République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A/Mira de Béjaia
Faculté des Sciences Exactes
Département d'Informatique

MÉMOIRE DE MASTER RECHERCHE

En
Informatique

Option
Intelligence Artificielle

Thème

Prise de décision à partir de la gestion de confiance dans les STI

Présenté par : M. BRAHAMI Lyes

Soutenu le 29 septembre 2022 devant le jury composé de :

Présidente	**Dr ALOUI Soraya**	**Maître de conf. A**	**U. A/Mira Béjaia.**
Rapporteur	**Dr AISSANI Sofiane**	**Maître de conf. A**	**U. A/Mira Béjaia.**
Rapporteur	**M. BELHOCINE Sidali**	**Doctorant**	**U. A/Mira Béjaia.**
Examinateur	**M. AMROUN Kamel**	**Professeur**	**U. A/Mira Béjaia.**

Résumé

Dans le cadre des systèmes de transport intelligents, l'échange d'informations est un atouts de ses systèmes, ce qui rend une collaboration entre les différentes parties. mais n'empêche certaines entité malicieuse peuvent toujours injecter des messages malicieux pour différents but, pour cela une sécurité au niveaux du réseau est primordiale. donc la gestion de la confiance est un outil de surveillance des fiabilité des messages.Au delà, après avoir obtenues les informations fiable, nous sommes sur le point de prise de décision, dans ce cas que notre travail apporte une aide à la prise de décision qui intègre l'avis du conducteur dans cette prise de décision.

pour cela nous avons conçue un chatbot orienté but qui va nous aider a connaître la décision du chauffeur afin de l'intégrer dans la prise de décision finale.

Mots clés : gestion de la confiance, Chatbot, Systèmes de transport intelligent, arbre de décision

Abstract

In the context of intelligent transport systems, the exchange of information is an asset of its systems, which makes a collaboration between the different parties. but does not prevent certain malicious entity can always inject malicious messages for different but, for that a security at the levels of the network is essential. therefore trust management is a tool for monitoring the reliability of messages. Beyond that, after having obtained the reliable information, we are on the point of decision-making, in this case that our work provides a decision-making aid which integrates the driver's opinion in this decision-making.

for this we have designed a goal-oriented chatbot that will help us to know the driver's decision in order to integrate it into the final decision-making.

Keywords : chatbot ; Trust management ; intelligent transportation systems ; decision tree.

Remerciements

Premièrement, je tiens à remercier Dieu de m'avoir donné la force de terminer ce travail. Mes parents ont toujours été là pour moi, ainsi que mes frères et toutes les personnes qui m'ont soutenu de près ou de loin.

Je tiens également à remercier mes deux encadrants, Dr. AISSANI Sofiane et M. BELHOCINE Sidali, pour leurs conseils, leurs informations et le temps qu'ils m'ont consacré.

Enfin, je tiens à remercier les membres du jury pour avoir pris le temps de lire et d'examiner mon travail.

Table des matières

Table des figures

Liste des tableaux

Introduction Génerale

Dans notre vie quotidienne, se déplacer est primordial. Tout le monde a besoin de transport, que ce soit pour se rendre au travail, faire ses courses, transporter des marchandises, etc. Le transport joue un rôle important dans nos vies de tous les jours, c'est pourquoi son développement est une nécessité pour améliorer notre quotidien.

Cependant, en examinant les problèmes causés par les systèmes de transport, de plus en plus de problèmes surgissent, tels que les embouteillages, les accidents, la pollution, etc. Pour résoudre tous ces problèmes, il est nécessaire d'avoir une gestion efficace des flux de circulation dans les villes. Avec le développement des technologies de l'information et de la communication, ces dernières ont donné une autre dimension où tout est devenu automatique.

L'apparition des STI a permis de résoudre certains problèmes liés à la circulation et au trafic routier, en assurant la sécurité des utilisateurs. Mais le plus important est de permettre aux différentes entités d'échanger des informations de manière permanente et en temps réel. La possibilité d'interaction entre les différentes composantes du système nous permet de prendre des décisions plus efficaces, mais le problème est que ces décisions reposent sur des données reçues. Par conséquent, la fiabilité des données est une chose nécessaire afin d'éviter des conséquences parfois douloureuses, surtout dans les cas critiques. Cela attire notre attention sur la nécessité de sécuriser les réseaux de communication. La gestion de la confiance est un moyen de résoudre l'énigme de la fiabilité.

La possibilité d'interaction entre les différentes composantes du systèmes nous permet de prendre des décision plus efficace, mais le problème est que ces décision sont reposer sur des données reçues, pour cela la fiabilité des données est une chose nécessaire afin d'éviter des conséquence parfois douloureuse surtout dans cas critique.Cela nous attire l'attention a sécurisé les réseaux de communications, la gestion de la confiance est moyen de résoudre l'énigme de la fiabilité.

La gestion de la confiance dans les STI permet une bonne surveillance des données échangées, ce qui permet aux utilisateurs d'avoir des données fiables et de détecter les véhicules malveillants. Cela assure la sécurité des usagers et offre également la possibilité aux usagers de prendre des décisions qui leur permettront de gagner du temps et d'éviter les dangers.

Notre projet est divisé en trois chapitres. Dans le premier chapitre, nous présenterons les généralités liées aux STI, à la gestion de la confiance et aux chatbots. Le deuxième chapitre consiste en un état de l'art sur la gestion de la confiance dans les STI. Dans le troisième chapitre, nous présenterons notre proposition qui consiste à apporter le chatbot dans la gestion de la confiance.

Chapitre 1

Généralités

1.1 Introduction

Plusieurs applications sont utilisées dans les systèmes de transport intelligents pour assurer le contrôle et la gestion des transports, et surtout pour résoudre certains problèmes tels que les embouteillages, les accidents, etc. L'échange d'informations entre différentes parties du système est un moyen d'aide à la prise de décision, comme le choix de l'itinéraire à prendre ou la signalisation d'un accident. Cependant, l'existence de fausses informations est un problème qui peut perturber le bon déroulement de certaines actions et causer des conséquences parfois graves. Cela signifie que la fiabilité de certaines informations est cruciale, en particulier lorsque de nouvelles sources telles que des véhicules ou des piétons sont rencontrées en cours de déplacement.

Les systèmes de gestion de confiance sont des moyens qui permettent d'évaluer la fiabilité de certaines informations, mais aussi de savoir à qui faire confiance. Dans ce chapitre, nous allons présenter quelques notions liées aux systèmes de transport intelligents, à la gestion de confiance et aux chatbots.

1.2 Système de transport intelligents (STI)

1.2.1 Définition

Système de transport intelligent dit (STI ou ITS en anglais pour Intelligent Transportation System) est un système qui relie toutes les composantes constituant le système de transport à travers les technologies de l'information et de la communication, pour améliorer la gestion du transport, assurer la sécurité et le confort des usagers. [11]

Il est dit « intelligent » car certaines applications permettent d'interagir d'une maniéré intelligente comme collecter et traiter des données, résoudre des problèmes d'interopérabilité, etc. Une majorité des STIs répondent à la définition de Jorion (1989) d'un système intelligent que l'auteur considère comme un « un système interlocuteur susceptible de jouer vis-à-vis de son utilisateur le rôle de collaborateur intelligent ». [9]

1.2.2 Technologies des STI

L'intégration de plusieurs technologies dans le domaine des transports a permis son développement, on cite quelques-unes [11]

— Technologie de communication sans fils (wifi, Dedicated Short Range Communication,...)
— Données de voitures et cellulaire flottantes qui nous indique la vitesse et la position du véhicule pendant son déplacement.
— Détection de véhicule à partir des caméras.
— Technologies de détection.
— Technologies de traitement de données.

