UNIVERSITÉ DU QUÉBEC

MÉMOIRE PRÉSENTÉ À

L'UNIVERSITÉ DU QUÉBEC À TROIS-RIVIÈRES

COMME EXIGENCE PARTIELLE

DE LA MAÎTRISE EN MATHÉMATIQUES ET INFORMATIQUE APPLIQUÉES

PAR

CAROLY GABRIELA PEREIRA DIAZ

DÉVELOPPEMENT D'UN MODÈLE HYBRIDE DE PRÉDICTION D'ATTAQUES POUR LES RÉSEAUX VÉHICULAIRES AD HOC (VANETs)

JUILLET 2018

À Dieu,
À ma mère,
À la mémoire de mon père,
À mes neveux Lucas, Maximiliano et le nouveau bébé à venir,
À mon cher Guillaume,
À toute la famille Morin,
Á tous ceux que j'aime.

Caroly

REMERCIEMENTS

Je voudrais tout d'abord adresser toute ma gratitude au directeur de ce mémoire, le Professeur Boucif Amar Bensaber, pour le temps qu'il a consacré à m'apporter les outils méthodologiques indispensables à la conduite de cette recherche. Pour sa patience, sa disponibilité et surtout pour sa confiance.

Avec beaucoup d'égard, je remercie les professeurs François Meunier et Ismail Biskri d'avoir accepté d'évaluer mon travail.

J'adresse mes sincères remerciements à toutes les personnes qui par leurs paroles, leurs écrits, leurs conseils et leurs critiques m'ont guidé pendant chaque étape de cette recherche.

Je désire aussi remercier les professeurs et tous mes collègues du département de mathématiques et d'informatique, qui m'ont fourni les outils nécessaires à la réussite de mes études.

Je voudrais exprimer ma reconnaissance envers mes amis qui m'ont apporté leur support moral et émotionnelle tout au long de ma démarche. Un grand merci à Evelin et Kelmys pour leur amitié et leur support inestimable. Enfin, je tiens à témoigner toute ma gratitude à Nathaly et Leonel, pour leur confiance, leur soutien inconditionnel et leur encouragement.

À tous ces intervenants, je présente mes remerciements, mon respect et ma gratitude.

LISTE DES ABRÉVIATIONS

ANFIS: Adaptive Neuro-Fuzzy Inference System.

DOS: Denial of Service.

DSRC: Dedicated Short Range Communication.

ECDSA: Elliptic Curve Digital Signature Algorithm.

ECIES: Elliptic Curve Integrated Encryption Scheme.

IEEE: Institute of Electrical and Electronics Engineers.

ITS: Intelligent Transport System.

MAC: Medium Access Control.

MANET: Mobile Ad hoc Network.

OBU: On Board Unit.

RSS: Received Signal Strength.

RSU: Road Side Unit.

SHA: Secure Hash Algorithm.

VANETs: Vehicular Ad hoc Networks.

V2V: Vehicle to Vehicle.

V2I: Vehicle to Infrastructure.

WAVE: Wireless Access in Vehicular Environments.

WLAN: Wireless Local Area Network

DÉVELOPPEMENT D'UN MODÈLE HYBRIDE DE PRÉDICTION D'ATTAQUES POUR LES RÉSEAUX VÉHICULAIRES AD HOC (VANETs)

Caroly Gabriela Pereira Diaz

SOMMAIRE

Les réseaux véhiculaires ad-hoc (VANETs) sont un type particulier de réseaux mobiles. Dans VANETs, les nœuds qui participent à la communication sont des véhicules. Les réseaux véhiculaires ont été conçus principalement comme support à la sécurité routière. Il y a plusieurs avantages à implémenter ce genre de réseau. Il nous permet de contrôler la circulation et d'améliorer les conditions de transport dans les véhicules en offrant des systèmes de divertissement connectés. Mais souvent, les informations qui circulent dans ces réseaux sont sensibles et comme ces systèmes de communication sont ouverts, alors tout nœud connecté au réseau est potentiellement vulnérable aux intrusions. Afin de répondre à cette problématique, le présent travail de recherche propose un modèle hybride de prédiction des attaques basé sur la logique floue et les réseaux neurones.

Aujourd'hui, il n'y a pas d'implémentation réelle des VANETs, mais il existe différents simulateurs qui permettent d'obtenir les informations sur le fonctionnement de ce réseau. Pour bâtir notre modèle, on s'est servi des résultats de simulation dans deux différents environnements. Le premier, un réseau sans attaque et le deuxième un réseau avec attaques. Les données ont été traitées et analysées statistiquement afin d'avoir plus de précision dans la prédiction. Finalement, on a conçu un modèle qui donne un indicateur qui permet de prédire s'il y a une attaque sur un véhicule.

DEVELOPMENT OF A HYBRIDE MODEL FOR ASSESSING SECURITY TO VEHICULAR AD HOC NETWORKS (VANETs)

Pereira Diaz, Caroly Gabriela

ABSTRACT

Vehicular Ad-hoc networks (VANETs) are a specific kind of mobile network. In VANETs, the nodes involved in communication are the vehicles. Vehicular networks have been designed mainly as a support for road safety. There are several advantages in implementing this kind of network. Among the most important, the traffic control and improvement in the vehicles transport conditions (infotainments).

The value of data circulating in the networks is very high. When, we talk about communication systems like VANETs, we know that any node connected to the network is potentially vulnerable to attacks. In the context of improving the security of vehicular networks, this research project proposes a hybrid model for attack prediction based on fuzzy logic and neural networks.

Today, there is no real implementation of VANETs, but there are different simulators that can obtain information about the operation of this network. To build our model, we used simulation results in two different environments. First, a network without attack and a second network with attack. The data was processed and analyzed statistically to ensure more precision in the prediction. Finally, a model has been designed to help measure the level of security in VANETs by predicting whether a vehicle is attacked or not.

TABLE DE MATIÈRES

LISTE DE FIGURES

INTRODUCTION

Dans les dernières années, l'évolution des appareils mobiles et l'utilisation des différentes technologies sans fil a avancé très rapidement. La plupart de ces nouvelles technologies ont nécessité des années d'étude et de recherche avant d'être mises en œuvre. L'évolution actuelle des systèmes de communication permet l'émergence de nouveaux domaines d'exploration, tel que les Systèmes de Transport Intelligents (ITS).

Les réseaux véhiculaires ad-hoc (VANETs), sont une nouvelle technologie qui devrait révolutionner les moyens de transport existants. Ils sont une représentation claire des tendances dans les communications du futur. Les réseaux interconnectés avec les communications de véhicules ont été étudiés depuis les années 1970 [1].

Les réseaux VANETs sont créés lorsque différents véhicules se connectent avec ou sans l'utilisation d'infrastructure. Dans certaines situations, l'absence d'infrastructure est un avantage, mais cela crée aussi beaucoup de défis qui doivent être surmontés. D'autres inconvénients dans cette technologie sont la vitesse avec laquelle les véhicules circulent et la topologie qui change constamment. Tout cela affecte la sécurité lors de la transmission de l'information.

La principale contribution dans ce réseau est le développement d'applications dans le cadre des systèmes de transport intelligents. Ces applications servent à fournir l'information sur le trafic, elles aident à améliorer la sécurité routière et en même temps elles contribuent à l'efficacité des transports privés et publiques.

Il y a plusieurs conditions techniques dans les opérations des VANETs qui mettent en risque la communication entre les nœuds. Le routage, la vitesse des véhicules et la perte d'informations à cause de la connexion sans fil, sont seulement quelques exemples de problèmes qui peuvent affecter la sécurité. Alors le réseau devient très vulnérable aux attaques.

De nombreux risques doivent être pris en compte dans ces réseaux. Les plus importants sont la gestion de l'identité des véhicules et la véracité de l'information. Pour minimiser ces

risques, il y a certains mécanismes qui peuvent être utilisés pour s'assurer de l'authentification des données et la protection de la confidentialité.

Ce travail présente une des premières propositions de « *soft computing* » pour la prédiction d'attaques dans VANET. Nous proposons un système d'inférence neuro-floue adaptatif (ANFIS) pour obtenir un modèle de prédiction d'un indicateur de sécurité dans les VANETs. Le processus de recherche commence par les simulations de réseau, avec l'objectif d'obtenir une base de données sans attaque et une autre avec l'occurrence d'attaques. Ensuite, cette base de données est préparée et analysée statistiquement. Dans tous les modèles de prédiction, il est très important de décrire le type de données à traiter, ainsi que de connaitre et d'analyser la relation entre les variables. Enfin, avec l'utilisation du logiciel MATLAB, nous obtenons un modèle capable de prédire un indicateur de sécurité qui permet d'estimer la vulnérabilité du réseau en cas d'attaques.

Le reste de ce document est organisé comme suit : dans le chapitre 1, on va présenter quelques définitions importantes sur les réseaux VANETs, leurs caractéristiques et leurs besoins en termes de sécurité. Dans le chapitre 2, nous présentons quelques travaux de littérature sur la sécurité des réseaux VANETs et des différentes approches proposées pour la détection d'attaques. Le chapitre 3 est une introduction des différentes méthodes de prédiction utilisées dans le cadre de cette recherche. Puis dans le chapitre 4 nous présentons la méthodologie et la description de notre modèle, sous forme d'un article scientifique. Dans le chapitre 5, nous discutons nos résultats. Enfin, dans le chapitre 6, nous présentons la conclusion générale de ce travail de recherche.

CHAPITRE 1

GÉNÉRALITÉS SUR LES VANETS

1.1. Les réseaux Ad-Hoc

Un réseau Ad-Hoc est un type de réseau composé d'un ensemble de nœuds qui sont capables de communiquer via une interface (généralement sans fil) de manière décentralisée. Chaque nœud est capable de transmettre de l'information au reste des composants, comme illustré sur la figure 1. La décision de retransmettre cette information est prise de manière dynamique en fonction de la connectivité du réseau.

Ainsi, chaque nœud participe au routage de l'information en envoyant les données aux autres nœuds de manière indépendante. C'est-à-dire, qu'un pont est établi entre l'origine et la destination grâce aux nœuds intermédiaires et l'information est transmise de nœud à nœud jusqu'au destinataire.

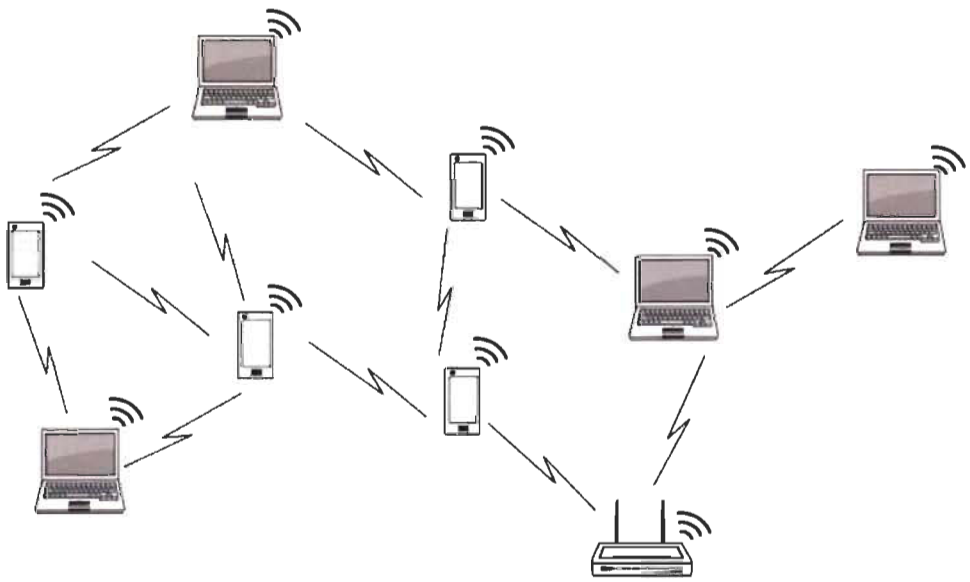

Figure 1. Réseau Ad Hoc

Il existe différents types de réseaux Ad-Hoc et ils peuvent être classés en fonction de leur domaine d'application.

1.2. Les réseaux MANETs (Mobile Ad Hoc Network)

Les MANETs sont un exemple de réseau ad-hoc qui ajoute la fonctionnalité de mobilité aux nœuds. Cela signifie que les liens entre les changent continuellement : il y a des nœuds qui s'incorporent ou quittent le réseau en tout temps. Donc la topologie du réseau est très variable et aléatoire. Tous les nœuds peuvent agir en tant qu'émetteurs, récepteurs ou routeurs, ceci est nécessaire puisque les routes pour atteindre une destination peuvent avoir plusieurs sauts.

Les réseaux véhiculaires sont considérés comme un type spécifique de MANETs, la principale différence est que les nœuds sont contraints de se déplacer uniquement le long des rues, des routes et des autoroutes.

1.3. Les réseaux VANETs (Vehicular Ad Hoc Network)

Dans les réseaux VANETs, chaque véhicule est défini comme un nœud du réseau. Les véhicules sont équipés d'une unité de communication appelé OBU (*On Board Unit*), elle sert pour la connexion avec l'Internet.

On peut considérer aussi des unités d'application pour montrer l'information au conducteur, elles sont connectées avec l'OBU. Ces unités peuvent être les tablettes, les téléphones intelligents ou les ordinateurs [3] mais ils ne sont pas une partie fondamentale des réseaux VANETs.

L'OBU sert pour l'échange de messages entre les nœuds et/ou avec les RSUs (*Road Unit Side*) qui sont les points d'accès fixes situés autour des routes. Les messages émis par l'OBU peuvent contenir des informations sur les conditions météorologiques, l'état de transit ainsi que des informations provenant d'autres véhicules qui font de longues distances tout en restant connecté au réseau. Une autre fonction de l'OBU est de connecter les véhicules aux différentes applications proposées [4].

1.3.1. Communications dans les réseaux VANETs

Dans ce réseau, il existe deux environnements de communication (cf. fig. 2) :

- **Environnement de communication véhiculaire :**

  Cet environnement est appelé V2V (*Vehicle To Vehicle*) dont l'architecture est décentralisée. C'est un mode de communication directe entre les nœuds du réseau, c'est-à-dire, de véhicule à véhicule. Alors, pour envoyer ou recevoir les messages, il n'est pas nécessaire d'avoir une infrastructure externe, il suffit que les nœuds soient dans le même périmètre de communication. Dans les réseaux VANETs, cet environnement de communication est très instable, étant donné la vitesse et la mobilité constante des nœuds.

- **Environnement d'infrastructure de communication :**

  Il s'agit d'un environnement avec deux entités, les véhicules et l'infrastructure de communication (V2I, *Vehicle To Infrastructure*). On peut dire que l'état de connexion dans cet environnement est plus stable. Une infrastructure de communication peut être une antenne, un satellite ou le RSU. Les différentes infrastructures comprises dans le réseau peuvent également établir des communications entre-elles d'une façon autonome.

