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
ROMAIN COUSSEMENT

MÉCANISME D'AIDE À LA DÉCISION POUR LES IDS DANS LES RÉSEAUX VANETS

JANVIER 2014

CE MÉMOIRE A ÉTÉ ÉVALUÉ

PAR UN JURY COMPOSÉ DE

M. Boucif Amar Bensaber, directeur de mémoire
Département de mathématiques et informatique
À l'Université du Québec à Trois-Rivières

M. Ismail Biskri, évaluateur
Département de mathématiques et informatique
À l'Université du Québec à Trois-Rivières

M. Adel Omar Dahmane, évaluateur
Département de génie électrique et génie informatique
À l'Université du Québec à Trois-Rivières

MÉCANISME D'AIDE À LA DÉCISION POUR LES IDS DANS LES RÉSEAUX VANETS.

Romain Coussement

SOMMAIRE

Les réseaux véhiculaires sans fil (VANETs) sont difficiles à sécuriser due à l'utilisation de la technologie sans fil et à ses nombreuses failles de sécurité. Pour se protéger contre les attaques, des méthodes et techniques ont été développées. Les systèmes de détection d'intrusion (IDS) peuvent détecter un comportement malveillant dans un système informatique. Dans les réseaux sans fil véhiculaires, les IDSs analysent les paquets entrants et sortants dans le réseau afin d'identifier une signature malveillante. Néanmoins, sans mécanisme de prise de décision, ceux-ci deviennent inefficaces. Notre travail conceptualise un protocole de prise de décision pour les informations de sécurité dans les réseaux VANETs. Notre étude est basée sur deux approches d'IDS. Dans la première, les IDSs sont installés dans les véhicules, tandis que dans la seconde, ils sont installés sur les équipements du bord de route (RSU). Dans les deux approches, nous effectuons une clusterisation des véhicules en fonction de leurs vitesses sur la route. La corroboration d'une attaque est basée sur le calcul de ratio entre les véhicules ou entre les RSUs ayant répondu à la signature de l'attaque. Notre but est de concevoir un mécanisme d'aide à la décision. La topologie dynamique des réseaux VANETs permet une forte prévention grâce à la diffusion d'information. C'est pourquoi, lorsqu'une attaque est détectée, le protocole permet la corroboration de celle-ci et en avertit les clusters voisins.

DECISION SUPPORT PROTOCOL FOR INTRUSION DETECTION IN VANETs

Romain Coussement

ABSTRACT

Vehicular Ad hoc Networks (VANETs) are so difficult to secure due to the wireless technology and its several known security holes. To protect against attacks, methods and techniques have been developed. The Intrusion Detection System (IDS) can detect malicious actions made to the system. In vehicular ad hoc networks, IDSs are in charge of analyzing incoming and outgoing packets to identify malicious signatures. However, without a decision making mechanism, they are useless. This work designs a decision making protocol for security information in VANETs. Our study is based on two IDS approaches. In the first one, the IDS are installed on vehicles, while in the second one they are installed on the Road Side Units (RSU). In both approaches, vehicles are grouped according to their speed. Corroboration of an attack is based on a probabilistic model of ratio computation between vehicles or RSUs having answered to the signature of the attack. Our aim is to design a decision support mechanism. The dynamic topology of VANET allows a strong prevention by broadcasting the information. So when an attack occurs, the protocol allows the corroboration of the latter and alert neighboring clusters.

REMERCIEMENTS

En premier lieu, je souhaite remercier monsieur Boucif Amar Bensaber, mon directeur de recherche, pour m'avoir judicieusement guidé et soutenu durant ma maitrise.

Je tiens également à remercier pour leurs judicieux conseils et pour avoir accepté de réviser ce mémoire, messieurs Ismail Biskri et Adel Omar Dahmane, membres du jury.

Je remercie Adigun Adetundji mon collègue et camarade avec qui j'ai pu échanger et améliorer des idées de recherche.

Je remercie toute ma famille pour les corrections et améliorations qu'ils ont pu apporter à l'ouvrage.

Enfin, je remercie Mlle Marie Bouchet pour avoir mis à mon service ses talents de graphiste.

Merci à vous !

TABLE DES MATIÈRES

LISTE DES FIGURES

LISTE DES TABLEAUX

INTRODUCTION GÉNÉRALE

Les gouvernements investissent massivement dans la prévention routière pour les véhicules et les routes de demain; leurs objectifs sont de réduire le nombre d'accidents sur la route et sauver des vies. Les réseaux VANETs sont une solution à ce problème. Actuellement, nos véhicules sont électronisés avec des ordinateurs de bord. Ils traitent des informations telles que : la température interne et externe, le GPS (*Global Positioning System*), le système de frein à main, etc. Malheureusement, ces informations sont confinées dans chaque véhicule et aucun système de communication d'information n'est présent pour diffuser ces informations vitales aux autres véhicules. Les communications sans fil peuvent résoudre ce problème en fournissant des applications de confort aux usagers et des applications de sécurité tels l'optimisation du trafic routier ou l'avertissement d'un risque de verglas.

Les communications sans fil 3G, Wifi et Bluetooth, sont largement utilisées de nos jours. Leurs coûts sont abordables pour des débits et des portées de transmissions de plus en plus élevés. De l'émergence de ces technologies sans fil sont nés les réseaux MANET (*Mobile Ad hoc NETwork*) connectant les ordinateurs entre eux et par dérivations, les réseaux VANETs (*Vehicular Ad hoc NETwork*) connectant les véhicules autoroutiers. Contrairement aux MANET, les VANETs sont soumis à : une topologie hautement dynamique, une forte mobilité des nœuds, une connectivité changeante, etc. Les autres types de réseaux sans fil s'accordent sur certains critères de stabilité au niveau topologique pour avoir des performances maximales. Néanmoins, la communication dans les VANETs se fait en temps réel, avec des véhicules pouvant aller à plus de 100 km/h (sur autoroute et en fonction des pays). La topologie est hautement dynamique. Des pertes de connectivités sont à prévoir et les connexions non fiables doivent être sécurisées par des protocoles.

Les applications de sécurité du trafic routier envoient des informations pertinentes aux usagers de la route. Les alertes d'accidents doivent être envoyées et relayées par les

véhicules ou par les RSUs (*Road Side Unit*) vers les autres véhicules afin d'éviter tout carambolage. Ces informations sont vitales aux objectifs intrinsèques des VANETs, c'est pourquoi la sécurité de ces réseaux est primordiale.

Afin d'augmenter la sécurité et stabiliser la topologie des VANETs, des groupes de véhicules (*Cluster*) ont été définis. Les clusters permettent de faciliter l'échange de données entre véhicules membres, mais également de mettre en place des mécanismes de sécurité supplémentaires dans le réseau comme les systèmes de détection d'intrusions.

Les IDS (*Intrusion Detection System*) sont définis comme étant la dernière ligne de défense lors d'une attaque. Ils permettent la détection d'attaques ciblant un véhicule ou un réseau. Néanmoins, ils n'offrent pas à ce jour de mécanismes en réponse aux attaques. Les IDS fournissent l'information qu'une attaque a été détectée, néanmoins, cette information n'est pertinente que si elle est utilisée. De même les questions : « Comment disposer les IDS dans notre réseau ? », « Doit-on les disposer sur les véhicules ou sur les RSUs ? », « Que faire des informations d'une intrusion ? » et « Serait-il intéressant de combiner des méthodes de clusterisation avec des IDS ? » sont à étudier. À ce jour, la recherche ne propose pas encore de solutions complètes à ces problèmes. Notre travail présente un protocole de prise de décision pour les informations de sécurité. Il combine une méthode de clusterisation et un IDS, tout en comparant les avantages liés entre les IDS basés véhicules et les IDS basés infrastructure. L'objectif est de diffuser l'information qu'une attaque a été détectée aux clusters voisins proches afin de mettre en place des politiques de sécurité pour les nouveaux véhicules entrant dans le cluster.

Ce mémoire se compose comme suit: Le chapitre 1 présente les réseaux VANETs et leurs spécificités. Le chapitre 2 présente l'état de l'art, nous relatons des propositions faites par la littérature sur la sécurité, sur les IDS ainsi que sur les clusters. Nous présentons la modélisation et la conception de notre protocole dans le chapitre 3. Le chapitre 4 présente les simulations effectuées ainsi que l'analyse des résultats. Enfin, le chapitre 5, conclut et propose des pistes de solution et des améliorations futures.

CHAPITRE I - LES RÉSEAUX VANETS

Avec plus de 2000 victimes de la route en 2011 [30], le gouvernement canadien investit massivement dans la recherche sur les réseaux véhiculaires sans fil. En plus de faire de la prévention routière, son objectif est d'améliorer les conditions de conduite des conducteurs, éviter les distractions et être averti au plus vite des risques de carambolage ou de collision. Les VANETS offrent des applications de confort comme la connexion à Internet, la vidéo, etc. dans le but de distraire les passagers et des applications de sécurité routière, comme les messages d'alerte accidents ou de prévention (exemple : information de température extérieure négative). Ces applications font partie de ce que l'on appelle les systèmes de transport intelligent (ITS, *Intelligent Transport System*) dont le but est d'améliorer la sécurité, l'efficacité, la convivialité dans les transports routiers grâce aux technologies innovantes de la recherche.

Ce chapitre se présente en six points pour définir les réseaux VANETs. Dans le point 1, « Vue d'ensemble sur les réseaux VANETs ». Nous présentons de manière générale les réseaux VANETs. Parmi les généralités on y retrouve, l'architecture et les caractéristiques des réseaux VANETs, mais aussi les technologies de communications dont ceux-ci sont équipés. Dans le point 2, « Développement des standards de communication pour les réseaux sans fil véhiculaires ». Nous présentons les standards adoptés pour les réseaux VANETs. Dans le point 3, « Sécurité dans les VANETs ». Nous présentons différents modèles d'attaques possibles dans le réseau. Dans le point 4, « Les systèmes de détection d'intrusions pour les VANETS ». Nous présentons les différents modèles d'IDS proposés. Enfin, dans le point 5, « La Clusterisation ». Nous présentons les méthodes de clusterisation utilisé pour les réseaux VANETs.

1.1 VUE D'ENSEMBLE SUR LES RÉSEAUX VANETS

Les différents aspects architecturaux de VANET sont étudiés dans cette première partie. On présente, les entités agissant dans le réseau, les modes de communications possibles, les types d'applications importantes dans VANET et les messages véhiculés par les applications. Les caractéristiques propres aux VANETS, comme l'environnement de déploiement du réseau et l'environnement du véhicule (mobilité, énergie, etc.) seront présentées dans le second aspect.

1.1.1 ARCHITECTURE

1.1.1.1 Les entités communicantes

Dans un réseau véhiculaire sans fil, il existe plusieurs entités permettant la communication, parmi ceux-ci : les véhicules, le RSU ainsi que l'équipement central [26]. Les équipements personnels, comme les téléphones, tablettes, etc. peuvent se connecter aux véhicules, néanmoins ceux-ci ne font pas partie des VANETs. Nous ne les considérons pas dans cette étude.

1.1.1.1.1 Véhicule

Les véhicules sont le centre des entités du réseau. Ils possèdent de nombreux capteurs et unités de calcul à bord permettant de gérer et traiter les informations reçues. Les véhicules sont équipés de bornes « *On Board Unit* » (OBU). L'OBU est l'interface de calcul, de localisation et d'émission/réception de messages dans le réseau. Le véhicule intelligent et son équipement, ainsi que l'intégralité des protocoles et des normes mise en place pour la communication sont appelés DSRC (*Dedicated Short Range Communication*).

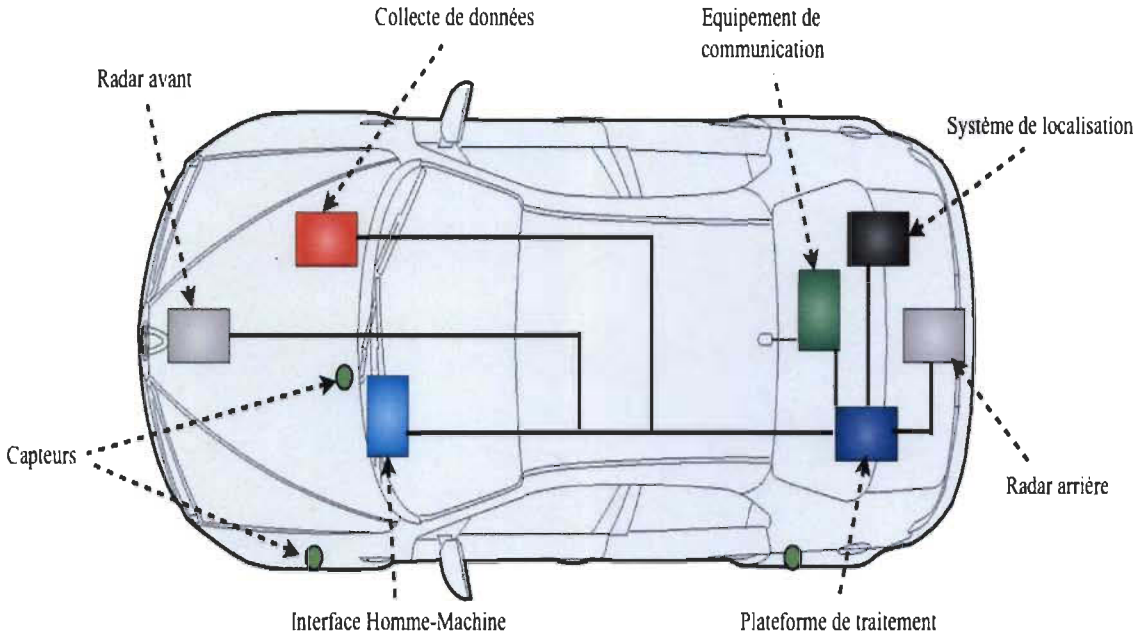


Figure 1 : Véhicule intelligent et ses composants [25]

1.1.1.1.2 RSU

Les RSUs (*Road Side Unit*) sont les bornes au bord de la route. Elles ont deux fonctions: dans un premier temps, elles diffusent les informations météorologiques, le trafic routier, etc. ; dans un second temps, elles permettent également de retransmettre l'information sur de longues distances entre les véhicules et vers les points d'entrée du réseau pour y connecter les véhicules aux différentes applications proposées.

1.1.1.1.3 Équipement central

L'équipement central est quant à lui transparent pour l'utilisateur. Il est utilisé côté serveur. Il est un point d'entrée au réseau internet et il fournit des services et applications pour les VANETs (exemple : paiement en ligne, vidéo à la demande, etc.).

1.1.1.2 Architectures de communication

Les VANETS ont pour objectif d'être ouverts et connectés aux réseaux pour utiliser les services proposés. Nous présentons ici les différents modes de communication mis en place pour répondre à ce besoin.

1.1.1.2.1 Véhicule à véhicule (V2V)

On parle de communication véhicule à véhicule (V2V) lorsqu'au moins deux véhicules communiquent ensemble par l'intermédiaire de leur OBU. Ce mode de communication est également appelé ad hoc comme dans les réseaux MANET, où chaque véhicule représente un nœud du réseau. Chaque véhicule est alors une passerelle pour relayer l'information aux autres participants dans le réseau. Ce mode de communication ne requiert pas d'infrastructure pour son fonctionnement. Il est très efficace pour diffuser rapidement les informations dans le réseau. Dans le cas où le RSU est dysfonctionnel, les véhicules doivent être capables de maintenir une connectivité suffisante dans le réseau. Ce mode permet au VANET de s'autosuffire. Il est clair qu'une forte mobilité des véhicules dans le réseau implique une connectivité instable dans le réseau.

1.1.1.2.2 Véhicule à Infrastructure (V2I)

On parle de communication véhicule à infrastructure (V2I) lorsque le véhicule via son OBU échange des informations avec l'infrastructure routière (RSU). Dans un fonctionnement classique, le RSU fournit toujours les applications de quelques natures qu'elle soit (internet, information routière, information météorologique, etc.) aux véhicules [27]. Le mode de communication V2I est le fonctionnement principal des VANETS. Ce mode de communication offre également une connectivité plus stable dans le réseau, due à sa longue portée de diffusion. Dans le cas où l'infrastructure communique avec les véhicules, on parlera également de communication V2I.

L'enjeu principal des RSUs est leur coût de déploiement très élevé, c'est pourquoi un mode de communication hybride permettra de faire communiquer toutes les entités du réseau.

1.1.1.2.3 Hybride

Les différents modes de communication présentés jusqu'à présent, qu'ils soient entre véhicules ou entre le véhicule et l'infrastructure sont des atouts majeurs. Néanmoins ceux-ci, pris séparément, présentent des limites dans les échanges d'informations des VANETs. Les communications uniquement véhiculaires sont de faible portée. Elles ne permettent pas de joindre rapidement des véhicules distants ; tandis que les communications uniquement véhicules à infrastructure permettent d'échanger des informations sur de longues distances, mais sans exploiter les forces de la topologie du réseau. L'utilisation des deux méthodes de communication simultanée est le point fort des VANETS. Ce mode hybride permet de diffuser efficacement les informations des applications sur courtes et longues portées en utilisant la topologie dynamique des VANETS.

1.1.1.3 Les différents types d'applications

Différents messages sont échangés dans les réseaux sans fil véhiculaires, dont ceux des applications ou services qu'on peut classer en 3 catégories [25] :

1.1.1.3.1 Application de confort

Les applications de confort ont pour but d'améliorer la qualité du voyage du conducteur comme des passagers. Comme certains voyages peuvent parfois être longs, dû au trajet ou aux congestions sur la route, il est important de soulager le conducteur de certaines tâches automatisables. C'est pourquoi les VANETS proposent des applications de paiement automatique sur les autoroutes, des affichages de restaurants, stations-service,

des propositions de routes alternatives, etc. susceptibles d'intéresser le conducteur pendant sa conduite. Les autres passagers auront la possibilité d'accéder à des vidéos à la demande, jeux en réseau sur Internet ou avec d'autres véhicules, musique, etc. Il existe un large champ d'applications à ces services et les perspectives d'applications de confort sont très prometteuses.

1.1.1.3.2 Application de Sécurité

Les applications de sécurité visent avant tout à prévenir des accidents, qu'ils soient dus aux conditions météorologiques (pluie, verglas, etc.), à l'inattention d'un conducteur (fatigue, événement surprenant, etc.) ou à tout problème technique interne au véhicule (pièce défectueuse ou usée). Pour pallier à ces problèmes, les véhicules intègrent des capteurs de température externe. Ceux-ci analysent en temps réel la température et envoient des alertes au conducteur ainsi qu'aux membres des VANETS proches pour valider le constat. Des capteurs de pression atmosphérique (baromètre) et d'humidité permettent également de relever des alertes météorologiques telles que la pluie, la grêle, etc. On retrouve également des outils de surveillance du conducteur, permettant de surveiller son état de fatigue afin que des propositions adéquates lui soient faites telles qu'un hôtel, une auberge, ou simplement une aire d'autoroute pour s'arrêter. Le système enverra des alertes aux véhicules proches en cas de malaise ou de l'endormissement du conducteur. Ces cas de figure diffusent des alertes de ralentissement anormales sur la route.

Dans le cas où l'accident est avéré, l'alerte sera dite majeure; les conducteurs se doivent de ralentir grandement et d'adapter leur conduite.

Dans tous les cas, un véhicule émettant une alerte définira un périmètre de danger pour les autres utilisateurs. Ceux-ci recevront une alerte à plusieurs kilomètres les informant de la nature du danger sur la route. Les conducteurs pourront alors adapter leur conduite à l'événement détecté. L'alerte est mémorisée dans le réseau tant qu'elle existe. Les nouveaux véhicules entrant sur la route devront être informés des perturbations existant sur la route.

1.1.1.3.3 Les différents types de messages

Les entités membres des réseaux sans fil véhiculaires vont générer et s'envoyer des messages. Dans ces échanges, différents types de messages vont être identifiés en fonction de l'environnement et des types d'applications utilisées. Nous pourrons discerner les types suivants : message de contrôle, message de sécurité et les autres types de message.

1.1.1.3.3.1 Message de contrôle

Les messages de contrôle sont envoyés à intervalles réguliers, par convention. Chaque véhicule émet un message de contrôle toutes les 100 ms. Dans la littérature, ces messages sont aussi appelés message « *beacon* ». Ils contiennent des informations personnelles sur les véhicules telles que : sa vitesse, sa position GPS, sa direction, etc. Les messages de contrôle permettent à chaque véhicule d'avoir une vision locale de son entourage. Grâce à ce type de message, les véhicules se font connaitre de leur entourage.

1.1.1.3.3.2 Message de sécurité

Le message de sécurité est généré lorsqu'un événement qui mérite l'attention du conducteur est détecté. Ces messages sont générés dans le cas d'un accident, de congestion, d'un obstacle sur la route, etc. Lorsqu'un message d'alerte est émis, il doit être retransmis à intervalle régulier pour assurer que l'alerte est toujours valide. De plus, ces messages doivent être de taille réduite pour pouvoir être retransmis rapidement dans le réseau. Les messages contiennent les informations des coordonnées du lieu de l'accident et les paramètres sur sa zone de retransmission.

1.1.1.3.3.3 Autres messages

Les autres types de messages sont tous les messages qui ne sont pas des messages de contrôle ou des messages de sécurité. Il peut s'agir des messages d'une application, de l'envoi de courriel, etc. Ces messages ne sont émis qu'une fois.

1.1.2 CARACTÉRISTIQUES

1.1.2.1 Environnements de déploiement

Les réseaux véhiculaires sans fil se distinguent principalement par plusieurs milieux de déploiement. Ces milieux se différencient par leur localisation (urbain, autoroutier, etc.), mais également par des voies terrestres (route, autoroute, chemin, etc.). Les VANETs sont exclusivement destinés aux zones urbaines et autoroutières.

1.1.2.1.1 Milieu urbain

Le milieu urbain est défini par des intersections, des points d'arrêts (« *Stop* », feu tricolore, « cédez le passage », etc.) ; mais également par une vitesse réduite (jusqu'à un maximum de 50km/h en ville) [28]. De plus, l'environnement est fortement perturbé par les ondes et la présence des matériaux des différents bâtiments [25]. Les milieux urbains ont un modèle de mobilité relativement complexe dû à la vitesse réduite et à leur forte densité de véhicule. L'installation des infrastructures routières en milieu urbain reste un problème complexe (exemple : manque de place). Les communications véhicule à véhicule sont également réalisables dans ce milieu et présentent l'avantage d'éviter le déploiement de RSU.

1.1.2.1.2 Milieu autoroutier

Le milieu autoroutier est défini par de longues routes avec des points d'entrées (voie d'accélération), des points de sorties (voie de décélération) et une vitesse importante (jusqu'à 100 km/h au Canada) [28]. On retrouve aussi une forte densité de véhicules et poids lourds en fonction des horaires. Sur autoroutes ce sont les poids lourds qui posent problème. Comme les bâtiments dans le milieu urbain, ils sont massifs, ils gênent la visibilité des automobilistes et empêchent la découverte des nouveaux véhicules dans le réseau. Les protocoles de découverte de véhicules environnants [18] et les applications de sécurité routière permettent de mieux appréhender le milieu autoroutier.

1.1.2.2 Environnement du véhicule

Bien que les MANETs et les VANETs se ressemblent, les réseaux VANETs possèdent des caractéristiques propres et bien différentes. Les caractéristiques et contraintes techniques sont présentées ci-dessous.

1.1.2.2.1 Énergie

Contrairement aux réseaux MANET dans lesquels l'énergie est l'une des contraintes principales, due à la taille finie des batteries ; les réseaux VANETs ne souffrent pas de ce problème. Ils disposent d'une source énergétique importante grâce au système d'alimentation véhiculaire, qui se renouvelle dans le temps.

1.1.2.2.2 Mobilité

Les réseaux MANET se distinguent par une faible mobilité. Les nœuds se déplacent lentement et la portée des ondes est comparable au réseau sans fil classique (exemple: WiFi domestique). Du fait d'une faible vélocité, la topologie est intrinsèquement faible. Il y a peu d'entrées/sorties de nœuds dans le temps, ce qui permet d'évaluer plus facilement le nombre de nœuds présents à l'instant t. En opposition avec les réseaux VANETs, la mobilité est extrêmement élevée. La vélocité est très importante. Les nœuds

peuvent se déplacer jusqu'à 130 km/h et le nombre d'entrées/sorties dans le réseau est élevé. D'après [25], les liens sur autoroute entre les membres du VANET sont de 50 secondes si les véhicules sont dans la même direction, sinon ils sont inférieurs à 5 secondes. Les infrastructures routières offrent un support pour les caractéristiques des VANETs. Elles relayent les informations sur de longues distances (exemple: les informations de sécurité routière) et permettent de joindre en tout temps un véhicule sur la route.

1.1.2.2.3 Topologie dynamique

Due à la vitesse de circulation des véhicules, la topologie des VANETs est instable. L'échange de données peut se faire entre véhicules allant dans la même direction, mais également en directions opposées. La connectivité dépendamment de la vitesse de chacun des véhicules peut ne durer qu'un instant. On estime le temps de connexion pour deux véhicules allant en directions opposées et roulant à 25 m/s à 10 secondes [33]. La réorganisation de la topologie du réseau est fréquente.

1.1.2.2.4 Connectivité

En raison de la forte topologie dynamique des VANETs, la connectivité sera de courte durée notamment en cas de faible densité des véhicules. Les réseaux VANETs tentent d'améliorer la connectivité en tous points du réseau avec les RSUs, ceux-ci permettant de retransmettre l'information sur de longues distances [33].

1.1.2.2.5 Géolocalisation

Les systèmes de localisation par satellite comme les GPS (*Global Positioning System*) sont utilisés dans les réseaux VANETs afin de localiser et de faciliter la communication entre les différentes entités du réseau.

1.1.2.2.6 Environnement de communication

Dans les réseaux VANETs, la communication se fait soit dans un environnement urbain soit dans un environnement autoroutier. On peut passer de l'un à l'autre en un instant. Ces deux environnements présentent toutefois des caractéristiques radicalement différentes. Les contraintes topologiques et la prévision des conditions météorologiques sont à prévoir et conduisent à des modèles de propagation d'ondes complexes [25].

1.1.2.2 Technologie de communication

Le déploiement d'applications nécessite des technologies de communication sans fil. Nous allons détailler celle existante et présenter leurs caractéristiques et leurs intérêts pour les réseaux VANETs. Il en existe deux systèmes [25] :

- Les réseaux VANETs requièrent une communication intravéhiculaire. Elle est composée des capteurs internes au véhicule qui regroupent et communique l'information à l'interne et ne vise pas à diffuser d'information vers l'extérieur du véhicule.
- Les systèmes extravéhiculaires qui visent à échanger des données entre l'entité et son environnement. On retrouve plusieurs sous-catégories à ces systèmes:
    - Les systèmes de radiodiffusion, qui permettent la réception de l'information de manière unidirectionnelle. Ils sont très utilisés par les applications de gestion du trafic routier.
    - Le système de communication informatique pour les réseaux VANETs, qui permet d'échanger des informations au sein du réseau. On utilise ce système pour les communications véhicules à véhicules (V2V) et véhicules à infrastructure (V2I).

1.1.2.2.1 Les systèmes intravéhiculaires

Les systèmes intravéhiculaires sont des systèmes qui ne diffusent aucune information à l'extérieur du véhicule, néanmoins ceux-ci partagent l'information à l'interne du

véhicule. Ils sont généralement composés de capteurs, d'unités de calcul (microprocesseur) et de réseaux filaires ou non filaires. On distinguera pour les véhicules intelligents les familles suivantes :

1.1.2.2.2 Les capteurs propriorecepteurs

Les capteurs proprioceptifs sont chargés de fournir des informations internes au véhicule. Ils transmettent des informations sur le comportement et sur les paramètres du véhicule en faisant abstraction de l'environnement de conduite. Ces capteurs fournissent toutefois des informations précieuses en termes de définition et de détermination du risque (exemple : informations sur l'état des plaquettes de frein, état du moteur, révisions à prévoir, etc.). Ces informations sont indispensables pour connaître l'état et les capacités du véhicule, pour mieux définir les risques encourus, mais également pour proposer une solution permettant de réduire le risque.

1.1.2.2.3 Les capteurs extéroceptifs

Les capteurs extéroceptifs sont embarqués sur le véhicule afin de percevoir l'environnement de navigation du véhicule. Ils fournissent des informations sur le véhicule lui-même et sur les objets qui l'entourent à partir de leur perception de l'environnement.

Dans les réseaux VANETs, ces capteurs ont un rôle passif, mais prodiguent une source importante d'informations (exemple : thermomètre extérieur, taux d'humidité dans l'air externe, état de la route, etc.). Il est intéressant de coupler aux systèmes de communication extravéhiculaire ces capteurs pour assurer la sérénité et la pérennité des usagers du réseau.

1.1.2.2.4 Les systèmes extravéhiculaires

Parmi les systèmes extravéhiculaires, on distingue trois catégories :

1.1.2.2.4.1 Les systèmes de télécommunication

Ces systèmes sont liés aux applications de confort. Parmi ceux-ci on regroupe les systèmes de télécommunication mobile, tels le GSM (*Global System for Mobile communications*), l'UMTS (*Universal Mobile Telecommunication System*) et le LTE (*Long Term Evolution*). Ces normes permettent l'utilisation de la voix, d'un point d'accès Internet et des vidéoconférences depuis les VANETs. Néanmoins, durant l'utilisation de ces communications, la qualité de service dépend de l'opérateur utilisé. Il n'y a pour le moment aucune garantie.

1.1.2.2.4.2 Les systèmes de radiodiffusion numérique

Les systèmes de radiodiffusion numériques proposent la diffusion d'informations depuis une station de base jusqu'aux utilisateurs. La communication se fait de manière unidirectionnelle. Ces systèmes sont notamment utilisés pour la gestion du trafic routier. Chaque utilisateur reçoit alors la même information au même instant t dans le réseau. L'utilisation à grande échelle est déjà faite, par la norme européenne RDS/TMC (*Radio Data System/Traffic Message Channel*), qui diffuse des données numériques afin d'alerter les usagers des routes et autoroutes. L'utilisation et le principe de fonctionnement de ces systèmes peuvent être utilisés et adaptés aux réseaux VANETs dans les communications infrastructure à véhicule (V2I).

1.1.2.2.4.3 Les réseaux informatiques extravéhiculaires

Les systèmes informatiques extravéhiculaires permettent l'échange d'informations au sein du réseau. Les réseaux VANETs peuvent utiliser les technologies décrites ci-dessous :

- **WPAN (*Wireless Personal Area Network*) :** Les réseaux personnels sans fil (appelés également réseaux individuels ou réseaux domestiques sans fil) sont des réseaux de faible portée, de l'ordre d'une dizaine de mètres. Ils servent à établir

des liaisons sans fil entre des équipements peu distants ou à relier des périphériques comme des imprimantes, des PDA, etc. La norme 802.15.1 aussi appelée Bluetooth est utilisée pour ces technologies. Elles sont peu gourmandes en énergie et offrent un débit théorique allant jusqu'à 1Mbit/s. Néanmoins l'échange de données peut être facilement perturbé par des obstacles.