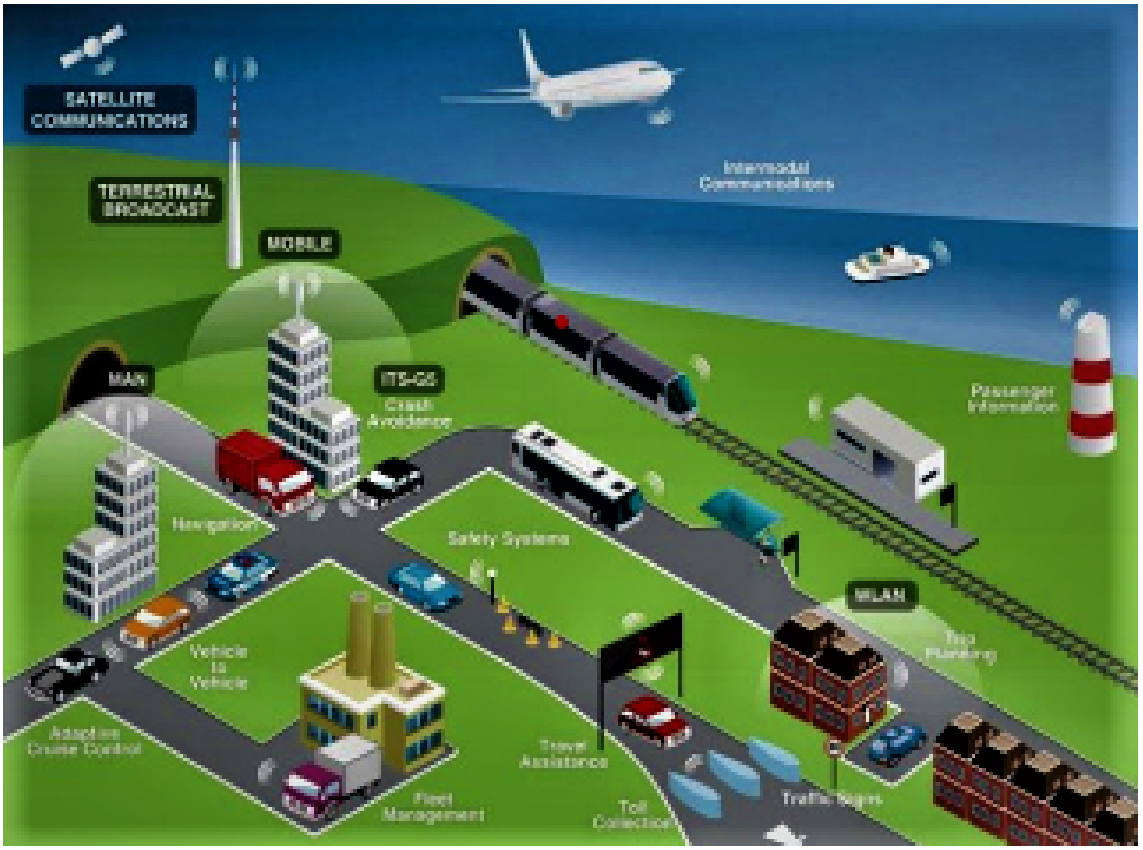

FIGURE 1.1 – Présentation des STI
[27]

1.2.3 Contexte et service des STI

Aujourd'hui, dans le cadre des transports routiers, les STI ont une activité importante à notre égard, car elles nous permettent de prendre de meilleures décisions en temps réel. Les STI sont présentes dans plusieurs champs d'activité, tels que l'optimisation de l'utilisation des infrastructures de transport, l'amélioration de la sécurité routière, les systèmes de contrôle et de surveillance, ainsi que dans le contexte du développement durable. Parmi les services pertinents des STI, on peut mentionner les suivants [11] :

— Adaptation intelligente de la vitesse
— Assistance aux usagers vulnérables de la route
— Systèmes de détection d'incidents et systèmes d'alerte de collision
— Contrôle du respect des limites de vitesse et des feux de circulations
— Systèmes de surveillance des conducteurs

1.2.4 Domaine d'applications des STI

Les STI forment une solution adéquate pour le domaine du transport pour cela nous allons énumérer certains sous domaines d'application : [20]

— Télépéage : Il s'agit d'une application de collecte des péages de manière électronique. Elle permet d'augmenter les performances des stations de péage, de réduire le temps de sécurité pour les voyageurs et d'aider à résoudre les problèmes environnementaux et de consommation de carburant.

— Collecte des données routières : La technologie de collecte de données routières permet d'acquérir des données sur le trafic routier dans un système de transport intelligent. Les systèmes de positionnement et de communication fonctionnent à l'aide de capteurs sur le réseau routier, fournissant des données de base au centre de contrôle du trafic pour calculer, analyser et identifier la congestion du trafic et les temps de trajet.

— Systèmes de gestion du trafic routier : Le système de gestion du trafic joue un rôle central dans le système de transport. Il collecte les informations en temps réel à partir de différents composants matériels tels que les caméras et les capteurs de vitesse, puis les transmet au centre de gestion des transports pour traitement et analyse.

— Préemption des véhicules d'urgence : Dans le cas des urgences, ces applications interviennent pour trouver les chemins les plus sûrs et les plus rapides. La préemption des véhicules réduit le taux d'accidents, favorise les stratégies d'entraide, en minimisant le temps de réponse et en maximisant la sécurité.

1.3 Confiance

1.3.0.1 Notion de la confiance

La confiance est un terme présent dans divers domaines de recherche tels que la philosophie, les sciences sociales, les technologies de l'information et de la communication, et bien d'autres. Dans notre contexte, elle peut être définie comme une relation entre deux parties, l'une accordant sa confiance et l'autre la recevant, dans un contexte donné. Pour les STIs, c'est la confiance décisive qui est utilisée, car les réseaux sont mobiles.[22, 10]

1.3.1 Propriétés de la confiance

Il existe plusieurs façons d'évaluer le concept de la confiance. Dans le cas des STI, voici quelques caractéristiques qui nous permettent d'avoir une idée de la manière de l'évaluer[17]

— **Partiellement transitive :** cela signifie qu'une relation de confiance peut être acquise directement ou indirectement entre deux entités. Directement, cela se fait à partir d'une interaction directe avec les entités concernées. Indirectement, c'est à partir des avis d'autres entités sur une entité cible qu'on peut évaluer la valeur de la confiance.

— **Statique et dynamique :** la confiance peut être statique ou dynamique, selon qu'elle reste la même avec le temps ou qu'elle évolue au fil du temps.

— **Dépendante de la situation :** : la confiance dépend de la sécurité du système. Si le système est sécurisé, alors la confiance sera élevée.

1.3.2 Métriques de la confiance

Il existe différentes méthodes pour évaluer la confiance dans le contexte des STI. Ces méthodes se basent sur les caractéristiques qui définissent la confiance, dans le but de distinguer les messages authentiques des faux messages. En d'autres termes, il s'agit de déterminer quels sont les critères à prendre en compte pour évaluer la confiance.[17]

1.3.3 Quelques attaques contre les systèmes de confiance

Certaines attaques peuvent être dirigées contre les systèmes de gestion de confiance afin de perturber les résultats de l'évaluation de la confiance. Nous pouvons citer quelques-unes de ces attaques[17] :

- **Infiltration de fausses informations** : consiste sur le fait qu'une entité malicieuse qui envoie de faux messages.
- **On-and-off** : consiste à ce qu'une entité malicieuse joue les deux rôles (d'injecter les mauvais messages et les bons) pour esquiver à la détection.
- **Sybil** : consiste à ce qu'une entité malicieuse crée de fausses identités pour tromper les entités cherchant de l'aide.
- **Collusion** : consiste en un groupe d'entité qui créent un groupe organiser qui font contrôler le système de gestion de confiance d'une manière malicieuse.

1.3.4 Gestion de la confiance

La gestion de la confiance est une méthode pour évaluer et établir la confiance entre les entités dans un système de communication. Cela permet d'assurer la sécurité et la fiabilité des échanges d'informations dans un environnement où les entités ne se connaissent pas mutuellement.

1.3.5 Exigences d'un système de gestion de confiance

Pour concevoir un modèle de gestion de confiance efficace pour une prise de décision fiable basée sur les données reçues, il doit répondre à certains critères essentiels pour obtenir des résultats acceptables. Nous présentons ci-dessous quelques-uns de ces critères [14] :

- **Efficacité en temps et en espace** : vue la fluidité du Trafic et la rapidité de déplacement des véhicules,
- **Précision** : pour une bonne prise de décision, la précision du modèle est une des caractéristiques importantes car elle permet d'identifier les véhicules malicieux dans différentes situations.
- **Sensible au contexte** : Plusieurs situations peuvent arriver, prenant exemple dans le cas d'une autoroute ou dans la ville, le nombre de véhicules et la fluidité sont différents, pour cela le modèle doit s'adapter et pouvoir réaliser les calculs dans n'importe quelle situation (que ça soit avec beaucoup de données ou moins de données existantes) d'une manière performante.
- **Assurer la sécurité et la confidentialité** : dans ce cas le modèle doit être sensible aux attaques comme les attaques de collision, créer par des nœuds malicieux qui visent à réduire la réputation des utilisateurs, ce qui peut engendrer le disfonctionnement du système et obtenir de faux résultat. Mais aussi dans le cas de transmission des données

y'en a des informations privées qui sont très sensible et que chaque utilisateur ne désire pas les divulguer, donc le système doit assurer la protection des ses informations.