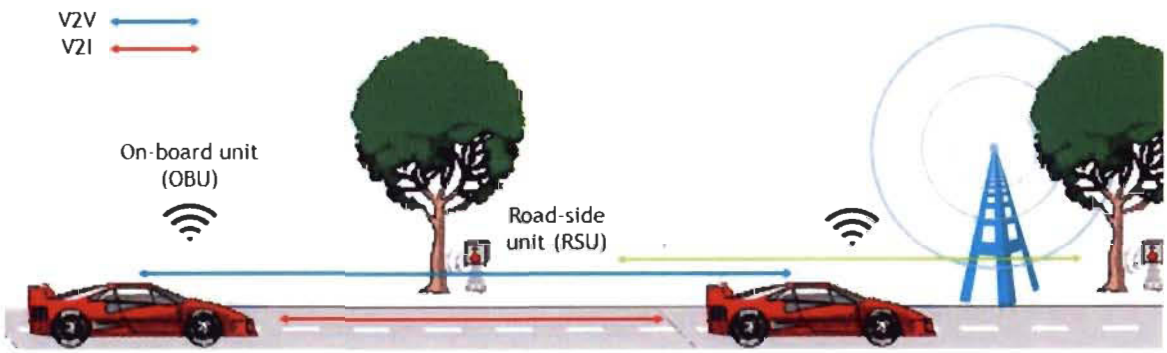

Figure 2. Modes de communication dans les VANETs

1.3.2. Les normes 802.11p et IEEE 1609.4

Les réseaux VANETs ont quelques caractéristiques très importantes qui les distinguent, comme la vitesse avec laquelle les nœuds (véhicules) se déplacent et le court temps pour gérer la connexion entre eux. D'où l'importance des normes IEEE 802.11p et IEEE 1606.4 qui ont été définies pour spécifier les détails techniques et d'opérations sur les WAVE (*Wireless Access in Vehicular Environment*) (figure 3).

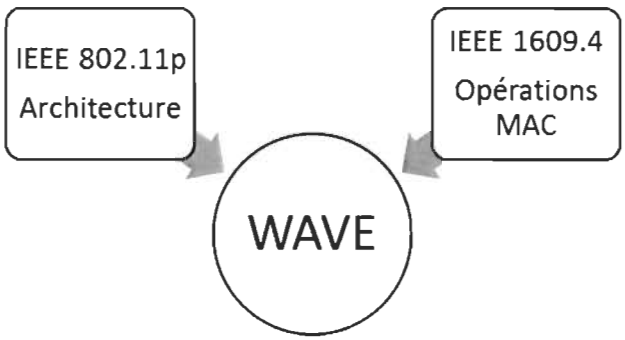

Figure 3. Normes IEEE 802.11p et IEEE 1609.4

Le standard 802.11 est la norme créée pour réguler les communications sans fil. Le groupe de travail de l'IEEE 802.11 a travaillé aussi sur la norme 802.11p [6]. Le WAVE est soumise à de multiples réglementations, dont l'une est la famille de normes IEEE 1609. Cette famille définit, entre autres facteurs, les aspects physiques et logiques de gestion de réseau, ainsi que les problèmes de sécurité associés. Le WAVE a évolué afin de répondre aux caractéristiques des réseaux VANETs [7]. Ces systèmes fournissent des appareils sans fil capables d'échanges d'information à court terme, tel que les véhicules qui se déplacent à vitesses élevées.

La norme IEEE 1609.4 est responsable de la coordination des canaux. Elle est composée de fonctionnalités supplémentaires pour les opérations dans la sous-couche MAC spécifiée dans IEEE 802.11p.

1.3.3. Domaines d'application

Les principaux domaines d'application des réseaux VANETs, sont dans les services publics, la sécurité routière, l'amélioration de la conduite, la publicité et le divertissement.

Avec la mise en œuvre des réseaux VANETs, les utilisateurs de véhicules ont à leur disposition des différents types d'applications qui leur fournissent une meilleure information sur les conditions du trafic. Ils peuvent accéder aux informations afin d'améliorer la qualité du voyage des passagers. On peut considérer deux types d'applications :

- **Applications de confort :**

  Ces applications sont dirigées vers le divertissement et l'amélioration des conditions de voyage pour les passagers et le conducteur. En utilisant l'Internet, elles offrent différents services, tels que les informations et la localisation des stations d'essence, restaurants, attractions, service de paiement automatique des péages sur les autoroutes, ainsi que les applications pour la vidéoconférence, les jeux en ligne et le partage de fichiers multimédia, entre autres.

- **Applications de sécurité et prévention :**

  En plus d'améliorer la conduite et le transport, ces réseaux ouvrent la porte à de nouveaux mécanismes qui visent à simplifier la tâche de conduite et d'accroître la sécurité routière. Ainsi, à travers ces réseaux, on peut fournir l'assistance au conducteur du véhicule [5]. Les services d'information et la sécurité routière ont particulièrement l'intérêt social pour réduire le nombre de morts tragiques dans les accidents sur les routes. Grâce aux VANETs, on peut alerter les véhicules à proximité d'un accident ou de la congestion, et ainsi les conducteurs peuvent prendre les mesures appropriées dans un temps opportun. De même, le conducteur peut changer sa trajectoire pour éviter la congestion véhiculaire, par exemple.

1.3.4. Caractéristiques

Pour les distinguer des réseaux MANETs, les VANETs ont leurs propres caractéristiques qui sont la base de la définition des technologies et des protocoles d'utilisation. Les

principales caractéristiques de la communication des VANETs sont décrites ci-dessous [3] :

- **Topologie dynamique** : les VANETs sont caractérisés par une connectivité sporadique, car un véhicule (nœud) peut rejoindre ou quitter un groupe de véhicules en un temps très court. Ce qui nous mène ainsi à avoir une topologie très dynamique constituée de plusieurs ilots séparés [9]. Décrire une topologie de réseau spécifique pour un réseau VANETs est particulièrement exigeant en raison de la nature même des véhicules. Les nœuds sont constamment en mouvement et les communications V2V et V2I peuvent se produire très rapidement, ce qui rend difficile d'identifier une topologie spécifique pour ces réseaux.

- **Canaux variables dans le temps et des fréquences** : plusieurs facteurs peuvent affecter la mobilité dans ces réseaux, tel que les infrastructures routières; par exemple : route, autoroute, panneaux de signalisation [10]. En raison de la vitesse des véhicules, les environnements et les possibles obstacles (bâtiments, arbres, etc.), la communication peut subir des pannes dans le temps de transmission ou dans la fréquence avec plus d'intensité que d'autres réseaux mobiles.

- **Autonomie** : se réfère à la liberté de chaque nœud dans le réseau, l'accès, la capacité de transmettre et de recevoir l'information en cas de besoin sans être sous l'influence d'un contrôle centralisé. Alors l'OBU et le RSU gèrent ces tâches de façon indépendante.

- **Offre illimitée de l'énergie :** contrairement au contexte des réseaux MANET où la contrainte d'énergie représente un défi, les éléments du réseau VANET disposent suffisamment d'énergie [9]. Les nœuds n'ont pas de restrictions sur la consommation d'énergie, la batterie du véhicule offre une quantité suffisante pour faire fonctionner l'OBU et les différents équipements électroniques d'une voiture intelligente.

1.3.5. Sécurité

L'importance des informations échangées via les communications véhiculaires rend l'opération de sécurisation de ces réseaux cruciale. Ceci constitue un pré-requis au déploiement des VANETs [11].

Une des questions cruciales est assurer l'information, ainsi que la protection de la vie privée. Ces aspects sont partiellement traités dans la norme IEEE 1609.2 [12]. Cette norme a été créé pour l'ensemble des protocoles utilisant WAVE (Wireless Access in Vehicular Environments). Les principales exigences de la sécurité dans les réseaux VANETs sont représentées la figure 4 [13].

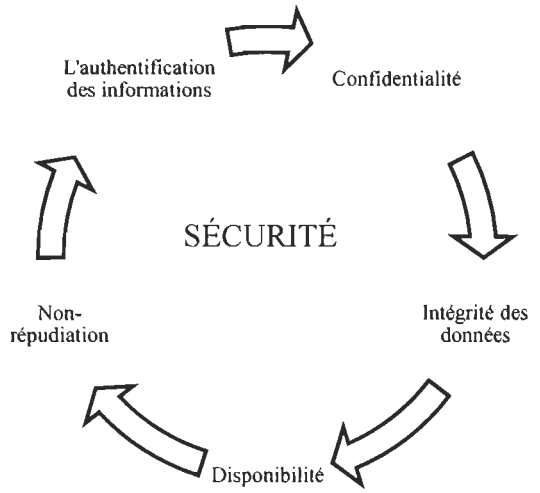

Figure 4. Principaux aspects de la sécurité dans les VANETs

- **Confidentialité du conducteur :**

  Si un véhicule utilise la même identification électronique pour une longue période de temps, alors un autre véhicule pourrait avoir accès à tous les messages échangés. Cela lui donne le pouvoir de reconstituer la trajectoire suivie par le premier véhicule. Afin de prévenir ce genre de comportement, divers mécanismes, comme l'utilisation de pseudonymes ou des informations d'identification anonymes ont été proposés.

- **L'authentification des informations :**

  Comme les informations échangées dans un réseau véhiculaire peuvent avoir un effet sur la sécurité routière, il est nécessaire de veiller à ce que les données soient authentiques et qu'ils reflètent fidèlement la réalité. Pour gérer l'authentification, la norme IEEE 1609.2 prévoit l'utilisation du mécanisme ECDSA (*Elliptic Curve Digital Signature Algorithm*), qui est un standard pour les signatures électroniques digitales. Les contributions faites dans ce cas visent à éliminer la menace de manière proactive, par exemple, prévenir la propagation de faux messages ou de manière réactive, en isolant les nœuds qui émettent de telles informations.

- **Intégrité des données :**

  Il est nécessaire de garantir que les données n'ont pas été falsifiées depuis qu'ils ont été émises par l'auteur original. En ce sens, la norme IEEE 1609.2 établit l'utilisation des fonctions SHA (*Secure Hash Algorithm*). Il s'agit de fonctions de hachage cryptographiques.

- **Confidentialité des informations :**

  On pourrait dire que la communication dans les réseaux véhiculaires est éminemment publique, étant donné la fourniture de certains services (par exemple, le télépéage) ou pour l'établissement de la communication privée entre les nœuds dans une région. Il est nécessaire de protéger la confidentialité de l'information. À cette fin, la norme IEEE 1609.2 définit l'utilisation du mécanisme ECIES (*Elliptic Curve Integrated Encryption Scheme*) basé sur la cryptographie à courbe elliptique.

1.3.6. Attaques sur les réseaux VANETs

Une fois que les exigences de sécurité ont été établies pour les VANETs, de nombreuses attaques peuvent être identifiées [14].

Il y a plusieurs attaques qui peuvent être présentes sur ces réseaux et qui peuvent être classées comme suit :

- **Falsification des informations :** avec l'injection de messages erronés, l'attaquant diffuse des informations fausses ou trompeuses, afin d'affecter le reste des véhicules.

- **Déni de service** (DOS, *Denial of Service*) **:** en utilisant un inhibiteur de fréquences, ce qui fait qu'un véhicule ne reçoit aucun signal dans une zone autour de lui.

- **Usurpation d'identité :** L'attaquant fait semblant d'être une autre entité. En conséquence, certains avertissements envoyés (ou reçus) par une entité spécifique serait envoyé à (ou reçu par) une entité indésirable.

- **Violation de la vie privée :** Les attaques sur la vie privée des VANETs sont principalement liés à obtenir illégalement des informations confidentielles sur les véhicules. Comme, il existe une relation entre un véhicule et son conducteur, obtenir certaines données sur un véhicule pourrait affecter sa vie privée.

- **Manipulation de l'information :** dans cette attaque, l'entité malveillante collecte des informations sur les transmissions pour affecter la réalité des messages, de telle façon qu'il génère des conflits dans le réseau.

1.4. Mécanismes de sécurité

Au cours des dernières années, il y a eu une pléthore de contributions liées à la sécurité des VANETs. Tous ces travaux sont basés sur différent techniques pour sécuriser et protéger les réseaux VANETs contre les possibles attaques.

1.4.1. Contrôle d'accès

Comme dans les réseaux traditionnels, les VANETs ont besoin d'un mécanisme qui contrôle l'accès au réseau et aux services qui sont fournis par le réseau. Le contrôle d'accès implique généralement l'authentification des utilisateurs du réseau. C'est-à-dire que pour

accéder au réseau, l'utilisateur doit être identifié avec un identificateur unique. Le réseau fait la vérification, et ensuite il donne l'accès demandé.

1.4.2. Sécurité de routage

Les nœuds dans les VANETs agissent comme des routeurs qui participent dans le protocole de routage pour découvrir et pour maintenir les routes des autres nœuds de réseau. Dans les réseaux traditionnels les routeurs sont gérés par des opérateurs de confiance, mais cela n'est pas vrai dans les VANETs, étant donné que chaque nœud qui rejoint le réseau est impliqué dans le processus de prise de décision.

1.4.3. Cryptage et la gestion des clés

Étant donné l'utilisation de techniques de cryptage et des signatures électroniques comme mécanismes de sécurité, il est nécessaire d'utiliser des clés cryptographiques qui seront partagées parmi tous les nœuds. Alors, on doit avoir un mécanisme pour la gestion de ces clés.

1.4.4. Système de détection d'intrusions (IDS)

Un IDS est un programme de détection d'intrusion ou d'accès non autorisé au réseau. Ces systèmes sont capables d'améliorer la sécurité des réseaux informatiques, et par conséquent ils peuvent fournir des solutions à un large éventail de problèmes de sécurité liés aux réseaux VANET [15].

Le fonctionnement de ces outils est basé sur une analyse détaillée du trafic réseau, qui est comparé à des signatures d'attaques connues ou à des comportements suspects. L'IDS analyse non seulement ce type de trafic, mais il vérifie également le contenu et leur comportement.

1.4.4.1. Les approches des IDS

D'une façon générale, dans les IDS nous pouvons distinguer deux techniques pour déterminer qu'une attaque est en cours (Figure 5).

- **Les IDS basée sur les signatures :**

  Il analyse les paquets du réseau et les compare avec les modèles d'attaques connus et préconfigurés. Ces modèles sont appelés signatures. Malgré que cette approche permet de détecter les attaques de manière efficace et rapide, les attaques inconnues ne peuvent être détectées, car les modèles d'attaques doivent être définis auparavant [15].

- **Les IDS basée sur l'anomalie :**

  En utilisant le calcul probabiliste, l'IDS détermine les motifs qui peuvent perturber l'activité normale du réseau. Il peut alerter lorsque le comportement normal varie, le classant comme anormal. Généralement les activités anormales peuvent être déterminées en effectuant des statistiques sur les actions effectuées par les utilisateurs, les techniques d'apprentissage automatique, le datamining et les réseaux de neurones peuvent aussi être utilisés dans ces IDS [15].