- **WLAN (*Wireless Local Area Network*) :** Les réseaux locaux sans fil (WLAN) font le pont entre le monde de la téléphonie et le monde informatique. Ils utilisent les normes 802.11 avec l'étiquette WiFi [31]. La dernière norme mise en place permet un débit théorique jusqu'à 300Mbit/s (IEEE 802.11n) sur plus de 100 mètres [29]. Parmi les autres nombreux avantages que présentent les WLAN, ceux-ci permettent:
    - De rendre mobiles les équipements informatiques.
    - De rendre compatibles les applications informatiques actuelles avec les débits.
    - L'utilisation des bandes de fréquences libres de droits.
    - L'utilisation de peu, ou pas d'infrastructures.

- **WMAN (*Wireless Metropolitan Area Network*) :** Les réseaux métropolitains sans fil (WMAN), connus également sous le nom WiMAX sont basés sur la norme 802.16e. Ils offrent un débit de l'ordre de 70 Mbit/s pour une portée théorique allant jusqu'à 50 kilomètres. Ces réseaux peuvent fournir un point d'accès Internet aux VANETs. Néanmoins, le principal problème réside dans les délais importants lors des communications véhicule à véhicule (V2V).

- **WWAN (*Wireless Wide Area Network*) :** Les réseaux sans fil étendus (WWAN) regroupent plusieurs types de réseaux, notamment les réseaux cellulaires et les réseaux satellitaires. Parmi les réseaux cellulaires, on retrouve l'utilisation des technologies comme le GSM (*Global System for Mobile*), le GPRS (*General*

Packet Radio Service) et EDGE, l'UMTS (*Universal Mobile Telecommunications*) et LTE (*Long Term Evolution*); tandis que les réseaux satellitaires s'appuient sur des normes comme DVB-S (*Digital Video Broadcasting Satellite*) proposant des débits plus élevés pour, par exemple, des retransmissions numériques en haute définition.

1.2 DÉVELOPPEMENT DES STANDARDS DE COMMUNICATION POUR LES RÉSEAUX SANS FIL VÉHICULAIRES

Pour subvenir aux besoins en communication des réseaux véhiculaires sans fil, l'IEEE a étendu les protocoles 802.11 avec le protocole 802.11p [4,34]. De plus, l'ASTM (*American Society for Testing and Materials*) [32] a défini un nouveau standard, DSRC (*Dedicated Short Range Communication*) basé sur le 802.11a [35]. Le DSRC a été étudié pour répondre aux exigences des réseaux VANETs, en modifiant la couche MAC et la couche physique. En complément, l'IEEE a défini la gamme de protocoles 1609, ceux-ci appelé également WAVE (*Wireless Access in Vehicular Environments*) permettent l'accès à la technologie sans fil à bord des véhicules. Le standard WAVE a été dérivé en quatre standards (de 1609.1 à 1609.4). Ils définissent pour chacun une couche réseau spécifique, dans l'ordre: l'architecture, le modèle de communication, la structure de gestion, la sureté et l'accès physique. La figure 2 présente la pile protocolaire complète pour les standards 802.11p et WAVE. WAVE utilise en sus deux piles protocolaires ; la première dédiée aux applications de sécurité routière et l'autre spécifique à tous les autres types d'applications [25].

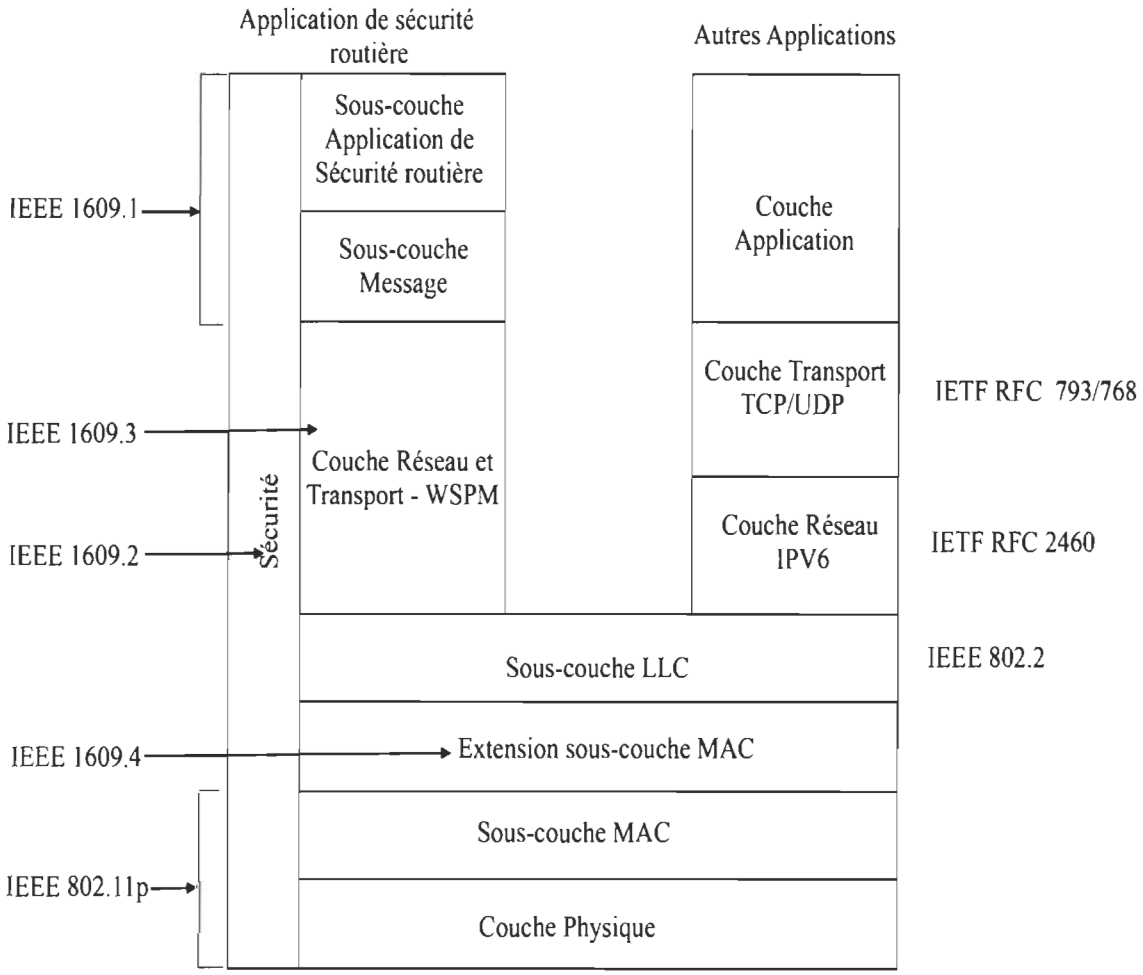


Figure 2 : Le modèle DSRC/WAVE [25]

1.2.1 DSRC

Le standard DSRC (Dedicated Short Range Communication) regroupe initialement des technologies dédiées aux communications pour les réseaux VANETs. À l'origine, ce modèle de communication était pour les faibles portées (entre 4 et 10 mètres) et avait des débits inférieurs à 1 Mbit/s. L'IEEE a ensuite fait évoluer ce standard en l'adaptant au 802.11a [35], redéfinissant un nouveau standard, le 802.11p, appelé aussi WAVE [36].

Ceux-ci répondent spécifiquement aux besoins des réseaux VANETs: faible temps d'établissement de connexion, adaptation à la forte mobilité, portée maximale de 1000 mètres, adaptation à une vélocité théorique jusqu'à 160 km/h, débit maximal de 54 Mbit/s, etc. [25].

Le DSRC utilise un spectre électromagnétique dans la bande des 5.9 GHz. La bande du canal de communication est segmentée en sept canaux de 10 MHz chacun [35]. Parmi les canaux on retrouve, un canal de contrôle réservé à la transmission des messages de gestion et de sécurité routière dans le réseau et six canaux de service destiné aux transmissions de données des services annoncés sur le canal de contrôle [37].

La figure 3 présente un exemple d'architecture réseau utilisant DSRC et une infrastructure (exemple : RSU) pour joindre d'autres types réseau.

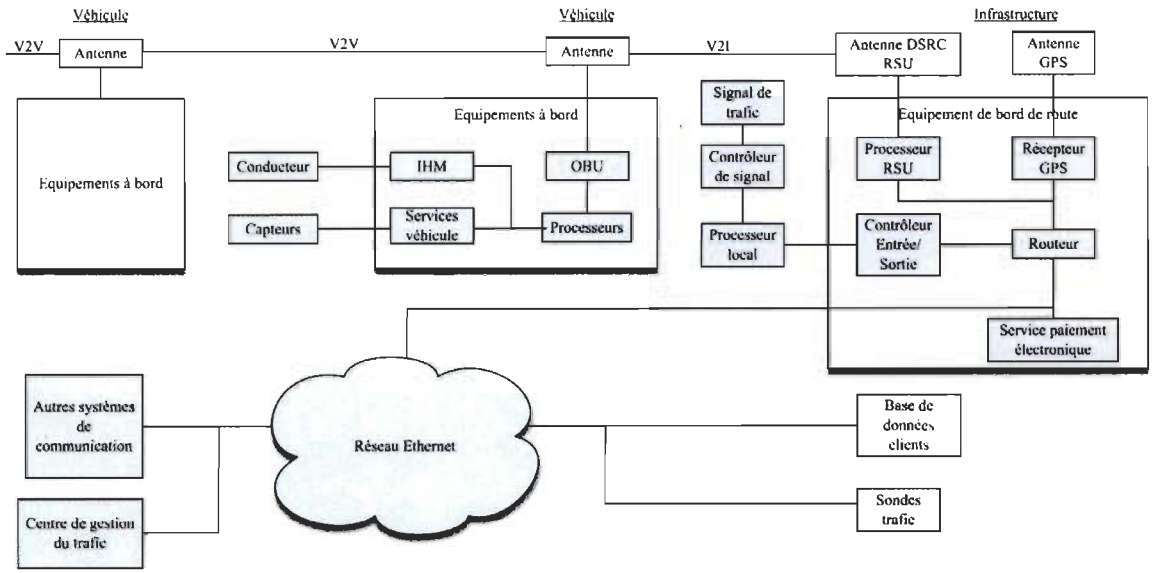


Figure 3 : Exemple d'architecture réseau de DSRC [25]

1.2.2 IEEE 802.11p

Le standard 802.11p est dérivé de la couche physique du standard 802.11a pour s'adapter aux caractéristiques de DSRC. De plus, afin de répondre aux exigences des systèmes de transport intelligent et assurer des communications viables, le 802.11p utilise une approche multicanal. Le standard ayant de fortes exigences en terme de portée (jusqu'à 1000 mètres), n'offre qu'un débit compris entre 6 et 27 Mbit/s. Sa couche MAC utilise des principes existants tels que le CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*) ou le EDCA (*Enhanced Distributed Channel Access*) pour améliorer la qualité de service et gérer efficacement les priorités des canaux de communication [39]. La figure 3 présente les différents canaux de communication du standard 802.11p.

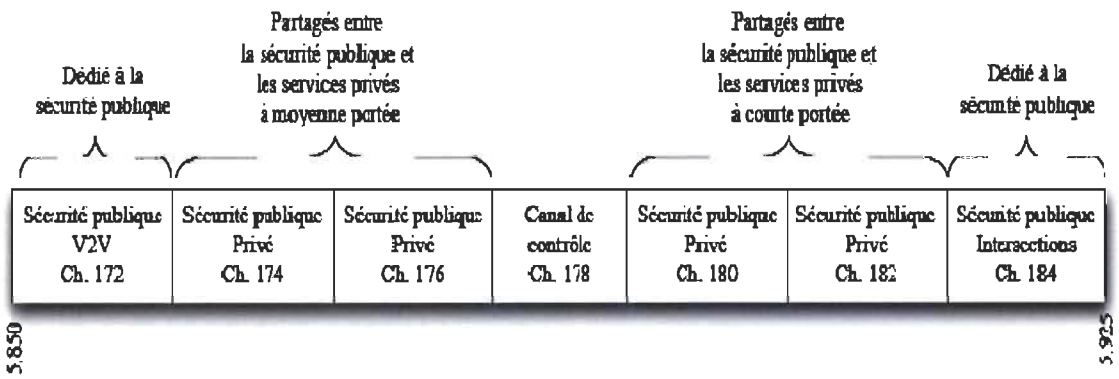


Figure 4 : Les différents canaux du standard IEEE 802.11p [25]

1.2.3 La famille des standards IEEE 1609

La norme IEEE 1609 regroupe 4 standards définis pour les réseaux sans fil véhiculaires. Ci-dessous nous détaillons leurs objectifs et leurs caractéristiques techniques.

1.2.3.1 IEEE 1609.1

Le standard IEEE 1609.1 définit un gestionnaire de ressources permettant la communication entre le mode ad hoc et le mode infrastructure [25, 38], mais également entre l'équipement de bord de route (RSU) et les OBUs des véhicules. Le standard définit aussi le niveau de la couche application, les formats des messages et le mode de stockage des données. Enfin, celui-ci détaille le fonctionnement de trois éléments de la couche application qui seront inclus dans les OBUs [25]. Parmi ceux-ci on retrouve :

- *Le Resource Manager* (RM) : le gestionnaire des ressources, il relaie le message du RMA vers le RCP et il gère les services permettant le contrôle des interfaces présentes dans l'OBU.
- *Le Resource Manager Applications* (RMA) : il s'agit de l'entité distante qui utilise le RM pour communiquer avec le RCP.
- *Le Resource Command Processor* (RCP) : il exécute les commandes données par le RMA et fournit une réponse au RMA via le RM.

La figure 5 présente les modules et le fonctionnement du standard IEEE 1609.1.

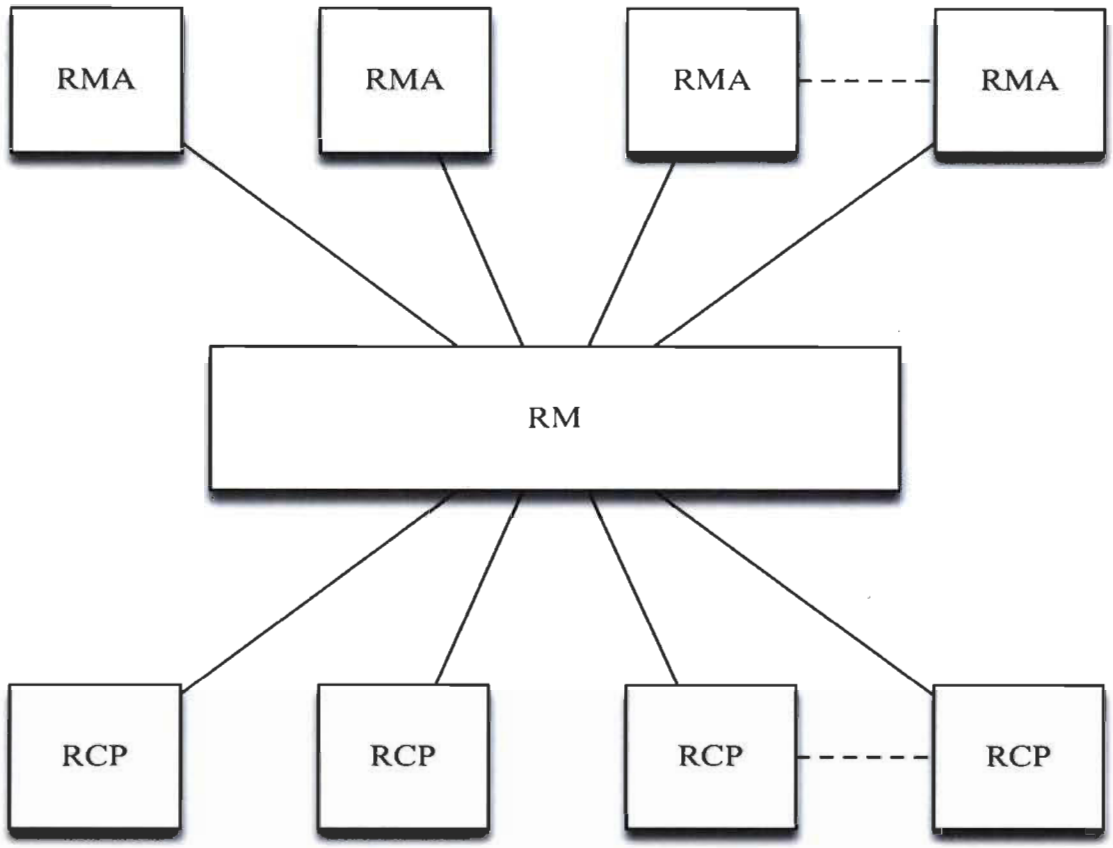


Figure 5 : Module du standard IEEE 1609.1 [25]

1.2.3.2 IEEE 1609.2

Le standard 1609.2 définit le format des messages sécurisés pour le système DRSC/WAVE. Il spécifie les algorithmes pour sécuriser les messages de gestion et d'application. Il décrit également les procédures pour assurer à chaque véhicule les services tels que l'authenticité, la confidentialité, l'intégrité et la non-répudiation des données. Toutes les applications ne requièrent pas ces services. Néanmoins, ils doivent être présents en cas de nécessité. Le standard 1609.2 protège les entités du réseau contre les attaques, telles que l'homme du milieu, l'usurpation d'identité, le rejeu de message, etc. [25, 38].

1.2.3.3 IEEE 1609.3

Le standard IEEE 1609.3 gère les services d'adressage et de routage dans le réseau [25]. Il définit le « *WAVE Short Message* » (WSM) et le protocole d'échange « *WAVE Short Message Protocol* » (WSMP). Ceux-ci assurent les fonctionnalités des couches réseau et transports pour les applications de sécurités routières. Due à sa faible latence, l'utilisation du WSMP est faite par les applications de sécurité [25, 38]. Le standard définit également le « *WAVE Service Advertisement* » (WSA), qui annonce la disponibilité des services DSRC à une localisation donnée. Ces services permettent le contrôle de la puissance de transmission, du canal, du débit, mais également l'annonce de ces caractéristiques techniques.

1.2.3.4 IEEE 1609.4

Le standard 1609.4 définit l'organisation, l'ordonnancement et l'utilisation des différents canaux de DSRC [25]. Son objectif est de fournir des mécanismes permettant à plusieurs équipements de s'accorder sur un même canal pour communiquer. Les mécanismes du standard 1609.4 sont très similaires aux mécanismes du mode EDCA (*Enhanced Distributed Channel Access*) agissant sur la sous-couche MAC (*Medium Access Control*).

1.3 LA SÉCURITÉ DANS LES RÉSEAUX VANETS

L'objectif des réseaux sans fil véhiculaires est d'améliorer le trafic routier, d'assurer la sécurité routière et de rendre plus confortable le trajet de ses utilisateurs grâce aux applications de gestion du trafic routier, de sécurité routière ou de confort. Néanmoins, sans les mesures de sécurité adéquates dans le réseau, les informations des applications

peuvent ne jamais arriver à destination, ou possiblement devenir des menaces et devenir la cause d'accident. Il est donc important de créer des mécanismes de sécurité pour assurer une utilisation optimale des réseaux VANETs pour les utilisateurs.
Dans cette section, on présente dans un premier temps les différents types d'attaquants, les attaques possibles dans les réseaux VANETs et les systèmes de détection d'intrusion avec leurs adaptations.

1.3.1 LES TYPES D'ATTAQUANTS

Avant de détailler les attaques, il est important d'identifier les types d'attaquants, leurs motivations et leurs objectifs. Dans [40], les auteurs classent les attaquants suivant les trois critères suivants :

- **Attaque interne vs attaque externe :** L'attaque interne provient d'une des entités du réseau. L'attaquant est dans le réseau, possède les mêmes privilèges et les mêmes caractéristiques que les autres entités du réseau. Il agit généralement dans le but de nuire aux utilisateurs du réseau. A contrario, l'attaquant externe est un intrus dans le réseau et est considéré comme tel par tous les nœuds de ce réseau. Généralement l'attaquant externe est plus limité quant à la diversité des attaques que l'attaquant interne.

- **Attaquant malveillant vs attaquant rationnel :** L'objectif de l'attaquant malveillant est de prouver une prouesse personnelle en détectant les faiblesses du réseau afin d'exploiter celle-ci. Ne ciblant aucune structure en particulier et n'étant pas forcement conscient des répercussions de ses actes, il peut s'avérer dangereux, mais il reste facilement identifiable. A contrario, l'attaquant rationnel est un professionnel. Ses attaques ciblent des points précis du réseau dans un objectif précis. Son identification peut s'avérer très difficile.

- **Attaquant actif vs attaquant passif :** un attaquant actif est un attaquant qui lors de l'attaque agit sur le réseau, par exemple en interceptant des messages et en les modifiant, les rejouant, les détruisant, etc. De nombreuses attaques identifiées dans les réseaux VANETs proposent des méthodes coopératives actives afin de rendre celle-ci plus facilement réalisable ou d'en augmenter l'impact. L'attaquant passif quant à lui écoute les messages du réseau et attend une information utile pour poursuivre son attaque.

1.3.2 Les attaques dans les réseaux VANETs

Les réseaux VANETs, comme tous les réseaux informatiques sont faillibles. C'est-à-dire, qu'il est possible grâce aux protocoles et à la technologie mise en place de monter une attaque pour modifier le comportement normal du réseau.

- **Attaque sur la cohérence de l'information (*Bogus information*) :** Cette attaque vise à injecter de fausses informations dans le réseau pour modifier le comportement des autres entités. Cette attaque peut modifier l'itinéraire d'un véhicule ou même changer la topologie du réseau.

- **Attaque sur la vie privée (*tracking*) :** l'objectif de cette attaque est d'identifier un nœud du réseau et de récupérer le maximum d'information sur celui-ci. Avec suffisamment d'informations sur celui-ci, on peut usurper son identité, accéder à ses données personnelles, etc. De nombreux articles [26, 20] mettent l'emphase sur la sécurité des véhicules, notamment sur leur non-traçabilité.

- **Usurpation d'identité ou de rôle (*Spoofing*) :** dans ce genre d'attaque, l'attaquant tente de se faire passer pour une entité du réseau qu'il n'est pas. Par exemple, il se fait passer pour une passerelle. En se déclarant aux nœuds du

réseau comme passerelle, tous les nœuds vont transmettre à l'attaquant toutes les informations échangées par les membres du réseau.

- **Déni de service (*Deny of Services*, DoS) :** voici l'attaque la plus simple à mettre en place. L'attaquant vise ici à empêcher toute communication entre les membres du réseau. Avec les réseaux VANETs, cette attaque peut se matérialiser par un brouilleur, entravant la propagation des ondes; mais aussi par un trop grand nombre de connexions à une entité, empêchant les autres nœuds d'accéder à celle-ci et à ses ressources.

- **Écoute de communication :** Cette attaque combine les concepts de « *spoofing* » et de « *tracking* », l'attaquant cible un véhicule sachant par exemple que celui-ci va effectuer un paiement et se met à l'écoute de ses communications en vue d'extraire un mot de passe.

- **Véhicule caché :** Cette attaque est la combinaison de plusieurs types d'attaque. Elle utilise le concept de nœud Sybille. L'attaquant génère de fausses identités de véhicules sur la route, ainsi que de fausse information de localisation de manière à être dans une position avantageuse. Son objectif est de s'octroyer de manière légitime des droits, en faisant penser aux vrais véhicules que sa localisation est la meilleure. L'attaquant peut alors émettre des alertes, prendre la tête d'un cluster, générer de fausse congestion, etc.

- ***Wormhole* :** Cette attaque suppose que l'attaque contrôle une autre entité plus loin dans le réseau ou qu'elle est effectuée de manière coopérative. L'objectif de l'attaquant est de modifier le routage et la topologie du réseau à grande échelle. Les deux entités attaquantes créent un tunnel entres-elles et laissent pensée aux autres nœuds que le routage est plus rapide par elles. Les entités perturbent le

routage et récupèrent les informations des nœuds. C'est une forme de « *spoofing* ».

1.4 LES SYSTÈMES DE DÉTECTION D'INTRUSIONS

Les systèmes de détection d'intrusion (IDS), sont des systèmes qui permettent de déceler des attaques de quelques natures que ce soient dans le réseau. Les IDS utilisent différents mécanismes tels que les signatures ou la recherche de motif pour arriver à leur fin. Nous présentons ici le fonctionnement classique de ces systèmes, ainsi que les mécanismes adaptés aux réseaux VANETs.

1.4.1 IDS BASÉ SUR UN SCÉNARIO

Les IDS basés sur les scénarios sont des IDS avec pour base de connaissance des signatures d'attaque connues. Grâce à sa base de données, ce type de système détecte facilement et rapidement les attaques et menaces présentes dans un flux réseau ou sur une machine. Il présente néanmoins des limites. Si l'attaque n'est pas connue (exemple : faille *0day*), le système ne détecte rien. Des mises à jour fréquentes doivent être faites sur ces systèmes pour qu'ils restent performants.

1.4.2 IDS BASÉ SUR L'APPROCHE COMPORTEMENTALE

Les IDS basés sur un bon comportement sont, a contrario des IDS basé signature, des systèmes de détection d'intrusions sans base de connaissance. Il requiert cependant un entrainement fait à partir du comportement normal d'un trafic réseau. Ces IDS utilisent

des méthodes de calcul probabiliste qui, associées à des méthodes de classifications de données, permettent de déterminer qu'une attaque a lieu ou non à partir d'un flux réseau. Ces systèmes ne requièrent aucune mise à jour et sont capables de détecter de nouvelles attaques (même les failles *0day*). Ils génèrent en revanche de nombreuses fausses alarmes (détection d'une attaque alors qu'il n'y en a pas), causées par une utilisation peu fréquente ou nouvelle d'un protocole, d'une requête, etc.

1.4.3 IDS BASÉ VÉHICULE DANS LES RÉSEAUX VANETs

Dans les réseaux VANETs, plusieurs méthodes ont été proposées pour positionner les IDS. Parmi celles-ci, l'IDS basé véhicule, ou chaque véhicule du réseau VANET serait équipé d'un de ces systèmes pour détecter les attaques dont il pourrait être la cible. Néanmoins ces systèmes, pour être performant requièrent des processeurs performants, ce qui pourrait ralentir certaines applications à bord du véhicule.

1.4.4 IDS BASÉ INFRASTRUCTURE DANS VANETs

Les IDS basés sur l'infrastructure sont quant à eux installés sur le RSU. Chacun des véhicules du réseau devient un nœud et retransmet toutes ses données reçues au RSU pour les faire analyser. Le RSU analyse toutes les données en vue d'une attaque. La décentralisation de l'IDS à l'avantage de ne pas ralentir les applications présentes sur les véhicules. De plus, le RSU peut facilement accueillir une grande capacité de calcul. Néanmoins, le trafic réseau généré sera plus important entre les véhicules et le RSU.

1.5 LA CLUSTERISATION

La clusterisation, est dans les réseaux informatiques classiques, un concept visant à regrouper des entités (ordinateur), appelée également nœud, entre eux. L'objectif étant la répartition du calcul sur plusieurs processeurs, le partage de données sur des disques durs communs, etc. Dans les réseaux VANETs, le concept de regroupement est le même : on rassemble des véhicules (nœuds) entre eux. Néanmoins, les objectifs diffèrent. La topologie dynamique des VANETs, permet, après la clusterisation d'améliorer la qualité des services proposés, mais également la sécurité des véhicules [54, 55, 56]. Il existe dans les VANETs deux types de clusterisation, passive, ou active, nous allons les détailler par la suite.

1.5.1 CLUSTERISATION ACTIVE

La clusterisation active est un type de clusterisation dans lequel chaque nouveau véhicule détecté dans le réseau doit immédiatement se clustériser. Les clusters et la tête de cluster sont ainsi reformés régulièrement, dépendamment des nœuds entrants et sortants.

1.5.2 CLUSTERISATION PASSIVE

La clusterisation passive quant à elle, est un type de clusterisation dans laquelle les véhicules ne se clustérisent pas immédiatement. Le processus n'est amorcé que lorsqu'un véhicule souhaite diffuser de l'information. Les véhicules présents dans la zone vont alors élire une tête de cluster pour retransmettre les informations dans le réseau.

1.6 CONCLUSION

Nous avons décrit dans la première partie de ce mémoire, ce que sont les réseaux véhiculaires sans fil, leurs architectures et leurs caractéristiques, ainsi que les attaques auxquelles ils sont confrontés. Des solutions pour améliorer la sécurité ont été abordées, telles que les méthodes de clusterisation, regroupant de manières stratégiques les véhicules et les systèmes de détection d'intrusions pour détecter les attaques dans le réseau. Dans le chapitre suivant, nous allons analyser et présenter les travaux de recherches liés à la clusterisation, à la sécurité, aux méthodes d'attaques et aux méthodes de détection d'intrusions dans les réseaux VANETs.

CHAPITRE II - ÉTAT DE L'ART

Dans la première partie, nous avons présenté les réseaux VANETs de manière générale, leurs caractéristiques, leurs architectures, ainsi que les attaques auxquelles ils sont confrontés. Considérant que les réseaux VANETs sont vulnérables et ouverts aux attaques externes dues à la technologie sans fil [48] [40], celle-ci rend l'implémentation de la sécurité et de ses polices difficiles. L'étude et la définition de nouveaux types d'attaques et la mise en place de nouvelles techniques pour les contrer sont des axes de recherche ouverts et en plein essor. On retrouve dans la littérature plusieurs recherches qui visent à intégrer des systèmes de détections d'intrusions (IDS) pour sécuriser les réseaux VANETs, mais un grand nombre de problèmes de sécurité récurrents [1] (*Spoofing*, *Deny of Services*, *Jamming*, *Packet forgery*, etc.) n'ont pas de solutions à ce jour. Dans cette seconde partie, nous allons analyser et exposer les recherches, les problématiques et les travaux liés aux méthodes d'attaques, de sécurité, de détection d'intrusions et de clusterisation dans les réseaux VANETs.

1.1 ATTAQUES DANS LES RÉSEAUX VANETS

Notre étude porte sur plusieurs des problèmes intrinsèques précités. Dans [1], les auteurs présentent une liste des attaques sur les réseaux VANETs. Ils ont proposé une méthode pour contrer les attaques de « création de paquets » en utilisant un mécanisme de corrélation des données et l'utilisation de plusieurs émetteurs-récepteurs opérants sur des bandes de fréquences disjointes afin de contrer les attaques de type DoS (Déni de Service) comme le brouillage. Une autre solution au problème du brouillage radio est proposée dans [51]. L'objectif de l'attaquant étant de dégrader la qualité de service et la qualité des communications du réseau VANET. Les auteurs ont proposé un modèle de détection basé sur la corrélation entre l'erreur et le temps de réception des données. La

méthode permet une détection efficace de l'attaque, néanmoins, aucune solution n'est encore proposée pour réduire l'effet du brouillage.

