République **A**lgérienne **D**émocratique Et **P**opulaire

Ministère de l'**E**nséignement **S**upérieur et de la **R**echerche **S**cientifique

UNIVERSITÉ **M**OULOUD **M**AMMERI **T**IZI-OUZOU

Faculté de Génie Électrique et d'Informatique

Département d'informatique

En vue de l'obtention de diplôme de Master en informatique

Option : Réseaux, Mobilités et Systèmes embarqués.

Thème

Détection d'attaque DOS dans les réseaux véhiculaires

Présenté par : Ouanes Yessinia.

Soutenue publiquement le 13/12/2020, devant le jury composé de :

M^{me} Oubabas Sarah	Encadreur
M^{me} Aoudjit Rachida	Président
M^{lle} Chemoun Karima	Examinateur

REMERCIEMENT

Avant de commencer la présentation de ce travail, je profite de l'occasion pour remercier toutes les personnes qui ont contribué de près ou de loin à la réalisation de ce projet de fin d'études.

J'exprime mes remerciements à ma promotrice Madame Oubabas Sarah d'avoir accepté de m'encadrer pour mon projet de fin d'études, ainsi que pour son soutiens, sa disponibilités, ses précieux conseils et pour sa confiance placé en moi.

Je remercie les membres du jury pour l'intérêt qu'ils ont bien voulu porter à mon travail.

Je réserve ici une place particulière pour remercier vivement ma famille pour leurs affections et leurs soutiens continu. Et à tous ceux qui, d'une manière ou d'une autre, m'ont aidé et encouragé à la réalisation de ce modeste travail.

Résumé :

La protection de la vie privée et de la sécurité sont devenues un sujet d'attention indispensable dans le réseau ad hoc de véhicules, qui est vulnérable à de nombreuses menaces de sécurité de nos jours. Parmi ces attaques, l'attaque par déni de service (DoS) ainsi la non coopération des nœuds communément appelé nœuds égoïstes.

Dans une attaque DOS, un nœud malveillant forge un grand nombre de fausses identités, afin de perturber le bon fonctionnement du transfert équitable de données entre deux véhicules. Dans ce document, une approche robuste est présentée pour se défendre contre ces attaques.

Dans ce système proposé, les véhicules malveillants sont repérer à l'aide d'un mécanisme de détection et de calcule de la confiance .Ensuite un deuxième mécanisme est exécuter pour l'isolement des nœuds malveillants ou de les exclure définitivement.

Avec notre approche, les nœuds égoïstes sont pleinement stimuler à coopérer ainsi les nœuds malveillant sont inciter à montrer un bon comportement.

Mots clés : réseau ad hoc de véhicules ,DOS , nœuds égoïstes .

Abstract :

Privacy and security have become an indispensable focus of attention in today's ad hoc vehicle network, which is vulnerable to many security threats. Among these attacks, the denial of service (DoS) attack as well as the non-cooperation of nodes commonly known as selfish nodes.

In a DoS attack, a malicious node forges a large number of false identities in order to disrupt the fair transfer of data between two fast vehicles. In this paper, a robust approach is presented to defend against such attacks.

In this proposed system, malicious vehicles are detected using a detection and confidence calculation mechanism, and then a second mechanism is executed to isolate the malicious nodes or exclude them permanently.

With our approach, selfish nodes are fully stimulated to cooperate and thus encourage malicious nodes to show good behavior.

Key words : ad hoc vehicle network ,DOS, selfish nodes.

Table des figures

Liste des tableaux

Glossaire des acronymes

MANET : Mobile Ad hoc Network.

VANET : Vehicular Ad hoc Network.

V2V : Vehicle to Vehicle communication.

V2I : Vehicle to infrastructure communication.

OBU : On Board Unit.

RSU : Road Side Unit.

UA : Application Unit.

DSRC : Dedicated Short-Range Communications.

WAVE : Wireless Access for Vehicular Environment.

IEEE : Institute of Electrical and Electronic Engineers.

GPS : Global Positioning System.

QoS : Quality of Service.

DOS : Denial of Service attack.

DDOS : Distributed Denial of Service attack.

ITS : Intelligent transportation system.

IVC: Inter-Vehicle Communications.

IP :Internet Protocol.

Table des matières

Introduction générale

L'une des principales caractéristiques qui ont façonné l'industrie automobile au cours des dernières années est l'intégration de composants embarqués dont le rôle principal est l'amélioration de la sécurité du conducteur. Pour diffuser les informations collectées et traitées par ces composants, des infrastructures de communication sans fil ont été utilisées.

Au début des années 1990, les véhicules intelligents sont apparus sous le nom de (ITS) (Intelligent Transportation System).Ce système de transport intelligent a été initialement développés pour objectifs de sécurité, a ensuite été étendus pour couvrir l'efficacité de la conduite ainsi que de services à valeur ajoutée, y compris l'info divertissement et les applications commerciales. Dans le proche avenir, les véhicules qui deviennent de plus en plus des systèmes intelligents devraient être équipés d'interfaces de radiocommunication. Les constructeurs automobiles ont réalisé le potentiel d'interconnexion de leurs véhicules [3].

Les VANETs sont un cas d'utilisation des réseaux mobiles ad hoc (MANET) où les voitures sont les nœuds mobiles. Dans les services de divertissement à bord, l'objectif essentiel des VANETs est d'améliorer la sécurité routière et aussi les conditions de conduite. Ainsi, la vie des utilisateurs est l'un des facteurs les plus impliqués, d'où l'importance primordiale de sécuriser les VANET contre tout type d'attaque qu'ils peuvent subir.

Du fait que les réseaux VANET sont un cas particulier de Mobile Ad hoc NETworks (MANET) et comme ils présentent plusieurs fonctionnalités uniques telles que la grande mobilité des nœuds, les temps de connexion courts, etc... , les mécanismes de sécurité conventionnels ne sont pas toujours efficaces. Plus précisément, dans les conditions mentionnées, différents types d'attaques conventionnelles sous lesquelles opèrent des réseaux mobiles en mode ad hoc sont valables pour VANETs.

Cependant, le comportement des VANET vis-à-vis de ces attaques et la proposition de solutions ne sont généralement pas les mêmes.

Compte tenu de la variété des attaques et des vulnérabilités pouvant existées dans les VANETs, plusieurs techniques et mécanismes existent pour éviter complètement ou minimiser les effets souhaités par l'attaquant.

Il est donc nécessaire de trouver des solutions à ces failles de sécurité existantes dans les VANET, essentiellement les attaques DOS et le comportement égoïstes. Ce mémoire a été proposé dans ce contexte.

Nous proposons une approche qui permet d'une part de contrer le comportement égoïste des véhicules qui utilisent le service d'acheminement d'autres nœuds sans acheminer correctement des paquets pour eux afin d'économiser ses ressources. D'autre part, notre solution permet de détecter les véhicules qui transmettent un grand nombre de messages sur le réseau(Dos) dans le but de le saturer. Une fois que notre mécanisme a détecté les véhicules présentant un comportement malveillant, notre système permet d'isoler ces véhicules de façon temporaire jusqu'à ce qu'ils épuisent toutes leurs chances de réintégrer le réseau pour enfin les exclure de façon définitive.

Ce mémoire est organisé en trois chapitres. Nous présentons dans le premier chapitre les réseaux véhiculaires ainsi que leurs caractéristiques spécifique.

Dans le deuxième chapitre, nous nous focalisons sur la sécurité. Nous décrivons tout d'abord les services et les mécanismes qui peuvent être mis en œuvre afin de réaliser la sécurité ainsi que la classification des attaques menaçant ce type de réseaux, et aussi une partie de ce chapitre sera consacré à la présentation de quelques solutions qui ont été proposés pour adresser le problème d'attaque d'DOS ainsi du comportement égoïste. Une comparaison sera effectuée entre les différentes techniques utilisées.

En effectuant cet état d'art nous allons finir par déceler les manques et delà résulte notre contribution qui est spécialement conçue afin de pouvoir trouver une solution à cette attaque (DOS) qui est jugée très dangereuse pour ces types de réseaux et du comportement égoïste des nœuds. Tous cela sera présenté dans le troisième chapitre, une partie d'analyse théorique sera consacré à l'étude de notre solution ainsi nous discutons les résultats obtenu. Nous conclurons par une conclusion générale résumant les points essentiels qui ont été abordés.

Chapitre 1

Généralités sur les VANETs

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 les réseaux ad hoc de manière générale, puis, nous abordons aux réseaux VANET, nous décrivons les différentes caractéristiques, et les modes de communication existants. Enfin nous aborderons les différents types de services offerts par ces réseaux; ainsi les différentes contraintes et défis.

1.2 Réseaux Ad-hoc ou MANET

Un réseau MANETS (Mobile Ad hoc Networks) appelé aussi réseau Ad hoc est un ensemble de nœuds mobiles interconnectés par des liaisons sans fil formant un réseau dynamique sans infrastructure préexistante ou une architecture centralisée. Les nœuds sont libres de se déplacer, de joindre ou de quitter le réseau à tout moment, créant ainsi un changement spontané de la topologie. Chaque nœud dans ce type de réseau communique directement avec les autres nœuds qui se trouvent dans son rayon de communication (portée radio). La communication avec les nœuds hors portée radio se fait à travers des nœuds intermédiaires, qui s'approprient le rôle d'un routeur et acheminent les messages à destination. Ce processus se fait grâce au protocole de routage. À cet effet, plusieurs protocoles de routage ont été proposés et standardisés par le groupe MANET (Mobile Ad hoc Network).

1.3 les réseaux VANETs

Le réseau ad hoc véhiculaire (VANET) est une sous-classe de réseaux ad hoc mobiles (MANET) dont les nœuds sont des unités routières fixes ou véhicules mobiles. Les nœuds communiquent entre eux en mode ad hoc et communiquent avec des équipements fixes sur les routes en mode infrastructure. Ainsi, les caractéristiques des VANET sont fondamentalement un mélange de caractéristiques de support sans fil et de caractéristiques des différentes topologies en modes ad hoc et infrastructure.

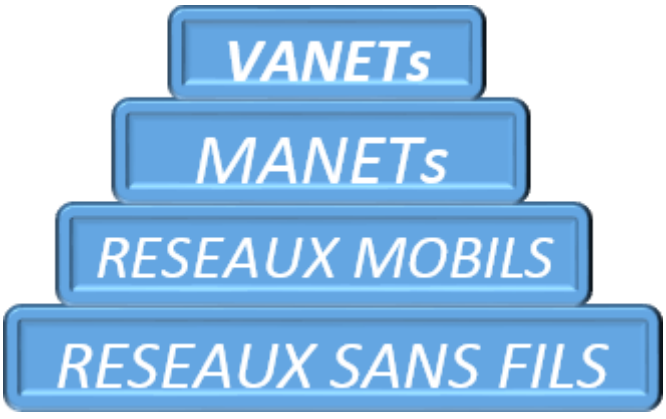


Figure 1-4 Hiérarchie des réseaux sans fil

1.4 Etat de l'art sur les réseaux VANETs

1.4.1 Architecture des réseau VANETs

1.4.1.1 Véhicule intelligent (smart vehicle)

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 ».

On retrouve également un système de positionnement tel que le système de positionnement mondial (GPS) par exemple, qui est essentiel pour localiser et conduire assistance.

Un véhicule intelligent est évidemment équipé d'un système de communication (peut être multi-interface), un système informatique, un dispositif d'enregistrement d'événements dont le fonctionnement est similaire à la boîte noire d'un avion.

Principalement et pour les mesures de sécurité, Hubaux et al. proposés dans [2] qu'un véhicule intelligent doit être équipés d'une plaque d'immatriculation électronique (ELP) ou d'un numéro de châssis électronique (ECN) qui représentent l'identité électronique du véhicule au lieu de l'identification par plaques d'immatriculation.

La terminologie actuelle des STI comprend certaines fonctionnalités telles que le transceiving, affichage et interactivité avec le conducteur dans une seule unité appelée OBU[4].

La figure 1-2 montre les différents composants qui peuvent être intégrés dans un véhicule intelligent :

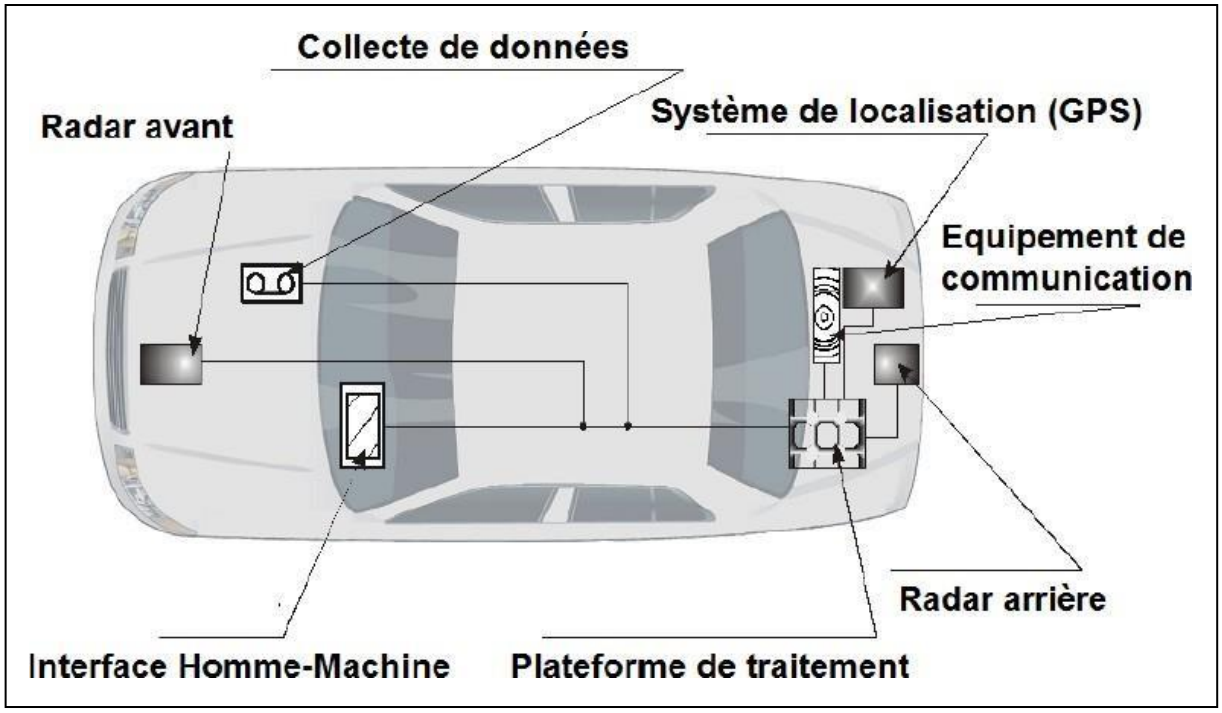


Figure 1-5 composants d'un véhicule intelligent [2].