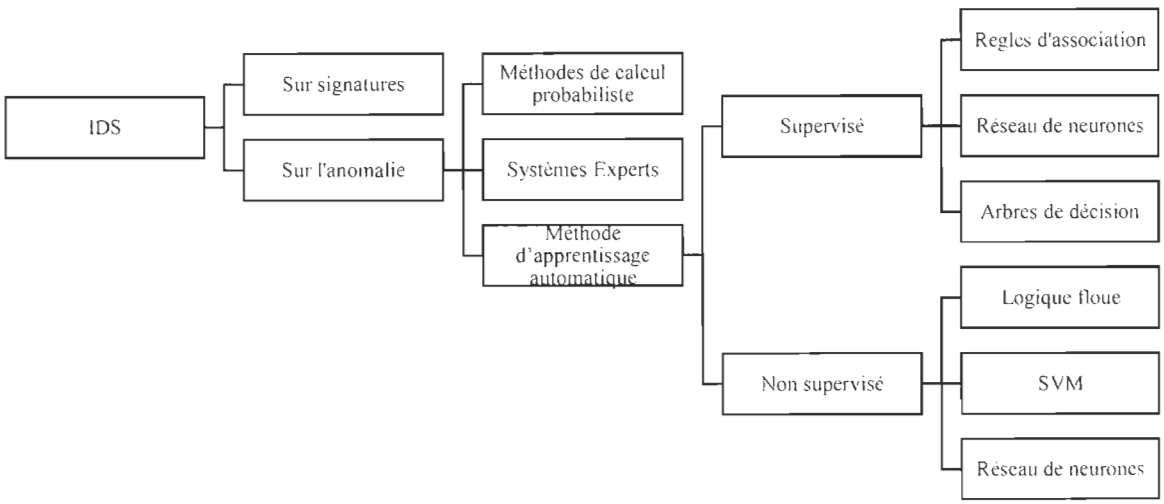

Figure 5. Techniques de détection d'intrusions

1.5. Conclusion

Les systèmes de transport intelligents offrent une technologie prometteuse pour le transport de nouvelle génération. Ils aident la société de manière multidimensionnelle. Ces systèmes permettent aux conducteurs d'être connectés à un réseau de communication pendant tout le trajet. De cette manière, les utilisateurs peuvent être informés tout le temps. Un des facteurs importants est que ces systèmes sont capables de garantir un haut niveau de sécurité lors de la conduite.

On pourrait dire que les réseaux VANETs sont des systèmes très complexes. Ces réseaux imbriquent plusieurs concepts et définitions au niveau du fonctionnement et surtout au niveau de la sécurité du réseau. Quand on parle de sécurité dans les VANETS, on fait référence à la sécurité des informations à partager et la vie privée du véhicule, c'est-à-dire à avoir une communication qui garde les aspects concernant l'authentification, la confidentialité, l'intégrité des données et leur disponibilité. Un point très évident est la vulnérabilité de ce réseau aux attaques. Dans ce chapitre, on a présenté quelques informations comme une introduction à notre sujet de recherche. Il est très important de bien comprendre les éléments clés énoncés ici, étant donné qu'ils sont la base du modèle qu'on va présenter dans ce mémoire.

Dans le chapitre suivant, nous allons présenter les résumés de quelques travaux de la littérature sur les enjeux de la sécurité qu'on vient de discuter dans le chapitre présent, les différentes attaques et quelques approches pour la détection des attaques.

CHAPITRE 2

REVUE DE LA LITTÉRATURE

Dans ce chapitre, nous allez présenter un état de l'art sur les enjeux de la sécurité pour les réseaux VANETs. Afin de ressortir cette problématique, nous présentons un résumé sur les attaques et les méthodes de détection des intrusions.

2.1. Défis de sécurité dans les réseaux VANETs

La sécurité est le problème majeur pour implémenter les réseaux VANETs. Dans [16], les auteurs présentent l'architecture de communication des réseaux VANETs et soulignent les défis en matière de confidentialité et de sécurité qui doivent être surmontés pour rendre la sécurité de ces réseaux utilisable dans la pratique. Ils identifient tous les problèmes de sécurité existants dans les VANETs et les classent d'un point de vue cryptographique. Ils regroupent, étudient et comparent les différents schémas cryptographiques qui ont été suggérés séparément pour les réseaux VANETs. Ils évaluent l'efficacité des solutions proposées et explorent certaines tendances futures qui façonneront la recherche dans les protocoles cryptographiques pour les systèmes de transport intelligents.

Les auteurs dans [17] étudient les exigences de sécurité et les défis pour mettre en œuvre la mesure de sécurité dans les réseaux VANETs. Différents types d'attaques et leurs solutions sont également discutés. Ils discutent de certaines technologies qui sont utilisées dans les différentes solutions. Les exigences d'authentification et de confidentialité sont les principaux problèmes dans les réseaux VANETs.

À partir des travaux [16] [17], on a pu faire un sommaire des attaques par rapport à chacun des aspects de sécurité dans les réseaux VANETs :

Attaque	Authentification	Confidentialité	Intégrité	Disponibilité	non-répudiation
Jamming				x	
Eavesdropping		x			
Traffic analysis		x			
DOS				x	
Sybil	x			x	
Message tampering			x	x	x

Broadcast tampering			x		
Brute force		x			
Timing attack				x	
Replay	x		x		
Key and/or certificate	x	x			
Illusion	x		x		
GPS spoofing/Position faking	x				
Man in the middle attack	x	x	x		
Loss of event treceability					x
Tracking/social engineering		x			
Node impersonation	x	x			x
Blackhole	x	x	x	x	x

Tableau 1. Attaques sur les réseaux VANETs

À partir du tableau 1, on peut déduire que les aspects de l'authentification, la confidentialité et la disponibilité de données sont les plus vulnérables aux attaques.

2.2. Détection d'attaques sur réseaux VANETs

Dans le cadre de la détection des attaques, un modèle Probabiliste basé sur la régression logistique a été présenté dans [18]. Cette méthode permet d'estimer l'occurrence d'une attaque en fonction des connaissances acquises préalablement. Elle se base sur un historique d'une base de connaissance qui permet d'estimer les paramètres de la régression logistique. La base de connaissance est constituée dans un premier temps de la quantification du nombre de véhicules ayant répondu positivement lors de la recherche d'un patron d'attaque dans les paquets de données. Il faut au préalable fournir à la base de connaissance des données testées sur des véhicules dans un contexte simulé. La base est ensuite implantée dans le RSU. Lorsque le modèle de régression est validé, il est utilisé pour estimer la probabilité d'une attaque et si cette dernière est supérieure au seuil fixé à l'avance (50%), l'attaque est alors corroborée.

Dans [19], les auteurs ont proposé une approche distribuée de détection d'attaque Sybil basée sur la vérification de plusieurs facteurs. Le Sybil est une attaque où l'assaillant utilise des fausses identités affectant la réputation du système. Dans ce système, chaque RSU calcule, stocke et vérifie divers paramètres, y compris le RSS (*Received Signal Strength*), la distance, l'angle de passage des véhicules par le processus de détection passive pour détecter les attaquants. La combinaison de différents paramètres rend cette approche de détection très précise.

En 2017, une nouvelle approche de détection appelée GDVAN (*Greedy Detection for VANETs*) pour les attaques Greedy [20]. La méthode proposée consiste principalement en deux phases appelées phase de suspicion et phase de décision. La phase de suspicion est basée sur le concept mathématique de régression linéaire alors que la phase de décision est basée sur un schéma de décision de logique floue. En surveillant les traces du trafic réseau, l'algorithme est capable d'affirmer l'existence ou non d'un nœud Greedy. Le comportement des nœuds Greedy a été largement abordé dans la littérature pour les réseaux locaux sans fil (WLAN, *Wireless Local Area Network*) et pour les réseaux mobiles ad hoc (MANETs). La détection d'un comportement d'un nœud Greedy est plus difficile pour les réseaux à haute mobilité tels que les VANETs. L'algorithme proposé non seulement détecte l'existence des nœuds Greedy, il établit également une liste des nœuds potentiellement compromis en utilisant trois métriques. L'un des principaux avantages de cette technique est qu'elle peut être exécutée par n'importe quel nœud du réseau et ne nécessite aucune modification de la norme IEEE 802.11p.

Dans [21], les auteurs ont analysé le comportement et les effets des attaques DOS sur le réseau en utilisant différents modèles mathématiques afin de trouver une solution efficace. Le principal résultat dans ce travail a été que les méthodes basées sur la régression logistique et les réseaux de neurones permettent de mieux analyser les données et de mieux prédire les attaques que les autres techniques mathématiques qui montrent des défauts d'efficacité.

Tous ces travaux convergent sur le même objectif, obtenir une méthode optimale pour la prédiction des différentes attaques. Le tableau 2 montre les principales caractéristiques de ces recherches.

Référence	Méthodologie	Attaque
[18]	Régression logistique	DOS, Black hole
[19]	Algorithme de vérification de plusieurs facteurs	Sybil
[20]	Régression linéaire, Schéma de décision de logique floue	DOS
[21]	Régression logistique, Réseaux de neurones, Erreur relative, Moyenne des carrés des écarts, L'écart absolu moyen	DOS

Tableau 2. Résumé des méthodes pour la prédiction d'attaques

2.3. Conclusion

Pour faire face aux attaques, différentes approches de recherche proposent plusieurs solutions pour améliorer les protocoles et l'architecture de sécurité de VANET. Cependant, pour assurer la sécurité de communication, nous n'avons pas seulement besoin de cadres de communication sécurisés, mais aussi d'algorithmes et de méthodes puissantes qui peuvent faciliter la détection d'intrusions malveillantes dans les réseaux.

Les méthodes de détection des attaques basées sur des modèles de prédiction sont une proposition de solution assez récente et peu abordée dans d'autres projets de recherche. C'est l'une des principales motivations pour bâtir notre modèle.

Dans le chapitre suivant, nous décrivons l'approche développé dans les systèmes d'inférences flous, nous présentons la notion de base de cette approche, notamment, la définition des réseaux de neurones artificiels et de la logique floue.

CHAPITRE 3

MODÈLES DE PRÉDICTION

Dans ce chapitre, nous introduisons les différents modèles de prédiction que nous allons utiliser par la suite pour définir notre proposition.

3.1. Réseau de neurones artificiels

Les réseaux de neurones artificiels sont des réseaux fortement connectés de processeurs élémentaires fonctionnant en parallèle. Chaque processeur élémentaire calcule une sortie unique sur la base des informations qu'il reçoit. Toute structure hiérarchique de réseaux est évidemment un réseau [22].

C'est à partir de l'hypothèse que le comportement intelligent émerge de la structure et du comportement des éléments de base par des neurones biologiques que les réseaux de neurones artificiels se sont développés. Les réseaux de neurones artificiels sont des modèles et à ce titre ils peuvent être décrits par leurs composants, leurs variables descriptives et les interactions des composants [22].

L'apprentissage est vraisemblablement la propriété la plus intéressante des réseaux neuronaux. Elle ne concerne cependant pas tous les modèles, mais les plus utilisés. L'apprentissage est une phase du développement d'un réseau de neurones durant laquelle le comportement du réseau est modifié jusqu'à l'obtention du comportement désiré. Dans le cas des réseaux de neurones artificiels, on ajoute souvent à la description du modèle l'algorithme d'apprentissage. Au niveau des algorithmes d'apprentissage, il a été défini deux grandes classes selon que l'apprentissage est dit supervisé ou non supervisé. Cette distinction repose sur la forme des exemples d'apprentissage [22].

3.2. Logique Floue

La logique floue a été développée par Lofti A. Zadeh en 1965 à partir de sa théorie des sous-ensembles flous. Les sous-ensembles flous sont une manière mathématique de représenter l'imprécision de la langue naturelle, ils peuvent être considérés comme une généralisation de la théorie des ensembles classiques. La logique floue est aussi appelée "logique linguistique" car ses valeurs de vérité sont des mots du langage courant : "plutôt vrai, presque faux, loin, si loin, près de, grand, petit...". La logique floue a pour objectif l'étude de la représentation des connaissances imprécises, des raisonnements approchés et elle cherche à modéliser les notions vagues du langage naturel [23].

3.3. Les systèmes d'inférences flous

Un système d'inférence floue a comme but de transformer les données d'entrée en données de sortie à partir de l'évaluation d'un ensemble des règles. Un système d'inférence floue est formé de trois blocs :

- Le premier bloc correspond à l'étape de fuzzification qui transforme les valeurs numériques en degrés d'appartenance. Chaque variable d'entrée et de sortie est associée à des sous-ensembles flous.
- Le second bloc est le moteur d'inférence et il est constitué par l'ensemble des règles.
- Enfin, une étape de défuzzification qui permet, si nécessaire, d'inférer une valeur nette.

Une règle floue est de la forme ***Si*** *je rencontre telle situation* ***Alors*** *j'en tire telle conclusion*. La situation, appelée prémisse ou antécédent de la règle, est définie par une combinaison de relations de la forme $x \; est \; A$ pour chacune des composantes du vecteur d'entrée. La partie conclusion de la règle est appelée conséquence, ou encore simplement conclusion.

Selon la structure particulière de la proposition conséquente, on peut distinguer deux types de modèles flous basés sur des règles :

1. Modèle flou linguistique (ou modèle Mamdani), dans lequel l'antécédent et le conséquent sont tous les deux des propositions floues qui utilisent des variables linguistiques.
2. Modèle flou Takagi-Sugeno, dans lequel le conséquent utilise des variables numériques plutôt que des variables linguistiques, sous la forme d'une constante, d'un polynôme ou de manière plus générale d'une fonction ou d'une équation différentielle dépendant des variables associées à la proposition antécédente.

3.4. Modèle ANFIS (*Adaptive Neuro-Fuzzy Inference System*)

ANFIS est un système d'inférence adaptatif neuro-flou qui consiste à utiliser un réseau de neurones à 5 couches (figure 6) pour lequel chaque couche correspond à la réalisation d'une étape d'un système d'inférence floue de type Takagi Sugeno. Pour la simplicité, nous supposons que le système d'inférence flou à deux entrées x et y, et à comme une sortie f. Supposer que la base de règle contient deux règles floues de type Takagi-Sugeno [24] :

Règle1 : SI x est A1 et y est B1 ALORS f1 = p1 x+q1 y+r1

Règle2 : SI x est A2 et y est B2 ALORS f2 = p2 x+q2 y+r2

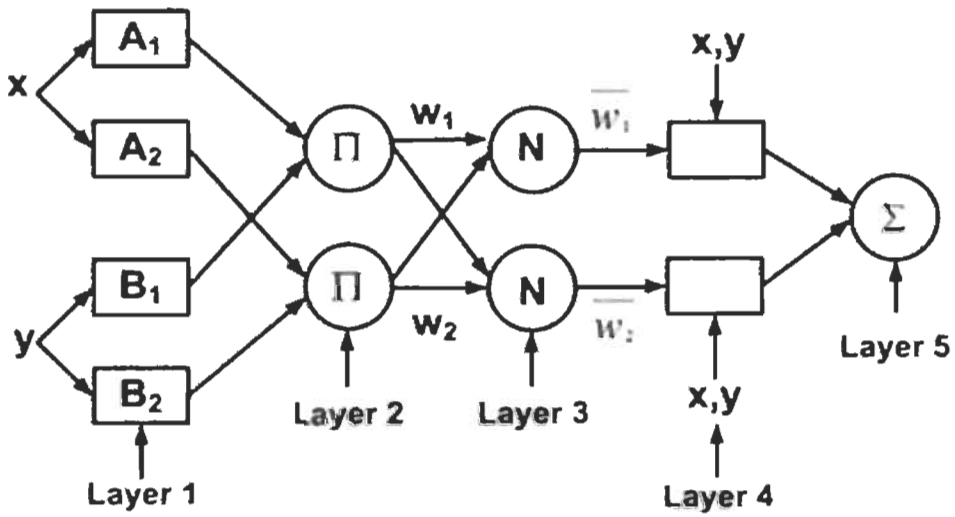

Figure 6. L'Architecture de l'ANFIS [25]

L'architecture classique d'un modèle ANFIS peut être décrite de la manière suivante [24] :

1. La première couche comporte autant de neurones qu'il y'a de sous-ensembles flous dans le système d'inférence représenté. Chaque neurone calcule le degré de vérité d'un sous ensemble flou particulier par sa fonction de transfert.

2. La deuxième couche cachée sert à calculer le degré d'activation des prémisses. Les neurones reçoivent en entrée le degré de vérité des différents sous-ensembles flous composant cette prémisse et ont en charge le calcul de son propre degré de vérité.