Dans les réseaux VANETs, il existe d'autres attaques qui nuisent à la qualité de service, mais également au routage. Ce type d'attaques appelé « Sybille » permet la génération de nœuds multiples sur la route. Ces nœuds sont détectés par les autres usagers comme étant des véhicules et interagissent de manière légitime dans le réseau. Les auteurs dans [3] ont présenté une méthode pour détecter les attaques Sybilles de manière coopérative. Chaque véhicule diffuse périodiquement ces informations de positions géographiques. Chaque véhicule mémorise la position de ses voisins les plus proches. Lorsqu'un véhicule est dans le réseau et qu'aucun véhicule ne connait sa position, alors on conclut qu'il s'agit d'une attaque. Le protocole détecte les incohérences et les catégorise comme nœud Sybille. Dans [53], les auteurs quantifient les effets et l'efficacité des attaques Sybilles en fonction du type d'antenne utilisé et de la puissance de transmission du signal. L'étude montre que l'utilisation d'une antenne bidirectionnelle augmente les chances de détecter l'attaque. Comparer les différentes méthodes de détection d'attaque Sybille avec ce type d'antenne permettrait de voir laquelle est la plus efficace. Dans [5], les auteurs présentent différents types d'attaques basées sur la création de multiples identités sur la route, générant de multiples faux véhicules. Il présente également une méthode pour détecter l'attaque : les RSUs vont calculer la vitesse des véhicules en fonction des messages « *Beacon* » envoyés périodiquement. Lorsqu'un RSU remarque une anomalie dans la vitesse, la position fournie ou dans les paquets, il considère qu'il s'agit d'un faux véhicule. Les auteurs dans [52] font la preuve d'une nouvelle attaque dite « Illusoire ». Dans celle-ci, l'attaquant diffuse des messages d'avertissement de trafic routier pour produire l'illusion qu'il y a des véhicules dans son voisinage. L'article démontre que les mécanismes d'authentifications traditionnelles ne sont pas suffisants et propose un modèle de plausibilité pour empêcher l'attaque. Les auteurs dans [4] proposent de détecter les fausses congestions dues aux attaques Sybilles. Ils utilisent un modèle de plausibilité permettant de vérifier les mouvements des véhicules. Le modèle permet la détection de faux véhicule même lorsque les mouvements des faux véhicules

sont plausibles. Les modèles mis en place pour détecter et contrer ces attaques sont complexes, quand est-il de la complexité pour mettre en place l'attaque ? L'article [45] présente une méthode probabiliste pour évaluer les risques d'une attaque dans les réseaux VANETs. L'approche permet d'identifier les scénarios des menaces en temps réel dans les réseaux, ce qui permet d'améliorer la sécurité du système. La définition d'un poids probabiliste en fonction de chaque attaque est aussi complexe que le problème des seuils. De plus on ne connait pas la réaction de la méthode face à une attaque non connue. Comment sera-t-elle capable d'en évaluer le risque ? L'utilisation de cette méthode mathématique couplée avec une méthode de détection pour les IDS serait un bon sujet d'étude. Permettre la détection de ce genre d'attaque est une bonne chose, mais doit-on intégrer l'approche à un IDS ou ce mécanisme doit-il être intégré indépendamment ?

1.2 MÉTHODE DE DÉTECTION ET IDS DANS LES RÉSEAUX VANETS.

Comme nous l'avons vu précédemment de nombreuses attaques sont possibles dans les réseaux VANETs. Les IDS détectent les attaques dans le réseau. Néanmoins, due à la topologie des VANETs, la question que nous nous posons est, quelles sont les conditions optimales de détection? Les études suivantes présentes des méthodes d'IDS, certaines sont basées sur différents contextes pour en valider l'efficacité et la faisabilité. Les auteurs dans [6] définissent un IDS basé sur les têtes de cluster, ceux-ci formant un bus de nœuds. Les bus de nœuds sont les intermédiaires entre le cluster et le RSU. Les informations sont transmises au RSU et celui-ci a alors une vision globale du réseau VANET et peut alors détecter les anomalies avec les données analysées. Dans [7], on propose une technique de « *Watchdog* » basée sur le niveau de confiance des voisins. L'IDS définit la confiance en récupérant tous les paquets reçus et en calculant le ratio entre les paquets reçus et les paquets retransmis. L'IDS a quelques problèmes avec les modèles réalistes ainsi qu'avec la métrique du niveau de confiance entre les véhicules.

Pour pallier aux problèmes des faux positifs et des faux négatifs, les auteurs ont introduit des mécanismes comme les seuils de tolérance ou les seuils de dévaluation. Dans [8], on présente un IDS basé sur « l'immunocomputing » et sur les systèmes immunitaires artificiels. L'IDS utilise un algorithme de sélection négative avec un modèle de comportement normal pour entrainer ses capteurs. On utilise également un algorithme de sélection clonal permettant la reconnaissance de nouveaux modèles d'attaques auxquels l'IDS résiste. Des méthodes de détection existent pour certaines attaques et sont à ce jour indépendantes des IDS. Celles-ci fournissent des solutions à des cas particuliers d'attaques n'agissant pas directement sur une entité du réseau et sont difficilement intégrables dans un IDS. Dans [50] les auteurs proposent une architecture active de détection et de validation des coordonnées des véhicules voisins. Leur méthode utilise un système de reconnaissance visuel et un système d'analyse des paquets de coordonnées. Lorsque la reconnaissance visuelle n'est plus possible due à un obstacle, la méthode devient inefficace. Dans [21] les auteurs, proposent une méthode de détection pour parer les attaques « *Wormhole* ». Ce type d'attaque se base sur la coopération de plusieurs entités malicieuses dans le réseau afin de perturber le routage du réseau. L'approche utilisée par les auteurs est un système de carte géographique. Elle permet une traçabilité des paquets afin de détecter les anomalies dans le routage. Les méthodes de détection permettent d'empêcher que certaines attaques soient effectuées sur les protocoles faillibles et connus comme AODV ou DSR. La sécurité permet de prévenir certains de ces problèmes, empêchant simplement que ce genre d'attaques ne soit effectué.

1.3 SÉCURITÉ

Les problèmes de sécurité sont nombreux dans les réseaux VANETs. Un des problèmes majeurs est la révocation des certificats de sécurité. Dans [49], les auteurs proposent un mécanisme sécurisé pour la révocation des certificats. La méthode permet la détection

des faux certificats et permet une gestion plus efficace de la révocation. La sécurité des informations des réseaux VANETs passe également par la vérification des informations envoyées aux autres membres de ce même réseau. L'article [20] propose de supprimer l'identifiant des véhicules dans les messages périodiques pour préserver la vie privée des utilisateurs. La suppression de cet identifiant améliore la vie privée et évite d'être traquée par un attaquant. Afin de fournir une souplesse dans la sécurité et de rendre les systèmes tolérants à l'erreur, des mécanismes doivent être mis en place. Dans [2], les auteurs présentent un mécanisme basé sur des seuils dynamiques pour donner ou non sa confiance à ses voisins. Avoir confiance en ses voisins sur la route permet de distinguer deux types d'informations provenant de deux sources différentes pour prendre la bonne décision sur un comportement à adopter. Les auteurs de [43] présentent un mécanisme basé sur des seuils dynamiques pour donner ou non sa confiance à ses voisins. La méthode proposée sécurise les réseaux VANETs contre les utilisateurs douteux en refusant une communication avec ceux-ci. La principale difficulté de ces méthodes réside dans la définition d'une bonne métrique de confiance. Le seuil doit également tolérer les erreurs d'envoi et de calcul qui sont normales pour un système informatique. En plus d'une tolérance à l'erreur, la tolérance à un dysfonctionnement, ou, à une mauvaise utilisation du matériel dans un véhicule, peut être la cause de la détection d'une attaque par d'autres entités du réseau. Les auteurs dans [22] proposent une technique pour gérer ces cas de figure. Le mécanisme de défense se base sur des seuils dynamiques, ceux-ci permettent une révocation automatique des certificats en cas de comportement anormal répété. La sécurité passe également par la prévention et par la conscience des véhicules de son entourage. Afin d'améliorer la détection des véhicules qui pourrait ne pas être directement en ligne de mire sur la route, les auteurs dans [18] ont proposé une détection coopérative des véhicules. La méthode proposée utilise une approche coopérative pour découvrir de nouveaux véhicules proches et valider leur position GPS. Sécuriser un système est une tâche complexe, les méthodes de sécurité présentées fournissent des pistes de solutions dans la recherche. Pour améliorer encore

les résultats, il est nécessaire de regrouper les entités du réseau en sous-groupe et nous gagnerons ainsi un plus grand contrôle des flux d'informations.

1.4 LA CLUSTERISATION

En plus de la sécurité et des systèmes de détection d'intrusions, les méthodes de clusterisation permettent d'améliorer la sécurité dans les réseaux VANETs. Elles définissent des groupes de véhicules pour échanger des données. Dans [14], les auteurs proposent un modèle de clusterisation multisauts. Leur méthode se base sur une dissémination rapide des données, mais elle nécessite plus de contrôle sur le cluster. Beaucoup de véhicules vont entrer et sortir du cluster et une attaque pourrait faire beaucoup de dégâts. Dans [12], chaque véhicule connait ses coordonnées GPS. Le cluster est créé en connaissant la direction et le sens des véhicules. La tête du cluster élue est celle ayant la meilleure dissémination des données dans le cluster. Dans [13] et [16], les auteurs présentent aussi des méthodes de clusterisation pour les zones urbaines, en utilisant les coordonnées GPS et la direction du véhicule grâce à des cartes électroniques. Ces méthodes pourraient être intéressantes sur les autoroutes, car elles réduisent la formation de clusters sur la route et le cluster est généralement plus stable. Mais comme dans [12], le problème étant qu'on ne peut pas déterminer à l'avance la direction des véhicules sur l'autoroute et on ne doit pas contraindre l'utilisateur à déterminer son voyage. Dans [17], les auteurs proposent une méthode de clusterisation pour les autoroutes. Les véhicules qui ont la même direction peuvent être clustérisés. La route est divisée en plusieurs sections. Chaque véhicule est clusterisé dans sa section. Cette approche génère beaucoup d'entrées et de sorties de véhicules dans les clusters, ce qui rend la méthode instable. Dans [15], on présente une approche de clusterisation passive basée sur la vitesse des véhicules sur la route. On propose une table qui met en relation la vitesse des véhicules avec un groupe. Chaque véhicule connait sa vitesse et celle de son groupe. La formation du cluster se fait lorsqu'un véhicule souhaite communiquer avec d'autres véhicules qui sont dans le même groupe de vélocité que lui.

Aucune sécurité n'a été proposée pour cette approche. Les auteurs de [44] propose une méthode de gestion de la clusterisation basée sur le RSU. Le RSU divise sa zone en sous-zone dans lesquels les véhicules communiqueront sur un même canal. La méthode améliore la communication entre les véhicules et réduit la perte de paquet. La méthode ne fonctionne pas sans RSU dans la zone et aucun mode ad hoc n'a été proposé à ce jour. Dans le document [46], une analyse et une comparaison de l'acquisition d'information entre des véhicules clusterisés et l'approche multisaut est faite. Les résultats de l'étude montrent que l'utilisation de cluster réduit la redondance des données dans le réseau et permet d'économiser des ressources. De nombreuses méthodes de clusterisation sont proposées à ce jour, néanmoins, aucune n'intègre les concepts de sécurité. L'utilisation des clusters permet d'avoir un contrôle des flux d'informations, une clusterisation prenant en compte des politiques de sécurité est une idée qui devrait être envisagée.

1.5 CONCLUSION

Dans ce second chapitre, nous avons présenté les différentes vulnérabilités et les problématiques intrinsèquement liées aux réseaux VANETs. Il existe de nombreux problèmes de sécurité qui n'ont pas de solution à ce jour et nous en avons présenté ici plusieurs. De nombreuses méthodes de détection d'attaques sont présentées, mais aucune n'inclut le RSU en coopération avec les véhicules pour construire un mécanisme puissant et préventif pour les systèmes de détection d'intrusions. De plus, les méthodes d'IDS génèrent des alertes qui peuvent être des vrais positifs/vrai négatifs. Il faut réduire l'impact des fausses alarmes dans le réseau, mais sans mécanisme de prise de décision ceci est impossible. Le but de notre travail est de concevoir un mécanisme d'aide à la décision basé sur la coopération des membres. Faire corroborer une attaque par plusieurs membres du réseau permet à une alerte du réseau d'être prise en considération avec une très forte probabilité. Nous allons proposer un mécanisme de corroboration basé sur les

entités du réseau qui permet la mise en place d'une sécurité adéquate au sein d'un cluster. Le chapitre suivant détaille notre protocole de prise de décisions pour les informations de sécurité dans les réseaux VANETs.

CHAPITRE III - MODÉLISATION DU PROTOCOLE

Dans les réseaux VANETs, il existe de nombreux problèmes de sécurité qui à ce jour n'ont pas de solution. Ceux-ci ont été présentés dans le chapitre précédent. De nombreuses méthodes de détection d'attaques sont présentées, mais aucune n'inclut le RSU en coopération avec les véhicules pour construire un mécanisme puissant et préventif pour les systèmes de détection d'intrusions. Avoir un IDS capable de diffuser rapidement l'information qu'une attaque a été détectée sur plusieurs kilomètres permettrait d'améliorer la prévention et de mettre en place des politiques de sécurité adéquates. Dans ce chapitre, nous présentons notre protocole. Celui-ci utilise deux approches d'IDS et une méthode de clusterisation pour améliorer la sécurité des VANETs. Dans la première, les IDS sont installés sur chacun des véhicules. Tandis que dans la seconde, ils sont installés sur les RSUs. Les deux approches utilisent une technique de clusterisation spécifique pour regrouper les véhicules en fonction de leurs vitesses sur la route. Si un véhicule souhaite communiquer, il doit faire partie d'un cluster et doit connaitre la tête de cluster. Sinon, l'algorithme de clusterisation est initialisé et l'élection de la tête de cluster débute. Dans la première approche, la tête de cluster (CH) est responsable de faire suivre les paquets à l'interne du cluster, à ses voisins dans le cluster et aux RSUs. Lorsque l'IDS détecte une attaque, l'information et le type d'attaque utilisé seront diffusés aux clusters voisins par le RSU et les véhicules. Dans la seconde approche, tous les paquets émis par le cluster sont transmis aux RSUs. Ceux-ci vont corroborer l'attaque avec les RSUs à portée et envoyer une alerte aux têtes de cluster de la zone. Dans les deux méthodes, lorsqu'une corroboration positive est faite, la tête de cluster met en place une politique de sécurité (exemple: ajustement de valeurs de confiance pour les nouveaux véhicules du cluster). Le protocole est amorcé lorsqu'une attaque est détectée.

3.1 COMPOSANTE DU PROTOCOLE

Dans ce travail, nous allons utiliser un IDS pour détecter qu'une attaque est en cours ou a été détectée. Lorsqu'un IDS détecte une attaque, il diffuse l'information et le type d'attaque utilisé a ses voisins directement devant et derrière lui. Lorsqu'un cluster reçoit l'information, une nouvelle politique de sécurité peut être mise en place.

Nous adaptons initialement la méthode de clusterisation décrite dans [15]. Celle-ci présente des caractéristiques intéressantes, que nous allons décrire par la suite pour notre méthode. La première partie de notre travail consiste à adapter la méthode de clusterisation. Nous allons expliquer comment celle-ci fonctionne et quelles sont les améliorations que nous y apportons pour répondre à notre problème.

3.1.1 DÉFINITION DU CLUSTER

Par définition, un groupe de véhicules doit être capable de s'autoformer comme cluster sur la route. De plus, il doit pouvoir élire une tête de cluster pour permettre une communication avec le RSU. La tête de cluster a un rôle spécifique; c'est une passerelle vers le RSU qui conserve des informations à propos des clusters de sa zone. Les informations sauvegardées sont ensuite envoyées aux RSUs à sa portée. Ces informations sont cruciales dans notre méthode.

L'algorithme de clusterisation que nous utilisons présente les caractéristiques suivantes :

- Simple d'utilisation. Nous pouvons facilement l'utiliser, le mettre en place, le modifier ou l'adapter à nos besoins.
- Bonne stabilité, une fois le cluster formé. Les véhicules de celui-ci doivent rester le plus longtemps possible au sein de ce dernier. De plus, une grande stabilité permet un plus grand contrôle de l'activité au sein des clusters.

- Bonne estimation de la densité des véhicules. Plus nous avons d'information sur la densité des véhicules, plus nous gagnons au niveau du contrôle et de la sécurité dans nos clusters.
- Conservation des propriétés de la méthode initiale décrite dans [15]. Le but de notre travail est d'avoir une méthode simple et efficace.

3.1.2 MÉCANISME INTERNE DU CLUSTER

Initialement, la méthode utilise la clusterisation passive. Le cluster est formé automatiquement en fonction de la vitesse des véhicules. Ils proposent une table statique faisant la correspondance entre les groupes de clusters et la vitesse du groupe [15]. Leurs postulats sont les suivants: chaque véhicule connait sa position et sa vitesse grâce au GPS (*Global Positioning System*). Chaque véhicule dans la même zone avec la même catégorie de vitesse est en mesure de se clusteriser.

Tableau 1 : Relation entre la vitesse de groupe et le groupe de cluster [15]

Speed interval (kmph)	Speed group	Clustering Group
0 - 30	0	0
30 - 45	1	1
45 - 60	2	1
60 - 75	3	2
75 - 90	4	2
90 - 110	5	2
110 – 120	6	3
120+	7	3

La méthode utilise des intervalles de vitesse, des groupes de vitesses et des groupes de clusters, comme montrés dans le Tableau 1. Les auteurs mentionnent seulement 3 différents groupes de clusters, on réduit ainsi la surcharge de paquets et les

communications entre les groupes. Si deux différents groupes souhaitent communiquer, ils vont utiliser le RSU pour faire suivre leurs paquets de données.
L'approche initiale définit 4 états pour les véhicules: initiale (INIT), Tête de cluster (CH), passerelle (GW) et ordinaire (ORD). Seuls le CH et la GW peuvent faire suivre les paquets de données. Les véhicules GW sont sélectionnés par le CH après un certain temps. Un véhicule quitte le cluster lors d'un changement de vitesse de groupe, celle-ci sera mise à jour après quelques secondes. Dans notre approche, le RSU est une passerelle permanente, chaque véhicule sur la route peut envoyer des informations de sécurité via celui-ci. Nous allons donc distinguer 2 types de passerelle, les statiques (RSU) et les dynamiques (véhicules). Les RSUs ne font pas partie des clusters.

Nous avons fait de nouvelles hypothèses pour le CH et nous avons modifié l'état GW. Les 4 états définis pour notre approche sont :

- INIT: Chaque véhicule débute dans cet état et peut devenir CH. Il n'y a qu'un CH par cluster. Les véhicules dans l'état INIT vont passer par l'état ORD et peuvent devenir CH ou GW.

- CH: la tête de cluster a pour charge de faire suivre les paquets d'une source vers d'autres véhicules et vers les passerelles. Seulement 2 sources peuvent être trouvées dans l'approche: les GWs et les ORDs. L'élection de la tête de cluster est simple; le premier véhicule déclarant « je suis la tête de cluster » le devient.

- ORD: chaque véhicule déjà présent dans le cluster et qui n'est ni CH, ni GW, est dans l'état ORD. C'est l'état basique des nœuds après l'élection de la tête de cluster. Celui-ci peut être éligible au rang de GW temporaire.

- GW: par défaut, le RSU est une passerelle statique. Le RSU fait suivre les paquets de données venant d'une GW, d'un CH ou d'un véhicule ORD. Il peut

aussi transmettre les paquets de sa zone vers une zone proche en faisant suivre les données par un autre RSU. Dans notre méthode, les seuls paquets retransmis sont les informations de sécurité. Les véhicules peuvent devenir GW lorsque le CH les proclame. Une réélection des GWs peut avoir lieu lorsqu'une GW quitte le cluster.

3.1.3 Algorithme de Clusterisation

Pour améliorer la sécurité au sein du cluster, nous avons supposé que tous les paquets transmis avant le processus de clusterisation, sont détruits. Un véhicule qui souhaite communiquer doit faire partie d'un cluster. Lorsqu'un véhicule est seul dans son cluster, il deviendra CH et pourra communiquer. Si d'autres véhicules viennent dans sa zone et souhaitent entrer dans le cluster alors l'élection du CH est réitérée.
Nous avons utilisé les 5 premières étapes de la méthode initiale. Les deux dernières étapes ont été adaptées pour notre protocole. Tous les véhicules sont dans l'état initial, aucune communication n'a encore été établie et aucun véhicule n'a encore envoyé de paquets.

1) Un véhicule souhaite envoyer des données, dépendamment de son groupe de vitesse et de son état; il estampille et ajoute ses informations à l'entête du paquet avant de l'envoyer. Ce véhicule ne peut pas être CH dès le départ, il ne sait pas s'il existe déjà un CH ou s'il n'y a pas au moins un autre véhicule dans le groupe. Le véhicule devient CH lorsqu'il n'y a pas de réponse durant un certain temps.
2) Un véhicule voisin récupère le paquet envoyé, il vérifié les informations de groupe et d'état de l'entête du paquet.
3) Lorsque le paquet vient d'un nœud du même groupe de cluster et que celui-ci n'est pas CH, le véhicule récipiendaire compétitionne pour le rôle de CH.
4) Le premier véhicule envoyant le message "Je suis le CH" le devient.

5) Tous les nœuds sont informés de l'identité du véhicule CH.
6) Le CH collecte périodiquement les informations envoyées par son cluster.
7) Le véhicule CH fait suivre les paquets de données dépendamment de nos approches d'IDS. La figure 6 résume notre algorithme.

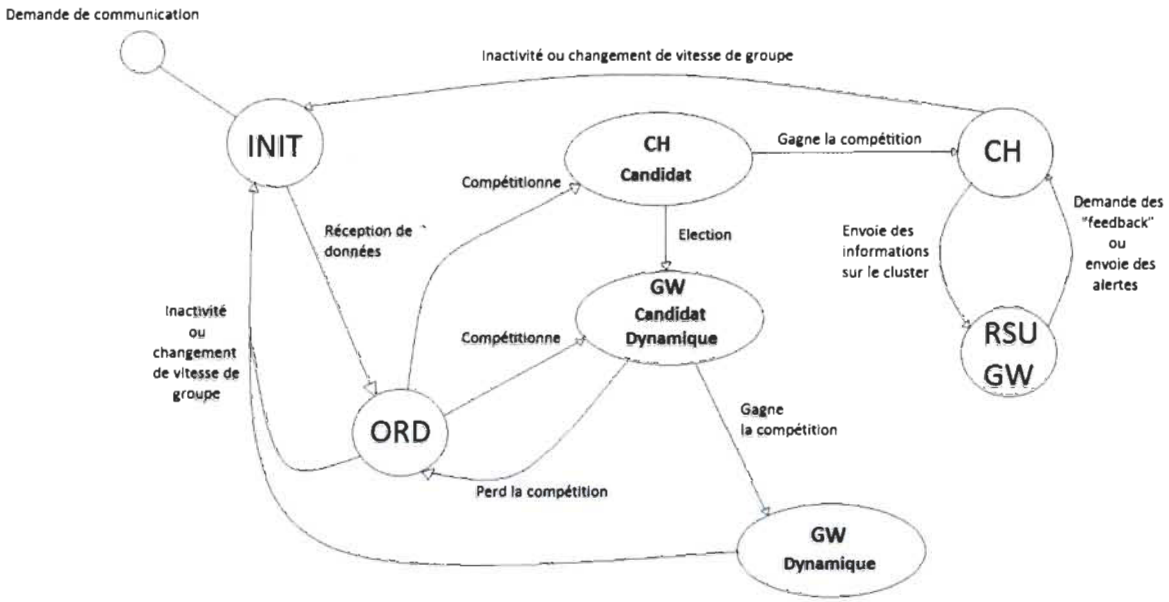


Figure 6: Déroulement du processus de clusterisation

3.1.4 DÉFINITION DES SYSTÈMES DE DÉTECTION D'INTRUSION

Notre travail est basé sur 2 approches d'IDS. Dans la première, la détection est faite au sein des véhicules, tandis que dans la seconde, elle est faite par les RSUs. Nous allons ensuite comparer les résultats des deux approches.

3.1.4.1 Approche d'IDS basées véhicules

Dans cette approche, chaque véhicule est équipé avec un IDS personnel. Le système de détection d'intrusions est actif en permanence. Les véhicules peuvent être isolés, seuls ou dans un groupe de cluster. Chacun des nœuds détecte de manière individuelle les attaques. Lorsqu'une attaque est détectée, l'information de l'attaque est transmise au CH. Celui-ci gère les informations d'alerte comme décrite dans l'approche ci-dessous.

3.1.4.1.1 Méthode mathématique de corroboration d'attaque pour les IDS basées véhicules

Corroborer l'information qu'une attaque est en cours est une amélioration majeure dans les réseaux VANETs. Pour les IDS basés véhicules, il y a une méthode simple pour valider qu'une attaque est réellement en cours. Voici les hypothèses de cette approche:

- Il y a un IDS installé sur chaque véhicule;
- Les communications entre les véhicules et entre les véhicules et les RSUS sont sécurisées. Les données sont chiffrées;
- Les RSUS sont fiables;
- Toutes les alertes transmises aux RSUS sont considérées comme vraies. Lorsqu'un IDS détecte une anomalie, on la considère toujours comme une attaque réelle. Nous ne considérons pas le cas des vrais-négatifs.

Lorsqu'un membre du cluster détecte une attaque, il envoie l'information et la signature de l'attaque à la tête de cluster. La tête de cluster analyse la signature et envoie ces informations aux autres membres du cluster pour avoir leurs opinions. Lorsque tous les véhicules ont fourni leurs avis sur la signature, la tête de cluster les transmet au RSU de sa zone. Celui-ci conserve les informations transmises et renvoie la signature à un autre cluster de la zone pour avoir leurs opinions. Le RSU calcule ensuite la probabilité de l'attaque $P_{attaque}$ en utilisant la formule (1).

$$(1) \quad P_{attaque} = \frac{Nb\_détection}{Nb\_véh\_total}$$

Ou :

- $P_{attaque}$ représente la probabilité de corroboration de l'attaque.
- $Nb\_détection$ représente le nombre de véhicules ayant détecté l'attaque.
- $Nb\_véh\_total$ est le nombre total de véhicule ayant donné leurs opinions.

Lorsque$P_{attaque} > 0{,}50$, plus de la moitié des véhicules ont validé l'alerte, il s'agit donc d'une attaque.

Nous demandons les opinions de deux clusters pour la raison suivante : lorsqu'un cluster contient une majorité d'attaquants, le véhicule attaqué ne pourra jamais faire corroborer ses alertes par notre protocole.

L'approche basée véhicule est expliqué par les figures ci-dessous. La figure 7 présente le processus détection et basé véhicule entre les membres du cluster et vers le RSU de la zone.

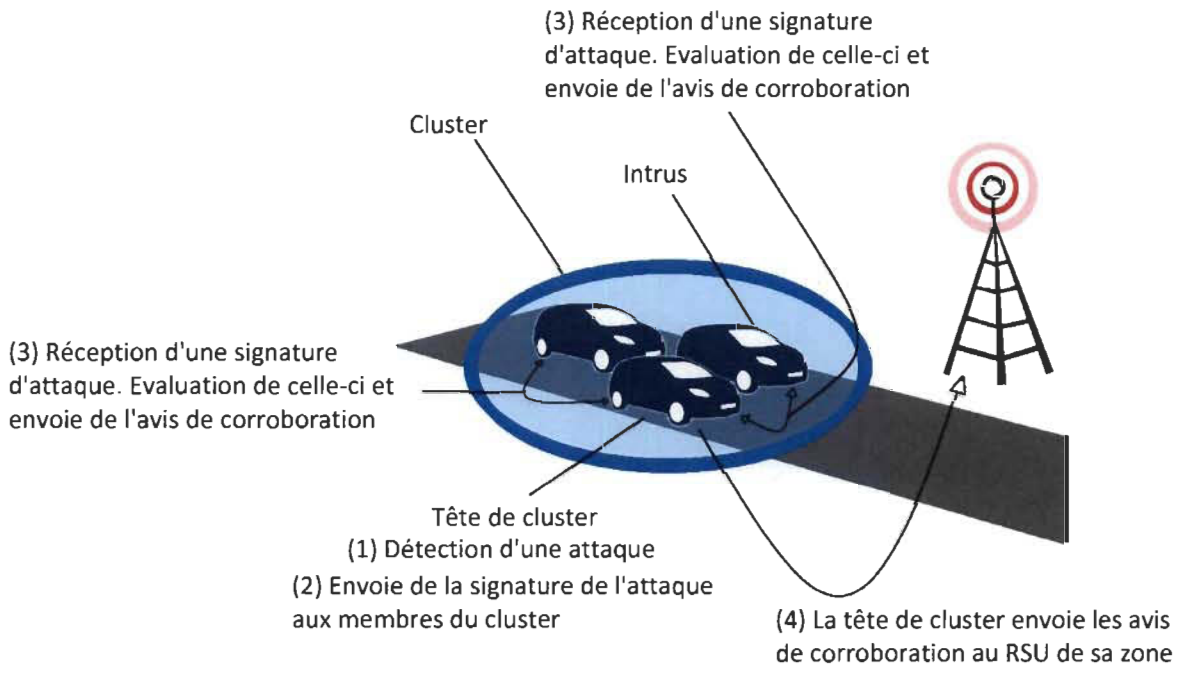


Figure 7: Processus de détection basé véhicule

La figure 8 présente le processus de corroboration par un autre cluster de la zone.

