



UNIVERSITE ELHADJ LAKHDER - BATNA
FACULTE DES SCIENCES DE L'INGENIEUR
DEPARTEMENT D'INFORMATIQUE



Mémoire

présenté en vue de l'obtention du diplôme

Magister en Informatique

Option: Ingénierie des systèmes informatiques (ISI)

Présenté et soutenu publiquement par :

Noureddine CHAIB

Titre :

La sécurité des communications dans les réseaux VANET

JURY

M. Abdelmadjid ZIDANI	Président	Maître de conférences, université de Batna.
M. Mohamed BENMOHAMED	Examineur	Professeur, université de Constantine.
M. Azzedine BILAMI	Examineur	Maître de conférences, université de Batna.
M. Mohamed YAGOUBI	Rapporteur	Maître de conférences, université de Laghouat.
M. Nasreddine LAGRAA	Invité	Maître de conférences, université de Laghouat.

Table des matières

Introduction générale	1
Chapitre 1 Introduction aux réseaux VANET	
1.1 Introduction.....	3
1.2 Les réseaux ad hoc	4
1.3 Les réseaux VANET	5
1.3.1 Les services offerts par les réseaux VANET.....	6
1.3.2 Les modes de communication dans les réseaux VANET	7
1.3.3 Les caractéristiques des VANETs	9
1.4 Conclusion	10
Chapitre 2 Notions et mécanismes de sécurité	11
2.1 Introduction.....	11
2.2 La sécurité dans les réseaux sans-fil ad hoc.....	12
2.2.1 Caractéristiques de la sécurité dans les réseaux sans-fil ad hoc.....	12
2.2.2 Les objectifs de la sécurité.....	13
2.2.3 Le modèle d'un attaquant	13
2.2.4 Les attaques dans les réseaux sans-fil ad hoc.....	14
2.3 Notions et mécanismes de base de la sécurité.....	15
2.4 Infrastructure à clés publiques PKI (<i>Public Key Infrastructure</i>).....	16
2.5 La sécurité dans les VANETs	16
2.5.1 Attaques spécifiques sur les VANETs	17
2.5.2 Les éléments de base de la sécurité dans les VANETs	19
2.5.3 La confidentialité dans les VANET.....	21
2.6 Les systèmes de détection d'intrusion	22
2.6.1 Notions sur les systèmes de détection d'intrusion	22
2.6.2 Les approches de détection	23
2.6.3 Le modèle de Denning	24
2.6.4 Applications et applicabilité des SDI dans les VANETs.....	27
2.7 Les systèmes de réputation.....	27

2.8	Conclusion	28
Chapitre 3 La sécurité de routage dans les réseaux ad hoc		30
	Introduction	30
3.1	Le routage dans les réseaux ad hoc	31
3.2	Classification des protocoles de routage dans les réseaux ad hoc	31
3.2.1	Les protocoles de routage basés sur la topologie	31
3.2.2	Les protocoles de routage géographique	32
3.3	Rappel sur les protocoles de routage ad hoc.....	32
3.3.1	AODV	33
3.3.2	GPSR	33
3.4	Les attaques contre les protocoles de routage.....	34
3.4.1	Pour quoi attaquer les protocoles de routage ?	34
3.4.2	Les mécanismes d’attaques contre les protocoles de routage	34
3.4.3	Exemples d’attaques contre les protocoles de routage.....	35
3.5	Les protocoles de routage ad hoc sécurisés	36
3.5.1	SRP.....	36
3.5.2	ARIADNE	38
3.5.3	SAODV	39
3.5.4	SPAAR	39
3.5.5	DSR avec WATCHDOG et PATHRATER	40
3.6	Etude comparative et synthèse	42
3.6.1	Performance	42
3.6.2	Discussion des aspects de sécurité et de confidentialité	44
3.7	Conclusion	45
Chapitre 4 La protection contre les nœuds malveillants		46
4.1	Introduction.....	46
4.2	La sécurité de routage dans les réseaux VANET	47
4.2.1	Les protocoles de routage existants dans les réseaux VANET	47
4.2.2	Le choix d’un protocole pour les VANETs	48
4.3	Les protocoles de révocation distribuée.....	49
4.3.1	Définition de la révocation distribuée	50

4.3.2	L'architecture d'un Protocole de Révocation Distribuée (PRD)	52
4.3.3	Les critères de performance d'un protocole de révocation distribuée.....	54
4.3.4	Le graphe d'accusation	55
4.3.5	Les protocoles de révocation distribuée basés sur le vote existants	56
4.4	Conclusion	63
Chapitre 5 Notre nouveau protocole SEDIREP (SEcure DIstributed REvocation Protocol)		
5.1	Introduction.....	65
5.2	Le modèle d'adversaire	66
5.3	Le protocole SEDIREP (SEcure DIstributed REvocation Protocol)	67
5.3.1	Les hypothèses de conception du protocole SEDIREP	67
5.3.2	Le mécanisme de détection d'intrusion.....	68
5.3.3	La description du protocole SEDIREP.....	70
5.4	Analyse de performance de l'algorithme utilisé par SEDIREP.....	78
5.4.1	Simulation.....	78
5.4.2	Résultats et discussions	80
5.4.3	Analyse de la complexité de l'algorithme utilisé.....	89
5.5	Conclusion	89
Bibliographie		92
Annexe		99
Glossaire.....		103

Table des figures

Figure 1.1 Exemple de transmission d'un message dans un réseau ad hoc	4
Figure 1.2 : Les éléments constituant le véhicule intelligent	6
Figure 1.3 : Les modes de communication dans les VANETs	8
Figure 2.1 : Attaques par l'envoi de messages falsifiés	17
Figure 2.2 : Attaque déni de service	18
Figure 2.3 : Attaque de révélation d'identité et de position géographique d'un véhicule	19
Figure 2.4 : Format d'un paquet balise.....	21
Figure 3.1 : Les opérations et le format de message de SRP	37
Figure 3.2 : Les opérations et le format de message d'ARIADNE basé sur la signature numérique	38
Figure 3.3 L'écoute en mode promiscuous	41
Figure 4.1 : L'importance de la révocation distribuée	51
Figure 4.2 L'architecture d'un protocole de révocation distribuée	53
Figure 4.3: Exemple d'un graphe d'accusation d'un nœud N.....	55
Figure 4.4 : Un graphe d'accusation illustratif	59
Figure 5.1: Les types d'accusations dans un graphe d'accusation	67
Figure 5.2 : Vérification de localisation en utilisant la zone de couverture	69
Figure 5.3: Le format de message du protocole SEDIREP	71
Figure 5.4 : Taux de détection des nœuds malveillants(cas 20% de nœuds sont malveillants et seuil=0.5) ..	80
Figure 5.5 : Taux des nœuds faux positifs (cas 20% de nœuds sont malveillants et seuil=0.5)	81
Figure 5.6 : Taux de détection des nœuds malveillants(cas 20% de nœuds sont malveillants et seuil=0.25) .	83
Figure 5.7 : Taux de faux positifs (cas 20% de nœuds sont malveillants et seuil=0.25).....	84
Figure 5.8 : Taux de détection des nœuds malveillants(cas 30% de nœuds sont malveillants et seuil=0.5) ...	85
Figure 5.9 : Taux de faux positifs (cas 30% de nœuds sont malveillants et seuil=0.5).....	86
Figure 5.10 : Taux de détection des nœuds malveillants(cas 30% de nœuds sont malveillants et seuil=0.25)	87
Figure 5.11 : Taux de faux positifs (cas 30% de nœuds sont malveillants et seuil=0.25).....	88
Figure 6.1 : Exemple illustrant les nœuds exclus par SEDIREP	99

Liste des tableaux

Table 1 : La performance des protocoles de routage ad hoc sécurisés dans les VANETs	44
Table 2: Les taux d'accusation en utilisant l'algorithme de Crépeau.....	59
Table 3 : Les taux d'accusation en utilisant le protocole LEAVE	62
Table 4 : Environnement de simulation	79
Table 5 : Illustration des valeurs de différentes fonctions de SEDIREP	102

À ma défunte mère,

À mon père,

À mes frères,

À mes sœurs,

À tous ceux qui me sont chers,...

Je dédie affectueusement ce modeste travail

Remerciements

Je tiens tout d'abord à exprimer mes sincères remerciements à mes encadreurs Mr. Mohamed YAGOUBI et Mr. Nasreddine LAGRAA. Pour leurs aides sans limite et leurs précieux conseils qu'ils m'ont donnés et sans lesquels ce travail n'aurait pas vu le jour. Ils m'ont ainsi offert l'opportunité de faire mes premiers pas de scientifique sur un travail de recherche passionnant et prometteur : le monde de la sécurité des communications dans les réseaux véhiculaires.

Je remercie les membres de jury qui ont accepté de juger ce travail :

Dr. Abdelmadjid ZIDANI, maître de conférences à l'université de Batna, qui me fait le grand honneur d'accepter la présidence du jury.

Pr. Mohamed BENMOHAMMED, professeur à l'université de Constantine et Dr. Azzedine BILAMI, maître de conférences à l'université de Batna pour l'honneur qu'ils me font en acceptant de participer à ce jury.

Je suis très reconnaissant à Mr. Rabeh BOUCHELGA pour son aide.

Je remercie également tous ceux qui de près ou de loin, m'ont accompagné et soutenu pour mener à bien ce travail, j'adresse un remerciement particulier à Mr. Abdoullah MAOUCHA.

Je remercie aussi mes professeurs, mes collègues, mes amis et toutes les personnes qui m'ont aidé durant mes études universitaires.

Résumé

Dans les prochaines années à venir, les réseaux véhiculaires seront capables de réduire significativement le nombre d'accidents via les messages d'alerte échangés entre les véhicules de proximité. La fonction de routage est un élément fondamental pour le système de communication véhiculaire ; par conséquent, il constituera une cible idéale pour les attaques qui pourrait viser à empêcher des messages d'alerte à atteindre leurs destinations, et mettre ainsi en danger les vies humaines. Malheureusement, les protocoles de routage basés seulement sur des techniques cryptographiques ne peuvent pas garantir la sécurité contre tous les attaques et particulièrement les attaques provenant de l'interne. Parmi les solutions qui répond à la contrainte temps réel des applications des VANET, l'utilisation d'un protocole de révocation distribuée conjointement avec un protocole de routage sécurisé afin de détecter et éliminer les nœuds malveillants rapidement. Cependant, la plupart des protocoles proposés sont vulnérables aux attaques de fausses alertes émises par plusieurs nœuds malveillants en coalition afin d'exclure un grand nombre de nœuds honnêtes. Dans ce travail, nous proposons un nouveau protocole de révocation distribuée SEDIREP (SEcure DIstributed REvocation Protocol) destiné aux réseaux VANET, il permet aux nœuds d'un réseau VANET d'éviter d'utiliser les nœuds malveillants comme relais pour l'acheminement des messages liés à la sécurité. Les résultats de simulation montrent que SEDIREP assure un taux de détection élevé et un faible taux de faux positifs même en présence d'un nombre élevé d'attaquants.

Mots clés: Révocation distribuée, Routage sécurisé, SDI, VANET

Abstract

In the next few years, vehicular networks will be able to reduce significantly the number of accidents by way of warning messages exchanged among nearby vehicles. The routing function is a building block for the vehicular communication system, so it will be an ideal target for attacks that could aim to prevent alert messages from reaching their destinations, thus endangering human lives. Unfortunately, routing protocols based only on cryptographic techniques cannot guarantee security against all attacks, especially insider attacks. Among the solutions that meet the real time constraint of VANET applications, using a distributed revocation protocol together with a secure routing protocol to detect and avoid malicious nodes quickly. However, most proposed systems are vulnerable to false alerts issued by several colluding malicious nodes to exclude a large number of honest nodes. In this work, we propose a novel distributed revocation protocol SEDIREP (SEcure DIstributed REvocation Protocol) for VANETs, it allows nodes in a VANET network to avoid using malicious nodes as relays for transmitting safety related messages. The simulation results show that SEDIREP provides a high detection rate and low false positive rate even in the presence of a large number of attackers.