1.4.1.2 Road Side Unit (RSU)

La RSU est un appareil à ondes généralement fixé le long du bord de la route ou dans des emplacements tels que les carrefours ou à proximité des espaces de stationnement dédiés aux communication à court portée basée sur la technologie radio IEEE 802.11p, et peut également être équipé d'un réseau infrastructurel [4]. Les principales fonctions de RSU sont :

- étendre la portée de communication.
- Fournir une connectivité Internet aux OBU.
- Fournir des applications de sécurité telles que l'avertissement d'accident [4].

1.4.1.3 Autorité de confiance(AC):

Ce sont des tiers chargés de travail de génération, de distribution et de révocation de certificats.

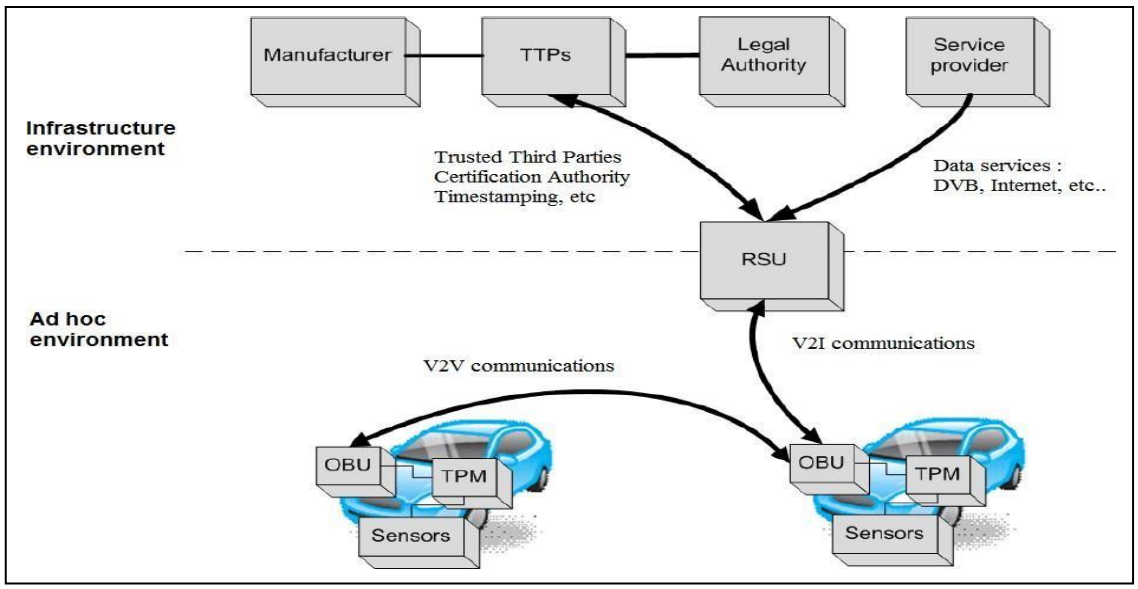
Peut être définit aussi comme un serveur de stockage et de transaction qui a la confiance de toutes les entités du réseau. Elle fournit des services et des applications à tous les utilisateurs, ainsi que les certificats, les clés ou pseudonymes de communication des véhicules .

1.4.1.4 On Board Unit (OBU):

Une OBU est une unité embarqué généralement monté à bord d'un véhicule utilisé pour modifier les informations avec des RSU ou avec d'autres OBU. Il se compose d'une ressource processeur de commande (RCP), et les ressources incluent une mémoire de lecture / écriture utilisée pour stocker et récupérer des informations, une interface utilisateur, une interface spécialisée pour se connectez à d'autres OBU et à un périphérique réseau pour des communications sans fil à courte portée basée sur la technologie radio IEEE 802.11p. Il peut en outre inclure un autre périphérique réseau pour les applications non liées à la sécurité basées sur d'autres technologies radio telles que IEEE 802.11a / b / g / n. Ces appareils connectés via une liaison sans fil sont basée sur le canal de radiofréquence IEEE 802.11p.Les principales fonctions de l'OBU sont l'accès radio sans fil, ad hoc et géoroutage graphique, contrôle de la congestion du réseau, transfert fiable des messages, sécurité des données et mobilité IP [4].

1.4.1.5 ApplicationUnit(AU)

L'AU est un dispositif électronique installé dans les véhicules pour assurer les communications avec l'autorité de confiance (CA), connecté à l'OBU afin d'exécuter des applications[5].



1-6 composants d'un réseau VANET [3].

1.4.2Types de communications dans les VANETs

1.4.2.1 Communication vehicle to vehicle (V2V)

Ce type de communication fonctionne à l'aide des dispositifs installés dans les véhicules appelés OBU (On-Board Unit). Il est semblable au type de communication entre les nœuds mobiles de réseau MANET.

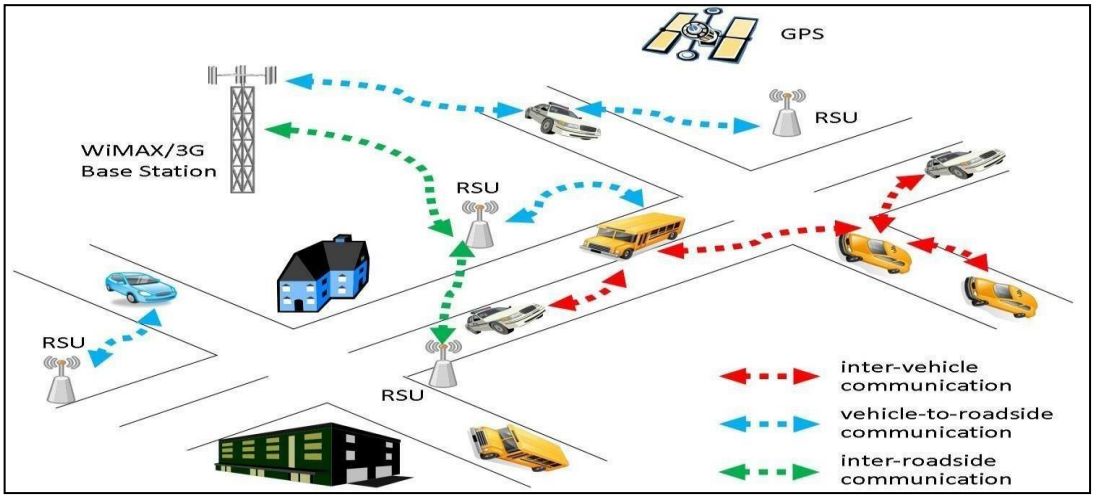
La communication entre deux véhicules se fait directement, en mode ad hoc inter-véhicules. Les véhicules n'ont pas besoin de faire appel aux infrastructures pour pouvoir communiquer entre eux. Deux véhicules peuvent communiquer directement si chaque véhicule est à portée de l'autre, sinon ils font appel à d'autres véhicules, qui vont jouer le rôle d'un pont (intermédiaires) pour router l'information à plusieurs sauts.

1.4.2.2 Communication vehicle to infrastructure (V2I)

La communication vehicle to infrastructure (V2I) est aussi appelée une communication en mode infrastructure qui est assurée grâce aux différentes entités du réseau VANET. En effet, les OBUs (On-Board Unit) des véhicules communiquent avec les RSUs (Road Side Unit) placées aux bords des routes pour envoyer leurs informations aux autres véhicules. Ce mode de communication assure une connectivité relativement forte par apport à la communication en mode V2V (vehicle to vehicle).

1.4.2.3 Le mode de communication hybride

Ce type de communication est une combinaison des deux modes de communications précédentes V2V et V2I, et comme les portées des infrastructures étant limitées alors que l'utilisation des véhicules comme relais permet d'étendre cette distance et d'éviter la multiplication des stations de base à chaque coin de la route et cela conduit à une communication hybride très intéressante et économique.



Figur1-7 communications dans les vanets [8].

1.4.5 Caractéristiques des VANETs

- **Haute mobilité:** la haute mobilité des nœuds VANET est l'une des plus importantes Caractéristiques. En fonctionnement normal du réseau, les nœuds se déplacent tout le temps avec des vitesses et directions. La grande mobilité des nœuds réduit le maillage dans le réseau (moins de routes entre les nœuds). Comparé à MANET, VANET la mobilité est relative- ment élevée. Des recherches comme catégories d'accès dans EDCA ont été spécialement consacrées à l'étude de l'impact du facteur de mobilité dans les réseaux ad hoc et surtout pour les réseaux véhiculaires [3].

- **Topologie dynamique:** Compte tenu de la grande mobilité, la topologie VANET évolue rapidement, elle est donc dynamique et imprévisible. Les temps de connexion sont courts sur- tout entre les nœuds se déplaçant dans des directions opposées. Cette topologie facilite l'attaque de l'ensemble du réseau et rend difficile la détection des dysfonctionnements [3].

- **Déconnexions fréquentes:** la topologie dynamique et la grande mobilité des nœuds ainsi que d'autres conditions telles que le climat, la densité du trafic provoque de fréquentes déconnexions de véhicules du réseau [3].

- **Disponibilité du support de transmission:** l'air est le support de transmission de VANETs. Bien que la disponibilité universelle de ce support de transmission sans fil qui est

l'un des grands avantages de l'IVC, devient l'origine de certains problèmes de sécurité questions liées à la nature de la transmission dans un environnement sans fil et à la sécurité des communications grâce à un support ouvert [3].

- **Anonymat du support:** la transmission de données via un support sans fil est généralement anonyme. Si nous laissons de côté les restrictions et les règlements d'utilisation, toute personne équipée avec un émetteur fonctionnant dans la même bande de fréquence peut transmettre et maintenir le bande.

- **Bande passante limitée:** la bande DSRC standardisée (5,850-5,925 GHz) pour VANET peut être considérée comme limitée, la largeur de toute la bande n'est que de 75 MHz. Restrictions de l'utilisation dans certains pays suggère que ces 75 MHz ne sont pas tous autorisés. Le maximum le débit théorique est de 27 Mbps [3].

- **Atténuations:** la bande DSRC a également des problèmes de transmission liés à la transmission numérique avec de telles fréquences, telles que la réflexion, la diffraction, la dispersion, de l'effet Doppler, des pertes et des retards de propagation dus aux réflexions à trajets multiples [3].

- **Puissance d'émission limitée:** la puissance d'émission est limitée dans l'archive WAVE tecture, ce qui limite la distance que les données peuvent atteindre. Cette distance peut atteindre 1000 m. Cependant, dans certains cas spécifiques tels que les urgences et la sécurité publique, il est autorisé pour transmettre avec une puissance plus élevée [3] .

-**Le potentiel énergétique :** À la différence des réseaux sans fil traditionnels où la contrainte d'énergie représente un facteur limitant important, les entités des réseaux véhiculaires disposent de grandes capacités énergétiques qu'elles tirent du système d'alimentation des véhicules.

-**Batterie et stockage illimités :** contrairement à d'autres types de réseaux mobiles, les VANET ne souffrent pas de capacité de calcul ou de panne de stockage. Cependant, exigence de traitement en temps réel d'une grande quantité d'informations est un défi pour garder à l'esprit.

1.4.5 Domaines d'application des réseaux VANETs

Les unités de bord de routes (RSU : Road Side Unit) peuvent être considérées comme des points d'accès ou des routeurs ou même des points tampons qui peuvent stocker des données et

les fournir au besoin aux véhicules demandeurs [1]. Toutes les données stockées sur les RSU peuvent être téléchargées par les véhicules. En tant qu'applications de voiture vers le trafic automobile, les applications vers l'infrastructure, les applications de la voiture vers la maison et les applications au profit du routage.

Par ailleurs, une classification des applications pourra être effectuée selon les modes de communication soit V2V ou V2I. Nous organisons les applications liées aux réseaux VANETs dans les classes suivantes [1] :

¬Orientée vers la sécurité

¬Orientée commercialement

¬ Orientée vers la commodité

¬ Applications productives

1.4.4.1 Application de sécurité

Les applications de sécurité peuvent être classées comme suite :

- Traffic en temps réel : Les données de trafic en temps réel peuvent être stockées dans les RSUs pour qu'elles soient disponibles aux véhicules. Cela peut jouer un rôle important dans la résolution des problèmes tels que les embouteillages, les alertes d'urgence telles que les accidents.
- Transfert de messages coopératifs : Un véhicule échangera des messages avec les RSUs et coopérera pour aider d'autres véhicules. Bien que la fiabilité et la latence soient très préoccupantes, cela peut automatiser des problèmes comme le freinage d'urgence pour éviter d'éventuels accidents.
- Notification post-crash : Un véhicule impliqué dans un accident diffusera des messages d'avertissement concernant sa position pour les véhicules en aval afin que ces derniers puissent prendre des décisions ainsi que pour la patrouille d'autoroute pour le soutien de remorquage.
- Notification de contrôle des dangers de la route : Les véhicules déclarent à d'autres véhicules des informations concernant l'état des routes telles que le glissement de terrain, l'existence d'un virage dangereux, la descente soudaine, etc.
- Avertissement de collision coopérative : Alerte aux conducteurs de l'existence d'un accident sur la route.

1.4.4.2 Application commerciales

Les applications commerciales fourniront aux conducteurs le divertissement et les services en tant qu'administrateur sur le web, en streaming audio et vidéo. Les applications commerciales peuvent être classées comme suit :

- Personnalisation/diagnostic de véhicule à distance : Il permet de télécharger des paramètres de véhicule personnalisés ou de télécharger des diagnostics de véhicules à partir d'une infrastructure.
- Accès à Internet : Les véhicules peuvent accéder à Internet via les RSUs si ces dernières fonctionnent comme routeurs.
- Téléchargement de la carte numérique : Les cartes routières des régions peuvent être téléchargées par les conducteurs selon l'exigence avant d'entrer dans une nouvelle zone pour le guidage des conducteurs. En outre, "Content Map Database Download" agit comme un portail pour obtenir des informations actualisées sur l'état des routes des régions en question.
- Publicité à valeur ajoutée : Spécialement pour les fournisseurs de services, qui souhaitent attirer les clients dans leurs magasins. Les annonces comme les pompes à essence, les restaurants routiers pour annoncer leurs services aux conducteurs dans la gamme de communication. Cette application peut être disponible même en absence d'Internet.

