans différents environnements et servir à de nombreuses fins, les systèmes biométriques, comme tout autre système de sécurité, présentent des vulnérabilités et sont sensibles aux menaces.

1. **Le risque de détournement d'usage**
   Les données peuvent contenir beaucoup plus de renseignements personnels que l'unique mesure captée. Par exemple, la lecture de l'iris et de la démarche peuvent indiquer une maladie ou un handicap [11].

2. **Le risque de vol et d'usurpation d'identité**
   Les données biométriques ne sont pas entièrement privées, car il est possible de s'approprier certaines données, telles que celles du visage, de l'iris, les empreintes digitales,etc... Cette particularité des données biométriques rend leurs utilisation risquées. Contrairement à un mot de passe que l'on peut retenir et qui demeure confidentiel, les données biométriques ne sont pas réellement secrètes et peuvent être collectées pour s'accaparer l'identité d'autrui [8].
   l'identité peut être usurper soit par le contournement de l'image biométrique, avant sa conversion en gabarit pour qu'elle soit comparer, ou aussi lors de la réussite d'un pirate à accéder à une base de données et à y insérer ses propres caractéristiques biométriques, associées aux renseignements personnelles d'une autre personne [11].

3. **Attaque de récupération d'échantillons**
   Dans ce type d'attaque, l'objectif de l'adversaire est de déterminer un nouveau modèle biométrique accepté par le serveur d'authentification. Elle peut étre effectuer en deux manières différentes [12] :

   — Via l'usurpation de modèle (par exemple, en extrayant l'empreinte digitale laissée sur un verre).
   — Via des techniques de force brute en se basant sur l'utilisation d'une parodie d'un trait biométrique. Cette parodie fait référence à un faux ou à un modèle biométrique artificiel qui ne correspond pas à une personne vivante. Par exemple, les doigts gommeux, des empreintes digitales résiduelles d'utilisateurs légitimes, des photographies d'utilisateurs légitimes ou des enregistrements vocaux d'utilisateurs légitimes,...etc.

4. **Attaque de récupération de référence biométrique**
   Elle s'agit de la menace la plus nuisible, elle permet de récupérer le modèle de référence (texte en clair).

Dans cette attaque, l'adversaire peut obtenir un accès non autorisé à tout système qui utilise comme modèle de référence et également collecter des informations sensibles sur les caractéristiques physiques.

5. **Traçabilité et distinction des utilisateurs**
   Cette attaque ne s'intéresse pas à la vie privée de l'utilisateur ni à collecter des informations sur les données biométrique, mais plutôt à profiler et identifier l'utilisateur cible parmi tous les utilisateurs d'un ou plusieurs systèmes biométriques.

   — Traçabilité : La principale stratégie pour tracer les utilisateurs s'appuit sur les différents droits d'accés que l'attaquant posséde aux différentes bases de données et cela en retracant les tentatives d'authentification d'un utilisateur et en vérifiant quel enregistrement de la base de données est interrogé [12].

   — Distinction : La distinction de l'utilisateur peut être considérée comme un suivi de l'utilisateur sur différentes tentatives d'authentification dans le même système ou dans des systèmes d'authentification différents. Autrement dit, l'attaquant peut reconnaître l'utilisateur cible parmi les autres utilisateurs présents dans le système d'authentification biométrique [12].

1.3.6 Identification et authentification biométrique

La biométrie peut fonctionner en deux modes distincts : en mode de vérification (authentification) ou en mode d'identification.

— **Authentification :** appelée également vérification, est le processus qui fait réference à une vérification automatique d'une personne basée sur des données biométriques spécifiques en comparant les caractéristiques provenant d'une personne, au modèle de référence biométrique de cette dernière, afin de déterminer la ressemblance [13].

— **Identification :** consiste à déterminer l'identité d'une personne. Il s'agit de saisir une donnée biométrique de cette personne. Ces données sont ensuite comparées aux données biométriques de plusieurs autres personnes qui figurent dans une base de données [13].

1.4 Algébre de processus

Les méthodes formelles sont incontournables pour la spécification et l'analyse des systèmes informatiques dans le but d'augmenter le niveau de sécurité. On appelle outils formels les mathé-

matiques appliquées à la modélisation et à l'analyse des systèmes informatiques. L'objectif d'utilisation des outils formels est de modéliser le système que l'on veut étudier. Le niveau d'abstraction adopté pour modéliser le système doit dépendre des propriétés qu'on veut étudier. Plusieurs méthodes formelles ont été adaptées ou développées dans le but de décrire mathématiquement, sans ambigüité des systèmes informatiques [14].

1.4.1 Définition d'algébre de processus

Les algèbres de processus sont un formalisme mathématique pour la description et l'étude des systèmes distribués ou parallèles par des moyens algébriques. Elles permettent de modéliser le fonctionnement des processus complexes en termes d'actions qu'ils peuvent réaliser [15]. Comme tout les langages formelles, l'algèbre de processus admet des régles syntaxiques et sémantiques . Il existe un nombre important d'algèbre de processus tels que :

- CCS : Calculus of Communicating Systems
- CSP :Communicating Sequential Processes
- ACP : Algebra of Communicating Processes
- LOTOS : Language Of Temporal Ordering Specification
- BPA :Basic Process Algébra

1.4.2 Langage de Specification $BPA^*_{0,1}$

Afin de pouvoir modéliser le comportement d'un conducteur, nous avons adopté l'une des variantes de l'algèbre de processus BPA (Basic Process Algebra) que nous avons enrichie avec les deux processus 0 et 1 ($BPA^*_{0,1}$) [16].

1.4.2.1 Syntaxe :

Soit A une collection finie (alphabet) d'actions atomiques a, b, e...(Nous insistons sur un alphabet fini pour sauvegarder la nature algébrique), Les processus finis sont générés à partir des processus atomiques dans A en utilisant le deux opérations "basiques" :
$+$: composition alternative.
$\bullet$: composition séquentielle.
Soit P,Q deux processus appartenant à un ensemble de processus p. La syntaxe de $BPA^*_{0,1}$ est définie par la grammaire BNF suivante :

$$P,Q ::= 0 \mid 1 \mid \text{a} \mid P{+}Q \mid P.Q \mid P^*Q$$

où :

- le chiffre 0 désigne un processus dans un état bloqué, et 1 un processus ayant normalement terminé son éxecution.
- a : une action élémentaire à executer.
- $P+Q$: c'est une compostion altérnative entre le processus P et Q, donc il exécute soit P soit Q .
- $P.Q$: c'est une composition séquentielle entre le processus P et Q, dont l'execution de Q ne se débute qu'a la términaisaon de l'execution de premier processus P.
- P^*Q : représenté également par le processus $P.(P^*Q) + Q$ (version binaire de l'opérateur étoile de Kleene).

1.4.2.2 Sémantique :

La sémantique est définie formellement, de manière axiomatique ou opérationnelle [17] [14].

1.4.2.3 Sémantique Axiomatique :

Une sémantique axiomatique consiste en un ensemble de lois algébriques (commutativité, associativité, distributivité des opérateurs, etc.) qui permettent de démontrer l'équivalence de termes. Le tableau ci-dessous représente les différents axiomes de lalgèbre BPA [14] [10] :

A1 :	P + Q = Q + P
A2 :	(P + Q) + R = P + (Q + R)
A3 :	P + P = P
A4 :	(P + Q).R = P.R + Q.R
A5 :	(P.Q).R = P.(Q.R)

TABLE 1.1 – Sémantique Axiomatique.

- A1 : (commutativité de "+") dit que P + Q et Q + P représentent un choix entre : P et Q ou entre Q et P.
- A2 : (associativité de "+") indique que (P + Q) + R et P + (Q + R) exprime le choix entre P et Q ensuite entre le résultat et R, ou bien entre Q et R ensuite entre P est le résultat signifie la même chose.
- A3 : (idempotence de "+") dit qu'un choix entre P et P équivaut à un choix pour P.
- A4 : (distribution droite de ".") indique que (P + Q).R et P.R + Q.R représentent un choix entre P et Q, suivi de R.
- A5 : (associativité de ".") indique que (P.Q).R = P.(Q.R) représentent P suivi de Q suivi de R.

1.4.2.4 Sémantique opérationnelle :

Une sémantique opérationnelle consiste en une relation de transition P, exprimant le fait qu'un processus P peut effectuer l'action a puis évoluer et se transformer en un processus p' ; cette relation de transition est généralement définie par induction structurelle sur la syntaxe des termes en utilisant des formats de règles standards qui garantissent par construction que la sémantique est correcte ; le tableau ci-dessous illustre l'ensemble de régles définies :

[!h]

$R^a = \frac{\odot}{a \xrightarrow{a} 1}$	$R^1 = \frac{\odot}{1\downarrow}$
$R^*\downarrow = \frac{Q\downarrow}{(P*Q)\downarrow}$	$R\downarrow = \frac{P\downarrow Q\downarrow}{(P.Q)\downarrow}$
$R_l = \frac{P\downarrow Q \xrightarrow{a} Q'}{(P.Q) \xrightarrow{a} Q}$	$R_r{}^{\cdot} = \frac{P \xrightarrow{a} P'}{P.Q \xrightarrow{a} P'.Q}$
$R_l{}^{+} = \frac{P \xrightarrow{a} P'}{P+Q \xrightarrow{a} P'}$	$R_l{}^{*} = \frac{P \xrightarrow{a} P'}{P^*Q \xrightarrow{a} P'.(P^*Q)}$
$R_r^* = \frac{Q \xrightarrow{a} Q'}{P^*Q \xrightarrow{a} Q'}$	$R_{l\downarrow}{}^{+} = \frac{P\downarrow}{(P+Q)\downarrow}$
$R_{r\downarrow}{}^{+} = \frac{Q\downarrow}{(P+Q)\downarrow}$	$R_r^+ = \frac{Q \xrightarrow{a} Q'}{P+Q \xrightarrow{a} Q'}$

[18]

— Les règles (R_l^+) ou (R_r^+) indiquent que la composition altérnative (P+Q) peut évoluer vers P' si P évolue vers P', ou vers Q' si le processus Q évolue vers Q'.

— Les règles (R_l) ou (R_r) spécifient que afin que la composition séquentille évolue, il faut que le premier processus peut évoluer ou bien le premier processus se termine et que le second peut evoluer .

— Les règles (R^l) ou (R^r) spécifient les comportements répétitifs (P^*) a le choix d'executer soit P soit Q, s'il éxecutre P il va retomber une autre fois sur la meme situation . Cette situation est réitérée jusqu'à ce qu'il décide d'exécuter le processus Q.

— Les règles $R_{r\downarrow}^+$,$R^*\downarrow$,($R_{l\downarrow}^+$) ,$R\downarrow$ spécifient les cas de terminaison des processus comme suit :

  — Pour que le processus P^*Q termine, il faut que le processus Q termine.