Keywords: Distributed revocation, Secure routing, IDS, VANET

Introduction générale

Le développement technologique qu'a vu le monde d'aujourd'hui a touché tous les domaines, particulièrement le secteur de la communication qui connaît une évolution considérable par l'apparition de la technologie sans-fil.

Les chercheurs pensent pouvoir exploiter cette technologie afin de permettre aux véhicules d'établir des liens entre eux, avec ou sans infrastructures installées aux bords des routes, ce qui constitue les nouveaux réseaux appelés VANET (*Vehicular Ad-Hoc NETWORK*). Une des applications prometteuse de ces réseaux consiste à permettre aux véhicules équipés de capteurs spécifiques de détecter l'environnement proche et d'avertir les conducteurs des véhicules aux alentours suffisamment tôt en cas de risques d'accident.

Vu l'importance des informations échangées entre les véhicules et l'ouverture de l'environnement VANET, un attaquant peut émettre des messages d'alerte dont le contenu est falsifié ou empêcher l'acheminement d'un message légitime afin de causer des accidents.

L'attaquant peut empêcher l'acheminement de ces messages en visant la disponibilité du réseau aux niveaux des différentes couches de la pile protocolaire. Comme le routage est un service fondamental dans tout système de communication, il peut être une cible idéale pour les attaques [1]. Malheureusement, les contraintes entraînées par la forte mobilité des nœuds dans ces réseaux et leur aspect décentralisé, rend la sécurité de routage plus problématique que tout autre type de réseau.

Parmi les solutions proposées pour améliorer la sécurité des protocoles de routage dans les réseaux ad hoc, il y a l'utilisation d'un système de détection d'intrusion (SDI) [2] afin de détecter et éviter de choisir les nœuds malveillants comme relais. Mais, les SDI ne peuvent assurer une détection rapide et efficace qu'au détriment d'une consommation élevée de la bande passante dans les VANETs, donc cette solution ne peut être envisagée pour la sécurité de routage dans les VANETs qui sont fortement contraignants en délai et en bande passante [3]. Ainsi, la solution consistant à intégrer les systèmes de réputation dans les protocoles de routage est difficile à appliquer dans ces réseaux caractérisés par une connectivité sporadique et de courte durée [4] [5].

La solution de révocation distribuée est considérée comme la solution la plus efficace et adéquate aux VANETs. Cependant, les protocoles de révocation distribuée (PRD) sont eux-mêmes vulnérables aux attaques de fausses alertes coordonnées qui visent à exclure un nombre important de nœuds.

Ce travail est consacré à l'étude du problème de l'exclusion des nœuds malveillants de l'opération de routage. Nous essayons à adapter un protocole de routage ad hoc sécurisé aux réseaux VANET, nous proposons des améliorations sur les PRD existants et nous proposons un nouveau protocole de révocation distribuée « SEDIREP ». Ce protocole est destiné à être utilisé conjointement avec un protocole de routage sécurisé dans les réseaux VANET, il a tous les mécanismes qui assurent un taux élevé de détection de nœuds malveillants tout en réduisant l'impact de fausses alertes sur la disponibilité du réseau.

Ce mémoire est composé de cinq chapitres : le premier chapitre est consacré aux généralités sur les réseaux ad hoc et particulièrement les réseaux VANET. Le second présente la sécurité dans les réseaux ad hoc de manière générale et montre les mécanismes utilisés et ceux qui peuvent être mis en œuvre pour la sécurité dans les VANETs. Le troisième chapitre présente la sécurité de routage dans les réseaux ad hoc. Le quatrième chapitre décrit le protocole de routage sécurisé SAODV que nous avons adapté aux réseaux VANET et présente les mécanismes de protection contre les nœuds malveillants. Enfin, le cinquième chapitre contient la description du protocole que nous avons proposé et analyse son efficacité par les différentes simulations.

Chapitre 1

Introduction aux réseaux VANET

1.1 Introduction

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

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

Dans ce chapitre, nous présentons d'abord les réseaux ad hoc de manière générale, puis, nous abordons aux réseaux VANET, les différents types de services offerts par ces réseaux et les modes de communication existants; enfin nous décrivons les différentes caractéristiques, contraintes et défis qui affronteront les concepteurs lors de la conception des protocoles dédiés à ce type de réseau.

1.2 Les réseaux ad hoc

Les réseaux ad hoc sont des réseaux sans-fil capables de s'organiser spontanément et de manière autonome dans l'environnement dans lequel ils sont déployés sans infrastructure définie préalablement. La tâche de la gestion du réseau est répartie sur l'ensemble d'entités communicantes par liaison sans-fil, ces entités sont souvent appelées «nœuds». Dans ces réseaux, les entités envisagées sont des terminaux légers et de taille réduite qui fonctionnent sur batterie, donc elles ont des capacités de traitement et de mémoire limitées [6].

Les réseaux ad hoc, dans leur configuration mobile, sont connus sous le nom de MANET (pour Mobile Ad-hoc NETWORKS).

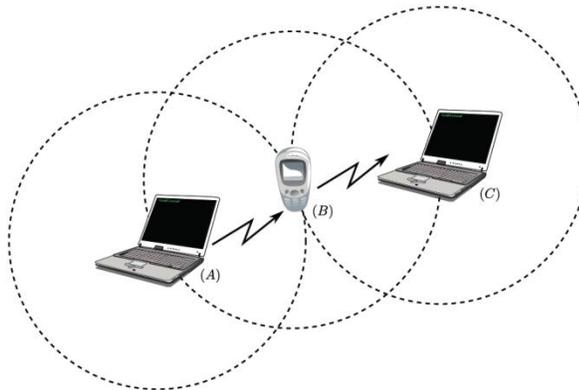


Figure 1.1 Exemple de transmission d'un message dans un réseau ad hoc [6] :l'entité A veut communiquer avec C. Puisqu'elles sont hors de portée directe de transmission, A transmet son message vers B, qui à son tour le relaie vers C

La figure 1.1 montre un exemple de transmission d'un message dans un réseau ad hoc entre deux équipements distants A et C, comme ces deux derniers ne peuvent pas communiquer directement à cause de la portée limitée de supports de transmission utilisés, alors ils utilisent l'équipement B comme relai.

Les réseaux ad hoc peuvent être utilisés dans tous les situations où le déploiement d'une infrastructure est contraignant ou coûteux. Parmi ces applications nous citons :

- **Applications militaires** : comme ces réseaux peuvent être déployés rapidement et avec très peu d'intervention humaine dans n'importe quelle situation, ils sont bien adaptés aux environnements hostiles tel que les champs de bataille [6].

- **Contrôle d'environnement** : des détecteurs (capteurs) éparpillés à travers une zone géographique peuvent être utilisés afin de collecter un ensemble d'informations (par exemple : la température, l'humidité), et de l'envoyer à travers un réseau ad hoc à une station traitant ces informations.
- **Opérations de secours**: les unités de secours peuvent utiliser ces réseaux, lorsque les infrastructures de télécommunications sont détruites (par exemple : à cause d'une catastrophe naturelle) et que l'établissement d'une liaison satellite pour chaque entité en communication est très coûteux.
- **Événements occasionnels**: les réseaux ad hoc peuvent être utilisés pour la mise en place instantanée d'un réseau reliant plusieurs ordinateurs portables entre eux. Ils s'avèrent particulièrement utiles lors de l'organisation d'événements tels que des conférences, des séminaires,...etc.

1.3 Les réseaux VANET

Les réseaux VANETs (Vehicular Ad hoc NETWORKs) constituent une nouvelle forme de réseaux ad hoc mobiles (MANET). 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 nœuds rendant la topologie du réseau fortement dynamique.

Pour la mise en place d'un tel réseau, certains équipements électroniques doivent être installés au sein de véhicules (cf. figure 1.2), tel: les dispositifs de perception de l'environnement (radars, caméras), un système de localisation GPS, et bien sûr une plateforme de traitement.

Plusieurs technologies peuvent être mises en œuvre pour l'établissement des communications véhiculaires, tel : les réseaux sans-fil de type 802.11, WIMAX, Bluetooth. Cependant, il existe une nouvelle famille de standards qui sont en cours de standardisation par l'équipe de travail IEEE1609.

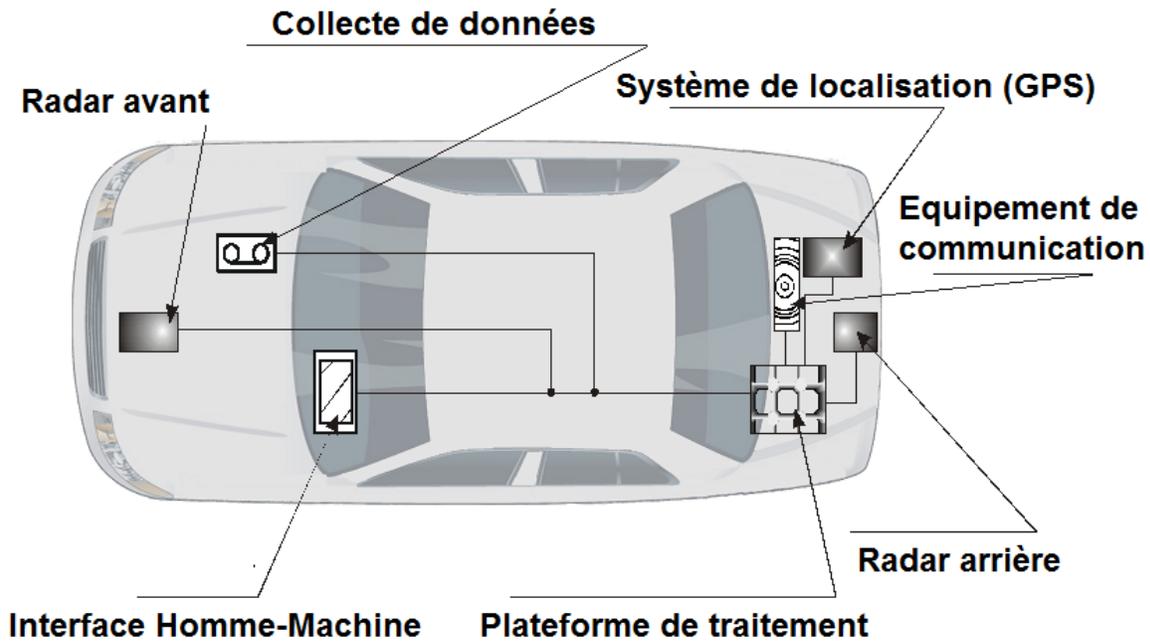


Figure 1.2 : Les éléments constituant le véhicule intelligent [7]

1.3.1 Les services offerts par les réseaux VANET

- **Les services liés à 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 (par exemple : les radars et les caméras) installés au niveau des véhicules ou bien au centre de contrôle, ainsi que la diffusion de messages fournissant des informations sur l'état du réseau routier (trafic, travaux, météo), ou rappelant au conducteur les limitations de vitesse, les distances de sécurité ou qu'il s'approche d'une intersection, avant même de la voir. Certains services peuvent automatiquement effectuer les actions appropriées pour éviter les accidents alors que d'autres services se contenteront d'assister les conducteurs.

- **Services liés au confort:**

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. Le champ d'application de ces services, à ce stade, est très large et offre des perspectives intéressantes aux opérateurs de télécommunications en leurs permettant de réaliser des bénéfices supplémentaires.

1.3.2 Les modes de communication dans les réseaux VANET

Dans les réseaux de véhicules, on peut distinguer deux modes de communication, les communications Véhicule-à-Véhicule (V2V) et les communications Véhicule-à-Infrastructure (V2I) [8] [9](cf. figure 1.3). Les véhicules peuvent utiliser un de ces deux modes ou bien les combiner s'ils ne peuvent pas communiquer directement avec les infrastructures. Dans cette section, nous présentons le principe et l'utilité de chaque mode :

a- Mode de communication Véhicule-à-Véhicule (V2V)

Ce mode de communication fonctionne suivant une architecture décentralisée, et représente un cas particulier des réseaux ad hoc mobiles, Il est basé sur la simple communication inter-véhicules ne nécessitant pas une infrastructure. En effet, un véhicule peut communiquer directement avec un autre véhicule s'il se situe dans sa zone radio, ou bien par le biais d'un protocole multi-sauts qui se charge de transmettre les messages de bout en bout en utilisant les nœuds voisins qui les séparent comme des relais. Dans ce mode, les supports de communication utilisés sont caractérisés par une petite latence et un grand débit de transmission [10] [11].