1.4.4.3 Applications de commodité

La solution de commodité concerne principalement la gestion du trafic dans le but d'améliorer l'efficacité du trafic en augmentant le degré de commodité des conducteurs. Les applications de commodité peuvent être classées comme suit :

- Routes : La planification de l'itinéraire et du voyage peut être faite en cas de congestion routière.
- Systèmes de collecte de péage électronique : Le paiement du péage peut se faire par voie électronique au moyen d'un point de collecte de péage. Un point de collecte de péage doit en mesure de lire l'OBU du véhicule. Les OBU fonctionnent en utilisant un GPS et l'odomètre et permettent aux techniciens à bord des routes de déterminer dans quelle mesure les véhicules ont voyagé en référence à une carte numérique et à un GSM pour autoriser le paiement du péage via un lien sans fil.
- Disponibilité du stationnement : Les notifications concernant la disponibilité du stationnement dans les villes métropolitaines permettent de trouver la disponibilité des créneaux horaires dans les parkings dans une certaine zone géographique.

- Prévision active : Elle anticipe la prochaine publication de la route, qui devait optimiser

l'utilisation du carburant en ajustant la vitesse de croisière avant de commencer une descente ou une montée.

1.4.4.4 Applications productives

Nous l'appelons intentionnellement comme productif, car ces applications sont additionnelles aux applications susmentionnées. Les applications productives peuvent être classées comme suit :

- Avantages environnementaux : Le programme de recherche AERIS consiste à générer et à acquérir des données de transport en temps réel pertinentes sur le plan environnemental et à utiliser ces données pour créer des informations pouvant être mises en évidence pour soutenir et faciliter les choix de transport par les utilisateurs et les opérateurs du système de transport. Dans le cadre d'une approche multimodale, le programme AERIS fonctionnera en collaboration avec l'effort de recherche de communication en mode V2V pour mieux définir la manière dont les données et les applications des véhicules connectés pourraient contribuer à atténuer certains impacts environnementaux négatifs.
- Le temps d'utilisation : Si un voyageur télécharge son courrier électronique, il peut transformer le trafic de bourrage en une tâche productive en consultant les informations retournées par le système embarqué implanté sur son véhicule et connaitre aussi si le trafic est bloqué en aval. On peut naviguer sur Internet quand quelqu'un attend en véhicule un parent ou un ami.

1.4.5 Défits

Qualité de service : La Qualité de service se mesure en fonction de l'application supportée. On peut distinguer plusieurs contraintes dans les applications utilisées dans les VANET, parmi : la latence, les messages doivent parvenir à destination dans des délais courts; une connectivité non intermittente, par exemple les applications de confort tel le transfert de fichiers ou le besoin de téléchargement nécessitent une connectivité permanente, …etc.

Canal radio fiable : Le rôle des mécanismes de gestion du canal radio est d'offrir des transmissions fiables et robustes et un partage équitable du médium de communication. Pour atteindre cet objectif dans le cas des réseaux véhiculaires, il est nécessaire de définir des méthodes qui permettent de faire face aux deux problèmes majeurs des transmissions qui sont,

les interférences inter-symboles dues à la propagation des ondes par trajets multiples et l'effet Doppler causé par le mouvement des véhicules.

Routage : 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. Les problèmes auxquels doivent faire face ces protocoles sont la connectivité intermittente qui rend les routes déjà établies obsolètes et le partitionnement du réseau qui empêche la propagation des paquets.

Sécurité : La sécurité dans les réseaux véhiculaires ad hoc est cruciale, car elle affecte la vie des gens. Il est essentiel, par exemple, que l'information vitale ne puisse pas être modifiés ou supprimés par un attaquant. Les communications passant par un véhicule du réseau ainsi que des informations sur les véhicules et leurs conducteurs doivent être garantis et protégés de façon à assurer le bon fonctionnement des systèmes de transport intelligents.

Conclusion

Dans ce chapitre nous avons présenté les réseaux VANETs qui sont apparus comme solution aux besoins des applications de sécurités routières ; mais actuellement ils permettent aussi de développer de nouveaux services aux usagers de la route comme (la localisation des stations d'essence, emplacements de parking libre et l'accès à Internet).

Afin de mieux comprendre les réseaux véhiculaires, nous avons présenté leurs caractéristiques principales et les différentes entités communicantes ainsi que les différents modes de communications existants.

Dans les chapitres qui suivent nous nous intéresserons à la sécurité dans les VANETs, ainsi que les attaques et mécanismes qui ont été mis en œuvre afin d'assurer la sécurité des véhicules et les messages échangées.

Chapitre 2

La sécurité dans les réseaux VANETs

2.1 Introduction

La sécurité est la première exigence des usagers de la route. C'est la recherche la plus stimulante et la plus prometteuse pour fournir un système de transport intelligent (ITS).Les applications du VANET peuvent être classées dans la catégorie de la sécurité, de commodité et d'applications commerciales. En raison de la grande mobilité des nœuds, des perturbations fréquentes et des attaques de sécurité, la mise en œuvre de VANET est un défi important mais intéressant pour le bon fonctionnement du système VANET.Le canal de réseau doit être disponible pour l'utilisateur tout le temps. Mais en raison de l'attaque DoS, la disponibilité du canal peut être obstruée. Cette attaque au plus fort niveau de risque car le canal complet peut être bloqué et nous ne pouvons pas envoyer nos informations aux autres nœuds. Il existe un nombre différent de méthodes destinées à éliminer l'attaque DoS, mais pour l'instant nous ne sommes pas dans une position de faire disparaître complètement cette attaque et donc beaucoup de recherches sont menées dans ce domaine. Nous ne pouvons que réduire le niveau de gravité de l'attaque de déni de service. Dans ce chapitre, nous ont discutés des différentes solutions possibles fournies par différents chercheurs qui peuvent réduire cette attaque y compris le comportement égoïstes des nœuds.

2.2 Attribus de sécurité des VANETs

Dans cette section, nous présentons les attributs de sécurité pour VANET. En ce qui concerne la sécurité, ces attributs ne peuvent être ignorés.

2.2.1 L'authenticité

Ce concept de sécurité permet aux entités du réseau de s'assurer de la bonne identité des entités avec lesquelles elles communiquent. L'authenticité permet aux différentes entités du réseau de se fier aux données et messages diffusés. Elle est la seule exigence qui permet la coopération entre les différents participants ; leur identification permet ainsi d'assurer le bon contrôle de l'authenticité des messages échangés [12]. Il convient de préciser ici qu'il existe deux types d'authentification : une authentification des messages qui permet d'en retracer la source et une authentification des entités qui permet d'identifier les nœuds du réseau [13].

2.2.2 La non-répudiation

Ce concept de sécurité permet de démontrer et localiser avec certitude l'origine des données. Grâce à ce principe, chaque entité diffusant un message sur le réseau ne peut le nier ou se rétracter de l'avoir émis. Ainsi, la non-répudiation permet d'identifier les entités malveillantes qui tentent de commettre des actes illégaux, ce qui permet d'écarter toute possibilité pour qu'un attaquant injecte des données erronées sans qu'elles ne soient immédiatement identifiées. Le concept de non-répudiation est essentiel dans les transactions commerciales en lignes et financières, ainsi que dans les opérations électroniques de facturation. Dans le contexte des VANETs, la signature numérique est utilisée pour garantir la non-répudiation des messages concernant les applications de sécurité et de gestion du trafic [27].

2.2.3 La confidentialité :

Ce concept de sécurité permet de garantir la non-divulgation des données transmises dans le réseau à des parties non autorisées. Seules les parties habilitées peuvent y accéder à travers le réseau .La confidentialité consiste ainsi à préserver les informations vitales liées aux véhicules par l'application des algorithmes de cryptographie asymétrique et symétrique, ce qui empêche les entités malveillantes de suivre et d'écouter les messages concernant un véhicule ciblé dans le réseau. Le standard IEEE 1609.2 utilise le chiffrement *Advanced Standard in CCM mode* (AES-22 CCM)[11] comme algorithme de cryptographie symétrique[27].

2.2.4 L'intégrité :

Ce concept de sécurité permet d'assurer que les messages diffusés ne seront pas modifiés ou altérés volontairement ou accidentellement entre la phase d'émission et de réception par des entités non autorisées (malveillantes). Cet objectif de sécurité vise ainsi à doter les destinataires d'un pouvoir permettant de détecter les manipulations de données effectuées durant leur transmission par les entités malveillantes et rejeter les paquets correspondants. L'intégrité peut être réalisée principalement par l'utilisation des fonctions de hachage et de la cryptographie sur des champs spécifiques des paquets. Cependant, dans les réseaux sans fil, se pose toujours la contrainte de l'intégrité qui n'est pas toujours forcément liée au terme de manipulation. En effet, bien des altérations sont le fait des conditions de propagation radio.

2.2.5 La disponibilité :

Ce concept de sécurité permet de garantir que toute entité autorisée puisse accéder aux ressources du réseau tout le temps avec une qualité de service (QoS) adéquate. En effet, tous les participants dans le réseau doivent avoir un accès effectif et rapide aux différents services de la gestion du trafic, aux applications de sécurité et de confort sollicités. Pour atteindre un bon niveau de disponibilité, il est indispensable d'installer du matériel et mettre en oeuvre des protocoles de sécurité de hautes performances. Cependant, ce concept est principalement menacé par les attaques de type dénis de services (DoS) et trou noir (Black Hole), qui sont des attaques très difficiles à prévoir et à contrôler [2]. Ainsi, il est certainement bien plus difficile d'atteindre cet objectif que les autres ; le but étant juste de réduire des effets de ce type d'attaques [27].

2.3 Les attaques dans le réseau VANET :

Dans cette section, nous présentons les différents types d'attaques possibles sur le réseau de véhicules ad hoc. L'impact de l'attaque sur le système dépend de l'efficacité de l'attaquant. Ces attaques sont imprévisibles et peuvent affecter l'application de sauvetage du réseau VANET. Ces attaques peuvent perturber l'ensemble du système ou peuvent modifier le fonctionnement du système pour obtenir le privilège du système.

2.3.1 Le modèle d'un attaquant :

Sur la base des attaques effectuées par un attaquant sur VANET, ces attaquants sont classés dans les types suivants [11] :

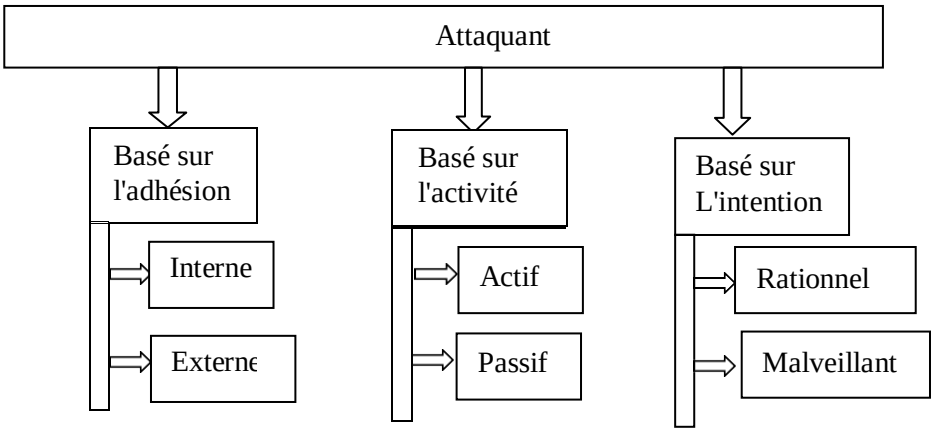


Figure 2-1 le modèle d'un attaquant.

- ***Classification basée sur l'adhésion :*** Sur la base de l'appartenance, deux types d'agresseurs sont possibles :

Les nœuds de confiance d'un réseau, qui communiquaient avec les autres membres du réseau, sont connus sous le nom d'**Interne**, ces membres autorisés du réseau effectuent cette attaque de différentes manières. Au contraire, les **Externes** n'ont pas d'accès direct pour communiquer avec le membre du réseau ; ils ont une capacité d'attaque limitée.

- ***Classification basée sur l'activité :*** Sur la base de l'activité, l'agresseur peut être actif ou passif.

Un attaquant **actif** tente de modifier les informations du réseau en générant des paquets ou des signaux malveillants. Ce type d'attaquant est beaucoup plus nocif que les attaquants passifs.

Alors que les attaquants **passifs** n'écoutent que le canal sans fil, ils n'altèrent pas les informations du réseau.

- ***Sur la base de l'intention :*** Ce terme décrit l'intention qui se cache derrière l'attaque.

Un attaquant **rationnel** cherche à tirer un bénéfice personnel en imposant une attaque sur le réseau, ces attaques sont plus prévisibles, alors que les attaquants **malveillants** n'en tirent aucun bénéfice personnel, et leur intention est de nuire au bon fonctionnement du réseau, il est difficile de prévoir une attaque malveillante.

2.3.2 Classes d'attaques possibles

Dans un réseau de véhicules, les attaquants veulent créer un impact négatif sur le réseau, et les attaques dépendent du comportement dynamique de leurs attaquants spécifiques. L'objectif des attaquants est de créer un maximum de problèmes pour tous les utilisateurs du réseau en lançant différents types d'attaques. Différents attaques possibles sont divisés en cinq classe et chaque classe décrit les niveaux de menace des attaques et leur priorité éventuelle. Dans cette classification d'attaques, la plupart des anciennes attaques ont été incluses et certaines nouvelles attaques possibles dans les communications véhiculaires sont également prises en compte. La figure 2-2 montre les classes d'attaques possibles [9].

Figure 2-2 Classe d'attaques.