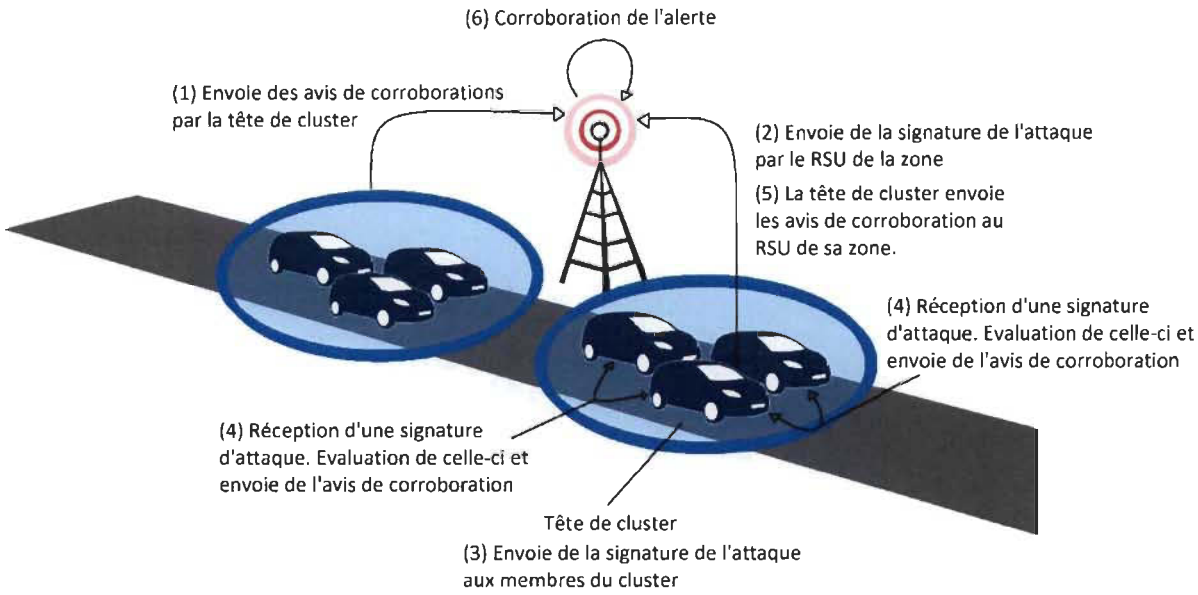


Figure 8: Processus de corroboration basé sur les véhicules

Ci-dessous, à la figure 9, on présente le graphe de la méthode IDS basé véhicule sous forme d'état/action. Cette forme de présentation aide à la compréhension des comportements des entités dans la méthode.

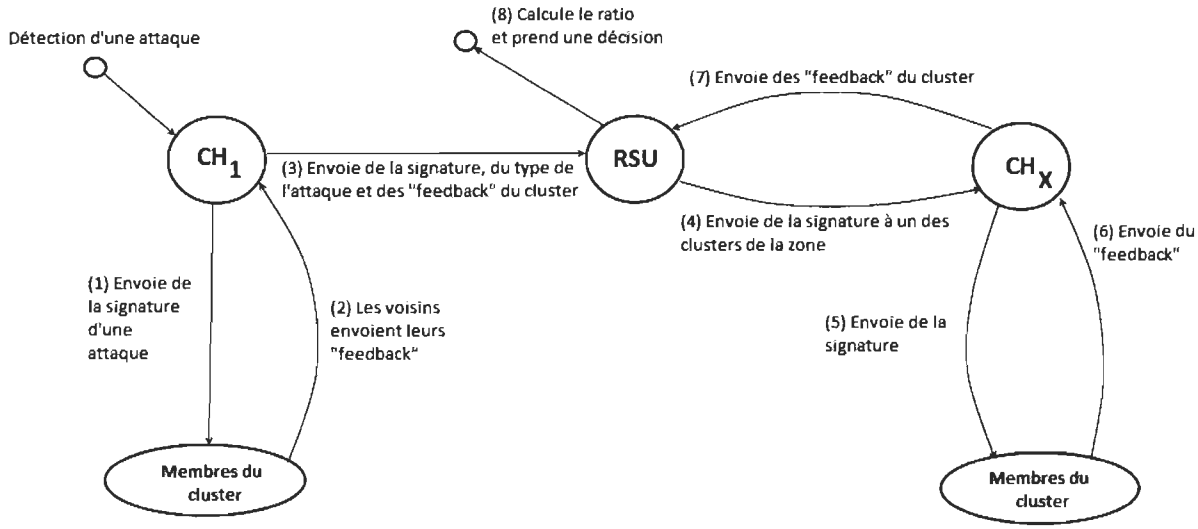


Figure 9 : Graphe état/action de la méthode IDS basée véhicule

3.1.4.2 Approche d'IDS basées RSUs

L'approche de détection d'intrusions basée sur les RSUs est une alternative à l'approche basée véhicules. Elle préserve une bonne sécurité du système, car les paquets sont analysés par une entité externe : le RSU.

3.1.4.2.1 Algorithme de l'approche d'IDS basées RSUs

Comme dans la première approche, voici les hypothèses que nous utilisons:

- Le cluster existe et le CH est déjà en place.
- Les données échangées au sein du cluster et vers le RSU sont:
    1. Les paquets de données de tous les véhicules sont envoyés au CH.
    2. Le CH fait suivre tous les paquets vers le RSU.
    3. Le RSU analyse ceux-ci. Lorsqu'une attaque est détectée, le CH est alerté comme expliqué ci-dessous.

3.1.4.2.2 Méthode mathématique de corroboration d'attaque pour les IDS basées RSUs

Une approche similaire est adaptée pour les RSUs. Les mêmes hypothèses et méthodes sont utilisées. Tous les paquets venant du cluster sont retransmis au RSU. Lorsque le RSU détecte une attaque, il envoie la signature de l'attaque aux RSUs suivants et précédents. Ceux-ci retournent leurs opinions au RSU initiateur du protocole. Le RSU calcule ensuite le ratio comme dans (1). Lorsque l'attaque est corroborée, une alerte est envoyée aux têtes de cluster de la zone comme présentées par les figures 10 et 11.

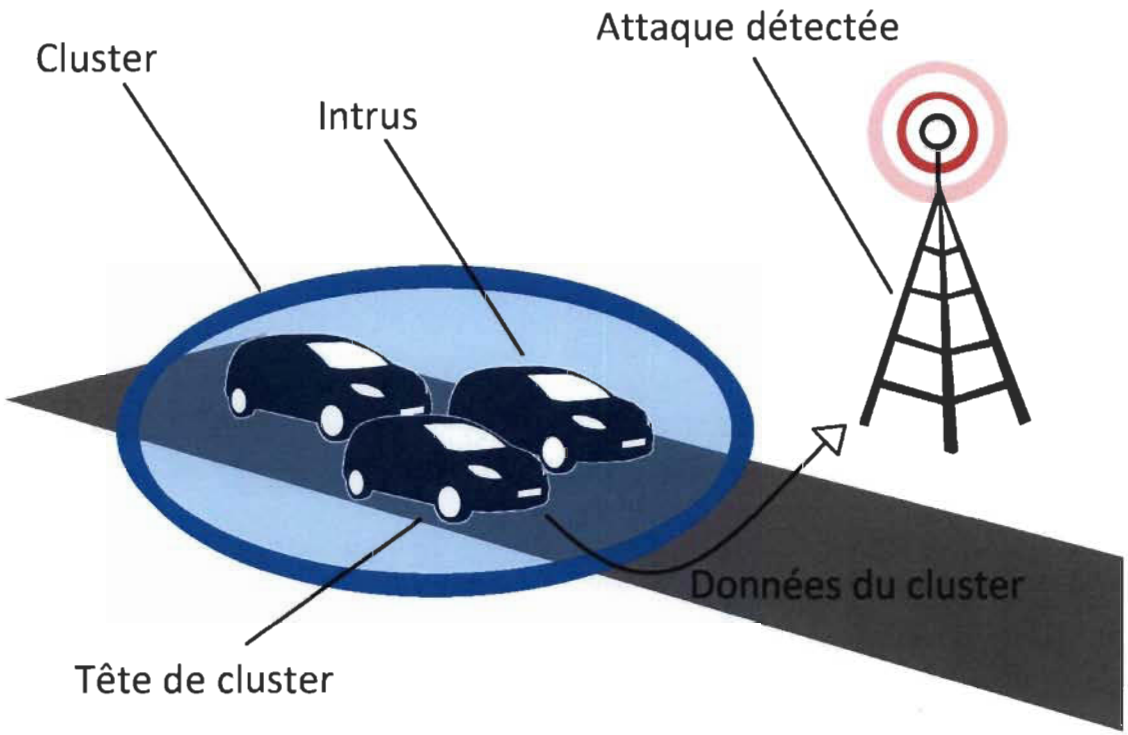


Figure 10 : Processus de détection basé RSU

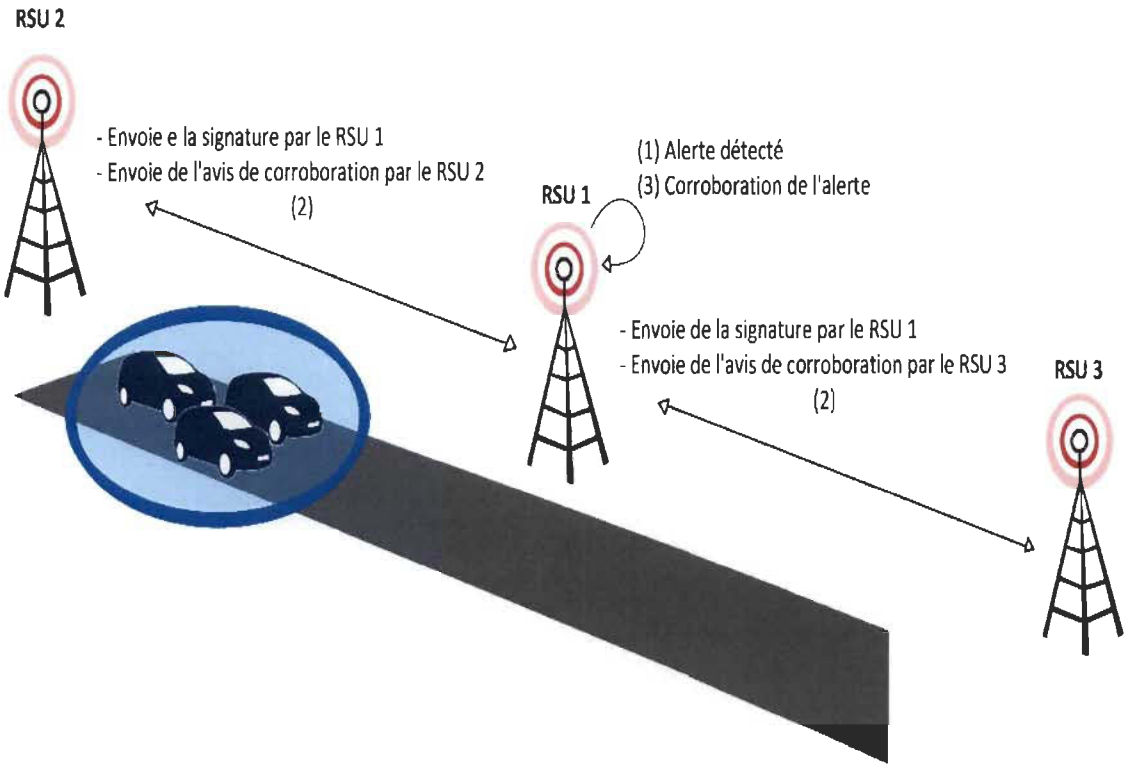


Figure 11 : Processus de corroboration basé RSU

Ci-dessous, la figure 12, celle-ci présente le graphe de la méthode IDS basé RSU sous forme d'état/action. Cette forme de présentation aide à la compréhension des comportements des entités dans la méthode.

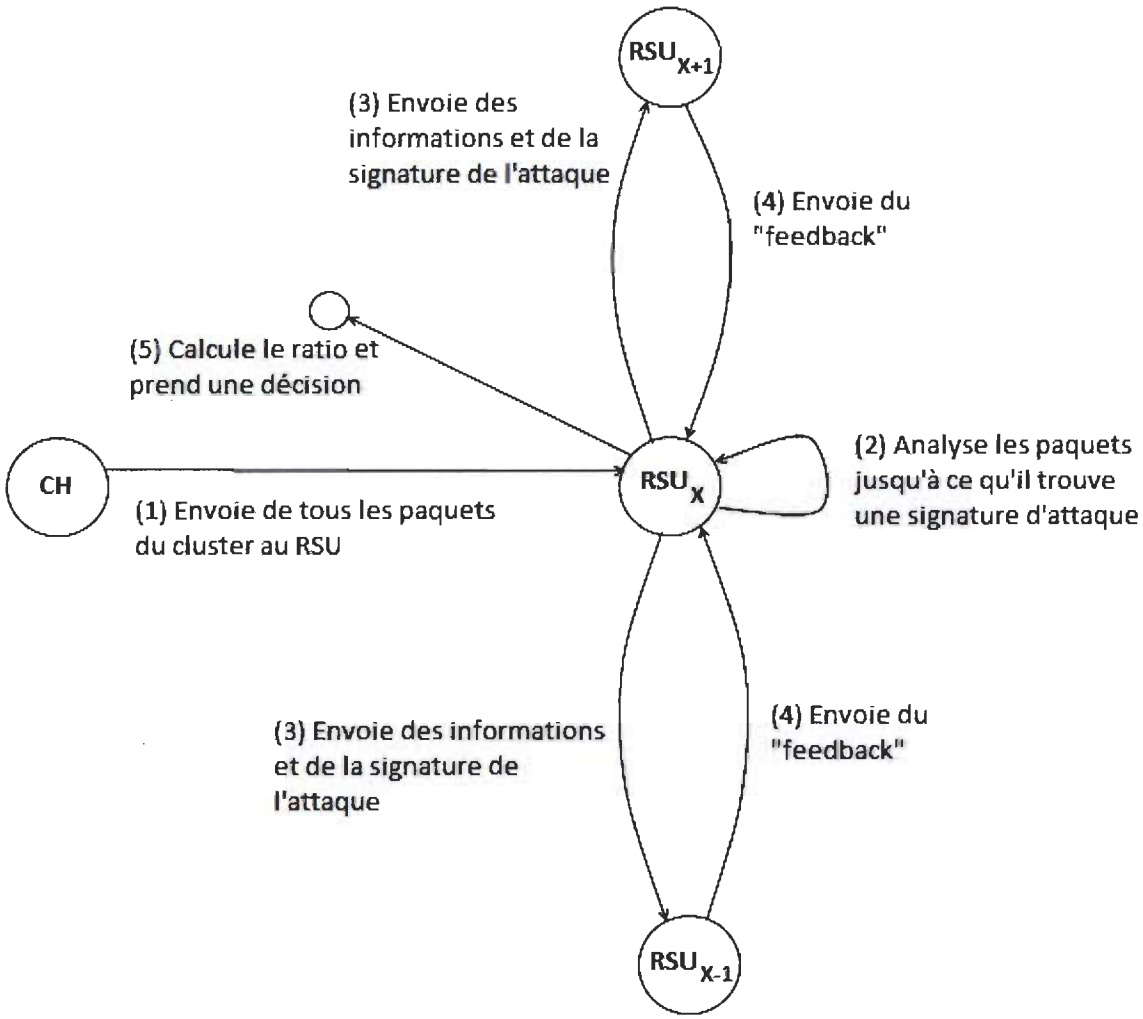


Figure 12 : Graphe état/action de la méthode IDS basée RSU

3.2 ROUTAGE DES INFORMATIONS DE SÉCURITÉ

Tous les composants utilisés par notre méthode ont été définis précédemment. Nous allons maintenant présenter les hypothèses, les mécanismes et l'algorithme de routage utilisés dans notre méthode.

3.2.1 HYPOTHÈSES

Pour maintenir la cohérence de nos résultats, les hypothèses suivantes sont utilisées pour le travail:

- Les RSUS sont à portée pour pouvoir communiquer.
- Chaque véhicule fait partie du cluster. Lorsqu'une attaque survient, nous savons de quelle zone elle provient et nous pouvons estimer sa proximité grâce aux informations sur les clusters.
- Les données échangées ne peuvent pas être modifiées.
- Chaque RSU connait le nombre de véhicule dans sa zone au temps *t*. Nous avons également une traçabilité des mouvements des véhicules d'un cluster à l'autre, et ce même durant les changements de zone.

3.2.1.1 Mécanismes internes

Les données envoyées par la tête de cluster vers le RSU sont :

- Le nombre de véhicules dans son cluster.
- La portée entre le premier et le dernier véhicule de son cluster. Chaque tête de cluster demande aux véhicules de son cluster ses coordonnées GPS au temps *t*. La tête de cluster recherche ensuite le premier et dernier véhicule du cluster. Celle-ci envoie ensuite les données au RSU. Cela nous permettra d'évaluer l'accessibilité des clusters.
- Chaque RSU est à portée de communication de deux RSUs voisins. Ceux-ci peuvent s'échanger des informations au temps *t*. Les informations demandées pour un cluster donné sont les suivantes: la position du premier véhicule, la position du dernier véhicule, la position de la tête de cluster et le nombre de véhicules dans le cluster. Nous pouvons ainsi déterminer si les véhicules de la zone d'un RSU sont à portée des véhicules du RSU courant.

Le tableau 2 présente les informations collectées par la tête de cluster, retransmis au RSU et échangées entre ceux-ci.

Tableau 2 : Informations collectées et retransmises

Notation	Description
Nb_veh	Nombre de véhicules dans le cluster
Pos_CH	Position GPS de la tête de cluster
Pos_CF	Position GPS du premier véhicule dans le cluster
Pos_CL	Position GPS du dernier véhicule dans le cluster

3.2.1.2 Description de l'algorithme

Nous allons distinguer 3 cas pour diffuser efficacement les informations: véhicule à véhicule (V2V), infrastructure à véhicule (I2V) et un fonctionnement hybride des deux méthodes.

Dans le fonctionnement V2V, le RSU sait quels sont les clusters devant et derrière le cluster attaqué dans sa zone. Celui-ci envoie au cluster attaqué la confirmation de l'attaque et lui demande de diffuser cette information aux clusters proches. La figure 13 décrit ce processus.

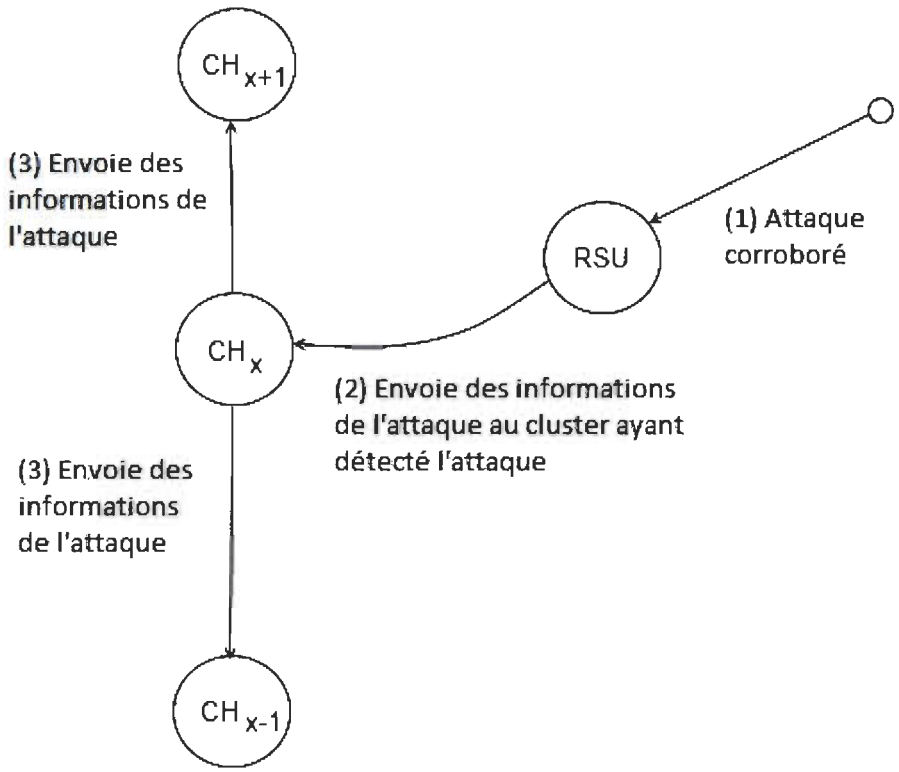


Figure 13: Diffusion de l'information de l'attaque par la méthode V2V

Dans l'approche V2I, le RSU sait que le cluster attaqué n'est pas à portée d'un autre cluster. Celui-ci envoie au cluster attaqué la confirmation de l'attaque et retransmet l'information aux RSUs à portée (dépendamment de la situation) comme expliquées dans la figure 14.

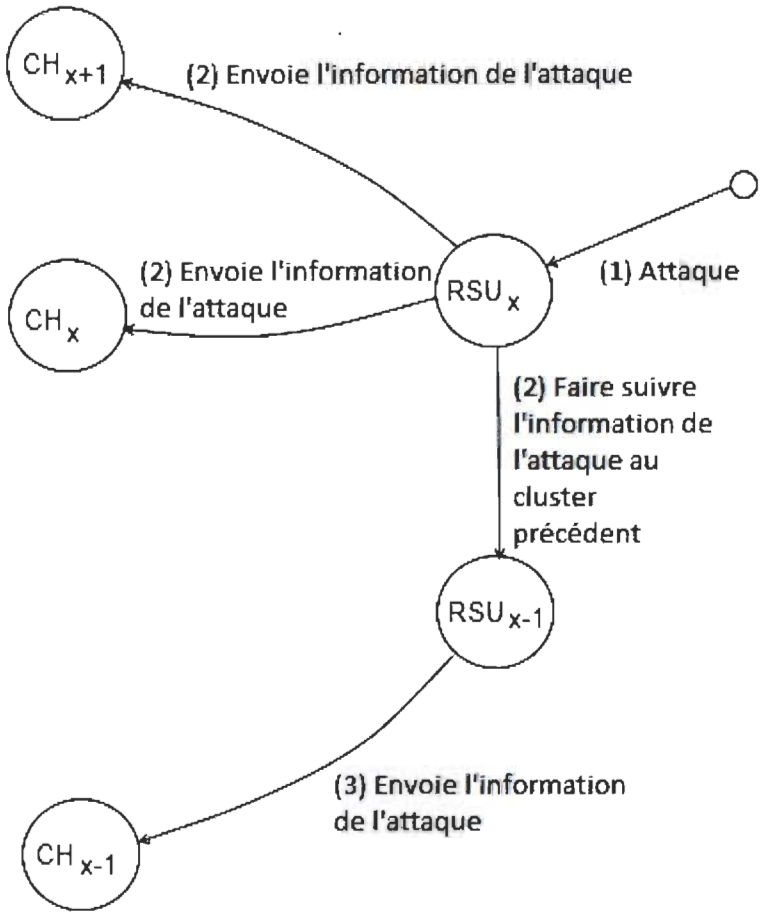


Figure 14: Diffusion de l'information de l'attaque par la méthode V2I

3.2.1.3 Les métriques

Nous nous sommes initialement concentrés sur la métrique de portée de diffusion. Notre méthode est intéressante pour les clusters proches. Dépendamment du standard 802.11p, les RSUs peuvent approximativement émettre dans une portée allant jusqu'à 1000 mètres. Dans notre méthode les RSUS vont être a portée de transmission les uns des autres. Idéalement la métrique de portée doit être suffisamment faible pour rencontrer les véhicules sur la route, mais également suffisamment grande pour que la majorité des véhicules puissent bénéficier de l'information.

3.3 CONCLUSION

Nous avons présenté, de manière théorique, notre protocole d'aide à la prise de décision pour les réseaux VANETs. Celui-ci permet la corroboration des informations de sécurité et diffuse l'information qu'une attaque a eu lieu au sein des clusters proches. Ces informations sont cruciales pour la sécurité des VANETs. Elles permettent la mise en place d'une politique de sécurité adéquate dans le cluster attaqué et dans les clusters proches afin de parer efficacement les prochaines attaques. Le chapitre suivant présente l'implémentation de notre méthode. Nous détaillerons les messages utilisés, les algorithmes en pseudo-code pour les clusters et l'implémentation de notre méthode.

CHAPITRE IV - SIMULATION & ANALYSE DES PERFORMANCES

Dans le chapitre précédent, nous avons présenté notre protocole de manière théorique. Dans cette partie, nous allons présenter l'implémentation et les résultats des simulations. La programmation a été faite en C++ avec le simulateur OMNeT++ et l'API Veins. Celle-ci étant spécialement conçue pour développer des composants pour les réseaux VANETs. Nous avons également utilisé le simulateur routier SUMO pour gérer la mobilité des nœuds sur la route. Nous présentons dans ce chapitre, les différents messages, les algorithmes « pseudo-code » utilisés pour le développement et finalement nous présentons les métriques évaluées et les résultats obtenus.

4.1 LES MESSAGES DE COMMUNICATIONS

Notre approche requiert des messages de communication. Ceux-ci sont propres à certaines entités (communication: entre véhicules, entre RSUs, entre véhicules et tête de cluster) et permettent de collecter, transmettre ou diffuser des informations importantes. Nous distinguerons différents messages dans nos 2 approches : l'approche IDS basée véhicule et l'approche IDS basée RSU. La taille des messages de communication est évaluée en octet.

4.1.1 APPROCHE IDS BASÉE VÉHICULE

Dans l'approche IDS basée véhicule nous avons défini 6 types de messages différents. On retrouve les messages de : "Data", "Clusterisation", "Cluster2RSU", "RSU2RSU", "Alert", "Alert2RSU". Une description de chaque message est donnée dans ce paragraphe.

Message 1 (20 octets): C'est le message de "***Data***" classique. Dans notre approche, il est diffusé par tous les véhicules de manière périodique. Il amorce le processus de clusterisation entre les véhicules. Il contient les champs GPS, TTL et ID_Cluster. Le tableau 3 détaille chaque champ du message « ***Data*** ».

Tableau 3 : Message Data

Nom de la variable	Type de données	Taille en octet	Description de la variable
GPS	**Coord**	12	Coordonnées X, Y, Z du véhicule émetteur.
TTL	**int**	4	Durée de vie du paquet.
ID_Cluster	**int**	4	Identifiant du cluster où le message est émis.

Message 2 (40 octets): C'est le message de clusterisation appelé "***Clustering***" dans la méthode. Il permet la clusterisation des véhicules en échangeant des informations telles que: l'identité de la tête de cluster, l'identité des véhicules présents dans le cluster, l'identité du véhicule émetteur, etc. Il permet également l'élection de la tête de cluster et des passerelles. La description des différents champs du message « Clustering » sont présentée ci-dessous dans le tableau 4.

Tableau 4 : Message Clustering

Nom de la variable	Type de données	Taille en octet	Description de la variable
TTL	**int**	4	Durée de vie du paquet.
ID_veh	**int**	4	Identité du véhicule émetteur

ID_cluster	**int**	4	Identifiant du cluster
T_CH	**simtime_t**	4	Temps d'émission du paquet. Utilisé lors de l'élection de la tête de cluster
Speed_Group	**int**	4	Vitesse de groupe du véhicule
State_Cluster	**bool**	4	État du cluster. (0: pas clusterisé; 1: clusterisé). Utilisé lors de l'initialisation du protocole.
GW	**bool**	4	Utilisé pour élire les passerelles. 0: Ce n'est pas une élection; 1: élection d'un véhicule.
State_CH	**bool**	4	Utilisé pour l'élection de la tête de cluster. 0: Pas d'élection; 1: élection du CH.
State_veh	**string**	4	État du véhicule. Par défaut INIT.
Liste_veh[5]	**int**	4	Liste des identifiants des véhicules dans le cluster.

Message 3 (48 octets): Le message « ***Cluster2RSU*** », permet de transmettre les informations de la tête de cluster vers le RSU et réciproquement. Après que la tête de cluster a collecté les informations de tous les véhicules à l'instant *t*, ce message est envoyé au RSU pour l'informer de l'activité du cluster. Les différents champs de ce message sont détaillés dans le tableau 5.

Tableau 5 : Message Cluster2RSU

Nom de la variable	Type de données	Taille en octet	Description de la variable
TTL	**int**	4	Durée de vie du paquet.
ID_cluster	**int**	4	Identifiant du cluster d'émission.
Nb_veh	**int**	4	Nombre de véhicules dans le cluster.
Pos_CH	**Coord**	12	Position GPS du cluster au temps t d'émission.
Pos_CF	**Coord**	12	Position GPS du premier véhicule dans le cluster.
Pos_CL	**Coord**	12	Position GPS du dernier véhicule dans le cluster.

Message 4 (48 octets): Le message « ***RSU2RSU*** » permet la communication des informations des clusters entre les RSUs proches. La transmission de ces informations permet d'avoir un suivi sur les clusters entrant dans la zone. Le détail de chaque champ est présenté ci-dessous dans le tableau 6.

Tableau 6 : Message RSU2RSU

Nom de la variable	Type de données	Taille en octet	Description de la variable
TTL	**int**	4	Durée de vie du paquet.
ID_cluster	**int**	4	Identifiant du cluster d'émission.
Nb_veh	**int**	4	Nombre de véhicules dans le cluster.

Pos_CH	**Coord**	12	Position GPS du cluster au temps t d'émission.
Pos_CF	**Coord**	12	Position GPS du premier véhicule dans le cluster.
Pos_CL	**Coord**	12	Position GPS du dernier véhicule dans le cluster.

Message 5 (46 octets): Le message « ***Alerte*** » est envoyé par un véhicule aux autres véhicules du groupe dans le but d'avoir leurs opinions sur la signature détectée. Chaque véhicule envoie son opinion à la tête de cluster. Le détail de chaque champ est présenté ci-dessous dans le tableau 7.

Tableau 7 : Message Alerte

Nom de la variable	Type de données	Taille en octet	Description de la variable
TTL	**int**	4	Durée de vie du paquet.
ID_veh_detectant	**int**	4	Identité du véhicule émetteur qui a détecté l'attaque.
ID_veh_rep	**int**	4	Identité du véhicule répondant à la signature.
ID_cluster	**int**	4	Identifiant du cluster
Rep_RSU	**int**	4	Message envoyé par le RSU. 0: Non; 1: Oui
Detected	**bool**	4	Réponse à la signature d'une attaque. 0: Opinion négative sur la signature; 1: Opinion positive sur la signature.
DetectionTime	**simtime_t**	4	Temps auquel l'attaque a été détectée.

Nb_veh	**int**	4	Nombre de véhicules dans le cluster.
CPT_veh	**int**	4	Nombre de véhicules ayant validé l'attaque.
Signature	**string**	10	Signature de l'attaque.

Message 6 (46 octets): Le message « ***Alert2RSU*** » permet la communication d'information d'alerte entre la tête de cluster et le RSU. Ce message est émis par la tête de cluster lorsque tous les véhicules ont répondu suite à une alerte donnée. Les opinions sont transmises au RSU afin qu'il corrobore l'alerte. Le détail de chaque champ est présenté ci-dessous dans le tableau 8.

Tableau 8 : Message Alert2RSU

Nom de la variable	Type de données	Taille en octet	Description de la variable
TTL	**int**	4	Durée de vie du paquet.
ID_veh_detectant	**int**	4	Identité du véhicule émetteur qui a détecté l'attaque.
ID_veh_rep[5]	**int**	4	Identité des véhicules ayant répondu à la signature.
ID_cluster	**int**	4	Identifiant du cluster
Rep_RSU	**int**	4	Message envoyé par le RSU. 0: Non; 1: Oui
Detected[5]	**bool**	4	Réponses à la signature d'une attaque. 0: Opinion négative sur la signature; 1: Opinion positive sur la signature.