Les communications V2V sont très efficaces pour le transfert des informations concernant les services liés à la sécurité routière, mais elles ne garantissent pas une connectivité permanente entre les véhicules.

b- Mode de communication de Véhicule à Infrastructure (V2I)

Ce mode de communication permet une meilleure utilisation des ressources partagées et démultiplie les services fournis (par exemple : accès à Internet, échange de données de voiture-à-domicile, communications de voiture-à-garage de réparation pour le diagnostic distant, ...etc.) grâce à des points d'accès RSU (*Road Side Units*) déployés aux bords des routes; ce mode est inadéquat pour les applications liées à la sécurité routière car les réseaux à infrastructure ne sont pas performants quant aux délais d'acheminement [12].

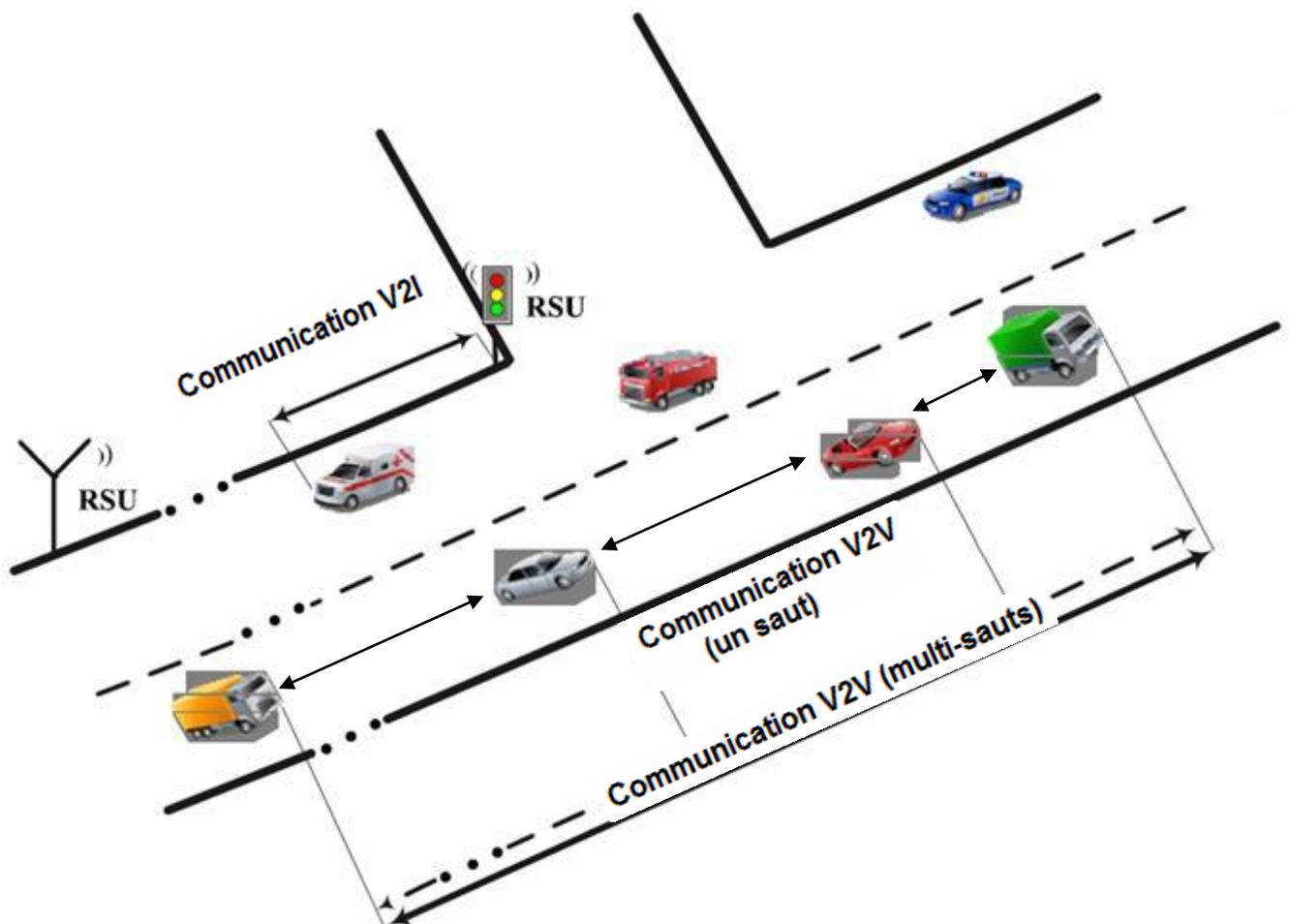


Figure 1.3 : Les modes de communication dans les VANETs [13]

1.3.3 Les caractéristiques des VANETs

Les réseaux véhiculaires ont des caractéristiques spécifiques qui les distinguent de réseaux ad hoc mobiles, Ces caractéristiques doivent être prises en compte lors de conception des protocoles pour les VANETs.

Dans cette partie, nous présentons quelques propriétés et contraintes concernant ce type de réseau :

- **La capacité d'énergie et stockage:** contrairement au contexte des réseaux MANET où la contrainte d'énergie représente un défi pour les chercheurs, les éléments du réseau VANET disposent suffisamment d'énergie [12] qui peut alimenter les différents équipements électroniques d'une voiture intelligente. Donc, les nœuds sont censés avoir une grande capacité de traitement et de stockage de données.
- **La topologie et la connectivité:** comme les réseaux ad hoc mobiles, les réseaux VANET sont caractérisés par une connectivité sporadique, car un véhicule (nœud) peut rejoindre ou quitter un groupe de véhicules en un temps très court, ce qui nous mène ainsi à avoir une topologie très dynamique constituée de plusieurs ilots séparés [12].
- **Le modèle de mobilité:** plusieurs facteurs peuvent affecter la mobilité dans ces réseaux comme les infrastructures routières; par exemple : route, autoroute, panneaux de signalisation [14]. En outre, la mobilité dans les VANETs est liée directement au comportement des conducteurs et leurs réactions face à des obstacles ou des situations différentes et complexes rencontrées; par exemple: les heures d'embouteillage, les accidents,... etc.
- **La sécurité et l'anonymat :** l'importance des informations échangées via les communications véhiculaires rend l'opération de sécurisation de ces réseaux cruciale qui constitue un pré-requis au déploiement des VANETs [15].

1.4 Conclusion

Dans ce chapitre, nous avons montré 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 attaques sur les VANETs, et nous présentons les mécanismes qui ont été mis en œuvre afin d'améliorer la sécurité de ces réseaux.

Chapitre 2

Notions et mécanismes de sécurité

2.1 Introduction

Les communications véhiculaires constitueront dans le futur le plus grand réseau ad hoc viable. De plus, la vie de milliers d'êtres humains sera dépendante des informations échangées entre les véhicules eux-mêmes et avec les infrastructures. A cause de l'importance des informations échangées et du nombre énorme d'utilisateurs, l'environnement des réseaux véhiculaires sera plus qu'hostile. En effet, les messages liés à la sécurité peuvent être falsifiés ou éliminés par des entités malveillantes afin de causer des accidents et mettre en péril la vie des personnes. Donc, avant le déploiement de ces réseaux, des mécanismes de sécurité appropriés doivent être mis en œuvre afin d'éviter ces mauvais scénarios et d'identifier les entités responsables de ces activités malveillantes.

Dans ce chapitre, nous présentons un récapitulatif sur les outils et mécanismes de base de la sécurité en générale, nous passons en revue la sécurité dans les réseaux sans-fil, ensuite nous présentons les problèmes et les mécanismes de base de sécurité dans les VANETs, enfin nous étudions les techniques et solutions de sécurité existantes qui peuvent être mises en œuvre afin de sécuriser les informations échangées à travers ces réseaux.

2.2 La sécurité dans les réseaux sans-fil ad hoc

Comme les réseaux VANET peuvent être considérés comme une sous classe des réseaux sans-fil ad hoc, ils en héritent les problèmes de sécurité. Dans cette section, nous nous intéressons à la sécurité des réseaux sans-fil ad hoc de manière générale, nous présentons quelques exemples d'attaques sur ces réseaux, ensuite nous en décrivons les objectifs de sécurité.

2.2.1 Caractéristiques de la sécurité dans les réseaux sans-fil ad hoc

Lors de l'analyse de la nature des communications dans les réseaux ad hoc, des propriétés spécifiques liées à la sécurité et la confidentialité doivent être prises en compte pour la conception des protocoles de communications, à savoir [16]:

- 1. Un support de transmission partagé:** comme avec tout système de communication sans-fil, l'utilisation des ondes radio permet aux attaquants d'intercepter facilement les messages échangés ou bien d'injecter de faux messages dans le réseau.
- 2. Les communications multi-sauts :** les protocoles de communications multi-sauts sont obligatoires pour avoir des communications sans-fil à longue portée dans les réseaux ad hoc; cela signifie que tous les nœuds doivent coopérer pour assurer le fonctionnement du réseau. Malheureusement, les nœuds malveillants peuvent exploiter ce principe et mettre en péril la sécurité du réseau, donc des mécanismes de sécurité appropriés doivent être mis en œuvre.
- 3. La diffusion d'information de la position géographique:** avec certains protocoles dans les réseaux ad hoc mobiles, les nœuds sont supposés envoyer périodiquement des messages (balises) indiquant leurs positions courantes ou éventuellement d'autres données nécessaires pour des services spécifiques. Par conséquent, les attaquants peuvent créer un profil sur les trajectoires des nœuds et donc les utilisateurs du réseau.
- 4. Les opérations autonomes:** les nœuds eux mêmes déterminent leurs états et décident des informations à envoyer de manière autonome. Par conséquent, il est facile pour les entités malveillantes qui ont le contrôle sur un ou plusieurs nœuds d'envoyer des informations falsifiées. Les systèmes de sécurité, à leur tour, doivent employer des mécanismes qui détectent et empêchent l'utilisation de ces informations.

2.2.2 Les objectifs de la sécurité

La sécurisation des communications dans les réseaux sans-fil comme dans les réseaux filaires nécessite la mise en œuvre de mécanismes permettant d'atteindre un certain nombre d'objectifs généraux de sécurité. Ces objectifs comprennent [17]:

- **L'authentification:** cet objectif de sécurité permet aux membres du réseau de s'assurer de la bonne identité des membres avec lesquels ils communiquent.
- **La non-répudiation:** cet objectif de sécurité permet de s'assurer qu'aucun émetteur ne peut nier d'être à l'origine d'un message. Cet objectif est indispensable dans les transactions électroniques et dans toutes les communications sensibles.
- **La confidentialité:** cet objectif de sécurité garantit que seules les parties autorisées peuvent accéder aux données transmises à travers le réseau. Ces données peuvent concerner la couche applicative ou les couches inférieures.
- **L'intégrité:** cet objectif de sécurité permet de s'assurer que les données échangées ne sont pas soumises à une altération volontaire ou accidentelle. Donc, il permet aux destinataires de détecter les manipulations de données effectuées par les entités non autorisées et rejeter les paquets correspondants.
- **La disponibilité:** cet objectif de sécurité vise à garantir aux entités autorisées d'accéder aux ressources du réseau avec une qualité de service adéquate [17].

2.2.3 Le modèle d'un attaquant

La première étape pour sécuriser un système est l'identification de la nature des éventuels attaquants. Dans les réseaux ad hoc, nous pouvons classifier un attaquant selon les dimensions suivantes:

- **Interne vs. Externe :** l'attaquant interne est perçu comme un membre normal du réseau et peut communiquer avec les autres membres. La présence des attaques internes est très problématique et difficile à détecter, car elle annule le niveau de sécurité assuré par les techniques cryptographiques. L'attaquant externe est considéré par les nœuds membres comme un intrus et est donc limité dans la diversité des attaques qu'il peut provoquer [18].