  — Pour que le processus P.Q termine, il faut que les processus P et Q terminent.

  — Pour que le processus P+Q termine, il faut que les processus P termine ou bien le processus Q termine.

1.4.3 Langage de spécification $CBPA^*_{0,1}$

$CBPA^*_{0,1}$ C'est la version étendue de la $BPA^*_{0,1}$, elle permet d'exprimer des actions conditionnelles et la notion des variables.

1.4.3.1 Définitions [18]

- **Un terme** : il represente soit une variable, soit une constante (fonction d'arité 0) ou bien une fonction de termes.
- L'ensemble des termes est notées T(F,X), F est l'ensemble des fonctions, X est l'ensemble des variables.
- Deux termes a et b de T(F,X) sont unifiables s'il existe une substitution (σ) tel que a(σ) $\doteq$ b(σ).
- mgu : (most general unifier) est la substitution la plus générale entre deux termes pour laquelle a(σ) $\doteq$ b(σ).
- Un terme est dit fermé s'il ne contient pas de variable.
- Un processus est dit fermé si toutes ses actions sont des termes fermés.
- L'ensemble des actions fermés est noté T(F).
  Si a est une action fermée alors on note $\bar{a}$ l'ensemble T(F) \a.

1.4.3.2 Syntaxe :

$$\text{P} ::= 0 \mid 1 \mid \text{c} \triangleright \text{a} \mid \text{P.Q} \mid \text{P+Q} \mid P^*\text{Q}$$

$c \triangleright a$: signifie que 'a' ne s'execute que si 'c' est vrai.

1.4.3.3 Sémantique :

$R^a = \frac{\odot}{c \triangleright a \xrightarrow{a} 1} c = 1$	$R^1 = \frac{\odot}{1\downarrow}$
$R^*\downarrow = \frac{Q\downarrow}{(P*Q)\downarrow}$	$R\downarrow = \frac{P\downarrow Q\downarrow}{(P.Q)\downarrow}$
$R_l = \frac{P\downarrow Q \xrightarrow{a} Q'}{(P.Q) \xrightarrow{a} Q}$	$R_r{}^{\cdot} = \frac{P \xrightarrow{a} P'}{P.Q \xrightarrow{a} P'.Q}$
$R_l{}^{+} = \frac{P \xrightarrow{a} P'}{P+Q \xrightarrow{a} P'}$	$R_l{}^{*} = \frac{P \xrightarrow{a} P'}{P^*Q \xrightarrow{a} P'.(P^*Q)}$
$R_r^* = \frac{Q \xrightarrow{a} Q'}{P^*Q \xrightarrow{a} Q'}$	$R_{l\downarrow}{}^{+} = \frac{P\downarrow}{(P+Q)\downarrow}$
$R_{r\downarrow}{}^{+} = \frac{Q\downarrow}{(P+Q)\downarrow}$	$R_r^+ = \frac{Q \xrightarrow{a} Q'}{P+Q \xrightarrow{a} Q'}$

TABLE 1.2 – Sémantique $CBPA^*_{0,1}$.
[18]

1.4.4 Opérateurs logiques

1.4.4.1 Définition

Les opérateurs logiques créent des conditions composées dans une formule, par exemple deux conditions ou plus qui doivent être satisfaites avant de sélectionner une méthode particulière de calcul. Les opérateurs logiques nous permettent de décrire de telles associations de conditions [19]. Nous avons choisis les operateurs les plus utilisés par les logiques, et qui correspondent à nos besoins pour exprimer les processus de notre proposition.

1. **L'opérateur OU inclusif** $\vee$ **:**est un opérateur logique à deux opérandes, qui peuvent avoir chacun la valeur VRAI ou FAUX. Il permet de Vérifie seulement qu'une des conditions est réalisée [19].

   — **Table de vérité :**

P	Q	$(P \vee Q)$
0	0	0
0	1	1
1	0	1
1	1	1

TABLE 1.3 – Table de vérité de OU logique .
[19]

— **Propriétés :**

Idempotence du « OU »	$(P \vee P \Leftrightarrow P)$
Commutativité du « OU »	$(P \vee Q \Leftrightarrow Q \vee P)$
Associativité du « OU »	$P \vee (Q \vee R) \Leftrightarrow (P \vee Q) \vee R$

TABLE 1.4 – Quelques Propriétés de OU logique.
[20]

2. **Le ET logique :** est un opérateur logique à deux opérandes, qui peuvent avoir chacun la valeur VRAI ou FAUX [20].

— **Table de vérité :**

P	Q	$(P \wedge Q)$
0	0	0
0	1	0
1	0	0
1	1	1

TABLE 1.5 – Tableau du vérité de ET logique.
[19]

— **Propriétés :**

Idempotence du « ET »	$(P \wedge P \Leftrightarrow P)$
Commutativité du « ET »	$(P \wedge Q \Leftrightarrow (P \wedge Q)$
Associativité du « ET »	$(P \wedge Q) \wedge R \Leftrightarrow P \wedge (Q \wedge R)$
Distributivité de « OU» par rapport à « ET »	$(P \vee (Q \wedge R)) \Rightarrow (P \vee Q) \wedge (P \vee R)$
Distributivité de « ET » par rapport à « OU »	$(P \wedge Q) \vee (P \wedge R)) \Rightarrow (P \vee (Q \wedge R))$

TABLE 1.6 – Quelques propriétés de ET logique.
[20]

1.5 Conclusion

Ce chapitre a été consacré aux pré-requis théoriques, nous avons d'abord abordés les généralités sur la biométrie en définissant les éléments les plus importants qu'on aura besoin pour notre étude, puis nous avons présenté les différents concepts des systèmes de transport intelligents. Ensuite, nous avons introduit quelques méthodes formelles utilisées dans la sécurité informatique.

Dans le second chapitre nous allons établir un état de l'art sur quelque traveaux existants dans la litérature concernant l'authentification dans les véhicules intélligents à base des techniques biométriques.

Chapitre 2

Etat de l'art sur les protocoles d'authentification biométrique d'un conducteur

2.1 Introduction

Dans le monde actuel, la technologie grandit de jour en jour et les chercheurs scientifiques présentent de nouveaux découvertes, le besoin de sécurité augmente également dans tous les domaines. À l'heure actuelle, l'utilisation du véhicule est une nécessité fondamentale pour toutes les personnes. Simultanément, la protection de ces véhicules contre le vol est également très importante. Parmi les techniques de sécurité proposées afin de remédier à ce problème, nous citons la biométrie qui est utilisée pour identifier ou authentifier un conduteur.

Dans ce chapitre, Nous passons en revue quelques travaux existants qui portent sur l'authentification biométriques des conducteurs en analysant leurs différences et une comparaison en fonction des critéres établis.

2.2 Classification des travaux passés en revus

Un certain nombre de caractéristiques sont utilisées dans les systémes d'authentifications d'un conducteur. Chaque caractéristique biométrique à ses avantages et ses inconvénients, c'est pourquoi le choix de la technique pour une telle application dépend d'une variété de questions en plus de sa performance. Bien qu'il existe un trés grand nombre de modalités biométriques nous pouvons distinguer trois catégories voir la (Figure 2.1). Peu de travaux basés sur l'analyse des traces biologiques existent et cela revient à la compléxités de la mise en oeuvre de ce type de la biométrie dans les systémes de reconnaissance usuelles, par contre plusieurs travaux basés sur les signaux physiques ont été proposés grâce à la simplicité du ces systémes et la disponibilité des moyens. Un

autre type de biométrie basée sur le comportement des individus est aussi utilisé pour l'authentification d'un conducteur .

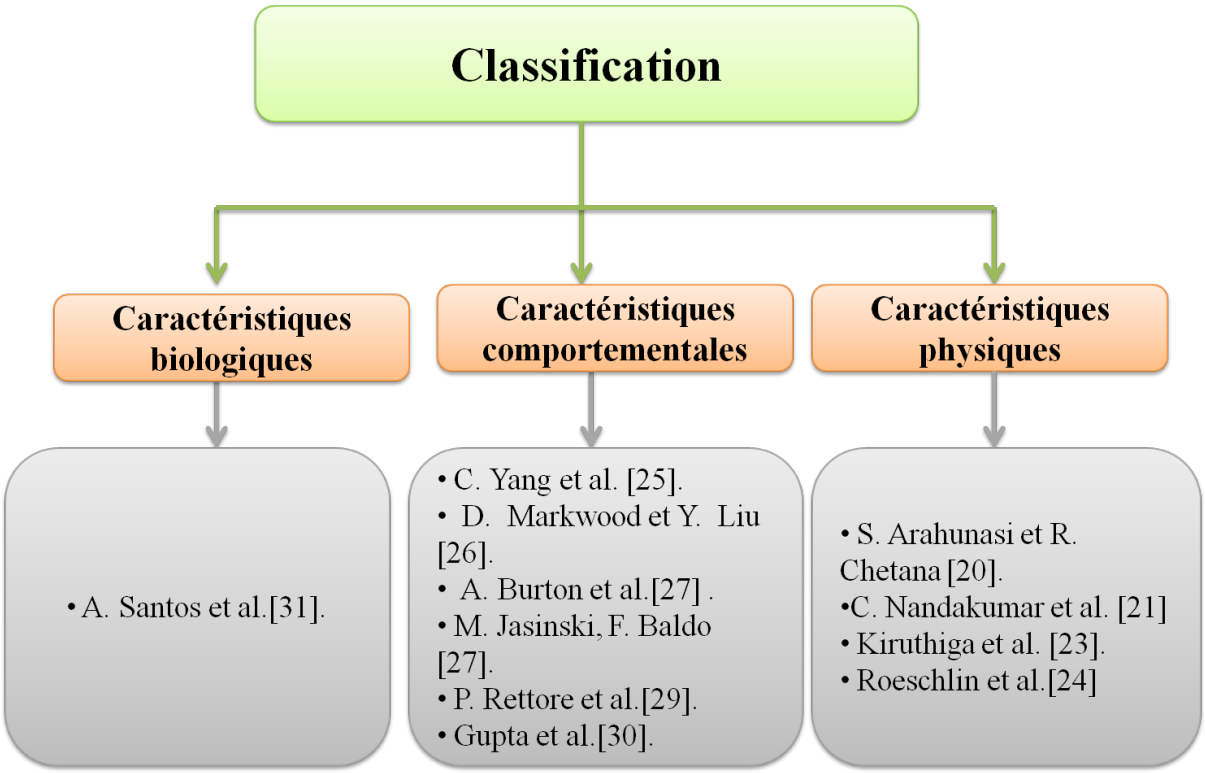

FIGURE 2.1 – Classification des travaux passés en revus.

