Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Mouloud Mammeri de Tizi-Ouzou

Mémoire

Présenté pour l'obtention du diplôme de :

MASTER

En Informatique

Option : Réseaux, mobilité et systèmes embarquées

La réputation dans les réseaux véhiculaires (VANETs)

Réalisé par :

Mr. Boudi Nour

Mr. Hamouni Nabil

Encadré par :

Mme. Aoudjit.R

Promotion : 2014 /2015

REMERCIMENT

Nous remercions et nous rendons grâce à Dieu, qui nous a bénéficié d'une volonté suffisante pour accomplir ce modeste travail.

Nous tenons à remercier Mme Aoudjit notre promotrice pour sa disponibilité, sa serviabilité et ses conseils constructifs qui nous ont énormément aidés tout au long de notre travail (projet).

Nous expriment notre gratitude aux membres du jury d'avoir accepté de juger ce travail.

Dédicaces

Je dédie ce travail a :

A mes chers parents qui ont toujours été la pour moi, qui m'ont donnée un magnifique modèle de labeur et de persévérance, pour leur attention, sacrifice et soutien tout au long de mes études.

Mes chers frères : zahir, Anis et Idris.

Mes adorables sœurs : Faiza, Ferroudja, Kenza et Djidjiga.

Mes chère grand-mère pour son encouragements et leurs prières à mon égard, à ceux je souhaite une longue vie.

À toute ma grande famille, oncles, tantes et leurs familles.

À Mon binôme Nour et sa famille.

A tous mes amis en particulier et ceux qui me connaissent

A toute la promotion technologies alimentaires 2014/2015.

« Nabil»

Dédicaces

Je dédie ce travail a :

A mes chers parents qui ont toujours été la pour moi, qui m'ont donnée un magnifique modèle de labeur et de persévérance, pour leur attention, sacrifice et soutien tout au long de mes études.

Mon frère

Mes adorables sœurs

À toute ma grande famille, oncles, tantes et leurs familles.

À Mon binôme Nabil et sa famille.

A tous mes amis et ceux qui me connaissent

A toute la promotion réseaux, mobilité et systèmes embarquées 2014/2015.

« Nour»

Liste des figures

Listes des figures

Sommaire

Sommaire

Chapitre 3 les méthodes de réputation

Chapitre4 conception du système de réputation

Introduction générale

Introduction Générale

Nous assistons ces dernières années à une importante évolution dans le domaine des télécommunications sans fil, cette évolution est due essentiellement aux besoins actuels en termes de disponibilité et d'accès aux données à n'importe quel moment et depuis n'importe quel endroit.

De nombreuses applications ont depuis vu le jour afin d'améliorer notre vie quotidienne : dans nos maisons, nos sociétés, nos voitures… en somme partout.

Une des applications de ce concept consiste à renforcer la prévention routière et à munir nos voitures et nos routes de capacités permettant de rendre la route plus sûre (les informations sur le trafic, les accidents, les dangers, les déviations possibles, les informations météorologiques, etc.), améliorer le confort des passagers et rendre le temps passé sur les routes plus conviviale (accès à internet, jeux interactifs entre les passagers des véhicules proches, service de chat, aider les personnes à se suivre sur la route, etc.). Cette application est l'exemple type de ce que nous appelons les systèmes de transports intelligents (ITS, Intelligent Transportation System) et dont le but est d'améliorer la sécurité, l'efficacité et la convivialité dans les transports routiers à travers l'utilisation des nouvelles technologies de l'information et de la communication (NTIC).

Avec le développement rapide des technologies de communications sans fil, une nouvelle architecture basée sur des communications véhicule à véhicule (V2V, Véhicule to Véhicule) suscite ces dernières années un réel intérêt auprès des constructeurs automobiles, de la communauté R&D et des opérateurs Télécoms. Ce type d'architecture est formé par les véhicules eux même sans l'appui d'une infrastructure fixe pour le relayage des données et des messages. Nous parlons dans ce cas d'un réseau Ad Hoc de véhicule (VANET).

Afin d'étudier les VANETs, le déploiement sur terrain n'est malheureusement pas envisageable à ce jour, d'où le recours à la simulation. Plusieurs simulateurs ont été mis à la disposition des chercheurs dans ce but (NS2, GloMoSim…). Lors d'une simulation, la mobilité est un paramètre à ne pas

négliger, car les unités dans un VANET peuvent se déplacer à grande vitesse suivant un schéma de mobilité particulier. Pour modéliser la mobilité des VANETs, plusieurs modèles ont été conçus. Ces modèles de mobilité doivent prendre en considération les contraintes de la mobilité véhiculaire, pour que la simulation soit proche de la réalité.

Noter projet consiste a concevoir un système de sécurisation pour les réseaux de VANETs eu utilisent des méthodes de réputation afin d'isoler tous les nœuds malicieux et inciter les nœuds égoïstes a coopères pour pouvoir améliores les performances de ces réseaux et des les protéger de différente attaques.

Notre mémoire est organisé en quatre chapitres :

Dans **Le premier chapitre,** nous donnons un état de l'art des réseaux Ad Hoc véhiculaires(VANET) et leurs caractéristiques.

Dans **Le deuxième chapitre,** nous traitons les nœuds égoïstes et malicieux dans les réseaux véhiculaires (VANET), leur comportement et leur conséquence su ces réseaux.

Dans **Le troisième chapitre,** nous traitons les méthodes de réputation dans les réseaux véhiculaires (VANET).

Le quatrième chapitre, est consacré à la conception d'un système de réputation pour la sécurisation des réseaux VANET.

Chapitre 1

Les VANETs (états de l'art)

1.1 Introduction :

Les réseaux VANET ne sont qu'une application des réseaux ad hoc mobiles(MANET). Ils constituent le noyau d'un Système de Transport Intelligent(STI) ayant comme objectif principal l'amélioration de la sécurité routière en tirant profit de l'émergence de la technologie de communication et la baisse du coût des dispositifs sans-fil. En effet, grâce à des capteurs installés au sein de véhicules, ou bien situés au bord des routes et des centres de contrôle, les communications véhiculaires permettront aux conducteurs d'être avertis suffisamment tôt de dangers éventuels.

De plus, ces réseaux ne se contenteront plus d'améliorer la sécurité routière seulement, mais ils permettront aussi d'offrir de nouveaux services aux usagers des routes rendant la route plus agréable.

Dans ce chapitre, nous présentons d'abord le réseau ad hoc d'une manière général (définition, mode de communication, domaines d'application), puis, nous aborderons les réseaux VANET : on nous parlerons d'abord des différent modes de communication, puis les caractéristique des ces réseau, ensuite les applications et les travaux, enfin on parlera de la sécurité dans ces réseaux.

1.2 Les réseaux Ad hoc :

Définition [1] :

Un réseau mobile ad hoc, appelé généralement MANET (Mobile Ad hoc Network), est un réseau sans fil qui consiste en une grande population, relativement dense, d'unités mobiles qui se déplacent dans un territoire quelconque et dont le seul moyen de communication est l'utilisation des interfaces sans fil généralement le medium radio, sans l'aide d'une infrastructure préexistante ou administration centralisée, ces unités mobiles jouent à la fois le rôle de terminaux et de routeurs pour permettre le passage de l'information entre elles.

Il permet donc à deux nœuds qui sont chacun à portée des ondes l'un de l'autre (condition appropriée de propagation d'ondes radio) de rentrer en communication directement.

Un réseau ad hoc doit être facilement déployé, les nœuds peuvent joindre ou quitter le réseau de manière totalement dynamique sans informer le réseau, et si possible sans effet de bord sur les communications des autres membres.

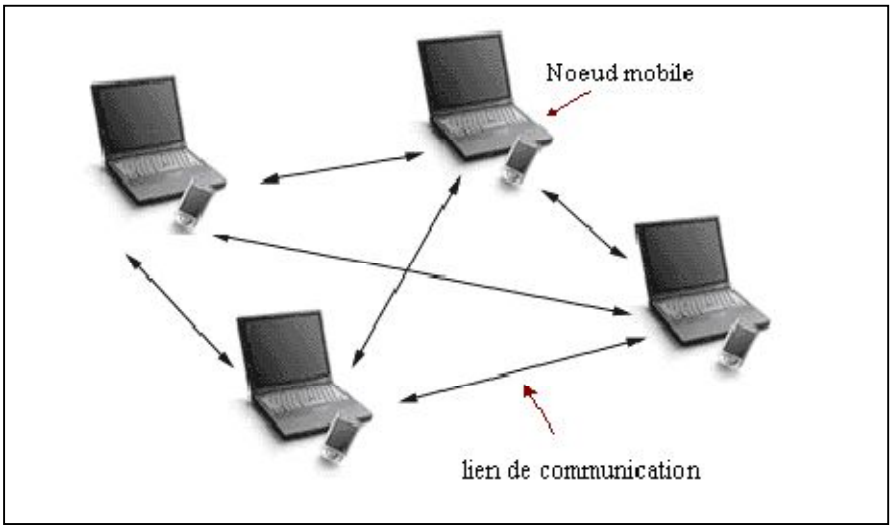


Figure1.1 : exemple d'un réseau ad hoc

1 .3 Modes de communication dans les réseaux mobile Ad Hoc [2] :

Les échanges de données dans les réseaux mobiles utilisent les modes de communication suivants :

- **Le mode Unicast :**

Le terme unicast définit une connexion réseau point à point. On entend par unicast, le fait de communiquer entre deux ordinateurs identifiés chacun par une adresse réseau unique.
Les paquets de données sont routés sur le réseau suivant l'adresse du destinataire, seul le destinataire intercepte et décode le paquet qui lui est adressé.

- **Le mode Multicast (multipoint) :**

On entend par multicast, le fait de communiquer simultanément avec un groupe d'ordinateurs identifié par une adresse spécifique (adresse de groupe). Son avantage par rapport au mode classique unicast devient évident quand on veut diffuser de la vidéo. Les paquets de données sont routés sur le réseau selon l'adresse des destinataires encapsulée

dans la trame transmise. Seuls les destinataires interceptent et décodent les paquets qui leurs sont adressés.

- **Le mode Broadcast (la diffusion) :**

Le broadcast est un terme anglais définissant une diffusion de données depuis une source unique à un ensemble de récepteurs. Contrairement à une communication Point à Point, il est possible d'adresser des paquets de données à un ensemble de machines d'un même réseau uniquement par des adresses spécifiques qui seront interceptées par toutes les machines du réseau ou sous réseau**.**

1.4 Domaines d'applications des réseaux ad hoc [3]:

Les réseaux mobiles ad hoc ont une très large palette d'utilisations. En effet, ils sont robustes, peu coûteux et s'adaptent aussi bien aux milieux urbains, qu'aux milieux ruraux.

Parmi les applications nous citons :

- **Les applications militaires :**

Un réseau mobile ad hoc est la solution idéale pour maintenir la liaison entre des chars d'assauts, des avions de chasse ou même entre des soldats et leur supérieurs au cours des exercices militaires ou dans un champ de bataille.

- **Opérations de secours :**

Lors des catastrophes naturelles (Incendies, inondations, tremblement de terre…etc.), les réseaux mobiles Ad Hoc peuvent résoudre le problème de communication là où une installation filaire ne peut être réalisée qu'après de très longs délais d'attente.

- **Applications commerciales :**

Pour un paiement électronique distant ou pour l'accès mobile à l'Internet, ou service de guide en fonction de la position de l'utilisateur.

- **Evénements occasionnels**:

Les réseaux ad hoc peuvent être utilisés pour la mise en place instantanée d'un réseau reliant plusieurs ordinateurs portables entre eux. Ils s'avèrent particulièrement utiles lors de l'organisation d'événements tels que des conférences, des séminaires,…etc.

1 .5 Les réseaux VANET :

Définition [4] :

Un réseau VANET est une particularité des réseaux MANET où les nœuds mobiles sont des véhicules (intelligents) équipés de calculateurs, de cartes réseau et de capteurs. Comme tout autre réseau Ad hoc, les véhicules peuvent communiquer entre eux (pour échanger les informations sur le trafic par exemple) ou avec des stations de base placées tout au long des routes (pour demander des informations ou accéder à internet…).

Les réseaux véhiculaires regroupent deux grandes classes d'applications, à savoir les applications qui permettent de bâtir un système de transport intelligent ITS (Intelligent transport System) et celles liées au confort ou avertissement du conducteur et des éventuels passagers.

1.5.1 Le Nœud du réseau VANET [5] :

Un nœud d'un réseau VANET est un véhicule équipé de terminaux tels que les calculateurs, les interfaces réseaux ainsi que des capteurs capables de collecter les informations et de les traiter. On parle de la notion de « véhicule intelligent ». La figure 2 modélise un véhicule intelligent.

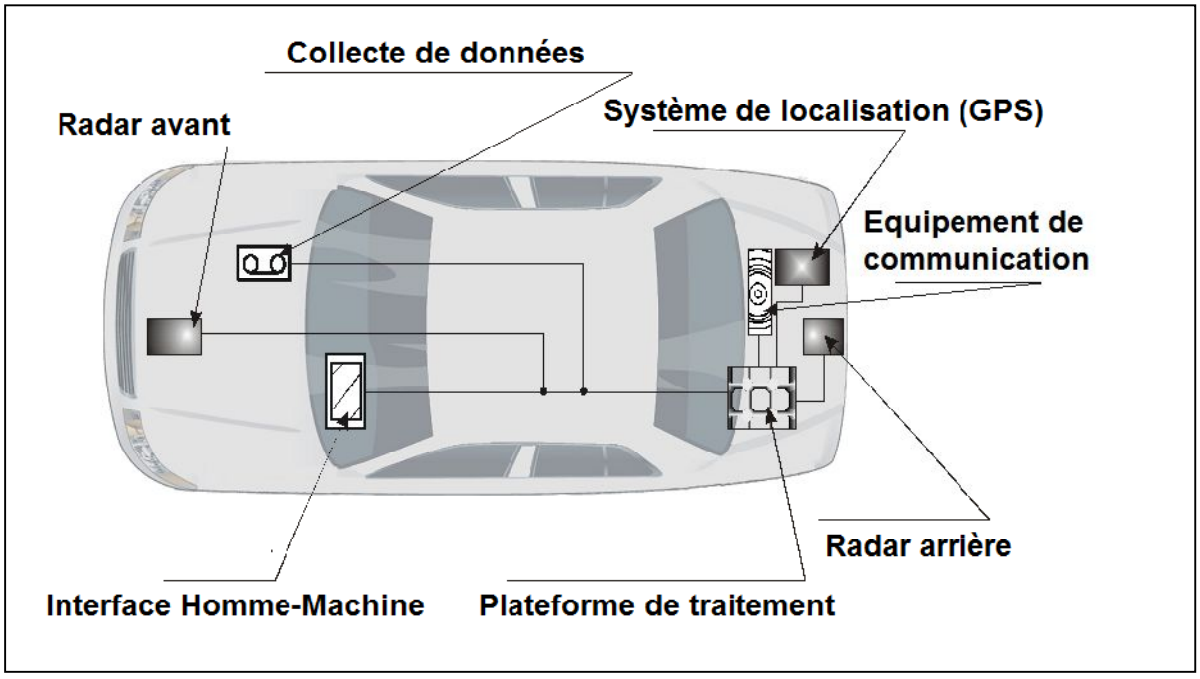


Figure1.2 : Véhicule intelligent

1.5.2 Les modes de communication dans les réseaux VANET [6] :

Les réseaux véhiculaires par analogie à ce qui existe dans les réseaux sans fil peuvent être déployés suivant trois catégories :

- **Communication de véhicule à véhicule :**

Dans cette catégorie, un réseau de véhicule est vu comme un cas particulier du réseau MANET (Mobile Ad Hoc Network) où les contraintes d'énergie, de mémoire et de capacité sont relaxées et où le modèle de mobilité n'est pas aléatoire mais prévisible avec une très grande mobilité. Cette architecture peut être utilisée dans le scénario de diffusion d'alertes (freinage d'urgence, collision, ralentissement…) ou pour la conduite coopérative.

Aucune infrastructure n'est utilisée, aucune installation n'est nécessaire sur les routes et tous les véhicules sont équipés pour communiquer directement entre eux n'importe où, que se soit sur les autoroutes, des routes de montagnes ou des routes urbaines, ce qui donne une communication moins coûteuse et plus flexible.

Cette approche souffre de certains inconvénients dont nous citons :

- Les délais de communication qui sont élevés, étant donné que la communication se fait en utilisant le multi sauts.
- Les déconnexions fréquentes dues au fait que les véhicules sont mobiles.
- La sécurité réseau est très limitée

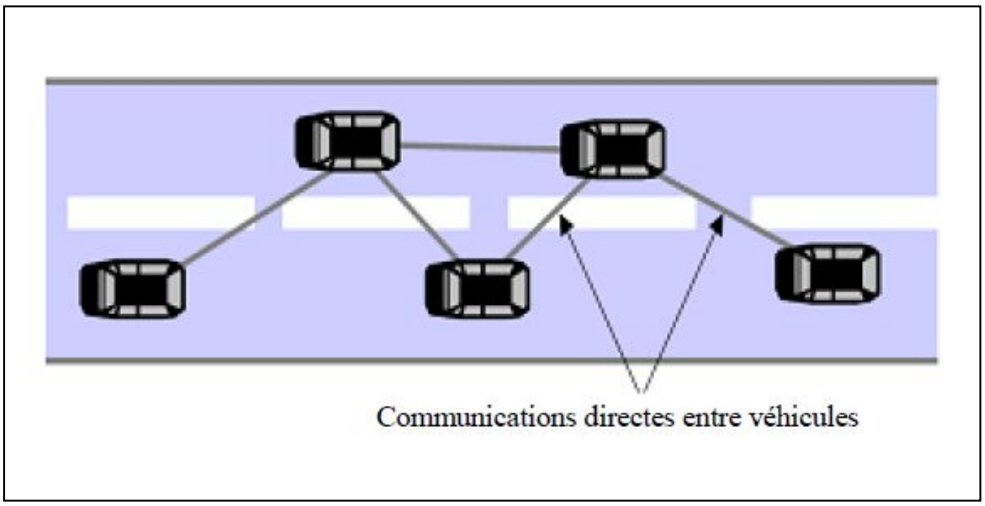


Figure1.3 : Communication véhicule à véhicule

- **Communication de véhicule avec utilisation d'infrastructures :**

Dans cette catégorie, on ne se concentre pas seulement sur des simples systèmes de communications inter véhicules mais aussi ceux qui utilisent des stations de bases ou points d'infrastructure RSU (Road Side Units, dénomination proposée par le consortium C2C-CC). Cette approche repose sur le modèle client/serveur où les véhicules sont les clients et les stations installées le long de la route sont les serveurs. Ces serveurs sont connectés entre eux via une interface filaire ou sans fil. Toute communication doit passer par eux. Ils peuvent aussi offrir aux utilisateurs plusieurs services concernant le trafic, accès à internet, échange de données de voiture-à-domicile et même la communication de voiture-à-garage pour le diagnostic distant.

L'inconvénient majeur de cette approche est que l'installation des stations le long des routes est une tâche coûteuse et prend beaucoup de temps, sans oublier les coûts relatifs à la maintenance des stations.

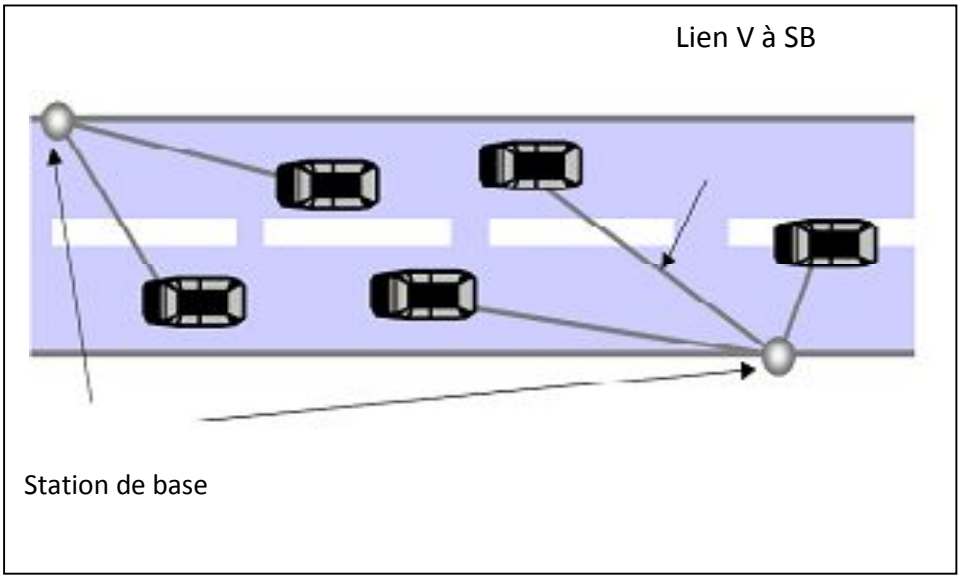


Figure1. 4 : ***Communication véhicule à station de base.***

- **Communication Hybride :**

La combinaison des communications véhicule à véhicules avec les communications de véhicules avec utilisation d'infrastructures, permet d'obtenir une communication hybride très intéressante. En effet, les portées des infrastructures (stations de bases) étant limitées, l'utilisation des véhicules comme relais permet d'étendre cette distance. Dans un but économique et afin d'éviter la multiplication des stations de bases à chaque coin de rue, l'utilisation des sauts par véhicules intermédiaires prend tout son importance.