- **Malveillant vs Rationnel** : un attaquant malveillant n'a pas d'intérêts personnels à travers ses attaques et a pour but le dysfonctionnement du réseau. Par conséquent, il peut employer tous les moyens sans tenir compte des coûts correspondants et des conséquences. Par contre, un attaquant rationnel cherche un profit personnel, et ainsi, on peut prévoir les cibles d'attaques et les moyens employés [18].
- **Passif vs. Actif** : l'attaquant passif écoute simplement les informations qui sont échangées entre les nœuds tandis que l'attaquant actif agit sur les informations qui sont échangées. Il peut les falsifier, les modifier, voire même les détruire [18].

2.2.4 Les attaques dans les réseaux sans-fil ad hoc

Dans les réseaux sans-fil ad hoc, la nature du support de transmission rend ces réseaux plus vulnérables aux attaques qu'un réseau filaire. Un réseau sans-fil qui n'est pas bien sécurisé est exposé à de plusieurs types d'attaques ; nous en citons :

- **L'écoute des communications** (en anglais, *eavesdropping* ou *sniffing*): dans ce type d'attaque, l'adversaire ou l'entité malveillante écoute sur le support de transmission afin d'extraire des informations sur le trafic échangé dans son voisinage; il se peut qu'il veuille espionner sur des informations personnelles, ou bien collecter des informations pour les analyser et effectuer ensuite d'autres types d'attaques.
- **L'accès non-autorisé** : dans cette attaque, les entités malveillantes accèdent aux services du réseau sans en avoir les droits ou les privilèges [17].
- **Le déni de service** (souvent dénoté par DoS abréviation de l'expression en anglais « *Denial of Service* ») : il consiste à rendre les différentes ressources et les services indisponibles pour les utilisateurs dans le réseau; il est généralement provoqué par d'autres attaques visant la bande passante ou les ressources énergétiques des autres nœuds. La technique la plus naïve pour causer un déni de service dans un réseau sans-fil consiste à causer le brouillage du canal (en anglais *Jamming*); une autre attaque appelée « privation de sommeil » qui consiste à demander un service que le nœud visé offre de manière répétitive afin de lui gaspiller ses ressources systèmes et de l'empêcher de "se reposer" [19].

- **L'usurpation de l'identité d'un nœud** (en anglais, *Spoofing* ou *Impersonation*) : dans ce type d'attaques, l'attaquant essaie de prendre l'identité d'un autre nœud afin de pouvoir recevoir ses messages ou d'avoir des privilèges qui ne lui sont pas accordés.

2.3 Notions et mécanismes de base de la sécurité

- **La cryptographie** : la cryptographie est une des disciplines de la cryptologie s'attachant à protéger des messages en employant souvent des secrets ou des clés. Elle consiste à appliquer des transformations sur le contenu d'un message à l'aide des algorithmes de chiffrement (afin de l'en rendre incompréhensible) et de déchiffrement (afin de reconstruire le message original).
- **La cryptographie symétrique** (ou cryptographie à clé secrète) : elle consiste à utiliser une seule clé secrète partagée entre l'expéditeur et le destinataire pour chiffrer et déchiffrer les données.
- **La cryptographie asymétrique**(ou cryptographie à clé publique) : elle repose sur l'utilisation d'une clé publique (qui est diffusée) et d'une clé privée (gardée secrète), l'une permettant de coder le message et l'autre de le décoder.
- **Le hachage** : il consiste à déterminer une information de taille fixe et réduite (appelée l'empreinte ou le condensé) à partir d'une donnée de taille indifférente.
- **Les fonctions de hachage à sens unique** : une fonction de hachage à sens unique est une fonction irréversible qui fournit l'empreinte à partir d'une chaîne fournie en entrée. La particularité de cette fonction est qu'il est aisé de calculer l'empreinte d'une chaîne donnée, mais il est difficile de retrouver ou déduire la chaîne initiale à partir de l'empreinte [20].
- **La signature numérique**: c'est un code numérique associé à un message électronique afin que les destinataires puissent en authentifier les origines et en vérifier l'intégrité. Son implémentation fait appel aux fonctions de hachage et à clé privée du signataire.
- **Le MAC (Message Authentication Code)** : c'est un code accompagnant des données qui assure les mêmes fonctionnalités de la signature numérique, mais son implémentation se base sur l'utilisation de la clé secrète et sur des fonctions similaires à celles de hachage.

- **Le certificat numérique:** c'est une structure de données permettant de prouver l'identité du propriétaire d'une clé publique. Les certificats numériques sont signés et délivrés par un tiers de confiance appelé l'**autorité de certification** (AC).

2.4 Infrastructure à clés publiques PKI (*Public Key Infrastructure*)

Une infrastructure à clés publiques est un ensemble de composants physiques (des ordinateurs, des équipements cryptographiques logiciels ou matériels), de procédures humaines (vérifications, validation) et de logiciels (système et application) qui permettent de gérer le cycle de vie des certificats numériques [21].

Une infrastructure à clés publiques fournit un ensemble de services pour le compte de ses utilisateurs comprenant leur enregistrement, la génération et le renouvellement de certificats et la publication de la liste de révocation de certificats LRC¹. Ce dernier service est vital pour la sécurité d'un réseau ad hoc, dans lequel les clés peuvent être compromises à n'importe quel moment ; donc les membres du réseau doivent pouvoir accéder à cette information à tout moment et avec un coût raisonnable en termes de bande passante et de traitement.

2.5 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 décrits dans la section 2.2.2, 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 mis en œuvre pour la sécurité de ces réseaux.

¹ La liste de révocation de certificat a pour objectif de gérer la situation quand la clé privée d'un utilisateur est compromise, ou le propriétaire de cette clé a été exclu du réseau par exemple.

2.5.1 Attaques spécifiques sur les VANETs

Dans cette section, nous passons en revue quelques attaques spécifiques sur les VANETs. Ces attaques comprennent :

- **L'injection des messages erronés** (cf. figure 2.1): 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.

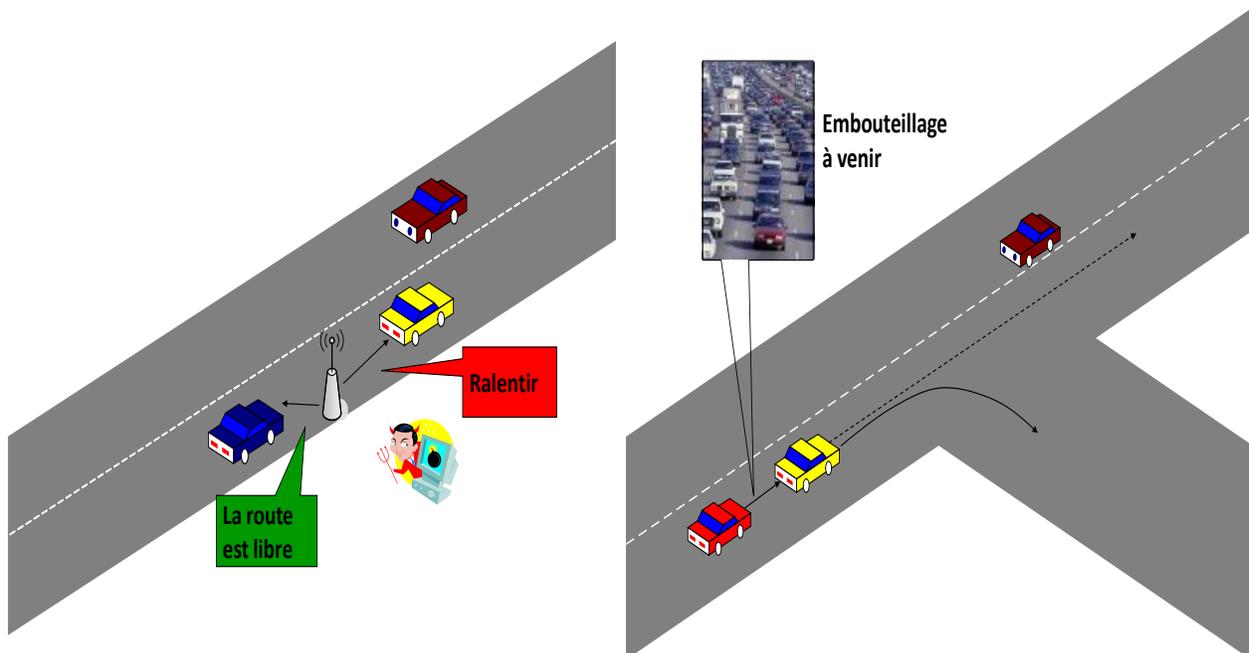


Figure 2.1 : Attaques par l'envoi de messages falsifiés [7]

- **Le déni de service** (cf. figure 2.2): 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.

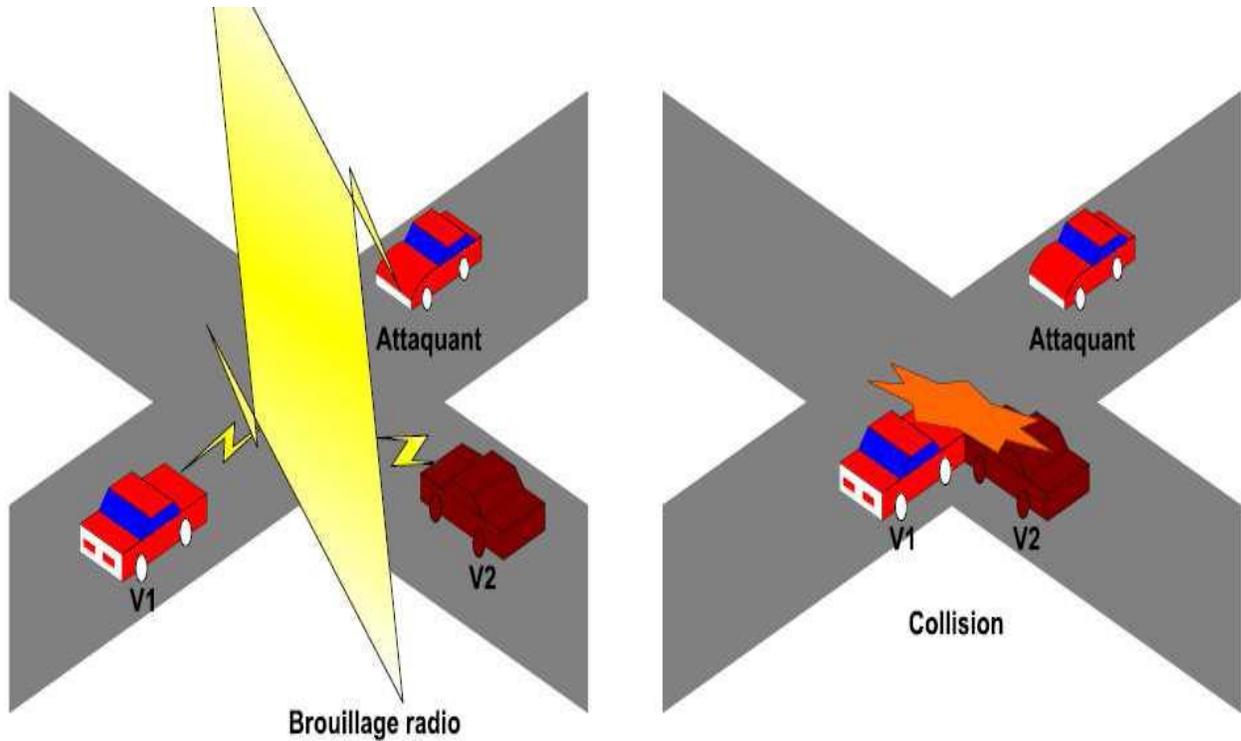


Figure 2.2 : Attaque déni de service [8] : en utilisant le brouillage du canal l'attaquant empêche V1 et V2 à recevoir les messages liés à la sécurité.

- **La révélation d'identité et de position géographique des autres véhicules** (cf. figure 2.3) : 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 (il peut être par exemple une entreprise de location de voitures qui veut suivre ses propres véhicules de manière illégitime).