2.3 Etude des travaux existants de l'authentification biométrique du conducteur dans les réseaux véhiculaires

L'identification des conducteurs est l'un des défis de recherche dans les véhicules intelligents. Quelques études ont démontré la faisabilité de l'authentification du conducteur par la biométrie ont s'appuyant sur les interactions des conducteurs à l'intérieur du véhicule afin d'extraire leurs caractéristiques biométriques. Selon la section précédente ces traveaux peuvent étre classifier en trois categories :

2.3.1 Solutions basées sur les signaux physiques

En biometrie physique, plusieurs travaux ont été élaborés prenant en compte différentes caractéristiques, les unes plus fiables que d'autres, mais toutes doivent être infalsifiables et uniques pour pouvoir être représentatives d'un et un seul individu.

— **Real Time Vehicle Security System through Face Recognition :**

Nandakumar et al.[21] ont proposé le système de sécurité qui se base sur la technique de traitement des images pour l'authentification d'un conducteur, en temps réel en se focalisant sur la détection de visage et les techniques de reconnaissance faciale. Dés que le conducteur entre dans une voiture garée, le capteur infrarouge attaché au siège du conducteur de la voiture active la caméra cachée fixée dans la position appropriée à l'intérieur du véhicule, une fois l'image est acquise de la caméra activée, un processus de traitement d'image sera déclenché. Ce processus implique deux parties, la détection de visage :l'image acquise est traitée pour détecter le visage à l'aide de l'algorithme Viola Jones, ces images sont amélioré en supprimant les information indésirables et sont stockées dans la base de données. La reconnaissance de visage cela en utilisant la base de données qui contient des images de visage normalisées, la reconnaissance est effectuée dans le système de sécurité du véhicule par l'algorithme LDA. Le test de l'image doit être comparé avec celles stockées dans la base de données et le classificateur utilisé dans l'algorithme décide si l'image est connue ou inconnue en utilisant la distance euclidienne. Dans le cas ou le visage détecté ne correspond pas au propriétaire de la voiture, un MMS des valeurs faciales et le GPS (Global Positioning System) lui seront envoyer.

— **Face Recognition System for Unlocking Automobiles Using GSM and Embedded Technology :**

Un autre protocole de reconnaissance et d'identification a été proposé par Arahunasi et Chetana. [22] afin d'offrir un systéme de sécurité avancé en voiture en utilisant à la fois des exigences matérielles et logicielles. Les composants matériels nécessitent principalement une alimentation, un microcontrôleur ARM7, un module GSM et un écran LCD, et la configuration logicielle comprend essentiellement une machine basée sur Matlab. Le GSM (Global System for Mobile) joue un rôle important dans ce système qui se base sur une vérification en deux étapes qui consistent à entrer le mot de passe du propriétaire afin que les autres personnes obtiennent la permission d'utiliser le véhicule, et la technologie FRS (Face Recognition System) utilisant Matlab qui permet à l'utilisateur d'en savoir plus d'information sur les visiteurs. Ensuite, elle compare les résultats obtenus par l'ensemble de l'approche prédéfinie, si elle correspond, le moteur s'allume automatiquement, sinon il ne démarre pas et par la suite, les preuves sont envoyées au propriétaire, à la suite d'un SMS d'alerte ce qui permet d'obtenir l'approche du voleur dans la base de données car le système stockera l'approche d'une personne illégale et peut gérer cette image pour d'autres enquêtes. l'algorithme optimisé LBP (modèle binaire local) est utilisé afin de détecter convenablement le visage des utilisateurs dans le réel.

— **Real Time Biometrics Based Vehicle Security System with GPS and GSM Technology :**

Kiruthiga et al. [23], ont proposé une tentative taciturne de conception et de développement d'un système de contrôle du vol de véhicule sans problème et à faible coût en utilisant un microcontrôleur, une technologie GSM (Global System for Mobile) GPS (Global Positioning System) pour la communication. Ce système comporte trois modules, technique de reconnaissance d'empreintes digitales rapide, fiable et économique afin de protéger le véhicule de tout accès non autorisé. Elle est basée sur des capteurs à ultrasons. Un module de communication homme-machine qui représente le système global pour mobiles (GSM) et module d'une carte principale intégrée avec divers composants.

Ce système de sécurité véhicule le statut du véhicule à la personne autorisée utilisant GSM. Si la personne est certifiée, l'accès au véhicule est autorisé. Sinon, un SMS sera envoyé au propriétaire et le moteur sera immobilisé. Le prototype du système de sécurité repose sur la plate-forme intégrée utilisant PIC Microcontrôleur, qui contrôle tous les processus et Lors de tentatives de vol extrêmes, la protection du véhicule est assurée par l'unité de commande du moteur (ECU) intégrée au microcontrôleur et avec la technologie GPS, le véhicule peut être identifier facilement et en deux modes, c'est-à-dire lorsque la batterie est fournie ou non.

— **Bionyms : Driver-centric Message Authentication using Biometric Measurements :**

Le protocole d'authentification proposé par Roeschlin et al. [24], se base sur la signature de message en utilisant les engagements anonyme appelés bionyme qui sont considérés comme des identifiants unique acquis à l'aide des caractéristiques biométriques du conducteur qui assure la traçabilité de chaque message. Ces caractéristiques sont détectées à l'aide des capteurs intégrés dans les véhicules.

Les signatures obtenues sont authentifiées et rattachées à l'identité du conducteur. Ce dernier doit être inscrit auprès du AC (autorité de confiance) en lui fournissant l'identité d, une mesure biométrique q et un secret s stockés sur un jeton, une fois les informations fournit sont vérifiés une clé k sera générer en utilisant une fonction irréversible qui sera encapsuler pour garantir la non extraction de la clé. Une fois l'inscription au niveau de AC est faite, l'acquisition de bionyme est nécessaire pour pouvoir échanger des messages VANET authentifiés .

2.3.2 Solutions basées sur le comportement

La biométrie physique présente malheureusement un inconvénient majeur ; en effet aucune des mesures utilisées ne se révèle être totalement exacte car il s'agit bien là d'une des caractéristique

majeure de tout organisme vivant, ce qui a conduit les chercheurs à penser aux caractéristiques comportementales.

— **A Novel GMM-Based Behavioral Modeling Approach for Smartwatch-Based Driver Authentication**

Yang et al. [25], ont proposé une méthode d'authentificaion qui est une amélioration du modèle de mélange gaussien GMM (Gaussian mixture model) afin de pouvoir l'utiliser dans la modélisation comportementale de la conduite. Cette méthode a été utilisée pour le développement d'un système d'authentification comportementale du conducteur à l'aide d'un accéléromètre et d'un capteur d'orientation d'un smartwatch.

Ce système permet d'évaluer le comportement du conducteur à partir de son utilisation du volant à l'aide des capteurs intégrés dans une montre qui est connecté à la main gauche du conducteur. Les auteurs ont crée pour chaque manœuvre de conduite un modèle de comportement basée sur le GMM proposée. Ce mécanisme d'authentification se base sur trois étapes principales :

1. Le prétraitement où les données capturé seront diviser en segment spécialisé sur un domaine opérationnel spécifique.
2. L'extraction des caractéristiques dont deux modèles de pilote basés sur GMM sont conçus pour extraire plusieurs caractéristiques des données prétraitées qui donnera deux types de fonctionnalités séparés formés à l'aide du modèle de classificateur SVM.
3. La phase de décision où les fonctionnalités seront combinés pour donner un modèle de comportement de conduite pour le conducteur.

— **Vehicle Self-Surveillance : Sensor-Enabled Automatic Driver Recognition**

Une autre approche efficace et persistante de reconnaissance automatique du conducteur qui identifie les conducteurs non autorisés a été developpée par Markwood et Liu [26]. Elle se base sur l'extraction des caractéristiques des comportements de conduites, qui ne peuvent pas être reproduites exactement par un voleur qui s'éloigne dans la voiture volée, tels que les déplacements des conducteurs dans la conduite élémentaire. Une classification des utilisateurs et une collection de données sont effectuées afin d'illustrer la méthodologie utilisée dans cette approche, suivi du traitement de ces données en événements de conduite élémentaire et en identifiant six événements de conduite généraux rencontrés dans un entrainement typique : augmentation de la vitesse, maintien de la vitesse (croisière), conduite en roue libre, freinage, virage et changement de voie.

— **Driver Identification and Authentication with Active Behavior Modeling**

Burton et al.[27], ont proposé un protocole de sécurité avancée sous forme de modélisation du conducteur et cela en s'identifiant et authentifiant les conducteurs via des caractéris-

tiques uniques. Ce protocole vise à résoudre le problème de l'insécurité et de systèmes de transport non fiables causés par une mauvaise utilisation du véhicule.
Une études préliminaire est effectuée afin de collecter les données sensorielles avec 10 sujets humains différent et un environnement de conduite simulé a été utilisé pour collecter les habitudes du conducteur en se basant sur cinq caractéristiques potentiellement discriminantes extraites : la distance euclidienne parcourue, la vitesse moyenne du véhicule, l'écart type de la position du volant, le changement moyen de pédale de frein et le changement moyen de la position de pédale d'accélérateur.
Le modèle d'activité de conduite a été construit en appliquant divers algorithmes d'apprentissage automatique (arbres de décision, machine à vecteurs de support (SVM) et k-plus proche voisin (kNN)) aux fonctionnalités collectées.

— **A Method to Identify Aggressive Driver Behaviour Based on Enriched GPS Data Analysis :**
Jasinski, Baldo [28], ont proposé un protocole de conduite qui tente à comprendre le comportement des conducteurs lors de chaque voyage en analysant leurs données enregistrées en mouvement via des dispositifs de collecte GPS non intrusifs. Ce protocole comprend quatres etapes : la collecte de données ; prétraitement ; Enrichissement par segment et le calcul de l'indicateur d'agressivité de la trajectoire (TAI). Cet indicateur varie de 0 à 100, 0 signifiant aucun comportement agressif et 100 signifiant comportement très agressif. En outre, la méthode peut informer rapidement les conducteurs de leurs comportements agressifs dans des situations spécifiques et les aider à changer de comportement afin d'éviter les accidents.
Une autre contribution est que l'indicateur d'agressivité pourrait être adapté en fonction de chaque demande. Les résultats préliminaires ont montré que la méthode permettait d'identifier un comportement agressif presque en temps réel, ce qui pourrait être utilisé pour signaler un comportement dangereux avant qu'un accident ne se produise.