— **Ne dépend pas des schémas de mobilité**

1.4 Chatbot

1.4.1 Définiton

Les chatbots, également connus sous le nom d'assistants virtuels ou d'agents conversationnels, simulent une conversation par échange textuel ou vocal. Ils utilisent un ensemble de données de réponses aux questions et cherchent des mots-clés spécifiques dans les questions posées pour y répondre en conséquence. S'ils ne trouvent pas de correspondance, ils répondent en indiquant qu'ils n'ont pas compris. Les champs d'application des chatbots sont presque illimités et leur amélioration est étroitement liée aux progrès de l'intelligence artificielle.[2]

1.4.2 Types de chatbots

Il existe différents types de chatbots classés en fonction des tâches qu'ils peuvent réaliser. Voici quelques exemples[2] :

— **Chatbots à réponse rapide :**ils fonctionnent sur la base d'un arbre de décision de questions-réponses préétablies.

— **Chatbots basés sur la reconnaissance de mots clés :** ils analysent les réponses de l'utilisateur à la recherche de mots-clés pour répondre.

— **Chatbots hybride :**ils combinent des éléments de chatbots à menu et de chatbots à reconnaissance de mots-clés.

— **Chatbots contextuelle :**ils utilisent l'intelligence artificielle et l'apprentissage automatique pour comprendre les demandes des utilisateurs et leur fournir des réponses de meilleure qualité.

— **Chatbots à commande vocale :** ils utilisent la reconnaissance vocale pour répondre aux demandes des utilisateurs.

1.5 Conclusion

Ce chapitre nous a permis de comprendre les systèmes de transport intelligents et les notions générales de confiance et gestion de confiance, ainsi que les attaques potentielles contre ces systèmes. Nous avons également examiné quelques définitions et types de chatbots. Le prochain chapitre se concentrera sur les approches et méthodes utilisées pour la gestion de la confiance.

Chapitre 2

Etat de l'art sur la gestion de confiance dans les STI

2.1 Introduction

Dans le contexte des systèmes de transport intelligents (STI), les échanges d'informations sont constants, ce qui permet aux véhicules de recevoir de nombreux messages de différentes entités. Cependant, il est crucial de savoir si ces messages sont fiables. Au fil du temps, plusieurs méthodes de gestion de confiance ont été proposées pour détecter les faux messages infiltrés dans le réseau et assurer sa sécurité. Chaque méthode possède des spécifications propres, et avec l'avènement de nouvelles techniques d'apprentissage automatique et profond pour le traitement efficace de grands volumes de données, plusieurs approches basées sur ces deux axes ont été adoptées pour la gestion de la confiance. Dans ce chapitre, nous examinerons quelques-unes de ces approches proposées.

2.1.1 Modèles basées entités

ces modèles sont basées sur l'évaluation de la confiance des véhicules

Malicious node detection in vehicular ad-hoc network using machine learning and deep learning

Eziama et al ont proposée une méthode pour la détection de noeud malicieux dans les VANET en utilisant le deep et le machine Learning pour assurer la fiabilité des informations échangé entre les véhicules et surtout aider à prendre de bonnes décisions. Cette méthode consiste sur une combinaison entre les réseaux de neurones et les réseaux bayésiens qu'est appelée réseau de neurone bayésien (BNN), les réseaux bayésiens sont utilisés pour renforcer le réseau de neurone en ajoutant le traitement de l'incertitude mais aussi pour le choix de paramètres des données pour la création du modèle. Elle assure une bonne performance de prédiction et la précision de la classification et la détection dans le cas d'une faible latence.[13]

Machine learning based trust management framework for vehicular networks

Hesham El-Sayed et al. ont proposés un cadre de confiance, où, pour calculer les coûts directs et confiance recommandée, diverses techniques sont utilisées, si un véhicule a des privilèges spéciaux, la confiance est calculée en fonction de leurs rôles et de mesures telles que le temps et la distance de transfert/réception des messages entre les nœuds. Mais si c'est un ordinaire, la confiance est calculée sur la base des recommandations des nœuds voisins, en utilisant des métriques telles que la distance euclidienne entre les unités côté route (RSU)/nœuds de transfert de message et RSU/nœuds de réception de message. Classification de l'arbre de décision (DT) est utilisé pour dériver des règles de confiance à partir des évaluations de confiance, qui sont ensuite utilisées par recommander des nœuds véhiculaires (nœuds à distance minimale des RSU et ayant de bonnes valeurs de confiance dans leur histoire de communication) afin de prendre des décisions appropriées en fonction des règles de confiance et les valeurs obtenues à l'aide du modèle de confiance proposé concernant la transmission des messages,qui est soit d'autoriser, de bloquer ou d'évaluer davantage avant de transmettre des messages à d'autres nœuds, Le réseau de neurones artificiels (ANN) est également utilisé par l'agent de contrôle (un nœud de recommandation) auto-former les nœuds véhiculaires pour obtenir les valeurs de confiance attendues. ANN est composé d'une couche d'entrée (nœuds de réception de messages), une couche cachée (nœuds de transmission de messages), une couche de sortie couche (valeurs de confiance cumulées des nœuds d'entrée et cachés) et fonction d'activation (Distance euclidienne et valeur de confiance recommandée). Lorsque la sortie attendue n'est pas obtenue, la rétro-propagation est effectuée, les poids correspondants sont ajustés et la propagation vers l'avant est effectuée à nouveau pour vérifier si la sortie attendue est obtenue. L'ensemble du processus est répété jusqu'à ce que la sortie attendue est obtenue.[12]

Smart Trust Management group vehicles for Vehicular Network

Ltifi et al. ont proposés une approche basée sur les clusters qui utilise la méthode de la cryptographie symétrique pour la gestion de confiance et du trafic, où les tâches de l'autorité de certification (CA) centrale sont répartis entre un ensemble de chefs de groupe dynamiques qui sont choisis selon un algorithm clustering. Dans cette approche, chaque véhicule est équipé d'un OBU (On Board Unit) et organisé en un ensemble de clusters, l'OBU est en charge de l'enregistrement, du calcul, de la localisation et envoyer des messages, tandis que le véhicule avec le niveau de confiance le plus élevé dans chaque cluster est sélectionné comme un chef de groupe (GL) par la réception d'un jeton, un GL change périodiquement, il est responsable réside dans la création et la mise à jour du modèle de confiance (qui contient toutes les informations sur membres du groupe, comme les identifiants, la valeur de confiance et les valeurs des compteurs de coopération) selon le comportements des membres ainsi que la gestion de la fiabilité des messages d'alerte. La gestion de confiance système offre une prise de décision autonome via un composant de l'OBU, qui est la connaissance de base de données. Lorsqu'un véhicule détecte un accident sur la route, il envoie un message d'avertissement au leader qui vérifie le niveau de confiance de l'expéditeur du véhicule en accédant à la base de connaissances et décide de traiter le message d'avertissement ou de l'ignorer.[16]

A Trust Management Scheme with Affinity Propagation

Shu Yang et al. ont proposés un schéma de détection d'anomalies basé sur la confiance pour véhicules intelligents (IV) pour détecter les véhicules anormaux et utiliser la propagation d'affinité pour construire un cluster fiable chefs (CH), qui sont responsables de la gestion de la confiance intracluster. Cluster et sa tête sont générés après plusieurs tours d'itération, chaque

IV diffusera périodiquement sa propre responsabilité et l'auto-disponibilité au quartier pour revendiquer l'opportunité de devenir un CH. Celui qui aura les meilleurs résultats sera élu CH selon l'algorithme AP, ce l'algorithme de cluster aide à transmettre les messages entre les nœuds, une fonction UntrustDegree comme "distance mesure "est conçu pour cet algorithme afin de trouver" le nœud le plus fiable ", avec le UntrustDegree global minimal, un IV peut observer les comportements des autres véhicules et donner un UntrustDegree en fonction de ses connaissances. Lorsqu'un groupe d'IV passe devant une RSU, la RSU télécharger/diffuser de manière proactive les réputations aux IV. Un modèle de superviseur est proposé pour atténuer tricher / se tromper dans le processus de diffusion, il peut recevoir presque la même diffusion informations en partageant le même canal sans fil. Chaque IV choisit automatiquement un supervisé par l'algorithme d'appariement du superviseur et vérifie le message lié au supervisé pour valider la disponibilité/ responsabilité, par calcul répété Si deux résultats ont une grande différence, alors le IV a triché donc une alerte sera lancée, elle sera donc ignorée par les voisins et signalée à CALIFORNIE. Dans n'importe quel tour, si un CH a été généré, il diffusera le message final, qui représente Évaluation finale de CH à chaque membre du cluster.[26]