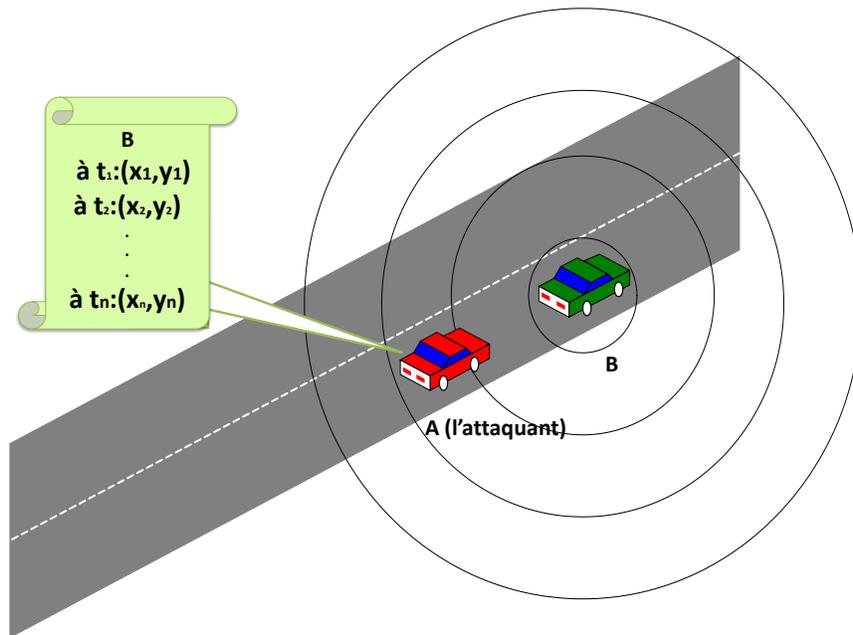


Figure 2.3 : Attaque de révélation d'identité et de position géographique d'un véhicule

2.5.2 Les éléments de base de la sécurité dans les VANETs

2.5.2.1 Le TPD (Tamper-Proof Device)

C'est un dispositif considéré comme inviolable utilisé pour stocker les informations sensibles comme les clés privées et toutes informations confidentielles, et chargé de signer les messages sortants.

Le TPD est conçu de manière à détruire automatiquement toutes les informations stockées lors de la manipulation matérielle. A cet effet, il contient un ensemble de capteurs qui lui permettent de détecter ces manipulations et effacer toutes les informations stockées afin de les empêcher d'être compromises [22]. Ce module est connu aussi sous le nom de HSM (Hardware Security Module) [23].

2.5.2.2 Les certificats dans les VANETs

Pour assurer les objectifs de sécurité dans ces réseaux, des outils cryptographiques doivent être mis en œuvre. La cryptographie asymétrique présente des solutions possibles pour les VANETs et paraît plus adéquate aux caractéristiques et exigences de ces réseaux. En effet, grâce à la cryptographie asymétrique, il est possible d'utiliser des certificats numériques pour identifier les véhicules de façon unique.

Dans les VANETs il existe deux types de certificats :

- **Le certificat à long terme** : chaque véhicule doit avoir un certificat indiquant le véhicule et son propriétaire de manière permanente ; ce type de certificat contient d'autres informations en plus comme celles concernant les caractéristiques des équipements du véhicule. Il peut être utilisé pour établir une communication sécurisée avec l'AC et renouveler les certificats à court terme.
- **Le certificat à court terme** : comme son nom l'indique, la durée de vie de ce certificat est très courte (d'environ une minute [13]); il ne doit pas contenir les informations indiquant le propriétaire du véhicule; à cet effet il utilise un pseudonyme qui permet d'identifier le véhicule de façon unique. Ce type de certificat est utilisé généralement dans les protocoles de routage.

Il faut souligner que chaque véhicule possède un seul certificat à long terme et plusieurs certificats à court terme. Ainsi, toutes les clés privées correspondantes aux clés publiques sont stockées dans le TPD, donc le TPD doit avoir une grande capacité de stockage afin que les véhicules puissent communiquer de manière sécurisée même en absence de connectivité avec l'AC pour des périodes très longues.

2.5.2.3 La sécurité du système de balisage

Le balisage (en anglais *Beaconing*) consiste en la diffusion périodique aux voisins à-un saut d'un paquet spécifique contenant des informations utiles pour les applications ou les protocoles exécutés au niveau des nœuds voisins. Généralement, les informations incluses dans les balises (en anglais *Beacons*) comprennent des informations sur le nœud tels l'identifiant, les coordonnées géographiques et la vitesse de déplacement. La fréquence des balises varie de 1HZ à 10HZ dans la plupart des cas.

Afin de sécuriser l'opération de balisage, chaque nœud V calcule la signature numérique $\text{sig}(E,m)$ sur les différents champs du paquet (m dénote les champs qui correspondent aux informations énoncées ci-dessus et E l'entête du paquet) à envoyer en utilisant sa propre clé privée CPr_V qui correspond à sa clé publique CPu_V . La signature numérique $\text{sig}(E,m)$ est ensuite ajoutée au message qui sera envoyé conjointement avec son propre certificat numérique CRT_V .

Les nœuds recevant ce message peuvent authentifier la source du message grâce à la clé publique CPu_V incluse dans le certificat numérique CRT_V . Le format d'un paquet balise est illustré dans la figure ci-dessous.

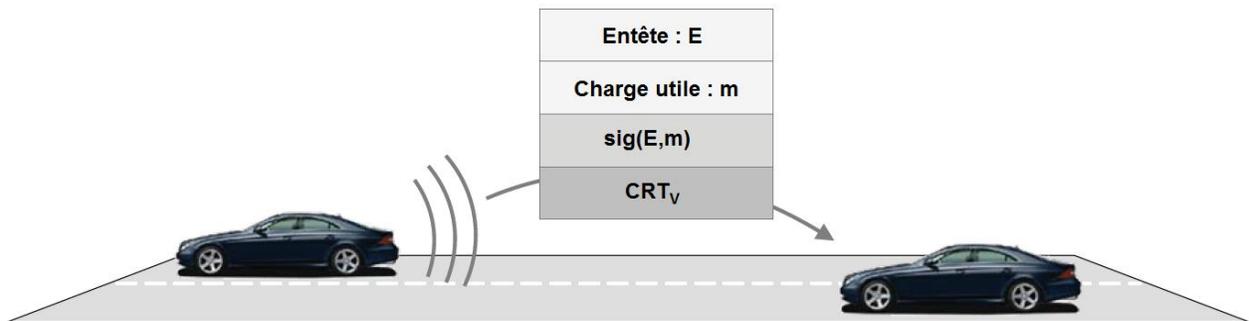


Figure 2.4 : Format d'un paquet balise [23]

2.5.3 La confidentialité dans les VANET

La confidentialité de l'identité et de la localisation sera parmi les préoccupations des propriétaires de véhicules et les techniques cryptographiques seules ne peuvent pas assurer cet objectif. La plupart des recherches établies à ce stade proposent l'utilisation de mécanismes de changement de pseudonymes qui assurent cet aspect de confidentialité à une certaine mesure, mais ces solutions ont toujours leur impact négatif sur la performance des protocoles de routage dans les VANETs [24].

2.6 Les systèmes de détection d'intrusion

Dans cette section, nous présentons les systèmes de détection d'intrusion de manière générale. Ces systèmes sont capables d'améliorer la sécurité des réseaux informatiques, et par conséquent ils peuvent fournir des solutions à un large éventail de problèmes de sécurité liés aux réseaux VANET.

2.6.1 Notions sur les systèmes de détection d'intrusion

Les intrusions dans un système d'information sont des actions qui violent la politique de sécurité du système; la détection d'intrusion est le processus utilisé pour identifier les intrusions [25], puis générer les alertes qui peuvent être utilisées (par les utilisateurs eux-mêmes ou d'autres modules de système) soit pour empêcher définitivement l'attaque ou bien pour prendre des contremesures permettant de minimiser son impact sur le système.

La détection d'intrusions ne remplace pas les techniques cryptographiques, mais elle peut être considérée comme une action complémentaire à la mise en place des mécanismes de sécurité.

Aussi elle suppose que le comportement d'un intrus sera sensiblement différent de celui d'un utilisateur légitime et que de nombreuses actions non autorisées seront détectables [26]. A cet effet, les systèmes de détection d'intrusion (SDI) surveillent les activités des utilisateurs par la vérification des fichiers d'audits qui contiennent des informations sur un ensemble d'actions effectuées sur le système. L'entité responsable de la création et la gestion de ces sources de données est appelée **l'observateur**. Ce dernier est supposé être capable de collecter ces sources de données à partir du trafic passant par lui ou par l'écoute des paquets transitant dans le support partagé (dans le cas où le système surveillé est reparti à travers un réseau). Dans les réseaux ad hoc mobiles le nombre des observateurs est défini suivant l'architecture des SDI adoptée; elle peut être **autonome** dans le cas où chaque nœud dans le réseau est un observateur; mais ce genre d'architecture ne peut être utilisé dans les réseaux à haute densité et fortement contraignants en énergie; elle peut être aussi une architecture **distribuée coopérative** qui doit identifier un certain nombre de nœuds dans le réseau pour être des observateurs; ces derniers échangent les informations entre eux afin d'améliorer le processus de détection. Il existe un autre type d'architecture basé sur des agents mobiles, capables de se déplacer à travers le réseau et collecter les sources de données nécessaires pour la détection.

2.6.2 Les approches de détection

La détection d'intrusion peut être effectuée suivant deux approches non exclusives : l'approche par scénario et l'approche par anomalie. Le but de la première approche est de détecter les attaques, celui de la seconde a comme objectif de les prévenir. Voici le principe et la description de chaque approche :

2.6.2.1 L'approche basée sur la signature

La détection basée sur la signature (en anglais *Misuse intrusion detection*) permet de détecter les intrusions qui suivent des modèles d'attaque bien définis et exploitent les faiblesses du système. La première étape dans le processus de détection consiste à identifier chaque attaque par une signature qui lui est propre et ensuite à en rechercher les traces dans les fichiers d'audits.

Généralement, cette approche est basée sur les techniques à base de règles comme les systèmes experts, les machines à états finis et les réseaux de pétri colorés [25].

Malgré que cette approche permette de détecter les attaques de manière efficace et rapide, les attaques inconnues ne peuvent être détectées, car les modèles d'attaques doivent être définis auparavant.

2.6.2.2 L'approche basée sur l'anomalie

L'approche basée sur l'anomalie (en anglais *Anomaly intrusion detection*) repose sur l'observation et sur la détection d'un comportement d'un utilisateur déviant par rapport à ses habitudes.

Cette approche suppose que les activités intrusives sont une sous-classe des activités anormales. Ceci est vrai dans une certaine mesure, sachant que le comportement et les objectifs d'un attaquant sont différents de ceux d'un utilisateur normal. Cependant, il est parfois possible qu'une activité intrusive ne coïncide pas avec une activité anormale; à partir de là on peut distinguer quatre possibilités, chacune d'entre elles avec une probabilité non nulle [27] :

- **Une activité est intrusive mais pas anormale:** cette activité est appelée un faux négatif. Le SDI la considère comme non intrusive à cause de l'absence de l'anomalie dans cette activité.

- **Une activité est non intrusive mais anormale:** cette activité est appelée un faux positif, elle est considérée à tort par le SDI comme intrusive du fait qu'elle est anormale.
- **Une activité n'est ni intrusive ni anormale:** cette activité est appelée un vrai négatif, elle est non intrusive et le SDI la considère comme non intrusive.
- **Une activité est intrusive et anormale:** cette activité est appelée un vrai positif, elle est détectée par le SDI car elle est anormale.

Généralement les activités anormales peuvent être déterminées en effectuant des statistiques sur les actions effectuées par les utilisateurs, les techniques d'apprentissage automatique, le *DATA-MINING* et les réseaux de neurones peuvent aussi être utilisés.

Finalement, la détection d'intrusion basée sur l'anomalie permet de détecter une partie importante des attaques inconnues. L'inconvénient majeur de cette approche réside dans la lenteur du processus de détection, et la plupart des techniques utilisées exigent un certain délai avant la détection.

2.6.3 Le modèle de Denning

Le modèle du SDI le plus connu est celui présenté par Denning et al. [28]; voici une description de ses composants:

2.6.3.1 Les métriques

Les mécanismes de détection d'intrusion statistiques nécessitent la définition de certaines métriques sur lesquelles l'ensemble des analyses statistiques seront effectuées. Ces métriques caractérisent l'utilisation de plusieurs ressources-système (c'est-à-dire l'utilisation du processeur, le nombre de fichiers consultés, le nombre de tentatives de connexion, ...etc.).