— **Driver Authentication in VANETs based on Intra-Vehicular Sensor Data**
En 2018, Rettore et al. [29], ont renforcé la sécurité des systèmes d'authentification, en utilisant le comportement du conducteur en tant que seconde facteur d'authentification. Pour cela ils ont proposé un système d'authentification qui s'appuie sur des fonctionnalités inhérentes au conducteur. Ce travail explore l'identification du pilote basée sur une méthodologie qui s'appuie sur six étapes en tant que facteur d'authentification supplémentaire afin de fournir des services locaux et des services de réseaux. Ils ont développé un capteur virtuel CV qui permet de détecter un ensemble de données disponibles via un OBD Paramètre ID (PID), ces données seront sélectionné on éliminant les fonctionnalité inutiles afin de fournir les informations les plus précieuses sur l'identité de conducteurs à partir d'un jeu de données précédemment étiqueté, et son comportement pour différencier un conducteur

légitime d'un suspect.

Pour compléter cette approche, ils ont également proposé que le véhicule avertisse périodiquement les autres chaque fois que le conducteur est illégitime. À la réception de cette avertissement, les véhicules voisins transmettent l'alerte aux autres jusqu'à il parvient à une autorité compétente, qui peut prendre les mesures appropriées.

La faisabilité de l'approche proposé a été démontré en effectuant un ensemble d'expérience selon différent scénario. Les résultats obtenues sont satisfaisable et montre que la présence de véhicules illégitimes peut compromettre la qualité des services essentiels fournis par VANETs. Par exemple, les véhicules illégitimes peuvent modifier les données sensibles diffusées à l'ensemble du réseau. ce qui affirme que l'identification des personnes illégitimes est primordial pour le bon fonctionnement des VANET.

— **DriverAuth : Behavioral biometric-based driver authentication mechanism for on-demand ride and ridesharing infrastructure :**

A partir des méfaits signalés contre les applications de covoiturage, Gupta et al. [30], ont proposé un protocole d'authentification basé sur une approche comportementale biométrique.

Le protocole proposé est basé sur des modalités biométriques comportementales (les mouvements de la main, les gestes de glissements, intervalle de temps entre deux toucher) pendant que l'utilisateur interagit avec le téléphone, ce système utilise une architecture client-serveur basée sur une couche de sécurité supplémentaire .

Coté client, une fois l'utilisateur interagit avec l'application le gestionnaire de session appelle la couche sécurité. Les capteurs collectent les données biométriques nécessaires telle que déterminée par le gestionnaire d'interface utilisateur, et les transfère au accumulateur ou ils seront stockées et au moteur de cryptage dont ils seront chiffrées, une fois la collection de données est achevées, ils seront mise en paquets et envoyées a la couche réseaux qui les transfère au fournisseur de services a fin de détecter l'identité de l'utilisateur. Simultanément, les données capturées sont traitées coté serveurs, et décrypté par le moteur de décryptage, ces dernières seront décomposé en modalités pour le prétraitement des données brutes et divers caractéristiques, les fonctions ou les caractéristiques sont fusionnées et sélectionnées.

La création du modèle est faite selon la fonctionnalité sélectionnées, un sous ensemble sera stocké dans la base de donnée comme un modèle de formation, puis un autre test est appliquée aux données non existante dans la base de données afin de vérifier l'identité du demandeur.

2.3.3 Solution basée sur mesure biologique

La biométrie biologique a pour but de mesurer les substances du corps humain ou les traces biologiques, Celle-ci se distingue toutefois nettement des autres types de technologies biométriques et ce, à plusieurs égards.

2.3.3.1 «ECG-Based User Authentication and Identification Method on VANETs», A. Santos et al.

En 2018, A. Santos et al.[31] ont exploité l'aspect biométrique des signaux ECG pour l'authentification continue dans les VANET. Ils ont utilisé les caractéristiques du signal ECG qui admet 5 déviation significatives q,r,s,t,et u, mais dans leurs études ils ont utilisé que sur le complexe QRS qui est considéré comme l'information la plus importante dans l'analyse cardiaque, et apporte des fonctionnalités de surveillance de la santé, et il est utilisé comme un facteur de sécurité.
Les données ECG sont traitées en suivant les étapes suivantes : prétraitement, extraction et sélection des caractéristiques, et classification des utilisateurs. Dans la première phase ils ont employé un algorithme de détection de points fiduciaux basé sur *Hill Climbing*, l'extraction des caractéristiques est faites par des techniques basées sur la fréquence qui sont les plus populaire, et un ensemble d'outils mathématiques appelés Transformées en ondelettes. Après l'extraction des caractéristiques, il est nécessaire de sélectionner que les caractéristiques les plus appropriées afin de construire un modèle d'apprentissage robustes. Enfin pour la classification du signal ils ont utilisé un arbre de décision basé sur *Random Forest*.

2.4 Etude comparative

2.4.1 Critéres de comparaison

Plusieurs plateformes ont été créées pour évaluer et comparer les systèmes d'authentification en se basant sur différents critères, parmi ces critéres nous citons les suivants :

- **Précision :** Représente la capacité des systémes de distinguer entre le conducteur ligitime et le conducteur illégitime.
- **Performance :** La performance mesure l'efficacite et la fiabilite d'un systeme d'authentification dans un contexte d'utilisation donné. Il regroupe le taux EER, FAR et FRR qui signifient :

  Taux d'erreur (EER) : taux d'exactitude croisée, est déterminé par le point d'intersection entre la courbe du taux de FAR et la courbe du taux de FRR.

  Taux de faux acceptations (FAR) : La FAR décrit la proportion des imposteurs qui ont été authentifié en tant qu'utilisateurs légitimes.

  Taux de faux rejets (FRR) : Le FRR décrit la proportion de véritables utilisateurs qui

ont été incorrectement rejetés d'un système d'authentification.

— **L'Acceptation par l'utilisateur :**Il est liée à des paramètres sociaux, psychologiques et parfois sanitaires qui indique la mesure dans laquelle les gens sont prêts à accepter l'utilisation d'un identifiant biométrique (caractéristique) dans leur vie quotidienne.

— **La simplicité d'utilisation :** Il peut être définie comme étant la quantité d'énergie fournie par un individu pour être reconnue par un système.

2.4.2 Tableau comparatif

Le tableau 2.1 illustre une étude comparative des travaux passés en revues.

Classification	Critères / Travaux	Performance	Précision	Simplicité d'utilisation	Acceptation par l'utilisateur
Biométrie physique	[21]	-	Basse	Haute	Moyenne
	[22]	-	Basse	Haute	Moyenne
	[23]	FRR=0.1% , FAR=0.01%	Haute	Moyenne	Basse
	[24]	FRR=8.6%	Basse	Moyenne	Basse
Biométrie comportementale	[25]	EER=7.86%	Moyenne	Moyenne	Haute
	[26]	-	Moyenne	Haute	Haute
	[27]	EER=14.7%	Moyenne	Moyenne	Haute
	[28]	-	Moyenne	Haute	Moyenne
	[29]	ERR=2%	Haute	Moyenne	Haute
	[30]	-	Moyenne	Moyenne	Moyenne
Biométrie biologique	[31]	EER=4,158%	Haute	Moyenne	Moyenne

TABLE 2.1 – Tableau comparatif.

2.4.3 Discussion

D'aprés l'étude de quelques travaux proposés dans la littérature sur les technologies biométriques qui couvrent un large ensemble de méthodes permettant d'identifier les conducteurs et d'automatiser leurs authentification en utilisant les caractéristiques physiques ou comportementales de ces dérniers, nous constatons malheureusement que la biométrie physique présente un certain nombre d'inconvénients qui agit sur la qualité de l'authentification, ces limites ne se situent pas seulement au niveau de la particularité physique sur laquelle ils reposent, mais aussi sur la façon avec laquelle ils la mesurent, et la marge d'erreur qu'ils autorisent. ces méthodes ne sont en effet pas toujours fiables à 100%, ce qui empêche les conducteurs de bonne foi d'accéder à leurs systèmes.

L'utilisation de la reconaissance faciale seule dans les systémes d'authentification (cas de [21][23]) n'est pas suffisant et reste toujour un probléme d'actualité non résolu. ceci revient à la sensibilité de cette technique aux différents facteurs tels que le changement d'éclairage : rendent la tache très difficile, variation de la position du visage, expressions faciales ainsi que le problème des vrais jumeaux que la vérification automatique de visage ne pourra jamais détecter les différences trés subtile qui existent entre eux.

D'autres systémes d'authentifiction sont fondée sur la plus ancienne des technologies d'identification dites empreintes digital [23], cette technique nécessite que le conducteur pose un doigt sur un capteur d'empreinte spécifique cette modalité est résistante jusqu'à un certain seuil, elle présente néanmoins quelques problèmes de fiabilité. En effet, les empreintes digitales d'un travailleur manuel le rendent réfractaire à toute identification. Elle se caractérise aussi par des problèmes de contraste (doigt propre et sec devient trop clair tandis qu'un doigt humide et recouvert d'un film gras devient foncé), et aussi la difficulté de lecture due à la sensibilité aux altérations pouvant survenir au cours de la vie (égratignure, cicatrice, vieillissement ou autres) et à certaines variations (température,humidité, saleté).

En opposition à la biométrie physique, la biométrie comportementale constitue un nouveau moyen de défense efficace, Nos traits physiques ne sont pas les seules choses qui nous rendent uniques. En effet, les manoeuvres du conducteur (les mouvements de la mains [25][30], la pression du conducteur sur la pédale d'accélération et de freinage [29][26][22], position de la main sur le volant [22] ...etc.) permettent de distinguer un individu d'un autre, de manière aussi fiable.
Il y a plusieurs raisons pour lesquelles la biométrie comportementale est plus rassurante.Tout d'abord, en raison du matériel nécessaire la biométrie pysiologique est coûteuse car elle nécessite un matériel spécialisé pour détecter les fonctionnalités alors que la biométrie comportementales est moin chère car aucun matériel spécialisé n'est nécessaire.Ainsi, les caractéristiques comporte-

mentales sont faciles à révéler ils peuvent être collectées sans que l'utilisateur ait à intervenir et permettent une surveillance d'authentification continue sans perturber les activités de l'utilisateur.

Tous les critères sur lesquels notre comparaison est basée, sont très importants, ils nous ont permis de relevé des insufisances qui permettent à des conducteurs illégitimes de se comporter comme étant les propriétaires de véhicules. D'après cette comparaison, nous avons remarqué que les caractéristiques physiques sont loins d'être parfaites et précises, donc dans ce contexte nous sommes intéressés à l'approche comportementale.

2.5 Conclusion

Ce deuxième chapitre nous a permis de faire le tour des différents systémes biométriques utilisés pour l'authentification d'un conducteur. Aprés avoir établit une comparaison entre les deux approches les plus utilisées (physiologique, comportementale), nous avons constaté que les performances dépendent de plusieurs facteurs qui varient de l'un à l'autre.