2321 Attaque de réseau

Dans cette classe, les attaquants peuvent affecter directement les autres véhicules et l'unité de bord de route (RSU). La priorité de cette classe d'attaques est élevée car elle affecte l'ensemble du réseau de communication et crée des problèmes pour ses utilisateurs légitimes.

J.T. Isaac et.al et S. Zeadally et.al[9] ont énuméré un certain nombre d'attaques dans un réseau de véhicules à savoir les véhicules malveillants, les attaques par force brute, les noeuds malveillants et défectueux, les utilisateurs malveillants et les noeuds malveillants, comme le résume la figure 2-3, qui inclut toutes les autres attaques possibles.

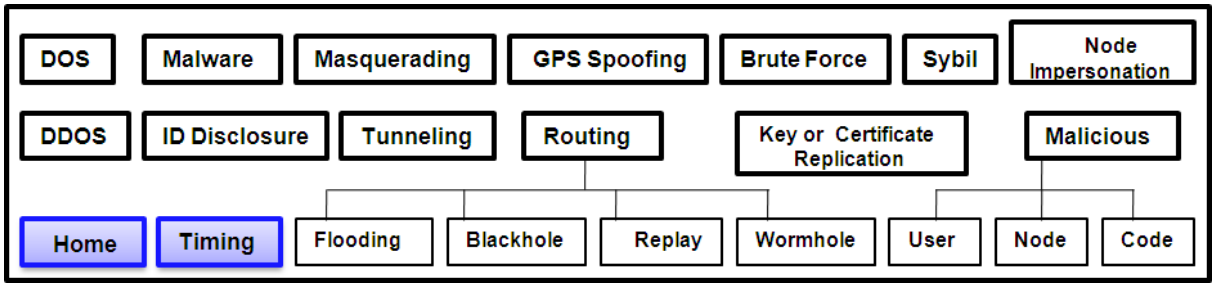


Figure 2-3 Les attaques possibles appartenant l'attaque de réseau.

- **Attaque par déni de service (DOS)**

La disponibilité du réseau est très importante dans un environnement de réseau véhiculaire où tous les utilisateurs dépendent du réseau. Le déni de service (DOS) est l'un des niveaux les plus graves des attaques dans le réseau de véhicules. Dans une attaque DOS, l'attaquant bloque le principal moyen de communication et le réseau n'est plus accessible aux utilisateurs légitimes. L'objectif principal de l'attaquant DOS est d'empêcher les utilisateurs authentiques d'accéder aux services du réseau [18].

La Figure 2-4 montre le scénario complet dans lequel l'attaquant A lance une attaque DOS sur un réseau de véhicules et brouille tout le moyen de communication entre V2V et V2I. En conséquence, les utilisateurs authentiques (B, C et D) ne peuvent pas communiquer entre eux ni avec l'infrastructure[17].

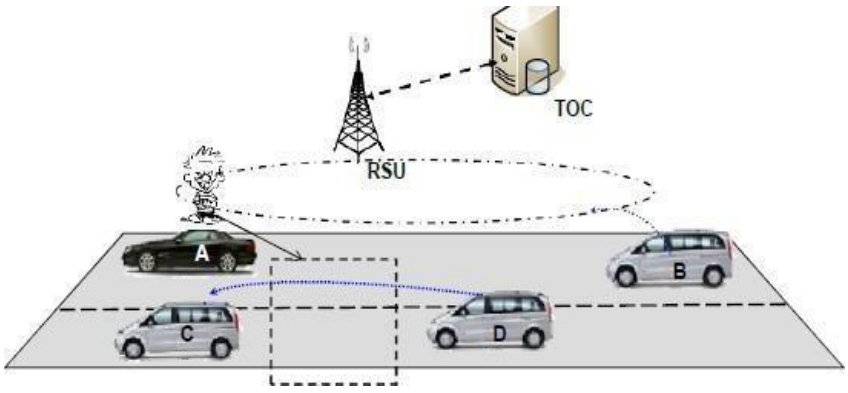


Figure 2-4 Attaques DOS entre V2V et V2I

- **Attaque par déni de service distribué (DDOS)**

Les attaques DDOS sont plus graves dans l'environnement des véhicules car le mécanisme de l'attaque est distribué. Dans ce cas, les attaquants lancent des attaques à partir de différent endroits. Ils peuvent utiliser des créneaux horaires différents pour envoyer les messages. La nature des messages et le créneau temporel peuvent varier d'un véhicule à l'autre. L'objectif des attaques est le même, à savoir la destruction du réseau.

- La figure 2-5 explique l'attaque DDOS pour les infrastructures où trois attaquants (B,C,D) dans le réseau et lancent des attaques sur l'infrastructure à partir de différents endroits. Lorsque d'autres véhicules (A,E) du réseau veulent accéder au réseau, l'infrastructure est surchargée.

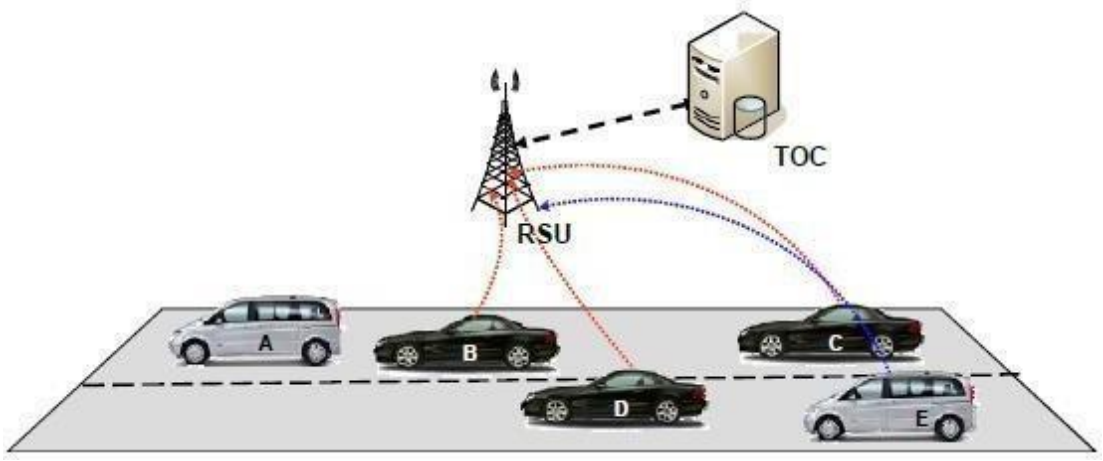


Figure 2-5 DDOS dans la communication entre véhicule et infrastructure

- **L'attaque de Sybille (Sybil attack)**

Dans l'attaque Sybille, l'attaquant envoie plusieurs messages à d'autres véhicules et chaque message contient une identité de source (ID) fabriquée différente. Il fournit une illusion aux autres véhicules en envoyant des messages erronés comme les messages d'embouteillage. [13]

- **Timing Attack**

Les utilisateurs ont besoin de l'information appropriée au bon moment, souvent immédiatement. Par conséquent, un facteur important pour les applications de sécurité et non de sureté est le temps. Le temps est un problème nouvellement considéré où il n'y a pas de changement du contenu des messages ; au

lieu de cela, l'attaquant provoque un retard dans les messages originaux en y ajoutant quelques tranches de temps. Ce faisant, l'utilisateur visé reçoit les messages trop tard pour être d'une quelconque utilité [14].

- **Attaque à domicile :**

Un autre type de nouvelle attaque est l'attaque à domicile [15]. L'internet fournit des services importants aux usagers de la route tout au long de leur voyage. Un attaquant prend le contrôle de tout véhicule de l'utilisateur sur la route grâce à la connexion Internet.

La figure 2-6 montre un scénario d'attaque à domicile:

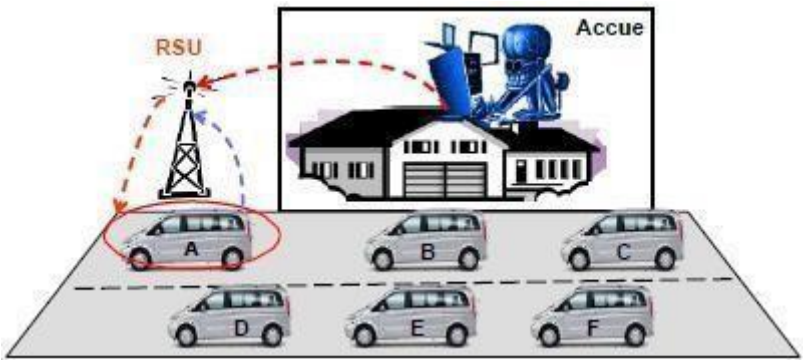


Figure 2-6 Attaque à domicile

2322 Attaque d'application (AP)

Les applications de sécurité et de non sureté sont deux types potentiels pour les véhicules. Dans cette catégorie, la principale préoccupation de l'agresseur est de modifier le contenu de ces applications et de les utiliser à son avantage. L'importance des applications de sécurité est plus grande ; des messages d'avertissement sont fournis aux autres utilisateurs. Les attaquants modifient le contenu du message réel et envoient des messages faux ou erronés à d'autres véhicules, ce qui provoque un accident. L'attaque par des informations erronées [16] est l'un des exemples d'attaque où l'attaquant envoie des informations erronées au réseau et où ces messages erronés affectent directement le comportement des utilisateurs sur la route[9].

2323 Attaque sociale

Tous les messages immoraux (attaques sociales) sont considérés dans cette classe et l'intention de l'attaquant d'envoyer ce genre de messages dans un réseau est de créer indirectement des problèmes pour les autres utilisateurs du réseau. Les utilisateurs authentiques

du réseau se mettraient en colère lorsqu'ils reçoivent ce genre de messages ; c'est exactement ce que veut l'attaquant, un changement de comportement positif des utilisateurs vers un comportement négatif de colère[9].

2324 l'attaque de Surveillance

La surveillance et le suivi des attaques de véhicules sont considérés dans cette classe. Dans l'attaque de surveillance, l'attaquant se contente de surveiller l'ensemble du réseau, en écoutant la communication entre V2V et V2I. Par exemple, la police prévoit de mener une opération contre des criminels dans une région spécifique, elle communique donc avec les autres et les informe du lieu de l'opération.

- **Attaque de l'homme du milieu (MiMA) :** MiMA est une attaque très connue dans le domaine de la communication. Elle implique que l'attaquant réside entre deux ou plusieurs véhicules et lance cette attaque. MiMA est une écoute active et établit des connexions indépendantes avec les véhicules des victimes. Les émetteurs et les récepteurs de cette attaque supposent qu'ils communiquent directement entre eux, mais en réalité l'attaquant contrôle tous les la communication, en injectant de fausses informations entre les véhicules, en écoutant la communication entre les véhicules[15].

2325 Attaque de spamming

Dans cette situation, le seul but de l'attaquant est d'augmenter la latence de la transmission et d'utiliser la largeur de bande du réseau afin qu'aucun service ne soit disponible pour les autres utilisateurs ; cela est réalisé en envoyant des messages de spam par le réseau. Il est presque impossible de contrôler ce type d'attaques lorsqu'il n'y a pas d'infrastructure de base ou d'administration centralisée disponible [19, 20].

De plus, des classes d'attaques présentées ci-dessus nous définissons un autre comportement qui peut nuire au bon fonctionnent des réseaux de véhicule :

- **L'égoïsme :** Les comportements égoïstes ne sont pas vraiment des attaques, mais des comportements des nœuds qui refusent de coopérer avec les autres pour assurer le bon fonctionnement du routage ad hoc, afin d'économiser la bande passante et les ressources de calcul.[6] Dans un réseau ad hoc il est difficile de détecter des nœuds égoïstes [35] qui peuvent tout simplement être silencieux et/ou refusent de transférer les données afin de préserver leur ressource. Quand de tels nœuds sont nombreux dans le réseau, la disponibilité du service de routage est touchée. Ce problème d'égoïsme n'existe pas dans

les réseaux traditionnels où les nœuds reposent sur les routeurs dédiés pour assurer la fonctionnalité de routage. Donc, de nouveaux mécanismes doivent être désignés pour garantir la coopération des nœuds dans les réseaux **VANETs**.

2.4 Travaux connexes

Dans cette section : nous nous concentrons sur les différentes techniques utilisées pour détection d'une attaque « DoS » et du comportement égoïste.

Abdul Quyoom et.al[23] ont proposé un système Malicious and Irrelevant Packet Detection Algorithm (MIPDA)utilisé pour s'assurer de l'absence de paquets malveillants et non pertinents. Il s'agit de détecter une certaine position des véhicules qui génèrera le message nuisible pour un autre véhicule. Après avoir détecté la position du véhicule, cette information est stockée dans le RSU concerné. Si le paquet est valide, alors le véhicule ne sera pas suivi, sinon le véhicule concerné sera suivi. Cet algorithme basé sur le changement continu de position d'un véhicule le long de la route. Il traite également La génération de paquets et renforce la sécurité du système VANET.

Usha Devi Gandhi et.al[21] présente L'algorithme APDA (Attacked Packet Detection Algorithm) détecte l'attaque DOS avant le temps de vérification. L'algorithme APDA fixe la portée de communication des véhicules. Que la portée soit appelée valeur seuil. Et il tient compte de la position, de l'horodatage, de la vitesse, etc.., pour de déterminer si elle se situe dans la portée du radar et pour la détection des fausses alertes. Si le nombre de paquets et la vitesse maximale est supérieure à la vitesse du véhicule, cependant il est considéré comme une attaque du fait que la position du véhicule change très rapidement. De même, s'ils sont très faibles, leurs positions ne changent pas très rapidement aussi dans ce cas considéré comme attaque. Après l'achèvement de ce processus, les véhicules sont validés et stockés dans la base de données de la RSRT (Road Side Radio Transdictor). L'algorithme RRDA (Requenst and Response Detection Algorithme) est utilisé pour la vérification des nouvelles demandes qui veulent rejoindre le réseau.

Aditya Sinha et.al [24] présente l'algorithme QLA(Queue Limiting Algorithm) pour la protection des véhicules. Dans ce système, chaque véhicule a une certaine barre supérieure pour recevoir un nombre limité de massages de sécurité. Ainsi, le fait de recevoir une limitation des massages de sécurité protégeront le nœud contre les attaques de déni de service. Pour trouver la limite supérieure de la réception du message (message de sécurité), le véhicule envoie un paquet de salutations dans le réseau à intervalle régulier et attends sa réponse. Lorsque la réponse arrive,

l'OBU compte le nombre de réponses. La performance de cette approche est mesurée, sur la base du routage des frais généraux, la réception des messages et le taux de livraison des paquets. Cette approche est capable d'empêcher VANET d'être attaqué par la DoS et de rendre la communication dans ses conditions normales pendant l'attaque.