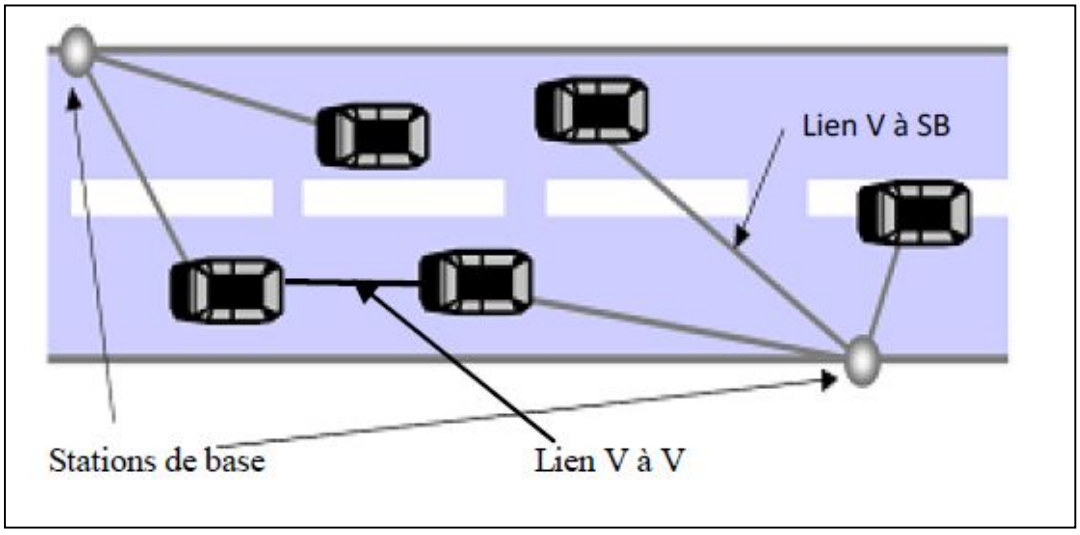


Figure 1.5 : Communication Hybride

1.5.3 Caractéristiques des réseaux VANET [7]:

Les réseaux véhiculaires ont des caractéristiques spécifiques qui les distinguent des réseaux Ad Hoc, à savoir :

- **La Collecte d'informations et la perception de l'environnement proche :**

La collecte d'informations se fait en utilisant différents capteurs de toutes catégories (caméras, capteurs de pollution, capteurs de pluies, capteurs de l'état de la route et de voiture, etc…) qui permettent au conducteur à bord de son véhicule de disposer d'un certain nombre d'informations et d'une meilleure visibilité pour pouvoir réagir d'une manière adéquate aux changements de son environnement proche.

- **Capacité de traitement, d'énergie et de communication :**

Contrairement au contexte des réseaux Ad Hoc où la contrainte d'énergie à titre d'exemple représente une des problématiques traitées, les éléments du réseau VANET n'ont pas de limite en terme d'énergie et disposent d'une grande capacité de traitement et peuvent avoir plusieurs interfaces de communication (WIFI, Bluetooth et autres). Grâce aux **N**ouvelles **T**echnologies de l'**I**nformation et de la **C**ommunication (NTIC) le conducteur peut prendre une décision à l'aide des traitements et des interprétations des informations collectées.

- **Environnement de déplacement et modèle de mobilité :**

Les environnements pris en compte par les réseaux Ad Hoc sont souvent limités à des espaces ouverts ou indoor (comme le cas d'une conférence ou à l'intérieur d'un bâtiment). Les déplacements des véhicules quant à eux sont liés aux structures des routes (intersections, panneaux de signalisation, etc…) et aux stations de base routières (infrastructures) que se soit dans les autoroutes ou au sein d'une zone métropolitaine. Les contraintes imposées par ce type d'environnement, à savoir les obstacles radio et les effets de la propagation à trajets multiples (multipath) ou d'évanouissement (fading), affectent considérablement le modèle de mobilité et la qualité des transmissions radio à prendre en compte dans les protocoles de routage. En outre la mobilité est un facteur lié directement au conducteur du véhicule.

- **Fortes mobilités, topologie du réseau et connectivité :**

A la différence des réseaux Ad Hoc, les réseaux VANET sont caractérisés par la forte mobilité des nœuds (véhicules), liée à la vitesse des voitures qui est très importante dans les autoroutes. Par conséquent, un nœud peut rejoindre ou quitter le réseau en un temps très court, ce qui rend les changements de topologie très fréquent. De plus, des problèmes peuvent apparaitre quand le système IVC (Inter Véhicule Communication) n'est pas équipé dans la majorité des véhicules.

- **Type de l'information transportée et diffusée :**

Un des objectifs des réseaux VANET étant la sécurité routière. Les types de communications s'axeront sur les diffusions de messages d'une source vers plusieurs destinataires. Néanmoins, les véhicules sont concernés par la diffusion d'informations en fonction de leurs positions géographiques et leurs degrés d'implication dans l'évènement déclenché. Dans de telles situations, les communications sont principalement unidirectionnelles.

1.5.4 Applications des réseaux VANET [8]:

Les principales applications des réseaux IVC peuvent être classées en trois catégories:

- applications de sécurité routière,
- applications d'aide à la conduite,
- applications de confort.

Nous détaillons ci-après ces catégories et donnons ensuite des exemples d'applications.

- **Applications pour la sécurité routière**

La sécurité routière est devenue une priorité dans la plupart des pays développés. Cette priorité est motivée par le nombre croissant d'accidents sur ses routes associé à un parc de véhicules de plus en plus important.

Afin d'améliorer la sécurité des déplacements et faire face aux accidents routiers, les IVC offrent la possibilité de prévenir les collisions et les travaux sur les routes, de détecter les obstacles (fixes ou mobiles) et de distribuer les informations météorologiques.

- **Applications pour les systèmes d'aide à la conduite et les véhicules coopératifs :**

Pour faciliter la conduite autonome et apporter un support au conducteur dans des situations particulières : aide aux dépassements de véhicules, prévention des sorties de voies en ligne ou en virage, etc. Nous pouvons citer également le cas des compagnies de transports utilisant les IVC dans un but de productivité pour réduire la consommation de carburant.

- **Applications de confort du conducteur et des passagers :**

En particulier les services de communication et d'informations des utilisateurs comme l'accès mobile à l'Internet, la messagerie, le chat inter-véhicules, les jeux en réseaux, etc.

Dans la suite de cette partie nous nous limitions à la description de quelques services et exemples d'application des systèmes de communication véhicule à véhicule.

- **Alerter en cas d'accidents :**

Ce service permet, dans le cas d'un accident, d'avertir les véhicules se dirigeant vers le lieu de l'accident que les conditions de circulation se trouvent modifiées et qu'il est nécessaire

de redoubler de vigilance. Il est nécessaire, également, en cas de densité réduite de véhicule de pouvoir conserver l'information pour pouvoir la retransmettre si un véhicule entre dans la zone de retransmission. Les messages de sécurité devront être émis à des périodes régulières. Ainsi le ou les nœuds désignés pour la retransmission des messages émettront des alertes à instants réguliers.

Les messages devront être de taille réduite pour être transmis le plus rapidement possible. Les messages devront comporter les coordonnées du lieu de l'accident et les paramètres de la zone de retransmission.

- **Alerter en cas de ralentissement anormal (bouchon, travaux, intempéries, etc) :**

Ce service permet d'avertir les automobilistes de situations de circulation particulières. L'information quelque soit la nature des difficultés de circulation renseigne l'automobiliste qu'il est nécessaire de ralentir. Le message d'alerte est émis par un véhicule détectant les difficultés de circulation (freinage important par exemple, déclenchement des feux de détresse, pluie).

Un véhicule banalisé effectuant des travaux peut également être à l'origine du message d'alerte. Comme pour le message d'alerte informant d'un accident, le message d'alerte informant d'un ralentissement doit être transmis aux autres véhicules de façon efficace et rapide.

- **La conduite collaborative :**

La conduite collaborative est un concept qui améliore considérablement la sécurité du transport routier, en plus de réduire le nombre de victimes lors d'accidents impliquant des véhicules automobiles.

Cette innovation est basée sur un échange de renseignements entre des véhicules munis d'instruments (capteurs par exemple) leur permettant de percevoir ce qui les entoure et de collaborer en groupes formés dynamiquement. Ces groupes de véhicules, ou réseaux ponctuels, peuvent élaborer une stratégie de conduite collective qui exigerait peu ou pas d'interventions de la part des conducteurs. Depuis les dernières années, différentes architectures de véhicules automatisés ont été proposées, mais la plupart d'entre elles n'ont pas, ou presque pas, attaqué le problème de communication inter véhicules.

- **Hot spot sur l'autoroute :**

Aujourd'hui, les personnes peuvent accéder à des sites web un peu avant qu'ils prennent le train, par exemple pour télécharger des films. En voiture, on peut imaginer d'acheter du contenu, au niveau d'une station essence, d'une gare ou même en pleine autoroute (en passant d'une voiture à une autre jusqu'au point d'accès le plus proche). Les passagers dans la voiture pourront ainsi jouer en réseaux, télécharger des fichiers MP3, envoyer des cartes à des amis, etc.

- **Gestion des espaces libres dans les parkings :**

Ce service permet de rassembler des informations sur la disponibilité de l'espace de stationnement dans les parkings et de coordonner entre automobilistes afin de les guider aux espaces libres (ex: projet SmartPark)

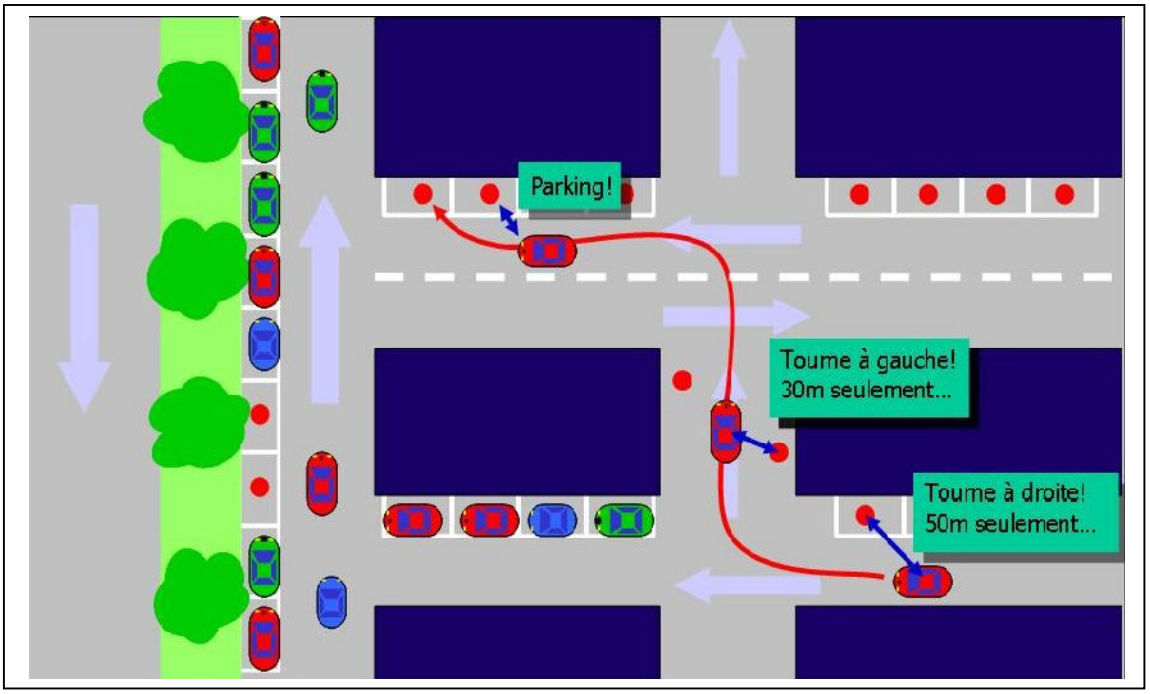


Figure 1.6 : Gestion des espaces libres dans les parkings

1.6 Travaux dans le domaine des VANET [9] :

Les propriétés des réseaux véhiculaires offrent des challenges importants, ce qui rend les VANET s'ouvrent à plusieurs domaines de recherche dont nous citons les plus importants:

- **Sécurité :**

La sécurité est un défi majeur ayant un grand impact sur le futur déploiement des réseaux véhiculaires ainsi que leurs applications. En raison de la sensibilité des domaines d'utilisation des VANET, une intrusion d'un véhicule malicieux aurait des conséquences graves sur l'ensemble des véhicules interconnectés. C'est pour cette raison que beaucoup de travaux de recherche ont été réalisés pour développer un mécanisme de sécurité instituant les relations de confiance entre les nœuds communicants et garantissant le contrôle d'accès aux services.

- **L'accès au canal :**

Les réseaux véhiculaires utilisent des communications radio. Par conséquent, il est important de concevoir des solutions spécifiques aux réseaux VANET qui permettent d'apporter de la qualité de service et de gérer les priorités en résolvant les problèmes d'interférences radio, des problèmes de propagation à multi-trajets des ondes ainsi que les irrégularités électromagnétiques.

- **Localisation des véhicules :**

Si l'un des véhicules du réseau doit être localisé (dans le cas d'un accident par exemple), les autres doivent être informés de sa position. Le problème est que tous les véhicules ne sont pas équipés d'un système de repérage par satellite (GPS). Pour cette raison, un mécanisme de localisation sans utilisation de GPS est nécessaire.

- **Problèmes de congestion :**

L'un des problèmes des VANET est que chaque véhicule communique avec tous ceux qui sont dans sa zone de couverture. Ceci entraîne une dégradation de la qualité de service (QoS) avec l'augmentation du nombre de véhicules. Ce problème a fait l'objet de plusieurs études.

- **Mobilité dans la simulation des réseaux :**

Dans la simulation des VANET, le facteur mobilité a longtemps été négligé. On ne considérait pas la différence de mouvements entre les nœuds des VANET et des MANET, ce qui pouvait biaiser les résultats de la simulation. Pour cette raison, de plus en plus d'équipes de recherche s'intéressent à l'étude de la mobilité dans les VANET.

Avec un bon simulateur, plus le modèle de mobilité est réaliste, plus les résultats de la simulation sont proches de la réalité. D'où l'impact direct des modèles de mobilité sur la réussite d'une simulation.

- **Routage :**

Le routage dans les réseaux VANET est un problème très difficile à gérer et un axe de recherche pour beaucoup de chercheurs. Pour que les véhicules puissent communiquer entre eux, un protocole de routage doit être défini. En effet quand les terminaux ne sont pas à une portée de transmission radio directe, le routage est exigé pour établir la communication entre les véhicules.

1.7 La sécurité dans les VANETs [10]:

A cause de l'importance de l'information envoyée aux équipements embarqués dans les véhicules, la sécurité des communications dans les VANETs ne consiste pas seulement à assurer les objectifs de la sécurité (L'authentification, La non-répudiation, La confidentialité, etc….) , mais d'autres objectifs et contraintes doivent être pris en compte tel que la consistance de données des messages générés par les autres véhicules et l'aspect temps réel des applications liées à la sécurité. Dans cette section, nous présentons les mécanismes de base qui ont été mis en œuvre pour la sécurité de ces réseaux.

1.7.1 Exigences de la sécurité [11]:

Un système de sécurité pour la messagerie sécurisé dans un VANET doit remplir les conditions suivantes :

- **Authentification**:

Réactions à des événements de véhicules devraient être fondées sur les messages légitimes (cet est à dire, généré par les expéditeurs légitimes). Nous avons donc besoin de s'authentifier les expéditeurs de ces messages.

- **Vérification de la cohérence des données**:

La légitimité de messages englobe également leur cohérence avec ceux similaires (ceux générés en étroite espace et le temps), parce que l'expéditeur peut être légitime tandis que le message contient des données fausses. Cette exigence est parfois appelé «plausibilité».

- **Disponibilité**:

Même en supposant un canal de communication robuste, certaines attaques (Par exemple, en brouillant DoS) peuvent faire baisser le réseau. Par conséquent, la disponibilité devrait être également soutenue par d'autres moyens.

- **Non-répudiation**:

Pilotes causer des accidents doivent être identifiés de façon fiable; une expéditeur ne devrait pas être en mesure de refuser la transmission d'un message (il peut être crucial pour enquête pour déterminer la séquence correcte et le contenu des messages échangées avant l'accident).

- **Confidentialité:**

Les gens sont de plus en plus se méfier de Big Brother technologies habilitantes. Par conséquent, la vie privée des conducteurs contre observateurs non autorisées doit être garantie.

- **contraintes temps réel**:

Aux très hautes vitesses typiques de VANETs, le temps strict contraints doivent être respectées

1.7.2 Solutions pour la sécurisation des VANETs :

Dans la littérature, plusieurs solutions ont été proposées pour adresser le problème de la sécurité dans les VANETs. Dans cette section, nous présentons certaines solutions et architectures.

Dans Raya et al**. [12]** Proposent une analyse détaillée des menaces qu'encourent les VANETs et proposent une architecture de sécurité. Ils ont présenté un ensemble de protocoles de sécurité de vie privée et la robustesse de ces protocoles. Après la présentation de certains requis de sécurité et des profils des attaquants, ils ont proposé leur propre solution. Dans un premier ils ont présenté les signatures numériques comme un block. Dans cette section, l'emphase a été mise dans le fait que dans les VANETs, les messages de sureté nécessitent une authentification et leur préférence pour la sécurisation des messages par signature numérique.

Dans un second temps ils ont présenté une façon de sécuriser les messages. Avant qu'un véhicule n'envoie un message de sureté, il le signe par une clé privée et inclure une autorité de certification (CA). Après la présentation de leur méthode de sécurisation, ils ont proposé un dispositif inviolable pour sécuriser physiquement des informations sécrètes, telles que les clés privées. Ce dispositif pourrait également signer les messages sortants.

Troisièmement, ils ont propose une façon de gérer les clés. En d'autres termes, ils ont adressé la question de la distribution des clés de certification et de révocation. À cette fin, ils ont identifié deux composants relatifs à la cryptographie: l'identité électronique et les pairs de clés anonymes qui sont utilisées pour la question de la confidentialité. Cette clé sera conservée et distribuée par les autorités gouvernementales de transport ou par les constructeurs automobiles. La clé doit être certifiée par une autorité de certification. La clé sera révoquée dans le cas d'une observation d'une activité compromettante. Dans le but d'assurer la vie privée des usagers, les auteurs proposent l'utilisation de clé publique anonymes. Pour l'authentification d'établissement de session, il est proposé d'utiliser des primitives cryptographiques symétriques. Pour prévenir les attaques de déni de service, il est

proposé de commuter entre différents canaux ou même des technologies de communication. Pour éviter les attaques de divulgation d'information erronées, il est propose de faire une vérification des données reçues d'un émetteur en les comparant avec des informations provenant d'autres sources. L'anonymat des usagers est assuré par un algorithme de changement de clé qui s'adapte à la vitesse du véhicule et prend en compte la corrélation de la clé par l'adversaire.

Dans, Frank Karl et al.**[30]** Ont suggéré la methode SECA (the Security-Requirements Engineering using Cluster Analysis). C'est une approche qui permet l'analyse d'un grand nombre d'applications en sélectionnant une représentation typique qui couvre les requis du cluster d'application, ensuite, ils développent une solution de sécurisation pour ce sous-ensemble d'application. Ainsi, dans un premier temps, ils collectent une liste d'application qui comprend les différents cas d'utilisation possibles. Dans un second temps, ils font une analyse préliminaire des caractéristiques des applications précédemment sélectionnées et les requis de sécurités de toutes les applications en question. Une fois l'analyse effectuée, ils regroupent les applications similaires en utilisant un cluster d'analyse. En quatrième lieu, ils appliquent des cas d'utilisation d'attaques à un sous-ensemble d'applications représentatives de chaque cluster et les analysent plus en détails. À partir de cette étape, ils sont capables de déterminer un ensemble de mécanisme de sécurité à appliquer à ce sous ensemble d'application pour les prévenir d'éventuelles attaques. En fin de compte, ils déterminent les mécanismes de sécurité pour tous les sous-ensembles d'applications formés.