DetectionTime	**simtime_t**	4	Temps auquel l'attaque a été détectée.
Nb_veh	**int**	4	Nombre de véhicules dans le cluster.
CPT_veh	**int**	4	Nombre de véhicules ayant validé l'attaque.
Signature	**string**	10	Signature de l'attaque.

4.1.2 Approche IDS basée RSU

Dans l'approche IDS basé RSU de nombreux messages de l'approche basée véhicules sont réutilisés. Parmi ceux-ci on retrouve les messages de "*Data*", "*Clustering*", "*Cluster2RSU*" et "*RSU2RSU*". Nous avons adapté le message "*Alerte*" pour les besoins des RSUs. Certaines informations étant prévues pour l'utilisation des véhicules, elles sont devenues obsolètes et ont été supprimées. Voici le message modifié pour cette approche basée RSU.

Message 1 (34 octets): Le message « ***Alerte*** » est envoyé par un RSU aux RSUS à portée dans le but d'avoir leurs opinions sur la signature détectée. Chaque RSU envoie son opinion au RSU émetteur. Lorsque l'attaque est corroborée, un message « ***Alerte*** » est envoyé aux clusters de la zone. La description du message « Alerte » est présentée ci-dessous dans le tableau 9.

Tableau 9 : Message d'Alerte pour la méthode basée RSU

Nom de la variable	Type de données	Taille en octet	Description de la variable
TTL	**int**	4	Durée de vie du paquet.

Rep_RSU	**int**	4	Message envoyé par le RSU. 0: Non; 1: Oui
Detected	**bool**	4	Réponses à la signature d'une attaque. 0: Opinion négative sur la signature; 1: Opinion positive sur la signature.
DetectionTime	**simtime_t**	4	Temps auquel l'attaque a été détectée.
ID_RSU_detectant	**int**	4	Identifiant du RSU qui a détecté l'attaque.
ID_RSU_rep	**int**	4	Identifiant du RSU fournissant une opinion sur une attaque.
Signature	**string**	10	Signature de l'attaque.

Nous avons présenté les messages de communications pour nos 2 approches. Ceux-ci permettent aux entités de transmettre des informations dans notre réseau via les têtes de clusters et les RSUs. Nous allons maintenant présenter les algorithmes, en commençant par celui de la clusterisation qui est le même pour les deux approches. Ensuite, nous détaillerons les algorithmes pour la méthode basée véhicules et enfin ceux de la méthode basée RSUs.

4.2 PRÉSENTATION DES ALGORITHMES

Nous avons précédemment établi les messages de communication pour nos deux approches. Nous présentons dans cette partie les algorithmes en pseudo-code utilisés pour nos deux méthodes. Celles-ci utilisant l'algorithme de clusterisation, nous le présentons ci-dessous.

4.2.1 ALGORITHME DE CLUSTERISATION

L'algorithme de clusterisation s'amorce sur la réception de paquet « *Clustering* ».

Début

Paramètre d'entrée: Un paquet de types clustering encapsuler dans un paquet WaveShortMessage.

```
paquet_clustering = Décapsuler le paquet du WaveShortMessage
Si (Ma Vitesse de groupe == paquet_clustering->vitesse de groupe){
        Si (Mon Rôle == "INIT"){
                Ajouter les nouveaux membres présents dans le paquet
                Si (Un CH est déjà présent dans le paquet reçu){
                        Ajouter les infos du CH
                }
                Mon Rôle = ORD
                Envoyé un paquet de confirmation aux membres que je suis bien rentré dans le Cluster
        }
        Sinon{
                Si ( Mon Rôle =="ORD"){
                        Si ( Le paquet est pour mon groupe de cluster){
                                Si ( C'est un paquet d'élection de GW et qu'il est pour moi){
                                        Mon Rôle = GW
                                }
                                Si ( Le CH n'a pas été élu){
                                        Ajouter les nouveaux membres présents dans le paquet
                                        Si ( Mon ID == ID_CH dans le paquet){
                                                Vérification et Validation de mon ID pour devenir
CH
                                        }
                                        Envoie aux membres de mon intention de devenir CH
                                }
                                Sinon{
                                        Si ( Mon T_CH ==0 || (Le T_CH du paquet <= Mon T_CH)){
                                                Mon T_CH = T_CH du paquet
                                                Envoie au membre de l'ID du véhicule ayant le plus
petit T_CH
                                        }
                                }
                        }
                        Sinon{
                                Si( Il reste de la place dans le cluster){
                                        Envoyer une invitation au nouveau membre
                                }
                        }
                }
                Sinon{
                        Si ( Mon Rôle == "GW"){
```

```
                    Si( Le paquet n'est pas pour moi){
                        Retransmettre le paquet
                    }
                    Sinon{
                        Si( Le membre n'est pas dans mon cluster){
                            Envoyé une invitation
                        }
                    }
                }
                Sinon{
                    Si (Mon Rôle=="CH"){
                        Si (Le membre n'est pas dans mon cluster){
                            Envoyé une invitation
                        }
                    }
                }
            }
        }
    }
```

Fin

4.2.2 ALGORITHME POUR LA MÉTHODE BASÉE VÉHICULE

Nous avons présenté l'algorithme de clusterisation basé sur les messages « *Clustering* » définis précédemment. Ci-dessous, nous définissons les algorithmes en pseudo-code de notre première méthode, IDS basé véhicule. Ceux-ci sont utilisés après que les véhicules aient été clusterisés.

4.2.2.1 Algorithme de collecte de données pour les véhicules

On présente ici l'algorithme gérant la collecte et la retransmission des données dans le cluster pour la méthode basée véhicule.

Début

Paramètre d'entrée: Un paquet de types "*Data*" encapsulé dans un paquet WaveShortMessage.

paquet_Data = Décapsuler le paquet du WaveShortMessage

```
Si ( Le paquet est pour mon groupe de cluster ){
        entier atk= générer un nombre aléatoire
        Si ( atk>seuil ){
                Diffuser aux véhicules voisins qu'une attaque est détecté
        }
        Si ( Mon rôle est CH ){
                Stocker mes coordonnées GPS et mon identifiant
                Stocker les coordonnées GPS et l'identifiant du paquet
                Si ( Tous les véhicules du cluster ont fourni leurs coordonnées )
                        Envoyer les coordonnées et les identifiants au Cluster de la zone
                        Réinitialisation du tableau de coordonnées
                }
        }
        Sinon{
                Si ( Mon rôle est GW ){
                        Retransmettre le paquet
                }
        }
}
Sinon{
        Si ( Je ne suis pas clusterisé ){
                Définir l'identifiant de groupe du message Data comme mon Identifiant de groupe
        }
        Si ( L'identifiant du véhicule émetteur n'est pas dans ma liste de cluster){
                Ajouter le nouveau membre
        }
        Si ( Mon cluster a des places disponibles ){
                Envoyé une invitation au nouveau membre
        }
}
```

Fin

4.2.2.2 Méthode de traitement des alertes pour les véhicules

On présente ici l'algorithme de traitement des alertes par les véhicules dans la méthode basée véhicule.

Début

Paramètre d'entrée: Un paquet de type "*Alert*" encapsulé dans un paquet WaveShortMessage.

paquet_Alert = Décapsuler le paquet du WaveShortMessage

```
Si ( Le paquet est une demande d'opinion de mon cluster){
        Si ( Mon rôle est CH ){
                Si ( L'alerte n'est pas déjà présente){
                        Ajouter l'alerte dans la liste des alertes
                        Ajouter mon opinion sur cette alerte
                }
        }
        Sinon{
                Si ( L'opinion sur l'alerte n'est pas présente ){
                        Ajouter l'opinion
                        Si ( Tous les véhicules ont donné leur opinion ){
                                Envoyer l'alerte et la liste des opinions de mon cluster
                        }
                }
        }
}
```

Fin

4.2.2.3 Méthode de traitement des messages venant d'un cluster

On présente ici l'algorithme permettant de traiter les messages venant d'un autre cluster et ayant transité par le RSU. Cet algorithme est utilisé pour la corroboration des attaques par un cluster proche.

Début

Paramètre d'entrée: un paquet de type "*Alert2RSU*" ou de type "*Cluster2RSU*" encapsulé dans un WaveShortMessage.

```
Si ( Le type du paquet est Cluster2RSU ){
        paquet_cluster= décapsuler le paquet Cluster2RSU
        Si ( Le cluster n'est pas présent ){
                Ajouter le cluster à la liste
                Ajouter ses informations
        }
        Sinon{
                Mettre a jour les informations du cluster
        }
}
Sinon{
        paquet_Alerte= décapsuler le paquet Alert2RSU
        Si ( L'alerte n'est pas présente ){
                Ajouter l'alerte à la liste des alertes
                Diffuser l'alerte à un autre cluster que celui d'où provient l'alerte
```

}
Sinon{
Si (L'alerte est une réponse à la demande de corroboration){

corroboration = $\frac{\sum véhicule\_détectant}{\sum véhicule\_totaux}$

Si (La corroboration > 0,50){
Diffuser l'alerte corroborer aux véhicules
}
}
}
}

Fin

4.2.3 ALGORITHME DE LA MÉTHODE BASÉE RSU.

Nous avons présenté les algorithmes pour la méthode IDS basé véhicule. Ci-dessous, nous présentons les algorithmes pseudo-code pour la méthode IDS basé RSU. Ces algorithmes sont utilisés après que les véhicules aient été clusterisés.

4.2.3.1 Algorithme de collecte de donnée pour les véhicules

On présente ici l'algorithme gérant la collecte et la retransmission des données dans le cluster pour la méthode basé RSU.

Début

Paramètre d'entrée: Un paquet de types « *Data* » encapsulé dans un paquet WaveShortMessage.

paquet_Data = Décapsuler le paquet du WaveShortMessage
Si (Le paquet est pour mon groupe de cluster){
Si (Mon rôle est CH){
Stocker mes coordonnées GPS et mon identifiant
Stocker les coordonnées GPS et l'identifiant du paquet
Si (Tous les véhicules du cluster ont fourni leurs coordonnées)
Envoyer les coordonnées et les identifiants au Cluster de la zone
Réinitialisation du tableau de coordonnées

```
                }
        }
        Sinon{
                Si ( Mon rôle est GW ){
                        Retransmettre le paquet
                }
        }
}
Sinon{
        Si ( Je ne suis pas clusterisé ){
                Définir l'identifiant de groupe du message Data comme mon Identifiant de groupe
        }
        Si ( L'identifiant du véhicule émetteur n'est pas dans ma liste de cluster){
                Ajouter le nouveau membre
        }
        Si ( Mon cluster a des places disponibles ){
                Envoyé une invitation au nouveau membre
        }
}
```

Fin

4.2.3.2 Méthode de traitement des paquets de Data reçu par les RSUs.

On présente ici l'algorithme gérant la collecte et la retransmission des données reçues par le RSU pour la méthode basée RSU.

Début

Paramètre d'entrée: Un paquet de types « *Data* » encapsulé dans un paquet WaveShortMessage.

```
paquet_Data = Décapsuler le paquet du WaveShortMessage
entier seuil prends des valeurs constantes comprise entre 50 et 90 définit pour la simulation.
entier atk = générer un nombre entre 0 et 100

Si ( atk>seuil ){
        Ajouter l'alerte à ma liste d'alerte détectée
        Envoyer l'alerte aux RSUS voisins
        Si ( Les alertes précédente n'ont pas eu de réponse ){
                Réémettre les alertes
        }
```

}

Fin

4.2.3.3 Méthode de traitement des paquets RSU2RSU et Alert2RSU reçu par les RSUs.

On présente ici l'algorithme de traitement et de retransmission des alertes par les RSU dans la méthode basée RSU.

Début

Paramètre d'entrée: Un paquet de types "*RSU2RSU*" ou de type "*Alert2RSU*" encapsulé dans un paquet WaveShortMessage.

```
Si ( C'est un message RSU2RSU ){
        Paquet_RSU2RSU = décapsuler le paquet
        Stocker les informations sur les clusters des zones voisines
}
Sinon{
        Si ( C'est un paquet Alert2RSU ){
                Alert2RSU= décapsuler le paquet
                Si ( Le champs Rep_RSU du  paquet Alert2RSU est égale à 0 )
                {
                        Envoie de mon opinion au RSU émetteur
                }
                Sinon
                {
                        Stocker la réponse du cluster à propos de l'alerte
                        Si ( Tous les RSUS ont fourni leur opinion ){
                                entier corrobore = Calculer la corroboration
                                Si ( corrobore>50 ){
                                        Diffuser l'information qu'une alerte a eu lieu
                                }
                        }
                }
        }
}
```

Fin

Nous avons présenté les algorithmes utilisés dans nos deux approches, ceux-ci ont été implémentés sous OMNet++. La partie suivante présente les simulateurs utilisés, les paramètres de simulation et analyse les résultats obtenus.

4.3 SIMULATION ET ANALYSE DES RÉSULTATS

Nous avons développé notre protocole de prise de décision avec ces algorithmes dans OMNet++ 4.2.2. La simulation a été faite sur une autoroute de 5km avec des voies d'accélération et de décélération. Nous avons simulé les deux approches avec 50, 100 et 150 nœuds. Il y a 19 nœuds fixes sur la carte, ils ont le rôle de RSU et ils sont disposés tous les 240 m. Nous avons fait varier le seuil de détection entre 50 et 90%. Les paramètres étudiés dans les deux approches sont : le nombre d'attaques détectées, le nombre d'attaques corroborées, le temps de corroboration moyen, le nombre total de paquets générés et le nombre total de paquets d'alertes générés. Nos résultats vont être présentés pour chacun des paramètres, en variant le nombre de nœuds.

4.3.1 NOMBRE D'ATTAQUES DÉTECTÉES

Les figures 15, 16 et 17 présentent le nombre d'attaques détectées en fonction du seuil de détection. Les résultats démontrent qu'en moyenne l'approche 1 lève des alertes à une plus grande fréquence que l'approche 2. Sachant que dans l'approche 1, chaque véhicule est équipé d'un IDS, ces résultats étaient prévisibles. La méthode 2 quant à elle ne possède qu'un IDS par RSU; alors le nombre d'alertes levé bien que plus faible reste non négligeable et relativement proche des résultats fournis par l'approche 1. Notons également, que plus le nombre d'alertes est important, plus il y a d'échange entre les entités et plus il y aura de traitement à faire.

4.3.1.1 Résultats pour une simulation avec 50 nœuds.

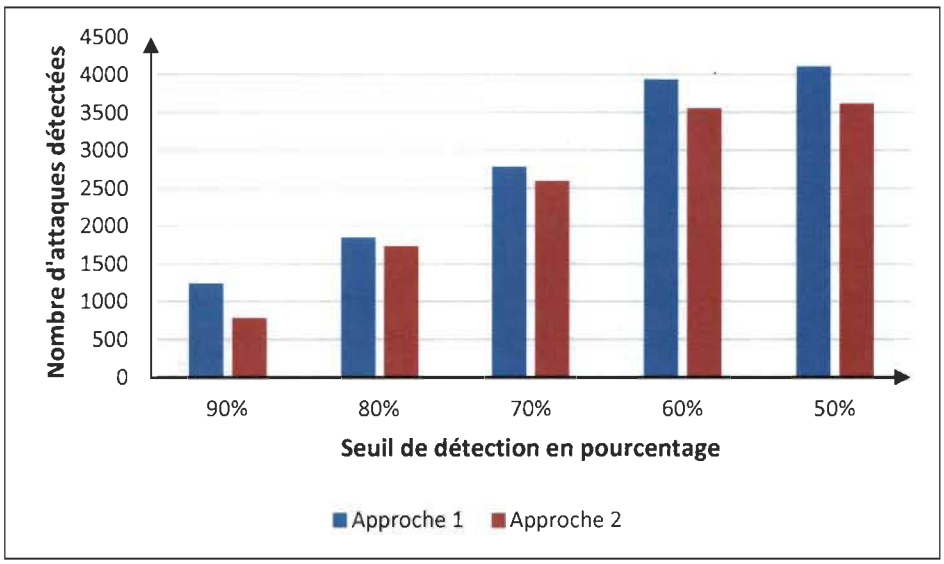


Figure 15 : Nombre d'attaques détectées en fonction du seuil de détection – 50 nœuds.

4.3.1.2 Résultats pour une simulation avec 100 nœuds.

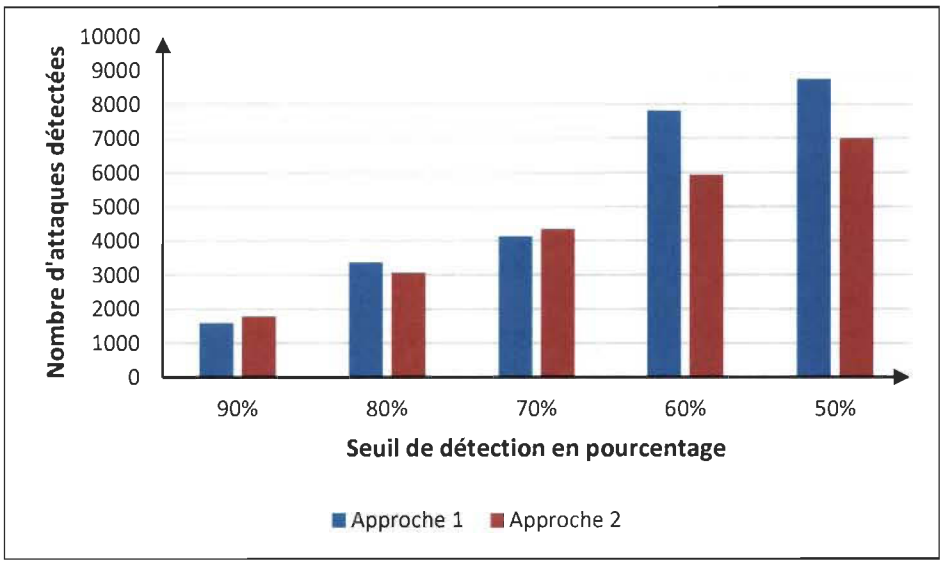


Figure 16 : Nombre d'attaques détectées en fonction du seuil de détection – 100 nœuds.

4.3.1.3 Résultats pour une simulation avec 150 nœuds.

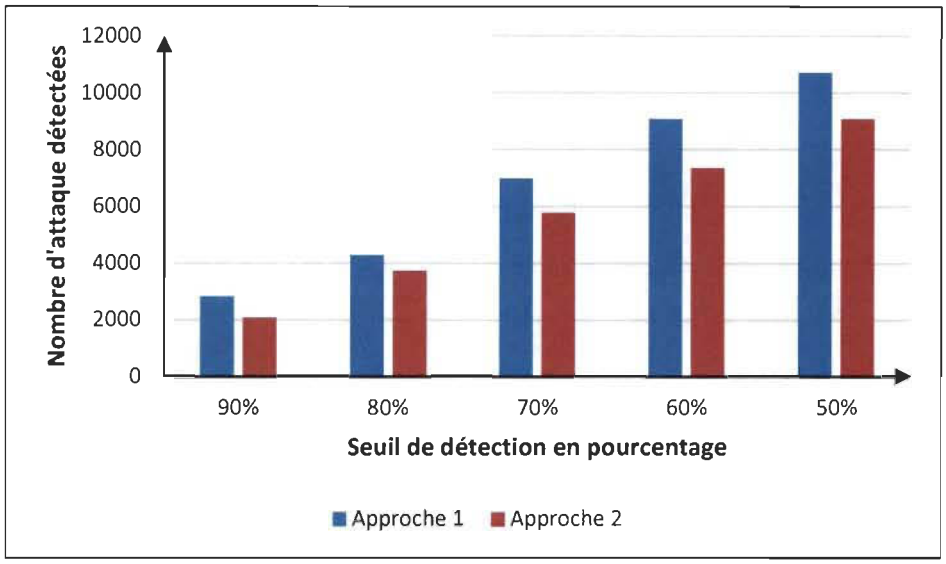


Figure 17 : Nombre d'attaques détectées en fonction du seuil de détection – 150 nœuds.

4.3.2 NOMBRE D'ATTAQUES CORROBORÉES

Les figures 18, 19 et 20 montrent le nombre d'attaques corroborées dans le réseau basé sur nos deux approches. Nous avons vu précédemment que l'approche 1 générait plus d'alertes. Par conséquent, il y a plus de traitement, plus d'échange de données et plus de perte de paquets dans la tentative de corroboration. Bien que l'approche 1 soit plus efficace dans la détection, elle le devient nettement moins dans la corroboration des alertes. L'approche 2 corrobore de façon plus efficace les alertes dans le réseau.

4.3.2.1 Résultats pour une simulation avec 50 nœuds.

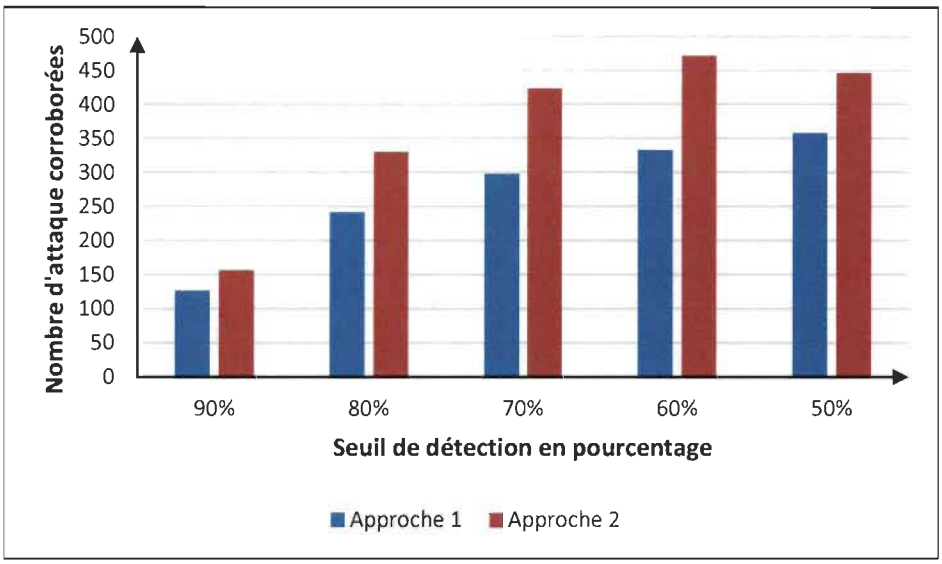


Figure 18 : Nombre d'attaques corroborées en fonction du seuil de détection – 50 nœuds.

4.3.2.2 Résultats pour une simulation avec 100 nœuds.

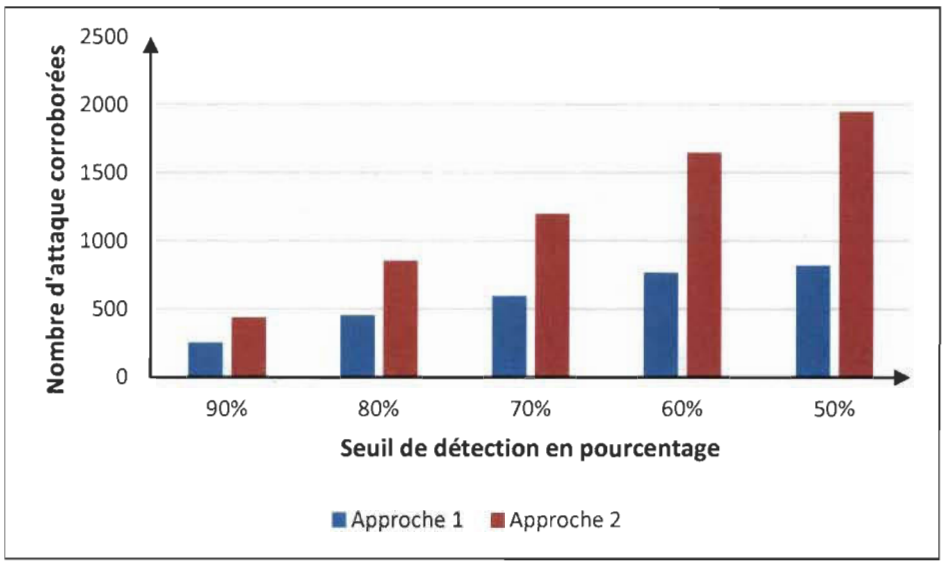


Figure 19 : Nombre d'attaques corroborées en fonction du seuil de détection – 100 nœuds.

4.3.2.3 Résultats pour une simulation avec 150 nœuds.

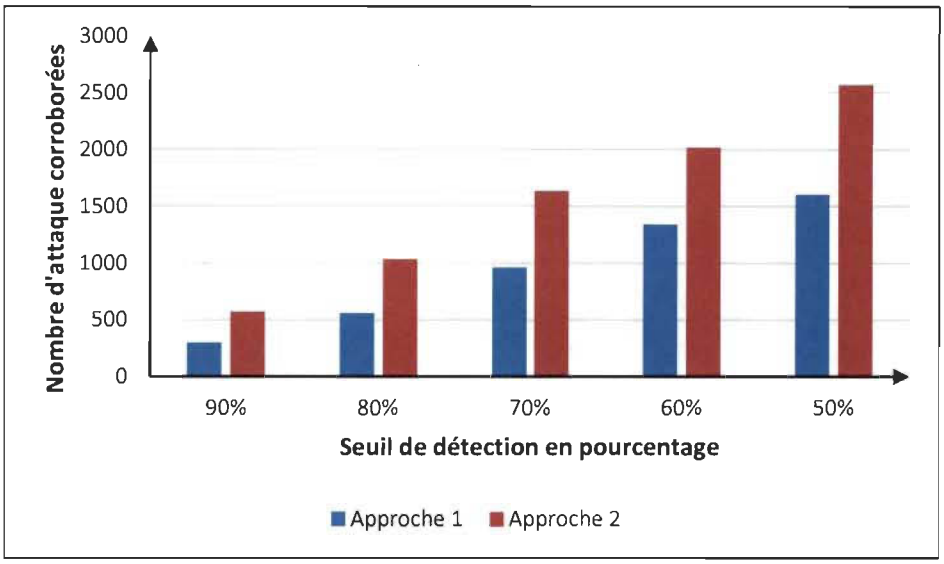


Figure 20 : Nombre d'attaques corroborées en fonction du seuil de détection – 150 nœuds.

4.3.3 TEMPS MOYEN DE CORROBORATION

Les figures 21, 22 et 23 montrent le temps moyen de corroboration d'une alerte en fonction de la méthode utilisée. Plus le temps est faible, meilleur est le temps de corroboration et meilleure sera l'anticipation sur une attaque dans le réseau. D'après les résultats, l'approche 2 corrobore plus rapidement les alertes. Dans celle-ci, peu de messages sont échangés, ce qui améliore grandement l'efficacité de corroboration.

4.3.3.1 Résultats pour une simulation avec 50 nœuds.

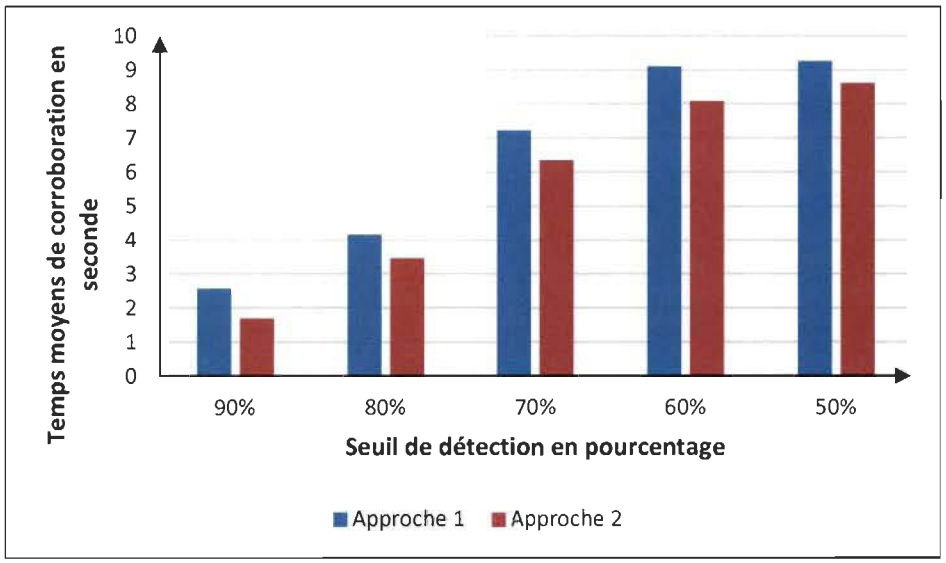


Figure 21 : Temps moyens de corroboration en fonction du seuil de détection – 50 nœuds.

4.3.3.2 Résultats pour une simulation avec 100 nœuds.

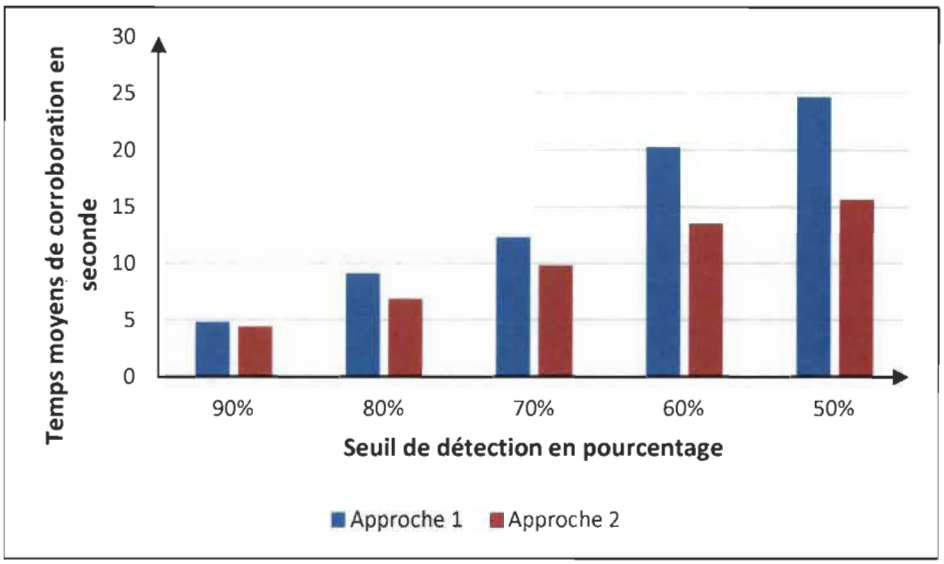


Figure 22 : Temps moyens de corroboration en fonction du seuil de détection – 100 nœuds.