Amarpreet Singh et.al [25] présente EAPDA (Enhanced Attacked Packet Detection Algorithme) pour détecter le nœud malveillant. Dans cette approche, chaque RSU fourni un mécanisme d'EAPDA. Le RSU procédera à la vérification de chaque nœud en envoyant une demande à tous les véhicules. Il enregistrera les informations relatives aux véhicules, telles que l'identité, le lieu, l'heure, etc. dans sa base de données. Lorsque le véhicule envoie une demande à la RSU, cette dernière enregistre l'identification du véhicule pour une utilisation future et elle accuse réception de la demande. Ainsi qu'un créneau horaire est calculé en utilisant le temps de communication moyen de chaque nœud. Les véhicules peuvent communiquer avec le RSU pour obtenir les informations relatives au trafic et autres dans le créneau horaire alloué. Pendant cette période, le RSU compare le nombre de paquets qui ont été transféré et analyse le comportement inhabituel des nœuds, s'il y en a, L'attaque DoS est détectée à l'aide de la tranche horaire. Ainsi, l'algorithme EAPDA est plus réactif et la vérification est effectuée avec moins de retard.

Mohamed Nidhal Mejri et.al [26]ont présenté deux approches de la sécurité basée sur la théorie des jeux. Dans un jeu, lorsqu'un joueur effectue une action, l'autre réagit par une réaction. Selon le principe général de la théorie des jeux, chaque joueur essaie de maximiser son gain et/ou de réduire sa perte. Les deux jeux proposés s'appelaient Jeu stratégique et Jeu extensif.

Dans le jeu stratégique dans lequel chaque joueur est conscient des mouvements de tous les autres joueurs. Le deuxième jeu avec des informations parfaites aussi appelée jeu dynamique. La performance des jeux de réaction ont été mesuré par le taux de livraison des paquets (PDR) et Packet Overhead. La comparaison des frais généraux de paquets de jeux étaient le fil conducteur de deux schémas de réaction surperforment leur régime de distribution et sous-performent leur régime hybride. Il convient de noter que les régimes auxquels comparer sont des jeux préventifs et non une pure stratégie de réaction.

Karnan Verma et.al [22]ont proposé l'approche appelée "IP CHOCK", basé sur le filtre Bloom

avec fonction de hachage pour prévenir les attaques par déni de service (DoS) qui consiste à identifier le véhicule malveillant sans échange d'informations secrètes. Pour détecter l'attaque DoS à un stade précoce. Ici, le détecteur de demande et le détecteur de réponse sont utilisés. Le détecteur de demande déployé à la périphérie du routeur d'hôtes et le détecteur de réponse est déployé par le détecteur de choc protégé pour détecter les attaques. Les attaques DoS peuvent être détectées sur la base d'un tableau de surveillance mis à jour. Il s'agit d'une structure de données efficace en matière de stockage, qui nécessite un tableau de longueur fixe pour enregistrer les informations pertinentes sur les véhicules[5].

Mahdi Bounouni et.al [10]propose l'approche **APS** (Acknowledgment-based punishment and stimulation scheme for mobile ad hoc network)qui s'articule autour de quatre modules coopératifs et interactifs : surveillance, réputation, stimulateur et isolateur. Le module de surveillance est chargé de contrôler la bonne transmission des paquets de données et du routage. Le module de réputation évalue la réputation de tous les voisins. Le système APS utilise un crédit comme incitation. Le module stimulateur est responsable de la gestion et de la mise à jour des comptes des nœuds. Le module isolateur punit les nœuds malveillants et égoïstes. L'approche APS peut être utilisée par exemple pour sécuriser les trafics multimédia sur MANETs.

Nous présentant ci-dessous un tableau récapitulant les différents travaux décrits ci-dessus :

AUTEUR	TECHNIQUE	DESCRIPTION	atouts	Limites
Abdul Quyoom, Raja Ali et Devki Nandan Gouttam, Harish Sharma	MIPDA	Cet algorithme fonctionne sur les exigences de changement de position continu d'un véhicule le long de la route. Les paquets malveillants et non pertinents sont analysés et identifiés	Cet algorithme peut également être appliqué avant le moment de la vérification afin d'analyser la force des signaux générés à chaque instant et d'augmenter la sécurité.	Cet algorithme ne compare que la fréquence et la vitesse.
Usha Dev Gandhi, R.y'S.M Keerthana	APDA & RRDA	L'algorithme APDA détecte l'attaque DOS avant la vérification. L'inondation peut être encore réduite par l'algorithme RRDA.	L'utilisation de deux algorithmes permet de réduire les inondations et les fausses alertes.	Le paquet de décisions sera généré ; il peut ne pas être sécurisé
Mahdi Bounouni, Louiza Bouallouce - Medjkoune	APS	L'approche APS est structurée autour de quatre modules interactifs : surveillance, réputation, stimulateur et isolateur .	punir les nœuds malveillants qui laissent tomber des paquets de données et de stimuler la coopération des nœuds égoïstes.	l'approche APS s'appuie sur l'échange de paquets d'accusé de réception, Cette technique introduit une surcharge supplémentaire dans le réseau.
Aditya Sinha, Prof Santosh K. Mishra	QLA	Chaque véhicule possède une barre supérieure pour recevoir un nombre limité de massages de sécurité. Ainsi, le fait de recevoir un nombre limité de massages de sécurité protégera le nœud contre les attaques de Dos.	Chaque véhicule a une capacité limitée de réception de messages (messages de sécurité) et cette capacité est décidée par cet algorithme.	La limitation de la réception des messages conduira à l'abandon des véhicules honnêtes.

Amarpreet Singh, Priya Sharma	EAPDA	RSU compare le nombre de paquets qui lui sont transférés à partir de chaque nœud pour identifier et analyser le comportement inhabituel des nœuds malveillants, le cas échéant Les nœuds malveillants seront détectés s'ils envoient environ le double du taux de paquets que le taux habituel.	L'attaque par déni de service est détectée à l'aide d'un intervalle de temps ; elle est donc essentiellement basée sur le temps de communication moyen des nœuds.	La performance n'est analysée que pour les trois facteurs. Débit Faux Taux positif et retard. Ici, le principal facteur est la livraison de paquets qui n'est pas prise en consideration
Mejri Mohamed Nidhal, Mohamed Hamd	JEU STRATÉGIQUE ET ÉTENDU	Essayez d'éviter de traverser les zones attaquées. Jeu stratégique : Des informations stratégiques à somme nulle avec des informations parfaites Jeu complet : Forme extensive avec des informations parfaites, également appelée jeu dynamique.	Selon le principe général de la théorie des jeux, chaque joueur essaie de maximiser son gain et/ou de réduire sa perte.	En raison de la grande mobilité et des changements rapides de topologie, la théorie des jeux est compliqué à mettre en œuvre.
Karnan Verma, Halabi Hasbullah Ashok Kumar	IP.CHOCK basé sur le filtrage des blooms avec fonction de hachage	Les adresses IP de la source et de la destination sont enregistrées dans la table de hachage. Les détecteurs de demande et de réponse sont utilisés pour détecter les attaques.	Ce système ne se contente pas de détecter l'attaque de la DoS, il donne l'alerte à chaque attaque. L'utilisation de la table de hachage et du filtrage des blooms est la force de ce système.	Évaluation des performances Certains paramètres sont définis manuellement, ce qui entraîne un manque de précision

Table 2-1 Tableau récapitulatif des différentes approches.

Conclusion

Pour conclure, nous remarquons que l'attaque DOS est d'une grande importance dans le domaine de la recherche vu qu'elle est abordée par une communauté importante de chercheurs. Les différents travaux s'intéressent à l'attaque sous différents angles, aux dégâts qu'elle peut causer et proposent des solutions. Cependant, certains nœuds peuvent se comporter de manière égoïste afin d'économiser leurs ressources en abandonnant des paquets de routage. De plus, dans la majorité des travaux proposés, les véhicules malveillants détectés sont exclus du réseau. En effet, l'exclusion définitive ces véhicules affectera de façon significative les tâches de routage dans le réseau.

C'est dans ce sens que nous allons proposer dans le prochain chapitre une solution qui permet non seulement de détecter les attaques DOS et le comportement égoïstes des véhicules dans le réseau mais aussi d'inciter les nœuds à coopérer dans le réseau en leur donnant des chances pour améliorer leur comportement au lieu de les exclure définitivement.

Chapitre 3

Mécanismes de détection et de sanction pour la sécurisation des VANETs contre les attaques DOS et les comportements égoïstes.

3.1 Introduction

Les réseaux ad-hoc de véhicules sont composés de participants ayant les mêmes caractéristiques en termes de ressources. Ce sont des nœuds qui communiquent de manière décentralisée à travers un réseau sans-fil. Ces réseaux ont pour particularité de dépendre fortement les uns des autres. De ce fait, il est important de s'assurer de l'effectivité des tâches effectuées par chaque participant du réseau en évitant des comportements égoïstes par des nœuds. Ou encore des attaques potentielles tel l'attaque DOS . Pour mener à bien ces tâches, chaque entité réseau observe le comportement de ses voisins en utilisant la technique de réputation.

Pour cela, dans ce chapitre nous allons présenter notre approche qui repose essentiellement sur deux mécanismes. En effet, nous présentons dans un premier temps un mécanisme de détection des nœuds malveillants et de calcul de la confiance. Par la suite nous proposons un mécanisme de sanction qui permet d'isoler les nœuds malintentionné du réseau de façon temporaire ou de les exclure définitivement.

3.2 Motivations

La mobilité croissante des personnes a entraîné un coût élevé pour les sociétés en raison du nombre croissant d'embouteillages, de décès et de blessures. Les réseaux ad hoc de véhicules (VANET) envisagent des services de soutien sur les systèmes de transport intelligents (STI), comme la surveillance collective du trafic, l'évitement des collisions, la navigation des véhicules, le contrôle des feux de circulation et la gestion des embouteillages par l'envoie des signalisations aux conducteurs. Cependant, certains comportements malveillants de la part des usagers malintentionnés peuvent nuire au bon fonctionnement de ces réseaux.

Pour les applications de sécurité, les informations doivent être exemptes d'erreurs et transmises en toute sécurité de l'expéditeur à la cible. Ainsi, la sécurité est très nécessaire car une petite déconnexion peut créer un gros problème pour les utilisateurs. Pour obtenir cette condition, le réseau doit être disponible pour les utilisateurs tout le temps car cette dernière est l'un des principales exigences de sécurité dans ce type de réseaux.

Mais en raison des attaques DoS et des comportements égoïstes, la disponibilité des canaux peuvent être obstrué. Le DoS est sur le réseau pour ralentir son fonctionnement en introduisant un trafic inutile. Il rend le réseau temporairement indisponible ou suspend les services d'un hôte connecté à l'internet, ainsi un nœud peut se comporter de manière égoïste et refuse de relayer l'information à ses voisins.

De ce fait, nous avons pensé à sécuriser davantage les usagers de véhicule, et apporter notre contribution pour la bonne marche du réseau routier.

3.3 Hypothéses

- Architecture plate, tous les nœuds possèdent les mêmes caractéristiques.
- Nous considérons un réseau composé de nœuds dont les comportements sont différents. Celui-ci peut être confiant, malveillant [28] ou égoïste [27] :
  - Les véhicules malveillants, un nœud défectueux transmet un grand nombre de messages inutiles demandant au réseau de valider les demandes dont l'adresse du retour est incorrecte. Par conséquent, le réseau ne sera pas en mesure pour rechercher l'adresse du nœud défectueux à ce moment-là lorsqu'elle doit envoyer l'approbation de l'authentification. Elle fait en sorte que le réseau tienne plus longtemps avant que le lien de communication soit établi. Lorsque le réseau s ferme le lien, un nœud défectueux enverra des messages excessifs pour son authenticité, qui ont une mauvaise adresse de retour. Par conséquent, la série de vérifications sera relancée et le serveur doit attendre longtemps, ce qui maintient le réseau suspendue.
  - Les véhicules égoïstes, contrairement aux malicieux, altèrent les performances du réseau de façon passive. Un véhicule égoïste peut refuser de relayer un message par exemple, pas pour alléger la charge du réseau mais parce que cette action diminue de ses ressources personnelles, comme par exemple son temps d'accès au canal. Il refuse alors, car la tâche ne lui apporte aucun bénéfice. Les véhicules égoïstes restent néanmoins rationnels et en aucun cas ils n'altèrent le contenu des messages à relayer.
- Tous les nœuds sont initialement confiants, chaque nœud a confiance à ces voisins avec un taux de confiance égale à 0.9.

3.4 Description

Dans notre travail, nous avons élaborés un mécanisme de sécurisation des VANETS basé essentiellement sur la détection et la sanction. En effet, nous proposons dans la première partie un algorithme qui permet de détecter les comportements malveillants des véhicules, par la suite nous calculons à chaque véhicule une valeur de confiance. Sur la base de cette dernière nous décidons de sanctionner les nœuds malveillants en se basant sur l'algorithme que nous proposons dans la deuxième partie de notre travail qui permet soit d'isoler les nœuds temporairement ou de les exclure définitivement du réseau.

3.5 Algorithme de détection et de calcul de la confiance

Dans notre approche, les nœuds du réseau communiquent entre eux. Sur la base des messages échangés, chaque nœud établit une confiance à ses voisins sans avoir recours aux recommandations des autres nœuds.

3.5.1 Hypothèses

- Initialement tous les nœuds du réseau sont supposés fiables.
- Les notations utilisées par l'algorithme de détection et de calcul de la confiance sont décrites dans le tableau suivant:

Notation	**Description**
N	Nombre de voisins .
nbMsg.	Nombre de messages reçu de chaque voisin.
Moy	Moyenne des messages reçus
σ	Ecart type
TauxCI	Taux de confiance initiale des nœuds.

DIFF1	le nombre de messages manquants pour atteindre la limite inferieure **(Moy-σ).**
DIFF2	le nombre de messages dépassants la limite supérieure **(Moy+σ).**
TauxCF(i)	Taux de confiance finale d'un nœud « i »

Table 3-1 Notations utilisés dans l'algorithme de détection et de calcule de confiance.