3. La troisième couche cachée normalise de degré d'activation des règles. L'ensemble des sorties de cette couche seront appelées les poids normalisés.

4. La quatrième couche cachée sert à déterminer les paramètres de la partie conséquence des règles.

5. La couche de sortie contient un seul neurone dans cette couche et c'est un neurone qui calcule la sortie globale comme l'addition de tous les signaux entrants.

3.5. Conclusion

Dans ce chapitre nous avons introduit des définitions théoriques très important, elles constituent la base de notre modèle que nous allons présenter dans le chapitre suivant. Ce système d'inférence adaptatif est très performant et largement utilisé dans les réalisations pratiques.

Dans le chapitre suivant, nous allons décrire l'objectif de notre travail. On va présenter de façon plus détaillée la méthodologie suivie et les techniques de prédiction qui ont été utilisées. Notre méthodologie s'appuie sur l'utilisation d'un réseau de neurones flou de type ANFIS. Notre article scientifique soumis est présenté à la fin du chapitre 4.

CHAPITRE 4

MÉTHODOLOGIE PROPOSÉE

Ce travail est basé sur une recherche expérimentale qui suit différentes étapes. Dans la première étape, il fallait comprendre le comportement des réseaux VANETs et les enjeux de sécurité. Cette étape a été présentée dans les chapitres précédents.

La sécurité dans les réseaux VANETs est un grand défi parce qu' il existe différents types d'attaques qui mettent en danger les communications. D'où, l'objectif principal de notre travail est la conception d'un système d'inférence adaptatif neuro-flou (ANFIS, *Adaptive Neuro-Fuzzy Inference System*). L'idée générale est d'avoir un modèle capable de prédire les attaques. Cette prédiction est faite en obtenant un indicateur du niveau de sécurité sur les réseaux VANETs.

Nous commençons avec différentes simulations du réseau pour obtenir la base de données contenant les différents paramètres comportementaux du réseau. Ensuite, nous analysons et préparons les données en utilisant des techniques statistiques différentes pour connaitre la nature des variables et sélectionner les meilleures méthodes à utiliser par la suite. Une fois les méthodes sélectionnées, nous proposons le modèle de prédiction.

4.1. Génération de la base de données

La simulation des réseaux véhiculaires a été réalisée en utilisant le simulateur VEINS (*Vehicles in Network Simulation*) [27]. En particulier, la solution proposée utilise deux systèmes de simulation open source : SUMO (simulateur de trafic) [28] et OMNeT ++ (simulateur de réseau) [26].

L'objectif de l'intégration d'un simulateur de réseau et d'un simulateur de trafic est de créer un scénario réaliste, dans lequel les conditions de la transmission de données et l'interaction des véhicules sous un modèle de trafic réel sont pris en compte.

Les simulations ont été générées à partir de deux scénarios. Dans le premier, nous avons simulé un réseau sans attaque et dans le second; nous avons simulé un réseau avec attaque(s). L'attaque fonctionne en insérant des informations non pertinentes pour saturer le réseau. Cette attaque est connue comme « *flooding* » ou inondation, il appartient aux attaques de type déni de service (DOS) [29]. Les principaux problèmes sur un réseau sous l'attaque « *flooding* » sont décrites comme suit :

1. Lors d'une attaque, la bande passante disponible est consommée en raison de faux paquets injectés dans le réseau.

2. Pour chaque transmission, une quantité importante d'énergie est consommée à cause de faux messages.

3. L'inondation dans le réseau produit la congestion dans la transmission d'information, cela provoque une perte de données assez significative.

4. Lors de ce type d'attaque, les ports de communication sont saturés avec un flux de données excessif, de sorte que la surcharge du système rend la communication impossible, en refusant les différentes demandes faites par les véhicules connectés [30].

Différents paramètres ont été extraits des résultats de la simulation. Ils sont définis en fonction des différentes caractéristiques du réseau (Tableau 3). Nous avons choisi parmi les paramètres de communication, ceux dont les résultats de simulation étaient différents de zéro.

Variable	**Description**	**Type**
RecivedBroadcast	*Broadcast* reçu	Quantitative
RXTXLostPackets	Nombre de paquets perdus pendant la transmission	Quantitative
SlotsBackoff	Nombre de *Slots* de temps à cause des *Backoff*	Quantitative
SNIRLostPackets	Nombre de paquets perdus à cause des erreurs internes	Quantitative
TimeIntoBackoff	Nombre de fois que le nœud est en *Backoff*	Quantitative

TotalBusyTime	Temps total lorsque le nœud est occupé	Quantitative
TotalLostPackets	Nombre total de paquets perdus	Quantitative

Tableau 3. Description des Variables

4.2. Analyse et préparation des données

Dans tout modèle de prédiction, il est très important d'effectuer une analyse exploratoire de données. De cette manière, nous obtiendrons une vision plus claire et globale d'ensemble des données [31].

Au travers de l'analyse exploratoire de données, on cherche essentiellement à résumer la distribution de chaque variable, en utilisant des graphiques et en obtenant quelques statistiques descriptives.

Dans certains cas, les caractéristiques du modèle peuvent suggérer une transformation des variables, compte tenu de la redondance de l'information ou de la dépendance des variables. L'une des analyses les plus populaires pour étudier les relations entre les variables est l'analyse de corrélation.

4.3. Méthodes de prédiction

Il existe différentes méthodes pour obtenir des modèles de prédiction. Pour ce travail, on a considéré le modèle ANFIS. Les avantages de cette technique sont les suivantes [25] :

1. Exploitation de la connaissance disponible, grâce à la base de règles.
2. Réduction de la taille de la base de règles : il suffit d'avoir des règles générales, les détails seront fournis par le réseau de neurones.
3. Réduction de la complexité de l'apprentissage : le réseau de neurones doit simplement apprendre les cas particuliers ou les exceptions, on n'a pas de problème complet.
4. Efficacité immédiate dès le début de l'apprentissage et possibilité d'éviter des comportements initiaux erratiques.

4.4. Article scientifique

DESIGN AND MODELING AN ADAPTIVE NEURO-FUZZY SYSTEM (ANFIS) FOR THE PREDICTION OF A SECURITY INDEX IN VANET

Soumis au journal *International Journal of Communication Systems*, Wiley.

Numéro papier: IJCS-18-0243

Soumis le 26 mars 2018.

RESEARCH ARTICLE

Design and modeling an Adaptive Neuro-Fuzzy Inference System (ANFIS) for the prediction of a security index in VANET

Caroly Gabriela Pereira Diaz [1*] | Boucif Amar Bensaber[2*] | Youssef Lahrouni[3*]

[1,2,3]Department of Mathematics and Computer Science, Université du Québec à Trois-Rivières, Trois-Rivières, Québec, G9A 5H7, Canada

Correspondence
Caroly Gabriela Pereira Diaz, Département de mathématiques et d'informatique, Université du Québec à Trois-Rivières, Trois-Rivières, Québec, G9A 5H7, Canada
Email: Caroly.Pereira@uqtr.ca

Funding Information
Natural Sciences and Engineering Research Council of Canada, Grant/Award Number: RGPIN 23972-2013

Vehicular Ad hoc NETworks (VANET) allow communications between vehicles using their own connection infrastructure. There are several advantages and applications in using this technology and one of most significant is road safety. As in most other networks, it is not only important to guarantee the transport but also the security of information. Security in VANET is a big challenge because there are different types of attacks that endanger communications of moving vehicles. This paper proposes an applied Adaptive Neuro-Fuzzy Inference System (ANFIS) to obtain a prediction model of security index in VANET. The research process starts with network simulations to obtain a database of occurrences of attacks. Then, this latter is prepared and analyzed statistically. Finally, using MATLAB toolbox, we show the proposed model of security level that allows estimating the network vulnerability in the event of an attack.

KEYWORDS
VANET security, attacks, fuzzy logic, soft computing, neural networks, ANFIS

* Equally contributing authors.

1 | INTRODUCTION

The era of communication advances faster, computers, telephones and millions of devices are connected to transmit and receive information. VANET is a kind of mobile network (MANETs) that allows communication with or without infrastructure installed at the edges of the roads [1]. In this type of network, the nodes are vehicles and one of the main features is that its topology can change quickly. The main contribution in this type of network is the development of applications in the framework of Intelligent Transport Systems (ITS), which are used to provide and improve traffic information and in this way, it increases road safety and transport efficiency.

The network security is very vulnerable, there are several technical challenges in VANET, the high mobility, routing, dynamic topology, loss of information through its wireless connection, among others [2]. Main security problems can occur during the transmission of information. Different types of attacks can violate and/or interrupt the connection and there are flaws or anomalies typical of the communication system. Security protocols, formalization of standards and different analysis of attacks, have been proposed to improve VANET security, but the field is still large to explore [3].

Following this line of research, this work is based in soft computing techniques and artificial intelligence. We select the fusion of fuzzy logic and neural networks as a method to design a model that predicts the security level against attack possibilities in VANET.

It is very important to highlight that to date; this is the first work that implements fuzzy logic techniques as a predictive method for the detection of attacks or anomalies in this type of network. To achieve a good model for this level of security, statistical and data processing tools were needed too.

As in all emerging technology, uncertainty and the impression of these types of system is a variable that significantly influences the progress of its development. The adaptive neuro-fuzzy inference system (ANFIS) is characterized by incorporating aspects of neural networks and fuzzy logic. The first one takes advantage of the ability to learn, as well as the ability to generalize. From the fuzzy logic is obtained the logical reasoning based on rules of inference, thus contributing, a powerful tool that allows to operate with linguistic variables and incorporates a broader treatment. The construction of models based on these two areas has proven to be an efficient mechanism when modeling real systems.

The remainder of this paper is organized as follows. In section 2, a Literature review (State of art) about security issues and attacks in VANET is presented. Section 3 presents the methodology and tools used in this work. In section 4, we present the analysis process and data treatments. Section 5 is focused on our proposal for a model aiming at measuring a security index in VANET. Finally, a discussion about results is presented in section 6.

2 | STATE OF ART

The use of different wireless technologies in vehicular environments has been studied since the 1970s [4]. As a complex system, it is very important to understand each component of VANET. Several works have been presented and served as reference for the definition of the main concepts in vehicular networks operations.

In [1], that can be established by short and medium range communication based on WLAN (Wireless Local Area Network) technology. For VANET, IEEE 802.11p and IEEE 1606.4 standards has been defined, to specify technical and operational details of the Wireless Access to Vehicular Environment (WAVE) [5] [6]. The exchange of information between vehicles is very important, that is why the security of communications becomes crucial in this network. This constitutes a prerequisite for the deployment of VANET Pathak and Shrawankar [7].

In [8], authors presented a detailed description of the main attacks in vehicular networks and a set of different solutions to counteract them. They focus their research mainly on the identification of different areas where the

vulnerability of communication between the vehicles can be affected. They identified anonymity, as a critical issue in VANET. The physical identity of a vehicle is a very important factor to protect. In 2010 [9], authors identified that one of the most significant questions in such networks is ensuring information and protection of privacy. Other security requirements as authentication, non-repudiation, confidentiality and integrity of information have been showed in this research.

Attacks in VANET are aimed at breaking down these aspects. Authors in [10] [11] agree that authentication, confidentiality and availability of data are the most vulnerable security characteristics to attack. Many attacks can be identified [12].

- Falsification of information: with the injection of erroneous messages, the attacker transmits false or misleading information to affect the rest of vehicles.
- Denial of service (DOS): use a frequency inhibitor, which means that a vehicle does not receive any signal around in a certain area.
- Impersonation: The attacker pretends to be another entity. Thus, certain warnings sent (or received) by a specific entity would be sent to or received by an undesirable entity.
- Violation of privacy: attacks on the privacy in VANET are mainly linked to illegally obtaining confidential information on vehicles, owners or its drivers.
- Information handling: in this attack, the malicious entity collects information about transmissions to affect the veracity of the produced messages, in such a way that it generates conflicts in the network.

To deal with attacks, different research approaches propose several solutions to improve the protocols and the security architecture of VANET. However, for a strong security of communication, we not only need secured communication frameworks but it is also necessary to have powerful routing algorithms that can facilitate the detection of malicious intrusion in networks and mitigate them [13].

In [14], authors have proposed a distributed Sybil attack detection approach based on the verification of multiple factors. Sybil attack is an attack where the attacker makes use of false identities affecting the reputation of the system. In this system, each Road Side Unit (RSU) computes, stores and verifies various parameters including RSS (Received Signal Strength), distance, angle of passing-by vehicles through passive overhearing process to detect Sybil attackers. The combination of different parameters makes this detection approach highly accurate.

In 2017, a new detection approach called GDVAN (Greedy Detection for VANET) for greedy behavior attacks in VANET was proposed [15]. The proposed method mainly consists of two phases called suspicion phase and decision phase. The suspicion phase is based on the linear regression mathematical concept while decision phase is based on a fuzzy logic decision scheme. By monitoring network traffic traces, the algorithm is able to affirm the existence or not of a greedy node.

Intrusion detection system (IDS) is another technique to detect intrusion or unauthorized access to the network. These systems can improve network security; therefore, they can provide solutions to a wide range of security issues related to VANET. IDS functioning is based on a detailed analysis of network traffic, which is compared to known attack signatures or suspicious behavior. IDS not only analyze this type of traffic; but it also checks the content and their behavior [16]. In general, IDS uses two approaches to determining that an attack is underway. The first one is called signature-based system. In this case, the system has a database behavior of certain attacks to which are compared the collected data. An attack is detected, if the data coincide with malicious behavior already registered [17]. The second one is anomaly detection system, so the system detects any behavior that deviates the standard pre-established behavior and triggers a response [18].

Authors in [19] propose a probabilistic model based on logistic regression. This method estimates the occurrence of three different attacks. The method is based on a knowledge base that considers occurrences of attacks. When the model of the regression is validated, it will be used to estimate the probability of an attack and if it exceeds the threshold set in advance, the attack is confirmed.

In [20], authors have analyzed DOS attacks behavior and effects on the network using different mathematical models. They have observed that logistic regression and neural network are better than other models, to analyze data and to predict DOS attacks.

All these works converge on the same objective, obtaining an optimal method for the prediction of different attacks. Table 1 summarizes the main characteristics of these papers.

TABLE 1 Summary of attack prediction methods

Reference	Methodology	Attacks
[14]	Algorithm of multiple factors verification	Sybil
[15]	The linear regression mathematical, fuzzy logic decision scheme	DOS
[19]	Logistic regression	DOS, Attack on privacy, Black hole
[20]	Logistic regression, neural network, RMS, MAV, MSE	DOS

RMS (Root Mean Square), MAV (Mean Absolute Value), MSE (Mean Squared Error)

The aim of these approaches is to improve communications for all applications using VANET and requiring security.

3 | METHODS AND TOOLS

This work aims to define a predictive model based on adaptive neuro-fuzzy systems (ANFIS) in order to obtain a security index in vehicular networks. To understand our approach, we present in this section a summary of different models we used. The ANFIS is a hybrid artificial intelligence methodology that combines the fuzzy logic with the ability of neural networks to detect patterns in data and to learn from the relationships in different systems.

3.1 | Artificial neural network

Neural networks are the implementation of mathematical models inspired by biological neurons. Like brain neurons, artificial neurons are interconnected and distributed in layers. In this case, the nodes send different types of response between them when they receive an input (Figure 1).