Dans le chapitre suivant, nous allons définir une approche qui permet d'authentifier un conducteur en se basant sur des caractéristiques comportementales modélisées à l'aide d'une méthode formelle qui est l'algébre de processus.

Chapitre 3

Proposition et évaluation de performances

Première partie

Proposition

3.1 Introduction

Pour résoudre le probléme d'authentification des conducteurs, plusieurs travaux basées sur la biométrie à aspect physiologique et comportementale ont été proposés, pour atteindre le même objectif on s'est intéressé à l'utilisation de l'algébre de processus pour définir le comportement d'un conducteur et d'assurer son authentification durant une session de conduite.

Ce chapitre contient deux parties, la premiére partie sera consacrée à la présentation de notre proposition d'authentification de conducteur qui se base sur la biométrie comportementale en s'appuyant sur les différentes manoeuvres de ce dernier. La deuxième partie sera consacrée l'évaluation de performances de notre proposition afin de démontrer à travers des simulations les performances de notre méthode .

3.2 Motivation

L'utilisation du véhicule est une nécessité fondamentale pour toutes les personnes. Simultanément, sa protection contre le vol est également très important. Pour protéger le véhicule de tout accès non autorisé plusieurs techniques d'authentification des conducteurs basées sur des métriques biométriques ont été proposé. La biométrie pour l'authentification d'un conducteur est devenue une option intéressante et réalisable, ces méthodes différent selon le type de caractéristiques utilisées.

D'aprés l'ensemble de méthodes d'authentification biométriques étudiées au cours de ce travail nous constatons que chaque méthode à ses propres limites telle que la difficulté d'extraction de données qui pose un probléme lorsque l'authentification est basée sur les caractéristiques physiques. Les performances de ses systémes dépendent de taux de fausse acceptation et le taux de faux rejet, ils permettent ainsi de démontrer leurs efficacités et faisabilités.

Le but de notre travail est de proposer une méthode d'authentification du conducteur ayant des meilleurs performances et cela en s'appuyant sur ces caractéristiques comportementales. Pour ce faire nous nous basons sur le changement des actions éffectuées par le conducteur durant sa conduite pour développer un modéle de conduite, ce qui permettera de déterminer s'il s'agit du conducteur ligitime.

3.3 Notre Proposition

Dans cette section nous presentons notre méthode d'authentification du conducteur dans les véhicule intélligent. Notre proposition se résume en deux phases : phase de modélisation des actions du conducteur et phase d'authentification. La premiére phase consiste à créer un modéle du comportement du conducteur à base d'un ensemble d'action sous forme d'un processus. La seconde phase consiste à authentifier un conducteur selon le modéle développé.

3.3.1 Phase de modélisation

La capacité d'un conducteur à maîtriser son véhicule est essentielle pour conduire en toute sécurité. Elle consiste en la maîtrise d'un ensemble d'actions que le conducteur doit être en mesure de réaliser. Cette phase vise à obtenir un modéle du comportement d'un conducteur à base d'un ensemble d'action tout en utilisant l'algébre de processus.

Dans cette section nous décrivons notre modélisation qui consiste à créer un modèle de comportement à base d'un ensemble d'action qu'on peux regrouper en deux catégories distictes : actions non répétées et actions répétées ainsi que les variables définies dans des intervalles qui permettent de déterminer les conditions d'exécution de chaque action pour chaque conducteur, cette modélisation sera présentée sous forme d'un processus .

3.3.1.1 Action Non Répétées

Aprés avoir analysé le comportement des conducteurs sur différents trajets nous avons constaté que ces dérniers effectuent un ensemble d'actions qui ne se répétent pas au cours de leurs conduite. Ces actions non répétées sont entre autre le réglages des retroviseurs, réglages du siége, réglages du volant ainsi que la mise en place de la ceinture de sécurité sont des actions indispensables qui permettent d'offrir au conducteur un champ de vision nécessaire et un confort pour se déplacer en sécurité. Bien régler ses éléments est donc une nécessité. Cette nécessité se différe d'un conducteur à un autre selon sa taille, son comportement...etc.

1. **Définitions des actions non répétées**

   (a) **Rétroviseurs** Un rétroviseur est un élément indispensable pour la visibilité et donc la sécurité d'un conducteur, la plupart des voitures ont trois rétroviseurs (Figure 3.1) :

   • **Le rétroviseur intérieur**, il doit être réglé afin de permettre à l'usager de voir la totalité de la vitre arrière, avec éventuellement un bout de la plage arrière.

   • **Les rétroviseurs extérieurs gauche et droit**, qui doivent être réglés de façon à montrer la poignée de la portière arrière dans l'angle en bas à droite des rétroviseurs.

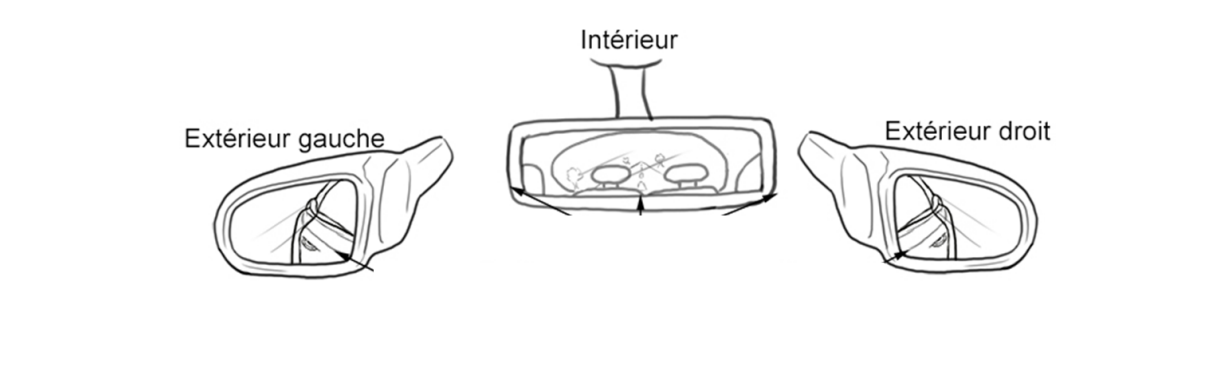

FIGURE 3.1 – Réglage des Rétrovisseurs
[32].

(b) **Ceinture de sécurité** La ceinture de sécurité est un équipement de sécurité passive, c'est-à-dire qu'elle permettra de limiter les blessures en cas d'accident. Cependant, la ceinture de sécurité a également des limites et une mauvaise installation de celle-ci peut entraîner des blessures [33] (Figure 3.2). Certains conducteurs préférent la mettre (avant le démarrage de la voiture ou pendant la conduite) tandis que d'autres l'ignorent carrément.

FIGURE 3.2 – Réglage du ceinture de sécurité
[34].

(c) **Volant** Le volant fait aussi partie des éléments du poste de conduite à régler. Sur la plupart des véhicules modernes, il est possible de régler la position du volant de la voiture, en hauteur et en profondeur afin d'avoir la meilleure position possible et d'assurer une distance adéquate au volant (Figure 3.3).

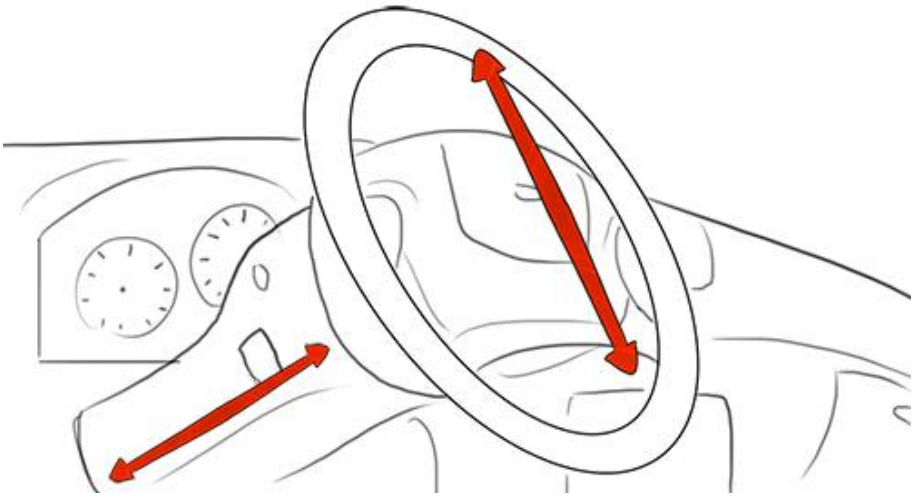

FIGURE 3.3 – Réglage du volant
[34].

(d) **Siège**

Le réglage du siége dépend d'un conducteur à un autre selon sa taille,
il existe de nombreuses fonctions de réglage [34], telle que :

• **Réglage de la profondeur :** c'est à dire faire glisser le siège en avant ou en arrière pour obtenir une position de conduite confortable [34] (Figure 3.4).

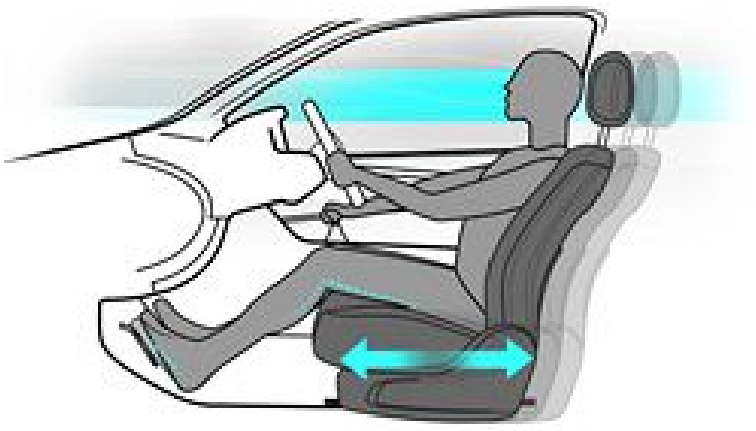

FIGURE 3.4 – Réglage de la profondeur du siége
[34].

• **Réglage de la hauteur :** régler la hauteur de manière à ce que les talons soient à plat sur le plancher [32] (Figure 3.5).