3.5.2 Principe de fonctionnement

Dans ce qui suit, nous allons décrire les étapes nécessaires au fonctionnement de l'algorithme de détection et de calcul de la confiance :

- Un nœud du réseau calcule le nombre de message reçu par chaque voisin.
- Ensuite, il procède au calcul de la moyenne et d'écart type comme suit :

La moyenne : $\boldsymbol{Moy = (1/n) \sum_{i=1}^{n} nbMsg}$. **[3.1]**

L'écart type : $\boldsymbol{\sigma = \sqrt{((1/n) \sum_{i=1}^{n} (nbMsg - Moy)^2)}}$ **[3.2]**

- Après l'étape précédente, le nombre de message est comparé à l'intervalle [***Moy- σ***, ***Moy+ σ]*** dont la borne supérieure est la somme de la moyenne et l'écart type et la borne inférieure est leur différence. Selon la position du nombre de messages par rapport à l'intervalle on déduit les trois cas possibles:

Cas 1 : ***Moy- σ ≤ nbMsg ≤ Moy+ σ***

Si le nombre de message reçu est dans l'intervalle [***Moy- σ***, ***Moy+ σ***] alors le nœud émetteur sera considéré comme nœud confiant ,et son taux de confiance reste inchangé.

TauxCF= TauxCI=0.9.

Cas2 : (*Moy+σ)<nbMsg*

Dans ce cas le nombre de message est plus grand que la borne supérieure ce qui implique qu'un nombre important de messages ont été envoyés. En conséquence, le nœud sera considéré comme un nœud malveillant effectuant des attaques DOS..

Son taux de confiance sera calculé ainsi :

Calculons : $\boldsymbol{Diff1 = |nbmsg - (Moy + \sigma)|}$. **[3.3]**

- Si **Diff1>1** alors le taux de confiance sera calculé ainsi : $\boldsymbol{TauxCF = 0.9^{Diff1}}$ **[3.4]**
  car plus la diff1 s'éloigne de la moyenne plus la pénalité sera importante,
  et cela se traduit par la diminution du taux de confiance .
- Si **Diff1≤1** alors la fonction de calcul sera ainsi : $\boldsymbol{TauxCF = 0.9^{Diff1+1}}$ **[3.5]**
  Vu que la différence est considérablement petite, toutefois sa pénalité ne sera pas très importante, et diminuera moins qu'en cas précédent.

Cas3 : *nbMsg<(Moy – σ)*

Si le nombre de messages reçus est inférieur à la borne inférieure de l'intervalle, le nœud sera considéré comme nœud égoïste.

Calculons : $\boldsymbol{Diff2 = |nbmsg - (Moy - \sigma)|}$ **[3.6]**

- Si **Diff2>1** alors le taux de confiance sera calculé ainsi: $\boldsymbol{TauxCF = 0.9^{Diff2}}$ **[3.7]**
- Si **Diff2≤1** alors la fonction de calcul sera ainsi: $\boldsymbol{TauxCF = 0.9^{Diff2+1}}$ [**3.8**]

L'algorithme suivant résume le principe de fonctionnement de la détection et du calcul de la confiance:

Algorithme1 : algorithme de détection et de calcule de confiance

---

Données : nbmsg, N, i**,** TauxCI=0.9 ;TauxCF

$\boldsymbol{Moy = (1/n) \sum_{i=1}^{n} nbmsg.}$

$\boldsymbol{\sigma = \sqrt{((1/n) \sum_{i=1}^{n} (nbMsg - Moy)^2)}}$

Si($Moy- \sigma \leq nbMsg \leq Moy+ \sigma$) alors

Ecrire("nœud confiant")

TauxCF= TauxCI=0.9

Sinon

Si ($nbMsg < Moy- \sigma$) alors

Ecrire ("nœud égoïste")

$Diff1 = |nbmsg - (Moy - \sigma)|$;

Si Diff1 ≤1 alors

$TauxCF = 0.9^{Diff1+1}$.

Sinon

$TauxCF = 0.9^{Diff1}$.

FIN SI

sinon

Ecrire ("attaque DOS")

$Diff2 = |nbmsg - (Moy + \sigma)|$;

Si Diff2 ≤1 alors

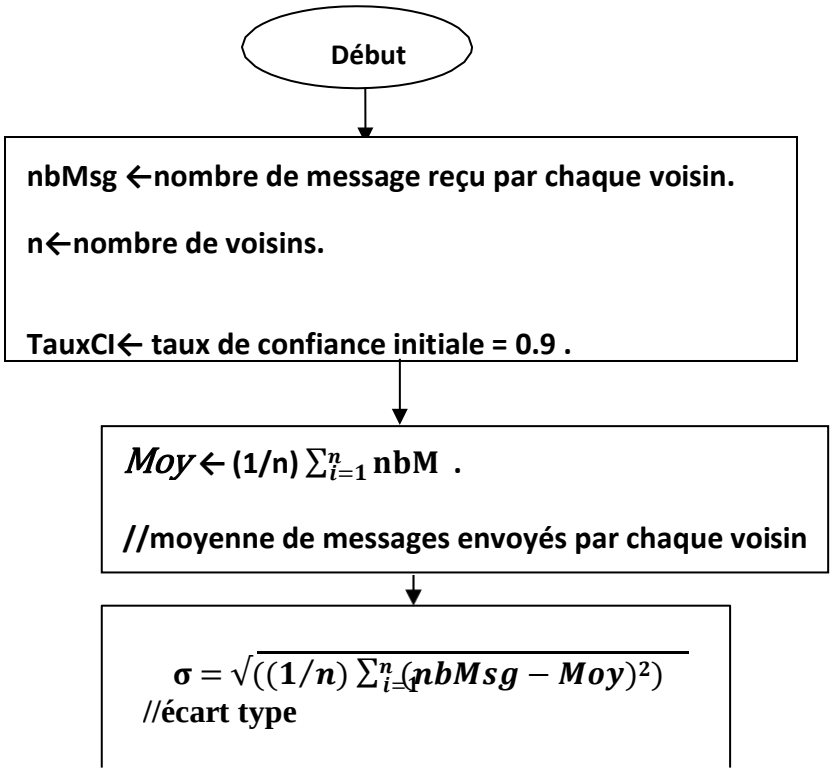
$TauxCF = 0.9^{Diff2+1}$.

Sinon

$TauxCF = 0.9^{Diff2}$.

Fin Fin si fin si

-Nous allons présenter ci-dessous un organigramme récapitulatif de l'algorithme :



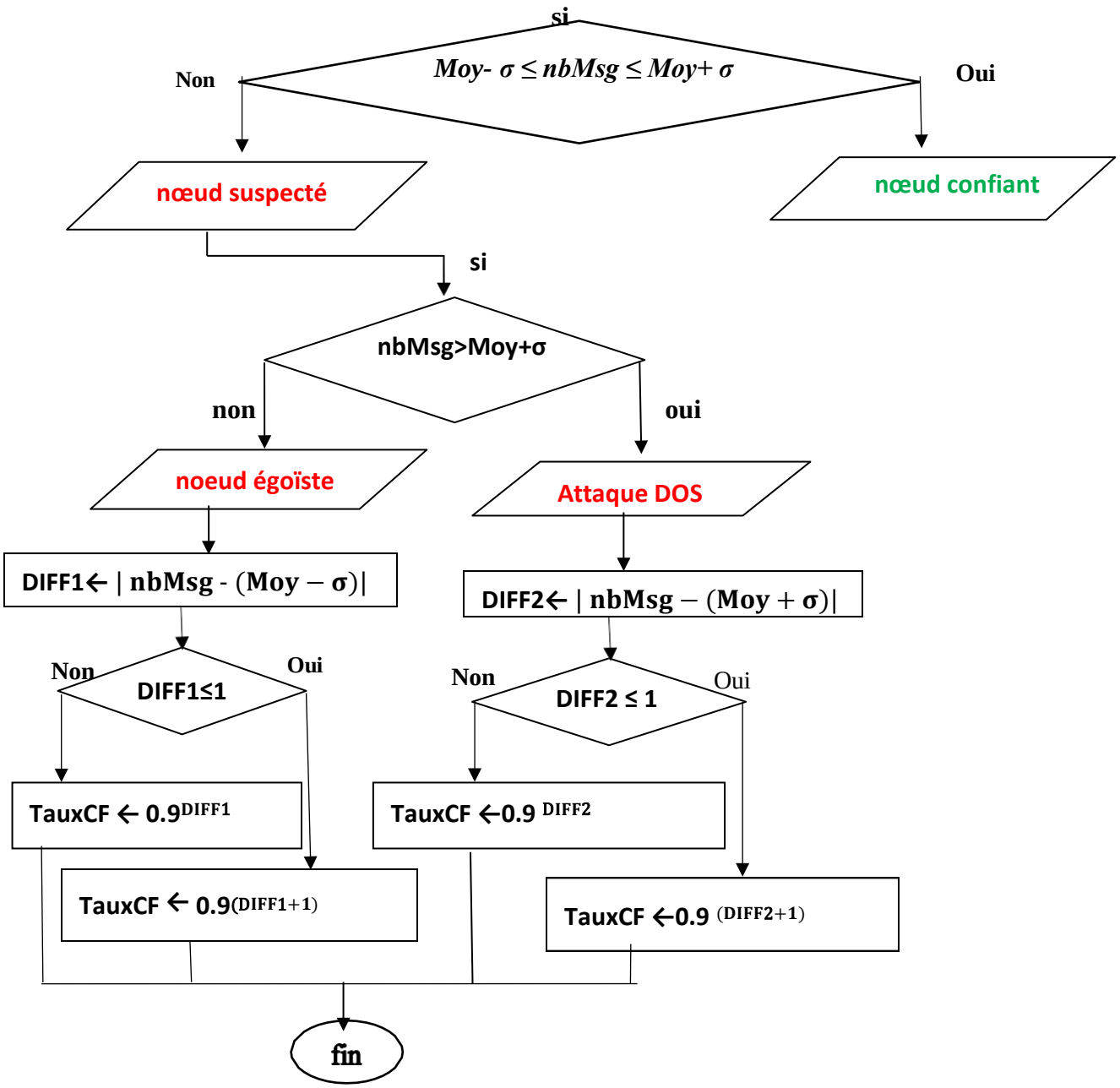


Figure 3-1 Organigrammes de l'algorithme de détection et de calcul de la confiance.

3.6 Mécanisme de sanction basé sur l'isolement :

Apres avoir détecté les nœuds malveillants et calculer leurs confiance, nous proposons dans ce qui suit un algorithme qui permet de sanctionner les nœuds malintentionnés.

Dans ce processus nous procédons pour l'isolement des cas défaillants temporairement selon leur taux de confiance, et on essaye de réintégrer les cas les moins récidiviste (ceux qui font moins de cas de défaillance), les autres seront rejetés définitivement.

3.6.1 Hypothéses

- nous déclarons 4 niveaux de confiance et chaque niveau on lui attribue un état de confiance : A=0.9 ; B=] 0.9, 0.6] ; C=] 0.6, 0.3]; D=] 0.3 ,0].
  - ❖ Confiance **entière** si le taux de confiance est égale **A.**
  - ❖ Confiance **haute** si le taux de confiance est égale **B.**
  - ❖ Confiance **faible** si le taux de confiance est égale **C.**
  - ❖ Confiance **très faible** si le taux de confiance est égale **D.**
- les notations utilisées dans notre algorithme sont représentées dans le tableau ci- dessous:

Notation	**Description**
$Per_{précédent}$	Période précédente
$Per_{actuelle}$	Période actuelle
TISO (i)	temps d'isolement d'un nœud « i »
K	Nombre de fois qu'un nœud est sanctionné (mis dans la liste noire)

Table 3-2 Notations utilisés dans l'algorithme d'isolement.

- Initialement chaque nœud va avoir un compteur 'k' initialisé à 0, qui représente le nombre de fois qu'un nœud est mis dans la liste noire.

3.6.2 Le principe de fonctionnement

- Le mécanisme d'isolement sera effectué ainsi :

- Si le nœud est de Confiance entière alors il transfère librement ses paquets.

- Sinon, si le nœud est de confiance haute, faible ou très faible alors il sera isolé et placé dans la liste noire. Son temps d'isolement dépend de son niveau de confiance. En effet, le temps d'isolement du nœud dans la liste noire sera calculé comme suit :

  - D'abord le nombre de sanction 'k' sera incrémenter , $\boldsymbol{k+1}$.
  - Attribuer pour chaque niveau de confiance un timer tel que: **timer1<timer2<timer3,** Nous aurons ainsi**:**
    - **confiance haute ⟵ timer1**
    - **confiance faible ⟵ timer2**
    - **confiance très faible ⟵ timer3**

- Le temps d'isolement est calculé de la manière suivante :

$$\boldsymbol{TISO = (TauCI - TauxCF(i)) * timer * k}$$

- Après que le temps d'isolement est écoulé, nous vérifions le compteur de nombre des sanctions:
  - Si **0<k<5** alors le nœud va réintégrer le réseau, sinon il sera supprimé définitivement du réseau car il a épuisé toutes ses chances.
  - Le nœud peut diminuer son nombre de sanction à chaque fois que son taux de confiance augmente par rapport au précédent.

-Nous présentons ci-dessous l'algorithme qui résume les étapes du mécanisme d'isolement :

Algorithme 2 : algorithme d'isolement

Données : A=0.9 ; B=] 0.9, 0.6] ; C=] 0.6 0.3];D=]0.3 0]

Timer1<timer2<timer3;$Per_{précédente}$;$Per_{actuelle}$.

si TauxCF=A alors

    Ecrire (" le nœud est de confiance entière") ;

sinon

    k=k+1 ;

Si TauxCF∈B

Ecrire ("le nœud est de confiance haute");

$$\boldsymbol{TISO = (TauCI - TauxCF(i)) * timer1 * k}$$

Sinon si TauxCF∈C alors

Ecrire ("le nœud est de confiance faible") ;

$$\boldsymbol{TISO = (TauCI - TauCF(i)) * timer2 * k}$$

Sinon

Ecrire ("le nœud est de confiance très faible ") ;

$$\boldsymbol{TISO = (TauCI - TauxCF(i)) * timer3 * k}$$

Fin **Fin** **Fin**

- Nous présentons ci-dessous un organigramme récapitulatif de l'algorithme précédent:
  - Comme expliquer précédemment on a 4 niveaux de confiance qui sont : A=0.9 ; B=] 0.9, 0.6] ; C=] 0.6, 0.3]; D=] 0.3 ,0].
  - Nous avons aussi déclarer 3 timers tel que timer<timer2<timer3 .