There are different types of neural networks, with special characteristics, but their structure and operating principle is basically the same. One of the main characteristics of artificial neural networks is their ability to learn like humans. They improve their performance through training. Once the network is trained, it will be able to deliver the expected output responses to the inputs presented. Known methods as learning algorithms are used to train networks. Some of them are supervised learning algorithms and others are unsupervising learning algorithms. The learning process typically amounts to modifying the weights and thresholds of the variables (i.e. the parameters of the artificial neural network) within the network [21].

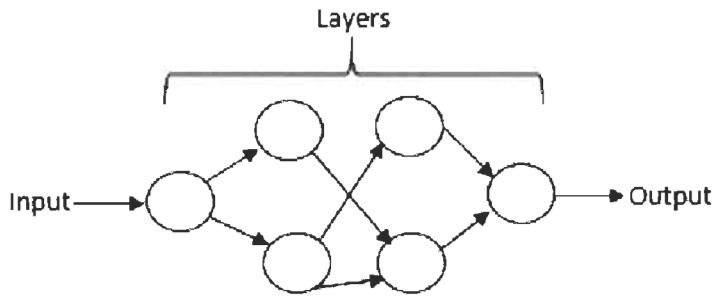

FIGURE 1 Artificial Neural Network

3.2 | Fuzzy Inference Systems

While variables in mathematics usually take numerical values, in fuzzy logic applications, the non-numeric linguistic variables are often used to facilitate the expression of rules and facts. A fuzzy inference system (FIS) can be extremely useful when there is a significant percentage of imprecision in the data. The basic structure of a fuzzy system is described in figure 2.

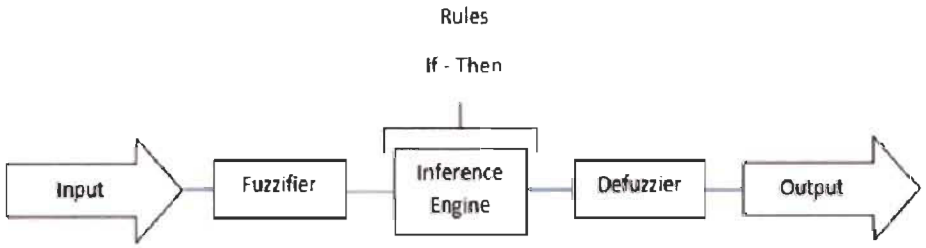

FIGURE 2 Fuzzy interference system

The first block is the fuzzification stage that transforms the numerical values (Input) into membership functions of the different fuzzy sets. The second block is the inference engine, consisting of the set "if-then" rules. Finally, a defuzzification stage makes it possible, if necessary, to infer a net value (Output). In classical logic (figure 3), an element belongs or does not belong to the set. However, the fuzzy logic what it does is to put a membership degree that is defined by the characteristic function associated with the diffuse set [22].

A fuzzy set A in the domain X is defined by a set of ordered pairs:

$$X = \{(x, \mu_A(x)) | x \epsilon X\} \quad (1)$$

Where $\mu A(x)$ is the membership function to the fuzzy set A:

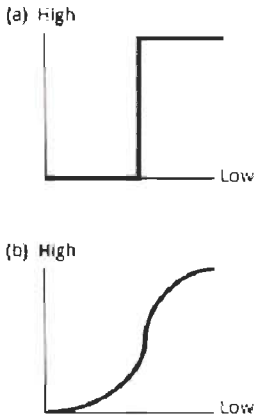

FIGURE 3 (a) Classic logic. (b) Fuzzy logic

$$\mu_A : X \rightarrow [0, 1] \tag{2}$$

The membership function assigns each element $x \epsilon X$ a value between 0 and 1; this value is the degree of membership of x in the set A.

There are different types of fuzzy inference systems, among the best known and used are Mandani systems and Takagi-Sugeno systems.

Rules that constitute the knowledge base for the inference engine are structured in two parts, the premise and the consequent. The main difference between Mamdani and Takagi-Sugeno type systems is the rules format. In Mamdani systems, both the premise and the consequent correspond to linguistic labels (Figure 4).

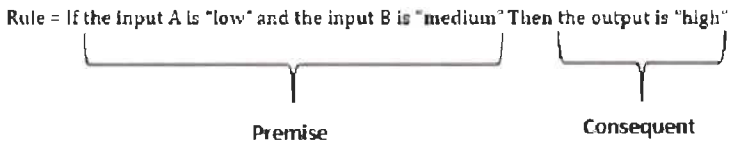

FIGURE 4 Rule "If - then" Mamdani

Figure 5 shows the scheme for Takagi-Sugeno rules. In this case, the consequent is no longer a linguistic label, but it is a function of the input.

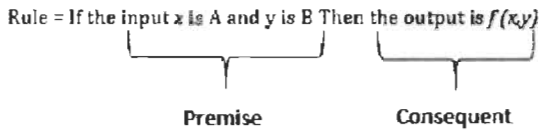

FIGURE 5 Rule "If - then" Sugeno

3.3 | Adaptive Neuro-Fuzzy Systems (ANFIS)

Neural networks have a high degree of adaptability and ability to learn and generalize [23]. An adaptive network is a multi-layer feed forward network in which each node performs a particular function (node function) on incoming signals as well as a set of parameters pertaining to this node [24]. The adaptive neuro-fuzzy systems fuse the benefits of fuzzy logic with these capabilities that neural networks provide to model real systems in an efficient way. In general, the principle of this system is based on the following:

1. The fuzzy controller is transformed into a neuronal network.
2. The network is trained by back propagation, which is an automatic neural network training system with hidden layers. This method is used to calculate the error contribution of each neuron after a batch of data is processed.
3. Differentiable operators and differentiable membership functions are used to define the fuzzy sets.

The basic learning rule of adaptive networks is based on the gradient descent and the chain rule. It is also called backward propagation of errors, because the error is calculated at the output and distributed back through the network layers [25].

ANFIS is an adaptive network that uses supervised learning, which has a function of Takagi–Sugeno fuzzy inference system. Figure 6 shows the fuzzy reasoning mechanism for Takagi–Sugeno model and Figure 7 shows ANFIS architecture [26].

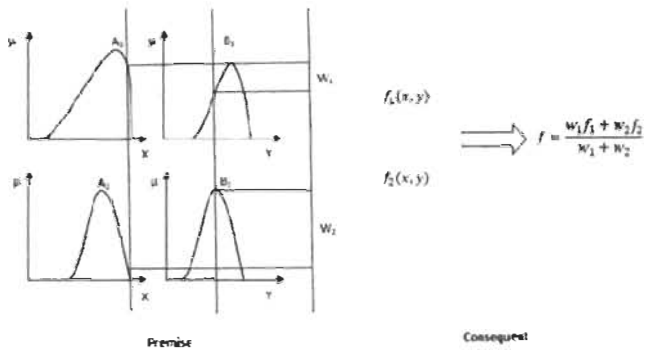

FIGURE 6 Sugeno fuzzy interference system "If-Then"

Assume that there are two inputs x and y, and one output f. Two rules were used in the method Takagi-Sugeno model, as follows:

Rule 1 = If x is A_1 and y is B_1 Then $f_1 = p_1 x + q_1 y + r_1$.

Rule 2 = If x is A_2 and y is B_2 Then $f_2 = p_2 x + q_2 y + r_2$.

Where A_1, A_2 and B_1, B_2 are the membership functions of each input x and y (part of the premises), while p_1, q_1, r_1 and p_2, q_2, r_2 are linear parameters in part-then (consequent part) of Takagi-Sugeno fuzzy inference model.

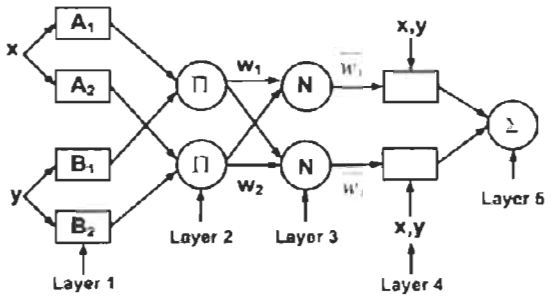

FIGURE 7 ANFIS architecture [25]

ANFIS architecture has five layers. The first and fourth layers contain an adaptive node, while the other layers contain a fixed node [25].

Layer 1: corresponds to input x, y. The nodes of this layer are adaptive, and each one calculates the degree of membership of the fuzzy set input $A_i(x)$. Its membership function can be defined in several ways, bearing in mind that it must be differentiable. For example, $A_i(x)$ could be represented by bell-shaped (equation 3) with maximum equals to 1 and minimum equals to 0.

$$A_i(x) = \frac{1}{1 + (\left(\frac{x - c_i}{a_i}\right)^2)^{b_i}} \tag{3}$$

Where x is the input and a_i, b_i, c_i is the set of parameters.

Layer 2: This layer is the rule layer. The nodes of this layer are non-adaptive and the output of each node is defined as the product of its inputs.

$$w_i = A_i(x) * B_i(y) \tag{4}$$

Layer 3: Nodes in this layer compute the normalized combination of degrees of membership of all linguistic statements. This combination is called degree of rule fulfillment or rule's firing strength, since it expresses how well a rule premise matches a specific input value. Every node in this layer is labeled N. The i-th node calculates the ratio of the i-th rule's firing strength to the sum of all rule's firing strengths.

$$\bar{w}_i = \frac{w_i}{(w_1 + w_2)} \tag{5}$$

Layer 4: Every node in this layer is a square node with a node function:

$$\bar{w}_i f_i = \bar{w}_i (p_i x + q_i y + r_i) \tag{6}$$

Where $\bar{w}_i$ is the output of layer 3, and $\{p_i, q_i, r_i\}$ is the parameters set.

Layer 5: The overall output, composed of a single node. The node of this layer is non-adaptive and its output is defined as the sum of the partial outputs of layer 4:

$$\sum \bar{w}_i f_i \tag{7}$$

3.4 | VANET Simulations

The database of our study was obtained through simulation results. We used the integration of three simulator types. OMNet++ 5.0 [27] as network simulators and distributed systems, Veins (Vehicles Network Simulation) 4.4 [28] and SUMO-0.25.0 for the simulation of urban mobile [29]. The simulation configuration values are found in table 2.

TABLE 2 Simulation setup

Item	Value
Time simulation	90s
Configuration Real City	Montreal - Config Map 5km
Mac protocol	IEEE 802.11p
Packet size	1024 bytes
Bit rate	18 Mbps
Number of RSU	1
Communication range of vehicle	800 m
Communication range of RSU	800 m
Total vehicles number	240

Since this is a premier approach implementing this methodology, we chose the simulation setup quite basic and a single attack. The number of vehicles was randomly selected. Simulations were generated from two scenarios. In the first one, we simulated a network without attack and in the second one; we simulated a network under a *flooding* (Denial of Service) attack. This attack work by inserting irrelevant information to saturate the network [30]. Key issues in the network with DOS flooding attack [31] are:

1. During an attack, due to false packets injected in the network, the available bandwidth is consumed.
2. For each transmission, a significant amount of energy is consumed, due to false control message.
3. Due to frequent flooding in the network, a congestion can be occurred and this causes frequent drop of packets in the network.

Different parameters have been extracted from simulation results. They are defined in relation to different characteristic levels of the network. They are listed in table 3.

TABLE 3 Simulation Result Parameter

Level	Parameters
Node	Posx
	Posy
	Speed
	Acceleration
Communication	SNIR Lost Packets
	RXTX Lost Packets
	Total Lost Packets
	Dropped Packets in MAC
	Time into Backoff
	Slots Backoff
	Total Busy Time
Mobility	Start time
	Total time
	Stop Time
	Min Speed
	Max Speed
	Total Distance

In the case of MANET and other kinds of networks, there are different types of databases with real information available in Internet or in other database repositories. In case of VANET, the only available data source is from simulation results. The VANET simulation tools allow understanding the main challenges and difficulties compared to other wireless networks, as well as carrying out studies that evaluate their performance.

4 | ANALYSIS AND DATA TREATMENT

We present in this section the details of the different steps required to obtain the data and the preparation of the variables to be included in our predictive model.

4.1 | Variables selection and description

The most important in this stage is to know which parameters contribute to the most significant information in our case study. This work focuses on parameters in the communication level (table 3). *Flooding* attacks increases the loss of network connectivity, due to resource overload (for example, broadcast). During this type of attacks, communication ports are saturated with excessive data flow, in such a way that the overload of the system makes communication impossible in a correct way, denying the different requests made by connected vehicles. Therefore, we chose from the communication parameters that are presented in table 3, those whose simulation results were different from zero. Then, we collected data from the simulation process of our two scenarios. A brief description of each selected variable is presented in table 4 below.

TABLE 4 Variables description

Variable	Description
ReciveBroadcast	Information received during the transmission of information
RXTXLLostPackets	Number of packet lost during transmission
SlotsBackoff	Number of slots due Backoff
SNIRLostBackoff	Number of packet lost due to internal causess
TimeIntoBackoff	Number of times the node is in backoff
TotalBusyTime	Total time the node is busy
TotalLostPackets	Total number of packets lost

4.2 | Data analysis

In a system in development such as VANET and in any process of variables modeling, it is very important to perform an exploratory analysis of data. In this way, we will obtain a clearer and global vision of datasets, which will help us to discover patterns or another kind of information useful to select techniques for the design of our model. Fuzzy logic models are flexibles, some of the most important and relevant reasons to choose them are:

1. Receive any kind of data.
2. Manage a large amount of information.
3. Work very well with uncertain or incomplete data.

For these reasons, in a fuzzy logic model, a detailed analysis of the data is not necessary. However, we believe it is essential and useful to have a correlation analysis in order to evaluate the dependence among the selected variables.

4.3 | Correlation analysis

Using the statistical program SPSS, the following results were obtained from the correlation analysis.

The correlation analysis is a technique of information analysis based on statistics and, therefore, mathematics. It consists of analyzing the relationship between, at least, two variables. In order to analyze the relationship between

variables, we used the correlation coefficients. In this case, we used the Pearson correlation coefficient. Results obtained are presented in table 5. As it is indicated, variables are strongly correlated. Especially the variable TotalLostPackets that is highly correlated with the variables RXTXLostPacket, SlotsBackoff, SNIRLostPackets and TimesIntoBakoff. Given this correlation and in order to obtain a model that gathers the greatest amount of information without the redundancy of values, we believe that the reduction of the number of variables is convenient and appropriate. For that, we use of a principal component analysis as complement to the data processing.

TABLE 5 Correlation analysis result

Correlations

		ReceivedBroadcasts	RXTXLostPackets	SlotsBackoff	SNIRLostPackets	TimesIntoBackoff	totalBusyTime	TotalLostPackets
ReceivedBroadcasts	Pearson Correlation	1	-,433**	-,409**	,222**	-,383**	,426**	-,368**
	Sig. (2-tailed)		,000	,000	,001	,000	,000	,000
	N	240	240	240	240	240	240	240
RXTXLostPackets	Pearson Correlation	-,433**	1	,889**	,665**	,935**	,059	,959**
	Sig. (2-tailed)	,000		,000	,000	,000	,365	,000
	N	240	240	240	240	240	240	240
SlotsBackoff	Pearson Correlation	-,409**	,889**	1	,627**	,916**	,061	,866**
	Sig. (2-tailed)	,000	,000		,000	,000	,346	,000
	N	240	240	240	240	240	240	240
SNIRLostPackets	Pearson Correlation	-,222**	,665**	,627**	1	,667**	,134*	,849**
	Sig. (2-tailed)	,001	,000	,000		,000	,038	,000
	N	240	240	240	240	240	240	240
TimesIntoBackoff	Pearson Correlation	-,383**	,935**	,916**	,667**	1	,082	,914**
	Sig. (2-tailed)	,000	,000	,000	,000		,207	,000
	N	240	240	240	240	240	240	240
totalBusyTime	Pearson Correlation	,426**	,059	,061	,134*	,082	1	,090
	Sig. (2-tailed)	,000	,365	,346	,038	,207		,165
	N	240	240	240	240	240	240	240
TotalLostPackets	Pearson Correlation	,353**	,959**	,866**	,849**	,914**	,090	1
	Sig. (2-tailed)	,000	,000	,000	,000	,000	,165	
	N	240	240	240	240	240	240	240

** Correlation is significant at the 0,01 level (2-tailed).

* Correlation is significant at the 0,05 level (2-tailed).