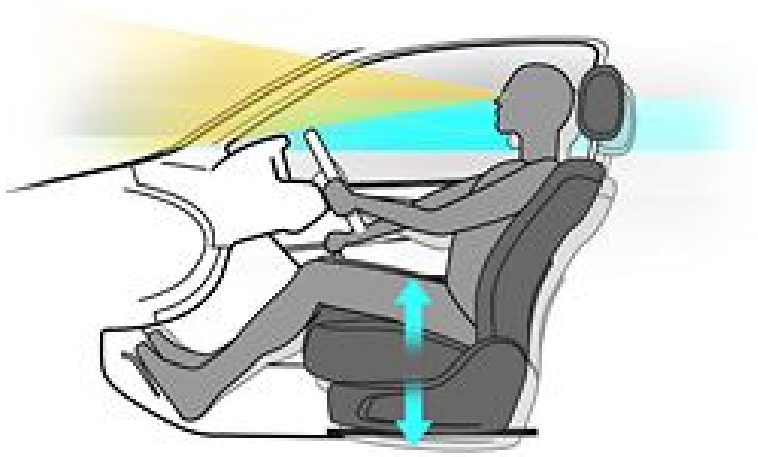

FIGURE 3.5 – Réglage de la hauteur du siége
[34].

• **Inclinaison du dossier :** incliner le dossier pour avoir un angle plus grand que 90 entre les cuisses et le torse, sans que les épaules ne quittent le dossier [32] (Figure 3.6).

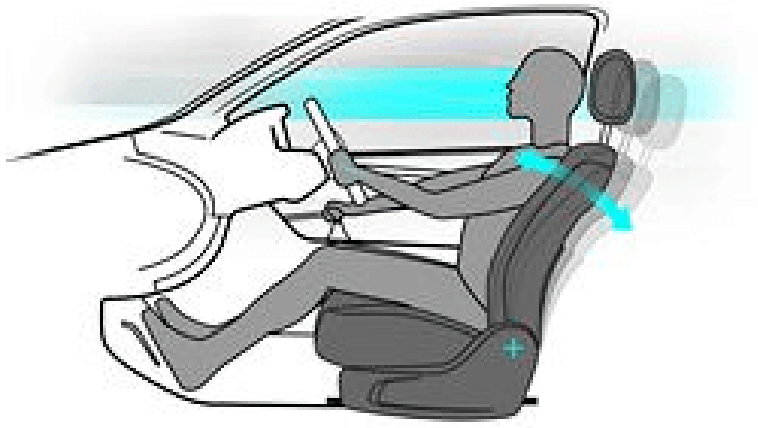

FIGURE 3.6 – Inclinaison du dossier
[34].

2. **Processus spécifiant les actions non répétées** Soit (Σ) l'ensemble des actions élémentaires et (Γ) l'ensemble des opérateurs :

$(\Sigma_1) = \{$ r , s , v , sc $\}$.
Dont :

— **r** : Réglages des rétroviseurs.
— **s** : Réglages du siége.
— **v** : Réglages du volant.
— **cs** : Ceinture de sécurité.

$(\Gamma_1) = \{\vee, \wedge\}$
Dont :

— $\vee$: Ou logique.
— $\wedge$: Et logique. .

L'ensemble des actions et leurs variables, ainsi que les unités de mesures et les intervalles sont représentés dans le tableau suivant (Tableau 3.5) :

Actions élémentaires	Variables	Unité de mesure	Intervalle
Réglages des rétroviseurs (r)	Rétroviseur central (RC)	RADIAN	$[a_1, a_2]$
	Rétroviseur gauche (RG)		$[a_3, a_4]$
	Rétroviseur droite (RD)		$[a_5, a_6]$
Réglages du siége (s)	Hauteur du siége (HS)	CM	$[b_1, b_2]$
	Profondeur du siége (PS)		$[b_3, b_4]$
	Inclinaison du dossier (IS)	RADIAN	$[a_7, a_8]$
Réglages du volant (v)	Profondeur du volant (PV)	CM	[b5,b6]
	Hauteur du volant (HV)	RADIAN	$[a_9, a_{10}]$
Ceinture de sécurité (cs)			

TABLE 3.1 – Paramétres des actions élémentaires.

Le processus (P) qui spécifie l'ensemble des actions non répétés est définit comme suit :

$P = (((a_1 < RC \wedge RC < a_2) \wedge (a_3 < RG \wedge RG < a_4) \wedge (a_5 < RD \wedge RD < a_6)) \rhd r) \vee (((b_1 < HS \wedge HS < b_2) \wedge (b_3 < PS \wedge PS < b_4) \wedge (a_7 < IS \wedge IS < a_8)) \rhd s) \vee (((b_5 < PV \wedge PV < b_6) \wedge (a_9 < HV \wedge HV < a_{10})) \rhd v) \vee cs.$
(3.1)

La génération de ce processus est basée sur un ensemble d'actions non répétées, chaque action a des variables bornée entre des intervalles qui varient d'un conducteur à un autre. Pour assurer l'éxécution de chaque action une ou plusieurs conditions doivent être satisfaites.

3.3.1.2 Actions répétées

Pendant le trajet, la vitesse de conduite varie selon les conditions routiére, le conducteur peut s'accélérer ou se rétrograder et cela aprés avoir atteindre une certaine vitesse. D'aprés notre analyse, nous allons conclue qu'on peut considérer le changement des vitesses comme étant des actions répétées dont la valeur de passage d'une vitesse à une autre se différe entre les conducteurs.

1. **Processus spécifiant les actions répétées**

$(\Sigma_2) = \{ v_1, v_2, v_3, v_4, v_5 \}$.
Dont :

- v_1 : Passage à la vitesse 01.
- v_2 : Passage à la vitesse 02.
- v_3 : Passage à la vitesse 03.
- v_4 : Passage à la vitesse 04.
- v_5 : Passage à la vitesse 05.

$(\Gamma_2) = \{\cdot, \wedge, +, *\}$
Dont :

- $\wedge$: Et logique.
- $\cdot$: l'opérateur Séquentiel.
- $+$: l'opérateur Altérnative .
- ***** : 0 ou plusieurs .

Actions élémentaires	Variables	Intervalle
Passage à la vitesse 01 (v_1)	Vitesse de la voiture (V)	$[a_{11}, a_{12}]$
Passage à la vitesse 02 (v_2)		$[a_{21}, a_{22}]$
Passage à la vitesse 03 (v_3)		$[a_{31}, a_{32}]$
Passage à la vitesse 04 (v_4)		$[a_{41}, a_{42}]$
Passage à la vitesse 05 (v_5)		$[a_{51}, a_{52}]$

TABLE 3.2 – Paramétres des actions élémentaires.

Le processus (Q) qui spécifie l'ensemble des actions répétés est définit comme suit :

$$Q = ((a_{11} < V \wedge V < a_{12}) \rhd v_1) \cdot [((a_{11} < V \wedge V < a_{12}) \rhd v_1) + ((a_{21} < V \wedge V < a_{22}) \rhd v_2) +$$

$$((a_{31} < V \wedge V < a_{32}) \rhd v_3) + ((a_{41} < V \wedge V < a_{42}) \rhd v_4) + ((a_{51} < V \wedge V < a_{52}) \rhd v_5)]^* (3.2)$$

Ce processus spécifie les action répétées durant la conduite, pour chaque changement de vitesse (accélération, retrogradation) la vitesse de la voiture (V) doit impérativement respecter l'intervalle définit pour cette action. Dans ce processus l'ordre de changement de vitesse n'est pas forcément respecté c'est à dire :le conducteur peut passer de la premiére vitesse à la troisiéme sans avoir passer de la deuxieme . Par contre lors de son démarrage il doit souvent commencer par la premiére vitesse.

3.3.2 Phase d'authentification

L'objectif de cette phase est de valider l'identité d'un conducteur en comparant les informations biométriques acquise avec le modéle de référence, ces informations s'agissent d'un ensemble de valeurs générées aléatoirement.

Dans le cas des actions non répétées alors une seule valeur sera générée :

— Si la valeur aléatoire générée appartient à l'intervalle du modéle de référence alors l'indice de correspondance sera incrémenté, sinon il sera décrémenté selon la fonction (3.3).

$$I \rightarrow I + 0.025 \times m + 0.03 \times n$$

(3.3)

Avec

$$\begin{cases} (n, m) = (0, 1) & \text{si c'est le bon conducteur} \\ (n, m) = (-1, 0) & \text{sinon} \end{cases}$$

Dans le cas des actions répétées alors plusieurs valeurs aléatoires seront générées et pour chaque valeur on vérifie :

— Si la valeur aléatoire générée appartient à l'intervalle du modéle de référence alors l'indice de correspondance sera incrémenté, sinon il sera décrémenté selon la fonction (3.4) :

$$I \to I + m \times \frac{\min(|V-V_{min}|,|V-V_{max}|)}{100} + n \times \frac{\frac{Intervalle}{1.5}-|V-V_{moy}|}{100} \tag{3.4}$$

Avec

$$\begin{cases} (n,m) = (0,1) & \text{si c'est la bonne action} \\ (n,m) = (-1,0) & \text{sinon} \end{cases}$$

V_{max} = Vitesse Maximale.
V_{min} = Vitesse Minimale.
Intervalle =$V_{max} - V_{min}$.
$V_{moy} = \frac{V_{max}+V_{min}}{2}$.

Une fois l'indice de correspondance de chaque conducteur est calculé il sera comparé à une valeur dite indice d'accepetation afin de valider la ligitimité du conducteur.

Deuxième partie

Simulation et Evaluation de Performances

3.4 Simulation et résultats

Cette partie est consacrée à l'analyse des performance de notre proposition. Pour ce faire nous effectuerons des simulations en utilisant le language de programmation JAVA. Nos données seront sauvegarder dans une base de données créer sous MySQL server.

3.4.1 Outil de développement

• **NetBeans** est un environnement de développement intégré (ou IDE) qui s'enrichit à l'aide de plugins utilisé pour la création des programmes d'ordinateur, il est placé en Open Source par Sun. En plus de Java, il permet également de supporter différents autres langages [35]. NetBeans est disponible sous Windows, Linux, Solaris, Mac OS X ou sous une version indépendante des systèmes d'exploitation (requérant une machine virtuelle Java). Un environnement Java développement Kit (JDK) qui désigne un ensemble de bibliothèques logicielles de base du langage de programmation Java, ainsi que les outils avec lesquels le code Java peut être compilé, est requis pour les développements en Java. Afin d'installer correctement NetBeans, il est nécessaire d'installer le JDK compatible à la version de NetBeans.

• **MySQL** C'est un système de Gestion de Bases de Données (SGBD) et un logiciel libre sous licence GPL. MySQL fonctionne sous linux et Windows et performant de point de vue stockage de données volumineuses.

3.4.2 Paramétre de simulation

La génération de données se fait par l'analyse des manoeuvres du conducteur pendant sa conduite, les données extraites pour chaque action sont délimitées par des intervalles bien définit, une fonction aléatoire permet de générer des valeurs comprises entre ces intervalle au cours de la simulation. L'interface de notre application (Figure 3.7) nous permet de saisir ces intervalles .

