N°d'ordre: .....

République Algerienne Démocratique et Populaire
Ministère de l'enseignement supérieur et de la Recherche scientifique

Université Djillali Liabès de Sidi Bel Abbès
Faculté des Sciences Exactes
Département d'informatique
Laboratoire EEDIS

Thèse de Doctorat

Filière : Informatique
Spécialité : Réseaux et sécurité de l'information

Par

Mme BENSAID Chaimaa

GESTION DES CERTIFICATS DANS LES RESEAUX VEHICULAIRES

Soutenue le 19-02- 2020 devant le jury :

Pr.	FERAOUN kamel Mohamed	UDL SBA	Président du jury
Dr.	ALI CHERIF Moussa	UDL SBA	Examinateur
Dr.	KESKES Nabil	ESI SBA	Examinateur
Dr.	BOUKLI HACENE Sofiane	UDL SBA	Directeur de thèse

Année Universitaire : 2019 - 2020

A Mes Parents. . .

Remerciements

Je remercie en priorité dieu le tout puissant de m'avoir donné le courage, la force et la volonté d'accomplir ce travail.

Je voudrais aussi remercier mon encadrant Mr BOUKLI HACENE Sofiane de m'avoir appris à développer jusqu'au bout mes idées. Pour les encouragements et pour l'intérêt qu'il m'a apportée dans l'accomplissement de ce projet

Table des matières

Table des matières **iv**

Liste des figures **vi**

Liste des tableaux **vii**

Préface **1**

1 Introduction aux Réseaux véhiculaires **3**
- 1.1 Introduction dans les réseaux sans fil . . . 4
- 1.2 les réseaux sans fil. . . . 4
- 1.3 Les environnements mobiles. . . . 5
  - 1.3.1 Les réseaux cellulaires. . . . 5
  - 1.3.2 Les réseaux AD HOC. . . . 6
- 1.4 Les réseaux véhiculaire (VANET). . . . 6
  - 1.4.1 Définition. . . . 6
  - 1.4.2 Applications des réseaux VANET . . . 7
  - 1.4.3 Entités de communication . . . 8
  - 1.4.4 Architectures de communication . . . 9
  - 1.4.5 caractéristiques des VANETs . . . 10
  - 1.4.6 Les modèles de propagation pour les VANET . . . 11
  - 1.4.7 Normes et Standardisations . . . 12
  - 1.4.8 Problèmes liée aux VANETs . . . 12
- 1.5 conclusion . . . 13

2 Le Routage dans les réseaux véhiculaires **15**
- 2.1 Introduction au routage . . . 16
- 2.2 La difficulté du routage dans les réseaux VANET . . . 16
- 2.3 Classification des protocoles de routage dans les réseaux mobiles Ad Hoc . . . 16
  - 2.3.1 Classification selon l'architecture . . . 17
  - 2.3.2 Classification selon L'approche de routage . . . 17
  - 2.3.3 Classification selon L'algorithme utilisé . . . 18
- 2.4 Le routage dans les réseaux VANET . . . 19
  - 2.4.1 Les protocoles de routage basés sur la topologie . . . 20
  - 2.4.2 Les protocoles de routage basés sur la géographie . . . 20
- 2.5 Les protocoles de routage employés dans notre étude . 22
  - 2.5.1 Le protocole de routage AODV . . . 22
  - 2.5.2 Le Protocole de routage OLSR . . . 26
- 2.6 Conclusion . . . 26

3 La sécurité et QOS dans les réseaux sans fil 28
3.1 Introduction . . . 29
3.2 La sécurité . . . 30
3.2.1 Qu'est ce que la sécurité . . . 30
3.2.2 Objectifs de la sécurité . . . 30
3.2.3 La cryptographie . . . 32
3.3 PKI (Public Key Infrastructure) . . . 34
3.3.1 Définition du PKI . . . 35
3.4 Les attaques contre les réseaux AD HOC . . . 39
3.4.1 Classification des attaques . . . 39
3.4.2 Présentation de quelques attaques . . . 39
3.5 Vulnérabilité des réseaux véhiculaires . . . 40
3.6 Attaques spécifiques sur les VANETs . . . 40
3.6.1 L'injection des messages erronés : . . . 41
3.6.2 Le déni de service : . . . 41
3.6.3 La révélation d'identité et de position géographique des autres véhicules . . . 41
3.7 La qualité de service . . . 41
3.7.1 Niveaux de service . . . 42
3.7.2 Critères ou paramètres de qualité de service . . . 42
3.8 Conclusion . . . 44

4 Détection et prévention des attaques blackholes dans les réseaux véhiculaires 45
4.1 inroduction . . . 46
4.2 Attaques contre le protocole AODV . . . 46
4.3 blackhole attack (problématique) . . . 47
4.4 état de l'art . . . 48
4.5 Nos propositions de détection et préventions des blackholes dans les VANETs . . . 51
4.5.1 Détection à base de temps de latence . . . 51
4.5.2 Détection à base de l'étude de comportement de chaque noeud . . . 52
4.6 Les performances réseau . . . 54
4.7 Les résultats de simulation . . . 54
4.7.1 Approches implémentés . . . 54
4.7.2 Les résultats de simulation . . . 55
4.8 Conclusion . . . 57

5 Gestion des certificats dans les réseaux véhiculaires 58
5.1 introduction . . . 59
5.2 Distribution partielle des autorités de certification . . . 59
5.3 Les chaines de certificats . . . 61
5.4 Chainage de certificats basé sur les clusters . . . 62
5.4.1 L'accord des certificats . . . 62
5.4.2 Renouvellement des certificats . . . 63
5.4.3 Notre proposition . . . 64
5.4.4 calcule de valeur de confiance . . . 64
5.4.5 clustering . . . 65
5.4.6 Certification . . . 65

5.4.7 Transfert du certificat 66
5.4.8 Renouvellement du certificat et révocation du certificat . 66
5.5 Les résultats de simulation 67
5.5.1 le scenario le la ville de Malaga 68
5.5.2 scenarios de VANETmobisim 69
5.6 Conclusion 73

Conclusion générale **74**

Bibliographie **77**

Notations **83**

Liste des figures

1.1 Le modèle des réseaux mobiles avec infrastructure. 5
1.2 Les éléments constituant le véhicule intelligent. 7
1.3 Applications des réseaux de véhicules. 8
1.4 Les modèles de communication dans les réseaux de véhicules. 10

2.1 les protocoles de routage dans les réseaux de véhicules. . . 20
2.2 format d'un paquet RREQ 23
2.3 format d'un paquet RREP 24
2.4 Découverte de route. 25
2.5 Réparation des chemins. 25

3.1 Objectifs de la sécurité. 30
3.2 Cryptographies symétrique. 32
3.3 Cryptographie asymétrique – confidentialité 33
3.4 Cryptographies asymétrique – authentification 33
3.5 structure de certificat X509v3 35
3.6 Déroulement d'un sysème PKI 36

4.1 l'attaque blackhole 47
4.2 Diagramme de détection de blackhole 53
4.3 l'effet de PDR 55
4.4 Les coûts additifs 56
4.5 La moyenne de temps de latence des paquets de données VS nombre de véhicules 56
4.6 Les paquets Perdues VS nombre de véhicules 57

5.1 Gestion des clés K/k configuration 60
5.2 Graphe de certificat et chemin de certificats entre le noeud u et v et le mélange de référentiel de certificats 62
5.3 Délivrance du certificat 63
5.4 Certficate generation 67

5.5 Le renouvellement des certificats 67
5.6 carte géographique de la zone utilisé 68
5.7 Le nombre de certificat 70
5.8 Fraction de livraison de paquets 71
5.9 paquets supprimés 71
5.10 les coût additifs 72
5.11 Le délai de communication de bout en bout 72

Liste des tableaux

4.1 paramètres de simulation. 55

5.1 dètail de la zone géographique utilisé 68
5.2 paramètres de simulation 69
5.3 paramètres de simulation 69

Introduction Générale

Les réseaux sans fil et les réseaux mobiles sont devenus très populaires ces dernières années. Ceci est du à leurs caractéristiques : Installation simple et facile,absence de câblage, les coûts de matériel ne sont pas prohibitifs, les utilisateurs se déplacent librement au sein de la zone de couverture du réseau. Donc ils peuvent être mis en place facilement et économiquement selon les besoins. Ils offrent en effet un large éventail d'applications, notamment dans les situations géographiques avec des contraintes terrestres telles que les champs de bataille, les applications militaires, et d'autres situations d'urgence et de catastrophe..

Parmi ces réseaux on trouve : les réseaux locaux sans fil, les réseaux de capteurs, les réseaux ad hoc et les réseaux VANETs (Vehicular ad hoc NETworks). Dans ce dernier type chaque noeud mobile est un véhicule intelligent équipé de moyen de communication (capteur).

La gestion de l'acheminement de données ou le routage, consiste à assurer une stratégie qui garantie, à n'importe quel moment, la connexion entre n'importe quelle paire de noeuds appartenant au réseau. La stratégie de routage doit prendre en considération les changements de la topologie ainsi que les autres caractéristiques du réseau VANET (bande passante, nombre de liens, ressources du réseau. . .etc.). En outre, Plusieurs protocoles de routage pour les réseaux ad hoc ont été développés. Chaque protocole essaye de maximiser les performances du réseau en minimisant le délai de livraison des paquets, l'utilisation de la bande passante et la consommation d'énergie. Les algorithmes de routage pour les réseaux ad hoc peuvent se classer en deux catégories, les protocoles de localisation,et les protocoles géographiques.

Cependant le grand problème de ces réseaux est la sécurité, les travaux de recherche indique que les réseaux sans fil sont plus vulnérables que les réseaux filaires en raison de leurs caractéristiques tels que le milieu ouvert, la topologie dynamique, l'absence d'administration centrale, la coopération distribuée, et la capacité restreinte (en termes de puissance et de calcul). L'utilisation de liaisons sans fil rend ces réseaux plus sujets à des menaces de sécurité physiques que les réseaux câblés, allant de l'écoute passive à l'interférence active. Sans aucune sécurité adéquate, les hôtes mobiles sont facilement capturés, compromis et détournés par des noeuds malveillants. L'adversaire peut écouter et/ou modifier les messages dans le canal de communication, injecter des messages erronés, supprimer des messages, et même passer par d'autres noeuds. Par conséquent, les mécanismes de sécurité dans de tels réseaux sont essentiels pour protéger les

données émises par les utilisateurs.

La sécurité d'un réseau VANET peut être réalisée à différents niveaux de la couche protocolaire (Application, MAC, Routage, Physique) et sans une certaine forme de sécurité au niveau de l'une de ces couches, un réseau VANET est vulnérable à plusieurs types d'attaques. Il est sans doute assez facile d'écouter le trafic, de rejouer les transmissions, de manipuler les en-tètes de paquets ou de rediriger les messages de routage. La plus part des protocoles de routage existant permettent l'acheminement efficace des données cependant l'aspect sécurité est négligé ce qui leur rend aussi vulnérables aux attaques menaçant la fiabilité des données en circulation, la question qui s'impose maintenant n'est plus la recherche de la route optimale mais la recherche du chemin le plus sécurisé.

En effet,Cette thèse présente d'une part une étude sur les propositions des améliorations sur le protocole de routage AODV dans les VANETs pour détecter l'attaque blackhole et améliorer la qualité de service dans les réseaux véhiculaires et d'autre part offre une amélioration d'une proposition de chaînage de certificats basé sur les clusters en ajoutant une méthode pour remédier aux problèmes de la disponibilité, le renouvellement et la révocation des certificats .

Le premier chapitre présente les réseaux mobiles.

Le deuxième chapitre présente le routage dans les réseaux véhiculaire

Le troisième chapitre exposons la sécurité dans le réseau sans fil, leurs objectifs et différentes techniques pour maintenir la sécurité

Le quatrième chapitre présente l'ensemble des solutions proposées pour détecter les attaques blackholes dans le réseau VANET ainsi notre proposition

Le cinquième chapitre présente l'ensemble des solutions proposées par les différentes équipes de recherche travaillant sur la gestion de certificats ainsi notre approche.

En fin nous terminons notre mémoire avec une conclusion et des perspectives.

Introduction aux Réseaux véhiculaires

1

Sommaire

1.1 Introduction dans les réseaux sans fil 4
1.2 les réseaux sans fil. 4
1.3 Les environnements mobiles. 5
1.3.1 Les réseaux cellulaires. 5
1.3.2 Les réseaux AD HOC. 6
1.4 Les réseaux véhiculaire (VANET). 6
1.4.1 Définition. 6
1.4.2 Applications des réseaux VANET 7
1.4.3 Entités de communication 8
1.4.4 Architectures de communication 9
1.4.5 caractéristiques des VANETs 10
1.4.6 Les modèles de propagation pour les VANET 11
1.4.7 Normes et Standardisations 12
1.4.8 Problèmes liée aux VANETs 12
1.5 conclusion 13

1.1 Introduction dans les réseaux sans fil

L'évolution récente de la technologie dans le domaine de la communication sans-fil poussent aujourd'hui les chercheurs à faire des efforts afin de réaliser le but des réseaux : "L'accès à l'information n'importe o'u et n'importe quand"

Le concept des réseaux mobiles ad hoc essaie d'étendre les notions de la mobilité à toutes les composantes de l'environnement. Ici, contrairement aux réseaux basés sur la communication cellulaire, aucune administration centralisée n'est disponible, ce sont les hôtes mobiles elles-mêmes qui forment, d'une manière ad hoc, une infrastructure du réseau. Aucune supposition ou limitation n'est faite sur la taille du réseau ad hoc, le réseau peut contenir des centaines ou des milliers d'unités mobiles.

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 les réseaux ad hoc de manière générale, puis, nous abordons aux réseaux VANET, les différents types de services offerts par ces réseaux et les modes de communication existants ; enfin nous décrivons les différentes caractéristiques des réseaux VANETs.

1.2 les réseaux sans fil.

Un réseau sans fils (en anglais wireless network) est, comme son nom l'indique, un réseau dans lequel au moins deux terminaux peuvent communiquer sans liaison filaire. Grâce aux réseaux sans fils, un utilisateur à la possibilité de rester connecté tout en se déplaçant dans un périmètre géographique plus ou moins étendu. Le développement constant de ces réseaux sans fil a amené la création de nouvelles normes afin de mieux interconnecter les machines [BURGODC 2007], .

On peut aussi définir un réseau sans fils comme un réseau dans lequel les différents éléments participants (ordinateur portable, PDA, téléphone portable . . .etc.) ne sont pas raccordés entre eux par un média physique. La transmission des données se fait via les ondes hertziennes (radio ou infrarouge). Ceci permet aux utilisateurs de se déplacer dans un périmètre de couverture pouvant aller d'une dizaine de mètres à quelques kilomètres [BACCOUR 2005]

1.3 Les environnements mobiles.

Un environnement mobile est un système composé de sites mobiles et qui permet à ses utilisateurs d'accéder à l'information indépendamment de leurs positions géographiques Les réseaux mobiles ou sans fil, peuvent être classés en deux classes : les réseaux avec infrastructure et les réseaux sans infrastructure. [BURGODC 2007]

1.3.1 Les réseaux cellulaires.

Ce mode de fonctionnement est très semblable au protocole Ethernet des réseaux filaires. Les machines se connectent à un point d'accès (AP), appelé aussi station de base, qui partage la bande passante disponible. Les stations de base sont munies d'une interface de communication sans fil avec les sites mobiles qui se trouvent dans sa zone géographique ou sa couverture radio. Dans le mode infrastructure, le modèle de système est composé de deux ensembles d'entités distinctes[WU *et al.* 2007] :

— les "sites fixes" d'un réseau de communication filaire classique (Wireless network),
— les "sites mobiles" (Wireless network).

Les sites fixes, appelés stations de base BSS (Basic Service Set) sont munis d'une interface de communication sans fil pour la communication directe avec les sites ou unités mobiles (UM), localisés dans une zone géographique limitée, appelée cellule (voir figure 1.1). A chaque station de base correspond une cellule à partir de laquelle des unités mobiles peuvent émettre et recevoir des messages. Les sites fixes sont interconnectés entre eux à travers un réseau de communication filaire, généralement fiable et d'un débit élevé. Les liaisons sans fil ont une bande passante limitée qui réduit sévèrement le volume des informations échangées. Dans ce modèle, une unité mobile ne peut être, à un instant donné, directement connectée qu'à une seule station de base. Elle peut communiquer avec les autres sites à travers la station à laquelle elle est directement rattachée [HAGGAR 2007].

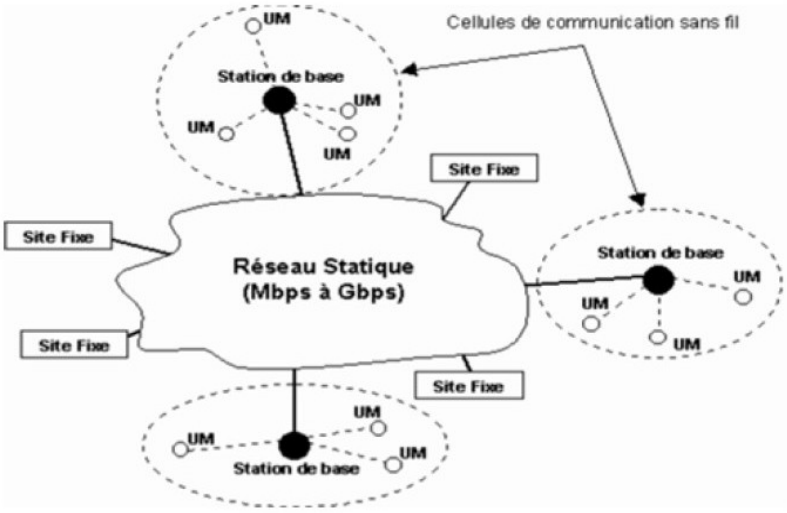

Figure 1.1 – *Le modèle des réseaux mobiles avec infrastructure.*

1.3.2 Les réseaux AD HOC.

Un réseau mobile Ad Hoc 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 (onde radio), sans l'aide d'une infrastructure préexistante ou administration centralisée [BACCOUR 2005] . Ce mode n'a pas besoin de point d'accés pour fonctionner, ce sont les stations elles mêmes qui entrent en communication sans s'appuyer sur un équipement extérieur.Tous les noeuds d'un réseau de ce type se comportent comme des routeurs et prennent part à la découverte et à la maintenance des chemins de communication entre les différentes machines. Ce type de réseau s'organise lui-même.Ce sont des réseaux qui s'organisent automatiquement de façon à être déployé rapidement, sans infrastructure fixe, et qui doivent pouvoir s'adapter aux conditions de propagation [DAOUD 2005]

1.4 Les réseaux véhiculaire (VANET).

1.4.1 Définition.

Un réseau VANET est une particularité des réseaux MANET ou les noeuds mobiles sont des véhicules intelligents équipés de moyens de communication(Capteur) (voir figure 1.2). Comme tout autre réseau Ad hoc,les véhicules peuvent communiquer entre eux ou avec des stations de base placées tout au long des routes. Ils permettent d'établir des communications entre véhicules ou bien avec une infrastructure située aux bords de routes. Par rapport à un réseau ad hoc classique,les réseaux VANET sont caractérisés par une forte mobilité des noeuds rendant la topologie du réseau fortement dynamique [BURMESTER *et al.* 2008]

Les noeuds dans un réseau VANET sont des véhicules intelligents équipés de calculateurs, capteurs et cartes réseaux capable de collecter, traiter et échanger des informations entre eux [PAUL *et al.* 2012].

Pour la mise en place d'un tel réseau, certains équipements électroniques doivent être installés au sein de véhicules, tel :les dispositifs de perception de l'environnement (radars, caméras), un système de localisation GPS, et bien sur une plateforme de traitement. Plusieurs technologies peuvent être mises en oeuvre pour l'établissement des communications véhiculaires, tel : les réseaux sans-fil de type 802.11, WIMAX, Bluetooth [CHOI *et al.* 2009] .

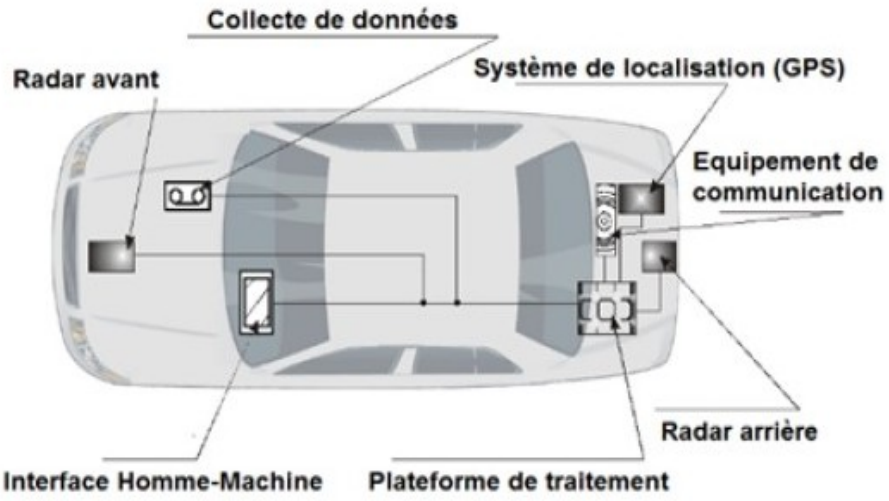

FIGURE 1.2 – *Les éléments constituant le véhicule intelligent.*

1.4.2 Applications des réseaux VANET

On peut donc distinguer deux types d'applications avec les réseaux de véhicules,les applications de confort et les applications de sécurité routière (voir figure 1.3). Nous décrivons dans les paragraphes suivants quelques applications

Application dans la prévention et la sécurité routière

Ces services concernent les applications ayant un impact direct sur la sécurité des personnes et des biens, c'est à dire les applications qui permettent de réduire le nombre des accidents routiers et d'améliorer les conditions de circulation. Les services liés à la sécurité routière se basent sur la détection de l'environnement proche au moyen de capteurs installés au niveau des véhicules ou bien au centre de contrôle, ainsi que la diffusion de messages d'alerte fournissant des informations sur l'état du réseau routier (trafic, travaux, météo) ou rappelant au conducteur (les limitations de vitesse, les distances de sécurité. .). Les messages d'alertes et de sécurité doivent être de taille réduite pour être transmis le plus rapidement[CHOI *et al.* 2009]

Application au confort du conducteur et des passagers

Les réseaux VANET ne se contenteront pas seulement à offrir des services liés à la sécurité des véhicules et leurs occupants, mais permettront aussi d'assurer le confort de ces derniers durant leurs voyages, ces services comprennent entre autres :la messagerie instantanée,les jeux en réseau,l'accès à Internet,les paiements automatiques et la diffusion d'informations utiles sur la disponibilité de l'espace de stationnement dans les parkings en indiquant aux conducteurs les espaces libres [XU & JIANG 2003] .

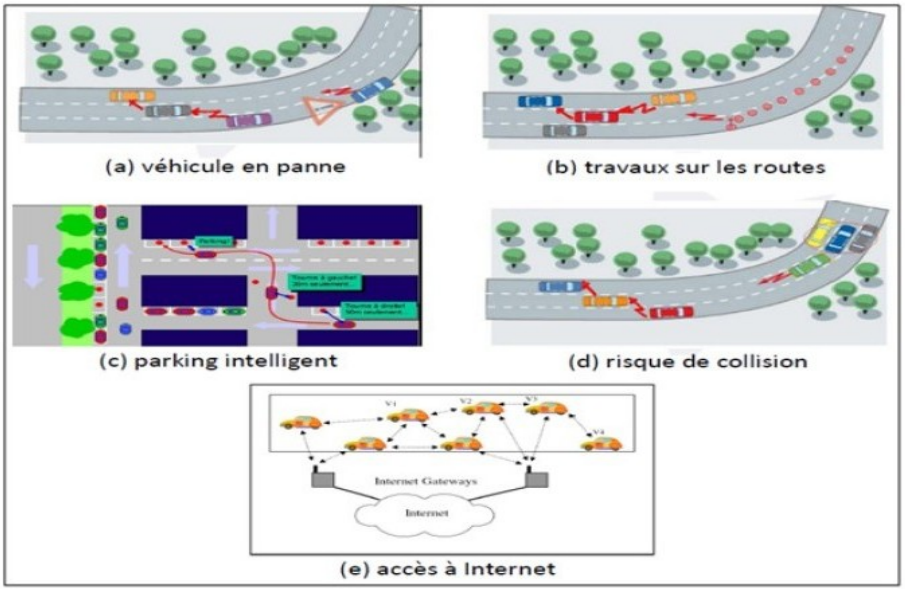

FIGURE 1.3 – *Applications des réseaux de véhicules.*

1.4.3 Entités de communication

Road Side Unit

Les Road Side Unit (RSU) sont des entités situées et installées au bord de la route. Ces entités présentent des points d'accès au réseau et sont déployées tout au long de la route. Chaque RSU a pour objectif de transmettre des messages aux véhicules qui se trouvent dans sa zone radio. Ces messages contiennent des informations sur les conditions météorologiques, ainsi que sur l' état de la route (vitesse maximale,autorisation de dépassement, etc.)[ADETUNJI 2014].

Autorité centrale

L'Autorité Centrale (CA) est 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[ADETUNJI 2014]

On Board Unit

L'On Board Unit (OBU) est une unité embarquée dans les véhicules intelligents. Son rôle est de permettre aux véhicules de se localiser, calculer, enregistrer et envoyer des messages sur une interface réseau à l'aide d'un ensemble de programmes. Dans le réseau VANET, le conducteur ou l' utilisateur peut voir les pseudonymes des véhicules à proximité dans son OBU à l' aide des messages beacon. Ainsi, l'utilisateur peut choisir le véhicule avec lequel il veut communiquer[ADETUNJI 2014].

1.4.4 Architectures de communication

Dans les réseaux véhiculaires, on peut distinguer trois modes de communication,les communications Véhicule-à-Véhicule (V2V), les communications Véhicule-à-Infrastructure (V2I) et les communications Hybrides (voir figure 1.4). Dans cette section, nous présentons le principe et l'utilité de chaque mode :

communication de Véhicule-à-Véhicule (V2V)

Dans cette catégorie, Les réseaux véhiculaires reprennent les mêmes principes architecturaux que les MANETs ou les contraintes d'énergie, de mémoire et de capacité sont relaxées et ou le modèle de mobilitè n'est pas aléatoire mais prévisible avec une très grande mobilité. Cette architecture peut être utilisée dans les applications ou les services liés à la sécurité routière (alerte accident, alerte ralentissement, alerte déviation, alerte travaux, alerte intempéries, aide aux dépassements de véhicules, prévention des sorties de voies en ligne ou en virage,conduite coopérative, ...)[XU & JIANG 2003]. Aucune infrastructure n'est utilisée, aucune installation n'est nécessaire sur les routes et tous les véhicules sont équipés pour communiquer directement entre eux que se soit dans la même zone radio, ou bien par le biais d'un protocole multisauts qui se charge de transmettre les messages de bout en bout en utilisant les noeuds voisins qui les séparent comme des relais[XU & JIANG 2003] .

Les communications V2V sont très efficaces pour le transfert des informations concernant les services liés à la sécurité routière mais tout de même cette approche souffre de certains inconvénients dont nous citons :

- Les délais de communications qui sont élevés (communication multi sauts).
- Les déconnexions fréquentes dues au fait que les véhicules sont mobiles.
- La sécurité du réseau est très limitée.