Ces métriques sont habituellement l'un des trois types suivants [28] :

- **Un compteur d'événements²** qui identifie les occurrences d'une action spécifique sur une période de temps. Ces mesures peuvent comprendre le nombre de tentatives de connexion, le

² Un événement est ce qui survient lorsque l'utilisateur effectue une action spécifique surveillée par le SDI.

nombre de fois qu'un fichier a été consulté, ou une mesure du nombre de mots de passe incorrects qui sont introduits [28].

- **Un compteur d'intervalle de temps** qui permet d'identifier l'intervalle de temps entre deux événements connexe [28].
- **Un quantificateur de ressources utilisées** pour en mesurer la quantité employée dans le système sur une période de temps donné. Cette métrique incorpore des compteurs d'événements et des compteurs d'intervalle de temps pour la quantification des ressources (Des exemples de quantificateurs de ressources comprennent ceux qui mesurent les consommations de cycles CPU, le nombre de documents écrits dans une base de données, ou le nombre de paquets transmis à travers le réseau) [28].

[Généralement, une métrique est calculée au moment de l'occurrence d'une action en relation avec cette métrique].

2.6.3.2 Les observations

On définit une observation par le tuple (m_n, t_n) où m_n est une métrique quantifiée à l'instant t_n ; donc le comportement d'un utilisateur par rapport à une métrique donnée peut être représenté sous forme d'une série de n observations (o_1, o_2, \dots, o_n) capturées pendant un intervalle de temps donné.

2.6.3.3 Les modèles

Etant donnée une métrique définie par une variable aléatoire x et (x_1, x_2, \dots, x_n) une série qui correspond à n observations, le but d'un modèle statistique pour une métrique donnée est de mesurer la déviation d'une nouvelle observation o_{n+1} correspondant à la variable x_{n+1} par rapport aux observations précédentes ou à une norme prédéfinie. Dans la littérature, il existe plusieurs modèles statistiques, dont les modèles suivants qui peuvent être utilisés [28] :

- **Le modèle opérationnel** : il permet d'identifier une anomalie par une comparaison d'une métrique à une limite prédéfinie. Ce modèle est utilisé dans les situations où un certain nombre d'événements (par exemple les connexions échouées) sont une indication directe d'une attaque probable [28].

- **La moyenne et l'écart type** : ce modèle est fondé sur l'hypothèse que la moyenne et l'écart type peuvent être calculés après la réception de la deuxième observation en utilisant les équations suivantes :

$$\text{Somme} = x_1 + x_2 + \dots + x_n$$

$$\text{Somme_de_carrés} = x_1^2 + x_2^2 + \dots + x_n^2$$

$$\text{Moyenne} = \text{Somme}/n$$

$$\sigma = \sqrt{\left(\left(\frac{\text{Sommedecarrés}}{n} \right) - \text{Moyenne}^2 \right)}$$

La valeur de x_{n+1} est jugée comme anormale si elle n'appartient pas à un certain intervalle de confiance défini comme suit par l'inégalité de Chebyshev :

$$[\text{Moyenne} - d * \sigma, \text{Moyenne} + d * \sigma]$$

où d est un paramètre qui permet d'identifier la probabilité maximale de non appartenance à l'intervalle précédent avec une probabilité égale à $1/d^2$; par exemple: si $d=4$ la probabilité sera égale à 0.0625.

L'avantage de ce modèle par rapport au modèle opérationnel est qu'il ne demande pas de définition des seuils pour les métriques; par contre, il apprend ce qui constitue une activité³ normale d'un utilisateur à partir des données des observations.

La moyenne et l'écart type peuvent être modifiés par la pondération des observations tout en donnant des poids élevés (plus de pertinence) aux observations plus récentes [28].

- **Le modèle multi-variable** : ce modèle est similaire au modèle précédent sauf qu'il est basé sur la corrélation de plusieurs métriques dont chacune d'elles est en relation avec l'autre. Par exemple corréler la métrique de tentative de connexion avec la durée de session [28].
- **Le modèle markovien** : il est utilisé avec le compteur d'événements pour déterminer la normalité d'un événement particulier, basé sur ceux qui l'ont précédé. Ce modèle est particulièrement utile lorsque l'ordre d'événements est important [28].

³Une **activité** est définie par un ensemble d'actions effectuées par un utilisateur.

2.6.3.4 Les profils

Après l'utilisation des modèles statistiques précédents pour mesurer la déviation de comportement par rapport à une métrique donnée, il est indispensable de déterminer la marge des déviations permises. Donc les profils ont pour objectif de définir les limites d'un comportement à considérer comme normal. Ils peuvent varier au cours du temps selon le modèle utilisé et les activités des utilisateurs [28].

2.6.4 Applications et applicabilité des SDI dans les VANETs

Les SDI peuvent être utilisés pour détecter les nœuds générant des messages (par exemple: des messages liés à la sécurité) dont le contenu est incohérent avec leurs propres observations et avec celles des autres nœuds [29] [30]. Mais ce type d'application exige que les nœuds observateurs échangent fréquemment les observations entre eux, ce qui entraîne une consommation élevée de la bande passante.

Les SDI peuvent être aussi intégrés dans les protocoles de routage afin de détecter et éviter les nœuds malveillants. Un exemple de ces protocoles sera présenté dans le chapitre 3, tandis que leurs inconvénients seront présentés dans le chapitre 4.

2.7 Les systèmes de réputation

Les systèmes de réputation (parfois appelés les SDI basés sur la réputation) sont un nouveau paradigme proposé pour améliorer la sécurité dans les différents domaines comme les transactions électroniques, les applications de partage de fichiers dans les réseaux, le pair-à-pair (en anglais *peer-to-peer*, souvent abrégé « P2P ») [31].

Les systèmes de réputation sont inspirés de nos comportements sociaux. Comme dans notre vie quotidienne quand on rencontre quelqu'un pour la première fois on lui attribue une réputation (concernant un sujet) sur la base de notre propre expérience (première main) et celle de quelqu'un d'autres (deuxième main). Les systèmes de réputation sont fondés sur ce principe, et sont utilisés pour décider à qui faire confiance, et pour encourager le comportement bienveillant.

Les objectifs des systèmes de réputation peuvent être résumés dans les trois points suivants [32]:

- Fournir des renseignements permettant de distinguer les nœuds dignes confiance.
- Encourager les nœuds à agir d'une manière fiable.
- Décourager les nœuds indignes de confiance de participer à fournir les services protégés par le système de réputation.

A la différence des SDI traditionnels où les nœuds vérificateurs surveillent et analysent chacune des activités indépendamment de l'autre dans la plupart des cas, dans les systèmes de réputation chaque nœud maintient un score de réputation concernant le comportement global de chacun des autres nœuds qu'il a observés. Ces scores représentent leurs degrés de confiance et peuvent être ajustés par les différentes observations captées au cours du temps. A cet effet, les systèmes de réputation utilisent les techniques de détection d'intrusion pour calculer ces degrés de confiance [33]. Dans les MANET, les systèmes de réputation requièrent que chaque nœud doit en continu surveiller les activités de ses voisins [4], ensuite ils exploitent les informations de deuxième main avec celles dérivés de leurs propres tables pour recalculer les degrés de confiance.

De manière générale, les systèmes de réputation sont difficiles à appliquer dans les réseaux VANET, car la forte mobilité dans ces réseaux rend le temps d'interaction entre les véhicules très court et les interactions répétées très rares [4] [5].

Dans la littérature, il existe plusieurs systèmes de réputation [34] [35] [36], dont CONFIDANT et CORE qui constituent un exemple de ces systèmes.

2.8 Conclusion

Les réseaux véhiculaires sont vulnérables aux attaques menaçant la vie de leurs usagers et les biens si des mécanismes appropriés n'ont pas été mis en œuvre. Les techniques cryptographiques existant peuvent apporter des solutions aux objectifs de l'authentification, l'intégrité et la non répudiation, mais la disponibilité est difficile à assurer car les attaques peuvent la viser au niveau des différentes couches de la pile protocolaire. L'objectif de la confidentialité ne peut être assuré qu'au détriment de la sécurité et de la performance du système de communication dans les VANETs; ainsi cet objectif ne doit pas empêcher les entités d'investigation de détecter les coupables causant les accidents. Donc, un compromis doit être mis en place entre ces différents aspects.

Nous avons présenté les solutions utilisées dans les réseaux ad hoc comme les systèmes de réputation les SDI, ces derniers peuvent être utilisés pour vérifier la consistance de données des messages d’alerte échangés entre les véhicules. Cependant les systèmes de réputation sont difficiles à appliquer dans les VANETs, car la réputation est difficile à bâtir dans un délai très court.

Dans le chapitre suivant, nous présenterons l’opération de routage dans les réseaux ad hoc, et les solutions qui peuvent être utilisées afin d’améliorer la sécurité et la performance des protocoles de routage sécurisés dans les VANETs.

Chapitre 3

La sécurité de routage dans les réseaux ad hoc

Introduction

Le routage est un service fondamental dans tout type de réseau, ce qui le rend une cible idéale pour les attaques dans les VANETs. En effet, si les règles du protocole de routage utilisées n'étaient pas bien conçues l'entité malveillante peut les manipuler afin d'interrompre l'acheminement d'un message lié à la sécurité; par conséquent, ces réseaux VANET auront un impact négatif sur la sécurité routière en présence des attaquants.

Dans la littérature, il existe plusieurs protocoles de routage sécurisés qui ont été développés pour les réseaux ad hoc de manière générale. Donc, ces protocoles ont été conçus sous des conditions plus ou moins contraignantes que les VANETs, ce qui oblige à une reconsidération de leur conception avant leur utilisation dans les VANETs.

Dans ce chapitre, nous présentons d'abord le routage dans les réseaux ad hoc de manière générale, puis les attaques sur les protocoles de routage. Ensuite, nous décrivons quelques protocoles de routage sécurisés connus dans les réseaux ad hoc, enfin nous faisons une étude comparative sur ces protocoles.

3.1 Le routage dans les réseaux ad hoc

En général, le routage est une méthode par laquelle les paquets de données sont acheminés vers une destination bien précise à travers un réseau de connexion donné. En outre, l'opération d'acheminement selon certains critères de performance doit être optimisée.

Dans le contexte ad hoc, il se peut que le nœud destinataire soit hors de la portée de transmission radio du nœud source, ce qui nécessite l'emploi de la technique du relayage où les nœuds intermédiaires peuvent servir comme relais pour acheminer les paquets vers la bonne destination.

3.2 Classification des protocoles de routage dans les réseaux ad hoc

Généralement, les protocoles de routage peuvent être classés en deux grandes familles [37]:

3.2.1 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 nœuds pour l'acheminement des paquets. Cette famille de protocoles peut être divisée en trois catégories : les protocoles proactifs, réactifs et hybrides.

Dans les protocoles proactifs (*table-driven*), chaque nœud maintient une ou plusieurs tables qui contiennent des informations de routage concernant toutes les destinations [38]. Cette catégorie de protocoles nécessite un échange périodique de paquets de contrôle entre les différents nœuds pour maintenir à jour les tables de routage.

Tandis que, dans les protocoles réactifs (*on-demand driven*), le chemin n'est calculé que sur demande, et l'opération de routage comporte donc deux étapes: la découverte de route pour l'acheminement de données vers une destination et la maintenance des routes existantes dans le cas de changement de la topologie du réseau.

Les protocoles hybrides combinent les principes des deux catégories précédentes. Ils utilisent les mécanismes des protocoles proactifs pour découvrir les proches voisins. Mais, pour le reste du réseau, cette catégorie agit comme les protocoles réactifs.

En général, les protocoles basés sur la topologie ne supportent pas les réseaux qui dépassent quelques centaines de nœuds [39].

Dans la littérature, il existe plusieurs protocoles topologiques tels que : AODV [40], DSR [41] et TORA [42] comme protocoles réactifs ; OLSR [43] et DSDV [44] comme protocoles proactifs et ZRP [45] comme protocole hybride.

3.2.2 Les protocoles de routage géographique

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 [46]. Pour atteindre cet objectif, les coordonnées géographiques des nœuds sont incluses dans les tables de routage.