4.4 | Principal Components Analysis (PCA)

PCA is a statistical description of the information, or the reduction of the dimension. The objective is to reduce to a smaller number of variables, losing as little information as possible. One of the first premises for applying the principal component analysis is that the variables are correlated. But, this is not enough, if we want to guarantee that the loss of information during the reduction of variables is minimal. Therefore, it is advisable to apply tests of independence of variables. From the null hypothesis that the variables are globally independent, we applied the Bartlett's test of sphericity.

TABLE 6 Bartlett's test of sphericity results

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy		,685
Bartlett's Test of Sphericity	Approx. Chi-Square	3068,650
	df	21
	Sig.	,000

As we can see, the level of significance obtained in Table 6 is lower than 0.05, so the hypothesis is rejected. That's mean the correlation matrix is not an identity matrix, which indicate that the variables are related. Consequently, it is possible to continue with the PCA. The components that retain most of the information in the database are the first and second components (cf. Table 7). Therefore, with this method, it was possible to reduce the seven variables at the start to only two, without losing important information.

TABLE 7 Principal Components Analysis

Component Matrix[a]

	Component	
	1	2
ReceivedBroadcasts	-,469	,732
RXTXLostPackets	,961	
SlotsBackoff	,930	
SNIRLostPackets	,796	,188
TimesIntoBackoff	,955	
totalBusyTime		,899
TotalLostPackets	,981	

Extraction Method: Principal Component Analysis

a. 2 components extracted

To have a better interpretation and approximation of these factors, it is advisable to use some rotation method. The best known is VARIMAX. After a rotation operation, we can see in the figure 8, that the ReceivedBroadcasts and total-BusyTime variables have higher correlation values with component 1. While the remaining variables: SNIRLostPackets, RXTXLostPackets, TotalLostPackets, SlotsBackoff, and TimesIntoBackoff have a very strong positive correlation with component 2.

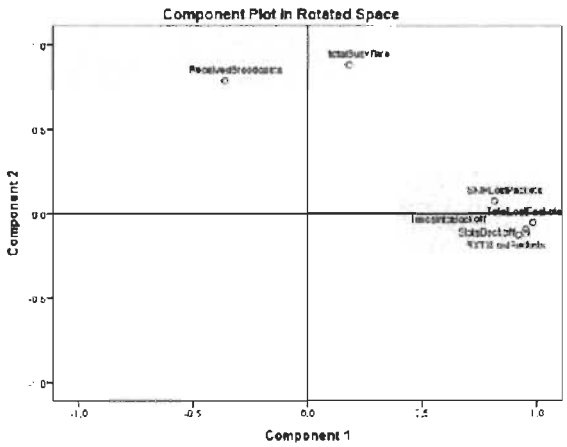

FIGURE 8 VARIMAX rotation result

To continue with the next step and to finish the data analysis in this section, we can say that the transmission of data during the communication in VANET are well represented for the first component, whereas the variables which can represent or measure the quantity of lost packets are explained for component 2. In this way, we can simplify and define two new variables for our model: $F1$ = Transmission and $F2$ = Lost packets.

5 | ANFIS MODEL FOR THE PREDICTION OF A SECURITY INDEX IN VANET

In this section, we will define and build the ANFIS model using MATLAB Toolbox (Figure 10). We start with the ANFIS training that is performed to obtain the optimized values of all its modifiable parameters of a diffuse inference system (FIS). The basic flow diagram of computations in ANFIS is show in figure 9.

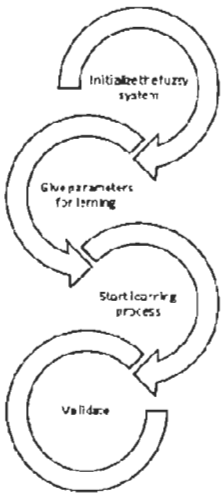

FIGURE 9 Flow diagram of computations in ANFIS

The architecture model is presented in figure 10. We have two input variables, which are the same as those obtained in the previous section. Then, we have an inference engine of Takagi-Sugeno type that is used to generate systematically the fuzzy set of rules from the input data and finally, the variable output that corresponds to a security index in VANET.

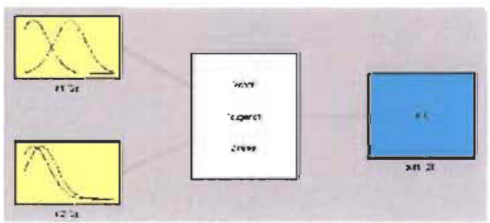

FIGURE 10 ANFIS model definition: 2 inputs, 1 output, 2 rules

The results of our ANFIS design are shown below:

```
1.  Name='Vanets_sugeno'
2.  Type='sugeno'
3.  Version=2.0
4.  NumInputs=2
5.  NumOutputs=1
6.  NumRules=2
7.  AndMethod='prod'
8.  OrMethod='probor'
9.  ImpMethod='prod'
10. AggMethod='sum'
11. DefuzzMethod='wtaver'

12. [Input1]
13. Name='Transmission'
14. Range=[-0.93147 3.76896]
15. NumMFs=2
16. MF1='Normal':'gaussmf',[0.876077677482302 -0.446959408778908]
17. MF2='Suspect':'gaussmf',[0.9573 1.709]

18. [Input2]
19. Name='Lost_Packets'
20. Range=[-1.43628 5.40696]
21. NumMFs=2
22. MF1='Normal':'gaussmf',[1.26409372094562 -0.0676941662457089]
23. MF2='Suspect':'gaussmf',[0.487572290915339 -0.140603724819121]

24. [Output1]
25. Name='Security'
26. Range=[0 1]
27. NumMFs=2
28. MF1='cuticluster1':'linear',[0.357240027754756 -0.0400368511906501 0.208333411094743]
29. MF2='cuticluster2':'linear',[0.357240027754756 -0.0400368511906501 0.208333411094743]

30. [Rules]
31. 1 1, 1 (1) : 1
32. 2 2, 2 (1) : 1
```

FIGURE 11 ANFIS design results

Figure 11 shows the details of the main parameters model and their configuration. The first section corresponds to fuzzy inference system properties. This is a Sugeno type system with 2 inputs and 1 output and each input has its methods: AND method (product of array elements), OR method (Probabilistic OR), implication method (product of array elements), aggregation method (Sum of array elements) and the defuzzification method (weighted average). Input1 (Transmission) and Input2 (Lost Packages), uses two linguistic labels about network behavior "Normal" and "Suspect" and their membership function is defined as Gaussian curve membership function. The variable "Security" has 2 outputs membership function, one for each fuzzy cluster. Properties of a fuzzy inference system depend on the type of clustering used. In this case, we chose the fuzzy c-means (FCM), which is a data clustering technique wherein each element has a degree that is specified by a membership grade. The rules partition themselves according to the fuzzy qualities are associated with each of the data clusters to automatically generate this fuzzy system type.

The basic idea proposed for neuro-adaptive learning technique in this model is very simple. This technique provides a method to diffuse modeling to learn from the data set information, and accordingly to compute the parameters of the membership functions that allow the associated fuzzy inference system to follow the given input and output data. In our case, an ANFIS model has been generated, based on a diffuse system, whose parameters have been adjusted. ANFIS is based on a structure of adaptive networks. The developed ANFIS model composed with 2 input neurons and 1 output neuron along with 4 hidden layers (input membership function, rule base, membership function and aggregated output) is shown in figure 12. Both inputs, neuron 1 and neuron 2 are connected to 2 fuzzy rules. In the layer 2, note that 2 by 2

rules are used. The hidden layers contain 2 neurons to deal with the selection of the proper rule base, because the rule base is written randomly in fuzzy, the neural network selects the right optimal rule base. The branches of this graph are color-coded. Color-coding of branches characterizes the rules and indicates if the logical operators ("and", "not", "or") are used in the rules. The leftmost nodes represent the input and the output is represented by the rightmost node. The node represents a normalization factor for the rules.

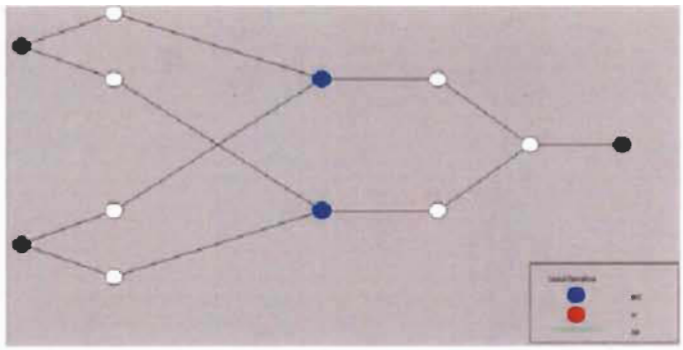

FIGURE 12 ANFIS model structure

6 | RESULTS DISCUSSION

Our aim was to use this model to predict a security index in VANET from simulation results. The input of the model is the message transmission and the lost packets during the communication. So, the output is the security index that allows to predict if the network is attacked or not. To test the predictive capability of the model, we developed it first; this later is then 'trained' on one set of data and it is 'tested' on previously unseen data we collected independently. Finally, the results are compared for their accuracy. Data were divided into two separate sets: the training data set and the checking data set. The training data set was used to train ANFIS, whereas the checking data set was used to verify the accuracy and the effectiveness of the trained ANFIS model for the adaptation of learning content. The main results of the ANFIS model for the prediction of a security index are shown in Figures 13 and 14.

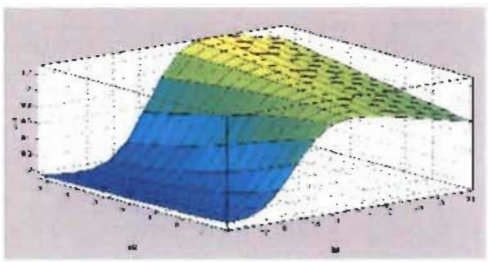

FIGURE 13 Surface of predicted security index

Figure 13 shows one of hyper planes which represents part of multimodal transformation (knowledge rules) with the possibility to map all the security level to given input parameters. This graph shows the surface that is formed as a result of the intersection of the values that the system variables take. In our case, we can see that according to the value of the intersection between the input 1 (In1) "Transmission" and the entry 2 (In2) "Lost packets" on axes "x" and "y", the value of the output (out1) takes a determined value in the z-axis. For example, for the point formed by a transmission value of 0.5 and the lost packets equal to 1, the value of the security index is kept close to zero, that is, the network is not in the presence of an attack. While for the point where the transmission is worth 2 and the lost packets is equal to 4, we have that the security index is greater than 1. This indicates that the network is in the presence of a possible attack.

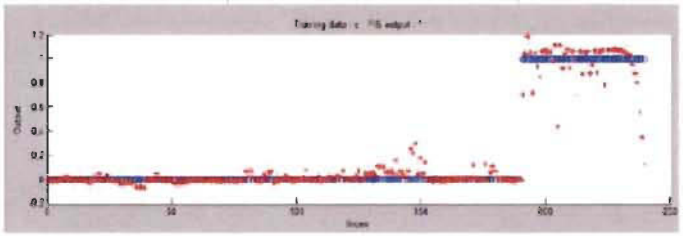

FIGURE 14 Real vs. predicted values

Figure 14 shows the comparison of the predicted value versus the target value of the test data. The model is tested for its ability to predict the accuracy towards achieving the estimated response. If we compare with the simulation results, we can see how the prediction of our model behaves in the case of whether a vehicle is attacked or not. The blue line represented by " o " corresponds to the real data and the red line represented by " * " corresponds to the prediction data. The results show how from our input variables a prediction of security index can be obtained in VANET. After the training of the data, our model shows a good approximation in the prediction of vehicles not attacked and a smaller adjustment in vehicles attacked. But the margin of error is still acceptable as to ensure the effectiveness of the model to predict an attack through our security indicator.

7 | CONCLUSION

Vehicular Ad hoc NETworks present great challenges. To ensure their implementation and effectiveness, many studies and research have been carried out these last years. This work presents one of the first proposal of soft computing for the prediction of attacks in this type of network. Fuzzy inference systems provide an intuitive and high-level mechanism for representing knowledge. Our model shows how by the use of neural networks and fuzzy logic, we can obtain a security index as a measure of protection and possible attack prediction. There are some advantages in our model. One of the most important is that the ANFIS scheme is computationally efficient. This system increases the dynamic performance and provides good stabilization when there is a sudden fluctuation in one of the system parameters. In our specific case, it was observed how the security index obtained responds according to the intersection of the variables "Transmission" and "Lost Packages". Another advantage of the model proposed is the learning capability using the neural networks. ANFIS system handles more complex parameters that was obtained from a variables' reduction with the APC. This proves the effectiveness of the sudden variation of our security index from a normal behavior of the network and its effects when a vehicle is facing an attack.

REFERENCES

[1] Hartenstein H, Laberteaux K. VANET: vehicular applications and inter-networking technologies, vol. 1. John Wiley & Sons; 2009.

[2] Sumra IA, Hasbullah H, et al. VANET security research and development ecosystem. In: National Postgraduate Conference (NPC), 2011 IEEE; 2011. p. 1–4.

[3] Hasrouny H, Samhat AE, Bassil C, Laouiti A. VANet security challenges and solutions: A survey. Vehicular Communications 2017;7:7–20.

[4] Le L, Festag A, Baldessari R, Zhang W. Vehicular wireless short-range communication for improving intersection safety. IEEE Communications Magazine 2009;47(11).

[5] Teixeira FA, e Silva VF, Leoni JL, Macedo DF, Nogueira JM. Vehicular networks using the ieee 802.11 p standard: An experimental analysis. Vehicular Communications 2014;1(2):91–96.

[6] Association IS, et al. Draft Standard for Wireless Access in Vehicular Environments (WAVE)-Multi-channel Operation. IEEE Std 16094-2010 2010;.

[7] Pathak SN, Shrawankar U. Secured communication in real time vanet. In: Emerging Trends in Engineering and Technology (ICETET), 2009 2nd International Conference on IEEE; 2009. p. 1151–1155.

[8] Isaac JT, Zeadally S, Camara JS. Security attacks and solutions for vehicular ad hoc networks. IET communications 2010;4(7):894–903.

[9] Fuentes JMd, González-Tablas AI, Ribagorda A. Overview of security issues in vehicular ad-hoc networks 2010;.

[10] La Vinh H, Cavalli AR. Security attacks and solutions in vehicular ad hoc networks: a survey. International journal on AdHoc networking systems (IJANS) 2014;4(2):1–20.

[11] Mejri MN, Ben-Othman J, Hamdi M. Survey on VANET security challenges and possible cryptographic solutions. Vehicular Communications 2014;1(2):53–66.

[12] Raw RS, Kumar M, Singh N. Security challenges, issues and their solutions for VANET. International Journal of Network Security & Its Applications 2013;5(5):95.