Nos simulations ont été réalisées avec 20 conducteur dont 50% repésentent des conducteurs ligitimes tandis que le reste représentent des conducteurs imposteurs. Cette simulation nous permet d'évaluer les performances de notre proposition en calculant le taux de fausse acceptation (FAR) et le taux de faux rejet (FRR). Afin de réaliser nos simulation nous avons initialisé les intervalles du modéle de références selon les données extraites du conducteur ligitime .

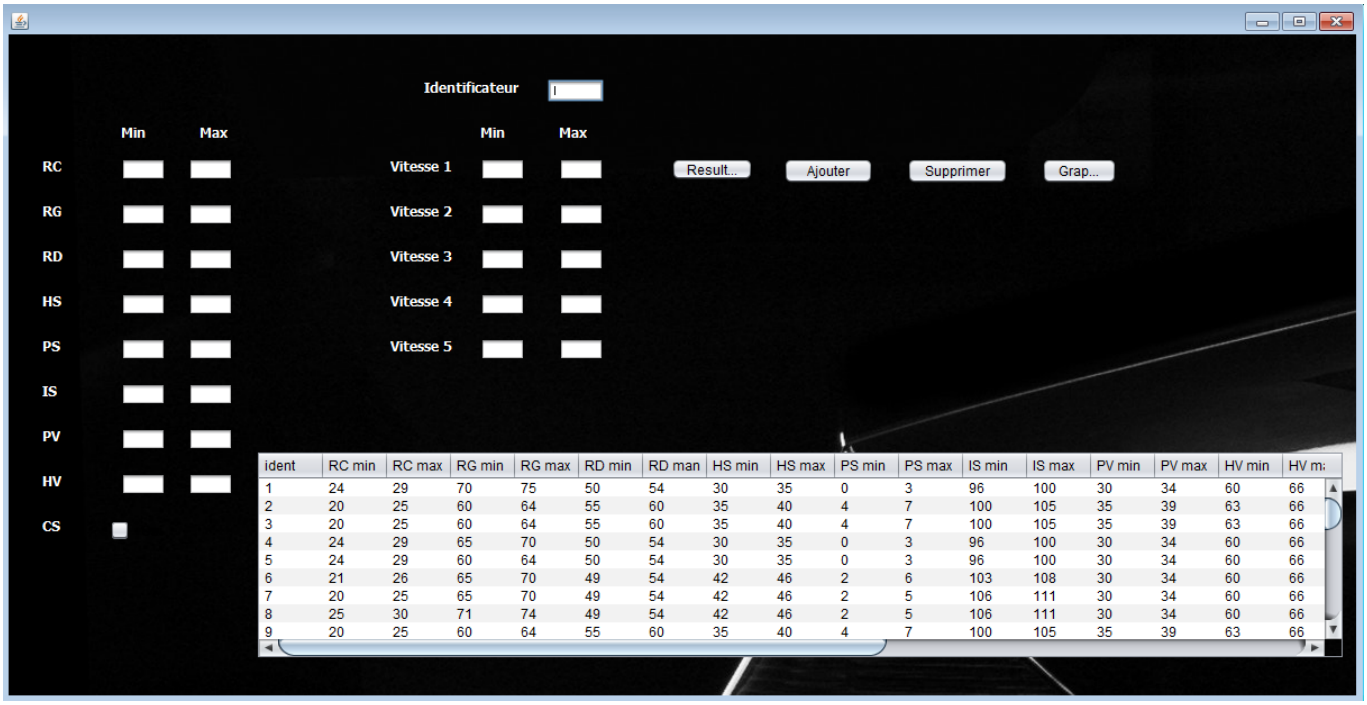

FIGURE 3.7 – Interface de notre systéme d'authentification.

Action	Variable	interval	Variable	interval
Actions non répétées	RC	[0.349066 , 0.436332]	RG	[1.13446 , 1.22173]
	RD	[0.959931 , 1.0472]	HS	[35 , 40]
	PS	[4 , 7]	IS	[1,74533 , 1.8326]
	PV	[35 , 39]	HV	[63 , 66]
	CS	True		
Actions répétées	V1	[0 , 10]	V2	[25 , 30]
	V3	[45 , 50]	V4	[60 , 65]
	V5	[75 , 80]		

TABLE 3.3 – Paramétres du modéle de simulation.

3.4.3 Résultats obtenus

Dans ce qui suit nous présentons les résultats de simulation de notre proposition, ainsi que la méthode qui nous a permis de fixer la valeur de l'indice d'acceptation auxquelle nous avons comparés l'indice de correspandance de chaque conducteur.

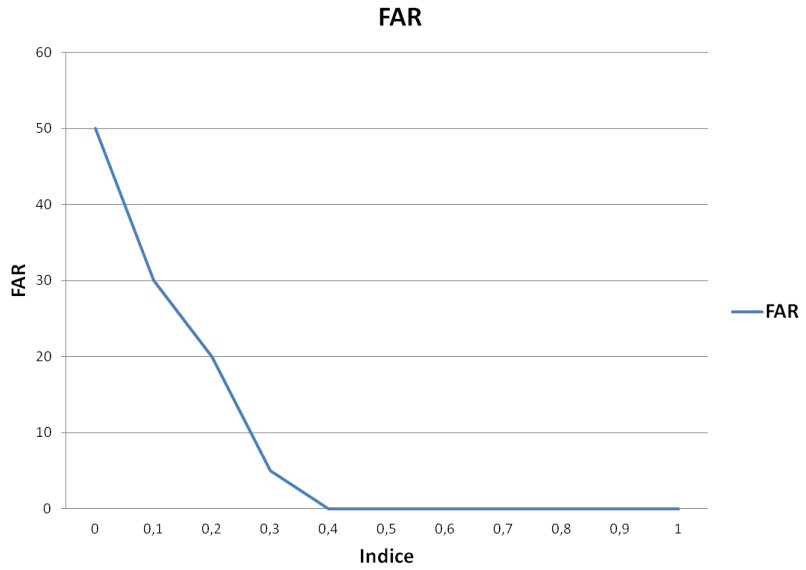

FIGURE 3.8 – Courbe représentative des valeurs du FAR.

La Figure 3.8 présente la variation du taux de fausse acceptation (FAR) en fonction de l'indice d'accepataion, le FAR est défini comme le pourcentage des conducteurs imposteurs qui ont été reconnu à tort comme un conducteur ligitime. Nous remarquons que la valeur de FAR se dégrade en augmentant la valeur de l'indice d'acceptation et a patir de 0.4 le taux de FAR tend vers 0,cela revient au nombre important de faux conducteurs ayant été acceptés par le systéme malgré que la valeur de leurs indices de correspandance était petite.

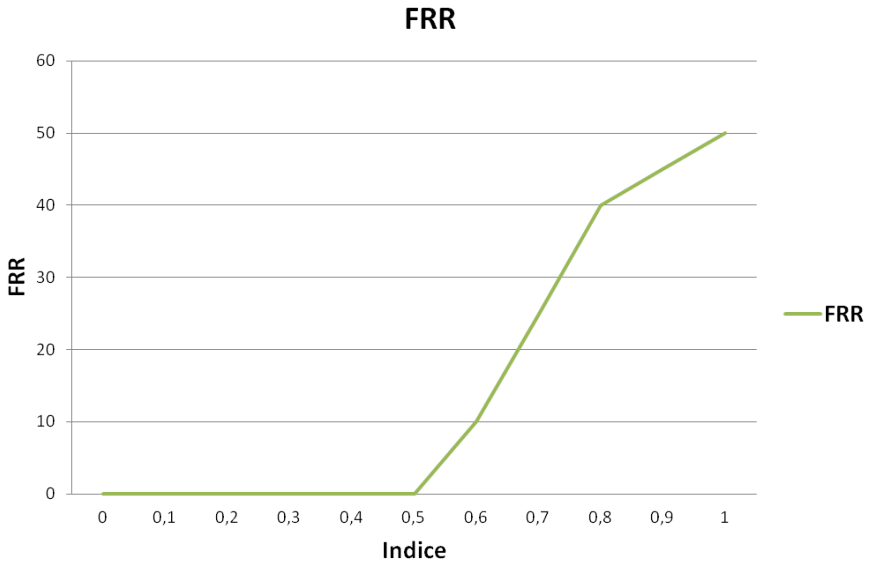

FIGURE 3.9 – Courbe représentative des valeurs du FRR.

La Figure 3.9 illustre la variation du taux de faux rejets FRR considéré comme le pourcentage des conducteurs ligitime qui ont été reconnu comme des imposteurs en fonction de l'indice d'acceptaion. Nous remarquons que si la valeur de l'indice d'acceptation est fixée entre [0,0.5] le FRR est nulle, au delà de cette valeur le FRR augmente jusqu'à atteindre le maximum,cela revient à la valeur de l'indice d'acceptation qui est supérieur à l'indice de correspandance des conducteurs ligitimes.

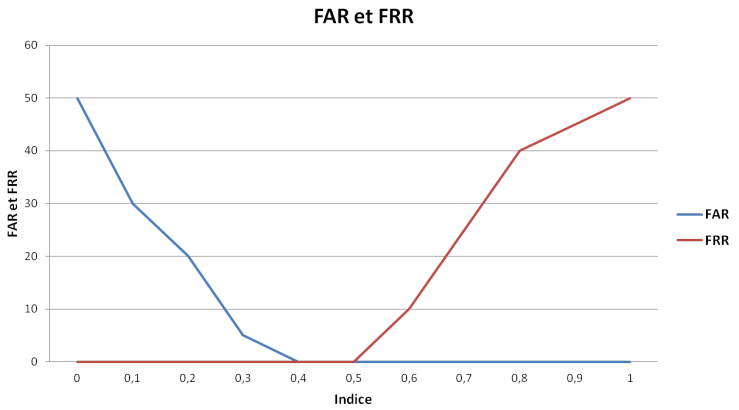

FIGURE 3.10 – Courbe représentative des valeurs du FAR et du FRR.

La Figure 3.10 représente l'évolution du FRR et du FAR en fonction de l'indice d'acceptation.

En comparant ces résultats on remarque que notre proposition atteint les meilleures performances lorsque l'indice d'acceptation est fixé entre 0.4 et 0.5.

Afin de pouvoir fixer la valeur de l'indice d'acceptation nous avons définit un autre scénario de simulation . Etant donné que l'indice de correspondance de chaque conducteur est calculé à base des valeurs générées aléatoirement donc pour chaque tentative d'authentification un nouveau indice de correspondance est généré.