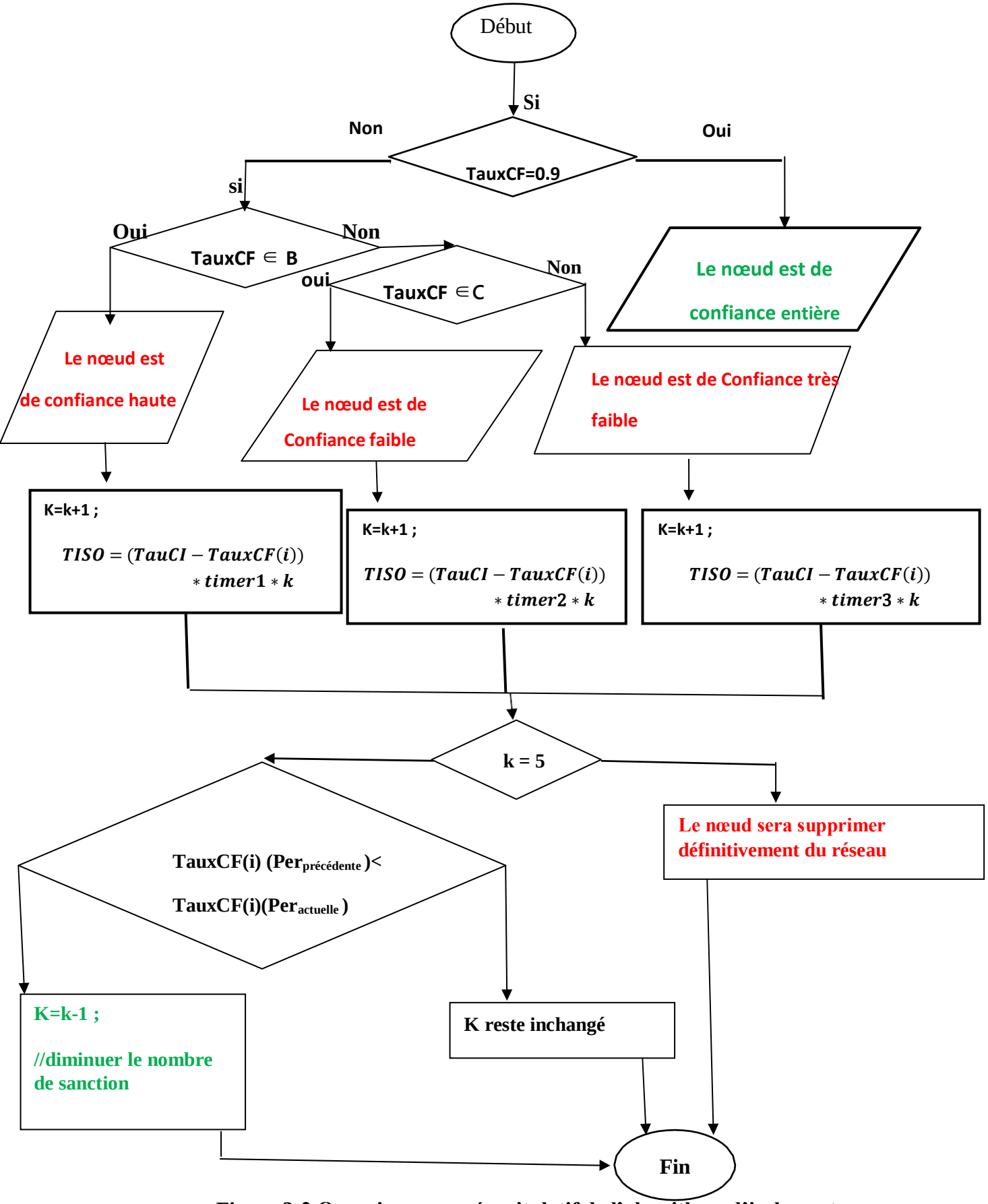


Figure 3-2 Organigramme récapitulatif de l'algorithme d'isolement.

3.7 Analyse :

Dans cette partie nous nous intéressons à la représentation graphique et par valeurs des algorithmes, ceci se traduira par des tableaux de valeurs consolidés par des représentations graphiques .Ce qui aidera à élucider la validité de notre approche,

3.7.1 Analyse de la fonction du taux deconfiance

3.7.1.1 Valeurs de confiance des nœuds lorsque Diff1et Diff2>1

les nœuds voisins de 'j'	Nombre de Msg	Détecter le type de nœud	DIFF1/2	Calcule du taux de confiance
18	0	nœud égoïste	7,3687	0,4601
7	3	nœud égoïste	4,3687	0,6311
14	4	nœud égoïste	3,3687	0,7012
6	5	nœud égoïste	2,3687	0,7791
20	11	confiant	/	0,9
1	12	confiant	/	0,9
2	16	confiant	/	0,9
19	22	confiant	/	0,9
9	35	confiant	/	0,9
16	41	confiant	/	0,9
11	48	confiant	/	0,9
3	58	confiant	/	0,9
10	63	confiant	/	0,9
15	63	Confiant	/	0,9
8	74	Confiant	/	0,9
13	78	Confiant	/	0,9
4	94	attaque DOS	3,8687	0,6652
17	98	attaque DOS	7,8687	0,4365
5	100	attaque DOS	9,8687	0,3535
12	150	attaque DOS	59,8687	0,0018

Moyenne	48,75
Ecart type	41,3813
Moy-σ	7,3687
Moy+σ	90,1313

Table3-3 Tableau représentant les taux de confiance finale lorsque Diff>1

- Ce tableau est un élément représentatif des valeurs dans une période donnée :
    - Dans la 1ére colonne on a l'ensemble des nœuds voisins (émetteurs) d'un nœud'j'.
    - 2 éme colonne représente nombres de messages émis pour le nœud 'j'.
    - 3éme colonne détecter le type du nœud, en comparant le nombre de messages (nbmsg) à l'intervalle [**Moy-σ, Moy+σ**].
    - 4éme colonne calculer la différence entre le nombre de messages et les limites inférieures ou supérieures uniquement dans le cas où le nbmsg en dehors de l'intervalle de confiance.
    - 5éme colonne : calculer le taux de confiance à partir des les formules **[3.(4,5,7,8)] ,** attribuer un taux '0.9' aux nœud confiants.

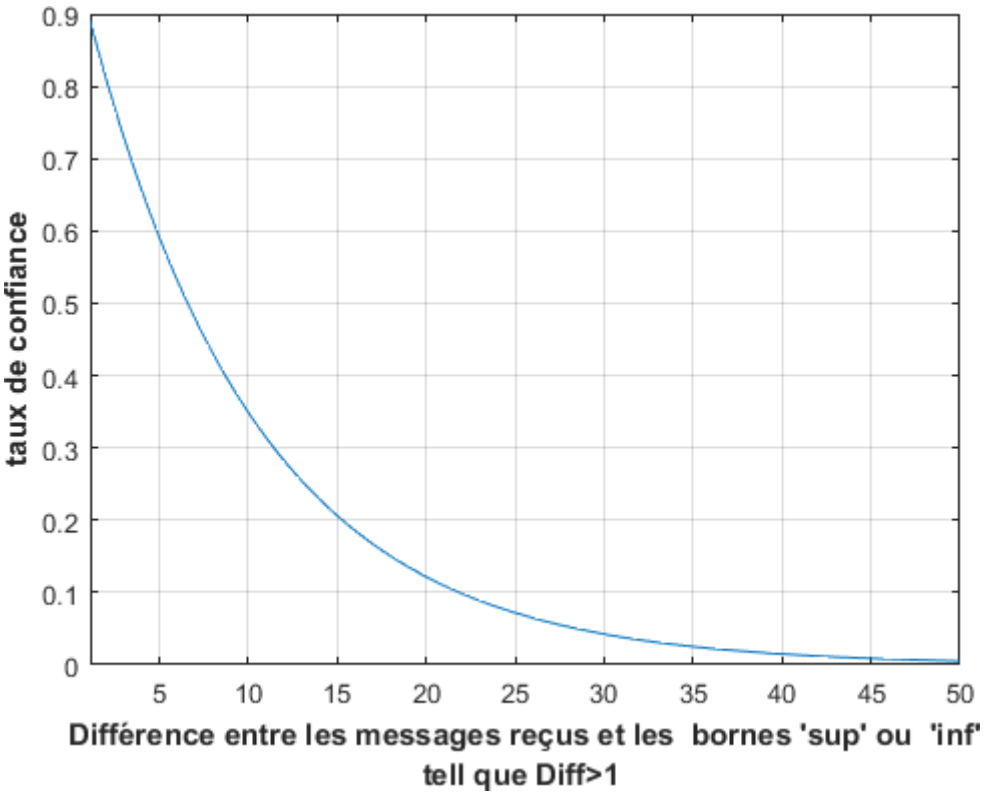


Figure 3-3 Courbe représentant les Taux de confiance en fonction de la différence entre les messages reçus et les bornes 'sup' ou 'inf'.

Dans ce graphe de la figure 3-3 , nous avons représenté en courbe le taux de confiance en fonction de la différence entre les messages reçus et les bornes inférieures et supérieures lorsqu'elle est >1. A partir du graphe nous pouvons constater que plus la valeur de Diff augmente, la valeur de confiance diminue jusqu'à ce qu'il tend vers 0. En effet, lorsque la différence entre le nombre de messages reçus par rapport à la limite inférieure ou supérieure est importante, cela signifie que le nœud est soit égoïste ou il effectue des attaque Dos, par conséquent la pénalité doit être importante également en diminuant sa valeur de confiance.

3.7.1.2 Valeurs de confiance des nœuds lorsque Diff1et Diff2≤1

DIFF1/2	Calcule du taux de confiance
0,1	0,8906
0,2	0,8812
0,3	0,8720
0,4	0,8629
0,5	0,8538
0,6	0,8449
0,7	0,8360
0,8	0,8272
0,9	0,8186
1	0,8100

Table3-4 Tableau représentant les taux de confiance finale lorsque Diff≤1

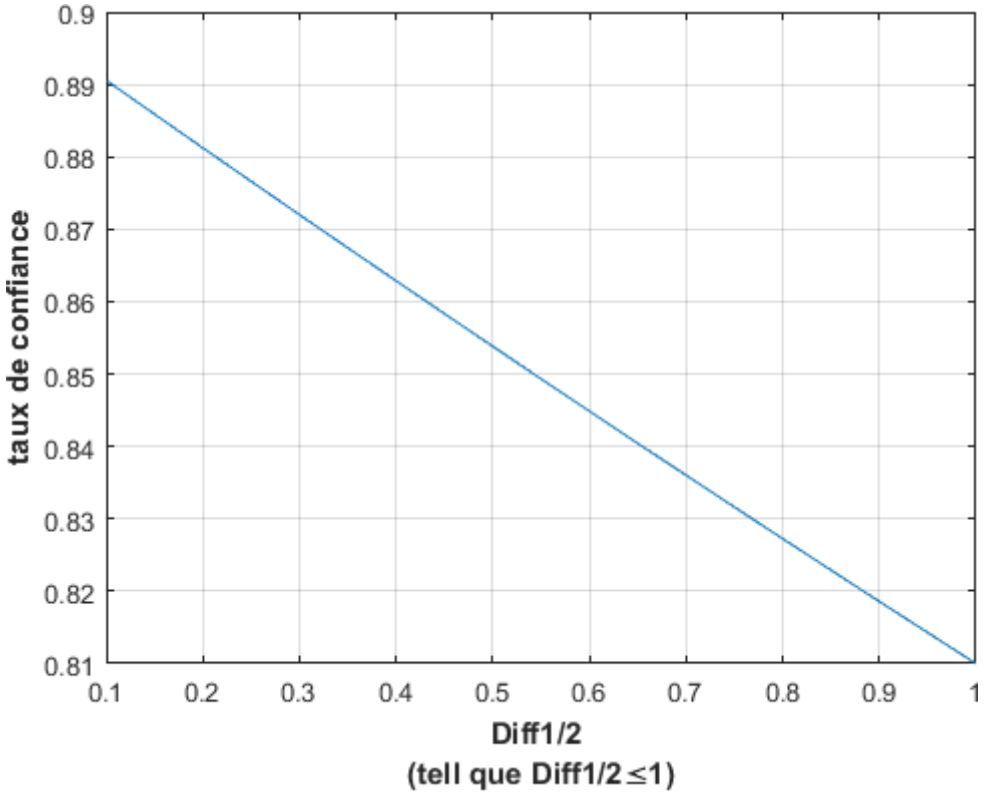


Figure 3-4 graphe représentant les valeurs des taux de confiance quand Diff≤1

Le graphe de la figue3-4 représente le taux de confiance en fonction de la différence entre les messages reçus et les bornes inférieures et supérieures. Nous pouvons remarquer que notre courbe est linéaire et les valeurs de confiance diminuent avec un taux de 0.1. En effet, lorsque Diff c'est à dire que la différence entre le nombre de messages reçus et la limite inférieur ou supérieur exigé par l'algorithme (ou) est très petite. Par conséquent la pénalité ne doit pas être importante.

3.7.2 Analyse de la fonction du temps d'isolement

- Dans les graphes des figures3-(5,6,7), nous avons représenté le taux de confiance finale par rapport au temps d'isolement où chaque graphe correspond à un intervalle d'état de confiance.
- Dans chaque graphe, nous avons représenté 4 droites simultanément qui correspondent aux quatre valeurs de 'k' qui varie de 1 à 4, car un nœud a au maximum quatre chances pour réintégrer le réseau après son isolement.