Communication de Véhicule à Infrastructure (V2I)

Dans cette catégorie, on ne se concentre pas seulement sur des simples systèmes de communications inter véhicules (Inter-Vehicle Communication IVC) mais aussi à ceux qui utilisent des stations de bases ou point d'infrastructure RSU (Road Side Units). Cette approche repose sur le modèle client/serveur o'u les véhicules sont les clients et les stations installées le long de la route sont les serveurs. Ces serveurs sont connectes 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 (par exemple : accès à Internet, échange de données de voiture-à-domicile, communications de voiture-à-garage de réparation pour le diagnostique distant, ...etc) [BURMESTER *et al.* 2008] .

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

communication hybride

La combinaison des deux communications véhicule à véhicule (V2V) avec la communication de véhicule à infrastructure (V2I), 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 [BURMESTER *et al.* 2008] .

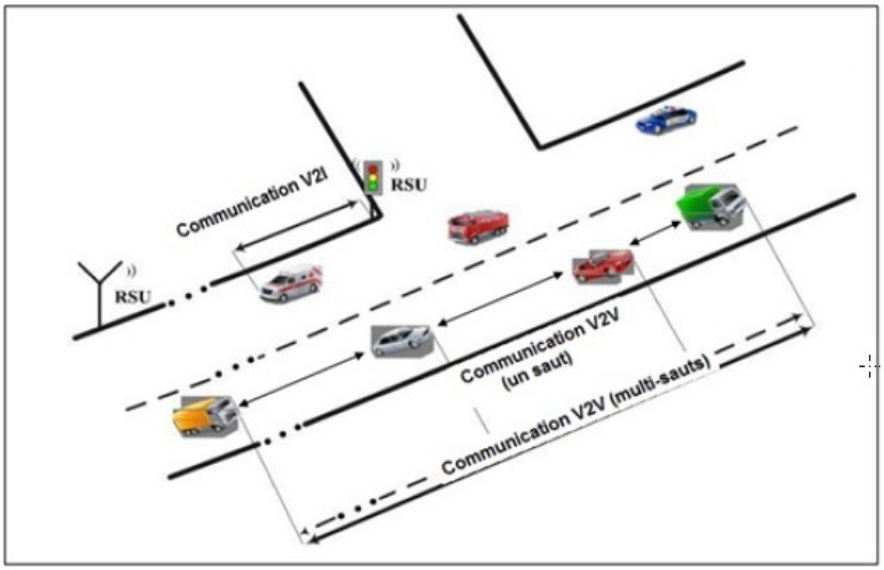

FIGURE 1.4 – *Les modèles de communication dans les réseaux de véhicules.*

1.4.5 caractéristiques des VANETs

Les réseaux véhiculaires ont des caractéristiques spécifiques qui les distinguent des réseaux Ad Hoc. Dans cette partie, nous présentons quelques propriétés et ccontraintes concernant ce type de réseau :

La collecte d'informations et la perception de l'environnement proche

La collecte d'informations se fait en utilisant différents capteurs de toutes catégories (cameras, capteurs de pollution, capteurs de pluies, capteurs de l'état de le route et de voiture) 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 [PATHAC & SHRAWAKER 2009].

La topologie et la connectivité

comme les réseaux ad hoc mobiles, les réseaux VANET sont caractérisés par une connectivité sporadique, car un véhicule (noeud) peut rejoindre ou quitter le réseau en un temps très court, ce qui rend les chan-

gements de topologie très fréquent. De plus, des problèmes peuvent apparaitre quand le système IVC (Inter-Vehicle Communication) n'est pas équipé dans la majorité des véhicules [PATHAC & SHRAWAKER 2009]

La sécurité dans les VANETs

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 , 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 des attaques spécifiques sur les VANETs, et les mécanismes de base qui ont été s mis en oeuvre pour la sécurité de ces réseaux [TCHEPNDA 2008]

— L'injection des messages erronés : dans cette attaque l'entité malveillante crée des messages contenant des informations erronées afin de causer un accident ou de rediriger le trafic routier de manière permettant la libération de la route utilisée [RAYA & HUBAUX 2007]
— Le déni de service l'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 [RAYA & HUBAUX 2007]
— La révélation d'identité et de position géographique des autres véhicules : dans cette attaque, l'entité malveillante collecte des informations sur les transmissions radio effectuées par le véhicule victime afin de surveiller sa trajectoire. L'utilité de cette attaque est diverse et dépend de l'entité collectant ces informations (elle peut ^etre par exemple une entreprise de location de voitures qui veut suivre ses propres véhicules de manière illégitime) [RAYA & HUBAUX 2007]

1.4.6 Les modèles de propagation pour les VANET

d'après [JERBI 2008a] Il existe différents modèles de propagation radio, les plus utilisé sont : le modèle Free Space qui suppose un seul chemin de propagation direct entre les noeuds communicants, le modèle Two-Ray-Ground qui ajoute au chemin direct un autre chemin réfléchi sur le sol, le modèle Shadowing qui ajoute une composante aléatoire à la perte du signal pour modéliser l'influence de l'environnement sur le signal, les modèles de fading Ricean et Rayleigh qui tiennent compte de la propagation à trajets multiples et, le modèle Nakagami qui est un modèle mathématique configurable qui permet de simuler plusieurs types d'environnements.

L'ensemble des modèles « Free Space et Two-Ray Ground » manquent de réalisme, ils supposent un environnement plat non obstrué et modélisent les zones de couverture par des cercles parfaits. Bien que les modèles Shadowing, Ricean, Rayleigh et Nakagami intègrent les obstacles dans la modélisation de la propagation des signaux.

1.4.7 Normes et Standardisations

Pour assurer et faciliter la communication réseau entre les différents produits provenant de différents fabriquant, un grand nombre de règles et des méthodes existent actuellement régissent la communication réseau ; ce sont les normes et standards qui nous permet de simplifier le développement et garantis que les produits fournis par différents fabriquant peuvent fonctionner ensemble. Il existe plusieurs normes et standards qui décrivent la communication inter-véhicule ; parmi eux on cite [JERBI 2008a] :

DSRC

En 2002, et pour assurer la communication inter-vehicules ; l'ASTM (American Society for Testing Materiel) a conçus le premier norme sans fil appelée DSRC (Dedicated Short Range Communication – les communications dédies courte porté) qui est basé sur la couche physique de la norme IEEE 802.11a ainsi sur la couche MAC de la norme IEEE 802.11e [KENNEY 2011]

WAVE et IEEE 802.11p

En 2003, un nouveau standard dédié aux communications enter-vehicules est apparus, c'est le standard WAVE (Wireless Ability in Vehicular Environments) aussi connus sous le nom IEEE 802.11p ; cette norme utilise le concept de multicanaux afin d'assurer les communications pour les applications de sécurité [WAVE 2010]

1.4.8 Problèmes liée aux VANETs

Il existe plusieurs défis qui caractérisent les réseaux véhiculaires que l'on peut résumer en ces points :

Qualité de service

la bonne qualité de service dépend des applications supportées. Ou la principale contrainte des applications est la latence. Pour que les informations ou les messages soient valides et considérés comme pertinents et significatifs, ils doivent arrivés aux destinataires dans des délais très courts [JERBI 2008a].

La sécurité

Dans les réseaux véhiculaires la sécurité pose un grande problème et un défis majeur pour dans la conception architecturale des réseaux et la conception des protocoles de communication. Les services de sécurité se diffèrent selon les fonctions des applications et comprennent en générale défirent mécanismes tel que la confidentialité, l'authenticité, l'intégrité, la non-répudiation, la disponibilité, la cohérence des données. Ces mécanisme et conçus pour détecté, prévenir ou contrer une attaque de

sécurité. La satisfaction de ces exigences dans des systèmes aussi dynamiques et mobiles que les réseaux véhiculaires est difficile mais particulièrement importante ; étant donné que des vies humaines sont concernées [BENCHABANA & BENSACI 2014].

La mobilité

La mobilité dans les réseaux VANETs présente le facteur majeur qui diffère ce dernier par rapport aux réseaux MANETs. Dans les premiers temps ce facteur été négligé mais aujourd'hui plusieurs chercheurs dans le domaine des VANETs s'intéressent de plus en plus à l'étude de la mobilité et son impacte sur les performances des protocoles conçus pour ce type de réseau, et construire plusieurs simulateurs de mobilité qui peuvent placer les protocoles de routage dédiés aux VANETs dans des scénarios proches de la réalité tel que : VanetMobisim, Sumo ... etc [BOUZEBIBA 2015]

Le routage

le problème de routage dans les réseaux véhiculaire présente un axe très important pour les chercheurs. Pour assurer l'acheminement des informations entre les véhicules connectés, un protocole de routage doit être établi pour permettre de déterminer la suite des noeuds que les paquets doivent traverser pour un échange d'information entre véhicules distantes. Les problèmes aux quels doivent répondre les protocoles de routage sont la connectivité intermittente qui tend les routes déjà établies obsolètes et le partitionnement du réseau qui empêche la propagation des paquets [JERBI 2008a]

Service de localisation

dans un réseau véhiculaire chaque véhicule est identifié par des contraintes géographiques et elle doit être capable de connaître les positions géographiques des autres véhicules, qui se trouvent dans sa zone de couverture. Les informations envoyées par un véhicule ne se diffusent que pour les véhicules qui se trouvent dans une zone géographique spécifique. La complexité dans la localisation géographique réside dans la détermination de la zone géographique et la définition d'un mécanisme de délayage efficace qui réduit la surcharge du réseau et qui soit adaptés à toutes les densités [BOUZEBIBA 2015]

1.5 CONCLUSION

L'étude effectuée sur les réseaux mobiles Ad hoc nous a permis de connaître leurs mode de transmissions et les différentes caractéristiques (absence d'infrastructure, topologie dynamique, bandes passantes limitées, sécurité physique limitée, contraintes d'énergie,. ...etc.). Nous avons montré aussi que les communications véhiculaires avec ces deux modes V2I et V2V permettent d'améliorer d'une part la sécurité routière grâce aux messages échangés entre les véhicules, et de rendre d'autre part les routes plus agréables grâce à la diversité des services offerts. Toutes ces

applications exigent des concepteurs la prise en compte de l'importance des informations échangées entre les véhicules. Ainsi, il n'y a aucune garantie que les membres des réseaux VANET ne créent pas des messages arbitrairement falsifiés ou ne changent pas le contenu d'un message lié à la sécurité afin de causer un accident par exemple. Dans le chapitre suivant, nous allons étudier les protocoles de routage dans les VANETs.

Le Routage dans les réseaux véhiculaires

2

Sommaire

2.1 Introduction au routage 16
2.2 La difficulté du routage dans les réseaux VANET 16
2.3 Classification des protocoles de routage dans les réseaux mobiles Ad Hoc 16
2.3.1 Classification selon l'architecture 17
2.3.2 Classification selon L'approche de routage 17
2.3.3 Classification selon L'algorithme utilisé 18
2.4 Le routage dans les réseaux VANET 19
2.4.1 Les protocoles de routage basés sur la topologie 20
2.4.2 Les protocoles de routage basés sur la géographie 20
2.5 Les protocoles de routage employés dans notre étude . 22
2.5.1 Le protocole de routage AODV 22
2.5.2 Le Protocole de routage OLSR 26
2.6 Conclusion 26

2.1 Introduction au routage

Les communications dans les réseaux de mobiles fortement dynamiques, tels que les réseaux de véhicules, requièrent l'utilisation de protocoles de communication spécifiques. La gestion de l'acheminement de données ou le routage, consiste à assurer une stratégie qui garantit à n'importe quel moment, la connexion entre n'importe quelle paire de noeuds appartenant au réseau. La stratégie de routage doit prendre en considération les changements de la topologie ainsi que les autres caractéristiques des réseaux de véhicules. Par ailleurs, la méthode adoptée dans le routage doit offrir le meilleur acheminement des données au vu des différentes métriques de performance (délai, fiabilité, surcharge).

De nombreux travaux ont été menés pour garantir l'acheminement des messages (couche réseau) dans les réseaux ad hoc mobiles (MANETs). Cependant,compte tenu de la nature très dynamique des réseaux de véhicules, Des mécanismes et des protocoles spécifiques doivent donc être utilisés afin d'effectuer un routage efficace et performant dans la partie ad hoc du réseau de véhicules.

On peut définir le routage comme la méthode d'acheminent des informations à la bonne destination à travers un réseau de connexions défini. Son intérêt consiste à trouver le chemin optimal au sens d'un certain critère de performance (bande passante, délai, etc.). Il doit aussi être de capable de s'adapter aux événements venant perturber le réseau (panne, congestion, etc.).

2.2 La difficulté du routage dans les réseaux VANET

. La difficulté de routage dans les réseaux de véhicules réside essentiellement dans l'instabilité des chemins causée par la forte mobilité des noeuds et les fragmentations fréquentes du réséeau. En effet, le fait que le réseau soit à connectivité partielle ou intermittente souligne que la gestion de routage doit être différente des approches topologiques utilisées dans les réseaux ad hoc classiques MANETs. Autre aspect de la problématique est du au fait que le routage géographique de base pose des problèmes dans le cas de communications dans des environnements ou il existe des obstacles (bâtiments) et des vides comme c'est le cas dans une ville. En effet, la topologie évoluant constamment en fonction des mouvements des mobiles, Le problème qui se pose dans le contexte des réseaux VANET est l'adaptation de la méthode d'acheminement utilisée avec le grand nombre d'unités existant dans un environnement caractérisé par de modestes capacités de calcul et de sauvegarde[RACHEDI 2008].

2.3 Classification des protocoles de routage dans les réseaux mobiles Ad Hoc

Les protocoles de routage destinés aux réseaux mobiles Ad Hoc peuvent être classés de différentes manières, selon plusieurs critères. Ils peuvent être classés selon :

— L'architecture (uniforme ou non uniforme).

— L'approche de routage (proactif, réactif, hybride).
— L'algorithme dynamique (vecteur de distance ou état de liens, source ou apprentissage en arrière).

2.3.1 Classification selon l'architecture

Ce critère divise les protocoles de routage en deux classes :

1. Les protocoles uniformes : Les protocoles de routage uniformes considèrent que tous les noeuds sont égaux, dans le même niveau hiérarchique et possèdent ainsi les mêmes rôles et fonctions. Par conséquent, aucune hiérarchie n'est définie entre les noeuds du réseau, chaque noeud envoie et reçoit des messages de contrôle de routage, la décision d'un noeud de router des paquets dépendra de sa position [MAHI 2010]
2. Les protocoles non uniformes : Les protocoles de routage non uniformes tentent de limiter la complexité du routage en réduisant le nombre de noeuds qui contribuent à la détermination des routes, ils fonctionnent en attribuant aux noeuds des rôles qui varient de l'un à l'autre. Une structure hiérarchique entre les noeuds est définie selon leurs fonctions. Certains noeuds sont élus pour accomplir des taches bien particulières qui conduisent à une vision en plusieurs niveaux de la topologie du réseau afin de faciliter l'équilibrage de la charge et de mieux la gérer (surtout dans les réseaux mobiles Ad Hoc de grande taille),ce qui conduit à une meilleure qualité de service [MAHI 2010]

2.3.2 Classification selon L'approche de routage

Ce critère divise les protocoles de routage en trois classes :

1. Le routage proactif : Les protocoles proactifs sont basés sur la même philosophie que les protocoles de routages utilisés dans les réseaux filaires conventionnels. C'est-à-dire qu'elle est fondée sur la méthode état de lien et vecteur de distance.Un protocole proactif est un protocole qui construit les tables de routage avant que la demande en soit effectuée. Il identifie en fait à chaque instant la topologie du réseau. Les protocoles proactifs utilisent l'échange régulier de messages de contrôle pour maintenir au niveau de chaque noeud des tables de routage (qui associent à chaque destination ou groupe de destinations un voisin direct par lequel les paquets doivent être relayés) vers toute destination atteignable [MUSTAFA 2004].Le maintient des tables de routages est réalisé par inondation, lors des mises à jour périodique ou lors d'un changement d'état d'un lien. L'inondation consiste à propager à l'ensemble du réseau une information. L'émetteur initial envoie à tous ses voisins une information, ces derniers se chargeant de la rediffuser à leurs tours.Actuellement ils existent plusieurs protocoles proactifs (DSDV, OLSR, FSR).
2. Le routage réactif : Le routage réactif est basé sur le principe de l'ouverture de route à la demande, ainsi lorsqu'un équipement veut communiquer avec une station distante, il est obligé de déterminer

une route dynamiquement. Cette technique permet de ne pas inonder le réseau de paquets de contrôle de routage et de ne conserver que les routes utilisées. Les protocoles de routages réactifs (à la demande) créent et maintiennent les routes selon les besoins. Lorsqu'un noeud à besoin d'une route, une procédure de découverte globale est lancée. Cette procédure s'achève par la découverte de la route ou lorsque toutes les permutations de routes possibles ont été examinées. La route trouvée est maintenue par une procédure de maintenance de routes jusqu'à ce que la destination soit inaccessible à partir du noeud source ou que le noeud source n'aura plus besoin de cette route [MUSTAFA 2004] . Actuellement ils existent plusieurs protocoles réactifs (DSR, AODV, TORA).

3. Le routage hybride : En plus des protocoles de routage proactifs et réactifs, il existe une famille de protocole de routage qui est une combinaison des deux précédents et est dite "hybride", Il utilise un protocole proactif, pour apprendre le proche voisinage Ainsi ils disposent des routes immédiatement dans le voisinage. Au-delà de cette zone prédéfinie, le protocole hybride fait appel aux techniques des protocoles réactifs pour chercher des routes. Le modèle hybride appara^ıt comme un bon compromis qui d'un coté utilise une procédure de détermination sur demande et de l'autre un coût de recherche limité [MUSTAFA 2004] . Il existe plusieurs protocoles hybrides tels que le protocole de routage " ZRP " et " CBRP".

2.3.3 Classification selon L'algorithme utilisé

Une autre classification basée sur le type d'algorithme utilisé est possible pour les protocoles de routage Ad Hoc. Il existe deux grandes familles d'algorithmes de routage dynamique (vecteur de distance et état de liens) et deux grandes familles d'algorithmes de routage à la demande (source et apprentissage en arrière)[CHAIB 2011] :

1. Les protocoles de routage à vecteur de distance (Distance Vector Protocols) : Ces protocoles sont basés sur l'algorithme de Bellman-Ford. Leur principe est basé sur l'échange entre les noeuds voisins d'informations de distance des destinations connues. Autrement dit, chaque noeud envoie à ses voisins la liste des destinations joignables et le coût (distance) associé au chemin le plus court menant vers cette destination. A chaque réception d'un paquet contenant les informations topologiques. Le noeud en question met à jour sa liste de destination par le coût minimum [CHAIB 2011] .
2. Les protocoles de routage à état de lien (Link state protocols) : Ces protocoles utilisent un algorithme plus efficace en calcul du plus court chemin qui est l'algorithme de Dijkstra. Ils sont basés sur l'état des liens (topologie) du réseau, l'ensemble de ces informations permet aux noeuds de dessiner une vue globale sur le réseau.une table de routage est maintenue dans chaque noeud. Elle est construite à partir des informations échangées sur l'état des liens du réseau. A partir de cette vue globale du réseau, il est facile de trouver des routes alternatives lorsqu'un lien est rompu. Ainsi

une route est immédiatement disponible à la demande. Il est même possible d'utiliser simultanément plusieurs routes vers une même destination, augmentant ainsi la répartition de la charge et la tolérance aux pannes dans le réseau. En contre partie, si le réseau est étendu, la quantité d'informations sur l'état de tous les liens du réseau au niveau de chaque noeud nécessite un espace de stockage considérable[BOUSSAD 2011].

3. Les protocoles de routage source : Chaque noeud doit posséder la topologie et les caractéristiques du réseau en entier. Les données doivent être parfaitement à jour. Ce routage convient aux réseaux de tailles moyennes (pour éviter la surcharge de la mémoire) à hauts débits (le calcul de routes est effectué une seule fois). Pour cela, le temps de calcul des routes ne doit pas être trop grand. Dans cet algorithme, afin d'émettre un paquet de données à travers lequel le paquet va passer pour atteindre la destination (route source). Par la suite, l'émetteur transmet le paquet via son interface, au premier noeud spécifié dans la route. Un noeud qui reçoit le paquet, et qui est différent de la destination, supprime son adresse de l'entête du paquet reçu et le transmet aux noeuds suivant identifié dans la route source. Ce processus se répète jusqu'à ce que le paquet atteigne sa destination finale. Enfin, le paquet est délivré à la couche réseau de dernier hôte [CHAIB 2011]
4. Le protocole de routage par apprentissage en arrière : Le chemin établi entre les noeuds est un chemin bidirectionnel simultané (full duplex). La source gardera une trace du chemin tant qu'il restera en cours d'utilisation. Ce type de routage nécessite moins de mémoire que le routage source. Par conséquent, il est plus adapté pour des réseaux de plus grandes tailles [JOHNSON and al 2004]. Afin de transmettre un paquet à l'aide de cette méthode, le noeud émetteur inonde le réseau avec sa requête. Ainsi chaque noeud intermédiaire, dit le transit, indique le chemin au noeud source lors de la réception de la requête. On dit qu'il apprend le chemin au noeud source, tout en sauvegardant la route dans la table transmise. Enfin, lorsque la requête arrive au noeud destinataire, et suivant le même chemin, ce dernier transmet sa réponse sous forme de requ^ete [CHAIB 2011]

2.4 Le routage dans les réseaux VANET

Le mécanisme de routage permet de trouver et maintenir l'acheminement pour assurer la communication entre une paire de noeuds, cette communication est faite selon des techniques spéciales pour assurer la transmission des messages dans les meilleurs délais et d'une manière plus fiable. En raison des caractéristique du réseau VANET les problèmes de routage doivent prendre en considération certains aspect, tel que : la changement de la topologie, absence d'une infrastructure,... etc[BOUSSAD 2011]. On distingue deux grandes classes de protocoles de routage selon le type d'informations utilisées pour acheminer les données. La première classe est celle des protocoles qui se basent sur des informations sur la topologie du réseau, ce sont les protocoles du groupe MANET.

La seconde classe est celle des nouveaux protocoles dits géographiques ou de position qui se basent sur des informations supplémentaires sur la position géographique (voir figure 2.1).

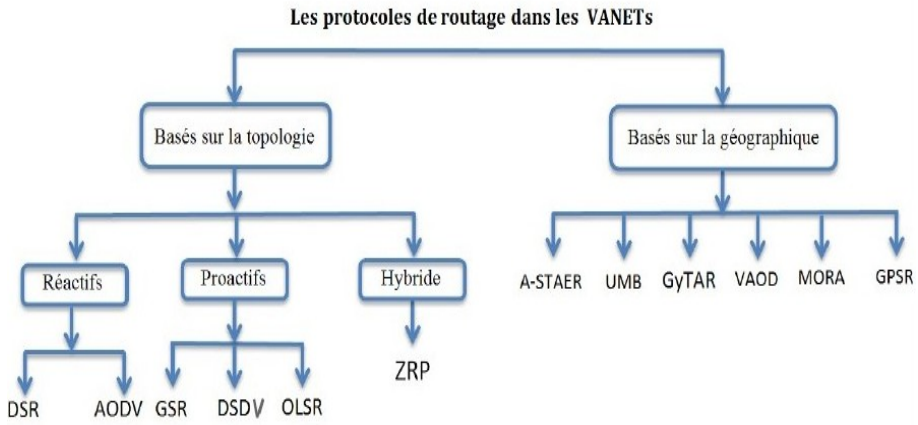

FIGURE 2.1 – *les protocoles de routage dans les réseaux de véhicules.*

2.4.1 Les protocoles de routage basés sur la topologie

Les protocoles de routage basés sur la topologie utilisent les informations sur les liens qui existent entre les noeuds pour l'acheminement des paquets. Cette famille de protocoles peut être divisée en trois catégories : proactifs, réactifs et hybrides, qui sont déjà défini dans ce chapitre. Chaque noeud utilise comme données l'état de ses connexions avec ses noeuds voisins ; cette information est ensuite transmise aux autres noeuds pour leur offrir une connaissance plus précise sur la topologie du réseau[YASINAC 2002].

2.4.2 Les protocoles de routage basés sur la géographie

Les protocoles de routage géographique (ou basés sur la position) utilisent des coordonnées géographiques (par exemple, fournies par GPS) afin de trouver un chemin vers la destination. Pour atteindre cet objectif, les coordonnées géographiques des noeuds sont incluses dans les tables de routage. Concrètement, un noeud inclut l'identifiant et la position de la destination (fournis par le protocole de routage lui même ou par un protocole de service de localisation indépendant) dans le paquet à envoyer, et par la suite les noeuds intermédiaires utilisent les informations géographiques incluses dans ce paquet et celles disponibles dans leurs tables de routage pour retransmettre le paquet et répètent le même mécanisme jusqu'à ce que celui-ci atteigne la destination[YASINAC 2002].

Les protocoles de routage géographiques sont les protocoles les plus adaptés par les réseaux VANETs ; la plupart de ces protocoles utilisent des coordonnés géographiques afin d'assurer l'acheminement des paquets d'informations de source vers le ou les destinataires. Le processus de routage géographique se divise en deux étapes [YASINAC 2002] :

1. La localisation de différents noeuds (sources et destinataires) : il est nécessaire que chaque noeud détermine sa position et la ou les posi-

tions des noeuds destinataires avant d'envoyer des paquets d'informations. Un service de localisation doit être utilisé afin que chaque noeud puisse détermine sa position géographique (généralement le service de localisation le plus utilisé est le GPS) ; les positions des noeuds voisins sont connues puisque chaque noeud envoie périodiquement sa position aux noeuds voisins.

2. L'acheminement ou le routage des paquets d'information : l'acheminement des paquets par un noeud source est essentiellement basé sur la position de ses voisins immédiats et la position du noeud destinataire. Chaque noeud source inclut l'identifiant et la position de la destination dans l'entête de tout paquet à envoyé ; les noeuds recevant ce paquet utilisent les informations géographiques incluses dans ce dernier et celle disponibles dans leurs tables de routage pour retransmettre le paquet et répètent le même processus jusqu'à ce que celui-ci atteigne la destination[WU *et al.* 2007]

On peut diviser les protocoles de routages géographique en trois sous classes : les protocoles basé sur la position géographique, les protocoles basé sur la cartographie routière et les protocoles basé sur le trafic routier

L'avantage majeur de ces protocoles par rapport aux protocoles précédents est qu'ils réduisent considérablement la signalisation (les paquets de contrôle), notamment dans les réseaux larges et dynamiques [YASINAC 2002] .

Dans la littérature, il existe plusieurs protocoles de routage géographique.Les plus connus sont : DREAM , GSR ,A-STAR , VADD.

GSR (Geographic Source Routing)

est un protocole de routage géographique qui combine le routage basé sur la localisation avec le routage basé sur la topologie des routes pour construire une connaissance adaptée à l'environnement urbain. Le principe de GSR est que le véhicule source désirant envoyer de données vers un véhicule cible, calcule le chemin de routage le plus court à partir des informations géographiques d'une carte routière et en utilisant les algorithmes de recherche du plus court chemin, par exemple Djikstra. A partir du chemin du routage calculé, le véhicule source sélectionne ensuite une séquence d'intersections par lesquelles le paquet de données doit transiter afin d'atteindre le véhicule destinataire. Cette séquence d'intersections est constituée d'un ensemble de points géographiques fixe de passage du paquet de données. Pour envoyer les messages d'une intersection à une autre [LPCHERT *et al.* 2003]. Les mêmes auteurs ont proposé un protocole GPCR (Greedy, Perimeter Coordinator Routing) qui est une combinaison du protocole GPSR et l'utilisation de la cartographie des routes [SEET *et al.* 2004] .