4.3.3.3 Résultats pour une simulation avec 150 nœuds.

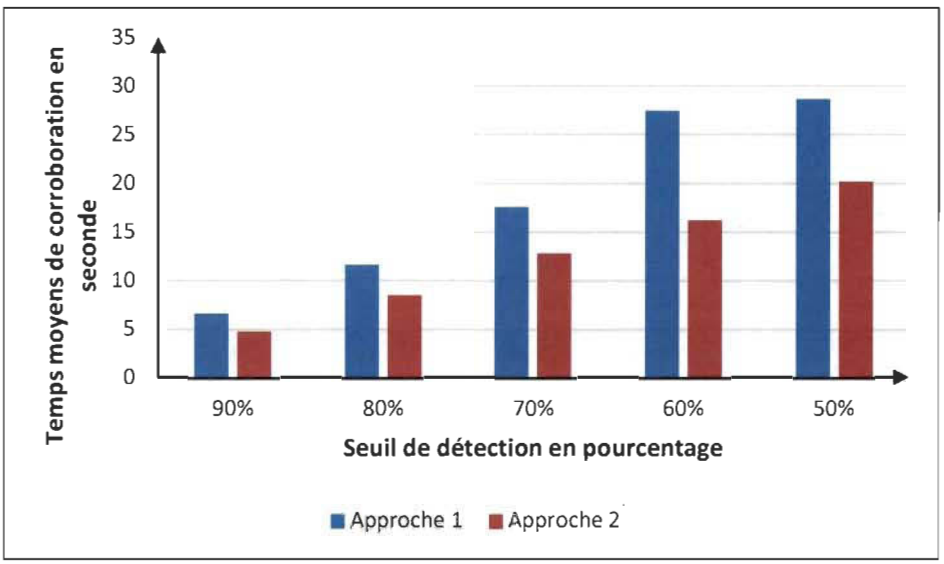


Figure 23 : Temps moyens de corroboration en fonction du seuil de détection – 150 nœuds.

4.3.4 Nombre total de paquets d'alertes générés.

Les figures 24, 25 et 26 montrent le nombre de paquets d'alertes totales généré entre toutes les entités du réseau. Nous pouvons constater que l'approche 1 génère un énorme trafic de paquets d'alertes. De plus due au grand nombre de paquets d'alertes généré, des pertes de paquets sont à prévoir, générant elles aussi une réémission des données. L'approche 2 génère moins de trafic. Les pertes de paquets, de même que les réémissions sont par conséquent moins nombreuses.

4.3.4.1 Résultats pour une simulation avec 50 nœuds.

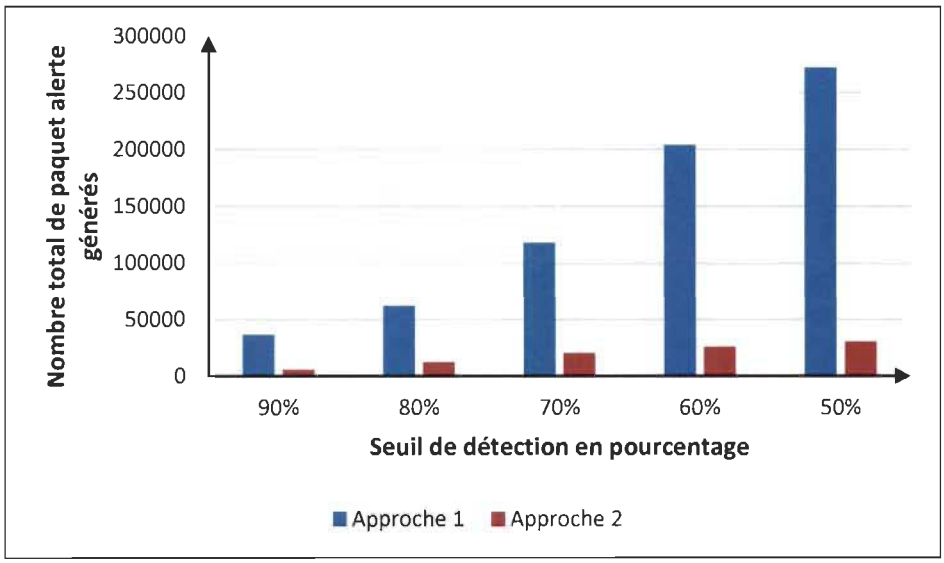


Figure 24 : Nombre de paquet total d'alerte générés en fonction du seuil de détection – 50 nœuds.

4.3.4.2 Résultats pour une simulation avec 100 nœuds.

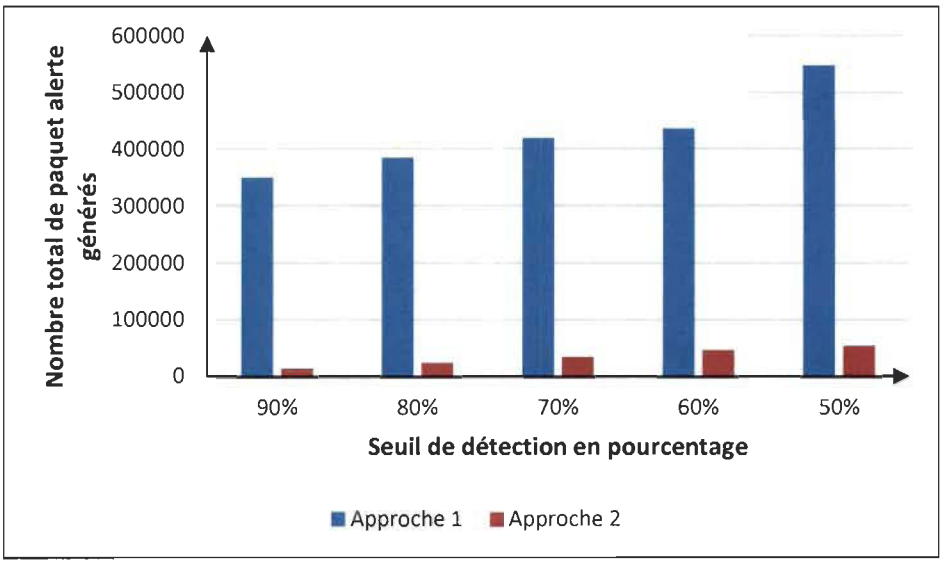


Figure 25 : Nombre de paquet total d'alerte générés en fonction du seuil de détection – 100 nœuds.

4.3.4.3 Résultats pour une simulation avec 150 nœuds.

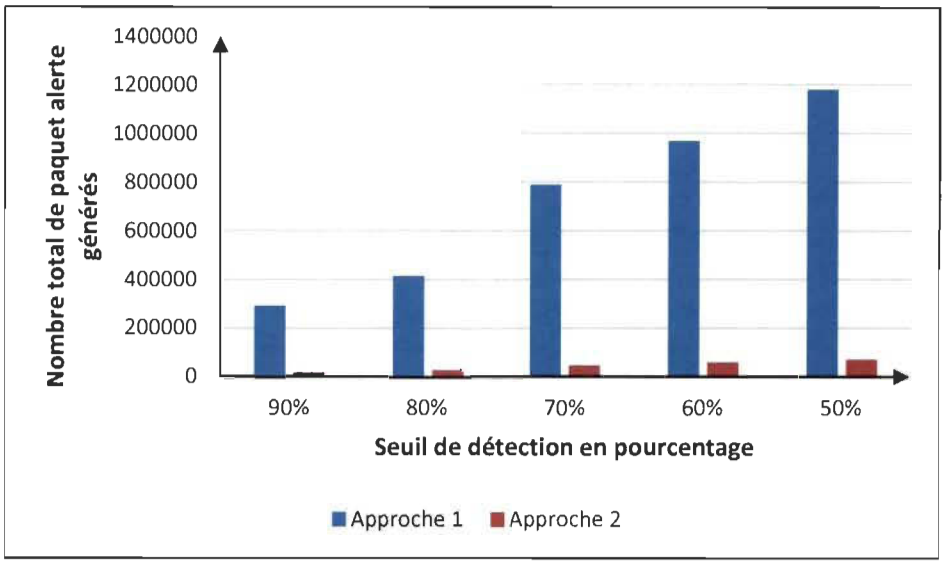


Figure 26 : Nombre de paquet total d'alerte générés en fonction du seuil de détection – 150 nœuds.

4.3.5 NOMBRE TOTAL DE PAQUETS GÉNÉRÉS.

Les figures 10, 11 et 12 montrent le nombre total de paquets généré en fonction des approches. Le nombre total de paquets comprend : les paquets de « ***Data*** », les paquets de « ***Clusterisation*** » et les paquets « ***Alerte*** ». Moins le nombre de paquets généré est élevé meilleur est la qualité de service. L'approche 2 montre un faible nombre de paquets généré dû au plus faible nombre d'échange de données. Celle-ci parait être la plus intéressante pour préserver la qualité de service dans le réseau.

4.3.5.1 Résultats pour une simulation avec 50 nœuds.

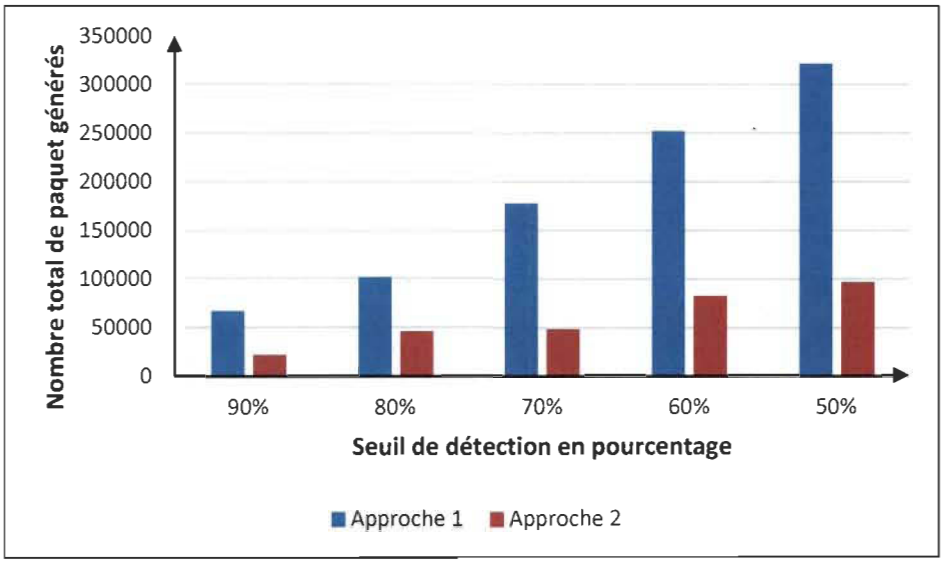


Figure 27 : Nombre total de paquet générés en fonction du seuil de détection – 50 nœuds.

4.3.5.2 Résultats pour une simulation avec 100 nœuds.

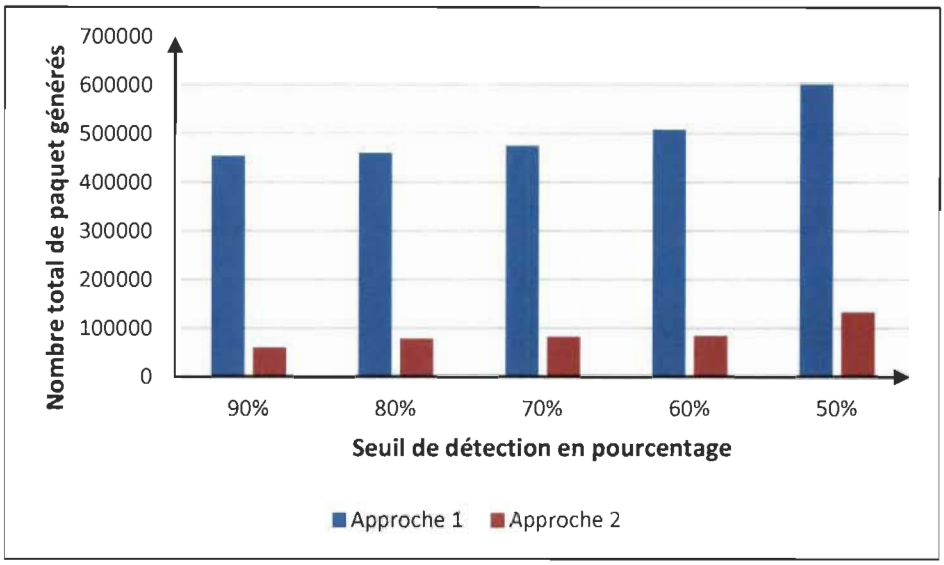


Figure 28 : Nombre total de paquet générés en fonction du seuil de détection – 100 nœuds.

4.3.5.3 Résultats pour une simulation avec 150 nœuds.

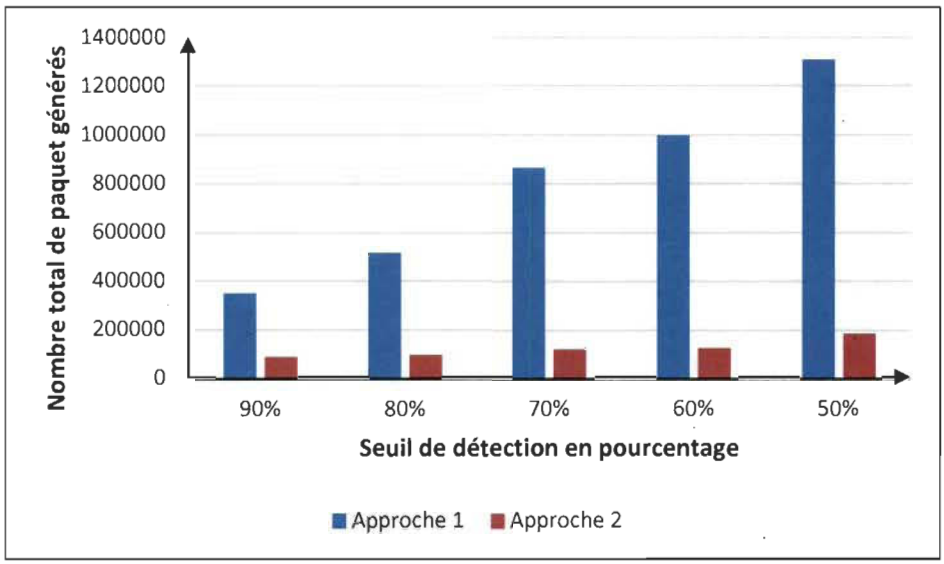


Figure 29 : Nombre total de paquet générés en fonction du seuil de détection – 150 nœuds.

4.3.6 CONCLUSION

D'après les résultats que nous avons obtenus et indépendamment du nombre de nœuds les conclusions que nous pouvons déduire reste les mêmes. L'approche IDS basée véhicule (Approche 1), détecte avec une plus grande efficacité les comportements anormaux des nœuds dans le réseau. De plus, elle permet avec une granularité fine de déterminer si une attaque est réellement en cours ou pas. Cette approche fournit une solution aux problèmes récurrents des IDS, à savoir, comment détecter les faux-positifs et les faux-négatifs. Néanmoins cette méthode à un coût, elle génère un grand nombre de paquets dans le réseau, ce qui nuit à la qualité de service. Préserver une bonne qualité de

service est l'un de nos problèmes. Cette solution ne sera pas retenue comme étant optimale. L'approche IDS basée RSU (Approche 2) est un compromis entre le nombre d'attaques détectés, le nombre d'attaques corroborées et le nombre de paquets total générés. En ce sens, elle correspond mieux à notre problématique de qualité de service. Néanmoins, elle ne permet pas de distinguer avec autant de précision les faux-positifs et les faux-négatifs.

CHAPITRE V - CONCLUSION

Ce travail a présenté les réseaux VANETs, leurs architectures, leurs caractéristiques, ainsi que les attaques auxquelles ils sont confrontés. Nous avons présenté des méthodes pour améliorer la sécurité, comme les méthodes de clusterisation, mais aussi les systèmes de détection d'intrusions pour détecter les attaques dans le réseau.

De nombreux problèmes de sécurité ont été présentés dans les réseaux VANETs, néanmoins, tous n'ont pas trouvé de solution à ce jour. Des méthodes de détection d'attaques ont été présentées, mais aucune n'inclus le RSU en coopération avec les véhicules. De plus, nous avons constaté que les IDS généraient des fausses alarmes. Nous avons proposé une solution à ces problèmes.

Dans ce travail, nous avons présenté un mécanisme d'aide à la décision pour les IDSs dans les réseaux VANETs. Nous avons utilisé une méthode d'IDS et une méthode de clusterisation. Nous avons eu pour objectif de faire corroborer une attaque détectée au sein d'un cluster. Nous avons défini deux méthodes, l'une basée sur les véhicules et l'autre basée sur les RSUs. Dans la première méthode, nous avons installé les IDSs à bord des véhicules, tandis que dans la seconde, nous avons installé les IDSs sur les RSUs. La corroboration d'une attaque est basée sur le calcul du ratio entre les véhicules ou entre les RSUs ayant répondu à la signature de l'attaque.

D'après les résultats obtenus, l'approche IDS basée véhicule détecte avec une très fine granularité les comportements anormaux. Elle permet également, lors de la corroboration d'une attaque, de valider si celle-ci est réellement en cours ou pas. Cette méthode solutionne le problème de faux-positif et faux-négatif. Néanmoins, comme nous avons pu le voir, le coût de la méthode est élevé. Elle génère un grand nombre de paquets dans le réseau, ce qui nuit à la qualité de service. La qualité de service étant l'une de nos considérations principales, la solution n'a pas été retenue comme optimale.

L'approche IDS basée RSU, est, comme nous l'avons vu un bon compromis entre le nombre d'attaques détectées, le nombre d'attaques corroborées et le nombre de paquets générés. Cette seconde approche a bien répondu à notre problème de qualité de service.

Le protocole présenté permet de nombreuses perspectives d'améliorations. L'une d'entre elle sera d'adapter et d'améliorer la méthode pour les milieux interurbains. Dans ces milieux, les risques d'attaques sont plus importants, dus à un plus grand nombre de véhicules (exemple : heure de grand trafic, congestion, etc.). Ceux-ci doivent être capables de s'adapter et de se protéger en cas d'une attaque corroborée. L'amélioration du cluster est également envisageable. Combiner cluster et politique de sécurité adéquate, sera une amélioration majeure pour le protocole. Une clusterisation réactive à la détection d'une attaque améliorera drastiquement la sécurité des réseaux VANETs. Une autre perspective sera d'utiliser un modèle mathématique permettant une corroboration de l'attaque plus rapide et réduisant ainsi le nombre total de paquets générés dans la méthode. Cette perspective améliorera grandement la qualité de service pour notre méthode.

BIBLIOGRAPHIE

[1] Panos Papadimitratos, JP Hubeaux; Securing Vehicular Communications, Maxim Raya. Wireless Communications, IEEE, Volume: 13, Issue: 5, 2006, Pages: 8 - 15.

[2] Jonathan Petit, Michael Feiri, Frank Kargl; Spoofed Data Detection in VANETS using Dynamic Thresholds. Vehicular Networking Conference (VNC), IEEE, Conference 14-16 Nov. 2011, Page(s): 25 - 32.

[3] Yong Hao, Jin Tang, Yu Cheng; Cooperative Sybillele Attack Detection for Position Based Applications in Privacy Preserved VANETs. Global Telecommunications Conference, IEEE, Conference: 5-9 Dec. 2011, Pages 1 - 5.

[4] Norbert Biβmeyer, Christian Stresing, Kpatcha M. Bayarou; Intrusion Detection in VANets Through Verification of Vehicle Movement Data. Vehicular Networking Conference (VNC), 2010 IEEE, Conference: 13-15 Dec. 2010, Jersey City, NJ, Pages: 166 - 173.

[5] Jyoti Grover, Manoj Singh Gaur, Vijay Laxmi; Position Forging Attacks in Vehicular Ad Hoc Networks: Implementation, Impact and Detection. Wireless Communications and Mobile Computing Conference (IWCMC), 2011 7th International, Conference: 4-8 July 2011, Conference Location: Istanbul, Pages: 701 - 706.

[6] Daxin Tiang, Yunpeng Wang, Guangquan Lu, Guizhen Yu; A Vehicular Ad Hoc Networks Intrusion Detection System Based on BUSNet. Future Computer and Communication (ICFCC), 2010 2nd International Conference, Date of Conference: 21-24 May 2010, Conference location: Wuhan, Pages: V1-225 - V1-229.

[7] Jorge Hortelano, Juan Carlos Ruiz, Pietro Manzoni; Evaluating the usefulness of watchdogs for intrusion detection in VANETS. Communications Workshops (ICC), 2010 IEEE International Conference, Date of Conference: 23-27 May 2010, Conference Location: Capetown, Pages: 1 - 5.

[8] Vadim D. Kotov, Vladimir I. Vasilyev; SIN'10 Immune Model Based Approach For Network Intrusion Detection. Proceedings of the 3rd international conference on Security of information and networks, ACM, 2010, Conference Location: New York, USA, Pages 233-237.

[9] Jiing Dong, Kurt E. Ackermann, Brett Bavar, Cristina Nita-Rotaru; Mitigating Attacks against Virtual Coordinate Based Routing in Wireless Sensor Networks. WiSec'08 Proceedings of the first ACM conference on Wireless network security, 2008, Conference Location New York, USA, Pages 89-99.

[10] Perkins, C.E; Ad-Hoc on demand distance vector routing. Sun Microsyst, Labs. Adv. Dev. Group, Menlo Park, CA Royer, E.M., Mobile Computing Systems and Applications, IEEE, Conference: 25-26 Feb 1999, Conference Location: New Orleans, LA, Pages: 90 - 100.

[11] Johnson, D.B; Routing in ad hoc networks of mobile hosts. Workshop on Mobile Computing Systems and Applications, Proceedings, Conference: 8-9 Dec 1994, Conference Location: Santa Cruz, CA, Pages: 158-163.

[12] Venkata Manoj D, M. M. Manohara Pai, Radhika M.Pai, Joseph MOUZNA; Traffic Monitoring and Routing in VANETs – A Cluster Based Approach. 11th International Conference on ITS Telecommunications (ITST), 2011, Conference: 23-25 Aug. 2011, Conference Location: St. Petersburg, Pages: 27 – 32.

[13] M. Boussedjra, J. Mouzna, H. Labiod, N. Maslekar; C-DRIVE: Clustering Based on Direction in Vehicular Environment. New Technologies, Mobility and Security (NTMS), 2011 4th IFIP, Conference: 7-10 Feb. 2011, Conference Location: Paris, Page(s): 1 – 5.

[14] Zhenxia Zhang, Azzedine Boukerche, Richard W.Pazzi; A Novel Multi-Hop Clustering Scheme for Vehicular Ad-hoc Networks. Proceedings of the 9th ACM International Symposium on Mobility Management and Wireless Access, 2011, Conference: 31oct-4Nov, Conference Location New York, USA, Pages: 19-26.

[15] O. Kayis, T. Acarman; Clustering Formation for Inter-Vehicle Communication. Intelligent Transportation Systems Conference, 2007, ITSC 2007. IEEE, Conference: Sept. 30-Oct. 3, Conference Location: Seattle, WA, Page(s): 636 – 641.

[16] M. Boussedjra, J. Mouzna, H. Labiod, N. Maslekar ; A Stable Clustering Algorithm for Efficiency Application in VANETs. Wireless Communications and Mobile Computing Conference (IWCMC), 2011 7th International, Conference: 4-8 July 2011, Conference Location: Istanbul, Page(s): 1188 – 1193.

[17] Tao Song, Weiwei Xia, Tiecheng Song, Lianfeng Shen; A Cluster-Based Directional Routing Protocol in VANET. International Conference on Communication Technology (ICCT), 2010 12th IEEE, Conference: 11-14 Nov. 2010, Conference Location: Nanjing, Page(s): 1172 – 1175.

[18] O. ABUMANSOOR, A. BOUKERCHE;A COOPERATIVE MULTI-HOP LOCATION VERIFICATION FOR NON LINE OF SIGHT (NLOS) IN VANET ; Wireless Communications and Networking Conference (WCNC), 2011 IEEE ; Date of Conference: 28-31 March 2011, Conference Location : Cancun, Quintana Roo ; Page(s): 773 – 778.

[19] M. Khanafer, M. Guennoun , H.T. Mouftah; Intrusion Detection for WSN-based Intelligent Transportation Systems; Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE ; Date of Conference: 6-10 Dec. 2010, Conference Location : Miami, FL; Page(s): 1-6.

[20] O. Abumansoor, A. Boukerche, Bjorn Landfeldt, Samer Samarah; Privacy preserving neighborhood awareness in VANET ; Q2SWinet'11; 2011 ACM; Date of Conference: 31Oct-4Nov. 2011, Conference Location : Miami, FL ; Page(s):17-20.

[21] S.M Safi, A. Movaghar, M. Mohammadizadeh ; A novel approach for avoiding wormhole attacks in VANET; International Conference on Internet, 2009. AH-ICI 2009. First Asian Himalayas; Date of Conference: 3-5 Nov. 2009, Conference Location: Kathmandu; Page(s):1-6.

[22] Jinyuan Sun, Yuguang Fang ; A defense technique against misbehavior in VANETs based on threshold authentification ; Military Communications Conference, 2008 MILCOM 2008, IEEE ; Date of Conference : 16-19 Nov. 2008, Conference Location : San Diego, CA ; Page(s) : 1-7.

[23] J. Sen, M.G Chandra, P. Balamuralidhar, S.G Harihara, H. Reddy ; A distributed protocol for detection packet dropping attack in mobile ad hoc networks; Telecommunications and Malaysia International Conference on Communications, 2007. ICT-MICC 2007. Date of Conference: 14-17 May 2007; Conference Location: Penang; Page(s):75-80.

[24] Noureddine CHAIB, « La sécurité des communications dans les réseaux VANET », Mémoire, Université ELHADJ LAKHDER-BATNA, FACULTE DES SCIENCES DE L'INGENIEUR DEPARTEMENT D'INFORMATIQUE, 05 Septembre 2011.

[25] Jonathan Petit, « Surcoût de l'authentification et du consensus dans la sécurité des réseaux sans fil véhiculaires », Thèse de Doctorat, Université de Toulouse, 13 Juillet 2011.

[26] Youngho Park and Kyung-Hyune Rhee, Chul Sur, "A Secure and Location Assurance Protocol for Location-Aware Services in VANETs", 50th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), pp.456-461, June 30 - July 2, 2011- Seoul, Korea.

[27] Hsin-Te, Wu, Wei-Shuo Li, Tung-Shih and Wen-Shyong Hsieh, " A Novel RSU-based Message Authentication Scheme for VANET", 50th International Conference on System and Networks Communications (ICSNC), pp.111-116, August 22-27, 2010-Nice, France.

[28] AuthentikCanada, code de la route du Canada, http://www.authentikcanada.com/code-route-canada/, date de dernière consultation, décembre 2013.

[29] Wikipédia, Wi-Fi, http://fr.wikipedia.org/wiki/Wi-Fi, date de dernière modification, janvier 2014.

[30] Transport Canada, Statistiques sur les collisions de la route au Canada en 2010, http://www.tc.gc.ca/fra/securiteroutiere/tp-1317.htm, date de dernière modification, décembre 2013.

[31] Wikipédia, Wireless LAN, http://en.wikipedia.org/wiki/Wireless_LAN, date de dernière modification, 4 janvier 2014.

[32] American Society for Testing and Materials (ASTM), http://www.astm.org/SNEWS/MAY_2004/dsrc_may04.html, date de dernière modification, mai 2004.

[33] Fan Li and Wang, "Routing in Vehicular Ad Hoc Networks: A Survey", IEEE Vehicular Technology Magazine Volume 2, pp. 12-22, June 2007.

[34] IEEE Standard 802.11p, « IEEE Standard for Information technology--Telecommunications and information exchange between systems--Local and metropolitan area networks--Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments », 2010.

[35] Arijit Khan, Shatrugna Sadhu, and Muralikrishna Yeleswarapu, "A comparative analysis of DSRC and 802.11 over Vehicular Ad hoc Networks"

[36] Wikipédia, Standard IEEE 802.11p, http://en.wikipedia.org/wiki/IEEE_802.11p, date de dernière modification, 28 décembre 2013.

[37] Christian TCHEPNDA, « Authentification dans les Réseaux Véhiculaires Opérés », Thèse de Doctorat, École Nationale Supérieure des Télécommunications Spécialité : Informatique et Réseaux, 18 Décembre 2008, Paris- France.

[38] Research and Innovative Technology Administration/Intelligent Transport System, http://www.standards.its.dot.gov, décembre 2013.

[39] Ahizoune Ahmed, « Un protocole de diffusion des messages dans les réseaux véhiculaires », Mémoire, Université de Montréal, Département d'informatique et de recherche opérationnelle, Faculté des arts et sciences, Avril 2011.

[40] Maxime Raya, Jean-Pierre Hubaux, ''The Security of Vehicular Ad Hoc Networks'', pp. 11-21, Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks (SASN '05), ACM New York, NY, USA, 2005

[41] Safi, S.M, Movaghar, A., Mohammadizadeh, M., A Novel Approach for Avoiding Wormhole Attacks in VANET, Second international workshop on Computer Science and Engineering, 2009. WCSE « 09. Date of Conference: 28-30 Oct.2009, Pages: 160-165. Conference Location: Qingdao.

[42] Jinyan Sun, Yuguang Fang,A defense technique against misbehavior in VANETs based on threshold authentication. IEEE Military Communications Conference, 2008. MILCOM 2008. Date of Conference: 16-19 November 2008. Pages: 1-7. Conference Location: San Diego, CA.

[43] Rawat D.B., Bista B.B, Gongjun Yan, Weigle M.C., Securing Vehicular Ad-hoc Networks Against Malicious Drivers: A Probabilistic Approach. International Conference on Complex, Intelligent and Software Intensive Systems (CISIS). Data of Conference: June 30 2011- July 2 2011. Pages: 146-151. Conference Location: Seoul.

[44] Chandra Rathore N., Verma S., Verma S., Tomar G.S., CMAC: A cluster based MAC protocol for VANETs. 2010 International Conference on Computer Information Systems and Industrial Management Applications (CISIM). Date of Conference: 8-10 Oct. 2010. Pages: 563-568. Conference Location: Krackow.

[45] Dandan Ren, Suguo Du, Haojin Zhu, A Novel Attack Tree Based Risk Assessment Approach for Location Privacy Preservation in the VANETs. 2011 IEEE International Conference on Communications (ICC). Date of Conference: 5-9 June 2011. Pages: 1-5. Conference Location: Kyoto.

[46] Wang Yizhi, Hu Jianming, Wang Qi, Zhang Yi, A Study of Distributed Traffic Information Acquisition Based on Clustered VANET. 2010 International Conference on Optoelectronics and Image Processing (ICOIP). Date of Conference: 11-12 Nov. 2010. Pages: 143-148. Conference Location: Haiko

[47] Osama Abumansoor, Azzedine Boukerche, Bjorn Landfeldt, Samer Samrah, Privacy preserving neighborhood awareness in vehicular ad hoc network. Q2SWinet « 11 Proceedings of the 7th ACM symposium on QoS and security for wireless and mobile networks. Date of Conference: October 31- November 4 2011. Pages: 17-20. Conference Location: Miami, US.