Concrètement, un nœud 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 [47] indépendant) dans le paquet à envoyer, et par la suite les nœuds 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.

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.

Dans la littérature, il existe plusieurs protocoles de routage géographique. Les plus connus sont: LAR [48], DREAM [49], GPSR [50].

3.3 Rappel sur les protocoles de routage ad hoc

Nous donnons ci-après deux exemples de protocoles de routage ad hoc, l'un est basé sur la topologie et l'autre est géographique :

3.3.1 AODV

L'AODV (Ad hoc On Demand Distance Vector) [40] est un protocole réactif. Dans ce protocole, les nœuds acheminent les paquets sur la base de leurs tables de routage. A cet effet, chaque nœud maintient sa propre table de routage, indiquant pour chaque destination le prochain nœud à utiliser comme un relais.

Le nœud source déclenche l'opération de découverte de route par la diffusion d'un paquet RREQ indiquant sa requête. Lorsqu'un autre nœud reçoit ce paquet, il vérifie dans sa table de routage, s'il y a une entrée indiquant le chemin pour accéder à la destination (ou si c'est lui même est le nœud destinataire); il envoie un paquet RREP au nœud source qui doit s'arrêter d'inonder le réseau. Sinon, il doit retransmettre la requête à ses voisins, et enregistre dans sa table de routage le nœud qui la lui a acheminé comme un relais pour accéder au nœud source.

En cas de rupture de lien, un message RERR est envoyé au nœud source qui décide ou non de recommencer l'envoi du paquet.

3.3.2 GPSR

GPSR (*Greedy Perimeter Stateless Routing*) [50] est un protocole de routage géographique basé sur les informations de localisation diffusées périodiquement dans des balises par les nœuds. Dans le protocole GPSR les nœuds utilisent deux stratégies différentes pour acheminer les paquets :

La transmission gloutonne (*Greedy Forwarding*) et la transmission de périmètre (*Perimeter Forwarding*). Le mode «*Greedy Forwarding*», est utilisée préférentiellement au cours d'acheminement des paquets; selon ce mode de transmission, le prochain voisin choisi comme relais est celui le plus proche de la destination. Dans le cas d'un maximum local, c'est-à-dire où le nœud intermédiaire acheminant le paquet se trouve plus proche de la destination que tous ses voisins à cause d'un trou dans la topologie. Ce nœud doit basculer en mode périmètre qui permet de router le paquet en contournant ce trou jusqu'à arriver à un nœud plus proche de la destination. Ensuite, le mode «*Greedy Forwarding* » est réutilisé. Les prochains nœuds intermédiaires doivent répéter le même processus jusqu'à ce que le paquet arrive à destination.

3.4 Les attaques contre les protocoles de routage

3.4.1 Pour quoi attaquer les protocoles de routage ?

Généralement, dans le contexte ad hoc, les attaques contre les protocoles de routage peuvent avoir les trois objectifs suivants [1] :

- Avoir plus de contrôle sur les communications entre certains nœuds.
- Dégrader la qualité de service fourni par le réseau (par exemple en termes de délais et de taux d'acheminement de paquets).
- Epuiser les différentes ressources critiques comme la bande passante, l'énergie et la capacité du traitement de quelques nœuds.

Il faut noter que ces objectifs ne sont pas entièrement indépendants les uns des autres, et parfois le fait d'atteindre l'un de ces objectifs mène directement aux autres.

3.4.2 Les mécanismes d'attaques contre les protocoles de routage

Dans les réseaux ad hoc, une attaque n'est qu'une combinaison spécifique de quelques mécanismes d'attaques ayant pour but d'atteindre un ou plusieurs objectifs présentés dans la section précédente. Ces mécanismes d'attaques comprennent des actions élémentaires comme l'écoute du trafic, le rejeu⁴ (*Replaying*), la modification et l'élimination des paquets de contrôle (c'est-à-dire les paquets utilisés dans l'opération de routage qui ne sont pas des paquets de données). En plus, l'attaquant peut essayer de forger des paquets de contrôle falsifiés (en anglais *Packet forgery*), ou bien créer des paquets de contrôle sous une fausse identité (en anglais *Spoofing*) [1].

Les attaquants peuvent rejouer et modifier les paquets de données, mais ces manipulations ne sont pas considérées typiquement comme une problématique de sécurisation de routage, et doivent être détectées à l'aide d'outils cryptographiques au niveau des couches supérieures (le modèle de vérification de bout en bout) ou des couches inférieures (le modèle de vérification de saut par saut).

⁴ Le rejeu d'un message aura lieu lorsqu'un message valide est retardée ou répété par un attaquant qui a intercepté le message dans le but de causer des états incorrects dans un système

Cependant, l'élimination des paquets de données est considérée comme une action visant la fonctionnalité de l'acheminement [1].

3.4.3 Exemples d'attaques contre les protocoles de routage

Dans cette section, nous décrivons quelques attaques connues sur les protocoles de routage dans les réseaux ad hoc:

- **Attaque Blackhole**: dans cette attaque, le nœud malveillant élimine tous les paquets de données passant par lui [51].
- **Attaque Grayhole** : c'est une variante de l'attaque *Blackhole* qui consiste à éliminer seulement les paquets de données de certaines applications qui sont vulnérables à la perte de paquets [51].
- **Attaque Sinkhole** : dans cette attaque un nœud malveillant essaie d'attirer les paquets de ses voisins à passer par lui, ce qui lui permet par la suite de modifier leurs contenus ou les éliminer [19]. Donc, l'attaque *Sinkhole* peut être utilisée pour monter d'autres attaques comme le *Blackhole* et le *Grayhole*.
- **Attaque Flooding** : elle consiste à inonder le réseau par un nombre élevé de paquets (paquets de demande de route, de formation de groupes...etc.) afin de générer un trafic supplémentaire important et causer une dégradation de performance du protocole de routage [19].
- **Attaque Sybil** : c'est une variante de l'attaque *Spoofing*, où un seul nœud prétend être plus qu'un seul en utilisant simultanément plusieurs identités différentes dans le réseau afin d'avoir la capacité de monter plus aisément des attaques. Cette attaque est très dangereuse sur le routage géographique, car un nœud peut prétendre être sur plusieurs positions stratégiques à la fois, afin d'être choisi comme relai pour l'acheminement de leurs paquets; ce qui donne lieu à une attaque *Sinkhole* [52].
- **Attaque trou de ver** (*Wormhole attack*) : elle consiste à rendre deux nœuds légitimes non voisins (la zone radio de transmission de l'un ne recouvre pas l'autre) échangent des paquets de contrôles entre eux afin de créer des routes inexistantes. Généralement, il s'agit de deux attaquants disposant d'une connexion réseau privée (tunnel de transmission) qui leur permet de transmettre les paquets de contrôle.

- **Attaque Tunneling** : elle est à peu près similaire au *Wormhole* ; la différence entre les deux est comme suit : dans le *Tunnelling* les attaquants utilisent le même réseau pour établir la connexion privée en encapsulant les paquets (par exemple de type RREQ) des autres nœuds dans la charge utile des paquets ordinaires, tandis que dans le *Wormhole*, les attaquants sont supposés être externes et utilisent un autre canal radio pour l'établissement de la connexion, généralement permettant d'acheminer les paquets de manière plus rapide [1].
- **Attaque Rushing** : l'attaque *Rushing* [53] concerne les protocoles de routage réactifs dans lesquels l'attaquant ne respecte pas les règles d'accès au canal, imposées par la couche MAC pour précipiter les paquets de RREQ passant par lui; par conséquent, ces paquets se propagent plus rapidement vers la destination et donc il est fort possible que tous les autres paquets seront éliminés. Car dans la plupart des protocoles de routage réactifs, les auteurs proposent des mécanismes de contrôle pour minimiser le coût de découverte de route, selon lesquels les nœuds intermédiaires rediffusent seulement les paquets de contrôle (les paquets RREQ) arrivant en premier, et éliminent tous les autres exemplaires de ce paquet arrivant ultérieurement.

3.5 Les protocoles de routage ad hoc sécurisés

Afin de remédier aux problèmes liés à la sécurité plusieurs protocoles ont été développés. Dans cette section nous présentons quelques protocoles de routage sécurisés :

3.5.1 SRP

Le protocole SRP (*Secure Routing Protocol*) [54] est conçu comme une extension sécurisée de protocole de routage réactif DSR, il est basé sur la cryptographie symétrique. Afin de rendre le protocole plus pratique dans les scénarios de volatilité des routes, le SRP ne suppose pas que tous les nœuds intermédiaires dans une route, partage une clé secrète avec le nœud source ou destinataire. Par conséquent, seuls les deux nœuds communicants (nœud source et nœud destination) partagent une clé secrète. De ceci résulte que la vérification et l'authentification de paquets de contrôle échangés ne sont effectuées qu'au niveau des nœuds communicants.

$S \rightarrow *:$ (RREQ; S; D; qid; sn; mac_S; [])

 $F_1 \rightarrow *:$ (RREQ; S; D; qid; sn; mac_S; [F1])

 $F_2 \rightarrow *:$ (RREQ; S; D; qid; sn; mac_S; [F1; F2])

 $D \rightarrow F_2:$ (RREP; S; D; qid; sn; [F1; F2]; mac_D)

 $F_2 \rightarrow F_1:$ (RREP; S; D; qid; sn; [F1; F2]; mac_D)

 $F_1 \rightarrow S:$ (RREP; S; D; qid; sn; [F1; F2]; mac_D)

Figure 3.1 : Les opérations et le format de message de SRP [1]: S est l'identifiant du nœud source, D l'identifiant du nœud destinataire, et F_1 et F_2 sont les identifiants des nœuds intermédiaires. qid est un nombre aléatoire pour identifier la requête, sn est le numéro de séquence maintenu par S et D, mac_S et mac_D sont des MACs générés par S et D calculés avec la clé secrète partagée sur les différents champs du paquet à envoyer.

La figure 3.1 illustre les opérations effectuées par SRP lors de la découverte de route déclenchée par un nœud S. Au début, S diffuse à ses voisins à un saut un paquet RREQ contenant un MAC calculé sur les différents champs avec la clé qu'il partage avec le nœud destinataire D. Ensuite chaque nœud intermédiaire recevant ce paquet ajoute son identifiant au descriptif de ce dernier. Dès que le nœud destinataire D intercepte le paquet contenant la route spécifiée dans le descriptif du paquet, il vérifie le MAC généré par S et ensuite envoie un paquet RREP à S via la route inverse; ce paquet contient le descriptif de la route trouvée et un MAC (calculé avec la clé secrète partagée avec S).

Les opérations du protocole SRP sont très optimisées en termes de bande passante et de traitement. Cependant, cet avantage disparaît en présence d'un attaquant qui peut ajouter des paquets RREQ falsifiés (par exemple contenant un identifiant d'un destinataire inexistant) ou altérer le descriptif d'une route en cours de construction. Ainsi, l'authentification et la vérification d'intégrité de ces paquets ne sont pas effectuées par les nœuds intermédiaires, ce qui provoque une consommation de ressources supplémentaire en présence d'attaquants.

3.5.2 ARIADNE

ARIADNE [55] a été proposé par Hu et al. comme un protocole de routage sécurisé réactif basé sur la source pour les réseaux ad hoc, les auteurs ont proposé trois variantes de ce protocole qui correspondent à trois techniques d'authentification : la signature numérique, le MAC, ou le *TESLA*⁵ [56].