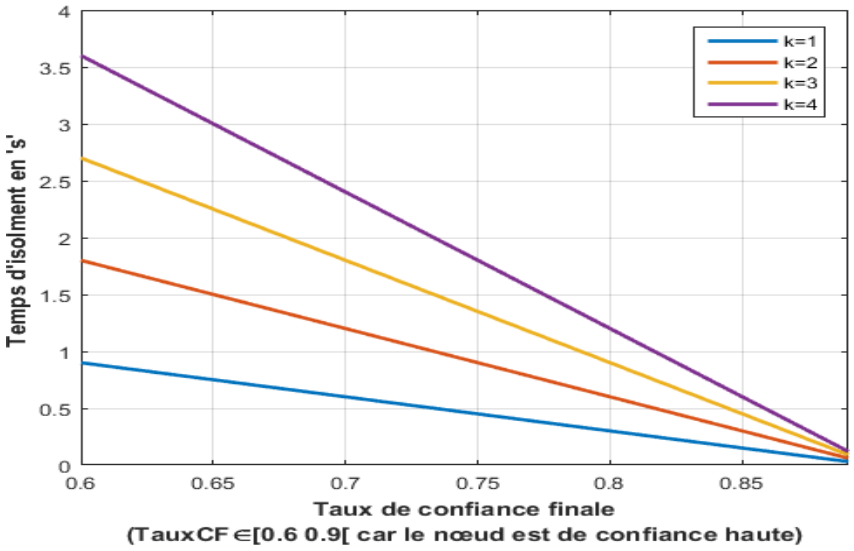


Figure 3-5 Représentation du temps d'isolement en fonction du taux de confiance ainsi du paramètre « k », ou TauxCF∈ [0.6 0.9[.

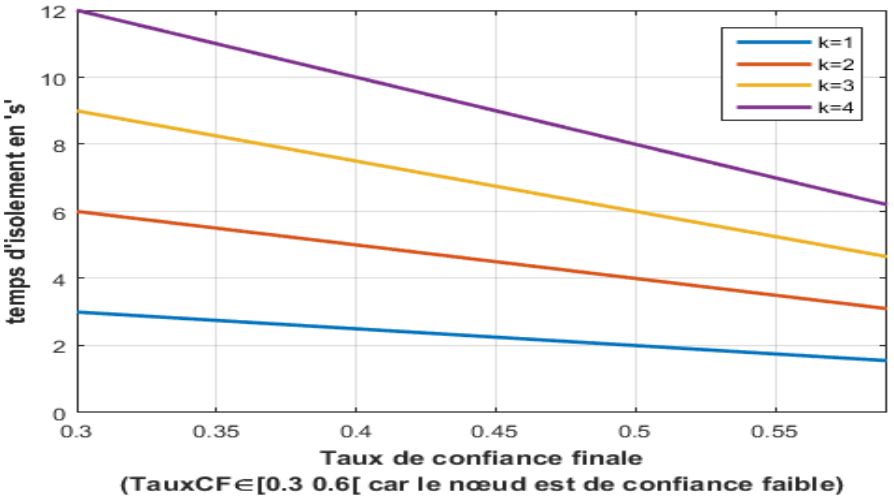


Figure 3-6 Représentation du temps d'isolement en fonction du taux de confiance ainsi du paramètre « k », ou TauxCF [0.3 0.6[.

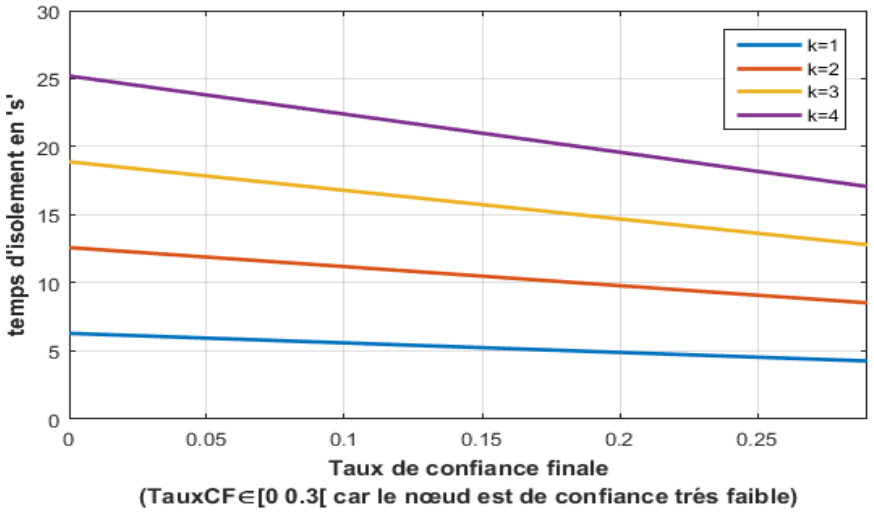


Figure 3-7 Représentation du temps d'isolement en fonction du taux de confiance ainsi du paramètre « k », ou TauxCF [0 0.3[.

- Dans l'ensemble, nous constatons à première vue que le taux de confiance est inversement proportionnel au temps d'isolement (plus le taux de confiance augmente plus le temps d'isolement diminue).
- Aussi, nous remarquons : tant que les intervalles de confiance dont les éléments sont petits, Les droites décroit lentement, ce qui veut dire si les taux de confiance composants l'intervalle sont moins importants, le temps d'isolement décroît moins vite.
- Dans le même graphe, nous constatons aussi, plus le 'k' augmente la pente des droites représentatifs augmente, l'augmentation est plus visible dans le 1er graphe (cas ou l'intervalle de confiance est important).

Conclusion

Dans ce chapitre, nous avons élaboré notre approche dont l'objectif est de détecter les véhicules malveillants et de calculer les confiances des voisins. Dans la suite de notre travail, nous avons introduit un mécanisme qui permet d'isoler les nœuds malintentionnés de façon temporaire. En effet, ce mécanisme permet ainsi d'inciter les nœuds du réseau à améliorer leur comportement en leur offrant plusieurs chances. Si au bout d'un certain nombre de tentatives, les nœuds montrent toujours des comportements malveillants, ils seront définitivement exclus du réseau. L'analyse théorique effectuée a montré que l'approche que nous avons proposé permet de contrer le comportement égoïste des véhicules et de détecter les attaques de type DOS tout en incitant les véhicules à montrer un bon comportement dans le réseau.

Conclusion générale et perspectives

Les attaques dans le réseau VANET sont un danger primordial qu'il faut absolument détecter. Elles menacent la vie privée des conducteurs et des passagers et peuvent causer des accidents et de la congestion sur la route. Il est donc très important de mettre en œuvre des protocoles et des mécanismes de sécurité pour contrôler les entités du réseau afin de préserver la sécurité des conducteurs et des passagers, ainsi que des véhicules.

L'attaque DOS et les comportements égoïstes sur le réseau VANET sont des sujets de recherche en plein essor dans de nombreux travaux, mais ils restent jusqu'à présents sans solution définitive.

Dans ce mémoire, nous avons présenté deux mécanismes de détection et de sanction utilisée pour punir les nœuds malveillants tout en motivant les nœuds égoïstes à coopérer.

La première technique consiste à détecter les nœuds malveillants, ainsi attribuer un taux de confiance pour chaque voisin.

La deuxième technique proposé pour l'isolement des nœuds malveillants pour un lapse de temps selon leur taux de confiance et autant de fois détecter malveillant, et après l'écoulement il sera réintégrer pour un nombre d'itération limité, dans l'autre cas il sera exclu définitivement.

Une partie est consacré à l'analyse théorique de notre approche par illustration de graphe qui montre son efficacité en stimulant les nœuds malveillants à présenter un bon comportement ainsi inciter les nœuds égoïstes à coopérer.

Afin d'étudier l'approche proposée dans ce mémoire, le déploiement sur le terrain n'est malheureusement pas envisageable à ce jour, d'où le recours à la simulation, que nous prévoyons de réaliser par nos soins dans l'avenir proche.

Ainsi nous prévoyons de réduire les frais généraux de reconnaissance de l'approche proposée sans affecter ses performances. Ainsi, ce type de modèle pourrait être adapté pour prédire d'autres types d'attaques existantes telle l'attaque DDOS.

Référence bibliographique

[1] Vishal Kumar1, Shailendra Mishra1, Narottam Chand2. Applications of VANETs: Present & Future .

[2] Jean-Pierre Hubaux, Srdjan Capkun, and Jun Luo. The security and privacyof smart vehicles. Security & Privacy, IEEE, 2(3):49{55, 2004.

[3] Mohamed Nidhal Mejri, Jalel Ben-Othman, and Mohamed Hamdi. Survey on vanet security challenges and possible cryptographic solutions. Vehicular Communications, 1(2):53{66, 2014.

[4] Farhan Aadil1, Shahzad Rizwan2, Adeel Akram3 Vehicular Ad Hoc Networks (VANETs), Past Present and Future: A survey, January 2013

[5] WALID BOUKSANI (2017) . GESTION DE LA PROTECTION DE LA VIE PRIVÉE DANS LES RESEAUX VEHICULAIRES (VANET) . MÉMOIRE PRÉSENTÉ À L'UNIVERSITÉ DU QUÉBEC À TROIS-RIVIÈRES.

[6] Muhammad Rizwan Ghori et al 2018 J. Phys. VANET Routing Protocols: Review, Implementation and Analysis: Conf. Ser. 1049 012064.

[7] Ayoub Benchabana , Ramla Bensaci "Analysis of Routing Protocols in VANETs" Thèse de Master, Université Kasdi Merbah-Ouargla (2014).

[8] Saleem-ullah, Dost Muhammad Khan, Aqeel ur Rehman, M. Abubakar Siddique, Abbas Khan: AN EFFECTIVE MODELING TO MINIMIZE THE TRANSMISSION TIME IN VANET BY REDUCING ROUTING OVERHEAD. AN EFFECTIVE MODELING TO MINIMIZE THE TRANSMISSION TIME IN VANET BY REDUCING ROUTING OVERHEAD

[9] Irshad Ahmed Sumra*, Halabi Bin Hasbullah*, Jamalul-lail Ab Manan**, Iftikhar Ahmad*, ***Daniyal M Alghazzawi « Classification of Attacks in Vehicular Ad hoc Network (VANET) »Department of Computer and Information Sciences, Universiti Teknologi PETRONAS, Bandar Seri Iskandar, 31750 Tronoh, Perak, Malaysia

[10] Mahdi Bounouni ,Louiza Bouallouche-Medjkoune :Acknowledgment-based punishment and stimulation scheme for mobile ad hoc network", Springer Science+Business Media, LLC, dans le cadre de Springer Nature 2018.

[11] Mohammad Saeed Al-kahtani, Survey on Security Attack in Vehicular Ad-hoc Networks, 6e conférence internationale sur le traitement du signal et les systèmes de communication, décembre 2012.

[12] K. Moghraoui, "Gestion de l'anonymat des communications dans les réseaux véhiculaires Ad hoc sans fil (VANETs)," Université du Québec à Trois-Rivières, 2015.

[13] J. Douceur, "The sybil Attack", Premier atelier international sur le système peer to peer (P2P), mars 2002, pp:251-260.

[14] Sumra. I.A, Manan. J.b, Hasbullah. H.B, Timing Attack in Vehicular Network, *Recent Researches in Computer Science,* WSEAS Greece, 14-17 juillet 2011. ISBN : 978-1- 61804- 019-0.

[15] Sumra, Irshad Ahmed ; Ahmad, Iftikhar ; Hasbullah, Halabi ; bin Ab Manan, Jamalul- lail , Behavior of attacker and some new possible attacks in Vehicular Ad hoc Network (VANET), *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT),* 2011 3rd International Congress on , vol., no., pp.1-8, 5-7 Oct. 2011.

[16] M. Raya, J. Pierre, Hubaux, "Securing vehicular ad hoc Networks" Journal of Computer Security,vol.15, janvier 2007, pp39-68.

[17] I.Ahmed Soomro, H.B. Hasbullah, J.lb.Ab Manan, "Déni de service

(DOS) Attack and Its Possible Solutions in VANET", WASET numéro 65, avril 2010 ISSN 2070-3724.

[18] B. Parno et A. Perrig, "Challenges in Securing Vehicular Networks,", Hot Topics in Networks (HotNets-IV), 2005.

[19] Zeadally. Sh, Hunt. R, Chen. Y-Sh, Irwin. A, Hassan. A, Réseaux ad hoc de véhicules (VANETS) : Status, Results, and Challenges ,*Telecommunication Systems* (9 décembre 2010), pp. 1-25.

[20] Sun.J, Fang.Y, A defense technique against misbehavior in VANETs based on threshold authentication, *Military Communications Conference,* 2008. MILCOM 2008. IEEE Issue Date: 16-19 Nov. 2008,Location : San Diego, CA.

[21] Gandhi, Usha & Keerthana, R.V.S.M. (2014). Request Response Detection Algorithm for detecting DoS attack in VANET. 192-194. 10.1109/ICROIT.2014.6798334.

[22] Karan Verma . Halabi Hasbullah - Ashok Kumar, "Prévention of DoS Attacks in VANET" publié dans Springer Science livraison, Business Media New York 2013.

[23] Abdul Quyoom, Raja Ali , DevkiNandan Gouttam et Harish Sharma", un nouveau mécanisme de détection du déni de service Attaque (DoS) dans VANET utilisant un paquet malveillant et non pertinent Detection Algorithm (MIPDA)" dans Conférence internationale sur Informatique, communication et automatisation (ICCCA2015).

[24] Aditya Sinha&Santosh K. Mishra, "Algorithme de limitation des files d'attente (QLA) pour la protection de VANET contre le déni de service (DoS) Attaque" publiée dans l'International Journal of Computer Demandes (0975 - 8887) Volume 86 - n° 8, janvier 2014

[25] Amarpreet Singh, D. Priya Sharma, "Un nouveau mécanisme pour détection d'une attaque DOS dans VANET à l'aide de l'outil Enhanced Attacked Packet Detection Algorithm", dans Conférence internationale RAECS UIET Université de Panjab Chandigarh 21-22 décembre,2015978-1-4673-8253-3/15/ IEEE, 2015, p. 850-855.

[26] Survey on VANET security challenges and possible cryptographic solutions MN Mejri, J Ben-Othman, M Hamdi - Vehicular Communications, 2014

[27] Christian TCHEPNDA, "Authentication dans les Réseaux Véhiculaires Opérés", Thèse de Doctorat, École Nationale Supérieure des Télécommunications, Spécialité: informatique et Réseaux, 18 décembre 2008, Paris- France.

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