2.1.2 Modèles basés données

ces modèles sont basées sur l'évaluation de la fiabilité des messages échangés

A dempster-shafer theory based traffic information trust model in vehicular ad hoc networks

Wu et al. ont proposée une méthode qui assure la fiabilité de l'information dans les réseaux VANET au bout d'un trajet sur l'état de la route. Cette méthode consiste sur l'évaluation de la confiance des données échangées entre les différents véhicules en utilisant la théorie Dempster-Shaffer de telle sorte à détecter les messages malicieux. Tout d'abord les messages échangés sont stockés dans une base de données (Mrec) locale en suivant un processus de stockage où chaque message est définie par 5 paramètre, le premier est l'identifiant du véhicule émetteur " i " attribuer par le système, le second est le segment de la route ou se trouve le véhicule " i ", le troisième consiste sur le temps pris par le véhicule i pour parcourir le segment de la route " j ", et le quatrième paramètre consiste sur l'horaire de l'envoie du message et le dernier sign(m,Kpriv(Vi)) consiste sur la signature cryptographique de l'identité du message m en utilisant Kpriv(vi) où Kpriv est la clé privé de Vi. Pour le calcul de la valeur de la confiance d'un message sur un segment de la route, on suppose qu'on a n message entrée sur par n différent véhicule, une fonction T est définie sur le temps indiquée dans le message par véhicule et nous retourne un triplet de masse (x, y, z) ou x : la masse de confiance ,y : la masse de la non confiance, z : la masse de l'incertitude, ensuite ces paramètre sont utiliser dans le calcule des valeurs de la confiance par la théorie de Dempster-Shaffer et le maximum de la valeur de x des résultats obtenus sera pris, si val(x) qui est Tmax $>$ seuil alors on va prendre en considération ce message sinon on attend un autre message.[25]

BIBRM :A Bayesian Inference Based Road Message Trust Model in Vehicular Ad Hoc Networks

Wang et Wu ont proposé un model de gestion de confiance dans les VANETs a base de l'inférence bayesienne afin de detécter les messages malicieux lors d'un segment de la route.C'est une approche basée sur les données. Dans cette méthode, Ils ont définie chaque message échangé sous la forme (Vi,rj,tij,T,Sign(rm,Kpriv(Vi)),ou le message contient les informations suivantes : Vi représente l'identifiant du véhicule émetteur, rj le segment de la route j, tij représente le temps pour parcourir le segment rj,T représente l'horaire de géneration du message, et le dernier champs représente l'identité cryptographique.Ensuite ces messages sont enregistré dans une base de données locale pour chaque zone,en suivant un certains nombre d'instructions.A partir de ces messages enregistré sur un évenement dans un segment de la route,en utilisant l'inférence bayésienne, ils calculent la valeur de la confiance de chaque message, ou cette valeur coorespond a la probabilité du message reçu par rapport aux autre messages situant dans la même cas, afin de choisir le message le plus correcte à diffuser dans la zone qui correspond a la locale map.[23]

Machine Learning Based Approach to Detect Position Falsification Attack in VANET

Pranav Kumar Singh et al. ont proposé une méthode qui se concentre sur la détection des attaques de falsification de position en utilisant des techniques d'apprentissage automatique (ML) telles que les machines à vecteurs de support (SVM), Régression logistique et description des fonctionnalités pour détecter le mauvais comportement. Utilisation du VeReMi ensemble de données, qui se compose de journaux de messages pour chaque véhicule de la simulation et d'un fichier de vérité sur terrain qui spécifie le comportement de l'attaquant pour former et tester nos modèles, chaque fois qu'un message est envoyé, il est également mis à jour dans le fichier de vérité sur terrain qui contient les valeurs réelles du position/vitesse et type d'attaquant. Les classificateurs binaires un contre reste sont utilisés pour prédire si le message est correct ou faux et en échantillonnant une distribution uniforme et en la comparant à la fraction d'attaquant paramètre, les véhicules qui ont des valeurs de position différentes de celles des véhicules légitimes sont classés en tant qu'attaquants, si un attaquant envoie une position aléatoire qui est au-delà de la plage théorique de communication, alors le récepteur serait capable de le détecter.[21]

A Deep Learning Based Intrusion Detection Method in VANET

Yi Zeng et al. ont proposés une méthode de détection d'intrusion de bout en bout basée sur le Deep Learning (DL), il utilise les modèles Convolutional Neural Network (CNN) et Long Short-Term Memory (LSTM), ne nécessitant que des données brutes, il aide à examiner le trafic qui passe par la communication véhiculaire Module (DeepVCM) et détecte automatiquement le trafic de logiciels malveillants pour les unités embarquées (OBU). DeepVCM extraira d'abord les fonctionnalités de la gamme spatiale à l'aide de 1Dimensional CNN, les données d'entrée seront traitées par la première couche convolutive et ses résultats seront saisis dans la fonction d'activation ReLU qui va être traitée via la mise en commun Max, et à la fin la couche de normalisation de la réponse locale (LRN) est ajoutée pour punir les réponses anormales ou la couche sortante pour un meilleur effet de généralisation. La sortie passe ensuite par une seconde couche convolutive semblable à la première. LSTM est appliqué dans DeepVCM pour apprendre les caractéristiques du point de vue temporel, l'entrée de LSTM sera la sortie du CNN, les données passera à travers une couche densément connectée, et le classificateur softmax obtient alors la sortie label à la fin du DeepVCM. Afin de démarrer le

processus de formation, nous définissons le même hyperparamètres pour la première partie et la deuxième partie du DeepVCM et les former en même temps, après la formation de DeepVCM, il sera automatiquement téléchargé sur les OBU et effectuer une détection du trafic de logiciels malveillants avant que le trafic ne passe par le VCM.[28]

2.1.3 Modèles hybride

ces modèles se base sur l'évaluation de la confiance liée aux véhicules et les données échangées.

Misbehavior detection based on support vector machine and dempster-shafer theory of evidence in vanets

Zhang et al. ont proposé une méthode pour la détection de mauvais comportement des véhicules dans les VANET en utilisant la théorie Dempstershaffer (DST) et une technique du Machine Learning la machine à vecteur de support ou SVM. Cette méthode consiste à détecter les messages et les véhicules malicieux, donc pour cela ils ont utilisé les deux modèles d'évaluation de la confiance basées entité et données. Pour le premier modèle consiste à détecter les véhicules malicieux à partir de leurs comportements et des messages déjà échangés et répond aux attaques par suppression de messages, et passe par deux étapes l'une est la locale trust model et l'autre la Trust Authority model, par contre le second consiste sur la détection des faux messages et réponds aux attaques par faux messages. Pour le model basée données, on utilise le model SVM pour classer les messages soit malicieux soit bon, où chaque message est défini par 5 paramètres : le type du véhicule, le type du message, la réputation, distance entre les deux véhicule, statut du message envoyé, après avoir obtenu la classe du message, s'il est bon alors on le prend en considération sinon on l'envoie au trust authority TA qui va s'en charger de la procédure de mise à jour de la réputation et de la valeur de la confiance du véhicule émetteur. Pour le model basé véhicule, on utilise la locale trust model pour classer les véhicules soit bon ou malicieux par rapport à leur comportement qui est défini par un vecteur de 4 paramètres qui sont, le taux de paquets retardés, le taux de paquets modifiés, le taux de paquets supprimés et le taux de paquets mal acheminés, par la suite un rapport sur le véhicule selon les résultats obtenus après la classification sera envoyé au Trust Authority. Enfin le trust authority, à partir des rapports envoyés par les véhicules adjacents seront agrégés par la théorie dempster-shaffer pour enfin prendre la décision à partir du résultat de la valeur de crédibilité. Et enfin, la réputation du véhicule sera mise à jour.[29]