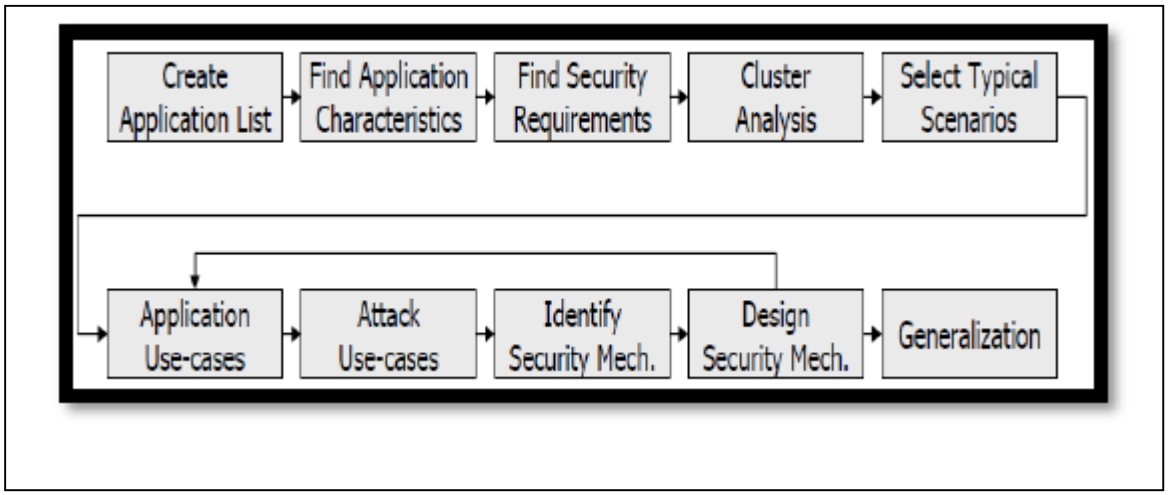


Figure 1.6 : Les étapes du processus « SECA »

Une autre approche connue pour la sécurisation des communications dans les réseaux de véhicules est l'utilisation d'une infrastructure de gestion de clés dédiée au VANET (VPKI). Dans cette approche, l'hypothèse fondamentale est que des stations de base sont disposées le long des routes pour supporter cette infrastructure et notamment la distribution et la révocation des clés.

Les solutions basées sur une VPKI résolvent le problème de protection de la vie privée en utilisant un ensemble de clés anonymes et un algorithme permettant de changer périodiquement la clé utilisée pour éviter la possibilité de pouvoir tracer un véhicule particulier .Si la clé utilisée n'était pas changée périodiquement, un véhicule utiliserait toujours la même clé pour signer tous ses messages. Il deviendrait alors simple pour une personne observant le trafic réseau de corréler une clé donnée avec le trajet d'un véhicule. Les VPKI sont une approche prometteuse pour la sécurité des réseaux de véhicules, néanmoins, leur déploiement à large échelle est long, difficile et potentiellement très coûteux car il nécessite des tests grandeur nature pour assurer le bon fonctionnement en conditions réelles.

Dans Dhurandher et al**[31]**. Présentent la sécurisation des véhicules par les algorithmes de réputation et de vérification (Vehicular Security through réputation and Plausibility Check Algorithme : VSRP). Pour déployer la sécurité dans les VANETs, leurs algorithmes prennent en considération trois types d'évènements : les embouteillages, les accidents et les applications de freinage. L'algorithme utilise un système base sur la réputation des capteurs, non seulement pour détecter mais aussi pour isoler les nœuds malicieux présents dans le réseau. Cet algorithme permet aussi de gérer les problèmes lies à l'agrégation et la suppression des données. Il exploite une approche orienté évènement. Trois types d'évènements sont répertoriés: 1) un-saut, 2) multi-saut, 3) intention malicieuse

1.8 Avantages et contraintes de VANET [13]:

a) Avantage des réseaux VANET :

- **Topologie dynamique :**

Les nœuds des réseaux VANET (véhicules) se déplaçant très rapidement, la topologie du réseaux et a chaque fois modifiée, mais les caractéristiques de VANET permettent le maintient des communications et l'échange de flux d'informations en dépit des changements fréquents des positions des nœuds.

- **Echange entre nœuds hétérogènes :**

Les véhicules des réseaux VANET sont de différentes marques et les composants réseaux qui les constituants utilisent différents technique, mais ils peuvent tout de même aboutir à un bon échange d'informations grâce aux protocoles instaurés par les concepteurs du réseau.

- **Propagation par trajet multiple :**

Les infos partagées par un véhicule peuvent êtres reçus par tous les autres véhicules se trouvant dans son entourage.

- **Relais d'informations :**

Deux véhicules distants de plusieurs KM peuvent se partager une information, cette information envoyée depuis un nœud A est relié par plusieurs nœuds intermédiaires avant d'arriver au destinataire B.

b) Inconvénients des réseaux VANET

- **Canal radio partagé et limité :**

Un canal radio a fréquences précises est utilisé par tous les nœuds, le flux d'information est donc limité et le débit de transmission diminue surtout dans les centre villes.

- **Faible bande passante :**

Le partage du canal limite la bande passante dont dispose chaque nœud pour partager les informations.

- **Les interférences :**

Les réseaux VANET utilisent les transmissions radio pour transmettre l'information, ce qui rend les communications exposées aux interférences radio, ces derniers sont de nature diverse comme : le rapprochement des fréquences d'émission (interférences entre deux nœuds), les bruits de l'environnement (équipements électriques, moteurs), et les phénomènes de réflexion, atténuation et dispersion qui déforment le signal. Ces interférences font augmenter le taux d'erreurs de transmission, et le rendent incompréhensible par le récepteur.

1.9 Conclusion :

Dans ce chapitre nous avons présenté les réseaux mobiles Ad Hoc (définition, mode de communication), puis nous avons présenté les réseaux de VANET ou on a décrit leurs architecteur et modes de communications, et nous avons parlé de travaux dans les VANET. Enfin nous avons brossée un état de l'art sur la sécurité de ces types de réseaux et leur avantage et contrainte.

Dans le chapitre suivant, nous intéressons aux nœuds égoïstes et malicieux et leur comportement dans les réseaux VANETs, et leurs conséquences sur les performances de ces réseaux.

Chapitre 2

Les nœuds égoïstes et malicieux dans les VANETs

2.1 Introduction

Le bon fonctionnement des applications de sureté nécessite l'intégrité des donnes échangées, l'authentification des véhicules source, l'acheminement des messages en un temps très court et un taux de réception élevé pour les véhicules concerner par une information. Car les informations échangées relèvent de la secréter des utilisateurs, un usager ne devrait jamais prendre en considération une information reçue sans la garantie de son authenticité. Chaque altération d'un message de sureté peut causer des accidents, comme par exemple dans le cas ou un utilisateur malicieux dissémine une fausse information pour faire dévier de leurs routes quelques véhicules, alors que la route proposée comprend des dangers tels qu'un glissement de terrain. Cependant, un véhicule n'a pas toujours le temps ou l'occasion de vérifier l'authenticité d'une information en amont, a cause de court délai de réflexion lie aux de sécurité routière. Cette vérification se complique davantage quand aucune infrastructure n'est déployée ou quand elles sont peu nombreuses.

Dans les réseaux collaboratifs ad hoc mobiles tel que les réseaux véhiculaires, les informations concernant le comportement de chaque membre sont asymétriques a cause de leur nombre important. En plus de cela, la forte mobilité des véhicules et l'étendue géographiques important des réseaux véhiculaires génèrent des connexions sporadiques entre les véhicules et donc des intervalles de rencontre irréguliers .Car établir et maintenu des connexions à un saut avec les autre véhicules est difficile, des membres (nœuds) malicieux et égoïstes ont apparus dans les réseaux véhiculaires qui perturbe le fonctionnement et diminuer les performances du réseau.

Dans ce chapitre nous définissons ces nœuds et leur comportement dans ces réseaux, et enfin nous proposons la solution pour remédier à ce genre de problème.

2.2 Nœud égoïste [14] :

Se sont des nœuds qui ne coopèrent jamais seulement s'ils bénéficient de leur acte de coopération, et peuvent compromettre les opérations de réseau. Ces nœuds ne sont pas nécessairement malveillants, car dans la plupart des cas, ces nœuds ne font ni attaquer, ni perturber le fonctionnement du réseau, ils sont juste réticents à coopérer puisque l'acte de

le faire va consommer leurs ressources limitées. Ces nœuds restent néanmoins relationnels et en aucun cas ils alternent le contenu des messages à relayer.

On trouve ces nœuds généralement dans les protocoles de routages dans les réseaux de VANETs , nous parlerons dans la section suivantes de l'égoïsme de quelques protocoles et les modèles de nœuds égoïstes qui existâtes.

2.3 Le comportement égoïste [15] :

L'efficacité des réseaux ad hoc (Manet) dépend de la volonté des nœuds participant à transmettre les données pour une autre. Par conséquent, la coopération joue un rôle essentiel à maximiser le taux de transfert de données.

Cependant, ce ne sont pas toujours le cas où il existe des nœuds qui ne coopèrent seulement s'ils bénéficient de leurs actions de coopération.
Ces nœuds, qui sont communément connus comme des nœuds égoïstes, peuvent compromettre les opérations du réseau. Les nœuds égoïstes ne sont pas nécessairement malveillants, car dans la plupart des cas, ces nœuds ne font ni attaquer, ni perturber le fonctionnement du réseau, ils sont juste réticents à coopérer puisque l'acte de le faire va consommer leurs ressources limitées.

Par conséquent, il est nécessaire de détecter l'égoïsme et de prendre les mesures nécessaires pour éviter la dégradation des performances du réseau.

La détection des nœuds égoïstes peut également aider à identifier les nœuds dont le niveau l'énergie est faible parce que le manque d'énergie est l'une des raisons pour ne pas coopérer dans le réseau.

Nous pourrions donc régler le fonctionnement du réseau pour assurer un fonctionnement sain et continu, comme découvrir de nouvelles routes qui composent nœuds relais avec plus énergie.

La plupart, sinon tous, les travaux publiés sur la stimulation de la coopération approches en particulier ceux ciblant la couche réseau supposent que le comportement égoïste peut être évaluée, mais ne le font pas explicitement indiquer comment.

Dans de tels cas, l'égoïsme est déterminé sur la base une valeur de seuil prédéfinie d'un seul ensemble d'actions telles que le nombre de paquets transmis et le nombre paquets reçus.

Par exemple, taux de transfert des paquets peut être défini comme suit :

$$taux\ de\ transmission = \frac{\text{nombre de paquets transmis}}{\text{nombre de paquets reçus}}$$

sur la base du nombre total de paquets qu'un nœud a réussi à transmettre par comparaison avec le nombre de paquets qu'il a reçu.

En tant que tel, lorsque le taux de transfert ne répond pas certain seuil (Évaluée sur la base d'une observation de première main), le nœud doit être considéré comme égoïste et l'état de comportement peut être soit conservés pour référence locale ou diffusées à travers le réseau.

Afin de renforcer l'évaluation de l'égoïsme sur la base d'observation de première main, les informations de comportement supplémentaire est généralement obtenue à partir d'observation de seconde main des autres nœuds sont enquises sur la base de leurs expériences traitant avec le même nœud de relais.

2.4 Quantification de l'effort d'un nœud [16] :

La quantification est définie ici comme une mesure explicite du comportement d'un nœud qui est fait par un nœud d'observation.

Mesure explicit signifie que le comportement d'un nœud doit être observé, évalués et assignés à des mesures quantifiables qui est le reflet de l'effort démontré par ce nœud.

pratique Commune qui a été appliqué dans de nombreux stimulation de la coopération qui consiste à représenter le comportement d'un nœud comme bonnes (Coopérative) ou mauvaise (égoïste) sans préciser réellement le niveau de l'effort qui a contribué un nœud.

Le mécanisme du chien de garde classique qui a été largement appliquée dans de nombreux schémas existants de détection de comportement présente le comportement d'un nœud dans la forme de valeur binaire «0» pour le nœud égoïste ou "1" pour la coopération nœud.

Présenter le comportement d'un nœud sur la base de la décision finale d'un nœud observateur ne reflète pas le niveau réel de l'effort qu'un nœud observé a mis, où l'évaluation peut ont pas été assez fait.

Cela est particulièrement vrai lorsque l'information à propos du comportement égoïste est obtenue sur la base de la confiance sur les rapports envoyé dans le réseau, où un nœud peut percevoir que le partage d'information est correcte sans obtenir une validation correcte sur toute accusation de mauvaise conduite ou de la revendication de bonne conduite d'un nœud particulier observé. Sans tenir compte du réel effort fourni par le nœud, le comportement observé peut ne pas être exacts.

Par conséquent, il est important d'avoir des mesures quantifiables qui reflète adéquatement l'effort d'un nœud particulier plutôt pas simplement à raconter le comportement sous forme binaire, à savoir bon ou mauvais.

Cette mesure devrait représenter l'effort d'un nœud où les éléments importants qui doivent être pris en considération (Si la disponibilité est possible) peuvent inclure:

- Niveau de charge de la transmission qu'un nœud de relais manipule, par exemple : le nombre de connexions.
- Taux de l'effort de renvoi qu'un nœud de relais offre à chaque connexion entrante à partir d'autres nœuds.
- les taux de transmission de paquets d'autres nœuds qui demandent un service du même nœud de relais.
- une quantité suffisante de temps pour observer et évaluer le comportement d'un nœud.

Ces éléments sont des aspects impératifs qui pourraient aider à l'obtention d'informations de comportement de nœud précis.

Avec la nature aléatoire de réseaux sans fil multi-sauts, de telles informations ne peuvent pas être facilement obtenu, mais la quantification doit être faite de telle sorte que l'étiquette de comportement peut être assez affectée.

2.5 Égoïsme dans le routage [17] :

Dans les protocoles de routage, la transmission de paquets est la tâche la plus fondamental qui doit être effectuée par des nœuds pour assurer l'achèvement de tout processus de communication initiée.

Toutefois, en raison des contraintes de ressources, le processus de transfert pourrait ne pas être atteint si les paquets sont abandonnés parce que le processus de transmission consomme l'énergie sans apporter aucun bénéfice direct à l'expéditeur. Le risque de l'épuisement de l'énergie a donné lieu à l'égoïsme dans le routage qui conduit à la dégradation du service. Dans cet article, nous allons discuter comportement égoïste du point de vue de la communication en utilisant le protocole de routage **AODV.**

- **Protocole de routage AODV :**

Dans le protocole de routage AODV, contrôler les paquets tels que demande de route (RREQ) et de la voie de réponse (MIQ) messages sont disséminée à travers le réseau chaque fois qu'un nœud particulier l'intention d'installer une voie de transmission de données à son désiré destination. Un RREQ est diffusé chaque fois qu'un nœud serait comme pour configurer une nouvelle voie d'acheminement vers une destination ou si le précédemment route établie a expiré. Il est donc essentiel pour nœuds intermédiaires pour aider à la diffusion de la RREQ jusqu'à le chemin d'accès à la destination prévue est trouvée et une RREP unicasted vers le nœud source pour établir un bidirectionnel flux de routage avant la transmission de données réelle. Ce processus ne peut être accompli avec succès si tous les nœuds coopèrent et participer à la transmission de ces messages de contrôle.

- **L'égoïsme dans AODV :**

Plusieurs scénarios de l'égoïsme se produisant dans AODV comprennent:

Nœuds ne transmettent pas les messages reçus à RREQ leur houblon prochaines correspondant, la route fait établi pas passer à travers ces nœuds.

Nœuds ne génèrent pas de messages en réponse à MIQ RREQs pour des destinations qu'ils ont des itinéraires, ou font pas aider à RREPs unicasting retour à la source pour compléter le processus de configuration de l'itinéraire.

Les nœuds ne annoncent Route erreur (RRER) messages lorsqu'une erreur de liaison est détectée ou chaque fois que nécessaire, provoquant d'autres nœuds pour ne pas être conscients de l'état courant de fuite, gaspillant ainsi les paquets de transmission d'énergie qui ne pouvait pas atteindre leur destination.

Nœuds aider à la configuration de la route, mais ne transmettre pas des paquets de données parce qu'ils ne sont intéressés à utiliser itinéraire l'établi pour leur propre transmission, donc des paquets de données à partir de autres nœuds ne parviennent pas à leurs destinations

2.6 Nœuds malicieux [18] :

Ces les nœuds les plus dangereux dans les réseaux véhiculaires, ces nœuds introduisent des fausses informations ou falsifient les informations reçues avant de les retransmettre. Quelques-uns d'entre eux agissent tout le temps de la sorte, d'autres alternent entre un comportement malicieux et un autre correcte pour éviter d'être détectes, et ils ont un comportement plus dévastateurs pour les performances du réseau. En effet, un nœud malicieux peut aussi faire en sorte qu'un nœud valide soit ajouté à la liste noire,

Ces sont eux qui provoque toutes les attaques sur le réseau véhiculaires, car ils ont la capacité d'usurper l'identité d'un nœud valide et falsifier les messages…..etc, dans la section suivante nous citons quelques attaques des nœuds malicieux sur les réseaux de VANET.

2.7 Attaques provoqué par les nœuds malicieux dans les VANETs [19]:

- **Le déni de service :**

  Cette attaque peut être considérée comme la plus populaire dans les réseaux classique et elle peut aussi être perpétrée dans les VANETs. L'intérêt de ce type d'attaque est de rendre le réseau dysfonctionnel. Ainsi donc le VANET ne sera plus disponible.

  Déni de service est toujours l'une des attaques au niveau les plus graves dans chaque réseau. Les scénarios à effectuer sont très diverses. L'objectif principal est d'empêcher les utilisateurs authentiques pour accéder aux services réseau. Dans les attaques DoS, les attaquants peuvent transmettre des messages factices pour brouiller le canal et donc, de réduire l'efficacité et la performance du réseau. Une

partie ou l'ensemble du réseau est plus disponible pour les utilisateurs légitimes. Figure2.1 Indique qu'une voiture noire malveillants forge un grand nombre de fausses identités et transmet un message factice "Lane près de l'avant" à une voiture derrière elle légitime et même à une RSU de créer un bourrage dans le réseau.

Un attaquant peut mettre en place cette attaque en inondant le réseau, en insérant des informations non pertinentes dans le réseau
Un farceur peut rendre le réseau indisponible pour la simple raison de prouver qu'il en est capable.

L'étendu de ce type d'attaque est généralement large, ce qui signifie que c'est une attaque qui concernera un grand nombre de nœuds. Ainsi donc, c'est une attaque qui peut s'étendre dans une zone géographique très large à travers plusieurs nœuds par des communications multi-sauts. De plus, l'impact de ce type d'attaques se reflète par le fait que l'attaque peut être détectée, mais il sera difficile de la corriger.

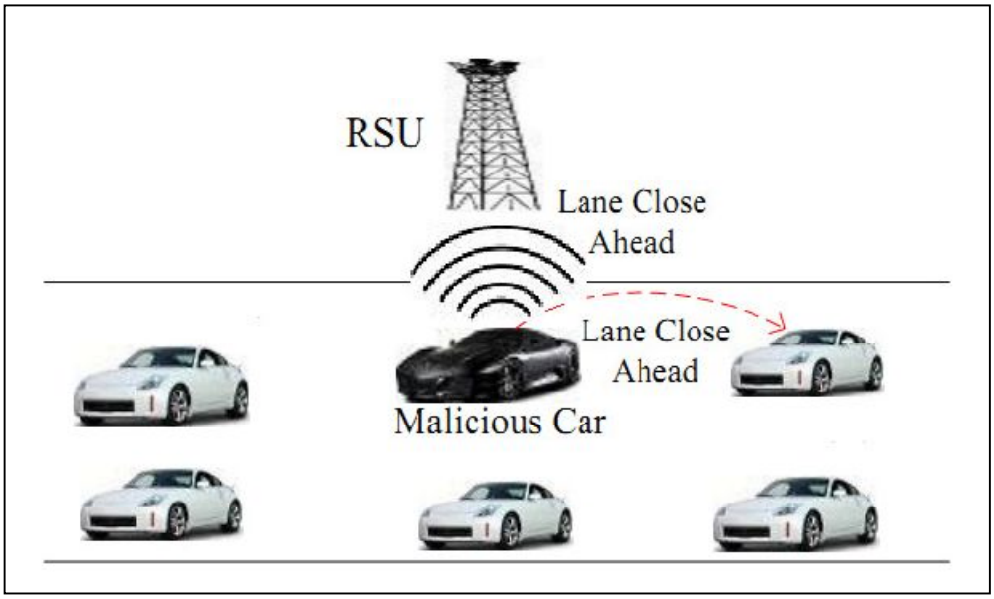


Figure 2.1: Le déni de service

Les requis concernés par ce type d'attaques sont : l'intégrité des données, certains messages pourraient être altérés si les lignes de communication ne sont pas disponibles. Il est évident que le requis de disponibilité sera aussi mis en cause. Si le

réseau est indisponible, il y'a de forte chance que les donnés ne soient pas disponibles pour les applications. Les contraintes de temps réels ne peuvent non plus être respectées dans ces conditions.

Le principal objectif de cette attaque est d'empêcher la réception d'un message lié à la sécurité, donc il vise à annuler les services de sécurité offerts par ces réseaux.