A-STAR (Anchor-based Street and Traffic Aware Routing)

est un protocole de routage basé sur la position pour un environnement véhiculaire métropolitain. Il utilise particulièrement les informations sur les itinéraires d'autobus de ville pour identifier une route d'ancre (anchor route) avec une collectivité élevée pour l'acheminement des paquets.

A-STAR est similaire au protocole GSRéen adoptant une approche de routage basée sur l'ancrage (anchor based) qui tient compte des caractéristiques des rues. Cependant, contrairement à GSR il calcule les "anchor paths" en fonction du trafic (trafics de bus, véhicules, etc...). Un poids est assigné à chaque rue en fonction de sa capacité (grande ou petite rue qui est desservie par un nombre de bus différent). Les informations de routes fournies par les bus donnent une idée sur la charge de trafic dans chaque rue. Ce qui donne une image de la ville à des moments différents [ZHAO & VADD 2006] . .

VADD (Vehicle-Assisted Data Delivery)

est un protocole de routage qui prend en consiération le contexte des réseaux de véhicules et exploite le mouvement prévisible des véhicules pour décider de retransmettre ou non le message. Il utilise particulièrement les informations sur le trafic routier au niveau d'une route pour estimer le délai mis par un paquet pour parcourir un tel segment. Par conséquent, les paquets seront acheminés le long d'un chemin ayant le plus faible délai de bout en bout[ZHAO & VADD 2006].

2.5 Les protocoles de routage employés dans notre étude

2.5.1 Le protocole de routage AODV

AODV est un algorithme de routage conçu par Charles E. Perkins et Elizabeth M. Royer. Il est adapté aux réseaux de topologie fortement dynamique et est basé sur le routage de vecteur de distance. Le protocole AODV minimise sensiblement le nombre des diffusions des messages en créant des chemins à la demande, Il est à la fois capable de routage unicast et multicast. Il est libre de boucle, auto-démarrant et s'accommode d'un grand nombre de noeuds mobiles (ou intermittents). Lorsqu'un noeud source demande une route, il crée les routes à la volée et les maintient tant que la source en a besoin. Pour les groupes multicast, AODV construit une arborescence.

Ce protocole de routage est peu gourmand en énergie et ne nécessite pas de grande puissance de calcul, il est donc facile à installer sur de petits équipements mobiles. [PERKINS *et al.* 2003] :

1. Route Request : "J'ai besoin d'une route", Le message de demande de route, est le message d'interrogation des routes disponibles. Il est constitué d'une trame de 24 octets (voir figure 2.2).

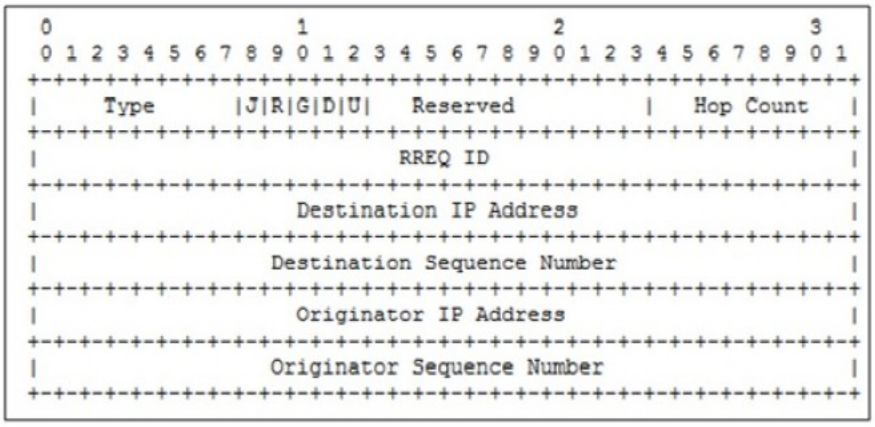

FIGURE 2.2 – *format d'un paquet RREQ*

– Type : 1 – "J" Joint du pavillon ; réservés pour le multicast.

– Indicateur de réparation R : réservés pour le multicast.

– Drapeau "G" RREP à titre gratuit ; indique si un RREP gratuite devrait être unicast vers le noeud spécifiée dans le champ Adresse IP de destination .

– Pavillon "D" Destination seulement ; indique que le destination peut répondre à cette RREQ .

– "U" nombre de séquence inconnue ; indique la destination numéro de séquence est inconnu .

– Réservé à 0 ; ignoré à la réception.

– Hop Count Le nombre de sauts à partir de l'adresse IP Créateur au noeud traitement de la demande.

– RREQ ID Un numéro de séquence unique d'identification de la RREQ particulier lorsqu'ils sont pris conjointement avec l'adresse IP d'origine du noeud.

– Adresse IP de destination L'adresse IP de la destination pour laquelle une route est souhaitée.

– Numéro de séquence de destination Le dernier numéro de séquence reçu dans le passé par l'émetteur pour tout route vers la destination.

– Adresse IP Créateur L'adresse IP du noeud qui à l'origine du Route Request.

– Numéro de séquence Créateur Le numéro de séquence courant pour être utilisé dans le trajet entrée pointant vers le donneur d'ordre de la route demande.

2. Route Reply : "Annoncer la route", Le message de réponse à la demande de route, est le message indiquant au demandeur les routes disponibles. Il est constitué d'une trame de 20 octets (voir figure 2.3).

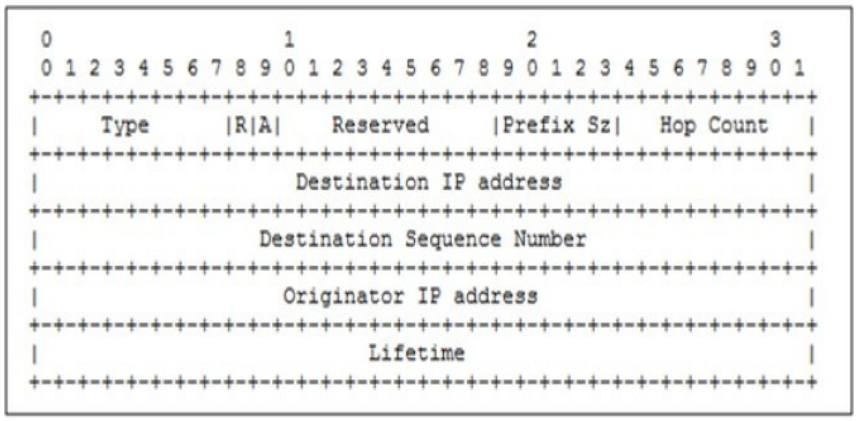

FIGURE 2.3 – *format d'un paquet RREP*

– Type : 2

– Indicateur de réparation R ; utilisé pour la multidiffusion.

– Un accusé de réception nécessaire

– Réservé à 0 ; ignoré à la réception.

– Taille Préfixe Si différent de zéro, la taille de préfixe 5-bit spécifie que le indiqué saut suivant peut être utilisé pour tous les noeuds avec le préfixe de routage même (tel que défini par le préfixe) Taille de la destination demandée[NING & SUN 2005].

– Hop Count : Le nombre de sauts à partir de l'adresse IP Créateur à l'adresse IP de destination. Pour route de multicast demandes ce qui indique le nombre de sauts à l' membre arbre multicast en envoyant le RREP.

– Adresse IP de destination : L'adresse IP de la destination pour laquelle une route est fourni.

– Numéro de séquence de destination : Le numéro de séquence de destination associée à trajet.

– Adresse IP Créateur :L'adresse IP du noeud qui à l'origine du RREQ pour lequel le trajet est fourni.

– Durée de vie : Le temps en millisecondes pour lesquelles des noeuds de réception RREP considérer la route pour être valide.

3. Route Error : "Annuler la route", indiquant une route en erreur est le message retour signalant au demandeur les routes en erreur. Il est constitué d'une trame de 20 octets.
4. Le message RREP-ACK : l'accusé de réception de route de repli, est le message indiquant la prise en compte d'une autre route disponible. Il est constitué d'une trame de 2 octets.

Lorsqu'un noeud source désire envoyer des données vers un destinataire, il vérifie tout d'abord dans sa table de routage s'il existe une route valide vers ce destinataire. Si la route n'est pas trouvée, le noeud source lance la procédure de découverte de route en diffusant en broadcast un paquet RREQ à la recherche d'un chemin vers le destinataire A la réception de ce paquet, le noeud répond par un paquet RREP s'il est lui-même le destinataire ou s'il possède dans sa table une route vers la destination.

Dans le cas contraire, c'est-à-dire si la table de routage ne contient pas de route vers le destinataire, le noeud rediffuse le RREQ. Une fois la route trouvée, le noeud source transmet les paquets de données en transitant de proche en proche et chaque noeud détermine le prochain relai à partir de sa table de routage(voir figure 2.4) [NING & SUN 2005].

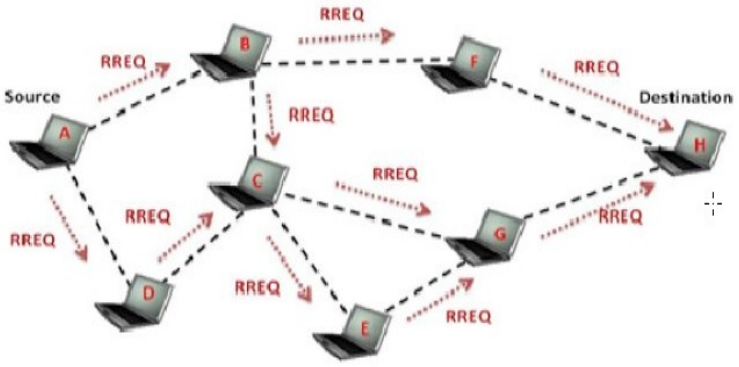

FIGURE 2.4 – *Découverte de route.*

En cas de rupture de route, le noeud intermédiaire envoie un paquet RERR pour informer la source qui décide ou non de recommencer l'envoi du paquet (voir figure 2.5).

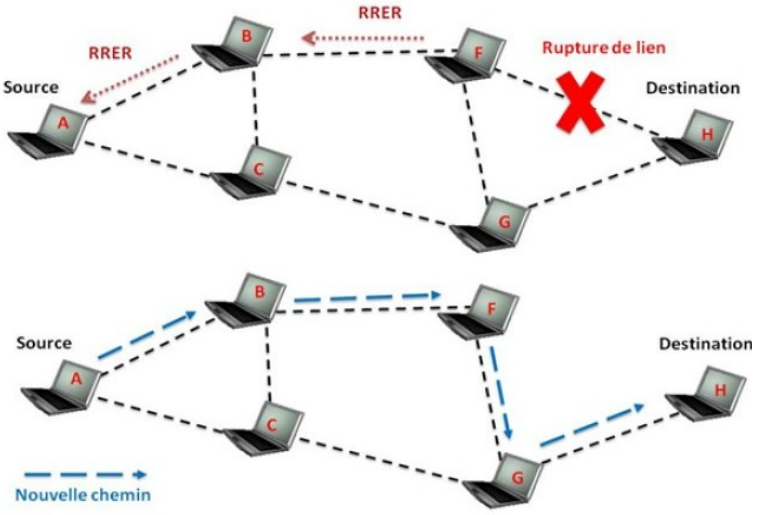

FIGURE 2.5 – *Réparation des chemins.*

L'un des avantages d'AODV est l'utilisation de numéro de séquence dans les messages. Ces numéros de séquences permettent l'éviter les problèmes de boucles infinies et sont essentiels au processus de mis à jour de la table de routage. Un autre avantage est le rappel de l'adresse IP du noeud origine dans chaque message. Ceci permet de ne pas perdre

la trace du noeud à l'origine de l'envoi du message lors des différents relais. Un inconvénient d'AODV est qu'il n'existe pas de format générique des messages. Chaque message a son propre format : RREQ, RREP, RERR[NING & SUN 2005].

2.5.2 Le Protocole de routage OLSR

OLSR signifie " Routage à états de liens optimisé "(Optimazed Link State Routing).OLSR est le résultat du travail d'HIPERCOM, équipe de recherche de l'INRIA Rocquencourt. Ce protocole se rapproche du protocole OSPF, protocole à état de liens. Par contre dans un protocole à état de liens, chaque noeud déclare ses liens directs avec ses voisins à tout le réseau, tandis que dans le cas d'OLSR, les noeuds ne déclarent qu'une sous-partie de leur voisinage grâce à la technique des relais multipoints. Cette technique permet d'optimiser la diffusion des messages de routage économisant une grande partie de la bande passante du réseau [LPCHERT *et al.* 2003].

Les relais multipoints consistent essentiellement, en un noeud donné, à ignorer un ensemble de liens et de voisins directs, qui ont redondant pour le calcul des routes de plus courts chemins. Plus précisément, dans l'ensemble des voisins d'un noeud, seul un sous-ensemble des ces voisins est considéré comme pertinent. Il est choisi de façon à pouvoir atteindre tout le voisinage à deux sauts (tous les voisins des voisins), cet ensemble est appelé l'ensemble des relais multipoints.

Ces relais multipoints sont utilisés pour diminuer le trafic du à la diffusion des messages de contrôle dans le réseau, et aussi pour diminuer le nombre de retransmission à tout le réseau puisque les routes sont construites à base des relais multipoint. La diffusion par relais multipoints utilise la règle suivante : Un noeud retransmet un message si et seulement s'il ne l'avait pas déjà reçu, et s'il vient de le recevoir d'un noeud dont il est un relais multipoint. Les noeuds s'échangent des informations périodiquement (messages " HELLO " et " TC ") afin de semaintenir à jour [LPCHERT *et al.* 2003].

Les messages "HELLO" contiennent la liste de leurs voisins pour s'informer du proche voisinage et permettre ainsi à chacun de choisir son ensemble de relais multipoints. Les messages " TC " (" Topology Control ") déclarent les sous ensembles de voisinage que constituent les relais multipoints. Ils sont diffusés en utilisant une diffusion optimisée par relais multipoints [LPCHERT *et al.* 2003].

Ces informations offrent une carte de réseau contenant tous les noeuds et un ensemble partiel des liens, mais suffisant pour la construction la table de routage. La table de routage est calculée par chacun des noeuds et le routage des données s'effectue saut par saut sans l'intervention d'OLSR dont son rôle s'arrête à la mise à jour de la table de routage [LPCHERT *et al.* 2003] .

2.6 Conclusion

Ce chapitre à été axé sur l'étude des protocoles de routage, on a présenter les trois classes des protocoles de routage(proactif, réactif, hybride) ainsi les autres techniques de routage spécifique pour les réseaux VANET.

Dans le chapitre suivant, nous présenterons une partie décrivant les différents mécanismes de sécurité dans réseaux VANETs.

La sécurité et QOS dans les réseaux sans fil

3

Sommaire

3.1 Introduction 29
3.2 La sécurité 30
3.2.1 Qu'est ce que la sécurité 30
3.2.2 Objectifs de la sécurité 30
3.2.3 La cryptographie 32
3.3 PKI (Public Key Infrastructure) 34
3.3.1 Définition du PKI 35
3.4 Les attaques contre les réseaux AD HOC 39
3.4.1 Classification des attaques 39
3.4.2 Présentation de quelques attaques 39
3.5 Vulnérabilité des réseaux véhiculaires 40
3.6 Attaques spécifiques sur les VANETs 40
3.6.1 L'injection des messages erronés : 41
3.6.2 Le déni de service : 41
3.6.3 La révélation d'identité et de position géographique des autres véhicules 41
3.7 La qualité de service 41
3.7.1 Niveaux de service 42
3.7.2 Critères ou paramètres de qualité de service 42
3.8 Conclusion 44

3.1 Introduction

Les réseaux sont de plus en plus populaires, ils vont intégrer dans un futur proche toutes les situations de notre vie quotidienne. Une nécessité accrue s'est faite sentir pour rendre ces réseaux fiables et hautement sécurisés afin de protéger la vie privée des utilisateurs et offrir une bonne qualité de service pour les applications.Une tâche qui s'avère difficile et compliquée. Etant donnée le concept et la nature des réseaux ad hoc les rendent facilement vulnérables à différents types d'attaques[KO & VAIDRA 1998].

Ce qui rend la t^ache encore plus difficile est que les noeuds du réseau se chargent eux-mêmes de la fonction de routage des données. Favorisé par la nature vulnérable des communications sans fil, n'importe qui peut se connecter sur le réseau et écouter les messages de contrôle échangés. Il pourra ensuite les supprimer, les modifier, ou mener d'autres attaques plus complexes, ce qui met en danger tout le réseau. Les protocoles de routage proposés dans le cadre du travail du groupe MANET offre un acheminement optimal des données mais n'offre aucun système de sécurité[ANJUM & MOUCHTARIS 2007].

De plus l'emploi des stratégies de sécurités robustes utilisées avec succès dans les réseaux filaires et les réseaux sans fil avec infrastructure se trouve contraint par l'absence d'infrastructure centralisée qui pourrait gérer le service de sécurité dans le réseau. Dans un réseau ad hoc, les noeuds doivent exécuter eux-mêmes les mécanismes de sécurité pour se protéger contre les attaques. Mais le problème qui se pose est que les noeuds sont caractérisés par de modestes capacités de calcul, de stockage, et d'énergie. Dans ce cas là, l'utilisation des systèmes de sécurité robustes et efficaces comme le cryptage par clé ou l'authentification sophistiquée qui consomment beaucoup de ressources ne donne pas toujours de bons résultats en pratique et peut affecter considérablement les performances du réseau[KO & VAIDRA 1998].

La sécurité des systèmes d'information en général et des réseaux en particulier est un enjeu essentiel, et particulièrement depuis l'avènement du développement d'internet et de l'intégration des systèmes d'information entre eux. Le chiffrement, et en particulier le chiffrement asymétrique représente un des moyens les plus sur pour garantir l'intégrité et la confidentialité de l'information. Son fonctionnement est simple : on distribue àchaque utilisateur une paire de clé (clé privée/clé publique) reliées mathématiquement par un algorithme très complexe. L'une est connue de tous (clé publique) afin que chaque utilisateur qui le désire puisse envoyer un message à une autre personne.

La clé privée est quant à elle connue uniquement par l'utilisateur qui la possède. Elle lui permet de décrypter un message dont il est destinataire. C'est pour gérer la problématique liée au cycle de vie des clés que l'infrastructure à clé publique a fait son apparition. Communément appelée PKI, celle-ci fournit des certificats garantissant le lien entre une identité et une clé publique. La PKI adresse la gestion des paires de clés asymétriques sous sa forme technologique en établissant un lien de confiance et en garantissant pour les échanges de mes-

sages entre des tiers, l'authentification, la confidentialité, l'intégrité et non répudiation[ANJUM & MOUCHTARIS 2007]

3.2 La sécurité

3.2.1 Qu'est ce que la sécurité

Plusieurs définitions existent dans la littérature de la sécurité. D'après [DLS 1932] , Celle-ci est définit comme suit " Sécurité. n.f. Confiance, tranquillité d'esprit qui résulte de l'opinion, bien ou mal fondée, qu'on n'a pas à craindre de danger".

Plusieurs aspects discutés ci-dessous, confirment que la sécurité est vue comme une situation caractérisée par l'absence de tout risque pour les personnes concernées (Je me sens en sécurité), bien évidement dans la réalité l'absence totale des risques n'est pas encore atteinte à cause de l'inflexibilité de l'environnement. Ce qu'on peut dire actuellement sur la sécurité c'est (A quel niveau je me sens en sécurité ?) et (quel est le prix que je dois payer pour avoir cette sécurité). Selon une autre vision, la sécurité est souvent vue comme l'art de partager les secrets. Cette définition de sécurité est celle donnée par les cryptologies, de très bas niveau, nécessaires mais insuffisantes dans beaucoup de contextes actuels. Elle se révèle difficile à appliquer sur des systèmes d'informations modernes dans une approche top-down.

On peut aussi définir la sécurité de l'ère numérique [CHAOUCHI & LAURENT 2007] comme une quête pour la protection des biens numériques et la protection des systèmes de traitement des biens numériques contre tout acte non voulu ou perçu comme un abus par les propriétaires. Les actes non voulus sont typiquement possibles à cause des vulnérabilités présentes dans les systèmes. L'exploitation des vulnérabilités crée des menaces et représente ainsi un risque du point de vue du propriétaire. Ainsi, les risques mènent à l'implémentation d'un ensemble de contre mesures. Cette définition se trouve alors au croisement de la définition habituelle

3.2.2 Objectifs de la sécurité

On peut rassembler les objectifs de la sécurité en quatre points importants (voir figure 3.1).

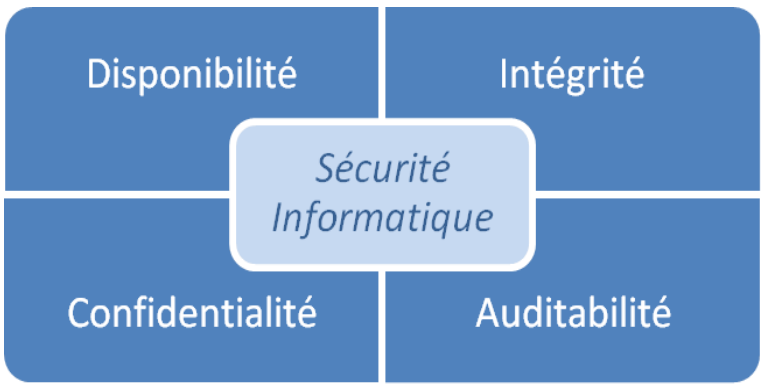

Figure 3.1 – *Objectifs de la sécurité.*

Confidentialité des données

La confidentialité empêche les données d'être consultées par des entités non autorisées. Des contr^oles d'accès strict doivent être mis en place pour garantir la confidentialité des données dans les réseaux ad hoc. étant donné que les communications sans fil transitent via les airs, elles sont donc potentiellement accessibles à tout possesseur du récepteur adéquat. Un message ou un échange de messages à sa confidentialité garantie dès lors que tout utilisateur non autorisé qui aurait pu le récupérer ne peut pas l'exploiter. Il n'est pas obligatoire de mettre en place des procédures pour empêcher cette " récupération " [GAYROUD *et al.* 2008] .

Intégrité des données

C'est un service qui garantit que les données n'ont pas été altérées pendant la transmission. Donc le récepteur d'un message s'assure que le message reçu est le même que le message envoyé. L'intégrité des données est une exigence importante pour les réseaux ad hoc. Elle peut être remise en cause par de nombreux évènements. Parmi ceux-ci, les attaques visant à modifier le contenu des messages et la faible fiabilité de liaisons sans fil. L'intégrité possède une portée plus ou moins grande (le message complet ou un champ spécifique du message seulement). Lorsque la communication a lieu en mode non connecté, seule la détection des modifications peut être mise en oeuvre. Les principes de la protection contre les erreurs : ajouter un bloc de contrôle d'erreur qui est le résultat d'un algorithme connu appliqué au message. Le récepteur refait le calcul sur le message qu'il a reçu et compare les deux blocs de contrôle d'erreurs. Il vérifie ainsi l'intégrité du message, cette seule méthode est insuffisante pour détecter des messages insérés dans un flux de données. Les protections mises en oeuvre s'inspirent du même principe [GAYROUD *et al.* 2008] .

Authentification

Dans un réseau, un adversaire peut facilement injecter des paquets additionnels, ainsi le récepteur doit s'assurer que les données reçues proviennent effectivement de la source supposée. Le service d'authentification garantit l'identité des correspondants ou des partenaires qui communiquent [RIAHLA 2008]. On distingue deux cas d'authentification simple et un cas d'authentification mutuelle :

— L'authentification de l'entité distante. Elle garantit que le récepteur est celui souhaité. Son action peut intervenir à l'établissement de la communication ou pendant le transfert des données. Son objectif principal est la lutte contre le déguisement, également appelé usurpation d'identité (spoofing).

— L'authentification de l'origine. Elle assure que l'émetteur est celui prétendu. Le service est inopérant contre la duplication d'entité. Comme le précédent, il s'agit d'authentification simple.

— L'authentification mutuelle. Elle assure que les deux entités émettrice et réceptrice se contr^olent l'une l'autre. Le service d'authentification est inutilisable dans le cas d'un réseau fonctionnant en mode sans

connexion : dans les réseaux, comme dans la vie courante, l'authentification nécessite un échange entre les deux partenaires.

Non-répudiation

La non-répudiation de l'origine fournit au récepteur une preuve empêchant l'émetteur de contester l'envoi d'un message ou le contenu d'un message effectivement reçu. La non-répudiation de la remise fournit à l'émetteur une preuve empêchant le récepteur de contester la réception d'un message ou le contenu d'un message effectivement émis [RIAHLA 2008].

3.2.3 La cryptographie

La cryptographie est la science d'écriture et de lecture de messages codés. En effet, elle joue un rôle essentiel dans toutes les communications sécurisée en chiffrant un message dit " texte clair " en un deuxième dit " texte crypté " à l'aide d'une clé en utilisant des moyens, matériels ou logiciels conçus à cet effet. Les informations originales sont restituées à partir de celles codées. Cette opération inverse est nommée décryptage [ARNAUD *et al.* 2004]. La cryptographie représente un outil efficace pour mettre en oeuvre la sécurité [GACHET 2011]et ces objectifs tout en utilisant des fonctions mathématiques et des mécanismes de protection, Deux familles de cryptographie existent depuis les années 1970. Elles se distinguent en fonction du type de clés utilisées. La cryptographie symétrique nécessite que les systèmes de chiffrement et de déchiffrement disposent de la même clé cryptographique tandis que la cryptographie asymétrique ou clés publiques considère deux clés complémentaires " les clés publique et privée " réalisant indifféremment l'une le chiffrement et l'autre le déchiffrement.

Cryptographies symétrique

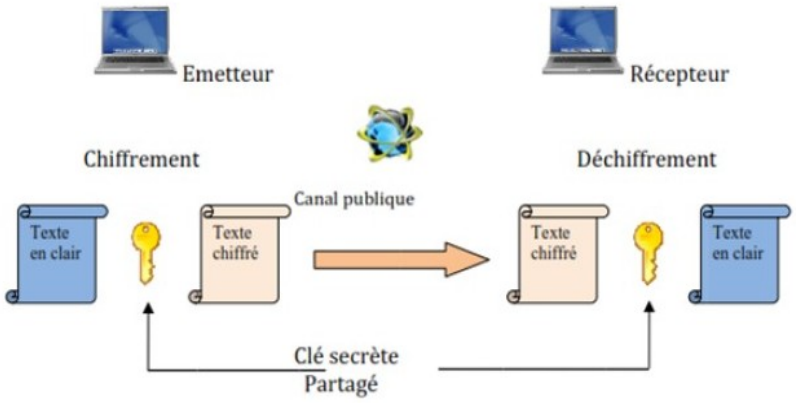

FIGURE 3.2 – *Cryptographies symétrique.*

La Cryptographie symétrique(ou à clé privé) (voir figure 3.2) se base sur l'usage d'une même clé pour chiffrer et déchiffrer des

données[GACHET 2011]. Dans le cadre d'échanges sur un réseau, une entité émettrice chiffre les données avec une clé et l'entité dessinatrice déchiffre les données avec la même clé.

L'échange de la clé doit se faire sur un canal sécuriser donc la sécurité repose totalement sur la confidentialité de la clé. Il y a deux catégories différentes de système à clé privée : le chiffrement par bloc et le chiffrement par flux.