Vehicular networks with security and trust management solutions via proposed secured message exchange via blockchain technology

Malik et al. ont proposés un système de gestion de confiance hybride qui utilise deux grandes phases, Dans le premier, afin d'assurer une communication sécurisée, la désinfection (dissimulation) des données sensibles les données avant la transmission sont requises et effectuées à l'aide d'une clé optimale, qui est générée par un algorithme d'optimisation appelé SLE-WOA (combination of Whale Optimization and Sea Lion Optimization Algorithm) par une requête envoyée au RSU, qui est en charge de la maintenance des clés utilisant la technologie blockchain. Une fois le message aseptisé diffusé parmi les véhicules, les véhicules récepteurs essaieront d'accéder aux données en demandant la clé optimale respective pour le RSU correspondant. Dans la deuxième phase, le RSU fera une évaluation de la confiance en utilisant la règle modèles

basés et basés sur le réseau de neurones pour décider si le nœud est authentifié ou non avant de fournir la clé. les valeurs de Packet delivery rate (PDR), Partenariats pour les énergies renouvelables (PFR) et l'indicateur d'intensité du signal reçu (RSSI) du nœud récepteur seront évalués et s'ils dépassent le seuil de chaque attaque de caractéristique respective, alors le nœud est réputé indigne de confiance et transmis au modèle NN qui est formé avec le comportement des nœuds pour PDR, PFR et RSSI et aide à prédire si le nœud est autorisé. si le RSU trouve le l'authentification soit un succès, il accorde la clé pour désinfecter et accéder aux données, sinon il néglige simplement sa demande.[19]

Trust Based Security Enhancements for Vehicular Ad hoc Networks

Wei and Boukerche a proposé une approche hybride qui détecte les véhicules qui se comportent mal en variation de vitesse et établit la confiance avec des interactions directes et des recommandations basées sur une combinaison de règles bayésiennes pour trouver la confiance et de la théorie de Dempster-Shafer (DST) pour la manipulation de l'incertitude. Chaque véhicule qui interagit avec un véhicule observé, peut juger si les messages sont digne de confiance ou non et fournir des preuves à un autre véhicule observateur de son point de vue, la valeur de la confiance est calculée à partir des preuves fournies par d'autres véhicules indépendamment. Chaque véhicule peut évaluer la confiance de ses véhicules voisins de manière distribuée, les interactions directes et recommandations sont ensuite combinées pour évaluer la confiance, la règle bayésienne est employée dans les interactions, qui peuvent continuellement réviser les valeurs de confiance grâce à de nouvelles preuves, tandis que la DST est utilisé pour tisser l'incertitude des recommandations de tiers dans l'évaluation de confiance pour améliorer la précision de la confiance, les valeurs de confiance sont alors stockées dans le module de référentiel de confiance et utilisé par les protocoles ou applications de la couche supérieure pour atteindre leurs objectifs.[24]

2.2 Classification

On peut déterminer trois de classe de modèle gestion de confiance dans les STI [15] :

— **Modèles basés entité :**
Les modèles basés sur les entités qui impliquent toutes les opérations du réseau, de manière temporaire ou permanente. La plupart des travaux proposés dans ce sous-ensemble adoptent une technique pour recueillir les recommandations d'autres nœuds, généralement en divisant les véhicules sur la route en différents clusters orchestrés par un clusterhead présélectionné.

— **Modèles basés données :**
Dans les modèles de confiance basés sur les entités, l'exclusion des nœuds malhonnêtes de toute opération peut entraîner un problème de déconnexion, surtout lorsqu'il y a de grands écarts entre les véhicules en raison d'un faible nombre de véhicules ou d'obstacles, ou en raison de révocations de nœuds en raison d'un comportement malhonnête ou égoïste inapproprié. L'idée de filtrer les messages malveillants sans révoquer leurs sources semble intéressante à considérer afin de réduire l'effet de ce problème de déconnexion.

— **Modèles hybrides** :
Les modèles hybrides, qui visent à assurer une communication fiable entre les nœuds face aux nœuds hostiles, ainsi qu'aux messages malveillants. La plupart des travaux existants adoptent une technique de clustering pour minimiser leur surcoût de communication , mais ces solutions centralisées échouent toujours dans le cas de clusterheads malveillants et dans des scénarios urbains très dynamiques.

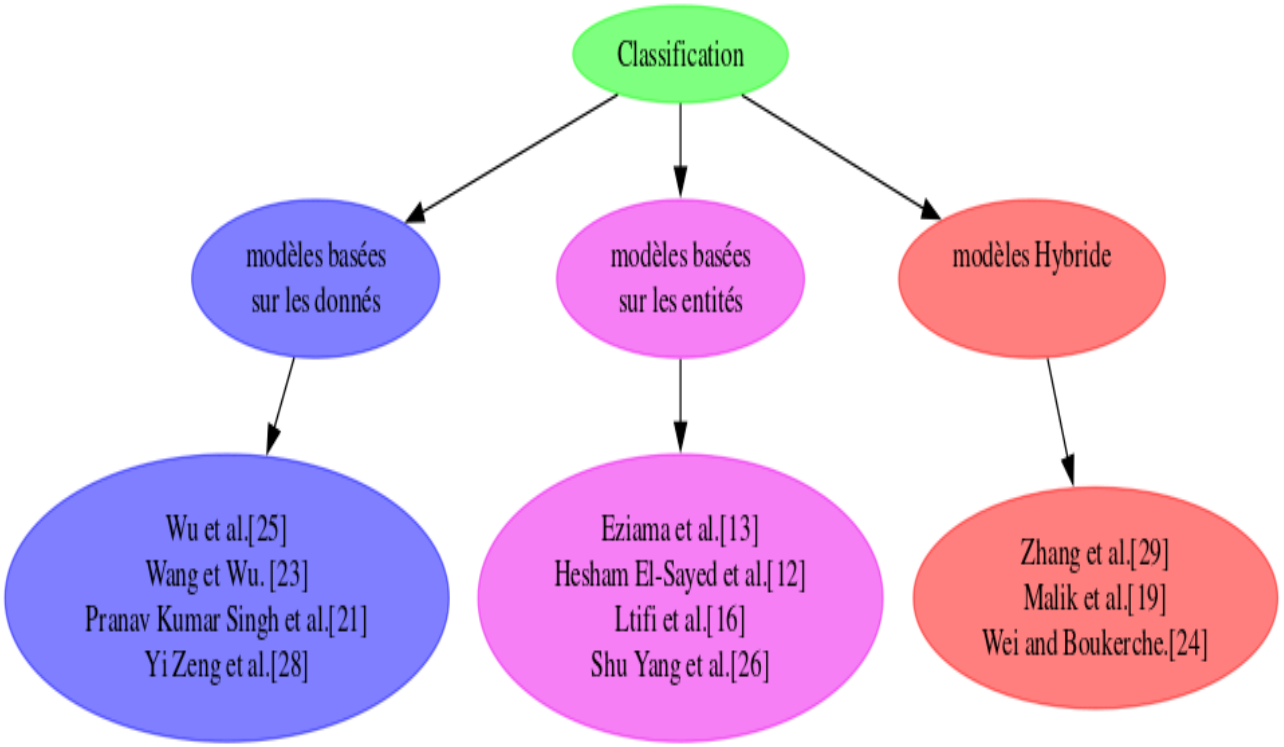

FIGURE 2.1 – Classification des articles proposées

2.3 Étude comparative

2.3.1 Paramètre de comparaison

nous allons prendre quelques paramètres afin de comparer entre les différent travaux vue auparavant :

— puissance de calcul (PC) :le débit de calcul du modèle, plus il utilise moins d'espace de calcul plus il est efficace

— espace de stockage utilisée (ES) :la quantité de consommation de stockage de mémoire utilisée par le modèle.