[13] Aijaz A, Bochow B, Dötzer F, Festag A, Gerlach M, Kroh R, et al. Attacks on inter vehicle communication systems-an analysis. Proc WIT 2006;p. 189–194.

[14] Grover J, Gaur MS, Laxmi V. Multivariate verification for sybil attack detection in VANET. Open Computer Science 2015;5(1).

[15] Mejri MN, Ben-Othman J. GDVAN: a new greedy behavior attack detection algorithm for VANETs. IEEE Transactions on Mobile Computing 2017;16(3):759–771.

[16] Erritali M, El Ouahidi B. A survey on VANET intrusion detection systems. In: Proceedings of the 2013 International Conference on Systems, Control, Signal Processing and Informatics; 2013. p. 16–19.

[17] Anjum F, Subhadrabandhu D, Sarkar S. Signature based intrusion detection for wireless ad-hoc networks: A comparative study of various routing protocols. In: Vehicular Technology Conference, 2003. VTC 2003-Fall. 2003 IEEE 58th, vol. 3 IEEE; 2003. p. 2152–2156.

[18] Ping Y, Xinghao J, Yue W, Ning L. Distributed intrusion detection for mobile ad hoc networks. Journal of systems engineering and electronics 2008;19(4):851–859.

[19] Karim L, Boucif AB, Mhamed M, Ismail B. A probabilistic model to corroborate three attacks in vehicular ad hoc networks. In: Computers and Communication (ISCC), 2015 IEEE Symposium on IEEE; 2015. p. 70–75.

[20] Lahrouni Y, Pereira C, Bensaber BA, Biskri I. Using Mathematical Methods Against Denial of Service (DoS) Attacks in VANET. In: Proceedings of the 15th ACM International Symposium on Mobility Management and Wireless Access ACM; 2017. p. 17–22.

[21] Zell A. Simulation neuronaler netze, vol. 1. Addison-Wesley Bonn; 1994.

[22] Bishop CM. Neural networks for pattern recognition. Oxford university press; 1995.

[23] Zadeh LA. On fuzzy algorithms. In: Fuzzy Sets, Fuzzy Logic, And Fuzzy Systems: Selected Papers by Lotfi A Zadeh World Scientific; 1996.p. 127–147.

[24] Suparta W, Alhasa KM. A comparison of ANFIS and MLP models for the prediction of precipitable water vapor. In: Space Science and Communication (IconSpace), 2013 IEEE International Conference on IEEE; 2013. p. 243–248.

[25] Jang JS. ANFIS: adaptive-network-based fuzzy inference system. IEEE transactions on systems, man, and cybernetics 1993;23(3):665–685.

[26] Suparta W, Alhasa KM. Modeling of tropospheric delays using ANFIS. Springer; 2016.

[27] OMNeT++, Discrete Event Simulator; 2017. https://omnetpp.org/.

[28] Veins, vehicular network simulator; 2017. http://veins.car2x.org/.

[29] SUMO, Simulation of Urban MObility; 2017. http://sumo.dlr.de/.

[30] Aad I, Hubaux JP, Knightly EW. Impact of denial of service attacks on ad hoc networks. IEEE/ACM transactions on networking 2008;16(4):791–802.

[31] Porwal V, Patel R, Kapoor R. An investigation of DoS flooding attack in VANET. International journal of advance foundation and research in computing (IJAFRC) 2014;1.

CHAPITRE 5

RÉSULTATS ET DISCUSSION

L'objectif principal de cette étude est de développer un modèle de prédiction sur un indicateur de sécurité dans les réseaux VANETs. Il est basé sur le système d'inférence neuro-floue adaptatif (ANFIS). La méthodologie ANFIS a été appliquée aux données d'échantillons obtenues par les résultats de simulation et après ces informations sont utilisées dans le logiciel MATLAB. L'information est donnée pour deux comportements dans les réseaux VANETs, un réseau sans attaque et un réseau avec attaque. Ensuite, les données d'échantillons sont utilisées pour l'entraînement des ensembles de données de l'ANFIS qui permettent la prédiction d'attaques.

5.1. Statistiques descriptives

Avant d'obtenir le modèle, une analyse des données a été effectuée afin de s'assurer que le modèle de prédiction sélectionné était adéquat pour représenter la population d'où proviennent les données de l'échantillon. Cette analyse était basée sur l'obtention de statistiques (Tableau 4) permettant d'explorer et d'identifier certaines caractéristiques, dans ce cas-ci toutes les variables étaient quantitatives.

Statistiques

		ReceivedBroadcasts	RXTXLostPackets	SlotsBackoff	SNIRLostPackets	TimesIntoBackoff	totalBusyTime	TotalLostPackets
N	Valide	240	240	240	240	240	240	240
	Manquante	0	0	0	0	0	0	0
Moyenne		16,18	5,25	7,37	6,68	1,98	,002686	11,90
Ecart-type		10,693	10,897	6,235	5,788	1,531	,0017807	15,343
Variance		114,337	118,749	38,879	33,501	2,342	,000	235,409
Intervalle		77	48	28	27	7	,0160	71
Minimum		3	0	0	0	1	,0006	0
Maximum		80	48	28	27	8	,0166	71

Tableau 4. Statistiques descriptives

5.2. Modèle Mandami

Au début de ce travail de recherche, un des premiers modèles qu'on a essayé d'utiliser était le modèle Mandami, Il est composé de sept variables d'entrée dont les données ont été obtenues à partir des résultats de simulation.

Les variables ont été modélisées à partir des statistiques descriptives qui ont été fournies par l'analyse exploratoire des données, alors on a pu définir les fonctions d'appartenance pour chaque variable, dans le cas d'un réseau sans attaque (Normal) et dans le cas d'un réseau avec suspicion d'attaque.

RecivedBroadcast (RB)

Fonction d'appartenance

$$\mu_{RB.Normal} = \begin{cases} 0 & si \quad (x \leq 9)\ ou\ (x \geq 24) \\ \dfrac{(x-9)}{4} & si \quad x \in (9,13] \\ 1 & si \quad x \in (13,16) \\ \dfrac{(24-x)}{8} & si \quad x \in (16,24) \end{cases}$$

$$\mu_{RB.Suspect} = \begin{cases} 0 & si \quad (x \leq 16)\ ou\ (x \geq 80) \\ \dfrac{(x-16)}{6} & si \quad x \in (16,22] \\ 1 & si \quad x \in (22,32) \\ \dfrac{(80-x)}{48} & si \quad x \in (32,80) \end{cases}$$

RXTXLostPackets (RXTXLP)

Fonction d'appartenance

$$\mu_{RXTXLP.Normal} = \begin{cases} 0 & si \ \ (x \leq 0) \ ou \ (x \geq 3) \\ \dfrac{x}{0.1} & si \quad x \in (0,0.1] \\ 1 & si \quad x \in (0.1,0.3) \\ \dfrac{(3-x)}{2.7} & si \quad x \in (0.3,3) \end{cases}$$

$$\mu_{RXTXLP.Suspect} = \begin{cases} 0 & si \ \ (x \leq 0.2) \ ou \ (x \geq 48) \\ \dfrac{(x-0.2)}{2.8} & si \quad x \in (0.2,3] \\ 1 & si \quad x \in (3,14) \\ \dfrac{(48-x)}{34} & si \quad x \in (14,48) \end{cases}$$

SlotsBackoff (SB)

Fonction d'appartenance

$$\mu_{SB.Normal} = \begin{cases} 0 & si \ \ (x \leq 0) \ ou \ (x \geq 13) \\ \dfrac{x}{2} & si \quad x \in (0,2] \\ 1 & si \quad x \in (2,6) \\ \dfrac{(13-x)}{7} & si \quad x \in (6,13) \end{cases}$$

$$\mu_{SB.Suspect} = \begin{cases} 0 & si \ \ (x \leq 4) \ ou \ (x \geq 28) \\ \dfrac{(x-4)}{7} & si \quad x \in (4,11] \\ 1 & si \quad x \in (11,20) \\ \dfrac{(28-x)}{8} & si \quad x \in (8,28) \end{cases}$$

SNIRLostPackets (SNIRLP)

Fonction d'appartenance

$$\mu_{SNIRLP.Normal} = \begin{cases} 0 & si \ \ (x \leq 0) \ ou \ (x \geq 13) \\ \frac{x}{2} & si \quad x \in (0,2] \\ 1 & si \quad x \in (2,6) \\ \frac{(13-x)}{7} & si \quad x \in (6,13) \end{cases}$$

$$\mu_{SNIRLP.Suspect} = \begin{cases} 0 & si \ \ (x \leq 4) \ ou \ (x \geq 28) \\ \frac{(x-4)}{3} & si \quad x \in (4,7] \\ 1 & si \quad x \in (7,11) \\ \frac{(28-x)}{17} & si \quad x \in (11,28) \end{cases}$$

TimeIntoBackoff (TB)

Fonction d'appartenance

$$\mu_{TB.Normal} = \begin{cases} 0 & si \ \ (x \leq 1) \ ou \ (x \geq 2) \\ \frac{(x-1)}{0.25} & si \quad x \in (1,1.25] \\ 1 & si \quad x \in (1.25,1.5) \\ \frac{(2-x)}{0.5} & si \quad x \in (1.5,2) \end{cases}$$

$$\mu_{TB.Suspect} = \begin{cases} 0 & si \ \ (x \leq 1.5) \ ou \ (x \geq 8) \\ \frac{(x-1.5)}{0.5} & si \quad x \in (1.5,2] \\ 1 & si \quad x \in (2,4) \\ \frac{(8-x)}{4} & si \quad x \in (4,8) \end{cases}$$

TotalBusyTime (TBT)

Fonction d'appartenance

$$\mu_{TBT.Normal} = \begin{cases} 0 & si \quad (x \leq 0.0014)\ ou\ (x \geq 0.0033) \\ \dfrac{(x - 0.0014)}{0.0004} & si \quad x \in (0.0014, 0.0018] \\ 1 & si \quad x \in (0.0018, 0.0022) \\ \dfrac{(0.0033 - x)}{0.0011} & si \quad x \in (0.0022, 0.0033) \end{cases}$$

$$\mu_{TBT.Suspect} = \begin{cases} 0 & si \quad (x \leq 0.0021)\ ou\ (x \geq 0.0166) \\ \dfrac{(x - 0.0021)}{0.0018} & si \quad x \in (0.0021, 0.003] \\ 1 & si \quad x \in (0.003, 0.004) \\ \dfrac{(0.0166 - x)}{0.0126} & si \quad x \in (0.004, 0.0166) \end{cases}$$

TotalLostPackets (TLP)

Fonction d'appartenance

$$\mu_{TLP.Normal} = \begin{cases} 0 & si \quad (x \leq 0)\ ou\ (x \geq 13) \\ \dfrac{x}{2} & si \quad x \in (0,2] \\ 1 & si \quad x \in (2,6) \\ \dfrac{(13 - x)}{7} & si \quad x \in (6,13) \end{cases}$$

$$\mu_{TLP.Suspect} = \begin{cases} 0 & si \quad (x \leq 5)\ ou\ (x \geq 71) \\ \dfrac{(x - 5)}{8} & si \quad x \in (5,13] \\ 1 & si \quad x \in (13,20) \\ \dfrac{(71 - x)}{51} & si \quad x \in (20,71) \end{cases}$$

Pour ce modèle on a défini 24 règles. Les résultats sont présentés dans la figure suivante :

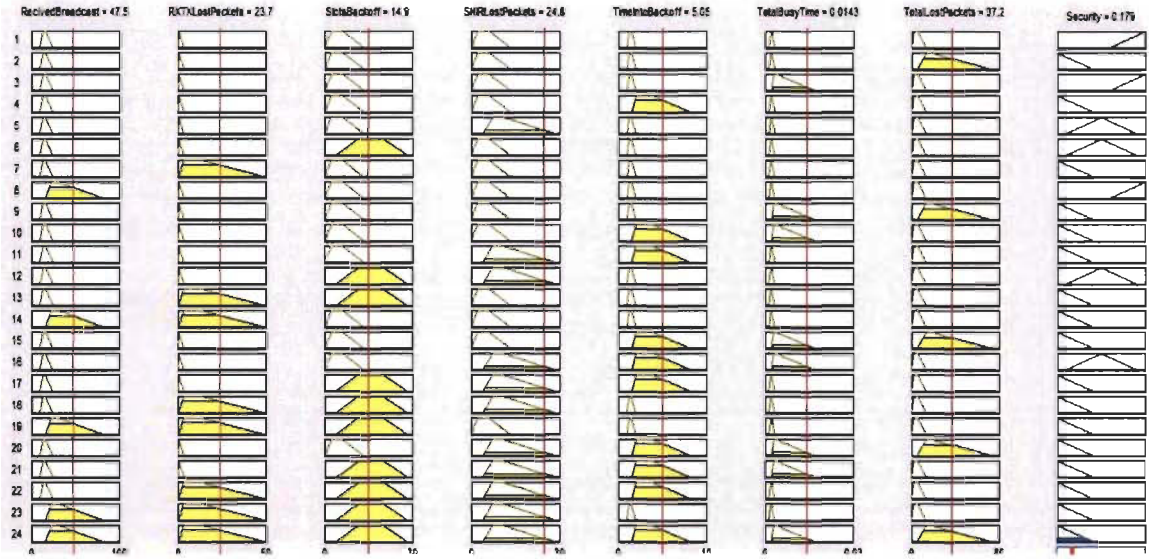

Figure 7. Modèle Mandami

5.3. Analyse de corrélation

On a fait un test d'hypothèses pour prouver que les variables sont globalement dépendantes. Le résultat le plus significatif de cette analyse était la forte corrélation entre différentes variables.

Corrélations

		ReceivedBroadcasts	RXTXLostPackets	SlotsBackoff	SNIRLostPackets	TimesIntoBackoff	totalBusyTime	TotalLostPackets
ReceivedBroadcasts	Corrélation de Pearson	1	-,403**	-,409**	-,222**	-,383**	,426**	-,369**
	Sig. (bilatérale)		,000	,000	,001	,000	,000	,000
	N	240	240	240	240	240	240	240
RXTXLostPackets	Corrélation de Pearson	-,403**	1	,889**	,665**	,935**	,059	,959**
	Sig. (bilatérale)	,000		,000	,000	,000	,365	,000
	N	240	240	240	240	240	240	240
SlotsBackoff	Corrélation de Pearson	-,409**	,889**	1	,627**	,916**	,061	,866**
	Sig. (bilatérale)	,000	,000		,000	,000	,346	,000
	N	240	240	240	240	240	240	240
SNIRLostPackets	Corrélation de Pearson	-,222**	,665**	,627**	1	,667**	,134*	,849**
	Sig. (bilatérale)	,001	,000	,000		,000	,038	,000
	N	240	240	240	240	240	240	240
TimesIntoBackoff	Corrélation de Pearson	-,383**	,935**	,916**	,667**	1	,082	,914**
	Sig. (bilatérale)	,000	,000	,000	,000		,207	,000
	N	240	240	240	240	240	240	240
totalBusyTime	Corrélation de Pearson	,426**	,059	,061	,134*	,082	1	,090
	Sig. (bilatérale)	,000	,365	,346	,038	,207		,165
	N	240	240	240	240	240	240	240
TotalLostPackets	Corrélation de Pearson	-,369**	,959**	,866**	,849**	,914**	,090	1
	Sig. (bilatérale)	,000	,000	,000	,000	,000	,165	
	N	240	240	240	240	240	240	240

**. La corrélation est significative au niveau 0.01 (bilatéral).

*. La corrélation est significative au niveau 0.05 (bilatéral).