- **L'écoute des messages** :

  Cette attaque consiste pour un attaquant de se positionner à une position dans un véhicule (en arrêt ou en mouvement) ou de se présenter comme un faux « RSU ». Le but de cet attaque est d'accéder à des informations concernant d'autres nœuds et ceci de façon illégal. Le requis mis en cause dans ce type d'attaque est celui de la confidentialité. Le cryptage du message est l'une des solutions préconisée pour y faire face.

- **L'usurpation d'identité :**

  Ce type d'attaque consiste à prendre l'identité de quelqu'un d'autre et de faire croire que vous êtes cette personne Ainsi un adversaire peut perpétrer des actions malicieuses en incorporant dans les messages l'identifiant d'un autre nœud.

  Lorsque les autorités recherchent le coupable de l'action malicieuse perpétrée, ils iront chercher la personne dont l'identifiant a été dérobé. Pendant ce temps, le vrai coupable sera dans la nature. C'est une attaque qui fonctionne pour une communication à un saut car l'attaquant attaque directement sa cible sans passer par des nœuds intermédiaires.

  Ce type d'attaque est difficile à détecter et même difficile à corriger, surtout si la cible est isolée. Les requis qui sont mis en cause dans ce type d'attaque sont : la non-répudiation, si l'identifiant est erroné il est presqu'impossible de retrouver le nœud réellement fautif. La confidentialité et le contrôle d'accès sont aussi en cause dans ce type d'attaques. Car le nœud malicieux peut recevoir des informations en lieu et place du propriétaire de l'identifiant volé. Ce derniers peut aussi accéder à des informations et des services qui étaient réservés pour le propriétaire de l'identifiant.

Cette attaque porte finalement accès à la vie privé de l'usager propriétaire de l'identifiant.

- **Attaque du trou de ver :**

Trou de ver est une attaque sévère dans VANETs et d'autres réseaux ad hoc qui pourrait être considéré comme une variante du Black Hole attaque. Dans cette attaque, deux ou plusieurs nœuds malveillants créer un tunnel pour transmettre des paquets de données à partir d'une extrémité au nœud malveillant à l'autre extrémité et ces paquets sont diffusé sur le réseau. En raison de la nature de la transmission sans fil, un nœud malveillant est capable de créer un trou de ver, même pour les paquets ne sont pas traitées à elle, simplement en les entendant dans un environnement sans fil qui les perce dans un tunnel pour le nœud de connivence à l'autre bout du trou de ver. Le trou de ver permet à l'attaquant d'obtenir un rôle très dominante en comparaison à d'autres nœuds, et il peut exploiter cette position dans une variété de façons, par exemple, d'obtenir un accès non autorisé, de perturber l'acheminement, ou d'effectuer un déni de service (DoS), ainsi, menacer la sécurité ssssde la transmission des paquets de données.

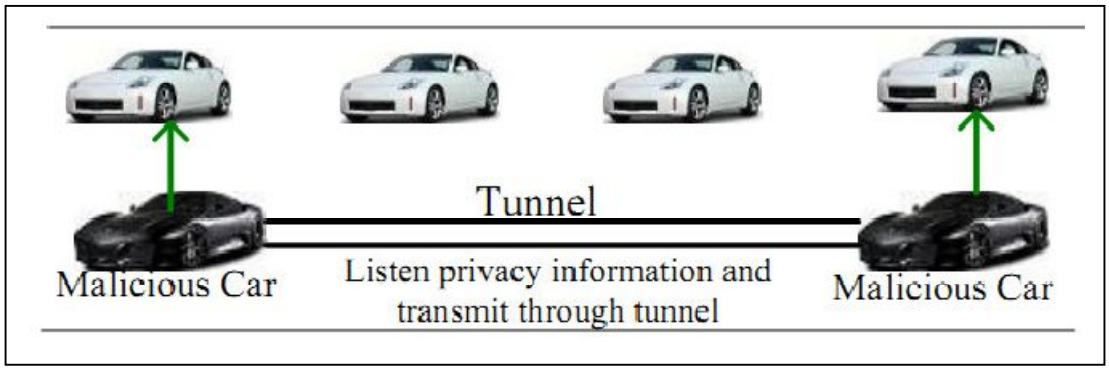


Figure 2.2 : Attaque du trou de ver

- **Altération/falsification des messages:**

La falsification des messages consiste à changer les informations contenues dans un message lors de son passage à travers un nœud. On parle ainsi d'attaque d'altération lorsque le contenu du message est altéré par un adversaire.

Un nœud malicieux peut ainsi changer le contenue ou même le type du message en faisant par exemple croire qu'il y'a un accident alors que ce n'est pas le cas.

Ce type d'attaque est souvent perpétrer par un nœud intermédiaire par lequel le message transite pour retrouver son récepteur. C'est donc une attaque qui est perpétré lors de communications multi-sauts. Par contre ce type d'attaque peut être détecté si le message transite par d'autres nœuds dans le réseau. Dans ce cas il est possible de déterminer que l'information provenant de ce nœud est différent de celle provenant d'autres nœuds du réseau. Mais si le nœud adversaire est le seul par lequel le message transite, il sera difficile de détecter et d'éviter l'attaque.

Cette attaque peut être étendue si plusieurs nœuds reçoivent l'information provenant seulement de l'adversaire. Si un seul nœud reçoit cette information alors l'attaque est limitée à ce seul nœud. Dans ce type d'attaque, le requis concerné est l'intégrité, car le message étant altéré, son intégrité n'est plus garantie.

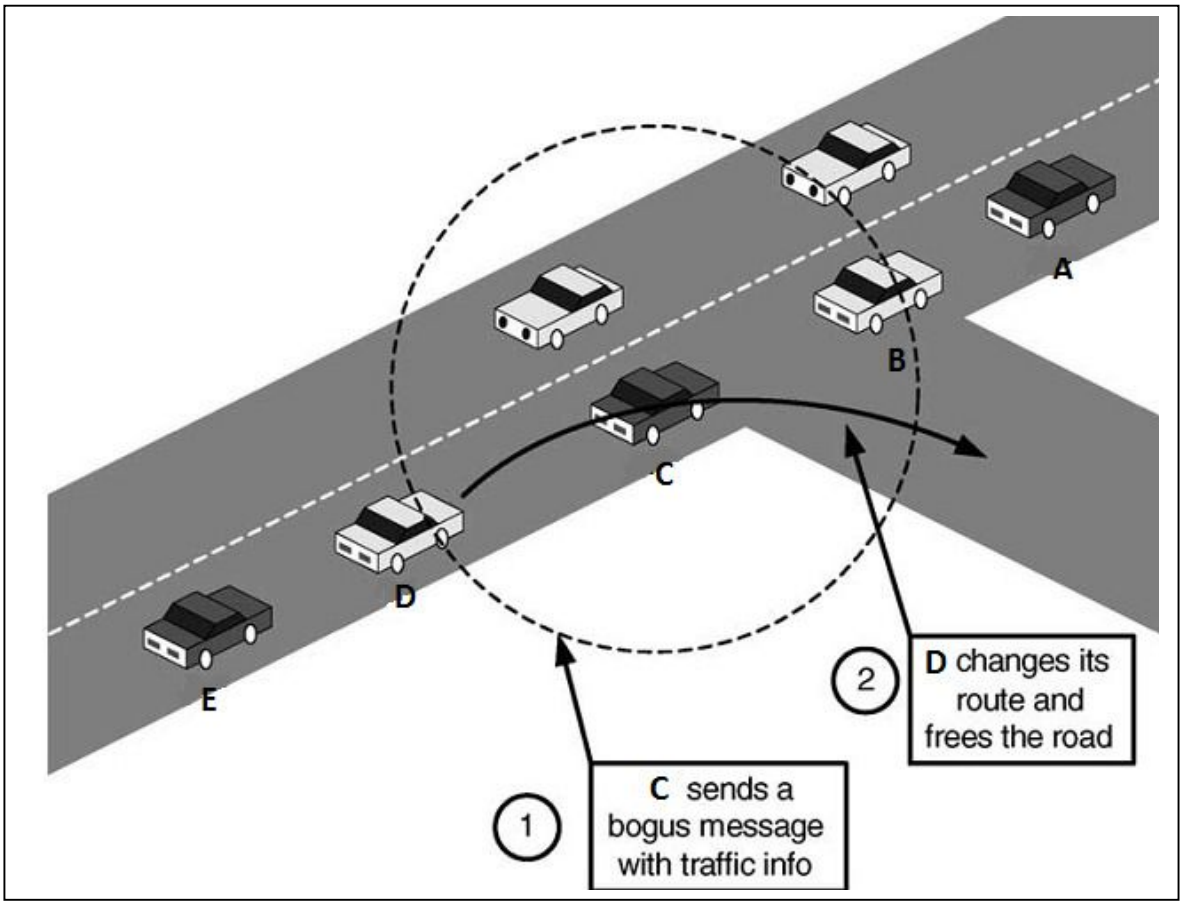


Figure 2.3: Altération/falsification des messages

- **Délai/Suppression des messages:**

  C'est le fait pour un adversaire de conserver le message pendant une certain durée avant le retransmettre. Cette situation a pour effet de créer un délai sur la transmission du message. Dans le pire des cas, l'adversaire peut tout simplement détruire le message et ne pas le transmettre. Le fait de créer un délai au transfert du message occasionne de graves conséquences; surtout s'il s'agit d'application exigent du temps réel. Par exemple un message à propos de l'avertissement d'un accident qui est supprimée causera l'aggravation de l'accident car les véhicules n'ayant pas été informé d'un accident iront s'engouffrer ce qui fera grandir l'ampleur de l'accident. D'autre part, un adversaire peut publier un ancien message concernant un accident. Cette situation aura pour conséquence de faire croire aux autres véhicules qu'il y'a réellement un accident et ainsi causer des situations malencontreuses des véhicules qui agiront comme s'il y'avait un accident.

  Cette attaque est similaire de celle précédemment présentée dans la mesure où le message est intercepté par un véhicule intermédiaire et utilisé à d'autres fins. Mais dans ce cas, ce n'est pas l'intégrité du message qui est en cause mais c'est le message lui-même. Dans le cadre des applications VANETs qui sont généralement contraintes au temps réel, cette situation n'est pas acceptable. C'est une attaque difficilement détectable et corrigible. Le principal requis en cause ici est celui du respect du temps réel et de la disponibilité.

- **Attaque sur le matériel :**

  Cette attaque concerne les équipements matériels. L'adversaire dans ce cas agit physiquement sur les équipements de façon à les rendre dysfonctionnels. Les équipements visés ici sont : les équipements des communications telles que les antennes ou les interfaces de communication, les équipements de calcul tel que l'ordinateur de bord ou encore les équipements de collecte d'information telle que les capteurs, les radars ou encore les récepteurs GPS. Le requis en cause dans ce cas est la disponibilité, les équipements n'étant pas fonctionnelles, il est impossible d'accéder aux ressources, aux services ou encore aux informations.

- **Man in the Middle Attack :**

Comme son nom l'indique, dans cette attaque, véhicule malveillants écouter les communications entre les deux véhicules, fait semblant d'être chacun d'entre eux de répondre l'autre et d'injecter de fausses informations entre les véhicules. Figure 2.4 montre un véhicule dans le scénario d'attaque Moyen, dans lequel le véhicule malveillants C est l'écoute de la communication entre les véhicules B et D ainsi que l'envoi de fausses informations reçues de A à véhicule E. Afin de faire face à ce genre d'attaques, raisonnable solutions sont les communications confidentielles (par exemple, par la cryptographie puissante) pour éviter le fait qu'un attaquant peut écouter la communication parmi les autres, et un sécurisées vérifications d'intégrité des données et l'authentification (par exemple, par des fonctions de hachage) pour éviter les messages modifications. Plusieurs solutions spécifiques qui assurent ces buts ont été présentées dans les parties précédentes.

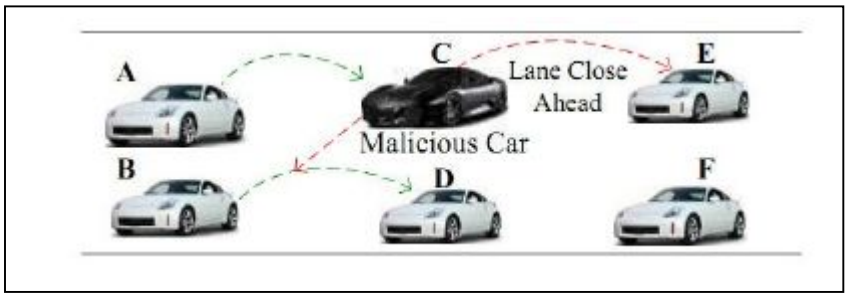


Figure 2.4: Man in the Middle Attack:

- **Attaque Sybil :**

L'attaque Sybil est une attaque blessante bien connu qui a été d'abord décrite et formalisée par Douceur dans le contexte des réseaux peer-to-peer. Pour effectuer ce type d'attaque, un véhicule déclare être plusieurs véhicules, soit en même temps ou successivement. Cette attaque est très dangereuse, car un véhicule peut prétendre être dans des positions différentes en même temps, créant ainsi les risques de chaos et d'énorme sécurité dans le réseau. Les dommages d'attaque Sybil topologies de réseau et des connexions ainsi que la consommation de bande passante réseau. Dans la Figure. 4, un attaquant A émet plusieurs messages avec des identités différentes

aux autres véhicules. Ainsi, d'autres véhicules se rendent compte qu'il existe actuellement un trafic lourd.

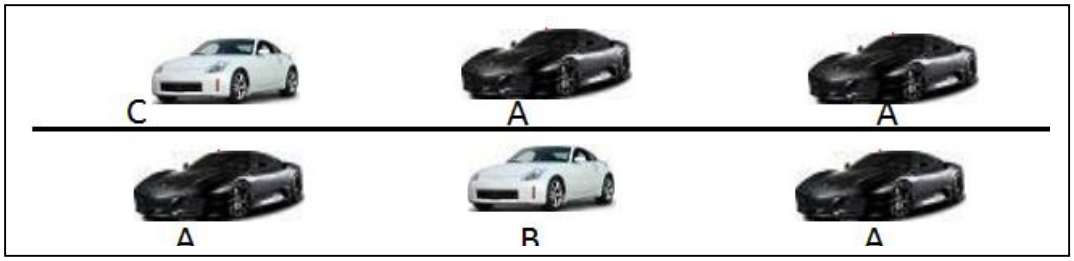


Figure 2.5: Attaque Sybil

Traditionnellement, dans les réseaux ad hoc, il existe trois types de défenses contre les attaques Sybil introduites, à savoir l'enregistrement, la vérification de la position, et l'essai de ressources radio. Enregistrement lui-même ne suffit pas à empêcher les attaques Sybil, car un nœud malveillant a la possibilité d'enregistrer avec des identités multiples par des moyens non techniques tels que le vol. Par ailleurs, un enregistrement strict peut conduire à des troubles graves de la vie privée.

Solutions proposé :

Tous ces problèmes causer par les nœuds égoïstes et malicieux dans les réseaux véhiculaires nous a menus vers une des solutions les plus utiliser et les plus performantes pour ce genre de réseaux, il s'agit des méthodes de réputation qui ont la capacité d'isoler les nœuds malicieux dans le réseau et inciter les nœuds égoïstes a coopérer. Ces méthodes permettent de rendre le plus performent et plus sécuriser.

2.8 Conclusion

Dans ce chapitre nous avons parlé des nœuds égoïstes et malicieux et leur comportement dans les réseaux véhiculaires, et on a parlé aussi des attaques causer par les nœuds malicieux dans ces réseaux.

Dans le chapitre suivant nous nous internant a la solution proposer pour remédier a ces problème, a savoir les méthodes de réputation ou nous allons présentes et expliquer quelques méthodes.

Chapitre 3

Les méthodes de réputation dans les VANETs

3.1 Introduction :

Le dictionnaire Larousse définit le concept de réputation comme étant l'opinion favorable ou défavorable du public à propos d'une personne ou d'une chose. En effet cette définition peut être considérée selon chaque contexte particulier. La réputation a été l'objet d'étude dans plusieurs domaines tels que l'économie, les sciences sociales, l'informatique. Certains sites de commerce électroniques ou de ventes aux enchères en ligne tel qu'eBay et Amazon respectivement sont des exemples où les systèmes de réputation ont été implémentés avec succès. Le concept de réputation peut aussi très bien sied aux réseaux informatiques auto-organisés tel que les réseaux pair à pair (P2P), les réseaux de capteurs et les réseaux ad-hoc mobiles. Ce concept trouve son intérêt dans le fait qu'il permet de doter les systèmes des moyens efficaces permettant aux acteurs de décider avec qui communiquer; dans des environnements où les acteurs n'ont pas une connaissance préalable les uns avec les autres. Ainsi une relation de confiance peut être établie et faciliter les échanges. Les systèmes de réputation appliqués dans un environnement de réseaux mobiles peuvent permettre d'éviter certaines attaques visant ces réseaux. Car la connaissance préalable de certaines informations sur le nœud émetteur, peuvent aider le nœud récepteur à prendre la bonne décision avant d'accepter ou non de communiquer avec ce dernier. Les systèmes de réputation ont fait leurs preuves dans plusieurs applications populaires (moteur de recherche Google…..etc.).

3.2 La notion de réputation [20] :

La **réputation** est l'opinion (plus techniquement, l'évaluation sociale) du public envers une personne, un groupe, ou une organisation. La réputation est un facteur important dans de nombreux domaines, tels que l'éducation, le commerce, le réseautage social ou le statut social.

La réputation est un mécanisme de contrôle social hautement efficace de par son ubiquité et sa spontanéité. Elle est un sujet d'étude en sciences sociales, en management, et en technologies des sciences. Son influence va des secteurs compétitifs tels que le marché, aux secteurs coopératifs comme les firmes, les organisations, les institutions ou les communautés. De plus, la réputation agit sur différents niveaux d'agencements, individuels

et supra-individuels. Au niveau supra-individuel, la réputation concerne les groupes, les communautés, les collectivités, et les entités sociales abstraites (tels que les firmes, les corporations, les organisations, les pays, les cultures, ou même les civilisations). La réputation affecte des phénomènes d'ampleurs très différentes, de la vie quotidienne aux relations entre les nations. La réputation est un instrument fondamental de l'ordre social basé sur un contrôle social distribué et spontané.

3.3 Intérêt de la réputation [21] :

De par sa capacité à être exploité dans les domaines divers, le concept de réputation présente un intérêt primordial pour l'analyse des comportements des entités dans un environnement donné. Dans les sciences sociales, la réputation permet l'étude de comportement des êtres humains dans un milieu social. En économie, la réputation sert plutôt à l'analyse et à la prédiction des tendances économiques en tenant compte des réalités présentes et passées. En informatique, le concept de réputation est utilisé aussi bien dans le domaine de l'intelligence artificielle, du commerce électronique ou encore dans les réseaux auto-organisés (Réseau Ad-hoc, Réseaux de capteurs, Réseaux Mobiles, etc.). Pour ce dernier cas, il permet de garantir la fiabilité des nœuds en communication. Il sert aussi de mesure de comportement des différents nœuds quant à leur collaboration dans la bonne marche du réseau.

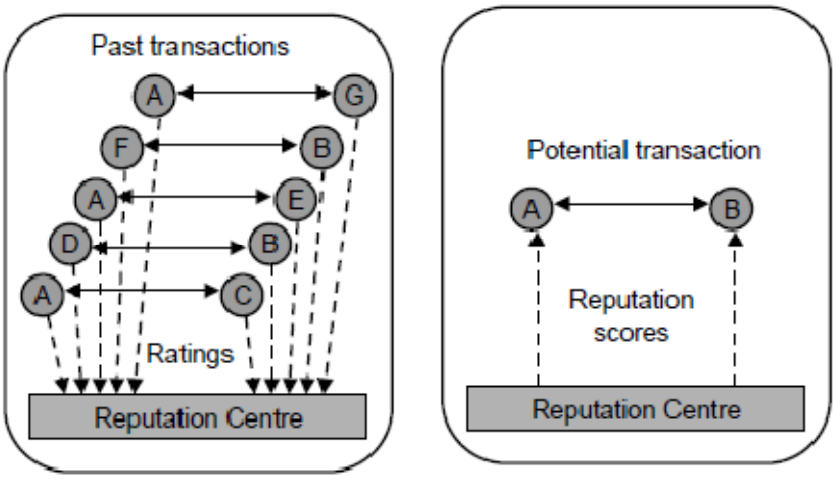
3.4 Architecture des systèmes de réputation [22] :

- **Centralisé :**

Le fonctionnement du premier, centralisé, est décrit figure 3.1. Considérons sept *utilisateurs*, ou *agents A*, *B, C, D, E*, *F* et *G*. Certains d'entre eux peuvent être *fournisseur de service* (par exemple proposer un objet à la vente sur eBay ou partager un fichier en P2P). En plus de ces agents, on considère un *serveur* central (Réputation Centre). Dans le passé, il y a eu des *interactions* ou *transactions*, c'est-à-dire des échanges entre agents. À la figure 3.1(a), *A* interagit avec *G*, *E* et *C* tandis que *B* échange avec *F* et *D*. Les *témoignages*, ou *retours* de chaque utilisateur sur ces transactions sont stockées dans le serveur de réputation. À la figure 3.1(b), *A* se demande si une interaction avec *B* est sûre, c'est-à-dire s'il peut faire

confiance à *B*. Afin d'en apprendre plus, il interroge le serveur pour obtenir la réputation de *B*, tandis que *B* fait la même chose pour *A*. Le serveur calcule le *score de réputation* des deux agents en fonction des témoignages des interactions passées. Compte tenu de la réponse du serveur, et donc des observations des échanges passés, ils décideront ensuite ou non de lancer l'interaction. Si *B* passe pour être un vendeur soigneux, prenant soin de ses colis et que *A* est un utilisateur sans histoire, il n'y a pas de raison pour que l'interaction ne se fasse pas. Au contraire, si *A* est rarement solvable ou que *B* ne protège pas suffisamment des colis fragiles, l'un des deux pourra refuser de prendre le risque de continuer la transaction.