— types d'attaque contrés (TAC) :nombre et type d'attaques a contrer

— taux de détection : il s'agit du pourcentage de détection de faux messages ou véhicule

2.3.2 Tableau de comparaison

ce tableau est un tableau de comparaison entre les travaux déjà vus :

Classe	approche	PC	ES	TAC	taux de détection
entité	[13]	moyenne	haute	varié	haute
	[12]	Moyenne-haute	basse	Varier	90-99
	[16]	basse-moyenne	basse	Vol d'identité ,falsification de données	Haute
	[26]	haute	haute	falsification de données	Haute
données	[25]	moyenne	basse	falsification de données	90
	[21]	haute	basse	varié	92-99
	[28]	haute	Moyenne	Position falsification	96-98
	[23]	haute	haute	falsification de messages	90
hybride	[29]	haute	haute	injection de faux messages	99
	[19]	Haute	Haute	KPA,CCA,KCA,CPA	88
	[24]	Haute	Moyenne	Attaques internes	Haute

TABLE 2.1 – tableau comparatif

Discussion

Grâce à l'étude de certains documents de recherche, nous avons découvert de nombreuses techniques et méthodes dont le but est d'assurer la sécurité dans la structure du trafic. Certaines de ces méthodes ne n'apportent que leur lot d'avantages mais aussi d'inconvénients, différentes stratégies semblent utiles contre certaines attaques mais sont aussi plus vulnérables envers d'autres.

Les techniques suivantes dans le travail [19] ont utilisé la blockchain, la blockchain aide assurer la sécurité des données et apporter de la robustesse à la structure mais malgré cela c'est aussi a des points faibles et est vulnérable aux menaces telles que Black Hole Miners, Bad Mouthing et Mineurs malveillants.

La méthode sur l'apprentissage profond dans le papier [28] offre une meilleure indépendance vis-à-vis des humains pour sélectionner des fonctionnalités, mais cela nécessite beaucoup de puissance de calcul et plus de données pour être aussi égales ou plus efficace que les réseaux de neurones

La fausse méthode de falsification de position utilisée dans [21] semble être super-efficace lorsqu'il s'agit pour positionner les attaques de type falsification, mais pas très utile pour tout autre type d'attaques, qui le rend non fiable dans d'autres situations et scénarios.

Tous les paramètres que nous avons utilisés pour faire la comparaison nous ont aidés à montrer quelques différences entre les modèles utilisés et l'impact de chacune des stratégies et méthodes sur eux,cela, nous prendrons en considération quels pourraient être les éléments optimaux auxquels prêter attention et proposer notre propre approche. Dans l'article [29], la proposition est hybride ou en voit que la réputation des véhicules est prise en considération et est modifié, mais aussi elle prend en considération du comportement du véhicule, et cette méthode apporte une bonne précision où le SVM avec un noyau gaussien est le plus précis, mais n'empêche quand le nombre de véhicules où la réputation est diminuée on voit une baisse de précision du modèle.

2.4 Conclusion

Dans ce chapitre, nous avons présenté un état de l'art sur la gestion de la confiance dans les systèmes de transports intelligents, ce qui nous a donné un petit aperçu sur les méthodes pro-

posées, ainsi que les différents paramètres pris en considération dans des situations différentes pour chaque approche. Mais le plus important dans ces approches, c'est la finalité des valeurs trouvées qui nous conduisent toujours vers une prise de décision. Pour cela, dans le prochain chapitre, nous allons proposer une méthode basée sur le chatbot qui va nous aider à identifier la décision à prendre.

Chapitre 3

Proposition

3.1 Introduction

Dans notre cas, la fiabilité des messages est une priorité, pour cela une méthode de gestion de confiance pour l'assurance de calcul de sa valeur est nécessaire. nous allons utilisée les résultats obtenue dans l'approche proposée l'année dernière dans le mémoire[7] afin de calculer la fiabilité du message. une fois que le message est fiable cela va nous permettre d'accéder à la prise de décision.

3.2 Problématique

Dans les méthodes proposées, on trouve que la plupart se basent sur le calcule de confiance d'un message ou d'une entité à partir des relations d'échange entre les véhicules et leurs réputation, afin de savoir si le message est fiable ou pas, mais la finalité de ce message est de prendre une décision sur le choix à prendre au cours du trajet. pour cela nous nous sommes posés la question qui consiste sur comment peut-on intégrer l'avis du chauffeur dans la décision à prendre ?

3.3 Prise de décision :

3.4 Méthode proposée pour résoudre le problème

3.4.1 Arbre de décision

Arbre de décision est un algorithme de l'apprentissage automatique. c'est un type d'apprentissage supervisée, qui consiste à partir d'une structure arborescente de définir la décision à prendre comme réponse à la question poser. c'est à dire que les informations sont classée d'une manière logique sur un arbre afin de déterminer la décision a prendre. Un arbre de décision est caractérisée par une racine, des branches porteuses et des feuilles.[1]

- racine : consiste sur la question à laquelle on va répondre, et elle consiste sur la décision à prendre.
- branches porteuses : consiste sur les choix pris.
- les feuilles : consiste sur les décision a prendre.

Dans notre cas, la racine et les noeuds consistent en les questions a poser, les branches représente les réponses aux questions, et enfin les feuilles les valeurs qui consistent en la représentation de l'avis du conducteur. voici une image qui représente l'arborescence sur lequel le chat bot est conçue.

Choix des questions : Valeurs en fonction de la réponse.

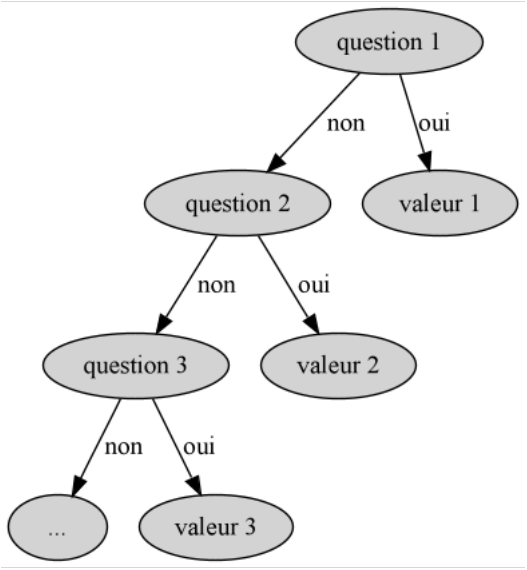

FIGURE 3.1 – l'arbre représentant le chat-bot

3.4.2 Outils utilisés

outils utilisées pour la conception du chabot sont comme suit :

3.4.3 Python

Python est un langage de programmation open source, le plus utilisé dans le domaine de l'apprentissage automatique. Créé en 1991 par le développeur Guido Van Rossum, le langage de programmation Python apparu à l'époque comme une façon d'automatiser les éléments les plus ennuyeux de l'écriture de scripts ou de réaliser rapidement des prototypes d'applications. Depuis quelques années, toutefois, ce langage de programmation est parmi les plus utilisés dans les domaines du développement de logiciels, de gestion d'infrastructure et d'analyse de données.il possède de nombreuse bibliothèque qui servent pour facilité certaines tâche.[5]

3.4.4 Pycharm

Pycharm est un environnement de développement intégré multiplateformes conçu par JeTBrains, qui est dédié au langage de programmation python. il comprend plusieurs spécification qui consiste à aider le programmeur à écrire son code dans de bonne conditions, ce qui le rend l'un des meilleurs environnement de développement en python.[4]

3.4.5 Bibliothèque

Bibliothèque constituent un ensemble de modules pré-définies qui représente des algorithmes existant, afin de les utilisées sans les refaire a chaque fois, généralement elles contiennent des fonctions de même thème.plusieurs bibliothèques existes dans python et chacune contient des fonctions prédéfinies pour des taches spécifiques.[3]

Tkinter : est une bibliothèque python spécialiser dans la réalisation des applications graphiques en python.[6]

3.5 Présentation du chatbot

Après avoir obtenu la valeur de la confiance, les messages qu'ont une valeur plus grande qu'un certain seuil, d'une autre manière on peut considérer le message comme étant fiable. dans ce cas,le chatbot qu'est de type à réponse rapide, qui va nous permettre de connaître l'avis du conducteur au cours d'un trajet, va nous permettre d'avoir une valeur qui va représenter le coefficient de confiance afin d'avoir la décision finale.