Tableau 5. Analyse de corrélation

Dans l'analyse de corrélation (Tableau 5), on a observé que la variable TotalLostPackets est très corrélée avec les variables RXTXLostPacket, SlotsBackoff, SNIRLostPackets et TimesIntoBakoff. Cette corrélation a été assez grande pour justifier la factorisation de la matrice des coefficients de corrélation. Il est important de noter qu'un modèle de prédiction qui inclut des variables hautement corrélées peut entraîner une redondance de l'information, Ce qui affecte l'approximation et la véracité du modèle.

5.4. Analyse en composantes principales

Pour la factorisation des variables, on a choisi l'analyse en composantes principales (ACP) qui appartient aux méthodes multivariées. C'est l'une des techniques multifactorielles utilisées pour résumer de la façon la plus fidèle un grand ensemble de données. Un des critères étudiés pour choisir le numéro de composants à garder, était l'obtention de la proportion de variance globale expliquée (Tableau 6).

Variance totale expliquée

Composante	Valeurs propres initiales			Extraction Sommes des carrés des facteurs retenus			Somme des carrés des facteurs retenus pour la rotation		
	Total	% de la variance	% cumulés	Total	% de la variance	% cumulés	Total	% de la variance	% cumulés
1	4,520	64,569	64,569	4,520	64,569	64,569	4,458	63,692	63,692
2	1,388	19,831	84,400	1,388	19,831	84,400	1,450	20,708	84,400
3	,488	6,978	91,377						
4	,412	5,886	97,263						
5	,127	1,812	99,075						
6	,065	,922	99,997						
7	,000	,003	100,000						

Méthode d'extraction : Analyse en composantes principales.

Tableau 6. Variance totale expliquée

Dans notre cas, on a 84.4% de variance avec les deux premiers composants. Donc, comme principal résultat de cette analyse, on a réussi à réduire le nombre de variables de 7 à seulement 2 variables (Tableau 7).

Matrice des composantes[a]

	Composante	
	1	2
ReceivedBroadcasts	-,469	,732
RXTXLostPackets	,961	
SlotsBackoff	,930	
SNIRLostPackets	,796	,188
TimesIntoBackoff	,955	
totalBusyTime		,899
TotalLostPackets	,981	

Méthode d'extraction : Analyse en composantes principales.

a. 2 composantes extraites.

Tableau 7. Matrice des composantes

Pour avoir une meilleure interprétation et approximation des facteurs, il est conseiller d'utiliser des méthodes de rotation et une méthode de rotation et la plus connue est la méthode VARIMAX.

Pour interpréter chaque composante principale, on a examiné la valeur et la direction des coefficients des 7 variables initiales. Plus la valeur absolue du coefficient est élevée et plus la variable correspondante est importante dans le calcul de la composante. La valeur absolue à partir de laquelle un coefficient peut être considéré comme important est subjective et basé sur les connaissances spécialisées par rapport au fonctionnement du réseau. Alors pour continuer avec l'étape suivante et à partir de cette analyse on a pu voir dans la figure 8 que la transmission des données est bien représentée par la composante 1, qu'on a défini par la variable « *Transmission* », alors que les variables qui peuvent représenter la quantité des paquets perdus sont expliquées par le composante 2 qu'on a redéfini comme la variable « *Lost Packets* ».

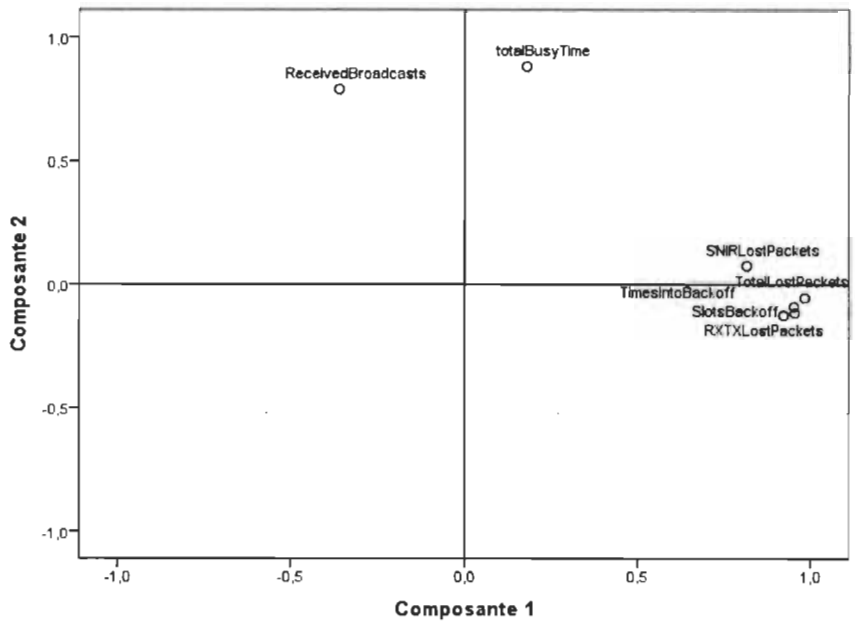

Figure 8. Diagramme de composantes dans l'espace après rotation

5.5. Modèle ANFIS

Notre modèle a montré comment en utilisant les réseaux de neurones et la logique floue, nous pouvons obtenir un indicateur de sécurité qui sert comme mesure de prédiction d'attaques. Il y a quelques avantages dans ce modèle. L'un des plus importants est que le système ANFIS est efficace au niveau du calcul informatique. Ce système augmente les performances dynamiques et fournit une bonne stabilisation en cas de fluctuation soudaine de l'un des paramètres du système. Dans notre cas particulier, on a observé comment l'indicateur de sécurité obtenu répond en fonction de l'intersection des paramètres utilisés. Un autre avantage du modèle proposé est la capacité d'apprentissage utilisant les réseaux neuronaux. Le système ANFIS gère des paramètres plus complexes obtenus à partir de la réduction des variables avec l'ACP. Cela prouve l'efficacité de la variation soudaine de notre indicateur de sécurité d'un comportement normal du réseau et de ses effets lorsqu'un véhicule est confronté à une attaque.

Les résultats de la simulation montrent que l'algorithme d'apprentissage de notre modèle ANFIS fonctionne bien dans le processus de détection d'attaques et il améliore le taux de convergence, avec une approximation satisfaisante.

CHAPITRE 6

CONCLUSION ET PERSPECTIVES

Aujourd'hui, les technologies évoluent très rapidement dans le temps, il y a beaucoup d'intérêt à implémenter les réseaux VANETs dans notre société. Ces réseaux fournissent de nombreux avantages, en particulier dans le domaine social. Un des objectifs les plus importants est que ces réseaux permettent d'améliorer la sécurité routière grâce aux messages échangés entre les véhicules pour diminuer le nombre d'accidents qui se produisent et éviter la perte de beaucoup de vies.

Les réseaux VANETs sont relativement récents. C'est vrai que la connaissance préalable des réseaux sans fil et des technologiques mobiles existants permet la conception de nouveaux systèmes, mais il est important de consacrer toutes les ressources nécessaires dans la recherche pour une technologie moins coûteuse, efficace et sécure.

Comme toute nouvelle technologie, il existe de nombreux défis et problèmes pour les réseaux VANETs et dans le cadre de ce mémoire, nous avons traité la problématique des attaques sur les véhicules.

Pour surmonter la problématique reliée aux possibles attaques, notre travail a suivi différentes étapes avant l'obtention de notre modèle final.

Ce mémoire présente une première approche d'un modèle de prédiction d'attaques dans les réseaux VANETs basé sur la logique floue. Les résultats nous montrent le contraste d'un premier modèle basé sur le modèle de Mandami à partir de 7 variables. Ce modèle est capable de prédire une attaque sur le réseau, cependant étant donné le nombre de variables et de règles, sa précision n'est pas la meilleure. Pour cette raison on a décidé d'optimiser le modèle en réduisant le nombre de variables et en utilisant le modèle ANFIS pour obtenir une meilleure approximation dans la prédiction.

Le système ANFIS proposé applique le mécanisme d'apprentissage des réseaux de neurones sur des techniques d'inférence floues. On a défini ANFIS comme un système

d'inférence floue dont les paramètres des fonctions d'appartenance sont ajustés en utilisant l'algorithme d'*apprentissage rétropropagation*.

Comme les technologies avancent avec le temps, les attaques et les systèmes dédies à perturber la stabilité des systèmes de communication changent rapidement. Les modèles de prédiction basés sur l'apprentissage automatique et les algorithmes non supervisés, comme celui de notre approche, sont avantageux étant donné leur capacité à évoluer avec leur propre système en permettant d'apercevoir des anomalies dans le fonctionnement du réseau ou de détecter de nouvelles attaques.

En ce qui concerne la sécurité des réseaux véhiculaires VANETs, il reste encore beaucoup de travail à faire. À l'avenir, ce type de modèle pourrait être appliqué pour prédire d'autres types d'attaques existantes.

Ce travail vise à servir de base pour les lignes de recherche futures de ce type de modèle de prédiction. Ces modèles soutiennent les systèmes de détection d'intrusion basées sur l'anomalies.

RÉFÉRENCES

[1] L. Long, A. Festag, R. Baldessari, Z. Wenhui, "Vehicular wireless short-range communication for improving intersection safety," Communications Magazine, IEEE, vol.47, no.11, pp.104-110, Novembre 2009.

[2] H. Hartenstein, K. Laberteaux, "VANET Vehicular Applications and Inter-Networking Technologies," 2009. ISBN 0470740620, 9780470740620.

[3] O. Orozco, G. Llano, "Aplicaciones para redes VANET Estimación del exponente de Hurst y dimensión fractal para el análisis de series de tiempo de absorbancia UV-Vis," Ciencia e Ingeniería Neogranadina, 24 (2), pp. 111 – 132, 2014.

[4] R. Coussement, « Mécanisme d'aide à la décision pour les IDS dans les réseaux VANETs», Mémoire, Université du Québec à Trois-Rivières, Département de mathématiques et d'informatique appliquée, Janvier 2014.

[5] Wikipédia, Vehicular Ad-Hoc Network, https://es.wikipedia.org/wiki/Vehicular_Ad-Hoc_Network#cite_note-3, date de dernière modification, 28 août 2015.

[6] IEEE, 802.11p, http://standards.ieee.org/getieee802/download/802.11p-2010.pdf, date de dernière modification, 25 août 2015.

[7] A. Adigun, « Gestion de l'anonymat et de la traçabilité dans les réseaux véhiculaires sans fil», Mémoire, Université du Québec à Trois-Rivières, Département de mathématiques et d'informatique appliquée, Février 2014.

[8] G. Gonzales, D. López, L. Pedraza, "Simulación y análisis de desempeño de protocolos unicast para Redes VANET," Revista Tecnuras, vol.16, no.31, pp.67-75, Janvier 2012.

[9] M. JERBI, « Protocoles pour les communications dans les réseaux de véhicules en environnement urbain: Routage et GeoCast basés sur les intersections », Thèse de doctorat, Universite d'Evry, Val d'Essonne, 2008.

[10] M. Fiore, J. Harri, F. Filali, and C. Bonnet, "Vehicular Mobility Simulation for VANETs," in Proceedings of the 40th Annual Simulation Symposium, Norfolk, VA , 2007, pp. 301-309.

[11] S. N. Pathak and U. Shrawankar, "Secured Communication in Real Time VANET," in Proceedings of the 2009 Second International Conference on Emerging Trends in Engineering & Technology, Nagpur , 2009, pp. 1151-1155.

[12] United Stated Deparment of Transportation, IEEE 1609 - Family of Standards for Wireless Access in Vehicular Environments (WAVE), https://www.standards.its.dot.gov/factsheets/factsheet/80, date de dernière modification, 03 Septembre 2015.

[13] J. Fuentes, A. González-Tablas, A. Ribagorda, "Overview of security issues in Vehicular Ad-hoc Networks," IGI Global, 2010.

[14] A. Aijaz, B. Bochow, F. Dötzer, A. Festag, M. Gerlach, K. Kroh. "Attacks on Inter-Vehicle Communication Systems - An Analysis", International Workshop on Intelligent Transportation. Hamburg, Germany: IEEE Communications Society, 2006.

[15] N. Chaid. « La sécurité des communications dans les réseaux VANET », Mémoire, Universite Elhadj Lakhder – Batna, Faculté des sciences de l'ingénieur, Département d'informatique.

[16] M. N. Mejri, J. Ben-Othman, M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions", Vehicular Communications, (2014), pp. 53–66.

[17] R. S. Raw, M. Kumar, N. Singh, "Security Challenges, issues and their Solutions for VANET", International Journal of Network Security & its Applications (IJNSA), Vol. 5, No. 5, 2013.

[18] K. Lauroussi, A. Bensaber, M. Mesfioui, I. Biskri, "A probabilistic model to corroborate three attacks in Vehicular Ad Hoc Networks," Université du Québec à Trois-Rivières, Département de mathématiques et d'informatique appliquée, 2015.

[19] Grover, J; Gaur, M.S; Vijay, L.; "Multivariate verication for sybil attack detection in VANET", DOI 10.1515/comp-2015-0006. Open Comput. Sci. 2015; 5:60–78.

[20] Mejri, M., Ben-Othman, J.: "GDVAN: A New Greedy Behavior Attack Detection Algorithm for VANETs," in IEEE Transactions on Mobile Computing, vol. 16, no. 3, pp. 759-771, March 1 2017. doi: 10.1109/TMC.2016.2577035.

[21] Lahrouni, Y.; Amar Bensaber, B.; Pereira, C; Biskri, I., "Using Mathematical Methods against Denial of Service (DoS) Attacks in VANET", MobiWac'17, November 21–25, 2017, Miami, FL, USA, ISBN 978-1-4503-5163-8/17/11, https://doi.org/10.1145/3132062.3132065.

[22] Touzet, C., "Les réseaux de neurones artificiels, introduction au connexionnisme". EC2, Paris, 1992.

[23] Zadeh, L.A.; "Fuzzy sets, Information and Control", Volume 8, Issue 3, 1965, Pages 338-353, ISSN 0019-9958, https://doi.org/10.1016/S0019-9958(65)90241-X.

[24] Djokhrab, A. E., "Planification et Optimisation de Trajectoire d'un Robot Manipulateur à 6 DDL par des Techniques Neuro-Floues." PhD diss., Université Mohamed Khider-Biskra, 2015.

[25] Zadeh, L.A.; "Fuzzy sets, Information and Control", Volume 8, Issue 3, 1965, Pages 338-353, ISSN 0019-9958, https://doi.org/10.1016/S0019-9958(65)90241-X.

[26] https://omnetpp.org/ (Consulté //2017).

[27] http://veins.car2x.org/ (Consulté //2017).

[28] https://sourceforge.net/ (Consulté //2017).

[29] Aad, I.; Hubaux, J.P.; Knightly, E.W., "Impact of Denial of Service Attacks on Ad Hoc Networks," in IEEE/ACM Transactions on Networking, vol. 16, no. 4, pp. 791-802, Aug. 2008. doi: 10.1109/TNET.2007.904002.

[30] Porwal, V.; Patel, R.; Kapoor, K.R.; "An Investigation of DOS Flooding Attack in VANET", International Journal of Advance Foundation and Research in Computer (IJAFRC) Volume 1, Issue 12, December 2014. ISSN 2348 – 4853.

[31] Tukey, J. W., "Exploratory data analysis", Vol. 2. 1977.