Une architecture centralisée utilise une entité unique sur laquelle repose toute la connaissance, et est donc un point unique de défaillance : si cette entité disparaît, elle emporte tout le système avec elle.

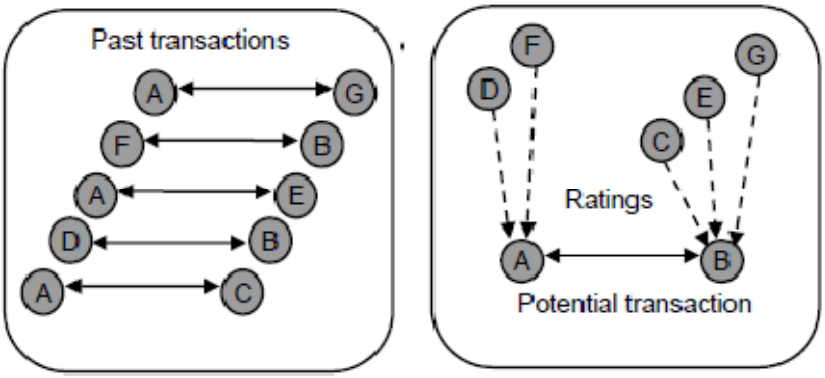


(a) Interactions passées (b) Interaction présente

Figure 3.1 – Interactions dans un système de réputation centralisé

- **Distribué :**

Josang et al. Décrivent une architecture décentralisée telle que présentée à la figure 3.2. Nous supposons les mêmes agents et interactions passées que pour l'exemple précédent. Quand *A* se demande s'il doit ou non interagir avec *B*, il fait un appel à *témoins*, c'est-à-dire aux personnes qui ont interagi avec *B* dans le passé. Ici seuls *D* et *F* vont répondre, tandis que *C*,*E* et *G* vont répondre à *B* à propos de *A*. Les deux pourront ensuite chacun calculer le score global de réputation de l'autre agent et finalement décider ou non d'interagir.



(a) Interactions passées (b) Interaction présente

Figure 3. 2 – Interactions dans un système de réputation distribué

3.5 Les systèmes de réputation [23] :

Un système de réputation calcule et publie des scores de réputation pour un ensemble d'objets (par exemple, les fournisseurs de services, des services, des marchandises ou des entités) au sein d'une communauté ou d'un domaine, basée sur une collection d'opinions que d'autres entités détiennent sur les objets. Les avis sont généralement passés comme notes à un endroit central où toutes les perceptions, les opinions et les évaluations peuvent être cumulées. Un centre de réputation utilise un algorithme de réputation spécifique pour calculer dynamiquement les scores de réputation basé sur les évaluations reçues. La réputation est un signe de confiance manifestée comme un témoignage par d'autres personnes. De nouvelles attentes et réalités sur la transparence, la disponibilité et la vie privée des personnes et des institutions émergent. Gestion de la réputation - l'exposition sélective de l'information et des activités personnelles - est un élément important de la façon dont les gens fonctionnent dans les réseaux car ils établissent pouvoirs, établir la confiance avec les autres, et de recueillir de l'information pour traiter des problèmes ou prendre des décisions.

Les systèmes de réputation sont liés à des systèmes de recommandation et de filtrage collaboratif, mais avec la différence que les systèmes de réputation de produire des scores en fonction des notes explicites de la communauté, alors que les systèmes de recommandations utilisent une consigne externe des entités et des événements (tels que l'achat de livres, de films, ou musique) afin de générer des recommandations de marketing

pour les utilisateurs. Le rôle des systèmes de réputation est de faciliter la confiance, et souvent fonctionne en faisant la réputation plus visible

3.5.1 Exemple de système de réputation [24] :

Les systèmes de réputation peuvent être classés selon leur niveau de complexité en partant des systèmes les plus simples basés sur le vote des participants, vers des systèmes utilisant des algorithmes complexes tels que les systèmes utilisés par Google avec PageRank. Dans la suite, nous présentons trois exemples de système de réputation. Il s'agit du système de notation des pages de Google, PageRank, le système de réputation utilisé par McAfee dans les laboratoires McAfee Labs pour la sécurisation des entités électroniques et enfin le système de réputation d'eBay plate-forme de commerce électronique.

- **Système de réputation PageRanke de google :**

Le **PageRank** ou PR est l'algorithme d'analyse des liens concourant au système de classement des pages Web utilisé par le moteur de recherche Google. Il mesure quantitativement la popularité d'une page web. Le PageRank n'est qu'un indicateur parmi d'autres dans l'algorithme qui permet de classer les pages du Web dans les résultats de recherche de Google. Ce système a été inventé par Larry Page, cofondateur de Google. Ce mot est une marque déposée.

Le principe de base est d'attribuer à chaque page une valeur (ou score) proportionnelle au nombre de fois que passerait par cette page un utilisateur parcourant le graphe du Web en cliquant aléatoirement, sur un des liens apparaissant sur chaque page. Ainsi, une page a un PageRank d'autant plus important qu'est grande la somme des PageRanks des pages qui pointent vers elle (elle comprise, s'il y a des liens internes). Le PageRank est une mesure de centralité sur le réseau du web.

Plus formellement, le déplacement de l'utilisateur est une marche aléatoire sur le graphe du Web, c'est-à-dire le graphe orienté dont les sommets représentent les pages du Web et les arcs les hyperliens. En supposant que l'utilisateur choisisse chaque lien indépendamment des pages précédemment visitées (le réalisme d'une telle hypothèse pouvant être discuté), il s'agit d'un processus de Markov. LePageRank est alors simplement la probabilité stationnaire

d'une chaîne de Markov, c'est-à-dire un vecteur de Perron-Frobenius de la matrice d'adjacence du graphe du Web[1,2]. La taille (gigantesque) de ce graphe et son évolution dynamique (modifications de pages et hyperliens, connexion ou déconnexion de serveur web…) rendent cependant impossible un calcul direct de ce vecteur propre : des algorithmes d'approximation sont utilisés.

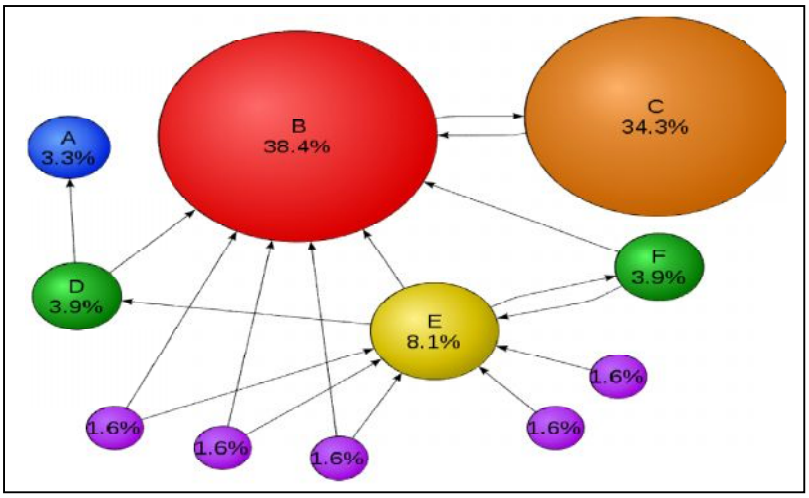


Figure 3.3 : système PageRank

- **Système de réputation de McFee Labs :**

Jamie Barnett présente le système de réputation implémenté dans les laboratoires McAfee Labs pour la sécurisation des données et des entités électroniques. En effet, McAfee calcule la réputation de centaines de millions d'entités électroniques — fichiers, sites et domaines web, messages électroniques, serveurs DNS et connexions réseau — au moyen d'un système de scores de réputation hautement granulaire reposant sur quantité d'informations relatives au comportement et aux caractéristiques de l'entité, ainsi que sur leur propre expérience du comportement d'entités comparables. Entre autres entrées, ils s'appuient sur les données télémétriques obtenues par le biais de milliards de requêtes lancées chaque jour par des dizaines de millions de produits McAfee (clients antimalwares, passerelles de l'environnement web et de la messagerie électronique, pare-feux, etc.) déployés aux quatre coins de la planète et qui servent de sondes pour leur moteur d'analyse dématérialisé.

- **Système de réputation d'eBay**

Avant de participer à une enchère, chaque participant, vendeur ou acheteur doit s'enregistrer en fournissant un certain nombre d'information à eBay. La seule information qu'eBay vérifie est la validité de l'email de l'utilisateur. Lors de l'enregistrement, l'usager choisi un pseudonyme ou un identifiant. C'est cet identifiant qui est montré aux autres membres participants à la transaction. Toutes les informations personnelles révélées à eBay restent confidentielles. Ainsi avec la facilité d'acquérir une adresse email gratuitement sur Yahoo ou Hotmail, chaque usager d'eBay peut rester totalement anonyme vis-à-vis de tous les autres participants. Les vendeurs et les acheteurs peuvent laisser des commentaires les uns sur les autres à la fin de chaque transaction. De plus ils ont la possibilité de laisser une note, +1 (note positive), -1 (note négative), 0 (neutre). Un calcul simple est effectué sur la note qui est donné par les utilisateurs. La valeur totale de la note est considérée en soustrayant les valeurs positives des valeurs négatives.

3.6 Les types de réputation :

La classification des systèmes de réputation peut être effectuée selon différentes approches. Les systèmes peuvent être classés selon plusieurs critères : Initialisation du score de réputation, le type d'observation qui est utilisé, la manière donc les observations sont exploitées, la façon donc les informations sont distribuées à travers le réseau. La majorité des systèmes de réputation sont initialisés de la façon suivante:

- Tous les nœuds du réseau sont initialement considérés comme étant fiables. Chaque nœud a confiance à ces voisins. Le score de réputation de chaque nœud décroit s'il agit de façon répréhensible.

- Chaque nœud du réseau est considéré comme non fiable au démarrage du réseau. Ainsi les nœuds n'ont pas confiance les uns aux autres. Le score de réputation augmente au fur et à mesure que les nœuds démontrent leur bon comportement.

- Chaque nœud du réseau est considéré ni fiable ni non fiable au démarrage du réseau. Chaque nœud démarre donc avec un score de réputation neutre. Le score de réputation changera selon le bon ou le mauvais comportement du nœud

Sur la base des observations qu'ils utilisent, les systèmes de réputation peuvent être classés en deux groupes :

a) **les systèmes utilisant les informations locales encore appelé information de première main :** la décision et le score de réputation sont définis en exploitant les informations provenant des observations réalisées localement,
b) **es systèmes utilisant à la fois les informations de première main et de seconde main pour construire une opinion :** utilisent les deux types d'informations exploitent non-seulement les informations provenant des observations locales mais aussi celles provenant des observations provenant des voisins.

La majorité des systèmes actuels de réputation prennent en compte les observations de première et de seconde main. Dans ce cas, les systèmes ont plus d'information pour pouvoir construire le score de réputation et de prendre les bonnes décisions.

Une autre façon de catégoriser les systèmes de réputation est de les distinguer selon la façon dont ils accèdent aux observations sur le réseau. (i) les systèmes symétriques, (ii) les systèmes asymétriques. Dans les systèmes de réputation symétriques, tous les nœuds du réseau ont accès au même niveau d'information, que ce soient les informations de première main ou de seconde main. Dans les systèmes de réputation asymétriques par contre, tous les nœuds n'ont pas accès au même niveau et à la même quantité d'information. Par exemple dans], les nœuds du « Nœud Sink » (SN) n'ont pas accès à des observations de première main. Cette contrainte peut être un inconvénient pour les nœuds qui ne disposent pas d'assez d'informations pour prendre la bonne décision.

La distribution de la réputation à travers le réseau peut permettre de catégoriser les systèmes de réputation : (i) Centralisée, (ii) Distribuée. Dans les systèmes centralisés, une entité centrale maintient les scores de réputation de tous les nœuds du réseau. Cette entité centrale peut être source de vulnérabilité en termes de sécurité. Parmi les exemples de ce type de système de réputation, nous pouvons citer les sites d'enchère eBay ou encore Yahoo. Dans les systèmes distribués de réputation, chaque nœud peut maintenir les scores

de réputation des nœuds de son voisinage ou encore maintenir les scores de réputation de tous les nœuds du réseau. Dans les réseaux de capteurs, chaque nœud maintient seulement les informations de réputation de son voisinage. Cette disposition réduit considérablement les problèmes de manque de mémoire de stockage.

3.7 La réputation dans les réseaux VANETs :

Introduction

Les VANETS (Vehicular Ad-Hoc Networks) sont considérés comme un ensemble de véhicules qui communiquent les uns avec les autres dans un environnement de transport publique. En fait les véhicules sont dotés d'un ensemble d'équipements qui leurs confèrent la capacité de réaliser un certain nombre d'actions telles que : collecter des informations sur leur environnement proche grâce aux senseurs et aux radars, savoir à chaque instant la position géographique à laquelle ils se trouvent grâce au GPS (Global Positioning System) et la distance des voisins les plus proches, être capable de communiquer les uns avec les autres grâce aux équipements de communications intégrés comme les antennes de communication, une plate-forme de transmission, etc. Les véhicules sont de ce fait intelligents. Ils sont d'ailleurs dotés d'un ordinateur de bord qui permet de traiter toutes les informations collectées par les différents équipements. Cette intelligence accrue dans les véhicules permet aux chercheurs de penser à un nouveau type de réseau informatique, un réseau qui permettrait à un ensemble de véhicules de se partager les informations sur la route de façon à rendre les routes plus sécuritaires, à rendre l'expérience de conduite ou de voyage en automobile plus conviviale et globalement de rendre le système des transports plus fiable. Ces réseaux véhiculaires trouvent d'ailleurs leur origine dans un type de réseau appelé MANET (Mobile Ad-hoc Networks) qui existait déjà. Les VANETs apportent de nombreux avantages pour les usagers de la route, car grâce à eux, plusieurs applications pourraient voir le jour. Malheureusement il s'agit toujours de réseaux informatiques, qui sont soumis à des menaces de sécurité des données transmises et même du réseau sous-jacent. Dans ce cas précis, toutes les brèches de sécurité encourues par les MANETs se trouvent reportées aux VANETs. En plus, il existe d'autres brèches de sécurité inhérentes au cas particulier des VANETs, par exemple l'attaque d'illusion, l'attaque de l'homme du milieu, etc. C'est la raison pour laquelle les exigences en termes de sécurité sont plus grandes dans

ces derniers. Des précautions ont été prises pour la sécurisation des messages transmis dans les VANETs notamment sur les protocoles utilisés pour la transmission des informations.

Depuis quelques années, une activité de recherche intense est menée par les chercheurs à travers le monde, ainsi plusieurs architectures, protocoles, algorithmes ont été proposés pour la sécurisation des VANETs. Certains chercheurs se sont concentrés sur la sécurisation des messages transmis notamment par des méthodes de cryptage par certificat et clé public/privé. D'autres par contre ont jeté leur dévolu sur la sécurisation des protocoles : les protocoles de dissémination des messages, les protocoles de routage des messages, etc. Une autre catégorie de chercheur s'est concentrée sur l'authentification et le filtrage des véhicules dans le réseau. Parmi ces derniers, il y en a certains qui ont choisi la sécurisation par la méthode de réputation. La réputation que nous avons présentée au chapitre précédent, est un concept qui est basé sur l'expérience et la confiance qui en découle. En effet avant d'accepter une communication avec un nœud qui demande à communiquer, le nœud hôte doit se rassurer de la réputation du nœud visiteur grâce à une série de vérification réalisée par lui-même et par ses voisins et ceci grâce à l'expérience des communications précédentes.

Dans sections suivantes nous présentons : les objectifs de la réputation et les types de véhicules dans les VANETS, puis on parlera des Les métriques d'honnêteté dans un système de réputation (La réputation subjective**,** La réputation indirecte, La réputation fonctionnelle) et enfin nous expliquons quelque méthodes de réputation.

3.7.1 Les objectifs d'un système de réputation :

Le système de réputation a deux objectifs :

- ✓ Permettre aux nœuds de trouver les meilleurs partenaires de communication
- ✓ donner à ceux-ci une raison de coopérer (par exemple pour le routage des informations).

Ces deux objectifs englobent les challenges qui guettent tous les réseaux auto-organisés. Notamment le partage des informations et des ressources du réseau pour un objectif commun de bonne marche du réseau. Malheureusement, ces objectifs ne sont pas facilement atteignables, car les instances de coopération dans le réseau n'ont pas tous intérêt à aider au fonctionnement du réseau. Certains nœuds préfèrent profiter des

ressources du réseau sans apporter de contributions; d'autres nœuds par contre souhaitent tout simplement nuire au bon fonctionnement du réseau. Il est donc nécessaire de se rassurer de l'envie de coopération qui anime les acteurs du réseau et surtout se rassurer des opportunités que leur apporte cette coopération.

3.8 Les métriques d'honnêteté dans un système de réputation [25] :

Les métriques d'honnêteté d'un système de réputation varient d'un environnement à un autre dépendamment des objectifs fixés. De plus, la construction de celles-ci impose une étude sérieuse et approfondie des outils utilisés pour arriver au résultat qui déterminera la prise de décision.

- **La réputation subjective**

Le terme réputation subjective est utilisé pour parler de la réputation calculée localement par le nœud hôte. On parle alors d'observation subjective. Une réputation subjective à un temps t par un nœud *si* est calculée en utilisant la moyenne pondérée des facteurs d'observation en donnant plus d'importance aux observations passées. Dans le modèle CORE, plus de pertinence est donnée aux observations passées à cause d'une éventuelle inconsistance des récentes observations. Dans le cadre des réseaux VANETs, cette hypothèse n'est plus valable car les nœuds se déplacent à une vitesse très élevée et l'analyse se fait sur des données récentes. La formule générale du calcul du score subjectif de réputation proposé dans le modèle CORE est la suivante:

$$r_{s_i}^{t}(s_j|f) = \sum \rho(t, t_k) \cdot \sigma_k$$

Ou $r_{s_i}^{t}(s_j|f)$ représente la valeur de réputation subjective calculée à l'instant *t* par le nœud hôte S_i à propos du nœud visiteur S_j en respectant la fonction *f*.

$\rho(t, t_k)$ Représente la fonction de temps qui permet de donner une plus grande pertinence à la valeur des observations.

ρ_k Représente le facteur de notation attribué à la k_{ieme} observation. L'on utilise un intervalle qui part de -1 pour une impression négative (signifiant que l'observation ne correspond pas au résultat espéré), à +1 pour une impression positive (qui signifie que l'observation correspond au résultat attendu). Lorsque la quantité et la qualité des observations collectées depuis le temps *t* ne sont pas suffisantes, la valeur de réputation subjective finale prend la valeur 0 qui exprime une impression de neutralité.

Finalement, en considérant que $\rho_k \in [-1,1]$ et que $\rho(t, t_k)$ est une valeur normalisée, alors

$$r_{s_i}^t(s_j|f) \in [-1,1].$$

L'ensemble s_j est considéré comme l'ensemble des voisins du nœud *i*, le voisinage de *i* est constitué de tous les nœuds qui sont dans le même rayon de transmission que *i*.

- **La réputation indirecte :**

Dans la partie précédente, il était question d'une réputation subjective, prenant en compte seulement les observations collectées par le nœud lui-même. Mais dans la réalité, les choses ne sont pas aussi simples. Dans certaines situations, l'on considère les observations collectées par les nœuds voisins. La réputation indirecte est donc constituée des observations faites par le nœud hôte et celles faites par d'autres nœuds (nœuds voisins préalablement considérés comme honnêtes). On la note: $ir_{s_i}^t(s_j|f)$: Réputation indirecte sur le nœud visiteur *j* par le nœud hôte *i* à l'instant *t* en suivant la fonction *f*. Quelques précautions doivent être prises lors de la collection des informations pour une réputation indirecte. Par exemple, l'on pourrait considérer seulement les notations positives pour éviter que des dénis de service perpétrés par des nœuds malicieux ne soient effectifs et contribuent à une note négative des nœuds légitimes et honnêtes. Une prise en compte du fait, que des nœuds malicieux se concertent afin de noter positivement d'autres nœuds négatifs, est à faire. Sinon, ceci contribuerait à avoir des cas de faux négatifs.