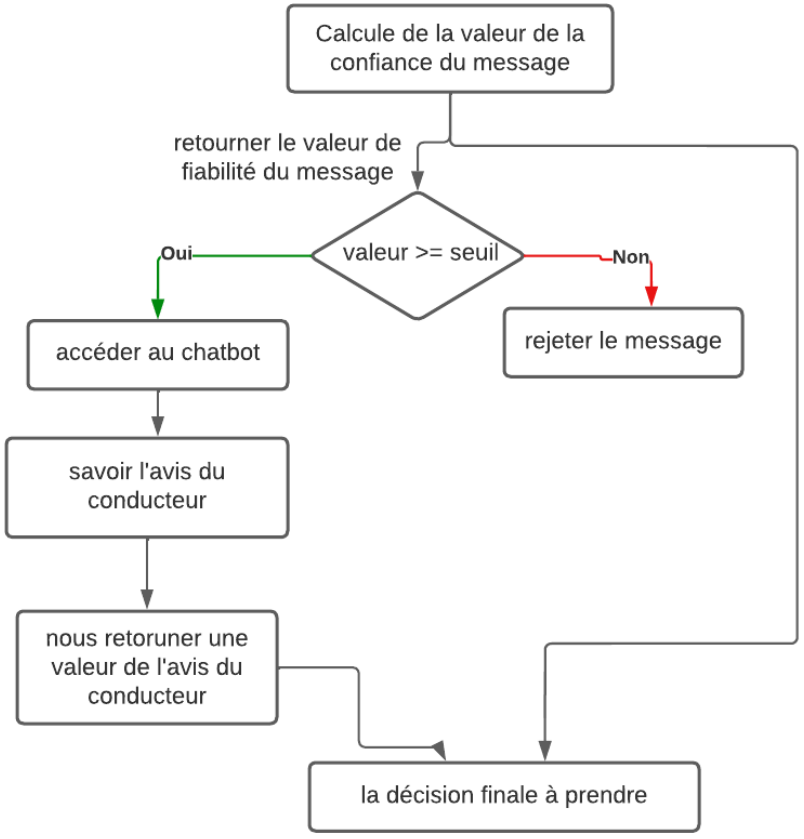

FIGURE 3.2 – un diagramme représentant le rôle du chatbot

Nous allons expliquer quelque notions sur ce diagramme :

— **seuil :** c'est la valeur minimale qu'on peut attribuer pour un message.

— **accès au chat bot :** c'est à dire que le chat-bot est activer que lorsque le message est fiable, et que une décision sera prise à partir de ce message.

— **la valeur de l'avis du conducteur :** cette valeur consiste sur les valeurs présenter dans l'arbre de la figure 3.1 . il s'agit d'une valeur trouver à partir d'une séquence de question poser qu'est guider à partir des réponses du conducteur.

— **décision finale à prendre :** cette décision consiste en une multiplication entre la valeur de confiance obtenu et la valeur de l'avis du conducteur. c'est à dire que cette valeur serait le coefficient de confiance. A partir de cette valeur, une réponse va être afficher dans

3.6 Présentation de quelques questions proposée :

On va présenter quelques questions proposées, ou on s'est basée sur les messages qui sont reliées à la circulation routière, comme les embouteillage, les accidents,....Pour cela les questions choisit seront sur l'itinéraire à choisir et sur l'état du conducteur (presser ou non) et sur d'autre possibilité à voir plus tard.ajoutant à cela que le choix des questions est important afin d'avoir le bon choix des valeurs à choisir.

Réponse au question : Pour répondre à la première question dès l'arrivée d'un message fiable, nous allons procéder comme suit :

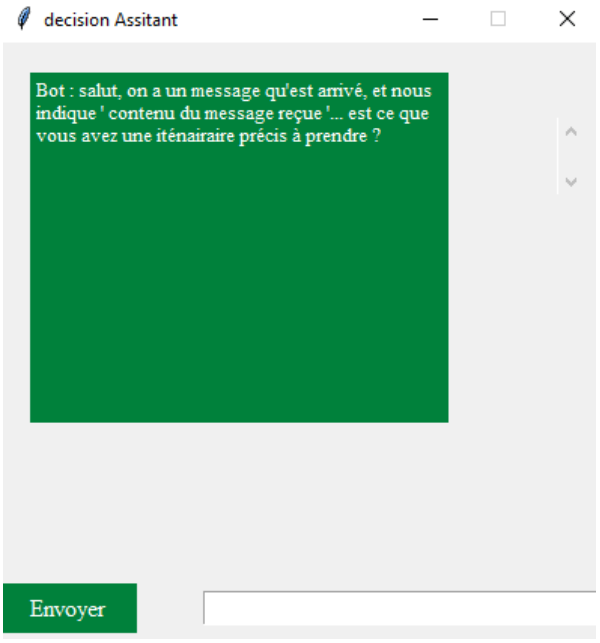

FIGURE 3.3 – première question

Si la réponse est positive (oui), alors l'avis du conducteur sera de choisir son itinéraire.

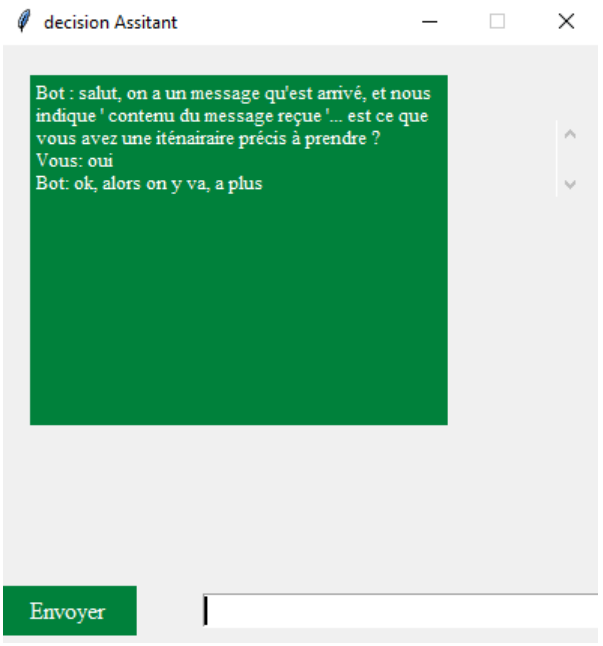

FIGURE 3.4 – deuxième question

Si la réponse du conducteur est "non", nous passons à la question suivante, comme suit :

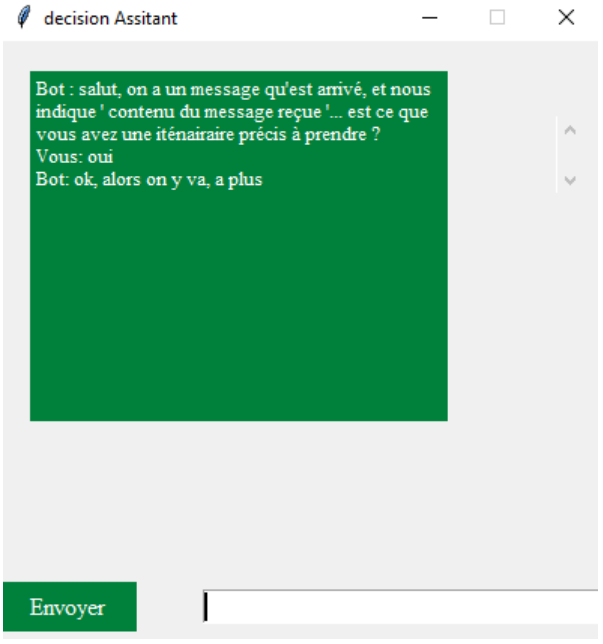

FIGURE 3.5 – Troisième question

dans le cas ou le conducteur répond 'non' alors on va dévier , c'est d'éviter le problème déclarer par le message reçue

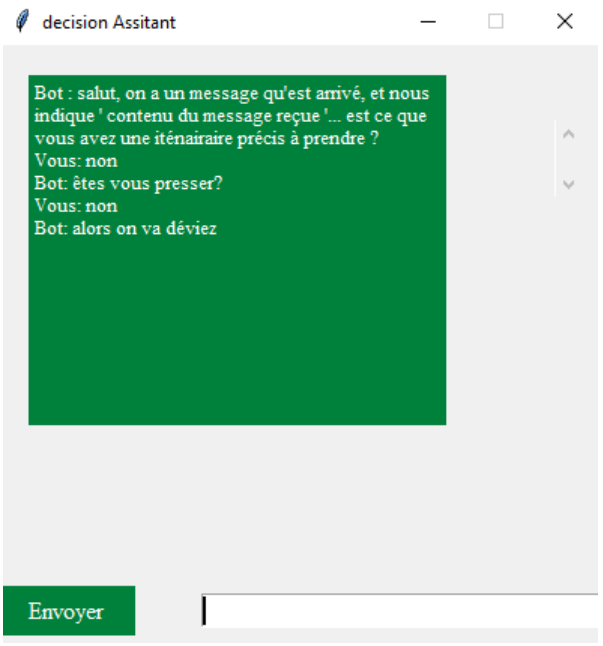

FIGURE 3.6 – quatrième question

3.6.1 Prise de décision :

Afin d'établir une décision à prendre,tout d'abord nous faisons appel a la valeur de la confiance qu'a été calculer dans le travail fait l'année dernière dans "Proposal for a new trust management system in intelligent transport systems" proposées par A.CHETTAB et Y.CHETTAB, où la valeur trouvées dans le cadre du calcule de la confiance. cette valeur trouvée,on va la noté ValConf. Ensuite afin de déterminer la décision a prendre nous allons calculer le produit de la valeur produite par le chatbot "Val" par la valeur de la confiance calculé déjà ValConf.
on obtiendra :

Decision = ValConf x Val

Après avoir calculer la valeur de la décision à prendre. Un seuil S sera déterminer après avoir calculer la valeur de la confiance, où (0<S<1) il va déterminer Si (Décision> S) Alors on va dire que la décision à prendre est celle du choix du conducteur, Sinon on va prendre la décision relier à la valeur de la confiance.