Cryptographie symétrique ou à clés publiques

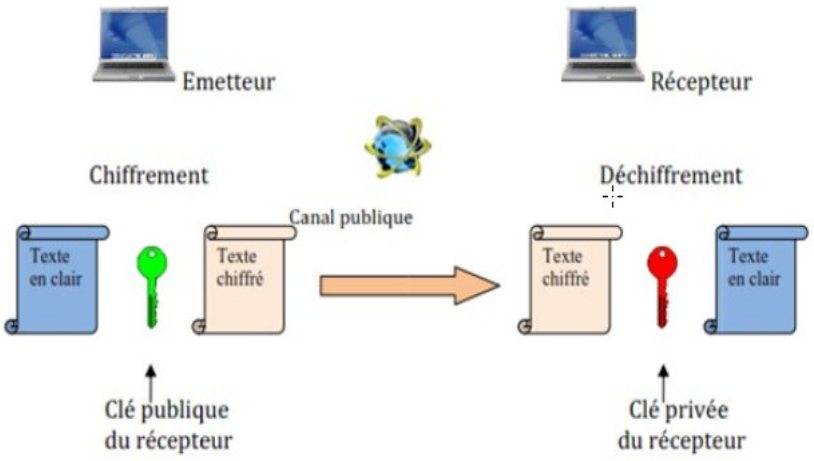

FIGURE 3.3 – *Cryptographie asymétrique – confidentialité*

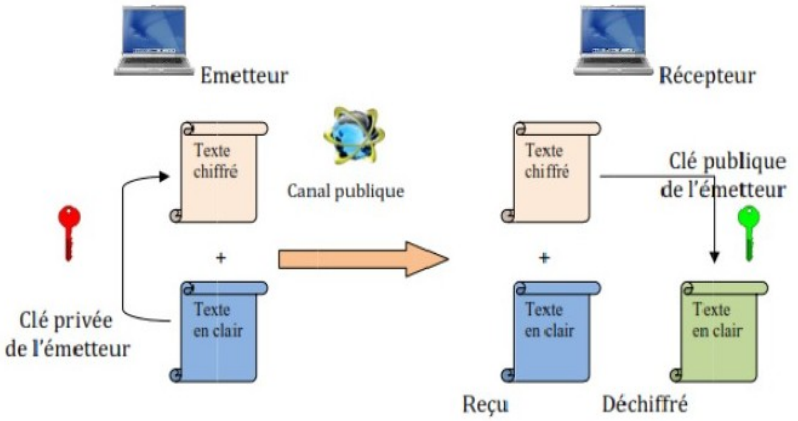

FIGURE 3.4 – *Cryptographies asymétrique – authentification*

La cryptographie asymétrique [BEGHRICHE 2009] ou à clé publique (voir figure 3.3 et 3.4). considère deux clés de chiffrement, dites "clés asymétriques". Ces deux clés sont générées simultanément et sont complémentaires car le chiffrement avec l'une de ces clés nécessite le déchiffrement avec l'autre clé. Chaque clé a un rôle bien défini. La clé privée connue seulement par sont propriétaire, utilisé pour décrypter ou pour signer le message. La clé publique connue par tout le monde, utilisé pour crypter ou pour la vérifier la signature. Bien entendu, la connaissance de la clé

publique ne doit pas permettre de déduire la clé privée complémentaire. Pour authentifier l'origine d'un message dans une communication sur un réseau, l'émetteur doit utiliser sa propre clé privée, le destinataire sera à même de vérifier la validité de la signature et aura une garantie sur la provenance du message. Pour garantir la confidentialité d'un message, il est nécessaire de chiffrer le message émis avec la clé publique du destinataire et le destinataire sera donc le seul à pouvoir déchiffrer le message par la clé privée. La propriété de confidentialité est ainsi obtenue. Les algorithmes asymétriques connus : RSA, Deffie Hellman, El Gamal. Dans notre travail nous avons utilisé l'algorithme RSA.

Fonctions de hachage

Une fonction de hachage [GALICE 2007] c'est une fonction qui permet de trouvé un condensé appelé aussi empreinte, de taille fixe à partir d'un texte de taille arbitraire finie. Les fonctions de hachage servent à rendre plus rapide l'identification des données. Les propriétés attendues de ces fonctions de hachage sont les suivantes :

— Un résultat sur un nombre limité d'octets . — L'impossibilité de retrouver le message original à partir du résultat de la fonction. — Deux messages différant de 1 bit seulement produisent deux résultats qui diffèrent d'au moins la moitié des bits.

Plusieurs termes désignent ces mêmes fonctions de hachage, à savoir : fonctions irréversibles, ou fonctions à sens nique. De même, plusieurs termes désignent e résultat de cette fonction appliquée à un message : hash, haché, mpreinte, ondensat ou encore condensé. Par la suite, on emploiera le terme : " empreinte"

3.3 PKI (Public Key Infrastructure)

L'utilisation massive de la cryptographie à clé publique dans les échanges informatiques engendre un problème circonstanciel de taille. A la façon d'un passeport ou d'une carte d'identité, la PKI va fournir une garantie d'identité numérique aux utilisateurs. Cette pièce d'identité numérique, appelée certificat numérique,contient la clé publique de l'utilisateur, mais également des informations personnelles sur l'utilisateur du certificat. Comme tout document formel, le certificat numérique est signé par l'autorité de certification et c'est cette signature qui lui donnera toute crédibilité aux yeux des utilisateurs. Un certificat est un élément d'information qui prouve l'identité du propriétaire d'une clé publique. Les certificats sont signés et transmis de façon sécuritaire par un tiers de confiance appelé autorité de certification (Certificate Authority, ou CA). L'autorité de certification est chargée de délivrer les certificats, de leur assigner une date de validité, ainsi que de révoquer éventuellement des certificats avant cette date en cas de compromission de la clé (ou du propriétaire). La structure des certificats est normalisée par le standard X.509 de l'UIT (voir figure 3.5).qui définit les informations contenues dans le certificat [GALICE 2007] :

— Version

— Numéro de série de l'autorité de certification

— Algorithme de signature du certificat
— Le nom de l'autorité de certification
— Le nom du propriétaire du certificat
— La date de validité du certificat
— Le propriétaire du certificat
— La clé publique du propriétaire

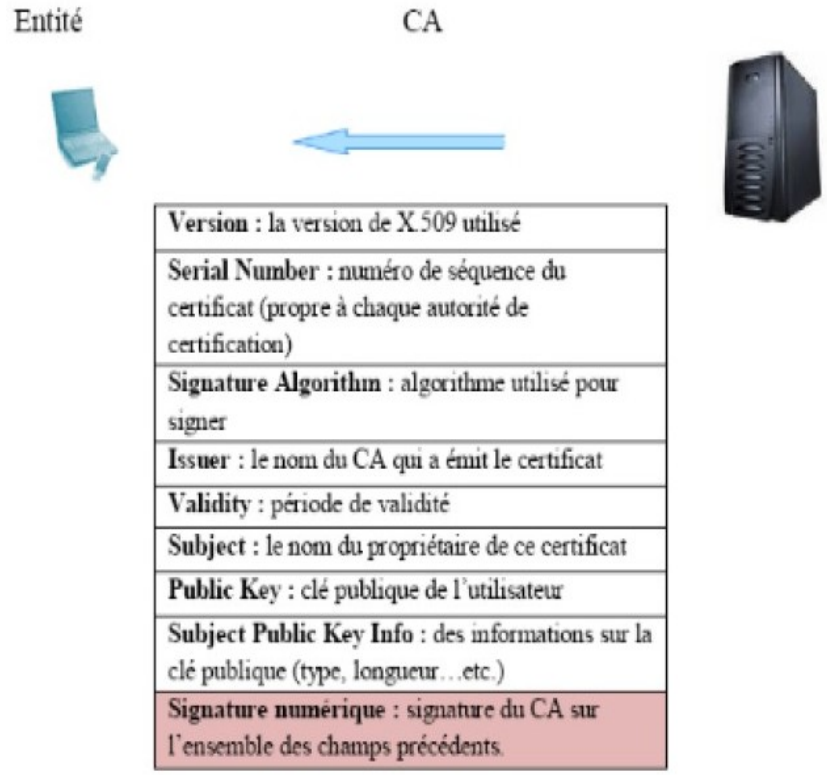

FIGURE 3.5 – *structure de certificat X509v3*

Mais contrairement à un passeport, le certificat numérique est largement publié, il n'a pas à être tenu secret, bien au contraire. Par exemple les browsers Web permettent de stocker les certificats des sites Web et de tout autre utilisateur dans sa base de données interne, Pour obtenir un certificat numérique, le client doit effectuer une requête auprès d'un organisme reconnu. Il transmet avec sa requête sa clé publique .

3.3.1 Définition du PKI

Public Key Infrastructure traduise par clé publique avec infrastructure (voir figure 3.6) [SOLUCOM 2001] , est un système de gestion des clés publiques qui permet de gérer des listes importantes de clés publiques et d'en assurer la fiabilité, pour des entités généralement dans un réseau. Elle offre des éléments important de sécurité tels que la confidentialité, l'authentification, l'intégrité et la non-répudiation tant au sein de l'entreprise que lors d'échanges d'information avec l'extérieur.

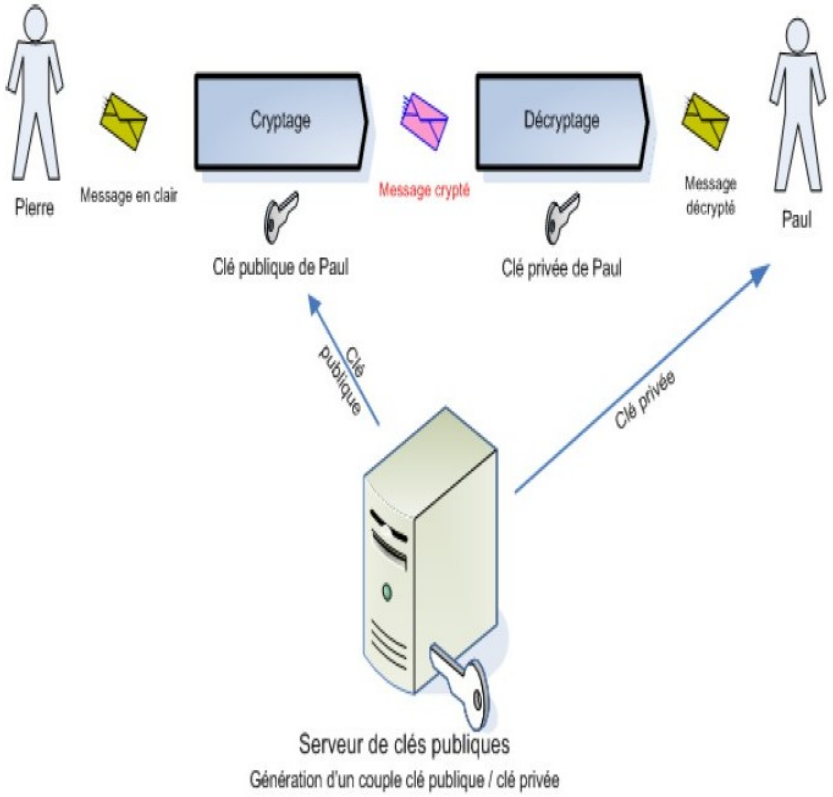

FIGURE 3.6 – *Déroulement d'un sysème PKI*
.

Autorité d'enregistrement RA (Registration Authority)

Cette autorité à la tache d'enrôler des nouveaux utilisateurs dans la PKI, elle reçoit des demandes de certificats CSR (Certificate Signing Request) ; elle à la responsabilité de vérifier la teneur de la demande. Les méthodes de vérification utilisées dépendent de la nature du certificat demandé et de la politique de certification choisie. La vérification peut être limitée à l'identité du demandeur sur un formulaire HTML, mais on peut aussi vérifier s'il possède bien la clé privée associée, s'il a bien l'autorisation de son organisation pour demander ce type de certificat, etc. Si la demande de certificats est acceptée, la demande est ensuite passée à l'autorité de certification CA qui n'a connaissance que des informations strictement indispensables à l'établissement du certificat [SOLUCOM 2001].

Autorité de certification CA (Certificate Authority)

L'autorité de certification représente le noyon d'un system PKI, qui a pour but de créer les certificats aux utilisateurs, La certification est l'opération qui consiste à lier l'identité d'un utilisateur à sa clé publique. Le certificat crée par le CA contient le nom du demandeur DN (Distinguished Name), sa clé publique, la date d'expiration et d'autre fonction de certificat. A fin de terminer le processus de création de certificat, le CA signe finalement le certificat à l'aide de sa clé privée, Etant donné que tout le système PKI est basé sur une chaıne de confiance, la clé privée de la CA

est un élément vital qui doit être protégé par tous les moyens, de ce fait la CA n'est pas nécessairement connectée à Internet. . Suivant la politique de certification choisie, la CA peut prendre à sa charge une partie ou la totalité des opérations de la RA, c'est-à-dire vérifier l'identité de l'utilisateur et la teneur du certificat [SOLUCOM 2001].

l'annuaire dans une PKI

Les composants critiques définis dans une PKI nécessitent un stockage organisé et une facilité d'accessibilité. Le service d'annuaire peut participer à cette tache en assurant une organisation adéquate des données de la PKI est permettre son accès de façon simple. Bien que l'annuaire ne soit pas la seule manière de gérer cette tache, elle est souvent privilégiée car elle permet d'utiliser un annuaire déjà en activité [SOLUCOM 2001] Le service d'annuaire est utile dans le cas d'une PKI pour différentes raisons :

— Les certificats générés par une PKI peuvent êtres stockés dans l'annuaire et récupérés facilement par les utilisateurs et les applications.

— L'annuaire peut stocker également la liste de révocation CRL, permettant ainsi aux utilisateurs de vérifier la validité d'un certificat de façon simple.

— Les organisations PKI qui permettent de gérer le recouvrement de clé, peuvent utiliser l'annuaire pour stocker les clés privées, cryptées bien évidemment

Génération des certificats

L'autorité de certification génère des bi-clés ou la vérification des bi-clés selon le contexte d'utilisation de PKI pour la génération de certificat. Aucun contrôle n'est effectué au cours de cette phase, hormis éventuellement celui du nommage d'entité, le nommage d'entité sert à préserver l'unicité du nommage[RACHEDI 2008].

Remise de certificat

Connue aussi par la distribution du certificat à l'entité à l'origine de la demande n'est pas tout a fait obligatoire. En effet, comme nous allons le voir, à l'issue de sa génération, le certificat peut être publié dans un dép^ot public afin d'être disponible pour les autres utilisateurs. Dans la pratique, le certificat généré est toutefois la plupart du temps remis à l'utilisateur. Le mode de remise dépend à la fois de choix organisationnels ou sécuritaires et d'éléments techniques tels que le lieu de génération de la bi-clé (génération locale ou génération par l'infrastructure) ou le support retenu pour stocker la clé privée et le certificat de l'entité utilisatrice. Si la bi-clé est générée localement par l'entité utilisatrice, la récupération du certificat est généralement à l'initiative de cette dernière. Dans ce cas, l'utilisateur peut récupérer son certificat par exemple sur un site Web, à l'aide d'un secret qui lui a été communiqué lors de son enregistrement. Cette remise peut aussi être à l'initiative de l'infrastructure, par exemple pour une remise du certificat par messagerie. Si l'infrastructure prend en charge la

génération la bi-clé, le certificat et la clé privée sont alors remis à l'utilisateur via l'Autorité d'Enregistrement. La clé privée doit être remise par un moyen très sur[ANJUM & MOUCHTARIS 2007].

Publication de certificat

Cette étape est considéré comme optionnel elle peut apparaitre selon l'usage du certificat et suivant la nécessité de publication. Par exemple la publication des certificats de signature n'est pas forcément utile. En effet, le certificat de signature est toujours joint à la transaction signée. En revanche, il est intéressant de publier les certificats de chiffrement. Lorsqu'un utilisateur veut envoyer des données confidentielles à un autre utilisateur, il lui faut être en possession de la clé publique de ce dernie[ANJUM & MOUCHTARIS 2007]r.

Suppression des clés

La suppression de clés intervient quand la clé à atteint sa fin de cycle, cela peut arriver à la fin de sa validité soit une suspicion quant à la confidentialité de la clé pousse à la faire. La suppression signifie la destruction des toutes les copies de la clé symétrique pour un système symétrique et de la clé publique pour un système asymétrique. Une exception à cette règle intervient si le système dispose d'un processus d'archivage, dans ce cas les clés archivées ne sont jamais détruites[ANJUM & MOUCHTARIS 2007].

Archivage des clés

L'archivage des clés permet de conserver une copie des clés même si elles ne sont plus utilisées, le but est de pouvoir valider des données qui ont été précédemment protégées par la clé. Toutefois des clés privées utilisées pour signer des documents ne devraient pas pouvoir être archivées car la sécurité des documents existants signés avec cette clé serait compromise. Dans tous les cas, une clé archivée ne peut pas être remise en service dans un environnement d'application[BOUSSAD 2011].

Recouvrement des clés (Key Recovery)

Le recouvrement des clés est une procédure délicate qui permet de retrouver la clé privée d'un client, elle peut être envisagée dans le cas o'u le client a perdu sa clé privée, un autre cas de figure peut appara^ıtre si l'employé disparaıt, toutes ses données encore chiffrées doivent pouvoir être recouvrées pour que son travail ne soit pas perdu. Dans ce cas, le principe de recouvrement de clés est souvent associé au recouvrement des données. Un module de recouvrement de clés a pour but de stocker un double crypté de la clé privée de tous les clients dans un emplacement spécial, en effet le recouvrement ne doit pas avoir pour but un espionnage des données personnelles des clients, à cet effet la procédure de recouvrement de clé doit être impérativement menée par plusieurs personnes responsables[ANJUM & MOUCHTARIS 2007].

3.4 Les attaques contre les réseaux AD HOC

3.4.1 Classification des attaques

Dans les réseaux ad hoc, selon le niveau d'intrusion des actions menées par un attaquant, on distingue généralement deux catégories d'attaques : les attaques passives et les attaques actives[CHRIS & WANGER 2003].

Attaque passive

L'adversaire ne fait que surveiller les canaux de communication. Une écoute se produit lorsqu'un attaquant capture un noeud et étudie le trafic qui le traverse sans en altérer le fonctionnement. Les données analysées aident l'intrus à agir plus tard. Un adversaire passif ne fait que menacer la confidentialité des données[CHRIS & WANGER 2003].

Attaque Active

Une attaque est active lorsqu'un noeud non autorisé altère des informations de routage en transit par des actions de modification, suppression, ou fabrication, ce qui conduit à des perturbations dans le fonctionnement du réseau[CHRIS & WANGER 2003].

3.4.2 Présentation de quelques attaques

Contrefaçon d'information

L'attaque la plus directe contre un protocole de routage est de viser les informations échangées entre les noeuds. Les paquets du protocole de routage peuvent être contrefaits, altérés ou rejoués. Ce qui permet aux adversaires de créer des boucles, attirer ou repousser le trafic du réseau, prolonger ou raccourcir les itinéraires, produire de faux messages d'erreur, diviser le réseau, augmenter la latence, etc.[CHRIS & WANGER 2003]

Replay ou rejeu

Un noeud malicieux réinjecte des messages dans le réseau. Des anciens messages continuent à circuler ce qui occupe de la bande passante et peut même affecter la justesse de la topologie[CHRIS & WANGER 2003].

Spoofing ou usurpation d'identité

Consiste à se faire passer pour quelqu'un d'autre en utilisant son identité. L'attaquant se présente en utilisant l'identité d'un noeud légitime et peut ainsi communiquer avec les noeuds du réseau sans être rejeté[CHRIS & WANGER 2003].

Attaque du trou noir (sinkhole)

Dans une attaque sinkhole, le noeud malveillant essaye d'attirer vers lui le plus de chemins possibles permettant le contrôle de la plus part des données circulant dans le réseau. Pour ce faire, l'attaquant doit apparaıtre

aux autres comme étant très attractif, en présentant des routes optimales et fraiches . L'attaquant se place généralement à un endroit stratégique et supprime tous les messages qu'il doit retransmettre ou bien permet la mise en oeuvre d'une autre attaque. Créant ainsi une sorte de puits ou " trou noir " dans le réseau. [YINGSHU *et al.* 2008]

Trou de ver (Wormhole)

Dans une attaque wormhole, un attaquant reçoit des paquets dans un point du réseau, puis les encapsulent et les envoient vers un autre attaquant pour les réintroduisent dans le réseau. Dans ce genre d'attaque, les adversaires coopèrent pour fournir un canal à basse latence pour la communication en utilisant une fréquence radio pour communiquer avec une puissance plus élevée et des liens à longue portée. Ceci encourage les noeuds voisins à acheminer leurs données à travers l'attaquant. [ILYAS & MAHJOUB 2005] .

Attaque Sybil

Dans cette attaque, le noeud présente des identités multiples aux autres noeuds du réseau, créant ainsi des inconsistances dans les tables de routage des noeuds voisins. Cela permet de créer plusieurs routes passant par le noeud malicieux, qui ne sont en réalité qu'un seul chemin [CHRIS & WANGER 2003].

3.5 Vulnérabilité des réseaux véhiculaires

Les réseaux véhiculaires par leur nature représentent quelques faiblesses, certaines sont liées à la technologie sans fil et d'autres aux caractéristiques de ces réseaux [MEHDI *et al.* 2007].La première vulnérabilité de ces réseaux est liée à la technologie sans fil où l'utilisation des ondes radio permet aux attaquants d'intercepter facilement les messages échangés ou bien d'injecter de faux messages dans le réseau. De plus, les noeuds eux-mêmes sont des points de vulnérabilités du réseau car un attaquant peut compromettre un élément laissé sans surveillance. Les mécanismes de routage sont d'autant plus critiques dans les réseaux véhiculaires que chaque entité participe à l'acheminement des paquets à travers le réseau. De plus, les messages de routage transitent sur les ondes radio.

3.6 Attaques spécifiques sur les VANETs

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 décrits dans ce chapitre , 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[MEHDI *et al.* 2007].

Dans cette section, nous présentons des attaques spécifiques sur les VANETs, et les mécanismes de base qui ont été mis en oeuvre pour la sécurité de ces réseaux

Nous passons en revue quelques attaques spécifiques sur les VANETs. Ces attaques comprennent :

3.6.1 L'injection des messages erronés :

Dans cette attaque l'entité malveillante crée des messages contenant des informations erronées afin de causer un accident ou de rediriger le trafic routier de manière permettant la libération de la route utilisée[MEHDI *et al.* 2007].

3.6.2 Le déni de service :

L'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[MEHDI *et al.* 2007].

3.6.3 La révélation d'identité et de position géographique des autres véhicules

Dans cette attaque, l'entité malveillante collecte des informations sur les transmissions radio effectuées par le véhicule victime afin de surveiller sa trajectoire. L'utilité de cette attaque est diverse et dépend de l'entité collectant ces informations (elle peut être par exemple une entreprise de location de voitures qui veut suivre ses propres véhicules de manière illégitime)[MEHDI *et al.* 2007].

3.7 La qualité de service

Le terme QoS acronyme de « Quality of Service », en français « Qualité de Service » désigne la capacité à fournir un service (notamment un support de communication) conforme à des exigences en matière de temps de réponse et de bande passante.

Appliquée aux réseaux à commutation de paquets (réseaux basés sur l'utilisation de routeurs), la QoS désigne l'aptitude à pouvoir garantir un niveau acceptable de perte de paquets, défini contractuellement, pour un usage donné (voix sur IP, vidéoconférence,... etc).

En effet, contrairement aux réseaux à commutation de circuits, tels que le réseau téléphonique commuté, où un circuit de communication est dédié pendant toute la durée de la communication, il est impossible sur internet de prédire le chemin emprunté par les différents paquets.

Ainsi, rien ne garantit qu'une communication nécessitant une régularité du débit puisse avoir lieu sans encombre. C'est pourquoi il existe des mécanismes, dits mécanismes de QoS, permettant de différencier les différents flux réseau et réserver une partie de la bande passante pour ceux nécessitant un service continu sans coupures, on parle ici sur la garantie [OUAZENE 2009].

3.7.1 Niveaux de service

Le terme « niveau de service » (en anglais Service level) définit le niveau d'exigence pour la capacité d'un réseau à fournir un service point à point ou de bout en bout avec un trafic donné. On définit généralement trois niveaux de QoS : [OUAZENE 2009]

- **Meilleur effort** : (en anglais best effort), ne fournissant aucune différenciation entre plusieurs flux réseaux et ne permettant aucune garantie. Ce niveau de service est ainsi parfois appelé «lack of QoS».
- **Service différencié** : (en anglais differentiated service ou soft QoS), permettant de définir des niveaux de priorité aux différents flux réseau sans toutefois fournir une garantie stricte.
- **Service garanti** : (en anglais guaranteed service ou hard QoS), consistant à réserver des ressources réseau pour certains types de flux. Le principal mécanisme utilisé pour obtenir un tel niveau de service est RSVP (Resource reSerVation Protocol, traduisez Protocole de réservation de ressources).

3.7.2 Critères ou paramètres de qualité de service

Les principaux critères permettant d'apprécier la qualité de service sont les suivants : [JERBI 2008b]

- **Débit** : (en anglais bandwidth), parfois appelé bande passante ou largeur de bande par abus de langage, il définit le volume maximal d'information (bits) par unité de temps.
- **Latence, délai, retard ou temps de réponse** : (en anglais delay) elle caractérise le retard entre l'émission et la réception d'un paquet.
- **Gigue** : (variation de retard en anglais jitter) elle représente la fluctuation du signal numérique, dans le temps ou en phase.
- **Perte de paquet** : (en anglais packet loss) elle correspond à la non-délivrance d'un paquet de données, la plupart du temps due à un encombrement du réseau.
- **Déséquencement** : (en anglais desequencing) il s'agit d'une modification de l'ordre d'arrivée des paquets.
  Les paramètres de QoS débit, retard, gigue et taux de perte sont appropriés aux applications multimédias et aussi à la couche MAC :

Débit : Du point de vue d'application, le débit se rapporte au taux de données (bits par seconde) produit par l'application. Le débit, mesuré en nombre de bits par seconde, parfois s'appelle débit binaire ou largeur de bande. La largeur de bande est considérée pour être la ressource du réseau qui doit être correctement contrôlée et affectée aux applications.

Le débit exigé par une application dépend des caractéristiques de cette application. Par exemple, dans une application de streaming vidéo, les différentes propriétés visuelles produisent des débits différents [JERBI 2008b].

Retard : Le retard a un impact direct sur la satisfaction des utilisateurs. Les applications temps réel exigent la fourniture d'informations de la source à la destination dans une certaine période du temps[OUAZENE 2009].

Les retards longs peuvent entraîner des incidents qui réduisent alternativement la fidélité de vidéo.

D'ailleurs, il peut entraîner l'anéantissement (frustration) d'utilisateur pendant des tâches interactives. Quand le trafic de données est porté à travers une série de composants dans un système de communication qui interconnecte la source et la destination, chaque composant introduit un retard [JERBI 2008b].