[48] Sabahi F., The Security of Vehicular Adhoc Networks. 2011Third International Conference on Computational Intelligence, Communication Systems and Networks (CICSyN). Date of Conference: 26-28 July 2011. Pages: 338-342. Conference Location: Bali.

[49] Samara G., Alsalihy, W.A.H.A, A New Security Mechanism for vehicular communication networks. 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec). Date of Conference: 26-28 June 2012. Pages:

18-22. Conference Location: Kuala Lumpur.

[50] Gongjun Yan, Bista B.B, Rawat D.B., Shaner E.F, General Active Position Detectors Protect VANET security. 2011 International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA). Date of Conference: 26-28 Oct. 2011. Pages: 11-17. Conference Location: Barcelona.

[51] Hamieh A., Ben-othman J., Mokdad L., Detection of Radio Interference Attacks in VANET. Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE. Date of Conference: Nov 30 2009-Dec. 4 2009. Pages: 1-5. Conference Location: Honolulu, HI.

[52] Nai-Wei Lo, Hsiao-Chien Tsai, Illusion Attack on VANET Applications - A Message Plausibility Problem. 2007 IEEE, Globecom Workshops. Date of Conference: 26-30 Nov. 2007. Pages: 1-8. Conference Location: Washington, DC.

[53] Guette G., Ducourthial B., On the Sybillele attack detection in VANET. IEEE International Conference on Mobile Adhoc and Sensor Systems, 2007. MASS 2007. Date of Conference: 8-11 Oct. 2007. Pages: 1-6. Conference Location: Pisa.

[54] Gazdar T., Benslimane A., Belghith A., Secure Clustering Scheme Based Keys Management in VANETs. Vehicular Technology Conference (VTC Spring), 2011 IEEE 73rd. Date of Conference: 15-18 May 2011. Pages: 1-5. Conference Location: Yokohama.

[55] Moslah J., Azzouz L.B., Security services for eSafety applications clusters. Wireless Communications and Mobile Computing Conference (IWCMC), 2011 7th International. Date of Conference: 4-8 July 2011. Pages: 707-712. Conference Location: Istanbul.

[56] Yuyi Luo, Wei Zhang, Yangqing Hu, A New Cluster Based Routing Protocol for VANET. Second International Conference on Networks Security Wireless Communications and Trusted Computing (NSWCTC), 2010. Date of Conference: 24-25 April 2010. Pages: 176-180. Conference Location: Wuhan, Hubei.

ANNEXE 1: POSTERS

Poster 1:

Romain Coussement, Boucif Amar Bensaber, Ismail Biskri, Routing protocol for security information in VANET networks. Second NSERC DIVA WORKSHOP; August 30-31, 2012. Location: Ottawa.

Poster 2:

Romain Coussement, Boucif Amar Bensaber, Ismail Biskri, Modeling of a Decision Support Protocol for IDS in VANET. Third NSERC DIVA Workshop, November 12-13, 2013. Location: Ottawa.

Routing protocol of security information in VANET networks

Romain Coussement, Boucif Amar Bensaber, Ismail Biskri
Laboratoire de mathématique et informatique LAMIA
Department of Mathematics and Computer Science, UQTR
{Romain.Coussement|Boucif.Amar.Bensaber|Ismail.Biskri} @uqtr.ca

Abstract

This document wants to show a proof of concept of a security information routing protocol. The protocol routes security information after discovering an attack and broadcasts it to the closest neighbours. In this work, first, we will use clustering algorithm and then we compare our method with different intrusion detection system and routing protocols that broadcast efficiently information when an attack occurred. We will determine metrics for the maximum cluster range and the optimal method to broadcast messages, from vehicle to vehicle or vehicle to infrastructure.

Protocol Component

We will use intrusion detection system to detect that an attack has occurred or is ongoing. The dynamic topology of VANET allows a strong prevention by broadcasting the information. When the IDS detects an attack, we will broadcast this information and the type of the attack used to neighbors clusters directly in front and directly behind us. When neighbors clusters receive information a new security policies could be set up. The method was designed on the road and out of urban areas.

Definition of the Intrusions Detection System

We choose to take two different IDS, the first making detections on vehicles, and the other one on the Road Side Units (RSU). We will then compare the two methods of intrusion detection to see which one fits our method best.

Assumptions

To maintain consistency in our results, following assumptions will be installed for this work.

- The RSU are reliable.
- The RSU are in communication range.
- Each vehicle is part of a cluster. When an attack occurs we know that it comes from an inner zone or close to the cluster.
- The exchange of data between vehicles, vehicles to RSUs and RSUs to RSUs is secure. The connection is encrypted.
- Exchanged data can't be modified.
- Each RSU knows the number of vehicles in his area at time t. We then have a material traceability of vehicle movement from one cluster to another or during area changing.

Metrics

We initially focused on the metric of broadcasting range. According to 802.11p standard, RSU can approximately emit in a range of 1000 meters. In our method RSUs would be in the transmission range of each other. This metric is thus difficult to define.

When a cluster head inform the RSU that an attack occurred, this process will be executed:

- With information on other clusters, the RSU can estimate the number of vehicles on the road in its area and the range between each of the clusters at time t. The RSU must determine which method to use to broadcast as quickly as possible the information of attack.
- Broadcasting would be through the RSU if clusters are too distant or between vehicles if they are within range.
- It will then calculate with information from its tables if the clusters are reachable from an area with clusters from the current zone.
- A request of broadcasting information is sent from vehicle to RSU, which confirm the method of sending data.
- When the first vehicle of the attacked cluster is in range of the last vehicle of the next cluster, attack information is broadcast vehicle to vehicle otherwise the information is sent by the RSU.

Cluster definition

The first step of our work is to define the cluster. A group of vehicles must be self-defined as a cluster on the road, moreover it must also be able to elect a cluster head to allow communication with the RSU. The cluster is used to gather vehicles and therefore the information transmitted by the group. The cluster head is a bridge to the RSU who also store information about its clusters. The information stored is then send to the RSUs.

Definition of the routing protocol

In our knowledge there is no information security routing protocol for VANET. We will use protocols like AODV or DSR to support information to broadcast, other routing protocols could also be used. Both of these protocols have already proved themselves and are effective, and despite their distinct known weaknesses, compare them according to our security approach could be a considerable asset.

Internal mechanisms

The internal mechanisms of this protocol are presented as follows:

- Vehicles in a cluster will elect a cluster head. The cluster head will be in charge of the information table about the next and the previous cluster.
- The RSU will collect and broadcast information to the cluster head in its area. It will ask to closest RSU if there is cluster near his area.
- When a vehicle in a cluster identifies an attack, it will send to its cluster head what kind and what type of attack it has detected. Then the information is sent from the cluster head to the RSU of the area, which broadcasts again the information to closest clusters.
- When the attacked cluster loses one of his members, it will broadcast the loss of this member to the closest cluster. These last can then establish a specific policy towards the new member.
- Each RSU is in communication range, so they can requests for information from other close RSU at time t.

The information that an new vehicle comes from a attacked cluster, comes from the RSU which knows the position of vehicles in its area.

Information about the cluster at the RSU are defined below:

Notation	Description
Nb_veh	Number of vehicles in the cluster.
Pos_CH	GPS position of the cluster head.
Pos_CF	GPS position of the first vehicle in the current cluster.
Pos_CL	GPS position of the last vehicle in the current cluster.

Information of RSU to RSUs are defined below:

Pos_NRSU_L	GPS position of the last vehicle in the next RSU area.
Pos_PRSU_F	GPS position of the first vehicle in the previous RSU area.

Conclusion

We have presented a proof of conception of security information in VANETs. Our future work is to define rules for clusters and security policy. We will simulate this approach with simulator (SUMO, NS-3). Our aim if to find the best metrics to preserve the quality of service.

REFERENCES

- Maxim Raya, Panos Papadimitratos, JP Hubeaux.,"Securing Vehicular Communications", Wireless Communications, IEEE, Volume: 13, Issue: 5, 2006, Pages: 8 - 15.
- Daxin Tiang, Yunpeng Wang, Guangquan Lu, Guizhen Yu., "A Vehicular Ad Hoc Networks Intrusion Detection System Based on BUSNet",, Future Computer and Communication (ICFCC), 2nd International Conference on, Conference: 21-24 May 2010, Pages: V1-225 - V1-229.
- Jorge Hortelano, Juan Carlos Ruiz, Pietro Manzoni., "Evaluating the usefulness of watchdogs for intrusion detection in VANETS", Communications Workshops, IEEE International Conference on, Conference: 23-27 May 2010, Pages: 1 - 5.

Modeling of a Decision Support Protocol for IDS in VANET

Romain Coussement, Boucif Amar Bensaber, Ismail Biskri
Laboratoire de mathématique et informatique LAMIA
Department of Mathematics and Computer Science, UQTR
{Romain.Coussement|Boucif.Amar.Bensaber|Ismail.Biskri} @uqtr.ca

Abstract

The Intrusion Detection System (IDS) can detect malicious actions made to systems. However, without a decision making mechanism, they are useless. We design a decision making protocol for security information in Vehicular Networks (VANETs).

We propose two methods :

- In the first one, IDS are installed on vehicles
- In the second one, they are installed on the Road Side Units (RSU).

Both approaches use a clustering method based on vehicle speed. Corroboration of an attack is based on computation between vehicles or RSUs having answered to the signature of the attack. So when an attack occurs, the protocol allows the corroboration of the latter and alert neighboring clusters.

Clustering method

We use the clustering passive approach defined in [2] and we adapted it. Each vehicle is clustered according to its velocity and its speed group.

Clustering process flow

Assumptions done for both method of the protocol

- The RSUs are in communication range.
- Each vehicle is part of a cluster. When an attack occurs, we know that it comes from an inner zone or closer zone to the cluster.
- Exchanged data cannot be altered.
- Each RSU knows the number of vehicles in its area at time t. We also have a material traceability of vehicle movements from one cluster to another or during area changing.

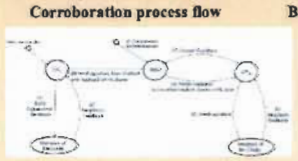
Assumptions of the protocol component

First method, IDS based RSU :

- The cluster already exists and the Cluster Head (CH) is elected.
- The exchange between the cluster and the IDS based RSU are:
  - Packets from vehicles are sent to the CH.
  - The CH forwards all the packets to the RSU.
  - IDS are installed on the RSU. Normal packets are retransmitted to the receiver to be read. When an attack is detected the CH is alerted.

Method 1, IDS based RSU

Corroboration process flow



Broadcasting of the information

Second method, IDS based vehicle:

- There is one IDS installed on each vehicle.
- The communication between vehicles and vehicles to RSUs is encrypted.
- RSUs are reliable.
- All the generated alerts given by the RSU are considered as true. When the IDS detect something it always considers it true. The false positive problem is handle by the numerous IDS in the network. If an IDS doesn't detect the attack, another will probably detects it.

Method 2, IDS based vehicle

Corroboration process flow

Broadcasting of the information

Simple method to corroborate an attack

$$P_{Attack} = \frac{Nb_{detection}}{Nb_{veh_{total}}}$$

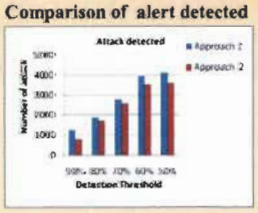
Where:

- P_{Attack} is the corroboration probability of the attack.
- $Nb\_detection$ is the number of vehicles having detected the attack.
- Nb_veh_total is the total number of vehicles who have given their feedback.

Simulation

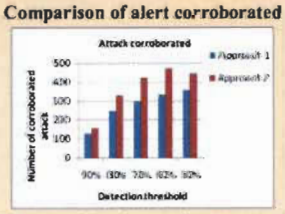
The simulation has been done with OMNET++ 4.2.2 under Windows 7 system. We have simulate on a 5km highway with input and output. The two approaches were done with 50 nodes and 19 fixed nodes that have the role of RSU. We have set the detection threshold between 50 and 90%.

Comparison of alert detected



The numbers of attacks increased depending on the detection threshold. Method 1 have much more IDS than method 2 so much more alerts.

Comparison of alert corroborated



The approach 1 is better to detects attacks but remain less efficient than approach 2 to corroborate efficiently an attack. RSUs generate fewer alerts and are not yet overloaded by the packet processing.

Conclusion

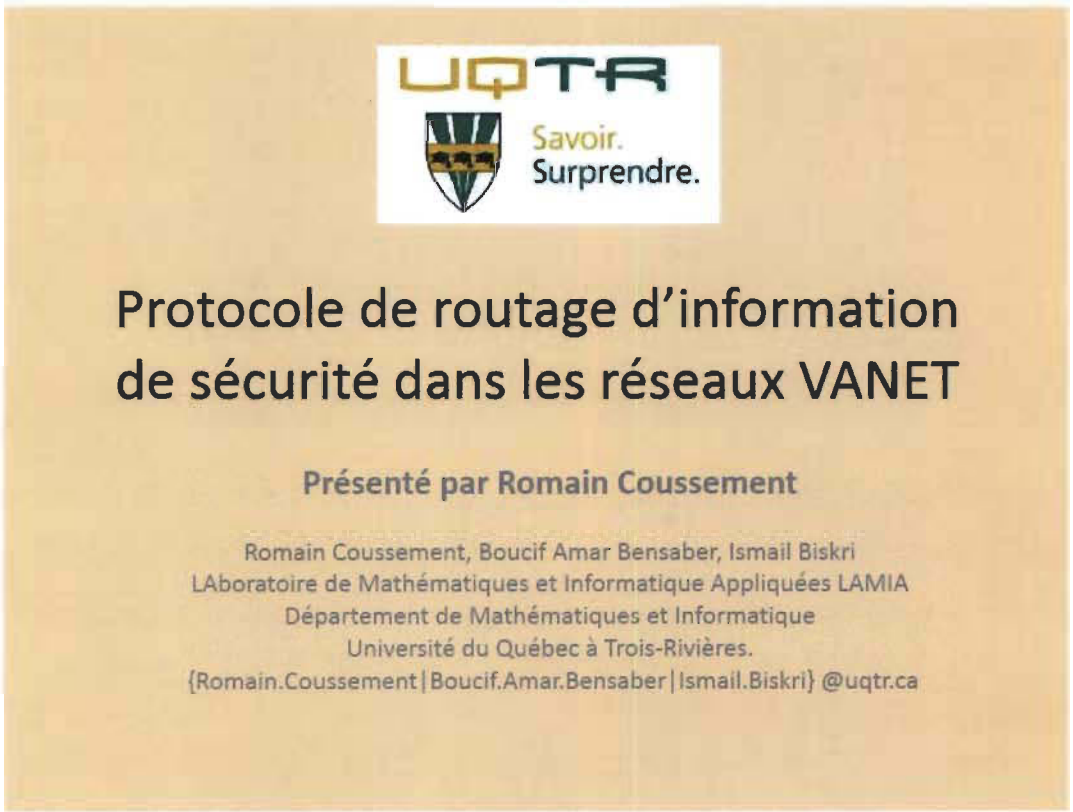
We have presented a modeling of a decision support protocol for IDS in VANET. Our future work could adapt it in urban areas. Improvement like clustering the RSUs among themselves or with vehicles is an approach which could be considered.

References

- [1] Maxim Raya, Panos Papadimitratos, JP Hubeaux, "Securing Vehicular Communications", Wireless Communications, IEEE, Volume: 13, Issue: 5, 2006, Pages: 8 - 15.
- [2] Daxin Tiang, Yunpeng Wang, Guangquan Lu, Guizhen Yu, "A Vehicular Ad Hoc Networks Intrusion Detection System Based on BUSNet", Future Computer and Communication (ICFCC), 2nd International Conference on, Conference: 21-24 May 2010, Pages: V1-225 - V1-229.
- [3] Tao Song, Weiwei Xia, Tiecheng Song, Lianfeng Shen; A Cluster-Based Directional Routing Protocol in VANET. Communication Technology (ICCT), 2010 12th IEEE International Conference on, Conference: 11-14 Nov. 2010, Page(s): 1172 - 1175.

ANNEXE 2 : COMMUNICATION

Romain Coussement, Boucif Amar Bensaber, Ismail Biskri, Protocole de routage d'information de sécurité dans les réseaux VANET. Technologie de l'information et des communications, nouvelles avancées technologique, 81ème congrès de lACFAS, Québec 2013.



Plan

- Introduction aux réseaux VANETs.
- Attaque, détection et clusterisation dans VANETs.
- Notre solution.
- Conclusion.

INTRODUCTION AUX RÉSEAUX VANETS

Introduction

- VANet : Vehicular Adhoc Network
- Ce type de réseau dérive des Wifi, MANet (Mobile Adhoc Network) et autres réseaux sans fil.

Introduction

- Les réseaux véhiculaires sans fil VANets nécessitent deux équipements pour fonctionner:
  - RSU : Road Side Unit
  - OBU : On Board Unit.

Exemple d'un réseau véhiculaire

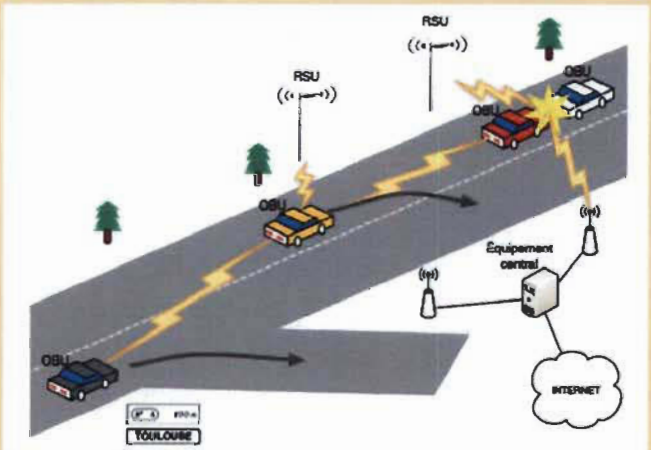


Figure 1-1. Exemple de réseau véhiculaire [LIN 06]

Objectifs

- Objectifs des VANets :
  - Fournir les informations sur le trafic.
  - Proposer des services (divertissement, informations sur les hôtels ou des restaurants,...)
  - Ordonner le trafic routier.

Caractéristiques Techniques

- Norme de VANet :
  - 802.11p (découle du 802.11a et du 802.11e)
  - 1609.2 (Spécification de sécurité)

Caractéristiques Techniques

- DSRC (dedicated short range communications):
  - Communication des OBU jusqu'à 500m
  - Communication des RSU jusqu'à 1000m

Caractéristiques Techniques

- Utilisation des protocoles basés sur les recommandations 1609 définissant :
  - Le format de sécurité des messages sécurisés pour le système DSRC/WAVE.
  - Les méthodes pour sécuriser les messages de gestion et d'application.
  - Les procédures que doit accomplir le véhicule afin d'assurer les services de sécurité (authentification, confidentialité, intégrité, non répudiation).

Caractéristiques Techniques

- Les réseaux VANETs permettent 2 types de communication :
  - La communication véhicule à véhicule (V2V).
  - La communication véhicule à infrastructure.

Caractéristiques Techniques

- Les différents type de messages :
  - Messages de contrôle
  - Messages d'alerte
  - Autres messages

Caractéristiques Techniques

- On peut classer les applications présentes dans les réseaux VANETs en trois classes :
  - Application de gestion du trafic routier
  - Application de confort
  - Application de sécurité du trafic routier

ATTAQUES, DÉTECTION D'INTRUSIONS ET CLUSTERISATION

Les attaques dans VANET

- Les principales attaques possibles dans VANET sont :
  - Attaque sur la cohérence de l'information.
  - Attaque sur la vie privée.
  - Usurpation d'identité.
  - Déni de service.
  - Écoute de communication.
  - Les attaques Sybiles.

Les systèmes de détection d'intrusions

- Pour déceler les attaques, nous utilisons des systèmes de détection d'intrusions (IDS).

- Il existe deux méthodes de détection pour les IDS:
  - Les mécanismes basés sur les signatures
  - La recherche de motif dangereux.

La clustérisation

- La clustérisation est un concept visant à regrouper des entités (ordinateur), appelé également nœud.
- La clustérisation permet d'améliorer la qualité des services proposés mais également la sécurité des véhicules.
- Il existe deux types de clustérisation :
  - Passive
  - Active.

État de l'art

- [1] Panos Papadimitratos, JP Hubeaux, « Securing Vehicular Communications ». L'article liste des attaques sur les réseaux VANET. Il propose une méthode pour contrer les attaques de «création de paquets» en utilisant un mécanisme de corrélation des données.

- [2] Daxin Tiang, Yunpeng Wang, Guangquan Lu, Guizhen Yu, « A Vehicular Ad Hoc Networks IDS Based on BUSNet », définit un IDS basé sur les têtes de cluster formant un bus de nœuds. Les bus de nœuds sont les intermédiaires entre le cluster et le RSU. Le RSU a alors une vision globale du réseau VANET et peut alors détecter les anomalies avec les données analysées.

- [3] M. Boussedjra, J. Mouzna, H. Labiod, N. Maslekar, « C-DRIVE: Clustering Based on Direction in Vehicular Environment». Les auteurs présentent aussi des méthodes de clustérisation pour les zones urbaines, en utilisant les coordonnées GPS et la direction du véhicule grâce à des cartes électroniques.

Problématique

- Dans les réseaux VANETs de nombreuses attaques ont été recensées, néanmoins la littérature ne propose pas de solution pour toutes.
- Les IDS sont chargés d'analyser le trafic entrant et sortant pour identifier les signatures malicieuses. Néanmoins sans mécanisme de prise de décision ils n'ont aucune utilité.

But de notre travail

- Concevoir un protocole de routage d'informations de sécurité pour les VANETs.

NOTRE SOLUTION

Méthode proposée

- Notre étude se base sur deux approches d'IDS.
- Dans la première, les IDS sont installés sur les véhicules, alors que dans la seconde, ils sont installés sur les infrastructures routières (RSU).
- Dans les deux approches, les véhicules sont regroupés en fonction de leurs vitesses.
- Si un véhicule souhaite communiquer, il doit faire partie d'un cluster et doit connaître la tête du cluster. Dans le cas contraire, l'algorithme de clustérisation s'initialise et l'élection de la tête du cluster s'amorce. Ce dernier a la charge de transmettre les paquets à l'interne du cluster, vers les clusters voisins et vers le RSU.
- Quand un IDS détecte une attaque, l'information et le type d'attaque utilisé seront diffusés aux clusters voisins.
- Le protocole s'amorce si l'attaque détectée est corroborée. La corroboration s'appuie sur un modèle probabiliste de calcul de ratio entre les véhicules ayant répondu à la signature de l'attaque.

Comment sont créés les clusters?

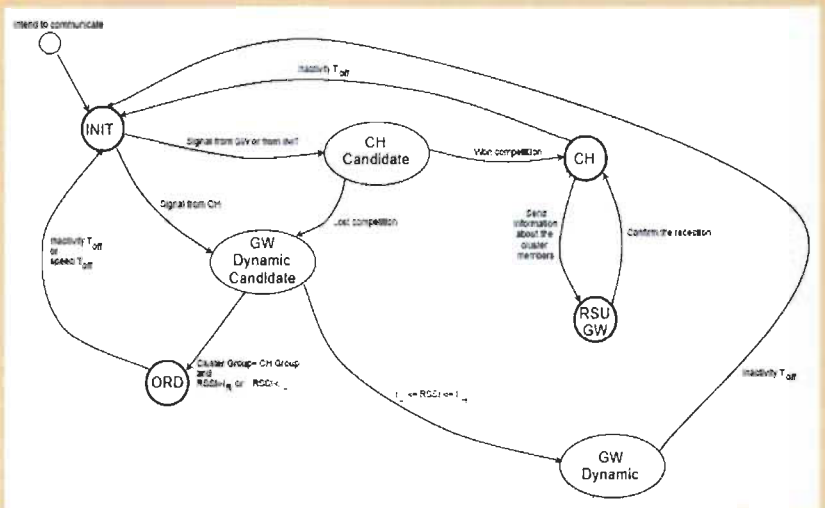
Speed interval (kmph)	Speed group	Clustering Group
0 - 30	0	0
30 - 45	1	1
45 - 60	2	1
60 - 75	3	2
75 - 90	4	2
90 - 110	5	2
110 – 120	6	3
120+	7	3

Table des relations entre : intervalle de vitesse, vitesse de groupe et groupe de cluster.

Quelques définitions

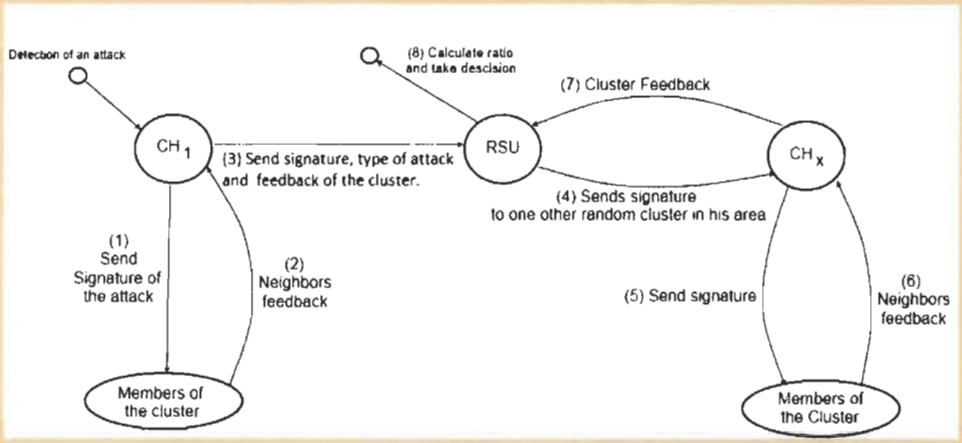
- INIT (Initial) : Chaque véhicule commence dans cet état initial.
- CH (Cluster Head) : Il est en charge de faire suivre les paquets des véhicules. L'élection du CH est simple, le premier véhicule qui l'annonce devient CH.
- ORD (Ordinary) : Un véhicule clusterisé est par défaut dans cet état.
- GW (Gateway) : Le CH élit un véhicule dans l'état ORD afin qu'il retransmettent les paquets du cluster.

Élection des états du cluster



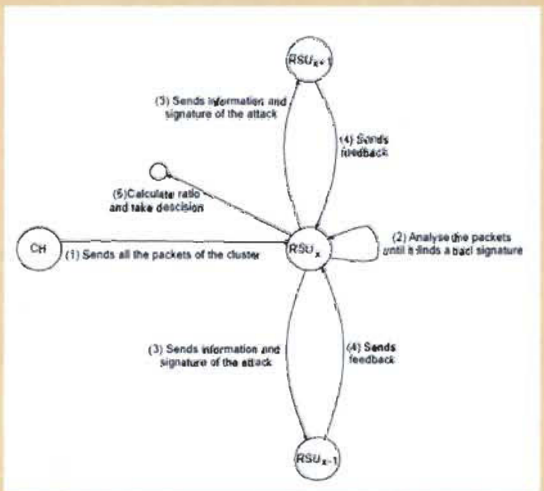
Déroulement du processus de Clusterisation

Méthode de corroboration basée véhicule



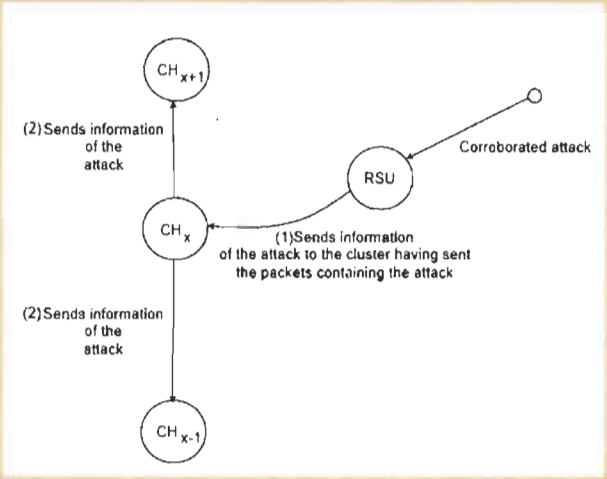
Déroulement du processus de corroboration basé véhicule.

Méthode de corroboration basée infrastructure



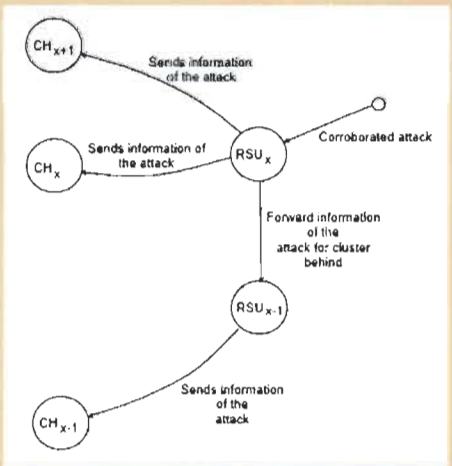
Déroulement du processus de corroboration basé infrastructure

Routage des informations de sécurité



Diffusion de l'information d'une attaque corroborée en mode V2V

Routage des informations de sécurité



Diffusion de l'information d'une attaque corroborée en mode I2V.

Conclusion

- Nous avons présenté un protocole de routage d'information de sécurité.
- Notre méthode est en cours d'implémentation avec le simulateur OMNeT++.
- Les études suivantes sont envisagées :
  - L'adaptation et la simulation de notre méthode en milieu urbain
  - Clusterisé les RSUs entre eux ou avec les véhicules sont des approches qui peuvent être considérées pour améliorer la dissemination des paquets sur l'autoroute ou en zone urbaine.

Références

- [1] Panos Papadimitratos, JP Hubeaux; Securing Vehicular Communications, Maxim Raya. Wireless Communications, IEEE, Volume: 13, Issue: 5, 2006, Pages: 8 - 15.
- [2] Daxin Tiang, Yunpeng Wang, Guangquan Lu, Guizhen Yu; A Vehicular Ad Hoc Networks Intrusion Detection System Based on BUSNet. Future Computer and Communication (ICFCC), 2010 2nd International Conference, Date of Conference: 21-24 May 2010, Conference location : Wuhan, Pages: V1-225 - V1-229.
- [3] M. Boussedjra, J. Mouzna, H. Labiod, N. Maslekar; C-DRIVE: Clustering Based on Direction in Vehicular Environment. New Technologies, Mobility and Security (NTMS), 2011 4th IFIP, Conference: 7-10 Feb. 2011, Conference Location : Paris, Page(s): 1 – 5.