- **La réputation fonctionnelle :**

Le terme de réputation fonctionnelle est utilisé pour représenter le cas où les réputations subjective et indirecte sont calculées en respectant une fonction différente *f*. Ce type de réputation donne la possibilité de calculer une valeur globale de réputation d'un sujet en prenant en compte des critères d'observation et d'évaluations différentes. Par exemple, le nœud hôte *si* peut évaluer la réputation subjective : $r_{s_i}^t\left(s_j|f(packet\ forwarding)\right)$

D'un sujet *sj* en respectant la fonction de transfert de paquets et la réputation subjective $r_{s_i}^t\left(s_j|f(routing)\right)$

en respectant la fonction de routage et ensuite les combiner en utilisant différents poids pour obtenir une réputation globale du nœud ^{S_j} .

Les informations de réputation sont combinées en utilisant la formule suivante:

$$r_{s_i}^t(s_j) = \sum w_k \cdot \{r_{s_i}^t(s_j|f_k) + \mathrm{ir}_{s_i}^t(s_j|f_k)\}$$

Où w_k représente le poids associé à la valeur de la fonction de réputation.

$r_{s_i}^t(s_j)$ Représente la valeur globale de réputation évaluée par chaque nœud. C'est l'agrégation de toutes les valeurs de réputation.

Le choix de w_k est primordial pour la pertinence de la valeur de réputation globale finale. Il est donc important de faire un choix raisonnable de cette variable.

Le choix du modèle pour la construction des métriques de réputation dans les réseaux ad-hoc mobile dépend des objectifs fixés par le concepteur du système. Dans cette section, nous avons présenté deux modèles de construction des métriques de réputation. Globalement, tous les systèmes de réputation visent la sécurisation et le bon fonctionnement des réseaux.

3.9 Les méthodes de réputation :

Il existe plusieurs méthodes (modèle) de réputation, nous expliquons les méthodes suivantes :

- **Watchdog et Pathrater [26]**

Watchdog est un mécanisme qui sert à détecter les nœuds malveillants. Le principe de ce mécanisme est de garder dans un buffer, pour chaque nœud, les paquets transmis et écouter les paquets renvoyés par les autres nœuds. Si les deux valeurs sont égales, cela veut dire que les nœuds ont bien renvoyé les paquets reçus et le paquet sera supprimé du buffer. Si un paquet reste dans le buffer durant un temps supérieur à un certain seuil, le compte d'échec d'envoi est augmenté par Wachdog pour le nœud responsable du renvoi du paquet. Si cette valeur d'échec est supérieure à un certain seuil, cela veut dire que le nœud est malicieux. Cette information sera envoyée au module *Pathrather* dont son objectif principal est la sélection des routes les plus sûres en évitant celles qui contiennent les nœuds malicieux.

Analyse :

Bien que cette approche permette d'éviter la construction des routes qui contiennent des nœuds malicieux, elle ne permet pas de les isoler. En effet, les nœuds détectés comme malveillants peuvent consommer les ressources des autres nœuds pour leur propre communication. De plus, la détection des nœuds malicieux ne fait pas la différence si l'échec d'envoi est dû à un comportement malicieux ou à un lien qui tombe en panne (erreurs de transmission).

3.9.1 CONFIDANT [27] :

Le principe du protocole CONFIDANT (*Cooperation Of Nodes-Fairness in Dynamic Ad hoc NeTworks*) est de traiter à la fois les nœuds malicieux et égoïstes à travers la supervision et l'analyse de deux processus du routage à savoir le transfert des données et la découverte des voisins.

Le protocole CONFIDANT est composé de quatre éléments complémentaires :

a) **Moniteur** :

Le rôle de ce module est de collecter les informations locales sur le comportement des nœuds dans le réseau, ensuite, classer un nœud comme honnête ou malveillant. L'information obtenue est basée donc sur une observation directe par le nœud *i* sur le nœud *j*. Cette information est appelée information *en première main (first-hand information)* ou information locale (F_{ij}). Elle est utilisée comme paramètre d'entrée pour le module gestionnaire de réputation.

b) **Gestionnaire de réputation** :

Le gestionnaire de réputation a pour rôle de gérer une table constituée de deux colonnes : une réservée aux identificateurs des nœuds et l'autre à leur valeur de réputation correspondante. Cette valeur de réputation ne change que si les deux conditions suivantes sont vérifiées : (i) Il y a suffisamment de preuves concernant le comportement malicieux du nœud; (ii) Le nombre d'occurrences du comportement malicieux dépasse un certain seuil. La mise à jour de la valeur de réputation est faite selon une fonction qui attribue des poids selon la provenance de la détection. En effet, une plus grande pondération est affectée à sa propre observation, une autre plus petite à des expériences du voisinage et une pondération faible à des observations rapportées. Cette différence d'attribution de pondération est basée sur le principe que le nœud fait plus confiance à ses propres expériences qu'aux autres. Si la valeur de réputation d'un nœud est inférieure à un certain seuil, le gestionnaire du chemin sera invoqué pour prendre les mesures nécessaires.

c) Système de gestion de confiance :

Le rôle de gestionnaire de confiance est de décider si on fait confiance à l'information globale reçue et de gérer la confiance attribuée aux autres nœuds. Ainsi, l'objectif de ce module est de minimiser le risque de fausses informations.

Des messages d'ALARME sont envoyés par le gestionnaire de confiance afin d'avertir les autres nœuds de la présence des nœuds malicieux. Ces messages d'ALARME sont générés par le nœud lui-même après vérification, observation ou réception d'un rapport sur un comportement malicieux d'un nœud.

Le module gestionnaire de confiance a trois composants qui sont : (a) une table d'ALARME qui contient des informations sur les messages d'ALARME reçus; (b) une table de confiance pour gérer les niveaux de confiance des nœuds afin de déterminer la sureté du message d'ALARME reçu et (c) une liste d'amis contenant la liste de tous les nœuds susceptibles d'envoyer des messages d'ALARME.

d) Gestionnaire de chemins :

Après la classification d'un nœud malveillant *j* par un nœud honnête *i,* il l'isole afin de l'empêcher de participer aux services du réseau. Cette isolation permet de réduire l'effet du comportement malveillant, de motiver les nœuds à coopérer et d'améliorer les services du réseau**.**

Le module gestionnaire de chemins exécute les mécanismes suivants : (i) classer les routes selon une métrique de sécurité (par exemple la réputation des nœuds); (ii) supprimer des routes contenant des nœuds malicieux; (iii) réagir après réception d'une requête RREQ envoyée par un nœud malveillant (par exemple, ignorer la requête et avertir la source) et (iv) réagir après réception de RREP envoyé par un nœud malicieux (par exemple, ignorer le paquet et n'envoyer aucun RREP reçu de ce nœud malveillant).

Fonctionnement du protocole CONFIDANT :

Chaque nœud gère le comportement de ses voisins immédiats et met à jour les réputations, des nœuds en conséquence. Cette mise à jour est faite en détectant un comportement

égoïste du prochain nœud. La détection peut être soit directe grâce à l'écoute passive des transmissions du prochain saut, ou indirectement grâce aux rapports envoyés dans le réseau.

Si un événement soupçonneux est détecté, cette information est envoyée au gestionnaire de réputation. Si cet événement est significatif, il vérifie l'occurrence de ce dernier. Si l'événement est répété pour un nombre qui dépasse un certain seuil (prédéfini par le protocole et qui est suffisamment grand pour différencier entre l'événement dû à un comportement malicieux de celui causé par une collision). Si ce seuil est dépassé, le gestionnaire de réputation met à jour la valeur de réputation du nœud qui a causé l'événement. Si cette valeur devient intolérable, cette information est rapportée au gestionnaire de routes. Ce dernier supprime toutes les routes enregistrées dans le cache du nœud qui contiennent le nœud malveillant. Le nœud continu à surveiller le voisinage et un message d'ALARME est envoyé à la source.

Ce message contient les informations suivantes : le type de violation du protocole, le nombre d'occurrences observées, l'adresse du nœud rapporteur de l'alerte, l'information pour savoir si le nœud qui a envoyé l'alerte est le générateur de l'alarme, l'adresse de la destination (et même le message peut contenir l'adresse source de la route ou l'adresse d'un ami qui pourrait être intéressé).

Lorsque le moniteur d'un nœud reçoit un message d'ALARME, il le transfert au gestionnaire de confiance qui évalue la confiance de la source du message. Si la source est un nœud de confiance (la confiance ne dépasse pas le seuil prédéfini par le protocole), la table contenant les messages d'ALARME est mise à jour. S'il y a suffisamment de preuves sur le comportement malicieux d'un nœud, cette information est rapportée au gestionnaire de réputation qui à son tour réévalue la valeur de réputation. Les preuves sont considérées comme suffisantes, si le message d'ALARME est envoyé par un nœud de confiance totale (la valeur de confiance dépasse le seuil prédéfini par le protocole), ou plusieurs nœuds de confiance partielle (la valeur de confiance est inférieure au seuil) envoient le même message d'ALARME dont la somme de leur valeur de confiance peut être attribuée à un nœud (ou plusieurs) de confiance totale.

La version initiale de CONFIDANT est faible contre la propagation des rumeurs il y a un compromis entre l'utilisation efficace des informations disponibles dans le réseau et la robustesse contre des fausses accusations.

Une amélioration a été proposée pour faire face à ce problème en se basant sur toutes les informations disponibles dans le réseau : expériences positives (comportement honnête) et négatives (comportement malveillant); ses propres observations et celles des autres. Dans cette amélioration, chaque nœud *i* a deux taux à propos d'un nœud *j*: 1- un *taux de réputation* (R_{ij}) qui reflète l'opinion du nœud *i* sur le nœud *j* à propos de son comportement dans le réseau (par exemple si le nœud *j* participe dans le routage); 2- un *taux de confiance* (T_{ij}) qui représente l'opinion du nœud *i* sur le nœud *j* à propos de son honnêteté dans le système de réputation (par exemple si les informations rapportées et diffusées par le nœud *j* sont vraies). De plus, le nœud *i* enregistre les premières informations obtenues sur *j*, dans une structure de donnée appelée (F_{ij}). Cette information (envoyée à *i*) décrit les opinions des autres nœuds sur le comportement du nœud

j. Le principe de cette amélioration est de tirer profit des informations de réputation diffusées dans le réseau, et de même des observations effectuées d'autres nœuds avant l'évaluation de sa propre expérience. Ceci est fait en respectant les étapes suivantes : 1- Si le nœud *i* fait sa première observation sur le comportement du nœud *j*, alors *i* met à jour la valeur de réputation R_{ij}, et la valeur de première information (*first hand information*) F_{ij}; 2- chaque nœud *i* publie périodiquement les valeurs de premières informations sur les nœuds *j*. Par conséquent, le nœud *i* recevra périodiquement des premières informations sur le nœud *i* par les nœuds *k* (*first hand information* F_{kj}). Si *k* est un nœud de confiance par rapport au nœud *i*, ou si F_{kj} est proche de R_{ij}, alors F_{kj} est accepté et sera utilisé pour modifier légèrement R_{ij}. Sinon, R_{ij} ne sera pas mise à jour. Dans tout les cas T_{ik} sera mise à jour. En effet, si F_{kj} est proche de R_{ij}, T_{ik} sera légèrement améliorée. Sinon, elle sera légèrement dégradée.

Les mises à jour utilisées sont faites en suivant un modèle Bayesian. Notons que dans cette nouvelle version de CONFIDANT, seulement les valeurs de F_{ij} seront diffusées périodiquement. Les valeurs de R_{ij} et (T_{ij}) sont utilisées pour classer les nœuds en *normaux/anormaux* (*normal/misbehaving*) et *honnêtes/malicieux (trusworthy/untrustworthy)* respectivement. Les deux classifications se basent sur l'approche Bayesienne pour la classification qui permet de réduire l'impact de fausse accusation.

Analyse :

Bien que le protocole CONFIDANT permette de détecter le comportement égoïste d'un nœud et de l'isoler, il souffre du problème de sociabilité. En effet, en augmentant le nombre des nœuds dans le réseau, la table de réputation pour chaque nœud devient gourmande. Ainsi, avec des scénarios de forte mobilité, la surcharge de réseau (*overhead*) augmente d'une manière considérable ce qui dégrade les performances du réseau. La classification des nœuds dans le protocole CONFIDANT est fondée sur une classification binaire *(normal/anormal ; honnête/malicieux*), cependant un système à n-niveaux s'avère plus flexible et plus fiable. De plus, les seuils utilisés dans le protocole CONFIDANT : le nombre d'occurrences, le seuil de réputation et de confiance sont des valeurs empiriques.

3.9.2 OCEAN [28] :

Le fonctionnement du protocole OCEAN est basé principalement sur les observations directes d'un nœud (*first hand observations).* Le protocole distingue entres deux différents comportements anormaux de nœuds : (1) un comportement appelé *trompeur (misleading),* c'est le cas où un nœud participe correctement aux processus d'envoi des requêtes de routes, mais il refuse d'expédier les paquets de données et (2) un autre comportement anormal plus précisément *égoïste (selfish)* pour lequel un nœud ne participe à aucun processus de routage sauf s'il s'agit de router ses propres paquets où il sollicitera les ressources des autres nœuds.

Architecture du protocole OCEAN :

Le protocole OCEAN est composé de cinq éléments :

a) Moniteur :

Ce module a pour rôle d'observer le comportement du voisinage d'un nœud. Il repose sur la nature omnidirectionnelle des antennes et suppose que les liens soient bidirectionnels. Après l'envoi d'un paquet, le moniteur enregistre un checksum du paquet dans un tampon et contrôle le canal sans fil. Si après un timeout (par défaut 1s), le moniteur n'écoute aucune expédition du paquet par le voisin, il enregistre un événement négatif contre ce dernier et supprime le checksum enregistré dans le tampon. Sinon, le moniteur vérifie le checksum du paquet expédié par le voisin et celui enregistré dans le tampon, dans le cas d'une égalité il enregistre un événement positif pour le nœud voisin et supprime le checksum du tampon. Si les deux checksums sont différents, il considère le paquet comme non envoyé. Les événements enregistrés sont rapportés au gestionnaire de route qui enregistre les estimations des nœuds voisins. Le moniteur est un module qui offre un service non garanti. En effet, il souffre de toutes les erreurs potentielles du mécanisme *Watchdog*, par exemple observer qu'un voisin envoie le paquet n'assure pas que ce paquet soit reçu avec succès.

b) Gestionnaire de route :

Il enregistre des estimations de tous les nœuds voisins. Cette estimation sera incrémentée ou décrémentée selon le type d'événement, respectivement positif, ou négatif, envoyé par le moniteur. Des études empiriques ont montré que la valeur absolue de décrément doit être supérieure d'un incrément. Lorsqu'une estimation est inférieure à un certain seuil (*faulty-threshold*), le nœud est ajouté à la liste des nœuds malicieux (*Faulty-list*).

Une route sera considérée comme bonne ou mauvaise selon l'appartenance ou non du nœud de prochain saut à la liste des nœuds malicieux.

c) Gestionnaire de réputation :

Ce module applique les informations collectées par le moniteur afin de filtrer les routes. Pour éviter les nœuds enregistrés dans la liste des nœuds malicieux, un champ de taille variable est ajouté dans l'entête du paquet RREQ appelé *avoidlist* et qui contient les nœuds enregistrés dans la liste des nœuds malicieux. Ce champ permet de spécifier les nœuds à

éviter lors de la diffusion des RREQs. Chaque nœud recevant RREQ vérifie tout d'abord le contenu du champ *avoid-list*. Si le chemin ne contient aucun nœud enregistré dans *avoid-list*, il peut traiter la requête RREQ (diffusion de RREQ ou envoi de RREP à la source). Sinon, le nœud supprime RREQ. Le traitement d'un paquet RREP est traité de la même manière que celui du paquet RREQ. En effet, si un nœud reçoit RREP dont le chemin ne contient aucun nœud qui se trouve dans *avoid-list*, il envoie le paquet RREP à son voisin, sinon il le supprime.

d) Gestionnaire des trafics malicieux :

Le gestionnaire des trafics malicieux rejette tous les trafics envoyés par les nœuds traités comme trompeurs. Ainsi, ce mécanisme empêche le nœud trompeur de relayer son propre trafic au nom d'un autre nœud.

e) Mécanisme de deuxième chance :

Le mécanisme de deuxième chance est utilisé pour permettre aux nœuds considérés comme trompeurs de redevenir normaux. Ceci est prévu car le moniteur n'offre pas un service garanti du moment où la détection d'un échec d'envoi ne fait pas la différence entre un refus d'envoi intentionnellement fait par un nœud malicieux ou causé par une erreur accidentelle d'un lien. Le principe est donc de supprimer le nœud malicieux qui se trouve dans la liste des nœuds malicieux après un timeout prédéfini dit *faulty-timeout*. Néanmoins, cette suppression n'implique pas la mise à neutre de la valeur de réputation du nœud. Ce qui permet d'ajouter rapidement un nœud si son comportement malveillant persiste.

Comportement égoïste :

Le but du protocole OCEAN est d'atténuer l'effet du comportement égoïste des nœuds.
L'idée est de punir les nœuds égoïstes en rejetant leur trafic dans le souhait qu'ils changeront leur comportement.
Pour atténuer l'effet du comportement égoïste des nœuds, OCEAN utilise le principe de monnaie virtuelle en se basant uniquement sur les expériences d'un nœud et les observations directes de ses voisins. Pour ceci, chaque nœud enregistre pour chaque voisin

un compteur appelé *chipcount* qui sera incrémenté lorsqu'un nœud sollicite un autre nœud pour envoyer un paquet et il sera décrémenté s'il y a une demande entrante à ce dernier. Supposons qu'un nœud *B* demande à un nœud *A* d'expédier ses paquets, le nœud *A* vérifie le *chipcount* de *B*. Si le *chipcount* de *B* est très bas alors il rejette ses paquets. Cette technique est injuste et pénalise les nœuds qui se trouvent dans l'extrémité du réseau ad hoc mobile, puisque ces derniers ne sont pas trop sollicités pour relayer les paquets des autres nœuds. Pour faire face à ce problème, OCEAN fait intervenir un nouveau paramètre qui calcule le taux d'accumulation de jetons dit CAR *(Chip Accumulation Rate).* CAR exprime le taux d'augmentation de c*hipcount* en fonction du temps. À cet effet, un nœud *A* peut relayer le trafic d'un nœud *B* qui se trouve dans le périmètre du réseau même avec un *chipcount* réduit.

Analyse

Le seuil *faulty-lithreshold* exprime la vitesse de détection d'un comportement malicieux d'un nœud. Des expériences ont montré qu'une valeur basse de ce seuil permet d'ajouter rapidement un nœud à *faulty-list*, tandis qu'une valeur élevée pourrait retarder la détection d'un comportement malicieux. De plus, les auteurs du protocole OCEAN proposent une valeur empirique à ce seuil.

Le champ *avoid-list* qui maintient la liste des nœuds malicieux n'est pas protégé contre la modification. En effet, n'importe quel nœud peut modifier facilement le contenu du champ et lancer facilement une attaque de type *wormhole*. Les études ont montré que le protocole préserve ses performances tant que le réseau est mobile.

Finalement, le protocole OCEAN diminue le comportement égoïste des nœuds en les motivant à coopérer via l'utilisation des compteurs *chipcounts*. Les résultats ont montré que ce mécanisme permet de dégrader les performances du protocole en termes de consommation de la bande passante.

3.9.3 VIME (a VANET Incentive Model with Exclusion for malicious nodes): [29]

Est une méthode de réputation qui est inspiré du modèle économique et qui est basé sur la monnaie virtuelle (crédit) elle permet d'éradiquer les véhicules malicieux, et à accroître la participation des nœuds égoïstes.

Chaque véhicule du réseau reçoit un crédit initial lors de son entré dans le réseau, ce crédit évoluera (augmentera ou diminuera) selon son comportement dans le réseau. Si un véhicule veut envoyer un message il doit payer un cout, ce cout est calculé selon la réputation du véhicule, un véhicule qui a une bonne réputation payera moins qu'un véhicule qu'en a une mauvaise réputation.

Quand un véhicule reçoit un message il vérifié la validité de se dernier et si il comme quoi il est valide alors il récompense la source en lui envoyant du crédit le score de réputation est calcul à partir de la valeur de réputation qu'il reçoit de ses voisin.

Lorsque les crédits sont insuffisants pour payer le coût correspondant, un véhicule ne peut pas envoyer son message il est expulsé du réseau et il est considéré comme malveillant.