Nous pouvons classer les sources principales de retard comme suit :

1. Retard de traitement de la source : (retard de numérisation et de mettre dans des paquets) : Ce retard, qui est introduit par la source qui produit des paquets, dépend de la configuration matériel de serveur de source (puissance CPU, RAM, carte mère, etc.) et de son chargement actuel (par exemple, le nombre de demandes fonctionnant simultanément et leurs ressources de matériel requises).
2. Retard de transmission :La période de transmission d'un paquet est une fonction de la longueur de paquet et de la vitesse de transmission.
3. Retard de réseau : On définit quatre classes pour le retard de réseau :
4. Retard de propagation : Le délai de propagation de la source à la destination est une fonction de la distance physique entre la source et la destination.
5. Retard de protocole : Le retard est causé par les protocoles de communication exécutés aux différentes parties du réseau telles que des routeurs, des passerelles, et des cartes d'interface réseau. Le retard dépend des protocoles, de la charge du réseau, et de la configuration matérielle qui exécute le protocole.
6. Retard de la file d'attente de sortie : Le retard est causé par le temps passé dans la file d'attente de sortie de lien avant qu'un paquet dans une partie du réseau. Par exemple, un tel retard peut être encouru à une file d'attente de sortie intermédiaire d'un routeur. Le retard dépend de la congestion du réseau, de la configuration du matériel, et de la vitesse de lien.
7. le retard de traitement de la destination :Ce retard est introduit par le traitement exigé à la destination. Par exemple, un tel retard peut être encouru dans le processus de reconstruction de paquet. Semblable au retard de traitement à la source, ce retard dépend de la configuration matérielle et de la charge de destination.
8. Gigue : La gigue est une métrique de QoS qui se rapporte à la variation du retard introduit par les composants le long de chemin de communication. Puisque chaque paquet dans le réseau prend des chemins différents, et les conditions du réseau peuvent être différents pour chaque paquet, le retard de bout en bout varie.

   Pour des données produites au débit constant, l'instabilité de retard déforme la synchronisation du trafic original.

   Les paquets voyagent par le réseau et éprouvent différents retards de bout en bout, atteignant la destination avec des déformations de synchronisation (signal inachevé ou différé) relativement au trafic initial [OUAZENE 2009].

9. Taux de perte ou d'erreur : La perte de paquets affecte directement la qualité perçue de l'application. Elle compromet l'intégrité des données et perturbe le service. Au niveau de réseau, la perte de paquets peut être causée par la congestion du réseau, qui a comme conséquence les paquets rejetés. Une autre cause de la perte est provoquée par les erreurs de bit qui se produisent en raison d'un canal de communication bruyant. Une telle perte se produira très probablement dans un canal sans fil. Il y a plusieurs techniques pour recouvrir la perte ou l'erreur de paquets telle que la retransmission de paquet, correction d'erreurs à la couche physique, ou au code à la couche application qui peut compenser ou cacher la perte [OUAZENE 2009].

3.8 Conclusion

Au cours de ce chapitre, nous avons abordé les aspects liés à la sécurité dans les réseaux, les particularités des réseaux sans fil et les mécanismes de sécurité : l'authentification, l'intégrité, la non-répudiation, etc. Ainsi nous avons abordé une des solutions les plus fiables pour sécuriser un réseau informatique le PKI (Public Key Infrastruture) ou infrastructure de clés publiques qui est un système de certificats numériques, qui émet les clés de chiffrement utilisées pour la signature électronique et pour le chiffrement des données. Ce qui garantit l'authentification et la confidentialité des communications.

Toutes les techniques étudiés dans ce chapitre, satisfont les besoins de la sécurité comme l'authentification, l'intégrité, la confidentialité, la non-répudiation... etc. En revanche, ils présentent quelques inconvénients .

Dans le chapitre suivant on présentera notre solution pour assurer la sécurité dans les VANETs, la solution se consacre à réaliser un besoin de la sécurité qui est l'authentification en plus aux autres exigences, et répond aux faiblesses des protocoles précédents.

4 Détection et prévention des attaques blackholes dans les réseaux véhiculaires

Sommaire

4.1 inroduction 46
4.2 Attaques contre le protocole AODV 46
4.3 blackhole attack (problématique) 47
4.4 état de l'art 48
4.5 Nos propositions de détection et préventions des blackholes dans les VANETs 51
4.5.1 Détection à base de temps de latence 51
4.5.2 Détection à base de l'étude de comportement de chaque noeud 52
4.6 Les performances réseau 54
4.7 Les résultats de simulation 54
4.7.1 Approches implémentés 54
4.7.2 Les résultats de simulation 55
4.8 Conclusion 57

4.1 INRODUCTION

Dans les réseaux véhiculaires la sécurité pose un grande problème et un défis majeur pour dans la conception architecturale des réseaux et la conception des protocoles de communication. Les services de sécurité se diffèrent selon les fonctions des applications et comprennent en générale défirent mécanismes tel que la confidentialité, l'authenticité, l'intégrité, la non-répudiation, la disponibilité, la cohérence des données. Ces mécanisme et conçus pour détecté, prévenir ou contrer une attaque de sécurité.

4.2 Attaques contre le protocole AODV

Parmi les nombreux protocoles de routage qui ont été développés pour permettre l'auto configuration et le routage dans les réseaux MANETs, le protocole AODV (Ad-hoc On-demand Distance Vector) a émergé comme l'un des plus populaires. Il a été le sujet de beaucoup de recherches universitaires . Ce protocole a été développé avec l'hypothèse que tous les noeuds du réseau sont honnêtes et coopératifs. Par conséquent, il existe de nombreuses vulnérabilités dans l'AODV qui permettent aux noeuds malveillants de perturber son fonctionnement.

Une analyse compréhensive des attaques possibles contre le protocole AODV a été présentée par [P.NING & K.SUN 2003] .

Ils classent les attaques en deux catégories : atomiques, qui représentent des manipulations indivisibles sur un seul message de routage et composés, qui représentent une collection d'attaques atomiques.

Ils décrivent en détails les scénarios dans lesquels le noeud malveillants exécute des attaques atomiques et composés sur les messages de routage. Ils identifient les quatre attaques atomiques suivantes [P.NING & K.SUN 2003] :

1. Suppression illégitime de messages ;
2. Modification illégitime d'un ou plusieurs champs d'un message avant de le retransmettre .
3. Fabrication d'une réponse de route suite à la réception d'une demande de route RREQ.
4. Fabrication active, ou la fabrication des messages n'est pas conditionné par la réception d'un message de routage

Dans notre travail on s'intéresse à une attaque de type "Suppression" , dans lequel on décrive trois type [GUERRORO & ASOKAN 2002]

1. Suppression de demande de route RREQ :Le noeud malveillant pourrait simplement supprimer toutes les demandes de route reçues. Par conséquent il ne fera pas partie des routes découvertes, et il n'aura aucun impact sur le routage. Dans certain cas le noeud malveillant supprime certaines demandes de routes pour ne pas consommer ses ressources dans le processus de routage des données appartenant aux autres noeuds, ce comportement est appelé dans la littérature égoïsme (selfishness).
2. Suppression de réponse de route RREP : Une fois le noeud malveillant est sélectionné sur la route entre la source et la destination,

il peut supprimer la réponse de route qu'il reçoit pour empêcher l'établissement de la route vers la destination. La suppression de la réponse de route engendre du trafic supplémentaire, et occasionne un délai plus long pour l'établissement de routes.

3. Suppression d'erreur de route RERR :Le noeud malveillant supprime les messages d'erreur de route RERR qu'il reçoit pour retarder la détection des liaisons défaillantes et par conséquent engendrer des retards de livraison .

4.3 BLACKHOLE ATTACK (PROBLÉMATIQUE)

L'attaque Blackhole [ABDELHAQ *et al.* 2011] est une attaque active dans la couche réseau de type DoS (voir figure 4.1) ,elle peut s'effectuer au moment ou un noeud source initie un processus de découverte de route en émettant un paquet RREQ. Le noeud destination va répondre par un paquet RREP avec un numéro de séquence non seulement erroné mais également élevé afin d'augmenter ses chances de faire partie de la route. En effet, si son paquet RREP atteint la source il peut s'intégrer dans la route pour intercepter et contrôler une partie ou la totalité du trafic échangé au sein du réseau, de façon à pouvoir surveiller, bloquer ou même détourner certains flux du trafic. Le trafic absorbé disparaître complètement.

Cette attaque est grave dans la mesure où les nœuds légitimes vont mettre à jour leurs tables de routage avec des informations fausses et le nœud malveillant n'a pas besoin d'intervenir une seconde fois.

La figure ci-dessous illustre cette attaque où la source 1 veut transmettre des données vers la destination 3, elle diffuse une requête RREQ (Route REQuest), le paquet RREQ va être reçu par les nœuds 2,4,5,6.

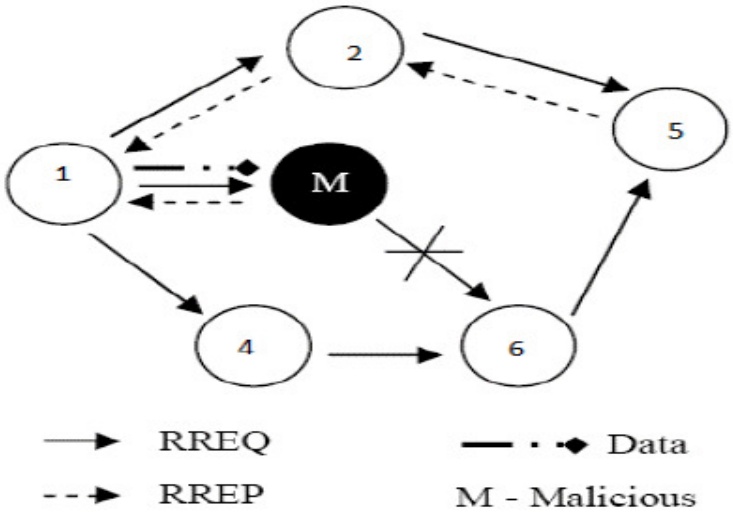

FIGURE 4.1 – *l'attaque blackhole*

4.4 ÉTAT DE L'ART

Plusieurs solutions ont été proposées pour pallier des problèmes de sécurité dans les réseaux sans fil (ad hoc ou Vanet). Dans cette section nous allons présenter les différentes propositions dans la littérature pour éviter l'attaque Blackhole :

Les auteurs dans [REN *et al.* 2002] ont proposé une solution contre l'attaque trou noir en modifiant le protocole AODV. Dans cette méthode chaque nœud intermédiaire doit inclure l'information« next hop » quand il envoie un paquet RREP. Une fois la source a reçu le paquet RREP et avant d'envoyer les paquets de données, il extrait l'adresse du « next hop » et lui envoie une nouvelle demande de route (Further Request) afin de vérifier qu'il possède une route vers le nœud intermédiaire qui a envoyé le message de réponse, et qu'il a aussi une route vers le nœud destination. Le « next hop » répond avec un paquet de réponse de route (Further Reply) qui comprend le résultat de contrôle. La source vérifie les informations des paquets FRREP et agit selon les règles suivantes :

1) Si le « next hop » possède une route vers le nœud intermédiaire et la destination, la source établit la route reçu du nœud intermédiaire et commence l'envoi des données.

2) Si le « next hop » a une route vers la destination, mais n'a pas de route vers le nœud intermédiaire, la source suppose que le nœud intermédiaire est un nœud malicieux.Ensuite, elle initie l'envoi des données via la nouvelle route à travers le next hop et diffuse un message d'alarme dans le réseau afin d'isoler le nœud malveillant.

3) Si le « next hop » n'a pas de routes vers le nœud intermédiaire et la destination, la source lancera un nouveau processus de découverte de route, et envoie également un message d'alarme afin d'isoler le nœud malveillant.

Les auteurs dans [MANDHATA & PATRO 2011]ont proposé un algorithme simple qui n'affecte pas le fonctionnement du protocole AODV, cependant, le protocole effetue un prétraitement sur les paquets RREP appelé Pre Process RREP. Le processus continu d'accepter les paquets RREP et fait appel à une procédure de comparaison -Compare Pkts (p1 paquet, p2 paquet) - qui compare effectivement les numéros de séquence de destination des deux paquets et sélectionne le paquet avec le numéro de séquence de destination d'ordre supérieur. Si la différence entre les deux numéros est élevée, le paquet contenant le numéro de séquence de destination exceptionnellement élevé est soupçonné d'être reçu de la part d'un noeud malveillant. Un message d'alerte contenant l'identifiant du noeud est généré, et diffusé vers les noeuds voisins de telle sorte que tout message reçu à partir du noeud malveillant sera rejeté. Une liste des noeuds malveillants peut être maintenue par les noeuds qui participent à la communication pour prévenir d'une attaque trou noir. dans cette méthode le problème est que lorsqu'un noeud reçoit un paquet RREP d'un noeud malveillant la comparaison n'a pas d'importance car le principe de leur algorithme est basé sur la comparaison des numéros de séquence entre deux paquets pour détecter la valeur non significative.

Les auteurs dans [SHRMAN *et al.* 2004] ont proposé deux solutions conçues pour cibler l'attaque Blackhole dans le protocole AODV. La pre-

miére solution proposée consiste à trouver plus d'une route vers la destination (au moins trois routes différentes). La station source envoie un paquet RREQ au noeud destination en utilisant ces trois routes. Le noeud destination, le noeud malicieux et les noeuds intermédiaires vont répondre à ce paquet. Le noeud expéditeur met ses paquets de données dans un tampon jusqu'à ce qu'il reçoit plus d'une réponse RREP ; lorsque la station source reçoit des RREP, si les routes menant à la station destinatrice ont des noeuds partagés, la station source peut reconnaître une chemin sûr vers la destination, et les paquets vont être transmis. Si aucun noeud partagé ne semblent être dans ces routes redondantes, le noeud source attendra un autre paquet RREP jusqu'à ce qu'un chemin avec des noeuds partagés sera trouvé ou le temps d'attente s'expiré. Cette solution peut garantir de trouver une route sécurisé vers la destination,mais le principal inconvénient est le délai d'attente. Plusieurs paquets RREP doivent être reçues et traitées par la station source. En outre, s'il n'ya pas de noeuds partagés entre les routes, les paquets ne seront jamais envoyé. La seconde solution proposée exploite le numéro de séquence inclus dans l'en-tête de chaque paquet. Le noeud dans cette situation à besoin d'avoir deux tables supplémentaires ;la premiére table comprend les numéros de séquence du dernier paquet envoyé à chaque noeud dans le réseau. La deuxiéme table contient le numéro de séquence reçu de chaque expéditeur. Pendant la phase de découverte de route, le noeud intermédiaire ou le noeud destination doit inclure le numéro de séquence du dernier paquet reçu de la station source qui a déclenché la demande de route. Une fois que le noeud source reçoit ce RREP, il extrait le dernier numéro de séquence, puis le comparer avec la valeur enregistrée dans sa table. Si les deux valeurs correspondent, la transmission aura lieu. Dans le cas echéant, le noeud correspondant est un noeud malveillant.Un message d'alarme sera diffusé pour révéler l'identité de ce noeud dans le réseau. Les deux solutions ont le délai de bout en bout comme inconvénient

Les auteurs dans [HIMRAL *et al.* 2011] ont proposé une méthode pour trouver les routes sécurisées et isoler les noeuds malveillants dans les MANET en vérifiant s'il existe une différence importante entre le numéro de séquence du noeud source et le noeud intermédiaire qui a envoyé la première RREP. En règle générale, la première réponse sera du noeud malveillant avec un numéro de séquence de destination très élevée, dans Ensuite, la station source va comparer le premier numéro de séquence de destination reçu avec son numéro de séquence, s'il existe une grande différence entre eux, certainement cette réponse vient du noeud malveillant, par conséquent, il va supprimer cette entrée de la table. La méthode proposée offre les avantages suivants :

1. Le noeud malveillant est identifié dans la phase initiale et il est retiré immédiatement.
2. Aucune modification n'est faite dans les autres opérations du protocole AODV.
3. Une meilleure performance en légère modification.

la méthode ne peut pas trouver de multiples noeuds malicieux.

Les auteurs dans [PAYAL *et al.* 2009] ont proposé la modification du comportement du protocole AODV pour inclure un mécanisme permet-

tant de vérifier le numéro de séquence de destination inclut dans le paquet RREP reçu. Quand le noeud source reçoit un paquet RREP, il compare le numéro de séquence du RREP reçu à une valeur de seuil. Un noeud répondant sera soupçonné d'être un trou noir si son numéro de séquence est supérieur à la valeur de seuil. Le noeud source ajoute le noeud suspect à sa liste noire, et propage un message de contrôle appelé une alarme contenant la liste noire pour informer ses voisins. Le seuil est une moyenne calculée à base de la différence entre le numéro de séquence de destination dans la table de routage et le numéro de séquence de destination dans le RREP dans une période de temps. Le principal avantage de ce protocole est que le noeud source annonce le trou noir à ses voisins afin d'être ignoré ou supprimé.

Le seuil est la moyenne calculée entre le numéro de séquence de destination dans la table de routage et le numéro de séquence de destination dans le RREP dans une période de temps

Selon la solution proposée par [TAMIL & NARAYANAN 2007] la source doit attendre d'autres réponses avec des détails sur le prochain saut avant d'envoyer les paquets de données vers la destination. Une fois un nœud a reçu la première RREQ, il fixe un temporisateur « timer » dans le "Timer Expired Table" pour collecter les nouvelles demandes venant des différents nœuds et les stocker dans un ordre séquentiel, la source va stocker le « numéro de séquence», et « le moment d'arrivé du paquet » dans « Collect Route Reply Table » (CRRT). La valeur "timeout" est basée sur le temps d'arrivé du premier RREQ. Elle vérifie d'abord dans la table CRRT afin de déterminer s'il existe un next hop répété dans les réponses de route reçus, dans ce cas il assume que les chemins sont corrects ou la chance de chemins malveillants est limitée. S'il n'ya pas de répétition, une route aléatoire est sélectionné de la table CRRT. L'inconvénient de la solution proposée est le délai de bout en bout, puisque le nœud source doit attendre d'autres réponses de route avant d'envoyer les données.

Les auteurs dans [VANI & RAO 2011] ont proposé une solution pour le problème d'attaque blackhole qui est la comparaison du numéro de séquence le plus élevé avec la valeur du seuil. Dans AODV, quand le noeud source reçoit un paquet RREP , il va vérifie d'abord la valeur du numéro de séquence dans sa table de routage ; la station source accepte le paquet RREP si le numéro de séquence qui est dans le RREQ est supérieure au numéro de séquence qui est dans la table de routage. Leurs solution ajoute une valeur de seuil pour savoir le numéro de séquence de destination dans le paquet RREP le plus élevé dans chaque intervalle de temps. Si la valeur du numéro de séquence est plus élevée que la valeur du seuil, le noeud est soupçonné d'être malveillant, il sera ajouté à la liste noire et tous les messages de réponse arrivant à travers ce noeud seront rejetés. Dans leurs simulation, si le RREQ est reçu par le trou noir, il va générer RREP avec :

— Numéro de séquence le plus élevé = 1000

— Numéro de séquence différence = 50

l'attaque à trou noir basé sur le numéro de séquence est un mot de 32 bits, ce dernier il peut atteint jusqu'au 4294967296 et dans cet article ils ont proposés que la valeur maximal est 1000 qui est un inconvénient. La valeur de seuil doit être mis à jour dans un intervalle de temps,qui va

être : la valeur mis à jour malgré que le numéro de séquence maximum n'a pas été atteint le seuil.

4.5 Nos propositions de détection et préventions des blackholes dans les VANETs

Comme nous avons vu dans la section précédente diverses solutions ont été proposées pour la sécurisation des réseaux VANETs contre l'attaque Blackhole. L'objectif principal de cette partie est de présenter nos contributions dans le cadre de ce mémoire. Nous commençons d'abord par une description des protocoles proposés, ensuite nous discutons de l'environnement utilisé pour l'implémentation des solution, enfin, nous analysons les performances de nos protocoles avec les différentes simulations.

4.5.1 Détection à base de temps de latence

Dans cette approche [BENSAID *et al.* 2016] nous allons étudié l'effet de l'attaque blackhole sur un réseau Vanet de type V2V. en plus nous allons proposé une approche basée sur le temps de latence,qui est le délai minimum de transmission ; elle se référe à la durée nécessaire pour qu'un paquet atteint sa destination dans un réseau. Dans notre solution, Chaque fois qu'un noeud reçoit un RREP, il va mesurer la valeur de latence par la formule suivante :

$$Latency.time = Current.time - \frac{time.Stamp}{Hop.count} \tag{4.1}$$

1. time.stamp = le moment quand le RREQ correspondant est envoyé.
2. Hop.count = le nombre de sauts.

Notons que si un voisin d'un noeud blackhole envoi un RREP,cette valeur de latence doit être égale à :

$$Latency.time = Current.time - time.Stamp \tag{4.2}$$

Par conséquent, si la valeur hop count = 1, le temps de latence est faible. Sinon, la valeur de latence augmente. Donc, si la valeur de latence est faible, la RREP est envoyé par un voisin direct ou par un noeud Blackhole. Après cela, nous allons comparer la différence entre les numéros de séquence destination dans la table de routage du noeud source et de destination dans le paquet RREP, si elle est grande, alors le noeud corres-

pondant est un noeud Blackhole. l'algorithme suivant (voir l'algorithme 1) présente l'idée générale de notre solution.

Algorithme 1 : détecter une attaque blackhole

```
MT : table malicious node ;
RT : routing table ;
P : RREP table ;
Src.IP : source IP adress ;
Dst.seq.no : destination sequence number ;
Src.seq.no : source sequence number ;
RecvReply()
if Src.IP in MT then
    drop (P);
end
if latency < 0,5 then
    if Dst.seq.no »> Src.seq.no then
        detect.blackhole.attack(Src.IP);
        add.in.MT(Src.IP);
        drop(P);
    end
    continue;
end
continue;
.
```

4.5.2 Détection à base de l'étude de comportement de chaque noeud

La notion de confiance s'est appliquée dans les télécommunications avec la notion de connaissance au préalable des identités. Mais aujourd'hui le développement de nouveaux modèles de communication tels que les réseaux ad hoc, les réseaux Vanets, rendent cette vision de la confiance obsolète. En outre la confiance n'est pas un problème technique, elle est un problème social à opposer à la notion de sécurité : on a besoin de confiance lorsque la sécurité n'est pas suffisante. Nous envisageons de proposer un nouveau protocole basé sur l'utilisation d'un modèle de confiance capable d'assurer les échanges sécurisés dans les réseaux véhiculaires, tout en tenant compte des caractéristiques de ces réseaux on se basant sur l'étude du comportement globale de chaque noeud.

Dans notre modèle [BENSAID *et al.* 2015], et afin d'évaluer le degré de confiance d'un nœud, chaque nœud dans le réseau maintient une table d'activité, dans cette table il sauvegarde l'identifiant d'un nœud, le nombre des paquets de données, le nombre des paquets de demande de route (RREQ) et le nombre des paquets de réponse (RREP) reçus de ce nœud. Quand un nœud légitime reçoit un paquet, selon le type du paquet reçu, il augmente le nombre dans sa table d'activité.

Si le paquet reçu est de type RREP, il consulte sa table d'activité pour utiliser l'algorithme ci-dessous, selon les valeurs stockées dans cette table, il décide si le nœud est un nœud de confiance ou bien non

A chaque fois qu'un nœud blackhole reçoit un paquet de données, il le supprime directement, ainsi quand il reçoit un paquet RREQ, il répond

en envoyant une fausse RREP sans consulter sa table de routage et il ne rediffuse pas le RREQ vers les autres nœuds. En se basant sur ce comportement, un nœud légitime ne recevra aucun paquet de données ou bien un paquet RREQ d'un nœud malicieux, il reçoit que des paquets de réponse RREP, par conséquent, Un noeud de blackhole possède les caractéristiques suivantes :

1. Un nombre de sauts égal à 1 et un numéro de séquence élevé.
2. le nombre de paquet RREQ envoyé par le blackhole est nul.
3. le nombre de paquets de données envoyées par le blackhole est nul.
4. Un nombre élevé de paquets RREP.

A l'aide de ces informations, on génére une "cache mémoire" distribuée entre les noeuds qui doit être mis à jour à chaque changement dans la topologie, chaque noeud qui détecte un changement dans la topologie . la cache mémoire contient n colonnes et 2 lignes, tel que n représente le nombre de noeuds dans le réseau, et les lignes sont représentés par :

1. N.RREQ : le nombre de RREQ envoyés par le noeud X
2. N.DATA : le nombre de données envoyés par le noeud X.

Si un noeud reçoit un RREP, il va utiliser le diagramme suivant (voir figure 4.2) pour détecter le blackhole

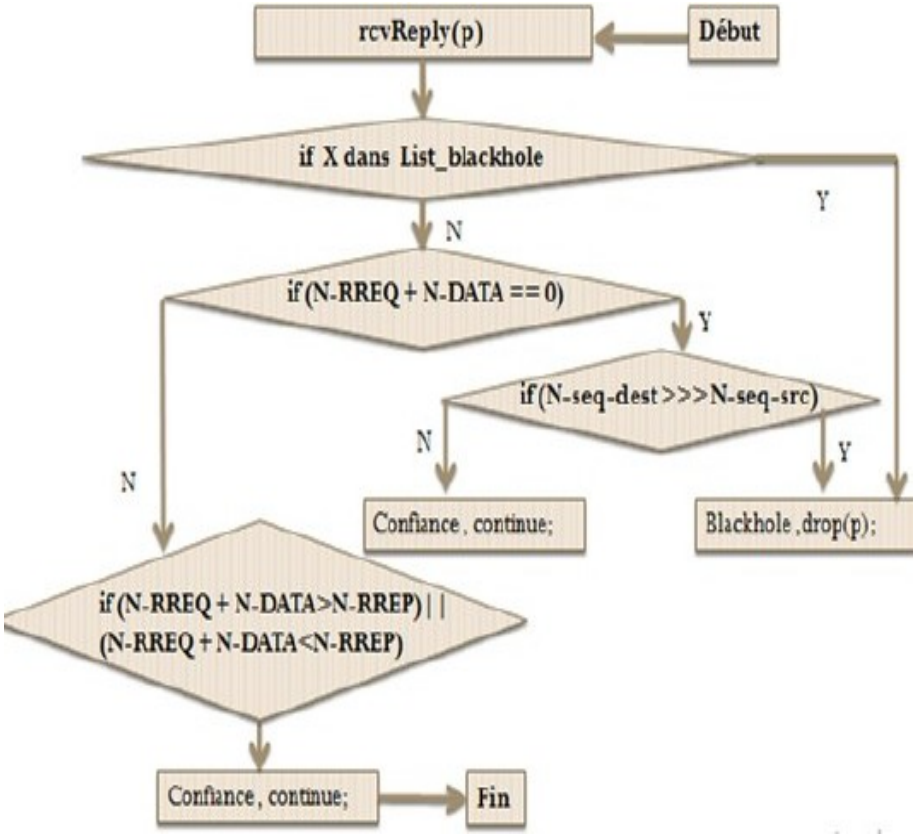

FIGURE 4.2 – *Diagramme de détection de blackhole*
.

4.6 Les performances réseau

Les métriques sont des paramètres de test du protocole de routage qui permettent de mesurer les performances de celui-ci a bases des quelles la comparaison entre les protocoles sera effectuée. Dans notre étude, nous avons pris en compte les métriques suivantes : [Meraihi 2011]

Le taux de délivrance des paquets de données (delivery ratio) :

Ce paramètre représente le pourcentage des paquets livrés à leurs destinations par rapport aux paquets émis dans le réseau.

Calcul du taux de surcharge de routage (Normalized Routing Load) :

La surcharge du réseau permet de mesurer le taux de paquets de contrôle de routage dans le réseau par rapport au nombre total de paquets reçus. Nous avons donc la formule suivante :

Surcharge = nombre de paquets de contrôle de routage / le nombre total des paquets reçus.