ANNEXE 3: PUBLICATION

Romain Coussement*, Boucif Amar Bensaber, Ismail Biskri, «Decision support for intrusion detection in VANETs», DIVANet '13, Proceedings of the second ACM international symposium on Design and analysis of intelligent vehicular networks and applications (16th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems), ISBN: 978-1-4503-2359-8, November 3-8, 2013, Barcelona, Spain, Pages: 31-38.

Decision support protocol for intrusion detection in VANETs

Romain Coussement
Laboratoire de Mathématiques et Informatique appliquées LAMIA
Department of Mathematics and Computer Science
University of Quebec at Trois-Rivieres,
Trois-Rivieres, Qc, Canada
1 819 3765011 ext. 3831
Romain.Coussement@uqtr.ca

Boucif Amar Bensaber
Laboratoire de Mathématiques et Informatique appliquées LAMIA
Department of Mathematics and Computer Science
University of Quebec at Trois-Rivieres,
Trois-Rivieres, Qc, Canada
1 819 3765011 ext. 3807
Boucif.Amar.Bensaber@uqtr.ca

Ismail Biskri
Laboratoire de Mathématiques et Informatique appliquées LAMIA
Department of Mathematics and Computer Science
University of Quebec at Trois-Rivieres,
Trois-Rivieres, Qc, Canada
1 819 3765011 ext. 3837
Ismail.Biskri@uqtr.ca

ABSTRACT

Vehicular Ad hoc Networks (VANETs) are so difficult to secure due to the wireless technology and its several known security holes. To protect against attacks, methods and techniques have been developed. The Intrusion Detection System (IDS) can detect malicious actions made to the system. In vehicular ad hoc networks, IDSs are in charge of analyzing incoming and outgoing packets to identify malicious signatures. However, without a decision making mechanism, they are useless. This paper designs a decision making protocol for security information in VANETs. Our study is based on two IDS approaches. In the first one, the IDS are installed on vehicles, while in the second one they are installed on the Road Side Units (RSU). In both approaches, vehicles are grouped according to their speed. Corroboration of an attack is based on a probabilistic model of ratio computation between vehicles or RSUs having answered to the signature of the attack. Our aim is to design a decision support mechanism. The dynamic topology of VANET allows a strong prevention by broadcasting the information. So when an attack occurs, the protocol allows the corroboration of the latter and alert neighboring clusters.

DIVANet'13, November 3–8, 2013, Barcelona, Spain.

DOI string from ACM form confirmation

Categories and Subject Descriptors

C.2.2 [**Network Protocols**]

General Terms

Security

Keywords

VANET, Security, Cluster, Routing protocol, Intrusion Detection System, Probabilistic Model.

1. INTRODUCTION

Vehicular Ad-Hoc Network (VANET) is a form of Mobile Ad-hoc Network (MANET), it provides communications among vehicles and between vehicles and the Road Side Unit (RSU).

Considering the importance of services in VANET, the security measures and the intrusion detection represent a growing research axis. Attacks are numerous (Jamming, Denial of Services, Wormhole, packet forgery, etc.) and the solutions proposed in the literature don't overcome all the problems. The Intrusions Detections Systems (IDS) are the last line of defense after an attack occurs. They are in charge of analyzing incoming and outgoing packets to identify malicious signatures. In VANETs, there are several IDS approaches and due to the generation of false negative / false positive by IDS, we have to reduce the impact of false alarms in the network; without a decision making mechanism, it's impossible.

The aim of our work is to design a decision support mechanism based on member corroboration. When an attack is corroborated by many nodes, there is a high probability to be a true attack. We will develop a decision making protocol for security information in VANETs. This solution haven't been proposed yet in the literature for VANETs.

Our study is about several intrinsic issues defined as follows. Section 2 describes the related work of attack techniques, IDS and clustering methods. In section 3, we present our protocol. Some preliminary results are presented in section 4. Finally in section 4, we conclude and present our future works.

2. STATE OF THE ART

The study and the definition of new kind of attacks and the establishment of new technical method to parry them is an important open axis of research. Many works in the literature integrate intrusion detection system (IDS) to secure VANETs but a lot of recurrent security problems still remain [1] (Spoofing, Denial of Services, Jamming, etc.) and have no solution yet. Our study focuses on several of these inherent problems.

In [1], the authors present a list of the different kind of attacks and vulnerabilities in VANET. They proposed a method to parry the "packet forgery" attacks using a mechanism for correlating the data. They also propose to use multiple transceivers operating in disjoint frequency bands to counter DoS attacks (Deny of Services) like jamming. In [2], the authors present a mechanism based on dynamic threshold. Their method allows a vehicle to give his trust on the neighboring nodes. Trust of nodes on the road allows distinguishing two types of information from two different sources to make the right decision on the behavior to adopt. In [3], the authors present a method to detect Sybil Attacks cooperatively. Each vehicle stores the position of its nearest neighbors. When the position of one vehicle in the network is not known by the others, the protocol refers it as Sybil node. In [4], the authors propose to detect false congestion using a plausibility model for the detection of false vehicle even if their movements are credible. In [5], the authors present attacks based on the creation of multiple identities on the road and they propose a method to detect them. The RSUs calculate vehicle's speed based on "Beacon" messages sent periodically. When the RSU notices an anomaly, it considers this as false vehicle. In [6], the authors define an IDS based on cluster heads forming a bus node (intermediate between the cluster and the RSU). Information is transmitted to the RSU and it has then a global vision of the network and can also detect anomalies. In [7], the authors propose a "watchdog" technique based on the trust level of neighbors. The IDS defines trust in retrieving all received packets and calculating the ratio between the received packets and the retransmitted packets. To overcome the problem of false positives and false negatives, the authors have introduced mechanisms based on tolerance or devaluation thresholds. However, the threshold based on trust are not yet reliable, their method works only locally without forwarding any information and doesn't use clustering to improve security of the VANET. There are many approaches defining intrusion detection system, many of them are not yet conceptualized for VANET. Even if the IDSs are needed for VANETs, it is not enough, there must be a mechanism to help decision making, and otherwise IDSs are useless. In [8], the authors present an IDS based on immunocomputing. They use a negative selection algorithm with a model of normal behavior to train its sensor and adapt it to new kind of attacks.

Combined with intrusions detection system, the clustering methods are widely useful. A Clustering method allows improved security in VANETs most of the time, defining a vehicle group to exchange data. In [14], the authors propose a multi-hop clustering model. The method is based on rapid dissemination of information but requires more control. Many vehicles enter and leave the cluster and an attack would do lots of damage. In [12], each vehicle knows his GPS localization. The cluster is created based on the direction and the distance of vehicles. The cluster head is elected by having the best dissemination of data in the cluster. In [13, 16], the authors present clustering method in urban areas, using GPS coordinates and the direction of the vehicle. These methods are useful in the highway area because they reduce the formation of clusters. But as in [12], you can't determine beforehand the direction and the journey of vehicles. In [17], the authors propose a method for highways where vehicles having the same direction are clustered. The road is divided into sections where each vehicle is clustered generating a lot of input/output in clusters and making the method unstable. In [15], the authors present a passive approach of clustering based on the vehicle's speed. Vehicles belonging to the same speed range are part of the same group. Cluster formation occurs when a vehicle wants to communicate with other vehicles in the same group velocity as it.

Finally, there are lots of methods for detecting attacks but none includes the RSU in cooperation with vehicles to build a strong and preventive attack detection system. Likewise, it might be interesting to have IDS able to quickly broadcast information about an attack on several kilometers to improve prevention and set new IDS's policies.

In the next section, we will present our protocol that uses two IDS approaches and a clustering method to increase security in VANETs. Our study is based on two IDS approaches. In the first one, IDSs are installed on vehicles, while in the second one they are installed on the RSUs. The different approaches use a clustering specific technique to group vehicles according to their velocities. If a vehicle wants to communicate, it must be part of a cluster and must know the cluster head. Otherwise, the clustering algorithm is initialized and the selection of the cluster head starts. In the first approach, the cluster head is responsible for forwarding packets to the members of its cluster, to the neighboring clusters and to the RSU. When an IDS detects an attack, the information and the type of attack used will be broadcasted to neighboring clusters by the RSU and the vehicles. In the second approach all the emitted packets by clusters are forwarded to RSUs. These latter will corroborate the attack with RSUs in scope and send an alert to the cluster head in the area. In both methods, when a positive corroboration is done, the cluster head sets up a security policy (e.g.: adjusting the trust values of vehicles coming in the cluster). The protocol is initiated when the attack is detected.

3. PROTOCOL COMPONENT

In this work, we will use an IDS to detect that an attack has occurred or is ongoing. When an IDS detects an attack, it will broadcast this information and the type of the attack used to neighboring clusters directly in front and directly behind it. When neighboring clusters receive information, a new security policy could be set up.

We initially adapt the clustering method described in [15]. It presents interesting characteristics of our method that we explain below. The first part of our work is the adaptation of the cluster. We will explain how it works and then we will present what we add on.

3.1 Cluster definition

A group of vehicles must be self-defined as a cluster on the road; moreover a group of vehicles must be able to elect a cluster head to allow communication with the RSU. The cluster head has a specific role; it is a bridge to the RSU who also stores information about its clusters. The information stored is then sent to the other RSUs. Information has a key role in this method.

The cluster algorithm that we use will meet the following characteristics:

- Simple to use. We can easily use it, put in place, modify adapt it to our needs.

- Give good cluster stability, once formed a cluster must remain as long as possible. Moreover, it provides a better control of the activity in our cluster.
- Be able to give a good estimation of vehicle's density. The more information we have about vehicle's density, the more control and security in our clusters we gain.

Has common characteristics with the initial scheme described in [15]. The goal is to have a simple and efficient method.

3.2 Cluster mechanism

Initially, the method uses a clustering passive method. The cluster is done automatically according to the velocity of vehicles. Authors proposed a static table making correspondence between cluster and velocity [15]. Their assumptions are: each vehicle knows his position and his velocity with the Global Positioning System (GPS). So each vehicle in the same velocity categories can be clustered together.

Speed interval (kmph)	Speed group	Clustering Group
0 - 30	0	0
30 - 45	1	1
45 - 60	2	1
60 - 75	3	2
75 - 90	4	2
90 - 110	5	2
110 – 120	6	3
120+	7	3

Table 1: Speed group/Clustering Group relationship used [15]

Their method uses speed interval, speed group and clustering group as in Figure 1. They mentioned only 3 clustering groups possible, to allow a reduction of packet overhead and communication between groups. If two different groups want to communicate, they will use the RSU to forward their data packets.

The initial approach defines 4 states for the vehicles: Initial (INIT), Cluster Head (CH), Gateway (GW) and Ordinary (ORD). Only CH and GW can forward data packets. A vehicle leaving the cluster because it has speed up or slow down, will update his group speed after a few seconds.

The RSU is a permanent gateway in our approach, so each vehicle on the road can broadcast security information. Here, we will distinguish two types of GW, the static one (RSU) and the dynamic one (vehicles). The RSU is not a part of the cluster.

We have done new assumptions for the CH and modified the GW states. The 4 states in our approach are:

- INIT: Each vehicle starts in this state and can become CH. There is only one CH per cluster. Vehicle in the INIT state will be in ORD state and can potentially become CH or GW.
- CH: The CH is in charge of forwarding packets from one source to the other vehicles and gateways. Only two sources can be found: GW and ORD. The CH election is simple; the first vehicle who claimed "I am the CH" with the smallest time t, becomes the CH.
- ORD: Each vehicle that is already in the cluster and that is not a CH or a GW is in the ORD state. It's the basic state of a node after electing the cluster head. ORD can be eligible for GW rank temporarily.
- GW: By default an RSU has the GW static state. The RSU forwards data packets coming from a GW, a CH or an ORD vehicle. It can also transmit packets from its area to a close one using another RSU. In our method the only forwarded packets are security information. Vehicles can become temporarily GW if they are near the Cluster head and in a calculated area of the CH.

3.3 Cluster algorithm

To improve security in the cluster, we assumed that all packets transmitted before the clustering processes are dropped. A vehicle that wants to communicate must be in a cluster.

When, a vehicle is alone in his cluster, it means that's he is the CH and can communicate. If another vehicle comes in its area and wants to enter its cluster then the CH election process is initiated.

We use the five first steps from the initial method. The two last steps are the requested adaptation to our protocol. All the vehicles are in an initial state, no communication has ever been established, and none has ever sent a packet.

1) A vehicle that wants to send a packet, according to its group/state information; it stamps it and add this information to the packet header before sending it. This vehicle can't be the CH at the beginning because it doesn't know if there is already a CH and if there is at least one vehicle in the same group. It becomes CH if there is no answer during a certain amount of time.
2) Neighborhood vehicles get the incoming message and check group information and the state of the packet header.
3) The packet comes from a non CH node of the same cluster. The receiving vehicle will compete for CH role.
4) The first vehicle sending "I am the CH" at smallest time t becomes the CH of the cluster.
5) All the nodes are informed about the CH vehicle.
6) The cluster head collects concurrently the information about its cluster according to the method defined below.
7) The CH vehicle forwards the data packets depending on our IDS approach. Figure 2 summarizes the algorithm.

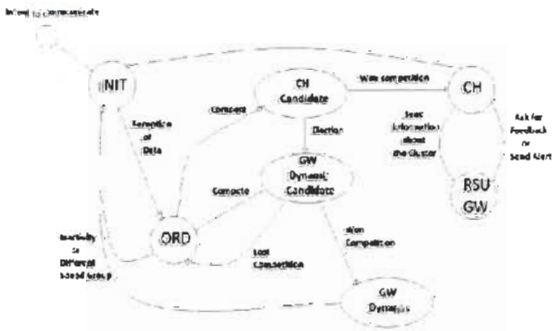


Fig.1 : Clustering process flow.

3.4 Definition of the Intrusions Detection System

Our work is based on two different IDS approaches. The first one makes detection on vehicles, and the second on RSUs. We will then compare the two approaches.

3.5 IDS based vehicle

Each vehicle is equipped with personal IDS equipment. Intrusion detection is active every time. The vehicle can be isolated or alone, or in a cluster group. Each node detects individually possible attacks. When an attack occurs, the information of the attack is forwarded to the CH. The CH handles the information according to our approach explained below.

3.5.1 Mathematical method to corroborate an attack for IDS based vehicle

Corroborate the information of a true attack is a major improvement. For IDS based vehicle there is a basic method to confirm that the IDS detect a real attack.

Let's start with the following assumptions:

- There is one IDS installed on each vehicle.
- The communication between vehicles and vehicles to RSUs are secure. Data is encrypted.
- RSUs are reliable.
- All the generated alerts given by the RSU are considered as true. When the IDS detect something it always considers it true. The false positive problem is handle by the numerous IDS in the network. If an IDS doesn't detect the attack, another will probably detects it.

When a member of the cluster detects an attack, it sends the information and the signature of the attack to the cluster head. The cluster head analyzes the signature and forwards the information to the other members to have their feedbacks. When all vehicles have given their feedbacks about the signature, the CH forwards them to the RSU. Also this latter, will send the signature to another random cluster on the road to have its feedback too. RSU then calculates the probability of the attack P_{Attack}:

$$(1) \quad P_{Attack} = \frac{Nb\ detection}{Nb\ veh\ total}$$

Where:

- P_{Attack} is the corroboration probability of the attack.
- $Nb\_detection$ is the number of vehicles having detected the attack.
- Nb_veh_total is the total number of vehicles who have given their feedback.

When $P_{Attack} > 0.50$, we consider that the signature is a real attack.

We are asking for the feedback of two clusters because if one of them contains a majority of attackers, the attacked vehicle can never send any information with our protocol.

This approach allows initiating the protocol explained below in Figure.3.

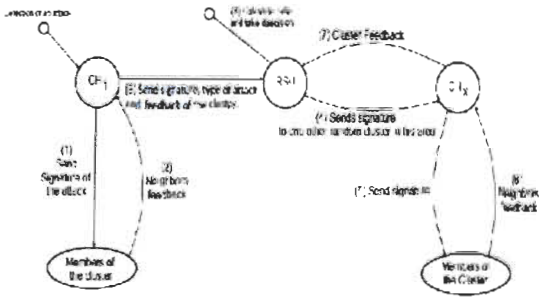


Fig. 2 : Corroboration method based vehicle

3.6 IDS based RSU

The intrusion detection system based RSU is an alternative to the IDS based vehicle. It preserves a better security in the system, because packets are analyzed by an external entity: the RSU.

3.6.1 IDS based RSU algorithm

Our assumptions are:

- The cluster already exists and the CH is elected.
- The exchange between the cluster and the IDS based RSU are:
  - Packets from vehicles are sent to the CH.
  - The CH forwards all the packets to the RSU.
  - The RSU analyses the packets. Normal packets are retransmitted to the receiver to be read. When an attack is detected the CH is alerted as explained in the next paragraph.

3.6.2 Mathematical method to corroborate attack for IDS based infrastructure

A similar approach is adopted for the RSU. Same assumptions and method are used.

All the packets from the cluster are forwarded to the RSU. When the RSU detects an attack, it will send the signature of the attack to the next and the previous RSUs. They give their feedback to RSU who initiate the protocol. The RSU computes P_{Attack} like in (1). When the attack is corroborated, the alarm is sent to the cluster head as presented in Figure. 4.

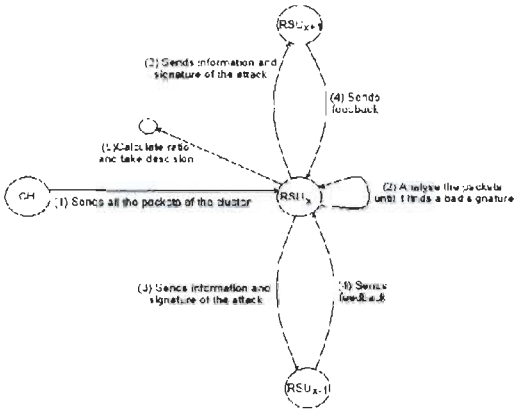


Fig 3 : Corroboration method based infrastructure

3.7 Routing protocol for security information

The entire components used by the protocol have been defined above. We will now present the assumptions, the mechanism and the algorithms of the method.

3.7.1 Assumptions

To maintain consistency in our results, the following assumptions will be installed in this work.

a) The RSUs are in communication range.
b) Each vehicle is part of a cluster. When an attack occurs we know that it comes from an inner zone or close to the cluster.
c) Exchanged data cannot be altered.
d) Each RSU knows the number of vehicles in its area at time t. We also have a material traceability of vehicle movements from one cluster to another or during area changing.

3.7.2 Internal mechanisms

Data sent from the cluster head to the RSU are:

- The number of vehicles in each cluster.
- The range between the current cluster and the cluster in front and behind it. To know this information, each cluster head provides its GPS coordinates at time t. The RSU will have a global view of its cluster from its area.
- The range between the first and last vehicle of each cluster. Each cluster head requests for vehicles in the cluster its GPS coordinates at time t. Cluster head searches for the first and last vehicle in its cluster. It then sends the data to the RSU. This will allow us to assess the accessibility of the clusters.
- Each RSU is in communication range, so they can request for information from other close RSU at time t. Information requested are: the position of the last vehicle in the next cluster, and the position of the first vehicle in the previous cluster. We can then determine if the vehicles in the area of an RSU are in range of vehicles in the area of the current RSU.

Information about the cluster at the RSU are defined below:

Notation	Description
Nb_veh	Number of vehicles in the cluster.
Pos_CH	GPS position of the cluster head.
Pos_CF	GPS position of the first vehicle in the current cluster.
Pos_CL	GPS position of the last vehicle in the current cluster.
Pos_NRSU_L	GPS position of the last vehicle in the next RSU area.
Pos_PRSU_F	GPS position of the first vehicle in the previous RSU area.

Table 2: The cluster at RSU information

3.7.3 Description of the algorithm

We will distinguish three cases to broadcast efficiently the information: vehicle to vehicle (V2V), infrastructure to vehicle (I2V) and hybrid which use V2V and I2V methods.

In V2V, the RSU knows that there are clusters in front and below the attacked cluster in his area. The latter sends to the attacked cluster the confirmation of the attack and asks him to broadcast this information to the closest clusters. Figure 5 below explains the process.

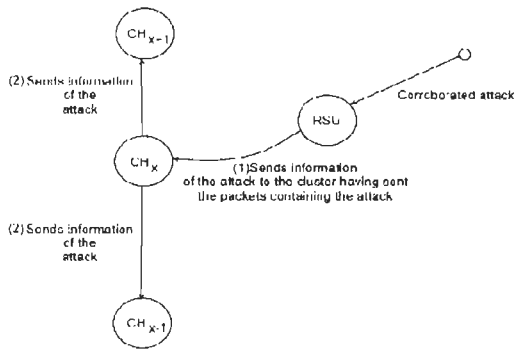


Fig. 4: Broadcasting information of the attack with V2V mode.

In V2I, the RSU knows that the attacked cluster is not in range of another cluster. The latter only sends to the attacked cluster the confirmation of the attack and forward the information to other RSU(s) (in front, below or both depending on the situation) as explained in Figure 6.

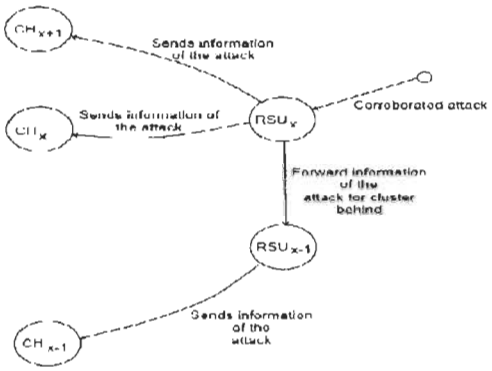


Fig 5: Broadcasting information of the attack with I2V mode.

Metrics

We initially focused on the metric of broadcasting range. Our method is interesting for close clusters. According to 802.11p standard, RSU can approximately emit in a range of 1000 meters. In our method, RSUs would be in the transmission range of each other. Ideally the metric range should be low enough so that we can meet vehicles on the road and far enough that the majority of the vehicles can benefit from the information.

4. SIMULATION

We have developed our decision making protocol on OMNET++ 4.2.2 under Windows 7 system. The simulation is done on a 5km highway with input and output. We simulated the two approaches with 50 nodes. There are 19 fixed nodes on the map that have the role of RSU; they are set up every 240m. We have set the detection threshold between 50 and 90%.

4.1 Comparison of alert detected

Fig. 6 shows the number of attacks detected in the network based on our two approaches.

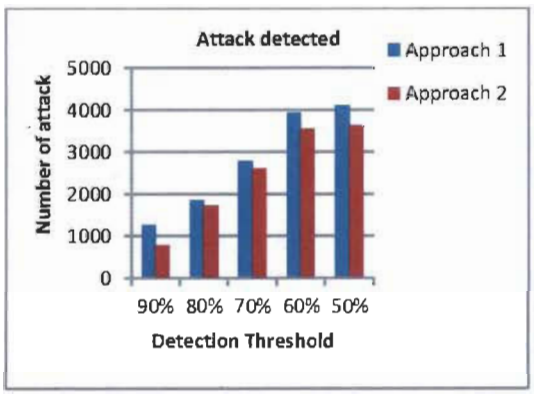


Fig. 6: The number of detected attacks based on the detection threshold.

The numbers of attacks increased depending on the detection threshold. We observe that the approach 1, generate much more alerts than approach 2. Knowing that approach 1 have much more IDS to detect alerts this results are normal. The approach 2 generate less alert but the results between the two approaches are not significant.

4.2 Comparison of alert corroborated

Fig. 7 shows the number of corroborated attacks in the network based on our two different approaches.

The graph shows the number of corroborated attacks. The approach 1 generate more alert and so more computing. The approach 1 is better to detects attacks but remain less efficient than approach 2 to corroborate efficiently an attack. RSUs generate fewer alerts and are not yet overloaded by the packet processing.

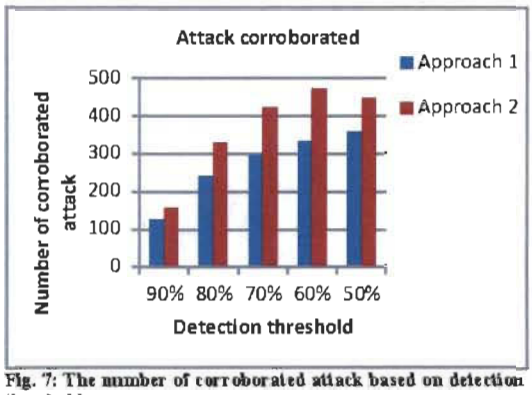


Fig. 7: The number of corroborated attack based on detection threshold.

4.3 Comparison of corroboration time

The Fig. 7 shows the average time taken to corroborate an attack. The average time of corroboration is the difference between: the average time when the alert is corroborated and average time when the alert is detected.The time is expressed in seconds.

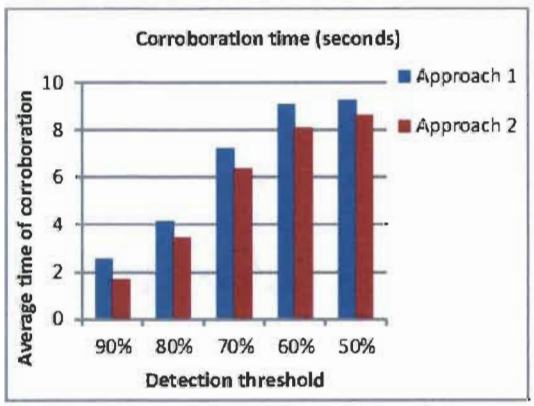


Fig. 8: Time to corroborate an attack based on detection threshold.

The graph shows that the corroboration time increases with the number of detected alerts. Most of the time, the approach 2 is more than or as efficient as approach 1. The approach 2 is still

efficient in the long term; it corroborates attacks also with a wide detection threshold.

According to our results, having several nodes or few is almost the same to detect alerts in VANET. The method 1 detects alerts efficiently with fine granularity when the threshold is low; as a result, it generates more traffic in the network. Nodes have to give their feedback to the CH. The method 2 is generally more effective in its corroboration. It generates fewer packets in the network and still corroborate with a large threshold.

5. CONCLUSIONS AND FUTURE WORK

We have presented a decision making protocol of security information in VANETs. It is based on clusterisation of nodes and on two IDS approaches. In the first one, the IDS are installed on vehicles, while in the second one they are installed in the Road Side Units (RSU). Our work defined and compares the two methods. We are about to expand our work with the simulator (SUMO, OMNET++) to find better metrics to preserve quality of service. Our future work could adapt it in urban areas. Improvement like clustering the RSUs among themselves or with vehicles is an approach which could be considered. In dense area the method could potentially flood the network and eventually obstruct vehicular communication when detecting. The overhead could also be an interesting study.

6. REFERENCES

[1] Panos Papadimitratos, JP Hubeaux; Securing Vehicular Communications, Maxim Raya. Wireless Communications, IEEE, Volume: 13, Issue: 5, 2006, Pages: 8 - 15.

[2] Jonathan Petit, Michael Feiri, Frank Kargl; Spoofed Data Detection in VANETS using Dynamic Thresholds. Vehicular Networking Conference (VNC), IEEE, Conference 14-16 Nov. 2011, Page(s): 25 - 32.

[3] Yong Hao, Jin Tang, Yu Cheng; Cooperative Sybil Attack Detection for Position Based Applications in Privacy Preserved VANETs. Global Telecommunications Conference, IEEE, Conference: 5-9 Dec. 2011, Pages 1 - 5.

[4] Norbert Bißmeyer, Christian Stresing, Kpatcha M. Bayarou; Intrusion Detection in VANets Through Verification of Vehicle Movement Data. Vehicular Networking Conference, IEEE, Conference: 13-15 Dec. 2010, Pages: 166 - 173.

[5] Jyoti Grover, Manoj Singh Gaur, Vijay Laxmi; Position Forging Attacks in Vehicular Ad Hoc Networks: Implementation, Impact and Detection. Wireless Communications and Mobile Computing Conference, 7th International, Conference: 4-8 July 2011, Pages: 701 - 706.

[6] Daxin Tiang, Yunpeng Wang, Guangquan Lu, Guizhen Yu; A Vehicular Ad Hoc Networks Intrusion Detection System Based on BUSNet. Future Computer and Communication (ICFCC), 2nd International Conference, Conference: 21-24 May 2010, Pages: V1-225 - V1-229.

[7] Jorge Hortelano, Juan Carlos Ruiz, Pietro Manzoni; Evaluating the usefulness of watchdogs for intrusion detection in VANETS. Communications Workshops, IEEE International Conference, Conference: 23-27 May 2010, Pages: 1 - 5.

[8] Vadim D. Kotov, Vladimir I. Vasilyev; Immune Model Based Approach For Network Intrusion Detection. Proceedings of the 3rd international conference on Security of information and networks, ACM, 2010, Pages 233-237.

[9] Perkins, C.E; Ad-Hoc on demand distance vector routing. Sun Microsyst. Labs., Adv. Dev. Group, Menlo Park, CA Royer, E.M., Mobile Computing Systems and Applications, IEEE, Conference: 25-26 Feb 1999, Pages: 90 - 100.

[10] Venkata Manoj D, M. M. Manohara Pai, Radhika M.Pai, Joseph MOUZNA; Traffic Monitoring and Routing in VANETs A Cluster Based Approach. 11th International Conference on ITS Telecommunications (ITST), 2011, Conference: 23-25 Aug. 2011, Pages: 27 32.

[11] M. Boussedjra, J. Mouzna, H. Labiod, N. Maslekar; C-DRIVE: Clustering Based on Direction in Vehicular Environment. International Conference on New Technologies, Mobility and Security (NTMS), 2011 4th IFIP, Conference: 7-10 Feb. 2011, Page(s): 1 5.

[12] Zhenxia Zhang, Azzedine Boukerche, Richard W.Pazzi; A Novel Multi-Hop Clustering Scheme for Vehicular Ad-hoc Networks. Proceedings of the 9th ACM International Symposium on Mobility Management and Wireless Access, 2011, Conference: 31oct-4Nov, Pages: 19-26.

[13] O. Kayis, T. Acarman; Clustering Formation for Inter-Vehicle Communication. Intelligent Transportation Systems Conference, 2007, ITSC 2007. IEEE, Conference: Sept. 30-Oct. 3, Page(s): 636 641.

[14] M. Boussedjra, J. Mouzna, H. Labiod, N. Maslekar; A Stable Clustering Algorithm for Efficiency Application in VANETs.Wireless Communications and Mobile Computing Conference (IWCMC), 2011 7th International, Conference: 4-8 July 2011, Page(s): 1188 1193.

[15] Tao Song, Weiwei Xia, Tiecheng Song, Lianfeng Shen; A Cluster-Based Directional Routing Protocol in VANET. Communication Technology (ICCT), 2010 12th IEEE International Conference on, Conference: 11-14 Nov. 2010, Page(s): 1172 1175.