Les fonctions utilisées par cette méthode sont représenté comme suit :

a) **Envoi Coût**:

Selon la stratégie de marché, une source nœud prend le rôle d'un fournisseur de service qui doit offrir un garantir à propos de ses produits à ses clients. Cette garantie dépend de nombreux paramètres tels que la réputation du nœud source, un coût standard fixé par l'application, et de l'importance des données. Un coût de garantie pour un message est individuel et diffère de la même information, même entre le nœud de source et le nœud relayé pour ce message. Dans notre environnement, ce garantie est traduit en un coût appelé le gendarme i (N (i)) l'habitude de diffuser un message du nœud i à ses voisins N (i). Ce coût doit être important pour le nœud de source selon son montant initial de crédits donnée lors de sa première connexion au réseau, init_credit. Il doit également être compatible avec quant à l'importance de l'information partagée, i_msg, situé sur une plage de 0 à 1. Enfin, il a pour répondre en même temps à toutes les attentes des voisins dans de garantie, de sorte que les récepteurs considèrent et acceptent le message.

b) Réputation Pertinence pour la Récompense

VIME utilise une fonction pour la pertinence de la réputation, W (Rt i (j)). Il attribue un poids à Rti (j), la valeur de la réputation d'un expéditeur / transitaire nœud j calculée par un nœud récepteur i au temps t. ce poids est utilisé pour l'estimation de récompense. Il permet une rémunération plus élevée pour la réputation élevée par rapport aux nœuds inférieurs de réputation pour la même action, incitant ainsi les nœuds pour maintenir une bonne réputation.

c) Calcul de la valeur de récompense :

L'objectif de la récompense est de faire en sorte que le système reste incitation pour les bons nœuds et de décourager à l'malveillants une. En outre, elle représente un coût de recevoir des informations. Ce diminue le nombre de crédit de nœuds quand récompenser nœuds source. En outre, afin de gagner des crédits, et la récompense reçue messages, nœuds égoïstes sont encouragées à coopérer. Lorsque le coût payé par un nœud source pour son message à la hauteur à la garantie prévue par le récepteur, le récepteur examine le message et décide de sa confiance sur les données. Si le récepteur considère le message comme valide, il récompense la source nœud en lui envoyant un peu de crédit par l'intermédiaire de son crédit d'inviolabilité compté. Le montant dépend du coût payé par la source, la densité autour d'elle, qui correspondent au potentiel rewarder nœuds, et la valeur de la réputation tenue sur le nœud source.

Analyse :

Le model VIME n’est pas protégé contre les fausse accusations et les faux témoignages car le score de réputation d’un nœud est calculé a partir des score de réputation des nœuds voisins c’est se qui n’empêche pas certain nœud de mettre de faux score de réputation et ainsi réduire la performance du réseau.

3.10 Conclusion :

Dans ce chapitre, nous avons présenté le concept de réputation et des systèmes de réputation, les catégories de systèmes de réputation ont aussi été abordées, les systèmes de réputation peuvent être catégorisés de plusieurs façons selon différentes caractéristiques. L'architecture des systèmes de réputation a aussi été abordée, un système de réputation doit disposer d'un processus d'observation, un processus de stockage des observations, un processus de traitement et un processus de prise de décision. Nous avons présenté trois exemples de systèmes de réputation. Puis on a abordée les méthodes de réputation dans les réseau de VANETs ou on a présenter trois méthodes (**Watchdog et Pathrater , CONFIDANT , OCEAN,VIME).** Nous nous inspirerons de ces méthodes pour mettre en place notre système de réputation pour la sécurisation des VANETs dans le chapitre suivant.

Chapitre 4

Conception d'un système de réputation

4.1 Introduction :

Dans notre travail, nous avons élaboré un système de réputation, que nous intégrons dans chaque nœud participant au réseau lui permettant de faire les analyses nécessaires, grâce à un algorithme, et ainsi de prendre la bonne décision quant au choix d'accepter ou non, de communiquer avec le nœud .

Ce système de réputation qui est basé sur la monnaie virtuel permet d'éliminer les nœuds égoïstes et malicieux du réseau ainsi que d'encouragé les nœuds égoïste a coopérer dans le nœud.

4.2 Conception du système :

Nous avons conçu notre système de réputation à partir du modèle VIME qui est basé sur la monnaie virtuel.

Nous avons changé la méthode de calcule du score de réputation de VIME et nous avons utilise la méthode de CONFIDANT car elle est basé sur les informations de première main.

En effet, la méthode de calcule du score de réputation de VIME est calculé a partir des score de réputation des nœuds voisins se qui n'empêche pas certain nœud de mettre de faux score de réputation et ainsi nuire au réseau.

4.3 Les requis du système :

Les systèmes de réputation sont utilisés dans les domaines aussi variés que les sciences sociales, l'économie, l'informatique et particulièrement dans l'intelligence artificielle ou encore les réseaux mobiles. En ce qui concerne les réseaux mobiles, ils sont utilisés pour la sécurisation et l'optimisation des réseaux auto-organisés. Le but d'un système de réputation est surtout d'aider à la prise de décision en dotant les usagers d'une capacité à déterminer la confiance d'un interlocuteur. Ces systèmes pour être fiables doivent disposer des caractéristiques suivantes : intégrer un processus d'observation, un processus de stockage de ces observations, un processus de traitement et un processus de prise de décision.

4.4 Les modèles du système :

Cette section présente les différentes entités qui constituent notre système de réputation. Dans un premier temps, nous présentons le modèle du véhicule, qui indique les équipements dont ce dernier est doté pour permettre l'implémentation du système de

réputation. Ensuite, nous présentons le modèle du réseau qui indique la topologie réseau dans laquelle les véhicules évoluent.

4.4.1 Le modèle du véhicule :

Jean Pierre Hubaux et al. ont proposé un modèle de véhicule constitué d'un certain nombre d'équipements et d'un ensemble de processeurs connectés à un ordinateur central, avec des connecteurs Ethernet, wifi, Bluetooth, USB et une interface de communication IEEE 802.11, qui permettent à un véhicule d'avoir une certaine intelligence. C'est ce modèle de véhicule que nous prenons en considération dans la réalisation de notre travail. En effet, ce véhicule est constitué des équipements suivants :

- Un enregistreur des données des évènements (EDR : Event Data Recorder). C'est un équipement inspiré de la boite noire dans les avions. Il enregistre toutes les informations durant tout le voyage et peut aussi aider à la reconstruction des évènements précédents un accident.

- Un récepteur GPS (Global Position System) permet de connaître la position du véhicule et la topologie de la route à tout instant.

- Des radars avants et arrières permettent de détecter les obstacles jusqu'à une distance de 200 mètres.

- Une interface de communication Wifi prend en compte les signaux DSRC (Dedicated Short Range Communication) et sont dédiés aux communications rapides spécialisés pour les VANETs.

- Un identificateur électronique unique du même type que la plaque d'immatriculation.

Globalement le véhicule est doté de capacité sensorielle, de mémoire, de traitement de l'information, et de détection de la position géographique, de communication et de comportement adaptatif.

Dans cette recherche, nous allons nous baser sur les travaux de Maxim Raya et al, pour considérer que la majorité des véhicules sur les routes sont honnêtes et se comportent de façon responsable. Les différentes informations exploitées sont considérées comme

disponibles grâce aux paquets envoyés par les nœuds qui tentent d'entrer en communication. Et les paramètres de vérifications utilisées par les véhicules qui effectuent l'analyse sont considérées comme disponibles via les différents équipements dont disposent ces véhicules. Il s'agit entre autre des radars, des GPS, des capteurs et aussi des informations déjà collectées par d'autres véhicules du réseau, le véhicule (récepteur) qui est sollicité pour la communication sera appelé véhicule hôte. Dans la suite, puisque nous considérons un environnement réseau, nous utiliserons les termes véhicule et nœud pour nommer les véhicules en communication.

4.4.2 Le modèle du réseau :

Nous considérons le scénario de communication d'une autoroute, et nous faisons fi des cas du centre-ville, des zones rurales, des zones résidentielles et tout autre environnement de transport public. Malgré la présence de deux types de cellules dans la littérature pour la modélisation des VANETs, nous considérons seulement le cas des cellules basées sur la position géographique. Ainsi l'ensemble des voisins sera l'ensemble des véhicules présents à l'intérieur du diamètre de la cellule et avec lesquels la communication est établie. Nous considérons que le rayon de transmission de chaque nœud est égal au diamètre de la cellule. Le type de cellule considéré est celui de la figure 4.2. Tout nœud qui tente d'entrer en communication avec les nœuds du réseau devra transmettre un message du même type que celui de la figure 4.1 proposé par Jyoti Grover et al. . Les variables publiées dans l'entête du message de la figure 4.1 dépend du type d'application. Deux acteurs sont concernés, le nœud hôte, les nœuds voisins au nœud hôte. Les nœuds voisins sont ceux qui appartiennent à la même cellule et qui ont déjà communiqué avec le nœud hôte.

ID	position	speed	time	crédit	cout du message …….	Message

Figure 4.1: Structure d'un paquet de type VANET

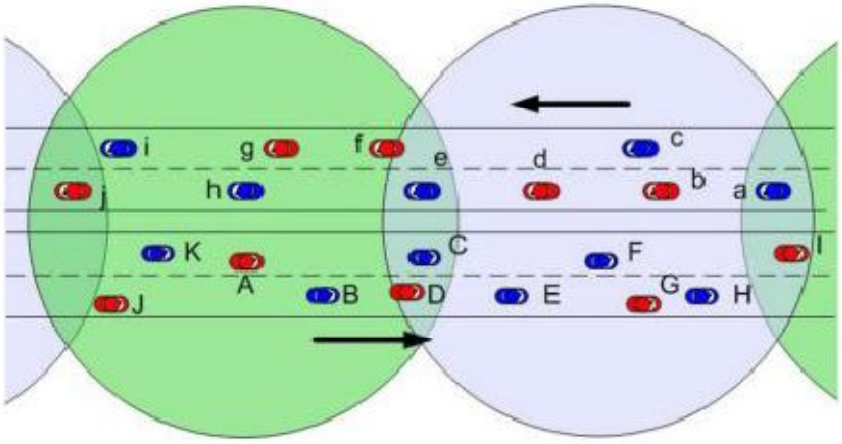


Figure 4.2: Structure d'une cellule VANET

4.5 Architecture :

Dans cette section, nous présentons l'architecture de notre système de réputation. Il est constitué de plusieurs parties qui contribuent au calcul du score global de réputation et donc à la prise de décision qui permettra au nœud hôte d'accepter ou de refuser les messages.

4.5.1 Présentation du parcours d'un paquet :

Avant de présenter notre architecture, nous présentons le contexte dans lequel nous considérons que le système de réputation fonctionnera.

En effet, le système de réputation agit à partir de l'interface réseau, entrée/sortie des paquets. Nous considérons qu'un message reçu par le nœud doit passer au travers du système qui est constitué d'un algorithme divisé en plusieurs modules de vérification avant d'être exploité par le VANET. Ainsi, nous présentons le parcours d'un paquet, à partir de son arrivée sur l'interface réseau jusqu'à son exploitation.

La figure 4.3 est une représentation de ce parcours. En effet, le paquet arrive à l'interface d'entrée du nœud. Ensuite, ce dernier est directement soumis au système de réputation qui vérifie que les variables publiées via ce paquet par le nœud sont conformes aux paramètres attendus par le noud hôte. Une fois cette vérification terminée, une décision est prise quant à l'acceptation ou le refus du paquet. Si le score des différentes variables est bon alors le paquet peut traverser le système de réputation avec succès et le noud est donc considéré comme honnête. Ensuite, l'intégrité des messages est vérifiée par un second module qui en a la charge. Si cette étape est traversée aussi avec succès, alors le paquet peut être exploité sans crainte.

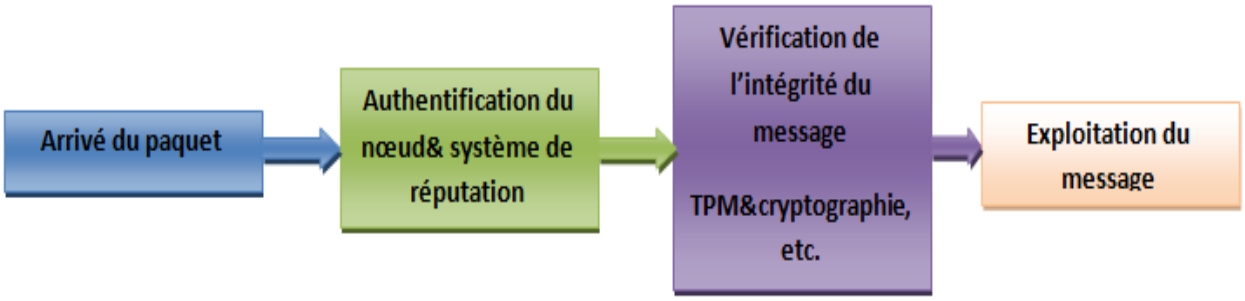


Figure 4.3: Parcours d'un paquet de son arrivé à son exploitation

Selon les cas, l'initiation de la communication se fait en plusieurs phases :

- la phase de découverte du réseau qui est classique pour tous les réseaux ad-hoc. Durant cette phase, le nœud envoie des trames beacon pour découvrir le réseau.
- dans la phase d'acceptation, les trames beacon sont soumises au système de réputation de chaque nœud qui l'a reçu avant que ce dernier l'accepte en tant que voisin.
- la phase de communication effective : si le nœud est accepté, alors il peut partager des informations avec les autres nœuds du réseau.

4.5.2 Fonctionnement interne de l'architecture proposée

L'architecture proposée pour le système de réputation décrit les différents modules qui le constituent. Il s'agit des variables reçues du nœud visiteur, des listes utilisées pour stocker les identifiants et les différents scores de réputation, les différentes fonctions d'analyses des variables, du module d'agrégation des notes obtenues pour chaque variable par chaque fonction d'analyse, du module d'agrégation des scores de réputation et du module de prise de décision.

- **Architecture du système de réputation :**

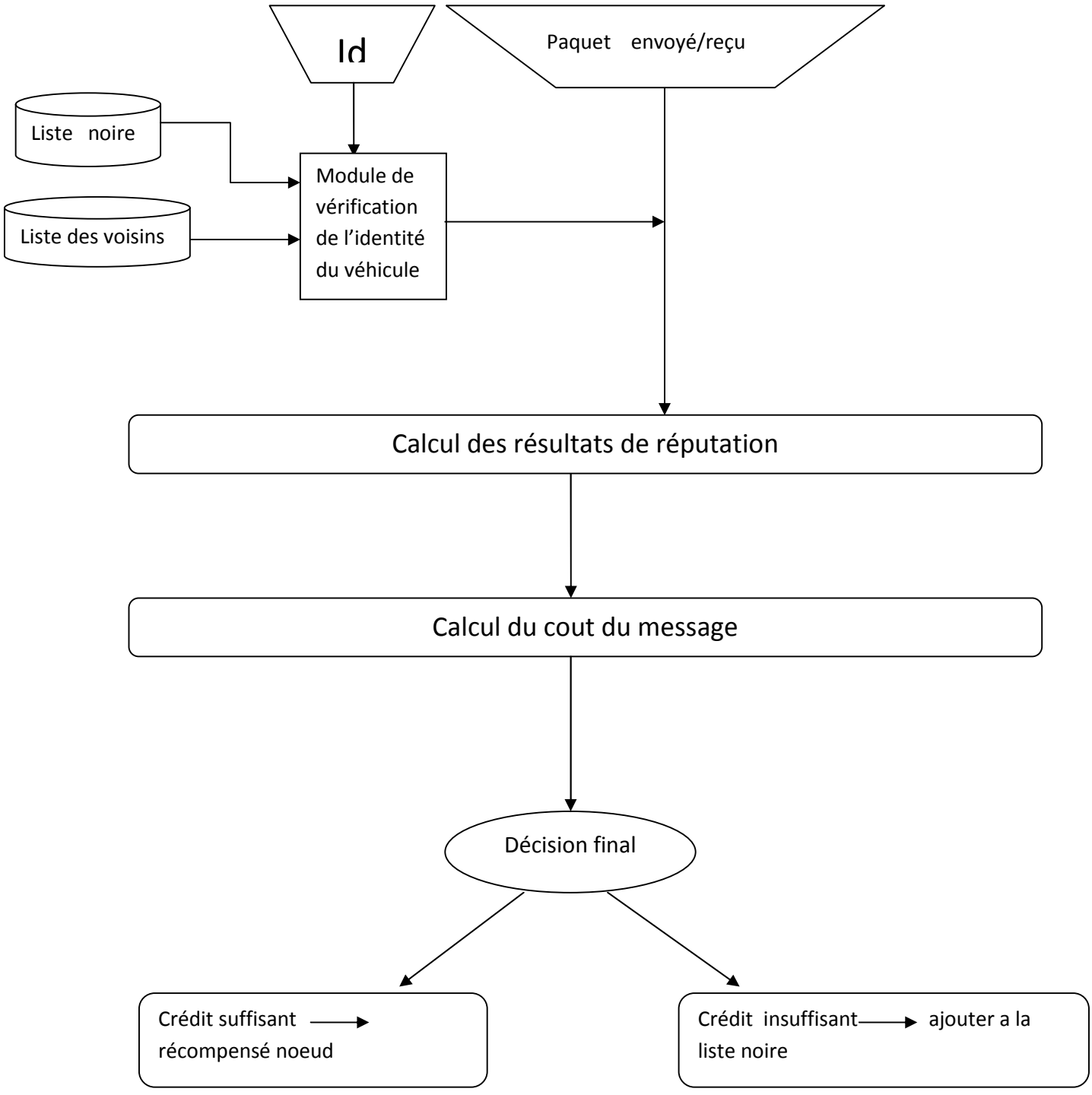


Figure 4.4 Architecture du système de réputation

Selon la figure 4.4, l'architecture du système de réputation, que nous proposons se divise en plusieurs parties **:** les variables fournies par le noud visiteur, les variables calculées par le noud hôte, les listes, les fonctions d'analyses pour chaque variable, le module d'agrégation de score de réputation , le module d'agrégation du cout du message, le module de l'identité du nœud et le module de prise de décision.

4.5.2.1 Les variables :

Ce sont les différentes informations qui seront analysées par les fonctions d'analyses pour tester la validité du noud. Il s'agit de :

- identifiant du véhicule.
- Le cout du message.
- Le crédit.

4.5.2.2 Les listes

- **La liste des voisins :**

L'ensemble des véhicules présents à l'intérieur du diamètre de la cellule et avec lesquels la communication peut être établie. On considère diamètre de la cellule est la distance ou le rayon de transmission peut atteindre.

- **La liste noire :**

Ensemble des nœuds qui sont considérer comme égoïste a cause de leur non coopération et qui sont exclut du réseau.

4.5.2.3 Module de vérification de l'identité du nœud:

Ce module a pour rôle de vérifie l'identité du nœud, ce nœud peut avoir deux statut le premier est le statut du nœud voisin et le deuxième est le statut de nœud malicieux.

Quand un nœud veut communiquer avec le nœud hôte ce dernier vérifié s'il ne figure pas dans la liste noire.

S'il fait partie de la liste noire alors il aura le statut de malicieux et il est éjecté du réseau.

Si il ne pas partie de la liste noire alors il fait partie de la liste des voisin et il peut communique avec le nœud hôte.

4.5.2.4 Module d'agrégation du score de réputation :

Le système de réputation calcule les valeurs de réputation d'un noud à partir des informations qu'elle obtient à partir du moniteur.

Les nœuds consomment généralement plus d'énergie quand ils transmettent des paquets de données de contrôle et les paquets de routage.

Le modèle de la réputation proposé se concentre davantage sur le nombre de paquets de données d'un nœud transmet pour d'autres nœuds que le nombre d'acheminer des paquets de commande qu'il transmet. Pour calculer la réputation d'un nœud, nous évaluons les informations provenant du moniteur en deux phases.

Soit $\hbar_1$ représentent la réputation du nœud basé sur les paquets de données qu'il transmet à d'autres, ψ_1 représentent la réputation du nœud basé sur les paquets de contrôle de routage qu'il transmet à d'autres nœuds.

Les variables utilisées dans le calcul de la réputation $\hbar_1$, ψ_1, sont présenté dans le tableau si dessous.

Notation des paquets	Définition
P_T	Les paquets transmis par le nœud hôte
P_{Tdata}	Paquets de données transmis par le nœud hôte
$P_{Tdata\text{-}self}$	Paquets de données transmis générés par le nœud hôte
$P_{Tdata\text{-}others}$	Paquets de données transmis générés par les autres nœuds.
$P_{Tcontrol}$	Paquets de contrôle de routage transmis par le nœud hôte.
$P_{Tctrl\text{-}self}$	Paquets de contrôle de routage généré et transmis par le nœud de cible

$P_{Tctrl\text{-}others}$	Paquets de contrôle de routage transmis générés par d'autres nœuds.
P_{Rdata}	Les paquets de données reçus à partir du nœud hôte.
$P_{Rdata\text{-}self}$	Paquets de données reçus du nœud d'hôte produit par lui-même.
$P_{Rdata\text{-}others}$	Les paquets de données reçus du nœud hôte générées par d'autres nœuds.
$P_{Rcontrol}$	Paquets de commande reçus du nœud d'hôte.
$P_{Rctrl\text{-}self}$	Paquets de contrôle de routage reçus produits par le nœud hôte.
$P_{Rctrl\text{-}others}$	Paquets de contrôle de routage reçus du nœud de hôte produit par d'autres nœuds.