Ce taux est recalcule a chaque émission ou réception d'un paquet au niveau de la couche Internet. Le calcul de surcharge de routage est important pour déterminer la nature des paquets qui occupe le réseau.

La moyenne de temps de latence des paquets de données (average end to end delay) :

C'est la moyenne des temps nécessaires pour livrer les paquets de données de la source à la destination avec succès, incluant les temps de latence dans les files d'attentes, le temps de stockage dans les tampons,... etc.

Paquets perdus (Dropped packets) :

C'est le nombre de paquet ignoré par le noeud blackhole ou bien perdu suite à une déconnexion d'un noeud (véhicule).

4.7 Les résultats de simulation

4.7.1 Approches implémentés

On a effectué la simulation de quatre protocoles :
- AODV sans attaque.
- AODV avec attaque blackhole.
- Notre première approche.
- Notre deuxième approche.

4.7.2 Les résultats de simulation

Pour les simulations, on a utilisé le simulateur réseau NS-2 (V-2.35), dans lequel on a utilisé le protocole IEEE 802.11ext, Le canal utilisé est le canal sans fil avec un modèle de propagation radio Nakagami. Lors de la couche réseau, nous utilisons AODV comme un protocole de routage. Enfin, UDP est utilisé dans la couche de transport. Tout les paquets de données sont de type CBR (débit continu). La taille du paquet est de 512 octets. Le taux de transmission des paquets est de 4 paquets/seconde. La zone géographique est 2Km * 1Km avec un nombre de véhicules variant de 10 à 60.Les paramètres de simulation sont résumés dans le tableau suivant :

paramétres	valeur
Nombre de noeud	10,15,20,30,45
Noeud Blackhole	2
Type de trafics	CBR
Taille de paquet	512 octets
Temps de simulation	180 s
Modèle de propagation radio	Propagation/Nakagami
Protocole de routage	AODV

TABLE 4.1 – *paramètres de simulation.*

Le taux de délivrance des paquets de données :

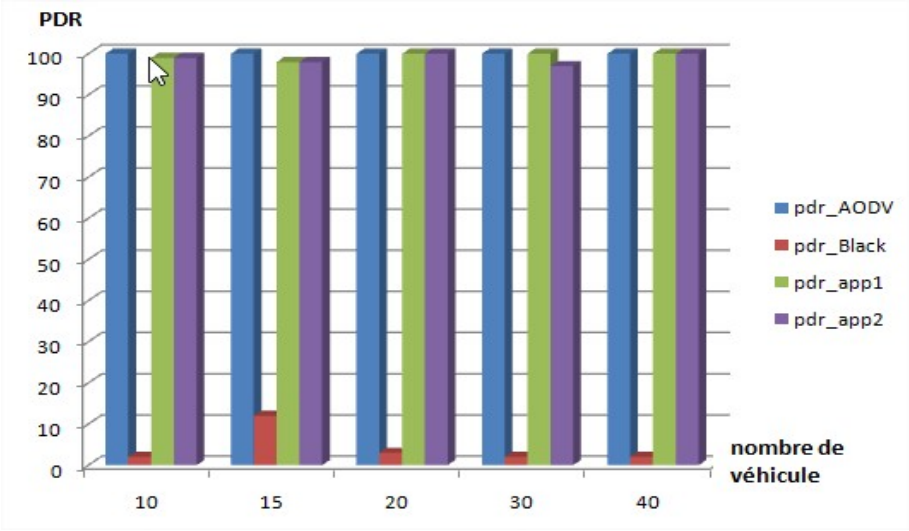

FIGURE 4.3 – *l'effet de PDR*

La figure 4.3 représente l'évolution du taux de paquets délivrés avec succès dans les cas ou les noeuds exécutent : AODV sous l'attaque blackhole, AODV sans l'attaque blackhole , ainsi nos approches. L'observation de cette figure montre l'évolution faible de PDR du protocole AODV sous l'attaque par rapport nos approches proposées,On observe aussi que si

le nombre de véhicules augmente le PDR augmente pour nos solutions jusqu'au 99.92

— Les coûts additifs (Normalized Routing Load) :

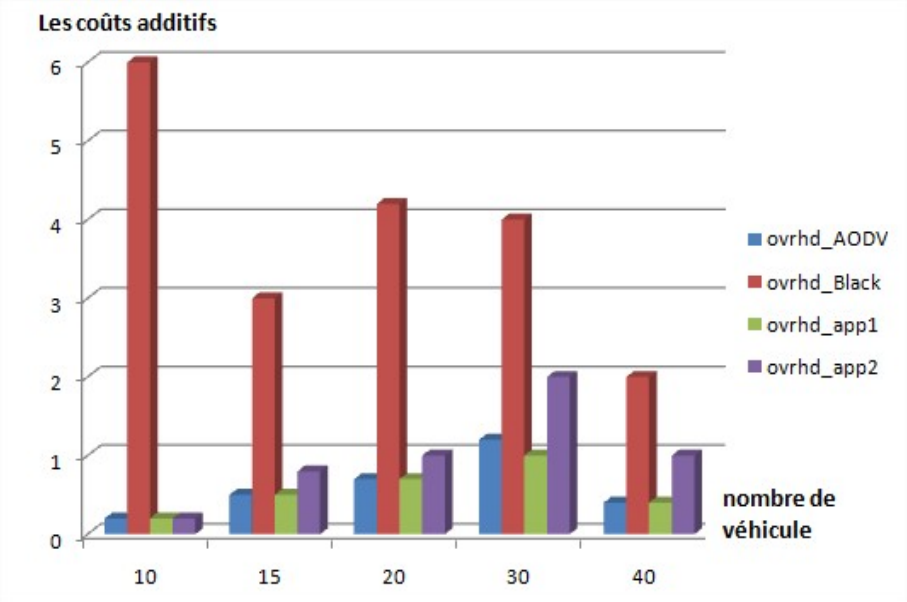

FIGURE 4.4 – *Les coûts additifs*

L'observation de la figure 4.4 montre l'évolution du trafic de contrôle en fonction de nombre de véhicules, Nous remarquons que l'approche 2 génère plus de trafic de contrôle.

— La moyenne de temps de latence des paquets de données (average end to end delay) :

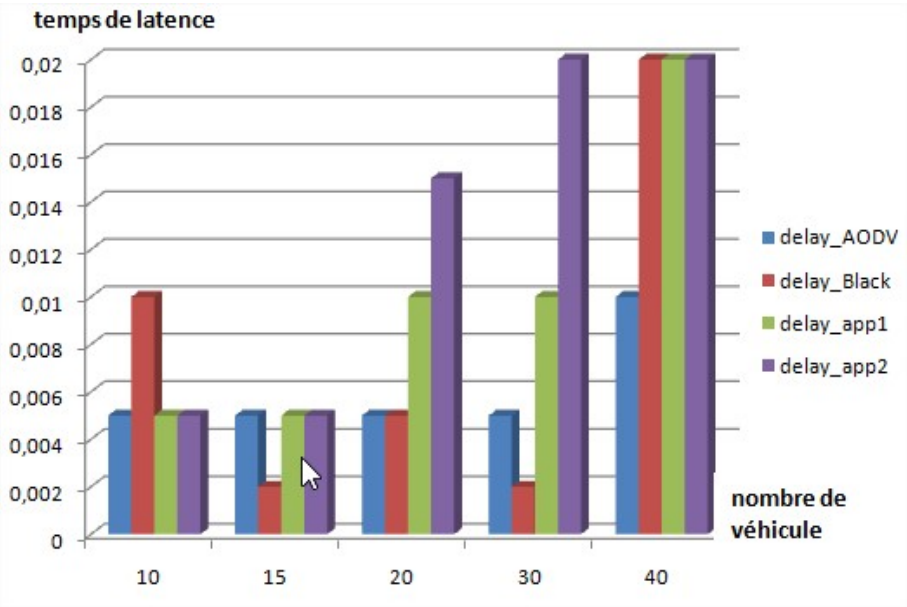

FIGURE 4.5 – *La moyenne de temps de latence des paquets de données VS nombre de véhicules*

La figure 4.5 montre l'évolution du délai moyen de bout en bout en

fonction de nombre de véhicules. On constate que le délai requis pour nos approches est supérieur à celui d'AODV sous l'attaque. Effectivement parce que les deux solutions utilisent des traitements en plus pour établir des routes assurées en évitant les noeuds malicieux, cela a un impact sur le délai de bout en bout. On observe aussi que le délai de bout en bout apporté par la deuxième l'approche est supérieur aux l'autre solution grâce au temps écoulé par le processus de mis à jour de la cache mémoire.

— Paquet Perdues :C'est le nombre de paquet ignoré par le noeud blackhole ou bien perdu suite à une déconnexion d'un noeud (véhicule).

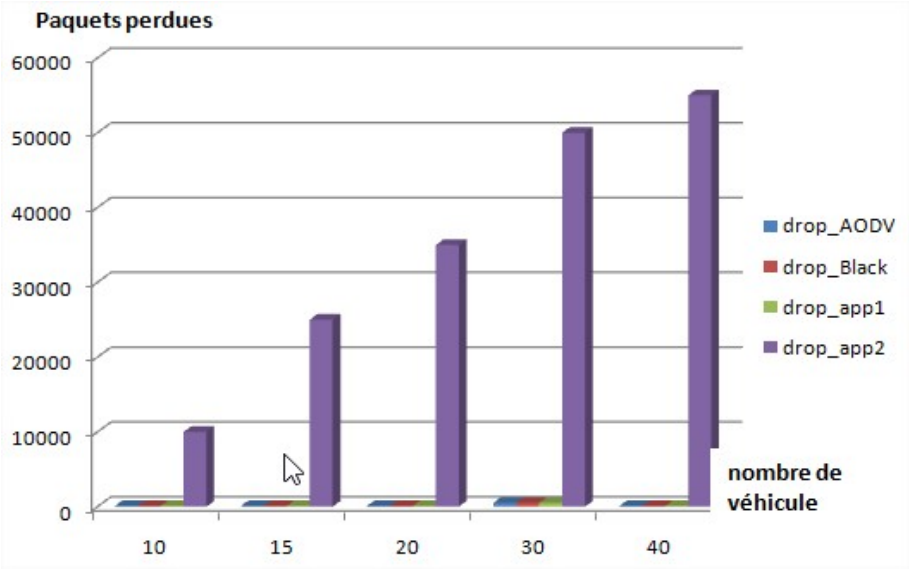

FIGURE 4.6 – *Les paquets Perdues VS nombre de véhicules*

La figure 4.6 représente le taux de paquets supprimé en fonction de nombre de véhicules, on observe que si le nombre de véhicules augmente,le nombre de paquets supprimé par le noeud malicieux augmente jusqu'au 53429 paquets dans le protocole AODV sous l'attaque blackhole. Dans les deux autres protocoles , ce nombre de paquets supprimé est inférieur par rapport au protocole AODV sous l'attaque, il diminue jusqu'au 69 si le nombre de véhicules est égal à 10.

4.8 Conclusion

Ce chapitre a fusionné les divers travaux liés aux mécanismes de détection de l'attaque Blackhole, les auteurs ont donné plusieurs propositions pour la détection et la prévention de cette attaque, chacune a ses proposes avantages et inconvénients.

Après avoir passé en revue les résultat de simulation nous avons remarqué une meilleure amélioration des performances grâce à nos approche pour détecter les noeuds malicieux et sécuriser l'échange de données dans les réseaux véhiculaires.Nous avons constater qu'il ya des améliorations nous avons discuté les résultats de simulation sous formes de graphes.

Gestion des certificats dans les réseaux véhiculaires 5

Sommaire

5.1 introduction 59
5.2 Distribution partielle des autorités de certification . 59
5.3 Les chaines de certificats 61
5.4 Chainage de certificats basé sur les clusters 62
5.4.1 L'accord des certificats 62
5.4.2 Renouvellement des certificats 63
5.4.3 Notre proposition 64
5.4.4 calcule de valeur de confiance 64
5.4.5 clustering 65
5.4.6 Certification 65
5.4.7 Transfert du certificat 66
5.4.8 Renouvellement du certificat et révocation du certificat . 66
5.5 Les résultats de simulation 67
5.5.1 le scenario le la ville de Malaga 68
5.5.2 scenarios de VANETmobisim 69
5.6 Conclusion 73

5.1 INTRODUCTION

Malgré l'évolution de Manet durant les dernières années, il y a encore un certain nombre de problèmes liée à la sécurité qui sont ouverts [CAPKUN & HUBAUX 2003], cela veut dire que la majorité mais pas la totalité, ne satisfait pas à tout les contraintes de Manet.Un protocole de routage peut utiliser différents mécanismes de sécurité pour diminuer les attaques sur l'infrastructure de routage. Certain de ces mécanismes sont : l'exploitation des redondances, diversité de codage, découverte de la route à la demande, techniques de maintenance des routes et les mécanismes de cryptographie.Tous ces différents mécanismes ont un certain degré d'efficacité qui dépend du mécanisme. Il est connu que les mécanismes de cryptographies peuvent fournir des techniques puissantes pour garantir la disponibilité, l'intégrité et la confidentialité des informations de routage.

Plusieurs classifications ont été déduites par les auteurs d'après les publications pour les protocoles actuelles :

- Distribution partielle des autoritées de certification .
- Distribution entière des autoritées de certification .
- Gestion de clé basée sur l'identité.
- Gestion de clé basée sur les clusters .
- Gestion de clé basée sur le prée-déploiement .
- Gestion de clé basée sur la mobilité .
- Gestion de clé parallèle .

La majorité de ces auteurs utilisent la cryptographie à clé publique à cause de leur supériorité dans la distribution des clés. On va s'intèresse maintenant à certains cas de ces propositions.

5.2 DISTRIBUTION PARTIELLE DES AUTORITÉS DE CERTIFICATION

La première approche pour résoudre les problèmes de gestion des clés dans Manet est publiée par [ZHOU and HAAS 1999], cette approche été étendue par [Yi & KRAVET 2004].

[ZHOU and HAAS 1999] ont proposé une distribution de gestion de clé publique dont la confiance est distribuée sur un ensemble des noeuds, ces noeuds partagent le secret de système (clé privée) basé sur la cryptographie à seuil. La distribution des autorités de certification DCA est constituée de n serveurs ; le système entier a une paire de clés publique/privée K/k , la clé publique K est connue par tout les noeuds dans le réseau tandis que la clé privée k est divisé en n parties (s1, s2, s3, . . . , sn), une pour chaque serveur. Cette distribution des autorités de certification signe des certificats par groupe de signature, comme le montre la figure 5.1, chaque serveur génère une portion de signature avec sa clé privée partagée et envoie cette dernière a un combinnateur C. Ce dernier peut être n'importe quel serveur et nécessite au moins t+1 signatures pour reconstruire le certificat.

Les noeuds qui ont besoin d'un certificat, contactent au moins t + 1

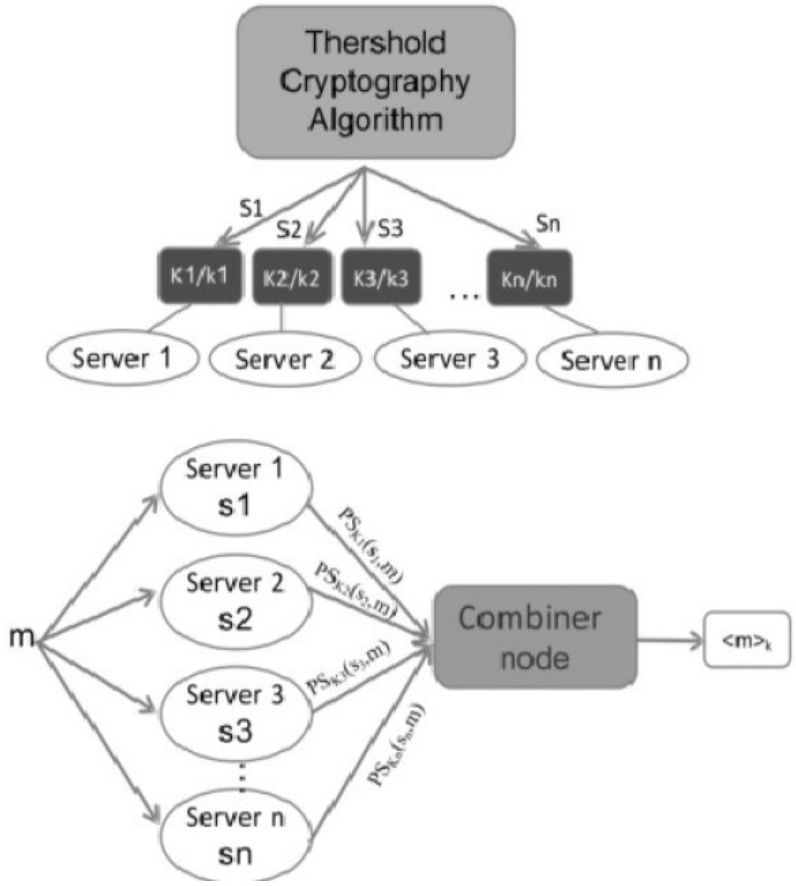

FIGURE 5.1 – *Gestion des clés K/k configuration*
.

hors des n serveurs de DCA pour réussir d'en avoir une. Comme l'illustre la figure 5.1, le schéma de signature à seuil proposée dans Zhou et Haas fait usage d'un noeud combinateur C pour combiner les signatures numériques partielles des t + 1 serveurs. Tout noeud de DCA peut être choisi comme un combinateur, puisque aucune information supplémentaire au sujet de la clé privée K est divulguée à C. Il est toujours possible pour un noeud combinateur d'être compromis par un adversaire ou d'être indisponible en raison de l'épuisement de la batterie ou de la mauvaise connectivité. Comme solution, [ZHOU & HASS 1999] ont proposé la sélection t+1 noeuds comme combinateur pour s'assurer qu'au moins un combinateur peut reconstruire avec succès la signature numérique. Tous les noeuds du réseau, y compris les combinateurs, peuvent vérifier la validité de la signature en utilisant la clé publique l'autorité de certification K.

La proposition présentée [Yi & KRAVET 2004] diffère de la proposition original dans [ZHOU & HASS 1999], puisque le schéma de signature a seuil de Yi et Kravets ne nécessite pas un noeud combinateur C pour construire la signature du groupe. Dans [Yi & KRAVET 2004], la DCA est appelée une autorité de certification Mobile(MObile Certificate Authority (MOCA). Dans le cadre de MOCA, le schéma de communication est l'un-vers-plusieurs et vise versa, ce qui signifie qu'un noeud qui nécessite

des services de certificat doit contacter au moins t+1 noeuds MOCA et recevoir les réponses de chacun d'eux. La combinaison des déférentes portions de signatures est donc effectuée par noeud qui cherche la certification.

Cette proposition se concentre principalement sur le one-to-many-to-one schéma de communication entre un noeud et le MOCA. Le protocole de certification MOCA permet à un noeud demandeur les services de certification de diffuser des paquets de demande de certification (CREQ). Tout noeud MOCA qui reçoit les paquets CREQ répond avec une réponse de certification (CREP) contenant sa signature partielle sur le certificat. Si le noeud reçoit avec succès t+1 CREP valable dans une période de temps déterminée, il peut reconstruire le certificat complet. Si le certificat est vérifié, pour être correcte, la demande de certification doit être réussie. Si le nombre de CREP est insuffisant après l'expiration du temps de CREQ du noeud, le processus échoue et le noeud peut lancer une autr requête. Inondation : Dans la première implémentation du protocole de certification présentée dans [Yi & KRAVET 2004], l'inondation est utilisée pour la diffusion des données fiables, la technique des inondations donne une approche efficace de contacter au moins t+1 serveurs, mais génère des flux de communication très élevés. Pour empêcher ce phénomène d'inondation, un ID de diffusion est utilisé (de façon similaire à ceux de Perkins et Belding-Royer), tels que tous les CREQs générés par la même requête, ils sont étiquetés avec le même ID, afin de permettre aux noeuds intermédiaires de rejeter les demandes qui ont déjà été transmis.

5.3 Les chaines de certificats

Une des propositions présentée dans [LUO & LU 2002] prend un pas de plus pour répondre aux contraintes de MANET. Contrairement aux solutions précédentes, l'infrastructure à clé publique (PKI) dans cette proposition ne nécessite aucune TTP. Cela rend le schéma totalement adapté à l'auto-organisation MANET.Chaque noeud émet ses propres certificats à d'autres noeuds dans une manière similaire à Pretty Good Privacy (PGP) (Zimmermann 1995). Elle diffère de PGP par le fait qu'il n'ya pas de chemin de gestion de certificat centralisée (serveurs de certificat en ligne), mais les certificats sont plutôt stockés et distribués par des noeuds dans une nature auto-organisés. Chaque noeud maintient un référentiel de certificats limités appelé "certificate repository" composé des noeuds voisins certifiés. Comme illustré dans la Figure 5.2 Quand un noeud u veut valider le certificat d'un autre noeud v, les noeuds doivent combiner leurs référentiels de certificat et les tentatives de u pour trouver une chaıne de validité certificats des clés publiques entre eux (voir figure 5.2).

La phase initiale du système est exécuté en quatre étapes : chaque noeud crée une paire de clés publique/privée; chaque noeud crée son propre certificat, envoie des certificats à d'autres noeuds, et construit un graphe certificat non mise à jour;es noeuds échangent les certificats, et créent des référentiels de certificats. Pour plus détails voir [LUO & LU 2002].

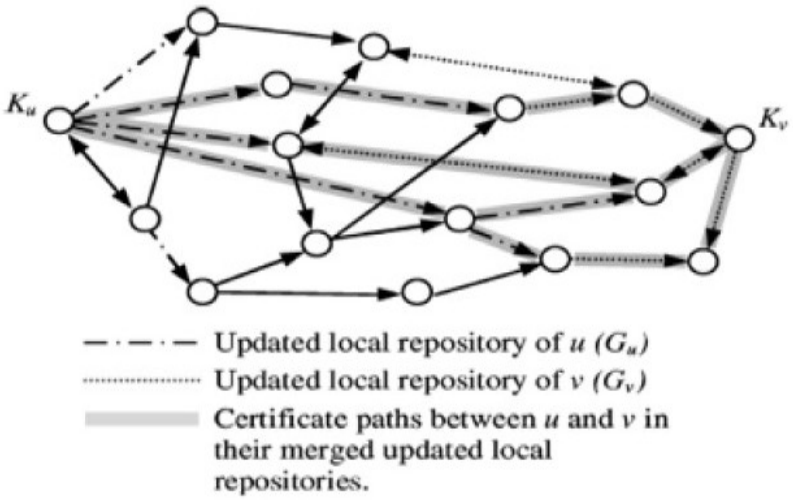

FIGURE 5.2 – *Graphe de certificat et chemin de certificats entre le noeud u et v et le mélange de référentiel de certificats*
.

5.4 CHAINAGE DE CERTIFICATS BASÉ SUR LES CLUSTERS

Une des propositions qui exploite les principes du chainage de certificat et les clusters pour améliorer la gestion des clés est la solution présenté par [HAHN *et al.* 2006] pour être utilisé dans le protocole AODV en profitant des données de routage de ce protocole.[HAHN *et al.* 2006] ont proposé une amélioration de la gestion des clés en combinant l'enchaînement de certificats et le protocole de routage CBRP basé sur des clusters. La solution suppose que tout les noeuds ont des pairs de clés Publique/privée et utilise la distribution des clés on se basant sur le cluster Head dans chaque cluster et applique le chainage de certificat s'il y a une communication inter cluster, le choix du cluster va résulter de l'algorithme de LOWEST-ID dans le principe est que le noeud qui a le plus petit ID est choisis comme un Cluster Head parmi les noeuds voisins.

En plus des structures de données de CBRP, le système nécessite un cache de certificat et le tableau CRL (une liste des certificats révoqués) ,Le cache de certificat de chaque noeud stocke les certificats de ses noeuds de communication. Les entrées de cache de certificat contient (L'ID d'un noeud correspond au certificat reçu, le certificat de noeud correspondant). Le tableau LCR contient des informations sur les traces des noeuds avec des certificats révoqués. Les entrées de la table CRL contient (L'ID d'un noeud avec un certificat révoqué, le numéro de série du certificat révoqué)

5.4.1 L'accord des certificats

L'accord des certificats se fait après la formation du cluster, chaque noeud peut obtenir son certificat, dans le schéma ils ont supposé qu'il y a deux noeuds qui délivrent les certificats, le premier est le cluster Head ou chef du cluster et l'autre est la passerelle. En règle générale, un certificat est généré par le cluster Head de chaque cluster. Cela indique que les fonctions du Cluster Head en tant virtuelle CA (Certificate Authority) et

fournit des certificats à ses membres afin de signer la clé publique, le certificat est ensuite stocké dans le cache de certificat de Cluster Head. Les passerelles ont pour rôle de signer la clé publique du Cluster Head au sein de son groupe et la clé publique du noeud de passerelle dans le cluster adjacent, le certificat est en suite délivré au Cluster Head est stocké dans le noeud passerelle. De même, le certificat pour le noeud passerelle dans le cluster voisin (voir figure 5.3). le certificat est construit dans l'un des cas suivants :

— Chaque fois qu'un noeud demande un certificat après un cluster est formé .
— Chaque fois qu'un noeud demande un certificat comme il se déplace en nouveau cluster
— Chaque fois un certificat doit être réédité à la suite de la révocation.

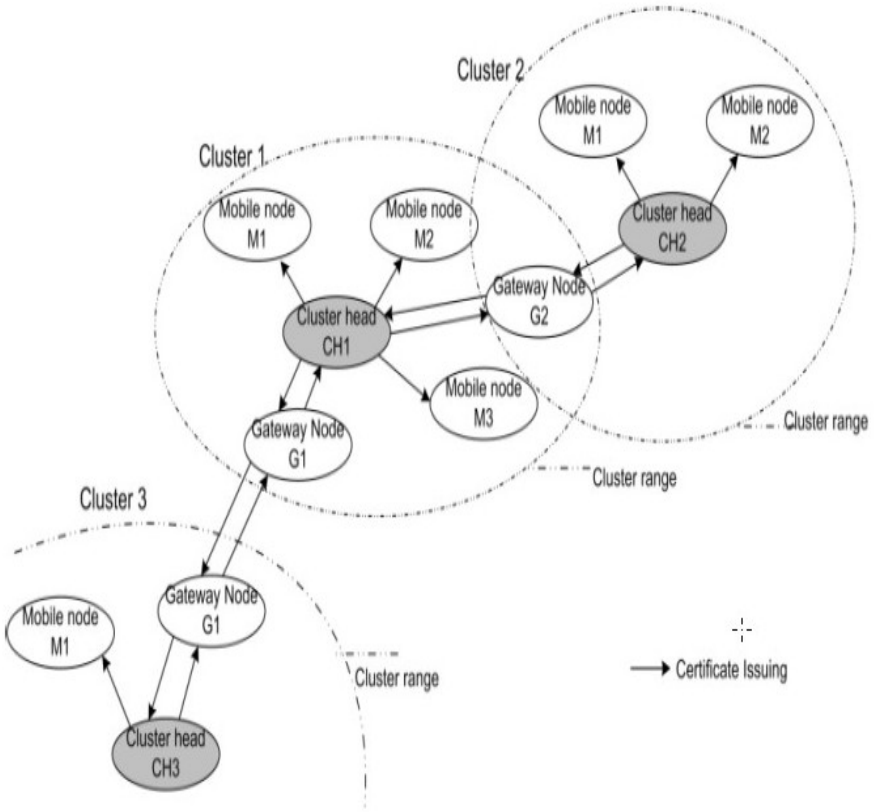

FIGURE 5.3 – *Délivrance du certificat*

5.4.2 Renouvellement des certificats

Tous les certificats sont valides dans la même période. Si un certificat est expiré. Un nouveau certificat doit être généré et envoyé au noeud avec un certificat expiré. C'est semblable à la génération du certificat. La différence est que le noeud doit présenter un certificat valide pour obtenir un nouveau, ce qui signifie que le certificat a expiré est envoyé à destination et vérifié par le Cluster Head dans le même cluster. Selon le résultat de la vérification, il peut obtenir un nouveau certificat ou non. Si le résultat de la vérification est légal, le noeud peut obtenir un nouveau certificat. Sinon,

il ne peut pas obtenir un nouveau. évidemment, c'est le cas ou un noeud ne laisse pas de cluster en cours après que son certificat est expiré. Autrement dit, si un noeud est toujours dans la couverture du même cluster après que le certificat est expiré, le certificat est mis à jour par le même cluster Head.