Notre simulation est faite sur un ensemble de 20 conducteurs chaque conducteur effectue 20 tentatives d'authentifications les résultats de notre simulation sont comme suit :

— Si l'indice d'acceptation est fixé à 0.4 alors on aura un conducteur illégitime qui sera deux fois accepté comme étant le bon conducteur donc :

$$\text{FAR} \simeq 0.005 \quad , \quad \text{FRR} \simeq 0.$$

— Si l'indice d'acceptation est fixé à 0.5 alors on aura deux conducteur ligitime qui seront rejetés dont l'un est rejeté deux fois et l'autre une seule fois donc :

$$\text{FAR} \simeq 0 \quad , \quad \text{FRR} \simeq 0.0075.$$

Selon les résultats obtenus par cette simulations, nous fixerons la valeur de l'indice d'acceptation auxquelle l'indice de correspondance sera comparé à 0.5, le choix de cette valeur est justifié par le faite qu'un conducteur qui a été faux rejeté peut se réauthentifier tandis que qu'un conducteur qui a été faux accepté peut engendrer des conséquences majeurs.

3.4.4 Conclusion

Ce chapitre a été consacré à la présentation de notre contribution pour l'authentification des conducteurs à partir de ses manoeuvres, Notre méthode d'authentification est basée sur l'algébre de processus.Nous avons aussi décrit les différentes phases d'éxpérimentation effectuées sur un ensemble des conducteurs stockés dans la base de donnée. Les résultats de la simulation ont démontré aprés l'analyse du modéle et la validation que notre proposition basée sur le comportement des conducteurs offre des meilleures performances en fixant la valeur de notre indice d'acceptation.

Conclusion générale et perspectives

Des efforts considérables sont effectués ces dernières années dans le domaine de la sécurité, ils ont rendu les systémes de transport intélligent de plus en plus surs, mais les menaces ne cessent de se multiplier dans ces systèmes. Les systèmes biométriques sont des systèmes de détection sophistiqués modernes qui utilisent des techniques basées sur les caractéristiques physiques, ainsi sur le comportement de l'individu, tels que le comportement d'un conducteur au volant qui diffère de l'un à l'autre, chaqu'un a un style de conduite habituel et distinct ; certains conduisent lentement et prudemment, tandis que d'autres conduisent rapidement et agressivement.

Dans ce mémoire, nous avons mené une étude critique des travaux existants dans la littérature qui se base sur l'utilisation de la biométrie pour l'authentification d'un conducteur ce qui nous a permis de proposer une autre solution biométrique pour l'authentification d'un conducteur dans les transports intélligents à base d'une méthode mathématique. Nous avons proposé à cet effet, une méthode qui permet d'authentifier un conducteur à partir de ces manœuvre de conduite. Nous avons évalué notre solution en calculant le taux de faux rejet et le taux de fausses acceptation, les résultats de cette expérimentation ont démontré l'éffacacité de notre proposition.

Pour la clôture de ce travail, nous présentons des perspectives qui feront l'objet de nos futures recherches. A commencer, nous envisageons d'intégrer dans notre solution d'autres actions telle que la pression de la jambe sur la pédale de frein et d'accélération, et d'inclure la notion de temps comme un paramétre de perfectionnement lors du passage d'une vitesse à une autre. Une autre perspective serait l'enrichissement de notre proposition en intégrant des scénarios réels de conduite qui dépend de l'état de la route (plat, montée, et déscente), car les monoeuvres effectués par le conducteur ont une relation directe avec l'environnement de conduite.

Bibliographie

[1] A. Nada. *L'intelligence ambiante et les systèmes de transport intelligents*. Thése de magistar, Université Badji Mokhtar ANNABA, Faculté des sciences de l'ingéniorat, Département d'informatique, 2014.

[2] R. Shin S. Hai, H. Lee. A survey of intelligent transportation systems. *Third International Conference on Computational Intelligence, Communication Systems and Networks*, pages 332–337, 2011.

[3] M. Grgic K. Delac. A survey of biometric recognition methods. *46th International Symposium Electronics in Marine*, pages 184–193, 2004.

[4] M. Schatten M. Baca, J. Seva. Modélisation des caractéristiques biométriques comportementales et physiques utilisées pour l'amélioration de la sécurité des sti. *Transport problems*, 2009.

[5] B. Hemery C. Rosenberger M. El-Abed, R. Giot. A study of users acceptance and satisfaction of biometric systems. *In 44th Annual 2010 IEEE International Carnahan Conference on Security Technology*, pages 170–178, 2010.

[6] T. Buvarp D. Gafurov, E. Snekkenes. Robustness of biometric gait authentica- tion against impersonation attack. *In On the Move to Meaningful Internet Systems : OTM 2006 Workshops*, 4278 :479–488, 2006.

[7] L. Chen H. Harb. Voice-based gender identification in multimedia application. *Journal of Intelligent Information Systems (JIIS)*, page 179–198, 2005.

[8] R. Belguech. *Sécurité des systèmes biométriques :révocabilité et protection de la vie privé*. Thèse de doctorat, école nationale supérieure d'informatiqu, Juin 2015.

[9] `https://www.tedsystems.com/category/access-control-systems/`, Consulté le 6 mai 2020.

[10] J. Wayman. Fundamentals of biometric authentication technologies. *International Journal of Image and Graphics*, pages 93–113, 2001.

[11] M. Gauthier. *Cadre juridique de l'utilisation de la biométrie au Québec : sécurité et vie privée*. Mémoire en vue de l'obtention du grade de maîtrise (l.l.m. , Université de Montréal, avril 2014.

[12] H. Chabanne S. Seys K. Simoens, J. Bringer. A framework for analyzing template security and privacy in biometric authentication systems. *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY*, 7, 2012.

[13] A. Alisherov M. Choi D. Bhattacharyya, R. Ranjan. Biometric authentication : Areview. *International Journal of u-and e-Service, Science and Technology*, 2 :13–28, 2009.

[14] J. Klop J. Bergstra. The algebra of recursively defined processes and the algebra of regular processes. pages 82–95.

[15] G. Boudol D. Austry. Algèbre de processus et synchronisation. *Theoretical Computer Science*, 30 :91–131, 1984.

[16] W. Fokkink. *Introduction to Process Algebra*. Springer-Verlag, 2nd edition, 2007.

[17] HuttelH F. GrooteJ. Undecidable equivalences for basic process algebra. *Information and Computation*, 115 :354–371, 1994.

[18] S. AISSANI. *Elaboration d'un cadre formel pour le renforcement de politiques de sécurité dans les programmes*. Mémoire de magister, Université Abderrahmane Mira de Bejaia, 2008.

[19] R. Lascar Cori. *Logique mathématique 1 - Calcul propositionnel ; algèbre de Boole*. Collection Axiomes, 1994.

[20] J. krivine G. kreisel. *Elément de la logique mathématique*. Dunod, 1964.

[21] N. Tharani C. Nandakumar, G. Muralidaran. Real time vehicle security system through face recognition. *International Review of Applied Engineering Research*, pages 371–378, 2014.

[22] Chetana V .Arahunasi. Face recognition system for unlocking automobiles using gsm and embedded technology. *International Journal of Advanced Research in Electrical,Electronics and Instrumentation Engineering*, pages 6090–6067, 2016.

[23] S. Thangasamy K. Narayanasamy, L. Latha. Real time biometrics based vehicle security system with gps and gsm technology. *Procedia Computer Science*, pages 471–479, 2015.

[24] B. Rasmussen I. Martinovic M. Roeschlin, C. Vaas. Bionyms : Driver-centric message authentication using biometric measurements. *IEEE Vehicular Networking Conference (VNC)*, 2018.

[25] D. Liang H. Yang, C. Chang. A novel gmm-based behavioral modeling approach for smartwatch-based driver authentication. pages 1–17, 2018.

[26] Y. Liu L. Markwood. vehicle self-surveillance : Sensor-enabled automatic driver recognition. *ACM*, pages 425–436, 2016.

[27] S. Mascarenhas J. Zhang J. Voris S. Artan W. Li A. Burton, T. Parikh. Driver identification and authentication with active behavior modeling,. *International Conference on Network and Service Management (CNSM)*, pages 388–393, 2016.

[28] F. Baldo M. Jasinski. A method to identify aggressive driver behaviour based on enriched gps data analysis. *The Ninth International Conference on Advanced Geographic Information Systems, Applications, and Services*, pages 97–102, 2017.

[29] A. Souza nG. Maia P. Rettore, B. Campolina. Ecg-based user authentication and identification method on vanets. *IEEE Symposium on Computers and Communications*, pages 78–83, 2018.

[30] B. Crispo P. Guptan, A. Buriro. Driverauth : Behavioral biometric-based driver authentication mechanism for on-demand ride and ridesharing infrastructure. *ICT Express*, pages 16–20, 2019.

[31] P. Resque D. Rosário A. Santos, I. Medeiros. Ecg-based user authentication and identification method on vanets. *Latin America Networking Conference*, pages 119–122, 2018.

[32] `https://www.auto-ecole.net/code/entree-et-sortie-du-vehicule/installation-au-poste-de-conduite`, Consulté le 28 juin 2020.

[33] `http://www.latribuneauto.com/`, Consulté le 28 juin 2020.

[34] `https://www.ornikar.com/permis/conseils-conduite/prendre-quitter-vehicule/installation-poste`, Consulté le 28 juin 2020.

[35] `https://netbeans.org/kb`, Consulté le 30 juin 2020.

RÉSUMÉ

Dans ce monde où la technologie évolue de jour en jour, les chercheurs scientifiques présentent des nouvelles découvertes, le besoin de sécurité augmente également dans tous les domaines. L'utilisation du transport est devenue une nécessité fondamentale dans la vie quotidienne des citoyens, donc la protection du véhicule contre le vol est devenue également très importante. L'objectif principal de ce mémoire est de répondre au probléme d'authentification des conducteurs dans les systémes de transport intélligent. Pour atteindre cet objectif nous avons proposé une méthode d'authentification d'un conducteur basée sur la biométrie comportementale en utilisant une approche algébrique afin de protéger le véhicule. Nous avons créé un système expérimental qui nous a permis d'effectuer nos simulation, les résultats obtenus ont démontré la faisabilité de notre proposition.

Mots clés : Authentification ; Systéme de Transport Intelligent ; Algébre de Processus ; Biométrie ; Biométrie Comportementale.

ABSTRACT

In this world where technology is evolving day by day, scientific researchers present new discoveries, the need for security is also increasing in all areas. The use of transport has become a fundamental necessity in the daily life of citizens, therefore the Protecting the vehicle from theft has also become very important. The main objective of this dissertation is to respond to the problem of authentication of drivers in intelligent transport systems. To achieve this objective we proposed a method of authenticating a driver based on behavioral biometrics using an algebraic approach to protect the vehicle. We created an experimental system which allowed us to carry out our simulations, the results obtained demonstrated the feasibility of our proposal.

Key words : Authentication ; Intelligent transportation System ; Process Algebra ; biometrics ; behavioral biometrics.