$\hbar_1$ est calculé comme représenté dans l'équation :

$$\hbar_1 = P_{T\ data\text{-}others} / (P_{T\ data\text{-}self} + P_{T\ data\text{-}others})$$

De même, ψ_1 est donnée à titre:

$$\psi_1 = P_{T\ ctrl\text{-}others} / (P_{T\ ctrl\text{-}self} + P_{T\ ctrl\text{-}others})$$

Pour calculer la réputation d'un nœud sur la base du nombre des paquets de données et de contrôle de routage reçu par le nœud hôte et qui ont été généré par d'autres nœuds.

$\hbar_2$ représentent les valeurs réputation sur la base de paquets de données reçus générés par d'autres nœuds et ψ_2 représentent les valeurs de réputation basé sur les paquets de contrôle de routage reçus générés par d'autres nœuds. On calcule $\hbar_2$ et ψ_2 comme suit:

$$\hbar_2 = P_{R\ data\text{-}others} / (P_{R\ data\text{-}self} + P_{R\ data\text{-}others})$$

$$\psi_2 = P_{R\ ctrl\text{-}others} / (P_{R\ ctrl\text{-}self} + P_{R\ ctrl\text{-}others})$$

Les variables utilisées dans le calcul de la réputation $\hbar_1$, ψ_1, $\hbar_2$ et ψ_2 sont présenté dans le tableau ci-dessous.

Notation	Définitions
$\hbar_1$, $\hbar_2$	Réputation en termes de paquets de données transmis
ψ_1 , ψ_2	Réputation en termes de paquets de contrôle de routage transmis
$\hbar_{data}$	Réputations finales en termes de paquets de données transmis
$\psi_{control}$	Réputations finales en termes de paquets de contrôle de routage transmis
$ɧ_T$	Réputation totale
$ɧ_0$	Réputation total initial
λ	Poids attribué à la réputation finale en termes de paquets de données transmis
ρ	Poids attribué à la réputation finale en ce qui concerne les paquets de control transmis
ω	Facteur de délabrement pour la valeur calculée de réputation.

Pour calculer la réputation finale d'un nœud en termes de paquets de données qu'il a transmis à d'autres nœuds, nous combinons $\hbar_1$ et $\hbar_2$. Ainsi, la réputation final d'un nœud surveillé en termes de paquets de données qu'il a transmis à d'autres nœuds est donnée à:

$$\hbar_{data} = \hbar_1 + \hbar_2$$

De même, la réputation finale des nœuds sur la base des paquets de contrôle de routage qu'il a transmis à d'autres nœuds est donnée par:

$$\psi_{control} = \psi_1 + \psi_2$$

- **Valeur de Réputation totale du nœud :**

La réputation totale d'un nœud dans le modèle proposé est désigné par la combinaison de la valeur finales de réputation d'un nœud en termes de paquets de données transmis, et les paquets de contrôle de routage transmis. Mathématiquement, $ɧ_T$ est donnée par l'équation ci-dessous

$$ɧ_T = \lambda\, ħ_{data} + \rho\, \psi_{control}$$

Où λ et *p* sont donnés à titre 0,8 et 0,2, respectivement. Les valeurs de λ et *p* sont basés sur le rapport importance accordée à la valeur de la réputation finale d'un nœud en ce qui concerne le type de paquets qu'il transmet en continu pour les autres nœuds.

- **Réputation initiale de nœuds dans les réseaux**

Au début de l'exploitation du réseau, les nœuds du réseau n'ont pas eu la possibilité de surveiller leurs nœuds voisins pour temps assez long avant pour calculer leurs valeurs de réputation. Afin de répondre à ce genre de situation, une réputation de valeur par défaut (réputation initial) est introduite pour tous les nœuds dans le réseau. Cette valeur est également affectée à un nœud qui se joint à nouveau le réseau.

Nous avons estimé que la réputation total de A et de nœud sera toujours entre [0, 2].

Compte tenu de cette gamme de valeurs, la valeur de la réputation par défaut pour tous les nœuds du réseau est définie comme $ɧ_0$.

Cela signifie que chaque nœud du réseau est attribué une valeur de la réputation initial, qui est aussi leur valeur de réputation totale au temps t égal à zéro. Mathématiquement, la réputation directe totale d'un nœud quand il est nouvellement connecter au réseau ou à l'apparition des activités du réseau est donnée par:

$$ɧ_T = ɧ_0$$

Après le suivi des différentes activités de nœuds pour une période de temps donnée, un nœud aurait recueillies suffisamment de preuves pour calculer la réputation individuelle de ses nœuds voisins. La réputation totale dans ce cas est une combinaison de la valeur initiale de la réputation initiale et la valeur de réputation actuelle mesurée. Notons la nouvelle valeur de la réputation totale $ɧ_T = ɧ_1$. Nous pouvons évaluer la nouvelle réputation totale $ɧ_1$ comme suit :

$$ɧ_1 = \omega ɧ_0 + (1 - \omega)\, ɧ_{M1}$$

Où ω est une petite valeur entre [0, 1] et $ɧ_{M1}$ est la valeur de la réputation d'un nœud calculé actuellement sur la base de nouveaux éléments recueillis par les activités de surveillance. Comme plus de preuves devient disponible, la réputation directe des nœuds sera régulièrement mise à jour à un intervalle de temps spécifique. Par exemple, nous évaluons la réputation directe de nœud à une période donnée de temps t $ɧ_1$. Nous pouvons donc dire qu'après un intervalle de temps de (t + 1), $ɧ_2$ sera donnée en tant que:

$$ɧ_2 = \omega ɧ_1 + (1 - \omega)\, ɧ_{M2}$$

Nous pouvons conclure que la réputation directe totale d'un nœud dans notre modèle peut être évaluée en utilisant l'équation ci-dessous:

$$ɧ_n = \omega^n ɧ_0 + \omega^{n-1}(1-\omega)\, ɧ_{M1} + \omega^{n-2}(1-\omega)\, ɧ_{M2} + \omega^{n-i}(1-\omega)\, ɧ_{Mi}$$

Où $ɧ_1$, $ɧ_{M2}$ et $ɧ_{Mi}$ sont les valeurs de réputation directe nouvellement mesurées à intervalles réguliers.

L'équation peut en outre être simplifiée comme:

$$ɧ_T = ɧ_n = \omega^n ɧ_0 + \sum_{i=1}^{n} \omega^{n-i}(1-\omega)\, ɧ_{Mi}$$

Ou n = 1, 2, 3, . . ., i.

4.5.2.5 Module d'agrégation du cout du message :

Cette fonction permet de calculé le cout Cs_i^t(N (*i*)) que doit payé un nœud (crédit) pour envoyé un message.

Ce cout est calculé essentiellement a partir du score de réputation du nœud et du montant du crédit initial donnée lors de sa première connexion au réseau.

Ce cout est calculé par l'équation si dessous :

$$Cs_i^t(\text{N }(i)) = \frac{init\_credit}{G} \times i\_msg \times (2 - ɧ_T)$$

G : Un paramètre G est utilisé pour le calcul des coûts. Il divise le crédit initial qui reçoit un nœud, afin d'établir une valeur de référence pour les coûts de message. G permet soit d'augmenter ou de diminuer le nombre de messages envoyés, dont le coût est payé seulement avec le crédit initial. En utilisant une petite valeur G, il permet l'appauvrissent rapidement le nombre de crédit d'un nœud malveillant (par exemple dans le cas d'aucune récompense), rendant ainsi incapable de participer au réseau. En utilisant une grande valeur G permet aux nœuds inconnus, par exemple, pour avoir plus de chances de partager leurs messages afin d'accroître leur réputation parmi leurs voisins.

init_credit : crédit initial que reçoit un nœud lors de sa première connexion au réseau.

i_msg : la pertinence des données.

$ɧ_{T:}$ représente le score de réputation du nœud *i*.

4.5.2.6 Module de prise de décision :

C'est un module qui détermine si le message est accepté sinon Il sera rejeté et le nœud est ajouté à la liste noire.

Pour que un nœud soit accepté il doit avoir suffisamment de crédit pour payé le cout du message sinon il serra considérer comme égoïste et malicieux et il serra exclut du réseau.

Si le message est accepté alors le nœud doit être récompensé.

- **Calcule de la récompense :**

L'objectif de la récompense est de faire en sorte que le système reste incitatif pour les bons nœuds et de décourager les nœuds malveillants.

Une récompense Rew est estimée en fonction d'un poids $w(ɧ_T)$ et à la réputation du nœud source, $ɧ_T$ et du nombre des nœuds voisins.

- **La pertinence de la réputation :**

La pertinence de la réputation, $w(ɧ_T)$ Elle permet d'attribuer un poids à la réputation $ɧ_T$, la valeur de la réputation nœud ce poids est utilisé pour l'estimation de récompense. Il permet une rémunération plus élevée pour la réputation élevée par rapport aux nœuds de

réputation inférieurs pour la même action, incitant ainsi les nœuds pour maintenir une bonne réputation.

$w(ϧ_T)$ est calculé avec l'équation (2), où un hyperbolique tangent est utilisé en raison de ses caractéristiques, à savoir son comportement qui ressemble étroitement à celui d'une exponentielle fonction à la fois des valeurs positives et négatives.

Le calcule de $w(ϧ_T)$ est représenté dans l'équation ci-dessous :

$$w(ϧ_T) = \tanh(ϧ_T) \times \frac{e^2+1}{e^2-1}$$

Le calcul de la récompense est représenté dans l'équation si dessous :

N(j) : nombre de voisins du nœud.

$Cs^t_i(N(i))$: Cout du message.

$w(ϧ_T)$: Pertinence de la réputation.

$$Rew^t_j(i) = \frac{(W(ϧ_T) + 1) \times Cs^t_i(N(i))}{|N(j)|}$$

4.6 L'algorithme :

Nous proposons un système de réputation qui permet de détecter les nœuds égoïstes et malicieux et de les éjecter du réseau. L'algorithme sur lequel se base notre système est présenté ci-dessous.

Cet algorithme est constitué d'un ensemble de fonctions qui analysent chacune des variables fournies par le paquet reçu provenant du nœud visiteur qui souhaite entrer en communication avec le nœud hôte. Les informations prises en compte dans chaque fonction ont été présentées dans le tableau ci-dessous. Cet algorithme agit à l'interface d'entrée du réseau pour chaque nœud lors de la réception de message. L'algorithme représenté ci-dessous est utilisé pour évaluer chaque message.

La description des symboles utilisés dans l'algorithme sont représenté dans le tableau si dessous.

N	Ensemble des nœuds de la liste noire
No	Ensemble des nœuds voisins
Id	Identificateur du nœud
n	Nœud
Tn	Le temps de vie du score de réputation
Credit(n)	Crédit actuel du nœud n

Tableau 4.1 : Description des symboles utilisés dans l'algorithme

Dans cette partie, nous présentons l'algorithme du système de réputation. Il est constitué de plusieurs fonctions qui réalisent chacune une tâche spécifique.

Les différentes fonctions utilisées dans l'algorithme sont présentées dans la suite :

vérIdMsg (msg(id)): fonction permettant de tester l'identifiant publié par le nœud.

PriseDeDicision (CoutMsg(ScoreRep(n)), Credit(n)): fonction dans laquelle la décision d'accepter le message ou de le refusé est prise selon le cout du message est du crédit.

Rejected (n) : fonction qui éjecte du réseau un nœud défini comme malicieux.

accepted (n) : fonction qui accepte un nœud visiteur dans le réseau.

chekTime (Tn) : fonction ayant pour tâche de vérifier si l'âge du score de réputations est

Inférieur à un âge limite fixé.

ScoreRep (n) : fonction qui calcule le score de réputation.

CoutMsg(ScoreRep(n)) : fonction qui calcule le cout du message.

Credit(n): la valeur du crédit que possède le nœud n.

L'algorithme :

```
Begin
vérIdMsg (msg(id))
If  (id ϵ N) then
  Rejected (n)
  else if (id ϵ no)
   chekTime (Tn)
        if  (chekTime (Tn) == true)then

            CoutMsg(ScoreRep(n))
           PriseDeDicision (CoutMsg(ScoreRep(n)), Credit(n))
 else
ScoreRep(n)
CoutMsg(ScoreRep(n))
    PriseDeDicision (CoutMsg(ScoreRep(n)), Credit(n))
End
 PriseDeDicision (CoutMsg(ScoreRep(n)), Credit(n))
If    Credit(n) > CoutMsg(ScoreRep(n) then
(Accepted (n)) AND (Recompense(n))
 else    (Rejected (n))
accepted (n)
no = no U  n
Rejected (n)
N = N  U  n
End
```

4.6.1 Description générale de l'algorithme

L'algorithme ci-dessus décrit le fonctionnement global du système de réputation que nous proposons. Dans cette partie. Dans un premier temps, le message reçu d'un hôte visiteur est soumis à un système d'évaluation des messages. Celui-ci vérifie l'identifiant du nœud vérIdMsg (msg(id)) .

Si le nœud fait partie de la liste noire, il est éjecté du réseau. Si par contre le nœud fait partie de la liste des voisins, alors le nœud hôte vérifie la durée de vie du score de réputation si celui la dépasse un certain seuil alors le score de réputation doit être mis a jour (recalculé).

Si la dure de vie n'est pas dépassé, le cout du message est calculer CoutMsg(ScoreRep(n) Et une décision est prise soit d'accepter ou rejeter le message si le nœud a eu suffisamment de crédit pour envoyé le message.

- **Module de calcul du score de réputation ScoreRep(n) :**

Ce module a pour rôle de calculer le score de réputation du nœud hôte.

- **Module de calcul du cout du message CoutMsg(ScoreRep(n)) :**

Ce module a pour rôle de calculer le cout que doit payé le nœud pour envoyé le message ce cout la est calculer a partir du score de réputation du nœud.

- **Module de prise de décision PriseDeDicision (CoutMsg(ScoreRep(n)), Credit(n)):**

Ce module a pour rôle de déterminé si le message sera accepter ou refuser selon le cout du message et la valeur du crédit que détiens le nœud si ile nœud a eu suffisamment de crédit pour payé le cout du message envoyé alors il sera accepter sinon il sera refuser.

Si le message est refusé alors le nœud sera ajoute à la liste noire Dans le cas contraire, ou le message est accepté alors le nœud est récompensé.

4.7 Conclusion

Dans ce chapitre, nous avons présenté notre système de réputation on commençant par son fonctionnement, son architecture, les différent modules qui le compose à savoir : le module d'indentification des nœuds, le module d'agrégation du score de réputation, le module de calcule du cout de message et le module de prise de décision et enfin l'algorithme de notre système.

Conclusion générale

Conclusion général

Les réseaux ad hoc de véhicules constituent un nouveau type de réseaux issu des réseaux ad hoc mobiles (MANET). Leur particularité provient des communications qui peuvent s'instaurer entre véhicules ou bien avec une infrastructure de stations de base. La mobilité est également largement plus contrainte que dans les réseaux ad hoc traditionnels.

Le comportement des véhicules dans le réseau est très important.

En effet, certain véhicule ont un comportement malicieux ou égoïste, ce qui dégrade fortement la performance du réseau, d'où la nécessité de les détecter et de les supprimer du réseau.

Pour détecter et supprimer le nœud malicieux et égoïste, il ya plusieurs méthodes de réputation on peut citer : CONFIDANT, OCEAN, VIME.

Nous avons proposé un système de réputation qui est basé sur le model VIME on la modifié pour qu'il soit plus performant et protégé contre les fausse informations.

Références Bibliographiques

Référence Bibliographique

[1] : Tayeb Lemlouma, « Le routage dans les réseaux mobiles ad hoc » www.opera.fr/people/TayebLemlouma/papers/AdHoc_presentation .pdf

[2]: Hassnaa Moustafa « Routage unicast et multicast dans les réseaux mobiles Ad Hoc » Thèse doctorat. Ecole Nationale Supérieure des Télécommunications de Paris, 2004

[3]: Anne Gégout, « Les réseaux Ad Hoc » Mars2005, www.tdf.fr/medias/view/?id=704

[4]: James Bernsen, and D. Manivannan, « Unicast Routing Protocols for Vehicular Ad Hoc Networks: A Critical Comparison and Classification», Elsevier Journal of Parvasive and Mobile Computing, vol. 5, pp. 1-18, 2009.

[5] : R. Meraihi, Mohamed Senouci, Moez Djebri « Réseau mobile Ad Hoc et réseaux de capteurs sans fil » chapitre de livre Edition Hermes 2006

[6]: Yacine Khaled, Hamid Menouar, Yacine Challal « Reactive and Adaptative Protocol for Inter Vehicle Communication (RAP-IVC) » UMR-CNRS France.

[7]: Gokhan Korkmaz, Eylem Ekici, and FusunOzguner « An Efficient Fully Ad-Hoc Multi-Hop Broadcast Protocol for Inter-Vehicular communication Systems ». Department of Electrical and Computer Engineering, The Ohio State University. 2006.

[8] :

[9]: *M. MERAIHI Yassine* , ROUTAGE DANS LES RESEAUX VEHICULAIRES (VANET) CAS D'UN ENVIRONNEMENT TYPE VILLE.

[10] :

[11] : C. TCHEPNDA, "Authentification dans les Réseaux Véhiculaires Opérés," Ecole Nationale Supérieure des Télécommunications Thèse de doctorat, 2008.

[12] : M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security,* vol. 15, pp. 39-68, 2007.

[13]: Communication inter véhiculaire, Raphael Mazot, Wahid Meslem, Madjid Layouni, Alexendre Tran. GMI – Arles Avignon.

[14]: P. Michiardi and R. Molva, "CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in *Proc. of 6th Joint Working Conference on Communications and Multimedia Security*, 2002, pp. 107-121.

[15]: L. Buttyan and J.P. Hubaux, “Stimulating cooperation in self-organizing mobile ad hoc networks,” *Mobile Networks and Applications*, vol. 8, no. 15, pp. 579-592, 2002.

[16]: S. Marti, T. J. Giuli, K. Lai, and M., Baker, “Mitigating routing misbehavior in mobile ad hoc networks,” in *6th Annual International Conference on Mobile Computing and Networking*, 6-11 August 2000, pp. 255-265.

[17]: K. Balakrishnan, J. Deng, and P.K. Varshney, “TWOACK: Preventing selfishness in mobile ad Hoc networks,” in *Proc. of IEEE Wireless Communications and Networking Conference (WCNC)*, 2005, pp. 2137- 2142.

[18]: J. Zhang. A survey on trust management for vanets. In *IEEE International Conference on Advanced Information Networking and Applications (AINA’ 12)*, Biopolis, Singapore, 2011.

[19]: M. Raya, J. Pierre Hubaux, “Securing vehicular ad hoc Networks”, in Journal of Computer Security,
vol.15, January 2007, pp. 39-68.

[20]: https://fr.wikipedia.org/wiki/R%C3%A9putation

[21]: A. Srinivasan, J. Teitelbaum, and J. Wu, "DRBTS: distributed reputation-based beacon trust system," in *Dependable, Autonomic and Secure Computing, 2nd IEEE International Symposium on*, 2006, pp. 277-283.

[22]: A. Josang, R. Ismail, and C. Boyd. A survey of trust and reputation systems for online service provision. *Decision Support Systems*, 43(2) :618–644, 2007.

[23]: J. Barnett, *La réputation pierre angulaire d’une protection efficace contre les menaces*

[24] : RICHARD ENGOULOU, SÉCURISATION DES VANETS PAR LA MÉTHODE DE RÉPUTATION DES NŒUDS, AVRIL 2013.

[25] : Q. Ding, X. Li, M. Jiang, and X. Zhou, "Reputation-based trust model in vehicular ad hoc networks," in *Wireless Communications and Signal Processing (WCSP), 2010 International Conference on*, 2010, pp. 1-6.

[26]: S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks", *in Proceedings of the Sixth annual ACM/IEEE International Conference on Mobile Computing and Networking*, 2000, pp. 255–265.

[27]: S. Buchegger, J.Y Le Boudec, "Performance analysis of the confidant protocol", *Proceeding ACM 3rd International Symposium on Mobile Ad hoc Networking and Computing* (MobiHoc’02), pp. 226-236, 2002.

[28]: S.Bansal, M. Baker, "Observation-based cooperation enforcement in ad-hoc networks", *Technical Report*, *Stanford University*, 2003.

[29]: “Trusted computing group: Tpm main specification. main specification version 1.2 rev. 116,” March 2011.

[30]: F. Kargl, Z. Ma, and E. Schoch, "Security engineering for vanets," in *4th Wksp. Embedded Sec. in Cars*, 2006.

[31]: S. K. Dhurandher, M. S. Obaidat, A. Jaiswal, A. Tiwari, and A. Tyagi, "Securing vehicular networks: A reputation and plausibility checks-based approach," in *GLOBECOM Workshops (GC Wkshps), 2010 IEEE*, 2010, pp. 1550-1554.