Le chaînage est effectué uniquement avec des nœuds sécurisés qui sont Cluster head OU des passerelles, contrairement au modèle PGP dans lequel la transaction est effectuée à l'aide de tous les nœuds du réseau. De plus, le chaînage est effectué dans une direction et tous les certificats des nœuds intermédiaires sont empilés linéairement, ce qui entraîne une surcharge très importante.

5.4.3 Notre proposition

L'idée réalisée par [HAHN *et al.* 2006] est d'étudier le modèle de cluster à base de PKI pour MANET ou le Cluster head agit comme un CA virtuel et émet des certificats pour ses membres. La chaıne de certificat construit par leur système permet l'échange des clés de session et, finalement, le cryptage / décryptage des données en cours de transfert. Cependant, à cause de la mobilité qui est une des caract éristiques de Vanet le noeud demande à nouveau un certificat au nouveau Cluster head du moment qu'il est devenu un nouveau membre. Ce qui constitue un processus de génération de certificat de plus pour le cluster Head et pour le membre en question. L'idée est de faire en sorte dès que le membre sort du domaine du Cluster head une information est diffusée à travers les passerelles pour inonder l'ensemble du réseau et signaler l'éventuelle arrivée de ce membre. Dans cette section nous développons cette contribuon en tenant compte de l'implémentation des clusters basé sur le PKI avec prédiction/préemption pour remédier au problème de la disponibilité et de renouvellement de certificats.

Dans ce travail, nous considérons que la zone de couverture d'un clusterhead qui forme le cluster est divisée en deux régions, une région sûre où un nœud mobile est proche de cluster head et ne risque pas de se déconnecter, et l'autre est incertain ou en préemption .

5.4.4 calcule de valeur de confiance

pour sécuriser les échanges de données dans les réseaux VANET,Nous proposons un modèle de confiance basé sur les clusters (CBTM) .

Pour dégrader l'efficacité du réseau Vanet, un nœud malveillant envoie un grande nombre de paquets RREP pour intercepter les paquets de données de ses voisins ou pour surcharger le réseau. pour cela ,il utilise un numéro de séquence très élevé dans le paquet RREP pour attirer ses voisins à passer par lui pour les supprimer plus tard ou les modifier.

Dans notre modèle [BENSAID & BOUKLI-HACENE 2019], chaque noeud du réseau est équipé par une cache mémoire , dans laquelle il enregistre le nombre de paquets de données envoyé par lui , le nombre de paquets de paquets de requête (RREQ) et le nombre de paquets de réponse de route (RREP) reçus et le numéro de séquence à chaque réception d'un paquet.

Chaque nœud mettra à jour sa cache mémoire avec les fonctions suivantes :

— recv RREQ () Cache [0] [@src] ++ ;
— recv Data () Cache [1] [@src] ++ ;
— recv Reply () Cache [2] [@src] ++ ;

Si un noeud reçoi un paquet RREP, Il utilisera l'algorithme suivant (voir l'algorithme 2). pour décider si le nœud est un nœud de confiance ou non.

Algorithme 2 : calcule de valeur de confiance

```
N_D : the number of data packets received from a node;
N_REQUEST : the number of RREQ packets received from a node;
N_REPLY : the number of RREP packets received from a node;
if N_D + N_REQUEST == 0 and N_seq_dest >>>>> N_seq_src
 then
    trusted_value=0;
else
    trusted_value=1;
if N_D + N_REQUEST! = 0 and N_RPLY < N_D + N_REQUEST
 then
    trusted_value=1;
if N_D + N_REQUEST == 0 and N_REPLY! = 0 then
    trusted_value=0;
.
```

5.4.5 clustering

Pour diviser les réseaux en clusters, chaque nœud utilise sa table des voisins. Dans notre implémentation, la taille de chaque groupe est fixée à 5, et il y a un seul cluster head dans chaque groupcluster. De plus,chaque membre du cluster est un noeud de confiance .

5.4.6 Certification

L'objectif de notre approche est d'éviter de faire une nouvelle demande de certificat dans le cas ou un noeud transite d'un cluster vers un autre et augmenter la possibilité de renouvellement lors de l'expiration de certificat on se basant sur la proposition de [HAHN *et al.* 2006].

nous considérons qu'un cluster possède deux régions une région dite sure et l'autre incertaine ou de préemption [BOUKLI-HACENE *et al.* 2006]. Un noeud est dans une région pas sure ou de préemption si le signal qu'il reçoit de son Clusterhead est inférieur à un seuil de puissance Pt. Une fois un noeud entre dans cette zone,on effectue au moins trois mesures consécutives de la puissance du signal des paquets HELLO ou donnée s'il y a à partir du Cluster Head,et on prévoie à l'aide de l'interpolation de Lagrange la rupture du lien de communication. La forme générale de cette interpolation est :

$$y = \sum_{i=0}^{n} \left[\frac{\prod_{j=0, j\neq i}^{n} (x - x_j)}{\prod_{j=0, j\neq i}^{n} (x_i - x_j)} \times y_i \right] \tag{5.1}$$

Nous stockons les puissances des trois signaux et leur temps d'occurrence.Lorsque deux mesures consécutives donnent la même valeur de puissance, nous stockons les temps de la deuxième occurrence.La puissance du signal P des paquets reçus est [BOUKLI-HACENE *et al.* 2006] :

$$P = \left(\frac{(t-t_1)\times(t-t_2)}{(t_0-t_1)\times(t_0-t_2)}\times P_0\right) + \left(\frac{(t-t_0)\times(t-t_2)}{(t_1-t_0)\times(t_1-t_2)}\times P_1\right) + \left(\frac{(t-t_0)\times(t-t_1)}{(t_2-t_0)\times(t_2-t_1)}\times P_2\right) \tag{5.2}$$

P_0 , P_1 , P_2 sont les puissances mesurées aux moments t_0 , t_1 , and t_2 espectivement. Le temps t est le total du temps nécessaire pour envoyé le certificat aux Cluster voisins (Inonde Period), le dernier temps de mesure t2, et la différence entre t2 et la valeur moyenne des temps de mesure to, t1 et t2. C'est-à-dire [BOUKLI-HACENE *et al.* 2006] [LARAOUI *et al.* 2018] :

$$t = 2\times t_2 - \left(\frac{t_0+t_1+t_2}{3}\right) + Inonde\_Period \tag{5.3}$$

Lorsque P est inférieur à la puissance minimale acceptée (-81 dB) un message d'avertissement est envoyé au Cluster Head. Le Cluster Head envoie le certificat vers les Cluster Head voisins [BOUKLI-HACENE *et al.* 2014]

Notre schéma nécessite une nouvelle structure de données dans laquelle le cluster head d'origine insère les adresses des noeuds qui vont quitter leur couverture et rejoindre un cluster adjacent. Lorsque le cluster head de destination détecte la présence d'un nœud dans son étendue à l'aide des paquets Hello, elle envoie une alerte au cluster head d'origine. Une fois que le cluster-head d'origine a reçoit le message d'alerte, il a placé l'ID et la clé publique du noeud transféré dans la structure de données.

5.4.7 Transfert du certificat

La fonction d'interpolation de Lagrange permet au noeud Clusterhead de prédire si le noeud membre va sortir de sa couverture, si c'est le cas, le Clusterhead envoie l'adresse du noeud correspondant à tout les Clusterhead voisin via les passerelles. Une fois le noeud en déplacement est détecté par un Clusterhead, celui-ci compare l'adresse reçue en alerte avec le certificat envoyé par le noeud en déplacement. Si cette comparaison s'avère positive, le cluster Head enregistre ce certificat sans générer un autre. Ceci permettra a un noeud de se déplacer d'un cluster vers un autre sans demander à chaque fois de générer un nouveau certificat même s'il y aura une coupure temporelle du lien . Ce qui permet ainsi d'offrir une grande possibilité de renouvellement de certificat même si le noeud transite vers un autre cluster (voir figure 5.4).

5.4.8 Renouvellement du certificat et révocation du certificat

Le renouvellement des certificats est effectué à l'expiration du certificat. Il peut être effectué par le cluster head ou les cluster head voisins dans un délai déterminé, afin d'éviter la surcharge de mémoire des cluster head. Contrairement à la méthode de Chaînage de certificats basée sur les cluster, un certificat peut être révoqué n'importe où dans le réseau (voir figure 5.5)

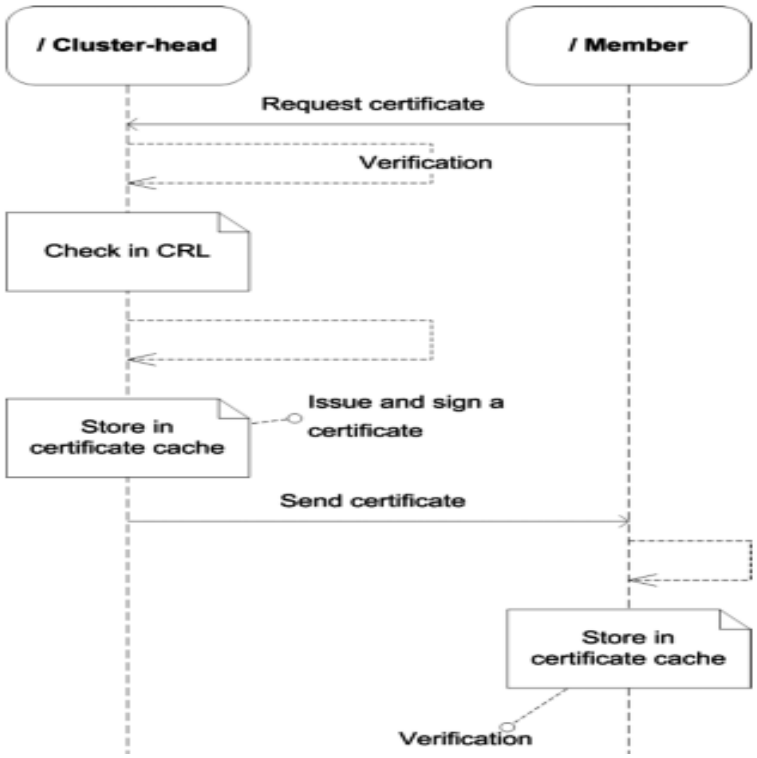

FIGURE 5.4 – *Certficate generation*

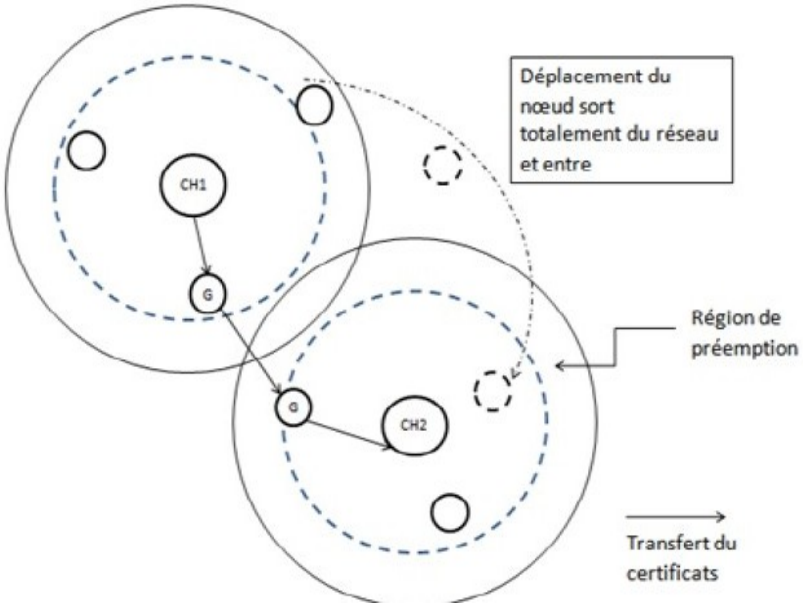

FIGURE 5.5 – *Le renouvellement des certificats*

5.5 Les résultats de simulation

Pour évaluer les performances, nous avons utilisé le simulateur NS2. Dans notre approche, nous avons utilisé deux scénarios de mobilité.le premier est de la ville de Malaga et le second est généré par le simulateur VANETmobisim

5.5.1 le scenario le la ville de Malaga

La Figure.5.6 présente une carte géographique de scénarios du centre-ville de Malaga,Espagne [TOUTOUH & ABLA 2011] . Il est composé de trois zones U1, U2 et U3. les Paramètres détaillés de simulation est présentée dans le tableau 5.1.

TABLE 5.1 – *dètail de la zone géographique utilisé*

Scénario	Taille de la zone	Nombre de véhicules	nombre de connections
U1	$120000m^2$	60	10
			15
U2	$240000m^2$	60	20
U3	$360000m^2$	60	30
			40

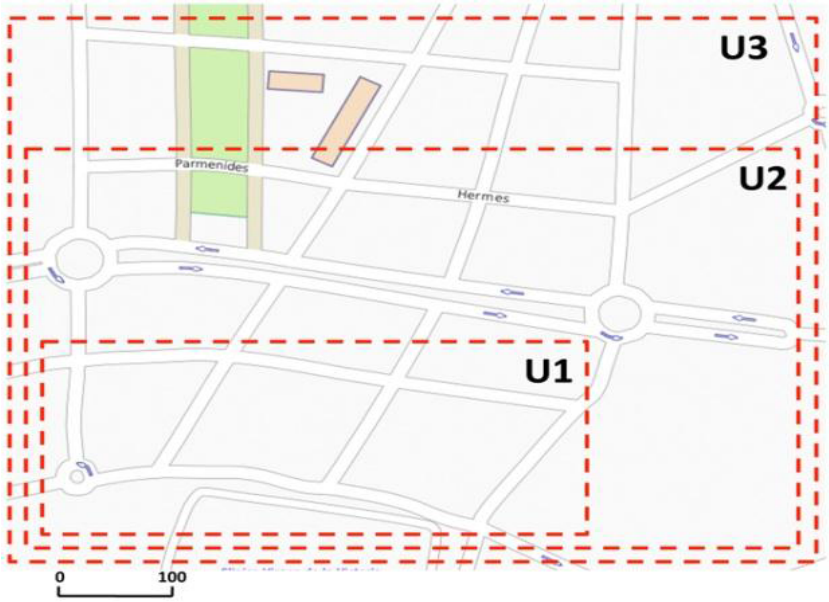

FIGURE 5.6 – *carte géographique de la zone utilisé*

Pour les simulations, on a utilisé le simulateur réseau NS-2 (V-2.35), dans lequel on a utilisé le protocole IEEE 802.11ext, Le canal utilisé est le canal sans fil avec un modèle de propagation radio Nakagami. Lors de la couche réseau, nous utilisons AODV comme un protocole de routage. Enfin, UDP est utilisé dans la couche de transport. Tout les paquets de données sont de type CBR (débit continu). La taille du paquet est de 1 Ko. La zone géographique est 2Km * 1Km avec un nombre de véhicules variant de 10 à 60.Les paramètres de simulation sont résumés dans le tableau suivant :

TABLE 5.2 – *paramètres de simulation*

Paramètres	valeur
Modèle de Propagation	Nakagami
couche physique	IEEE 802.11p
couche MAC	IEEE 802.11p
couche réseau	AODV
couche transport	UDP
taille de CBR packet	1024 bytes
vitesse de transmission	100kbps
temps de Simulation	180 s

5.5.2 scenarios de VANETmobisim

Le simulateur de mobilité de réseaux VANET (VANETMobiSim) [TOUTOUH 2006] est un ensemble des extensions du framework de modélisation de la mobilité des utilisateurs CanuMobiSim, utilisé par le Groupe de recherche CANU dans les réseaux AdHoc pour l'informatique ubiquitaire, Il comprend un module de visualisation, des modèles de mobilité, ainsi que analyseurs de divers formats pour les sources de données géographiques. il est basé sur le concept de modules enfichables. L'ensemble des extensions fournies par VANETMobiSim consiste principalement en un modèle spatial de véhicule utilisant des données conformes à la structure de GDF et un ensemble de modèles de mobilité orientés vers les véhicules.

Le tableau 5.3 détaille tous les paramètres utilisés dans ce scénario

TABLE 5.3 – *paramètres de simulation*

Paramètres	valeur
Propagation Model	Nakagami
PHY layer	IEEE 802.11p
MAC layer	IEEE 802.11p
Area size	1000*1000 m
Vehicule speed	from 8.33 to 13.89 m/s
CBR packet size	1024 bytes
CBR packet rate	100kbps
Simulation time	900 s
Number of malicious nodes	3

Les métriques sont des paramètres de test du protocole de routage qui permettent de mesurer les performances de celui-ci a bases des quelles la comparaison entre les protocoles sera effectuée. Dans notre étude, nous avons pris en compte les métriques suivantes :

— Le taux de délivrance des paquets de données (delivery ratio) :Ce paramètre représente le pourcentage des paquets livrés à leurs destinations

— Calcul du taux de surcharge de routage (Normalized Routing Load) :La surcharge du réseau permet de mesurer le taux de paquets de contrôle de routage dans le réseau par rapport au nombre total de paquets reçus.Ce taux est recalcule a chaque émission ou réception d'un paquet au niveau de la couche Internet. Le calcul de

surcharge de routage est important pour déterminer la nature des paquets qui occupe le réseau.
— La moyenne de temps de latence des paquets de données (average end to end delay) :C'est la moyenne des temps nécessaires pour livrer les paquets de donnéesde la source à la destination avec succès, incluant les temps de latence dans les files d'attentes, le temps de stockage dans les tampons,. . . etc.
— Paquets perdus (Dropped packets) :C'est le nombre de paquet ignoré par le noeud malicieux ou bien perdu suite à une déconnexion d'un noeud (véhicule).
— Nombre de certificat généré dans le réseau

Les scénarios de simulation sont les suivants :
— AODV avecle modèle vanetmobisim sous l'attaque .
— CBTM vanetmobisim représente notre approche sous l'attaque avec le scénario vatenmobisim.
— AODV avec le modèle de Malaga sous l'attaque.
— CBTM malaga représente notre approche sous l'attaque utilisée selon le scénario de Malaga.

Le taux de certificats :

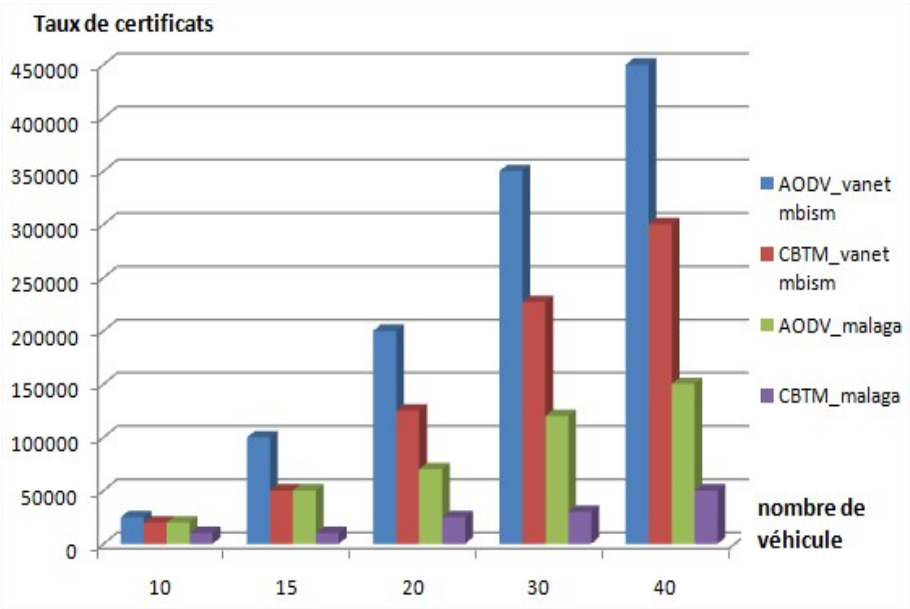

FIGURE 5.7 – *Le nombre de certificat*

La Figure5.7 illustre la surcharge de réseau par les certificat.Nous observons que le nombre des certificats générées augmentent si le nombre de connexions augmente parce que de nombreux nœuds demandent un nouveau certificat à l'autorité de certification et à l'autorité de certification adjacente lorsqu'un nœud est déplacé.

Cependant, nous illustrons que notre approche est meilleure de l'origine avec 6,01% à 44,88% de certificats en moins par modèle de mobilité malaga et 40,40% à 69,42% de certificats en moins par modèle généré par VANETmobisim.

Le taux de délivrance des paquets de données :

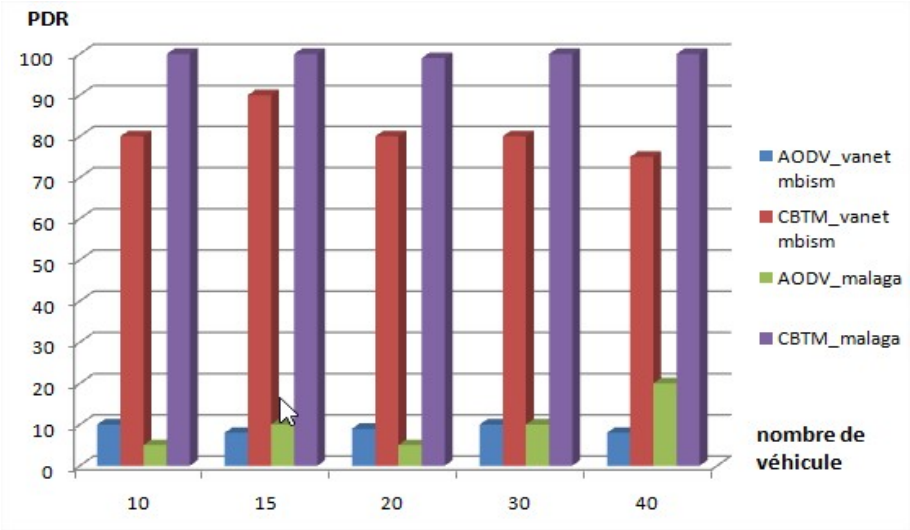

FIGURE 5.8 – *Fraction de livraison de paquets*

La Figure 5.8 montre l'évolution décroissante de la PDF dans le protocole AODV sous l'attaque contre notre approche avec deux modèles de mobilité. Lorsque le nombre de véhicules est élevé, le PDF de notre approche enregistre une légère dégradation. Cela est dû aux fréquents changements de topologie du réseau avec un grand nombre de connexions. Nous observons également que si le nombre de véhicules augmente, le PDF augmente pour notre solution. mais dans le protocole AODV sous l'attaque, le PDF atteint 19.98 %

Paquets supprimés :

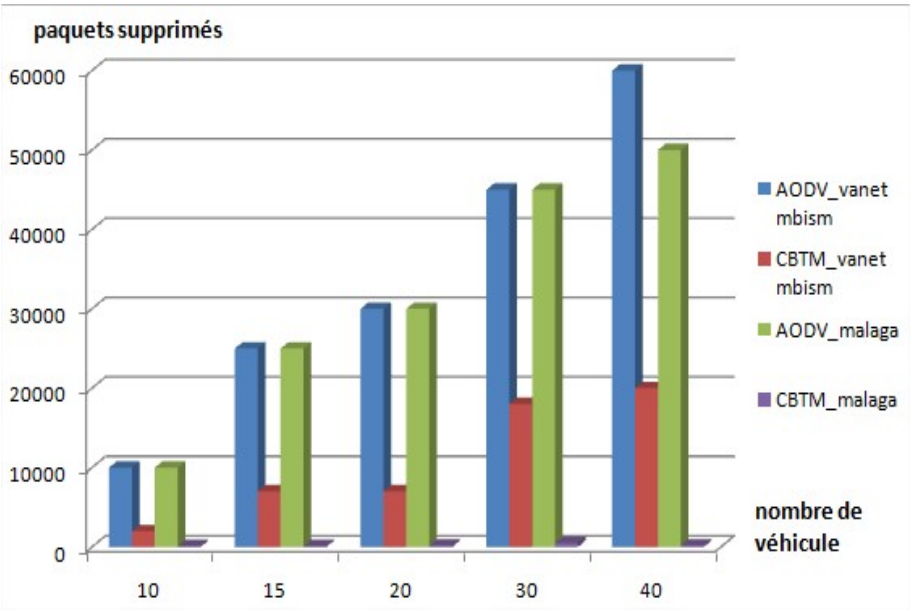

FIGURE 5.9 – *paquets supprimés*

La Figure5.9 présente le nombre de paquets supprimé en fonction du nombre de véhicules. Dans notre proposition,avec 10 sources de connexion, le nombre de paquets perdus est de 69 e pour l'AODV sous l'attaque atteint 9971 paquets dans le modèle de mobilité malaga. Lorsque le nombre de connexions augmente,le nœud malveillant intercepte une grande quantité de paquets , mais dans notre proposition reste efficace.

Les coûts additifs :

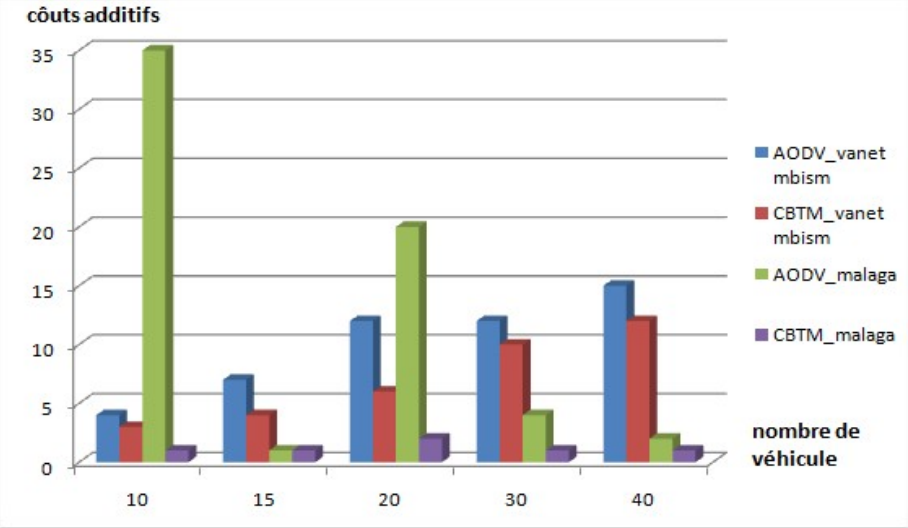

FIGURE 5.10 – *les coût additifs*

Les résultats de la simulation à la Figure5.10 montrent que nos propositions sont meilleure que l'AODV sous l'attaque. Cela est dû au fait que lorsque un paquet est intercepté,le nœud source tente de réparer les chemins avec des paquets RRER ce qui surcharge le réseau.