3.7 Conclusion

En conclusion,Ce que nous avons apporter dans le cadre du calcule de la confiance réaliser dans le travail [8] ,c'est dans le coté de la décision finale après avoir trouvé que le message reçu est correcte. On peut dire que le chatbot nous a permis de connaître l'avis du conducteur, et de l'intégrer dans la prise de décision au cours du trajet a partir du message reçue.

Conclusion et perspectives

Dans notre travail, nous avons examiné différentes approches pour le calcul de la gestion de la confiance dans les systèmes de transport intelligents. En réfléchissant à une alternative, nous avons proposé d'intégrer l'avis du conducteur dans la prise de décision après le calcul de fiabilité des données, à travers un chatbot orienté but. Pour cela, nous avons utilisé la méthode de calcul de la valeur de confiance présentée dans le mémoire [8], puis nous avons utilisé cette valeur pour déterminer la décision finale.

À l'avenir, nous envisageons de mettre en place un chatbot basé sur l'intelligence artificielle et l'apprentissage automatique, capable de sélectionner les messages fiables et de communiquer avec le conducteur pour recueillir son avis en analysant ses sentiments. Cette amélioration permettrait d'optimiser la prise de décision en prenant en compte les préférences et les avis des conducteurs.

Bibliographie

[1] arbre de decision. https://everlaab.com/arbre-de-decision/. (consulter le 27/08/2022).

[2] bibliothèque. https://www.techtarget.com/searchcustomerexperience/definition/chatbot. (consulter le 27/08/2022).

[3] bibliothèque. https://www.data-bird.co/python/bibliotheque-python. (consulter le 27/08/2022).

[4] pycharm. https://www.rswebsols.com/tutorials/programming/pycharm-mandatory-python-programmer. (consulter le 27/08/2022).

[5] python. https://fr.tuto.com/blog/2020/11/python.htm. (consulter le 27/08/2022).

[6] tkinter. http://www.xavierdupre.fr/app/teachpyx/helpsphinx/c_gui/tkinter.html#introduction. (consulter le 27/08/2022).

[7] CHETTAB Abdelkader and Yasmine CHETTAB. Proposal for a new trust management system in intelligent transport systems. 2021.

[8] Yasmine CHETTAB Abdelkader CHETTAB. *Proposal for a new trust management system in intelligent transport systems.* PhD thesis, 2021.

[9] Flavien Balbo, Emmanuel Adam, and René Mandiau. Positionnement des systèmes multi-agents pour les systèmes de transport intelligents. *Revue des Sciences et Technologies de l'Information - Série RIA : Revue d'Intelligence Artificielle*, 30(3) :299–327, 2016.

[10] Aït-Salem Boussad. *Sécurisation des réseaux ad hoc : systèmes de confiance et de détection de répliques.* PhD thesis, Université de Limoges, 2011.

[11] Cherif TOLBA Djamel BEKTACHE and Nassira GHOUALMI. *Application et Modélisation d'un Protocole de Communication pour la Sécurité Routière.* PhD thesis, Univérsité Badji Mokhtar Annaba, 2014.

[12] Hesham El-Sayed, Henry Alexander Ignatious, Parag Kulkarni, and Salah Bouktif. Machine learning based trust management framework for vehicular networks. *Vehicular Communications*, 25 :100256, 2020.

[13] Elvin Eziama, Kemal Tepe, Ali Balador, Kenneth Sorle Nwizege, and Luz MS Jaimes. Malicious node detection in vehicular ad-hoc network using machine learning and deep learning. pages 1–6, 2018.

[14] Gregorio Martínez Pérez Félix Gómez Mármol. Trip, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks, 2018.

[15] Chaker Abdelaziz Kerrache, Nasreddine Lagraa, Carlos T. Calafate, Juan-Carlos Cano, and Pietro Manzoni. T-vnets : A novel trust architecture for vehicular networks using the standardized messaging services of etsi its. *Computer Communications*, 93 :68–83, 2016. Multi-radio, Multi-technology, Multi-system Vehicular Communications.

[16] Amel Ltifi, Ahmed Zouinkhi, and Med Salim Bouhlel. Smart trust management for vehicular networks. *International Journal of Electronics and Communication Engineering*, 10(8) :1128–1135, 2016.

[17] Shuo Ma, Ouri Wolfson, and Jie Lin. A survey on trust management for intelligent transportation system. CTS '11, page 18–23, New York, NY, USA, 2011. Association for Computing Machinery.

[18] Ali Mirza Mahmood, Naganjaneyulu Satuluri, Mrithyumjaya Rao Kuppa, et al. An overview of recent and traditional decision tree classifiers in machine learning. *International Journal of Research and Reviews in Ad Hoc Networks*, 1(1) :2011, 2011.

[19] Nisha Malik, Priyadarsi Nanda, Xiangjian He, and Ren Ping Liu. Vehicular networks with security and trust management solutions : proposed secured message exchange via blockchain technology. *Wireless Networks*, 26(6) :4207–4226, 2020.

[20] Kashif Naseer Qureshi and Hanan Abdullah. A survey on intelligent transportation systems. *International Journal of Electronics and Communication Engineering*, 2013.

[21] Pranav Kumar Singh, Shivam Gupta, Ritveeka Vashistha, Sunit Kumar Nandi, and Sukumar Nandi. Machine learning based approach to detect position falsification attack in vanets. In *International Conference on Security & Privacy*, pages 166–178. Springer, 2019.

[22] Van-Hoan Vu. *Infrastructure de gestion de la confiance sur internet.* PhD thesis, Ecole Nationale Supérieure des Mines de Saint-Etienne, 2010.

[23] Guanghao Wang and Yue Wu. Bibrm : A bayesian inference based road message trust model in vehicular ad hoc networks. In *2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications*, pages 481–486, 2014.

[24] Zhexiong Wei, Fei Richard Yu, and Azzedine Boukerche. Trust based security enhancements for vehicular ad hocnetworks. In *Proceedings of the fourth ACM international symposium on Development and analysis of intelligent vehicular networks and applications*, pages 103–109, 2014.

[25] Yue Wu, Fanchao Meng, Guanghao Wang, and Ping Yi. A dempster-shafer theory based traffic information trust model in vehicular ad hoc networks. In *2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)*, pages 1–7. IEEE, 2015.

[26] Shu Yang, Zhihan Liu, Jinglin Li, Shangguang Wang, and Fangchun Yang. Anomaly detection for internet of vehicles : A trust management scheme with affinity propagation. *Mobile Information Systems*, 2016, 2016.

[27] Benyamina Zakaria, Fateh Bounaama, and Khelifa benahmed. Les systemes de transport intelligent (sti). 06 2017.

[28] Yi Zeng, Meikang Qiu, Dan Zhu, Zhihao Xue, Jian Xiong, and Meiqin Liu. Deepvcm : a deep learning based intrusion detection method in vanet. In *2019 IEEE 5th intl conference on big data security on cloud (BigDataSecurity), IEEE intl conference on high performance and smart computing,(HPSC) and IEEE intl conference on intelligent data and security (IDS)*, pages 288–293. IEEE, 2019.

[29] Chunhua Zhang, Kangqiang Chen, Xin Zeng, and Xiaoping Xue. Misbehavior detection based on support vector machine and dempster-shafer theory of evidence in vanets. *IEEE Access*, 6 :59860–59870, 2018.