Délai moyen de bout en bout

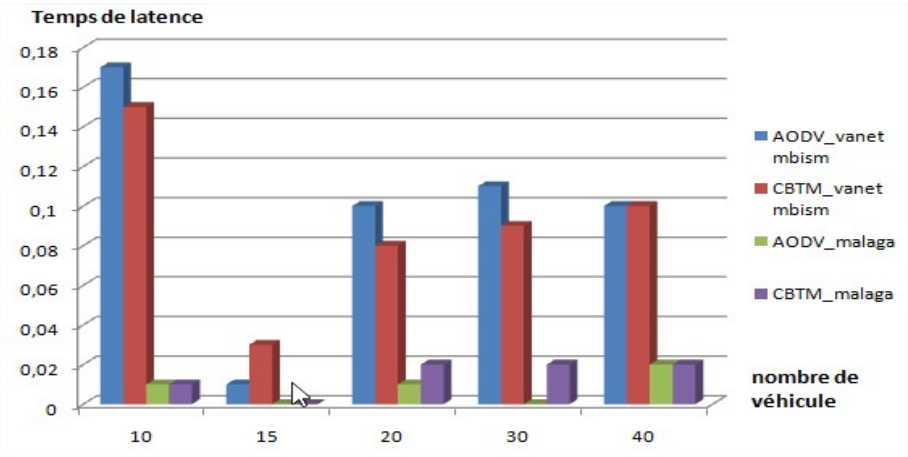

FIGURE 5.11 – *Le délai de communication de bout en bout*

La Figure 5.11 montre l'évolution du délai moyen de bout en bout, en fonction du nombre de véhicules dans notre approche et de l'AODV sous l'attaque avec deux modèles de mobilité.le temps requis par notre proposition est supérieur à celui de l'AODV sous l'attaque. Cela peut être justifié par l'utilisationn d'un processus supplémentaire dans notre solution pour créer les certificats et le mettre à jour les caches mémoires.

5.6 Conclusion

Dans ce chapitre, nous avons présenté une nouvelle proposition basée sur un modèle de confiance. Dans notre proposition, nous nous sommes intéressés au système de communication V2V où le cluustre head agit comme une autorité de certification virtuelle. L'idée principale est de calculer un niveau de confiance pour chaque nœud à l'aide de son comportement et en évitant le problème de la nouvelle demande de certificat en cas de déplacement d'un nœud .

Conclusion générale

Les réseaux véhiculaires constituent un nouveau type des réseaux issu des réseaux ad hoc mobiles, leur particularité provient des communications qui peuvent s'instaurer entre véhicules ou bien avec une infrastructure de station de base. Ces réseaux souffrent de certaines contraintes telles que la mobilité causée par la vitesse de déplacement élevée des véhicules, qui peut causer des changements fréquents de la topologie de réseaux. La sécurité des réseaux véhiculaires est un prérequis pour leurs déploiement, de fait que ces réseaux sont une catégorie des réseaux sans fil et l'importance de l'information échangés qui peut mettre la vie des utilisateurs en danger, la sécurité de ces réseaux ne cesse de recevoir un intérêt particulier chez les communautés de recherche dans les milieux académiques et industriels. C'est pour cela, que nous nous sommes intéressés à notre tour à l'étude de certains protocoles de sécurité et leurs mécanismes de fonctionnement.

Réaliser la sécurité dans un réseau véhiculaire est une tâche difficile, puisque la topologie de ces réseaux change fréquemment à cause de la mobilité des noeuds qui est très élevée. Dans ce projet, nous avons proposé deux nouvelle approches pour sécuriser l'échange de données dans ces réseaux. Nous nous somme intéressés à la sécurité au niveau routage,plus précisément nous avons basé notre étude sur le protocole AODV.

Les caractéristiques particulières des réseaux véhiculaires les rendent très vulnérables à plusieurs formes d'attaques. Un exemple spécifique de l'une de ces attaques est l'attaque Blackhole. Ce type d'attaque peut représenter une menace importante pour le bon fonctionnement du réseau.

Dans ce projet de fin cycle , nous nous sommes intéressés à l'analyse de l'attaque Blackhole et la gestion des certificats dans les réseaux véhiculaires.Pour évaluer les performances des protocoles, nous avons implémenté nos solutions sous le simulateur NS-2.

Nous avons également présenté une nouvelle proposition basée sur un modèle de confiance. Dans notre proposition, nous nous sommes intéressés au système de communication V2V où le nœud de cluster head agit comme une autorité de certification virtuelle. L'idée principale est de calculer un niveau de confiance pour chaque nœud en se basant sur son comportement en évitant le problème de la nouvelle demande de certificat en cas de déplacement .

Ce projet nous a offert l'occasion de découvrir l'outil de simulation des réseaux NS-2, découvrir et enrichir nos connaissances sur des domaines de recherche très vastes, à savoir les réseaux véhiculaires, la sécurité des réseaux en général et les systèmes de détection d'intrusion en particulier. Grâce à notre étude, nous avons aussi constaté qu'il ne peut y avoir une sécurité absolue. Cela est dû au nombre important des facteurs qui conditionnent les performances d'un protocole sécurisé à 100

Ce travail a fait l'objet d'une expérience intéressante, qui nous a permis d'améliorer nos connaissance dans le domaine des réseaux véhiculaire et la sécurité en général. En guise de perspectives, ce travail peut être enrichi dans un premier temps par des simulations afin de mesurer les forces et les faiblesses du la solution et de concrétiser des résultats pour d'éventuelles comparaisons et améliorations.

comme perspective, nous proposons d'ajouter une technique pour améliorer le surcoût des certificats et gérer les échecs de liaison sur le réseau en cas de déplacement de véhicule.

Publications et Communications

— C.Bensaid, S. Boukli-Hacene and M. K. Feraoun, ”Detection and Ignoring of Blackhole Attack in Vanets Networks” International Journal of Cloud Applications and Computing (IJCAC), Vol. 6, No. 2, 2016
— C.Bensaid, S. Boukli-Hacene, ” AODV-based Key Management in VANET Network",Advances in Systems Science and Applications, Vol 19 No 2 (2019)
— C.Bensaid, S. Boukli-Hacene and M. K. Feraoun,”Cluster Based Key Management in VANET Networks” International Conference of Telecommunication and TIC , May 2015 Oran.
— C.Bensaid, S. Boukli-Hacene and M. K. Feraoun,”Cluster Based Key Management in VANET Networks” Programming and Systems (ISPS), 2015 12th International Symposium , april 2015.
— C.Bensaid, S. Boukli-Hacene and M. K. Feraoun,"Detection and Ignoring Of Blackhole Attacks In VANET Networks" , International Conference on automatic control and telecommunications and signals , November 2015, ANNABA
— C.Bensaid, S. Boukli-Hacene and M. K. Feraoun,”Detection of Blackhole attacks in VANET Networks” , 6th seminar of Detection System ,February 2014, Algeries

Bibliographie

[ABDELHAQ *et al.* 2011] M. ABDELHAQ, S. SERHAN, R. ALSAQOUR et A. SATRIA. *Security Routing Mechanism for Black Hole Attack over AODV MANET Routing Protocol*. Australian Journal of Basic and Applied Sciences, vol. ISSN 1991-8178, no. 5(10), pages 1137–1145, 2011.

[ADETUNJI 2014] A. ADETUNJI. *gestion de l'anonymat et de la traçabilité dans les réseaux véhiculaires sans fil*. Thèse de doctorat, Département de mathématiques et informatique appliquées. Université du Québec à Trois-Rivières, 2014.

[ANJUM & MOUCHTARIS 2007] F. ANJUM et P. MOUCHTARIS. *Security for Wireless Ad hoc networks*. Book from senior scientist at Telcordia Technologies, Published by John Wiley and Sons, New Jersey,, 2007.

[ARNAUD *et al.* 2004] J. ARNAUD, S. VERONIQUE Sainson et M. BENDAJA. *Le grand livre de la sécurité*. Livre Edition sécurité informatique. http ://www.securiteinfi.com, pages 75–90, 2004.

[BACCOUR 2005] N. BACCOUR. *Etude comparative de deux simulateurs pour les réseaux sans fil Intervention Part II*. Mémoire présenté à l'École Nationale d'Ingénieurs de Sfax, Tunisie., 2005.

[BEGHRICHE 2009] A. BEGHRICHE. *De la Sécurité à la E-Confiance basée sur la Cryptographie à Seuil dans les Réseaux sans fil Ad hoc*. mémoire de magister , Université de L'Hadj Lakhdar-Batna, 2009.

[BENCHABANA & BENSACI 2014] A. BENCHABANA et R. BENSACI. *Analyse des protocoles de routage dans les réseaux VANET*. mémoire de Magister, Département d'Informatique, Université d'Ourgla, 2014.

[BENSAID & BOUKLI-HACENE 2019] C. BENSAID et S. BOUKLI-HACENE. *AODV-based Key Management in VANET Network*. Advances in Systems Science and Applications, Vol 19 No 2, pages 80–89, 2019.

[BENSAID *et al.* 2015] C. BENSAID, S. BOUKLI-HACENE et M. K. FARAOUN. *Detection and Ignoring Of Blackhole Attacks In VANET Networks*. International Conference on automatic control and telecommunications and signals , ANNABA, 2015.

[BENSAID *et al.* 2016] C. BENSAID, S. BOUKLI-HACENE et M. K. FARAOUN. *Detection and Ignoring of Blackhole Attack in Vanets Networks*. International Journal of Cloud Applications and Computing (IJCAC), Vol. 6, No. 2, pages 40–59, 2016.

[BOUKLI-HACENE *et al.* 2006] S. BOUKLI-HACENE, A. LEHIRECHE AHMED et A. MEDDAHI. *Predictive preemptive ad hoc on-demand distance vector routing*. Malaysian Journal of Computer Science, 19(2), pages 189–195, 2006.

[BOUKLI-HACENE *et al.* 2014] S. BOUKLI-HACENE, A. OUALI et A. BASSOU. *Predictive preemptive certificate transfer in cluster-based certificate chain.* International Journal of Communication Networks and Information Security, 6(1)., pages 44–51, 2014.

[BOUSSAD 2011] A. BOUSSAD. *Sécurisation des Réseaux Ad hoc :Systèmes de Confiance et de Détection de Répliques*. Thèse de doctorat, Université de Limoges, 2011.

[BOUZEBIBA 2015] H. BOUZEBIBA. *Impact des modèles de mobilités sur les performances des protocoles de routage en milieu urbain réaliste dans les réseaux VANET (V2V)*. Mémoire de Magister, université de Tlemcen,, 2015.

[BURGODC 2007] A. BURGODC. *Contribution à la sécurisation du routage dans les réseaux ad hoc*. thèse de doctorat,uiversité de limoges, 2007.

[BURMESTER *et al.* 2008] M. BURMESTER, E. MAGKOS et V. CHRISSI. *Strengthening Privacy Protection in VANETs*. IEEE International Conference on Wireless and Mobile Computing, Networking and Communications(WIMOB), 2008.

[CAPKUN & HUBAUX 2003] S. CAPKUN et J.P. HUBAUX. *Self organized public-key management for mobile ad hoc networks*. Ieee Transactions on Mobile Computing, Vol. 2, pp. 52-64, 2003.

[CHAIB 2011] N. CHAIB. *La sécurité des communications dans les réseaux VANET*. Mémoire de Magister,université el hadj lakhder- Batna ,Algerie, pages 54–57, 2011.

[CHAOUCHI & LAURENT 2007] H. CHAOUCHI et M. LAURENT. *La sécurité dans les réseaux sans fil et moiles*. Thèse de doctorat, pages 239–241, 2007.

[CHOI *et al.* 2009] J. CHOI, S. JUNG, Y. KIM et M. YOO. *A Fast and Efficient Handover Authentication Achieving Conditional Privacy in V2I Networks*. Proceedings of the 9th International Conference on Smart Spaces and Next Generation Wired/Wireless Networking and Second Conference on Smart Spaces St. Petersburg, Russia, pages 291–300, 2009.

[CHRIS & WANGER 2003] K. CHRIS et D. WANGER. *Modèle de sécurité dynamique pour les réseaux spontanés*. Secure routing in wireless sensor networks : attacks and countermeasures., page 293–315, 2003.

[DAOUD 2005] M. DAOUD. *Analyse du protocole AODV*. In thèse de doctorat,Université libanaise, Faculté des sciences 2-212-11154-1, 2005.

[DLS 1932] DLS. *Dictionnaire de l'Académie française*. (8e édition), Paris, 1932.

[GACHET 2011] P. GACHET. *Déploiement de solutions VPN : PKI Etude de cas*. travail du diplôme : Ecole d'ingénieur du Canton de Vaud, 2011.

[GALICE 2007] S. GALICE. *Modèle de sécurité dynamique pour les réseaux spontanés*. Thèse de doctorat. Institut National des Sciences Appliquées de Lyon., 2007.

[GAYROUD *et al.* 2008] V. GAYROUD, L. NUAMI, F. DUPONT, S. GOMBAULT et B. THARON. *La Sécurité dans les Réseaux Sans Fil Ad Hoc*. symposium sur la sécurité des technologies de l'information et de la Communication SSTIC,Renne France, 2008.

[GUERRORO & ASOKAN 2002] Z. GUERRORO et Z. ASOKAN. *Securing ad hoc routing protocols.* Proceedings of the 2002 ACM workshop on wireless security (WiSe 2002), Atlanta, Georgia, USA,, page 1–10, 2002.

[HAGGAR 2007] S. HAGGAR. *Les protocoles de routage dans les réseaux*. Rapport de stage,Université de Reims - UFR Sciences,, juin 2007.

[HAHN *et al.* 2006] G. HAHN, T. KWON, S. KIM et J. SONG. *Cluster-Based Certificate Chain for Mobile Ad Hoc Networks*. International Conference on Computational Science and Applications (ICCSA) , pp. 769-778, 2006.

[HIMRAL *et al.* 2011] L. HIMRAL, V.VIG et N. CHAND. *Preventing AODV Routing Protocol from Black Hole Attack*. International Journal of Engineering Science and Technology (IJEST), pages 80–89, 2011.

[ILYAS & MAHJOUB 2005] M. ILYAS et I. MAHJOUB. *Handbook of Sensor Networks : Compact Wireless and Wired Sensing Systems*. chapitre 32, CRC Press LLC, 2005.

[JERBI 2008a] M. JERBI. *Protocoles pour les communications dans les réseaux de véhicules en environnement urbain : Routage et GeoCast basés sur les intersections*. Université d'Evry Val d'Essonne, Thèse de Doctorat, 2008.

[JERBI 2008b] M. JERBI. *Protocoles pour les communications dans les réseaux de véhicules en environnement urbain : Routage et GeoCast basés sur les intersections*. Université d'Evry Val d'Essonne, Thèse de Doctorat soutenue en Novembre, 2008.

[KENNEY 2011] J. KENNEY. *Dedicated short-range communications (DSRC) standards in the United States*. Proceedings of the IEEE, vol. 99, no. 7,, page 1162–1182, 2011.

[KO & VAIDRA 1998] Y. KO et H. VAIDRA. *"Location-aided routing(LAR) in mobile ad hoc networks"*. Proceedings of the ACM/IEEE International Conference on Mobile Computing and Networking (Mobicom98), page 66–75, 1998.

[LARAOUI *et al.* 2018] M. LARAOUI, F. SELLAMI, B. NOUR, H. MOUNGLA, A. AFIFI et S. BOUKLI-HACENE. *Driving path stability in VANETs*. IEEE Global Communications Conference (GLOBECOM) (pp. 1-6). IEEE., 2018.

[LPCHERT *et al.* 2003] C. LPCHERT, H. HARTENSTEIN et M. MAUVE J. TIAN D. HERRAMANN. *A Routing Strategy for Vehicular Ad Hoc Networks in City Environments*. In IEEE Intelligent Vehicles Symposium, volume 4792, pages 156–161. IV2003 Columbus, OH, USA,, 2003.

[LUO & LU 2002] H. LUO et S. LU. *Providing Robust and Ubiquitous Security Support for Mobile Ad Hoc Networks*. icnp (Vol. 1, pages 251–260, 2002.

[MAHI 2010] S. MAHI. *l'authentification dans les réseaux ad hoc, université de mostaghanem*. mémoire de magister, page 39–68, 2010.

[MANDHATA & PATRO 2011] S. CHANDRA MANDHATA et S. Narayan PATRO. *Acounter measure to Black hole attack on AODV- based Mobile Ad-Hoc Networks*. International Journal of Computer and Communication Technology (IJCCT), vol. 4, pages 137–175, 2011.

[MEHDI *et al.* 2007] M. MEHDI, A. ANOU, S. ZAIR et M. BENSEBTI et M. DJEBARI. *La Sécurité dans les Réseaux Ad Hoc*. 4th International Conference : Sciences of Electronic, Technologies of Information and Telecommunications, TUNISIA,, page 25–29, 2007.

[Meraihi 2011] Y. Meraihi. *Routage dans les réseaux véhiculaires (VANET) : cas d'un environnement de type ville*. These de Magister, Université de Boumerdes, 2011.

[MUSTAFA 2004] H. MUSTAFA. *Routage unicast et multicast dans les r2seaux mobiles ad hoc*. Thèse de doctorat, page 39–54, 2004.

[NING & SUN 2005] P. NING et K. SUN. *"How to misuse AODV : a case study of insider attacks against mobile ad-hoc routing protocols ",*. Ad Hoc Networks journal., vol. 3, no 6,,, pages 795–819, 2005.

[OUAZENE 2009] N. OUAZENE. *Pour une QoS au niveau de la Couche MAC dans les Réseaux Sans Fil*. memoire de Magister :UNIVERSITE ELHADJ LAKHDER - BATNA, 2009.

[PATHAC & SHRAWAKER 2009] S. PATHAC et U. SHRAWAKER. *Secured Communication in Real Time VANET,"*. In the Second International Conference on Emerging Trends in Engineering and Technology, pages 1151–1155, 2009.

[PAUL *et al.* 2012] B. PAUL, M. IBRAHIM et M. Bikas. *Vanet Routing Protocols : Pros and Cons*. International Journal of Computer Applications, vol. 20, no. 3, pages 28–34, 2012.

[PAYAL *et al.* 2009] L. PAYAL, N. RAJI, P. RASHANT et B. SWADAS. *DPRAODV :A Dynamic Learning System against Blackhole Attack in*

AODV based MANET. IJCSI International Journal of Computer Science Issues, 2009.

[PERKINS *et al.* 2003] C. PERKINS, E. BELDING-ROYER et S. DAS. *Ad Hoc On Demand Distance Vector (AODV) Routing*. IETF RFC 3561, 2003.

[P.NING & K.SUN 2003] P.NING et K.SUN. *How to misuse AODV : a case study of insider attacks againstmobile ad-hoc routing protocols*. Proc. IEEE Systems, Man and Cybernetics Society, Information Assurance Workshop (IAW'03) , IEEE, page 60–67, 2003.

[RACHEDI 2008] A. RACHEDI. *Contributions à la sécurité dans les réseaux mobiles ad Hoc.* Thèse de doctorat, Université d'Avignon et des Pays de Vaucluse., 2008.

[RAYA & HUBAUX 2007] M. RAYA et J. P. HUBAUX. *Securing vehicular ad hoc networks*. Journal of Computer Security, vol. 15, page 39–68, 2007.

[REN *et al.* 2002] K. REN, T.Y. LI, Z. G. WAN, F. BAO, R. H. DENG, et K. KIM. *Routing security in wireless ad hoc networks*. Communications Magazine, IEEE, 2002.

[RIAHLA 2008] M. RIAHLA. *Conception et mise en oeuvre d'un nouveau protocole de routage Multi chemins sécurisé pour les réseaux ad hoc basé sur les colonies de fourmis*. Thèse de magister, université de Boumerdes, pages 39–41, 2008.

[SEET *et al.* 2004] C. SEET, G. LIU, B. LEE, C. FOH, K. J. WONG et K. LEE. *A-STAR : A Mobile Ad Hoc Routing Strategy for Metropolis Vehicular Communications*. international conference of information networking, Springer press, pages 134–143, 2004.

[SHRMAN *et al.* 2004] A. SHRMAN, M. YOO et S. PARK. *Black hole Attack in Mobile Ad Hoc Networks*. ACM Southeast Regional Conference, 2004.

[SOLUCOM 2001] SOLUCOM. *Les PKI :*. Vers une Infrastructure Globale de Sécurité, 2001.

[TAMIL & NARAYANAN 2007] S. TAMIL et S. NARAYANAN. *Prevention of Blackhole Attack in MANET*. The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, Aus Wireless, 2007.

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

[TOUTOUH & ABLA 2011] J. TOUTOUH et R. ABLA. *An efficient routing protocol for green communications in vehicular ad-hoc networks*. Proceedings of the 13th annual conference companion on Genetic and evolutionary computation ACM, pages 719–726, 2011.

[TOUTOUH 2006] J. TOUTOUH. *Malaga city downtown scenario*. vanet scenaio for http ://neo.lcc.uma.es/staff/jamal/VANET/ ?q=node/11, 2006.

[VANI & RAO 2011] A. VANI et D. SREENIVASA RAO. *Removal of blackhole attack in ad hoc wireless networks to provide confidentiality security service*. nternational Journal of Engineering Science and Technology (IJEST) ,ISSN : 0975-5462, 2011.

[WAVE 2010] J. WAVE. *IEEE Std 1609.3-2010 (Revision of IEEE Std 1609.3-2007),*. IEEE Standard forWireless Access in Vehicular Environments (WAVE) Networking Services, 2010.

[WU *et al.* 2007] B. WU, J. CHEN et M. CARDEI. *A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks*. Wireless/Mobile Network Security, Springer, Berlin,, page 125–144, 2007.

[XU & JIANG 2003] Q. XU et D. JIANG. *Design and analysis of highway safety communication protocol in 5.9 GHz dedicated short range communication spectrum*. In Vehicular Technology Conference, volume 4, pages 2451–2455, 2003.

[YASINAC 2002] A. YASINAC. *An Environment for Security Protocol Intrusion Detection*. Journal of Computer Security, Vol. 10, No. 1-2, 2002, pages 77–88, 2002.

[Yi & KRAVET 2004] S. Yi et R. KRAVET. *MOCA : Mobile certificate authority for wireless ad hoc networks*. Proceedings of the Second Annual PKI Research Workshop (PKI 03),, 2004.

[YINGSHU *et al.* 2008] L. YINGSHU, T. THAI et W. WEILLI. Wireless sensor networks and applications (signals and communication technology). Springer ; 2008 edition (1 April 2008), 2008.

[ZHAO & VADD 2006] O. ZHAO et C. VADD. *Les protocoles de routage dans les réseaux ad hoc*. Rapport de stage,Université de Reims - UFR Sciences, 2006.

[ZHOU & HASS 1999] L.D. ZHOU et J.Z. HASS. *Securing ad hoc networks., 13(6)*. IEEE network AND SECURITY, pages 24–30, 1999.

Notations

A-STAR	Anchor-ased Street and Traffic Aware Routing
CRL	Certificate Revocation List
GPRS	General Packet Radio Service
GPS	Global Positionning System
GSM	Global System Mobile communication
GSR	Geographic Source Routing
IEEE	Institute of Electrical and Electronics Engineers
ITS	Intelligent Transportation System
MAC	Medium Access Control | | Massage Authentification Code
MANET	Mobile Ad hoc NETwork
WAVE	Wireless Access for Vehicular Environments
WiFi	Wireless Fidelity
V2I	Vehicle-to-Infrastructure
V2V	Vehicule-to-Vehicule
VADD	Vehicle-Assisted Data Delivery
RSA	Rivest Shamir Adleman
RSU	Road Side Unit
MPRs	MultiPoint Relays
NS2	Network Simulation 2
OLSR	Optimized Link State Routing
RREP	Route Reply
RREQ	Route Request
SN	Sequence Number
SUMO	Simulation of Urban Mobility
TC	Topology Control
TCL	Tools Commande Langage
TCP	Transport Control Protocol
UDP	User Datagram Protocole
VANET	Vehicule Adhoc Network
ACK	SYNchronize-ACKnowlegement
AODV	Ad Hoc On-Demand Distance Vector Routing
A-STAR	Anchor-based Street and Traffic Aware Routing
DSDV	Destination Sequenced Distance Vector Routing
DSR	Dynamic Source Routing
GPS	Global Positioning System
GPSR	Greedy Perimeter Stateless Routing
GSR	Geographic Source Routing

GF	Greedy Forwarding
GG	Gabriel Graph
IVC	Inter-Vehicle Communication
ITS	Intelligent Transportation Systems
MANET	Mobile Ad hoc Network
PDF	Packet Delivery Fraction
DoS	denial of service

إدارة الشهادات في شبكات المركبات

شبكة المركبات هي شكل من أشكال الشبكة اللاسلكية المتنقلة لتوفير الاتصالات في مجموعة من المركبات التي تختلف عن بعضها البعض وبين المركبات والمعدات الثابتة ، وعادة ما تسمى معدات الطرق. شبكات المركبات هي مشروع لأنظمة النقل الذكي. تتواصل المركبات مع بعضها البعض من خلال الاتصالات المشتركة بين المركبات بالإضافة إلى معدات الطرق عبر معدات الاتصالات إلى المركبة. والهدف من ذلك هو أن شبكة المركبات المثلى تساهم في توفير طرق أكثر أمانًا وأكثر كفاءة في المستقبل من خلال توفير المعلومات في الوقت المناسب للسائقين والسلطات المعنية. تعد شبكات الأمان الخاصة بالمركبات موضوع بحث مفتوحًا وتحدًا كبيرًا للتحدي من تعرضها لهجمات مختلفة

Résumé

Vehicular Ad-Hoc Network ou VANET, est une forme de réseau sans fil mobile Ad-Hoc, pour fournir des communications au sein d'un groupe de véhicules à portée les uns des autres et entre les véhicules et les équipements fixes à portée, usuellement appelés équipements de la route. Les réseaux véhiculaires sont des projections des systèmes de transports intelligents (Intelligent Transportation Systems -ITS). Les véhicules communiquent les uns avec les autres par l'intermédiaire de la communication inter-véhicule (Inter-Vehicle Communication -IVC) aussi bien qu'avec les équipements de la route par l'intermédiaire de la communication d'équipement-à-Véhicule (Roadside-to-Vehicle Communication RVC). Le but optimal est que les réseaux véhiculaires contribuent à des routes plus sûres et plus efficaces à l'avenir en fournissant des informations opportunes aux conducteurs et aux autorités intéressées. La sécurité des réseaux véhiculaires représente un sujet de recherche ouvert et un défi majeur au regard de leur vulnérabilité aux différentes attaques

Abstract

Vehicular Ad-Hoc Network (Ad-Hoc network of vehicles), or VANET, is a form of mobile wireless network (Ad-Hoc Mobile Ad-hoc NETworks-MANET), to provide communications in a group of vehicles within range of each other and between vehicles and stationary equipment range, usually called road equipment. Vehicular networks are a projection of Intelligent Transport Systems (ITS-Intelligent Transportation Systems). Vehicles communicate with each other through inter-vehicle communications (Inter-Vehicle Communication-IVC) as well with road equipment via the communication equipment to vehicle (Roadside-to-Vehicle Communication- RVC). The goal is that the optimal vehicular networks will contribute to safer roads and more efficient in the future by providing timely information to drivers and concerned authorities. The security of vehicular networks is an open research topic and a major challenge in terms of their vulnerability to various attacks