La variante ARIADNE basée sur la signature numérique est conceptuellement la plus simple par rapport aux autres variantes; la figure 3.2 représente une séquence des opérations effectuées par ARIADNE basé sur la signature numérique.

```

S :  $hs = MAC_{SD}(rreq; S; D; qid)$ 
S → * :  $(rreq; S; D; id; hs; [ ]; [ ])$ 
F1 :  $h_{F1} = H(F_1; hs)$ 
F1 → * :  $(rreq; S; D; id; h_{F1}; [F_1]; [sig_{F1}])$ 
F2 :  $h_{F2} = H(F_2; h_{F1})$ 
F2 → * :  $(rreq; S; D; id; h_{F2}; [F_1; F_2]; [sig_{F1}; sig_{F2}])$ 
D → F2 :  $(rrep; D; S; [F_1; F_2]; [sig_{F1}; sig_{F2}]; sig_D)$ 
F2 → F1 :  $(rrep; D; S; [F_1; F_2]; [sig_{F1}; sig_{F2}]; sig_D)$ 
F1 → S :  $(rrep; D; S; [F_1; F_2]; [sig_{F1}; sig_{F2}]; sig_D)$ 

```

Figure 3.2 : Les opérations et le format de message d'ARIADNE basé sur la signature numérique [1] :

S est l'identifiant du nœud source, D l'identifiant du nœud destinataire, et F₁ et F₂ sont les identifiants des nœuds intermédiaires. qid est un nombre aléatoire pour identifier la requête, H une fonction de hachage à sens unique connu, MAC_{SD} est calculé à l'aide d'une clé partagée entre S et D, sig est la signature numérique.

Les opérations de la variante d'ARIADNE basées sur le MAC sont à peu près les mêmes illustrées dans le schéma ci-dessus, la principale différence consiste en l'utilisation des MACs au lieu des signatures numériques. Il en est de même pour ARIADNE basé sur le TESLA, mais les nœuds intermédiaires calculent les MACs à l'aide de leurs clés TESLA.

⁵ Le Tesla est un mécanisme d'authentification dans lequel l'émetteur ajoute un MAC dépendant d'une clé secrète qui n'est divulguée qu'après un certain délai; ce dernier doit être assez suffisant pour que le message atteigne sa destination et assurer par conséquent l'intégrité du message.

L'avantage de ces deux dernières variantes est que les MACs peuvent être calculés de manière plus efficace que la signature numérique. Cependant, l'inconvénient de l'application de TESLA est qu'elle procure des délais dans le processus de découverte de route; par conséquent, ARIADNE basé sur TESLA n'est pas recommandée pour les réseaux à forte mobilité comme les VANETs [1].

3.5.3 SAODV

SAODV [57] est une variante sécurisée de protocole AODV; ses opérations sont similaires à celles du AODV, mais il utilise une extension cryptographique pour assurer l'authenticité et l'intégrité des messages de routage, et pour éviter les manipulations de la valeur de nombre de sauts (HOP-COUNT).

Conceptuellement, les messages de routage de SAODV (*Route_Reply* et *Route_Request*) ont une partie constante (non mutable) et une autre non constante (mutable). La partie constante est protégée par la signature numérique et inclut entre autres les champs suivants: le numéro de séquence, les adresses des nœuds source et destinataire et l'identifiant de requête. Tandis que la partie non constante qui inclut le compteur de sauts est protégée par une technique basée sur les chaînes de hachage, qui permet aux nœuds intermédiaires (selon les concepteurs de ce protocole) de vérifier que sa valeur n'a pas été décrétementée abusivement.

Cette dernière technique de protection n'est toutefois pas totale et la valeur de compteur du nombre de sauts peut être rendue par un nœud malveillant supérieure ou inférieure à sa valeur réelle. Donc, le nœud malveillant peut faire apparaître les routes plus courtes.

Ce protocole présente l'inconvénient que les nœuds doivent utiliser un serveur en ligne afin de vérifier les signatures numériques.

3.5.4 SPAAR

Le protocole SPAAR (Secure Position Aided Ad hoc Routing) [58] a été mis au point par Carter et al. , il utilise les informations géographiques des nœuds pour améliorer l'efficacité des réseaux ad hoc mobiles. Il a été conçu pour l'usage dans les environnements où la sécurité est une préoccupation majeure. Il utilise les informations géographiques dans le processus de routage pour réduire le nombre de paquets de contrôle.

En utilisant SPAAR, chaque nœud, dans le réseau doit avoir une paire de clés cryptographiques propres à lui (publique et privée), et la clé publique du serveur de certificats (pour authentifier les certificats des autres nœuds).

Outre la paire de clés publique et privée, chaque nœud a également besoin d'une autre paire de clés (appelés clé publique/privée de voisins) pour la communication avec ses voisins. Ces deux dernières clés sont générées et échangées avec ses voisins, à l'aide des leurs clés générées par le centre d'autorité, lorsque les nouveaux voisins sont détectés (grâce aux messages balises diffusés périodiquement aux voisins à un saut).

Quand un nœud diffuse un paquet de contrôle, comme un RREQ ou un RREP, il doit être signé avec sa clé privée et crypté avec la clé publique de ses voisins. Donc, chaque nœud peut vérifier que le paquet a été envoyé par un voisin à un saut.

Ce protocole exige que chaque nœud doit maintenir deux tables, une pour les voisins à un saut, et l'autre pour les nœuds destinataires communiquant avec lui; cette dernière table doit inclure les informations géographiques de ces nœuds qui peuvent être obtenues grâce à deux messages *location-request* et *location-reply*. Dans le cas où le nœud source ne dispose pas de l'information géographique du nœud destinataire, un message *location-request* est diffusé. Une fois le message est intercepté par un nœud qui dispose de cette information, il doit répondre par un message *location-reply*. L'utilité de l'information géographique du nœud destinataire est qu'il est utilisé par les nœuds intermédiaires pour orienter la propagation des paquets RREQ vers la destination (seulement les nœuds les plus proches de la destination doivent rediffuser les paquets RREQ); donc SPAAR ne trouve pas forcément un itinéraire vers la destination

Les informations géographiques du nœud destinataire comprenant la position et le vecteur de vitesse peuvent être véhiculées dans les paquets de données échangés puis utilisés pour renouveler et prédire les futures coordonnées de la destination [59].

3.5.5 DSR avec WATCHDOG et PATHRATER

S. Marti et al. [60] proposent un SDI qui peut être utilisé conjointement avec n'importe quel protocole de routage par la source dont le but de détecter les nœuds égoïstes et par conséquent

améliorer la disponibilité dans le réseau. Ils ont traité particulièrement le cas DSR en proposant deux extensions : le chien de garde (WATCHDOG) et l'évaluateur de chemins (PATHRATER).

Le WATCHDOG est le processus de contrôle exécuté par chaque nœud, pour vérifier que le nœud suivant situé sur la route achemine correctement les paquets; cette vérification est effectuée grâce à la technique d'écoute en mode *promiscuous* « mode promiscuité »; selon cette technique un nœud capture les paquets transitant sur le support physique qui ne lui sont pas destinés(cf. figure 3.3), et par conséquent il peut vérifier si un relai retransmet les paquets qu'il a reçu d'une part et au bon destinataire conformément au descriptif de la route inclus dans l'en-tête de chaque paquet. Dans le cas où le nombre de non-retransmissions dépasse un certain seuil, une notification est envoyée à la source pour la prévenir de la faute [61].

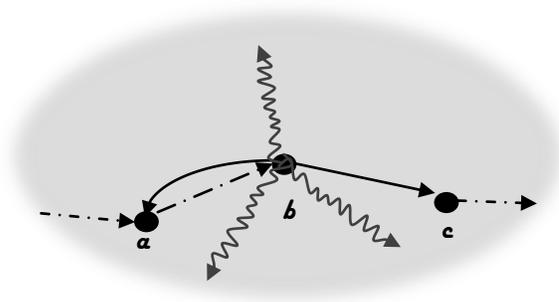


Figure 3.3 L'écoute en mode *promiscuous* : **a** vient de transmettre à **b** qui retransmet à **c** et **a** est capable de vérifier cette transmission [84]

Les informations collectées grâce au WATCHDOG sont exploitées par un processus appelé PATHRATER (l'évaluateur de chemin) qui attribue des poids ou des scores pour un certain ensemble de nœuds. Au début, les nœuds sont assignés à un score dit neutre, ce score est réévalué suivant le nombre de paquets retransmis. On peut noter que les scores des nœuds qui ne sont pas chargés de retransmettre les paquets restent inchangés [61].

Cette proposition présente les limites suivantes :

- Un nœud n'est pas toujours capable de capter les transmissions de ses voisins à cause des potentielles collisions ou lorsqu'un voisin utilise une puissance de signal différente (dans le cas où les liens entre les nœuds ne sont pas symétriques).

- Un attaquant qui possède une antenne unidirectionnelle⁶, peut l'orienter de telle manière que le prochain relai ne peut pas capturer le paquet et seul l'émetteur peut le faire, et de cette manière l'attaquant reste indétectable.
- Le WATCHDOG n'utilise pas les outils cryptographiques, donc il est vulnérable à l'attaque *Spoofing*
- Les nœuds détectés comme égoïstes ne sont pas sanctionnés.

3.6 Etude comparative et synthèse

3.6.1 Performance

L'analyse de performance d'un protocole doit être effectuée suivant certains critères, la dégradation de l'un de ces critères peut influencer sur l'autre. La table 1 résume les performances des protocoles précédents en termes de ces critères:

- **L'adaptation aux changements de la topologie :** les MANETs sont caractérisés par une topologie très dynamique; donc la connectivité de courte durée entre les nœuds doit être prise en compte et les routes créées doivent être suffisamment durables. De manière générale, tous les protocoles précédents sont conçus de manière qu'ils optimisent le nombre de sauts et les délais d'acheminement de paquets vers la destination. Malheureusement, ceci conduit à avoir des ruptures de lien fréquentes.
- **La scalabilité :** les réseaux MANET à grande échelle constituant éventuellement des topologies avec un grand nombre de nœuds complètement connectés; une partie importante de ces derniers peuvent aussi solliciter simultanément l'établissement de routes. Cette situation fait appel à penser à optimiser les opérations de découverte de routes. Tous les protocoles de routage basés sur la topologie (SRP, ARIADNE, SAODV et DSR avec Watchdog et Pathrater) ne disposent pas d'un mécanisme approprié optimisant suffisamment la découverte de route. D'autre part, le

⁶ Une antenne unidirectionnelle est une antenne diffusant les trames seulement vers une zone angulaire généralement afin de préserver l'énergie et prolonger la portée de signal.

protocole SPAAR réduit le trafic résultant de cette opération en orientant la propagation des paquets de découverte de route vers la position géographique de destination.

- **Le traitement et l'overhead de paquets :** à cause de la taille réduite des MACs, et la rapidité de leur calcul, les protocoles de routage basés sur le MAC sont les plus performants en termes de consommation de bande passante et de traitement.

Dans le protocole SPAAR, les signatures numériques doivent être générées et vérifiées pour chaque saut. Mais, il minimise la consommation globale des ressources de bande passante et de traitement, car il utilise d'un mécanisme d'optimisation de découverte de route.

Dans le protocole SAODV, seuls les nœuds communicants génèrent les signatures numériques, ce qui le rend plus performant par rapport aux autres protocoles basés sur la signature numérique.

Le protocole DSR avec Watchdog et Pathrater ne consomme pas les ressources car il n'utilise pas les opérations cryptographiques.

- **Les contraintes temps réel :** dans certaines applications des réseaux MANET, le délai d'acheminement des messages est une préoccupation majeure; nous pouvons distinguer deux types de délais influençant sur l'acheminement d'un message : les délais dûs aux mécanismes d'authentification utilisés, et les délais dûs aux opérations normales du routage qui ne sont pas liées à l'authentification. Pour ce qui concerne les délais liés aux mécanismes d'authentification, les protocoles basés sur le MAC (SRP, ARIADNE basé sur le MAC) surpassent tous les autres protocoles (à l'exception du DSR avec Watchdog et Pathrater qui n'utilise aucun mécanisme cryptographique), car le calcul des MACs est souvent fait rapidement. La variante d'ARIADNE basée sur le TESLA constitue le plus pire des cas à cause des propriétés spécifiques de son mécanisme d'authentification, tandis que les protocoles SAODV et SPAAR peuvent réduire les délais dûs à l'utilisation de la cryptographie asymétrique reposant sur les capacités de traitement des dispositifs dans les VANETs. En ce qui concerne le deuxième type de délais, les protocoles SRP, ARIADNE basé sur le MAC et DSR avec Watchdog et Pathrater choisissent les routes les plus optimales en nombre de sauts; ces routes ne sont donc pas forcément optimales en terme de délai, ce dont il résulte que ces protocoles entraînent des délais supplémentaires dans les situations de congestion.

		Adaptation aux changements de la topologie	Scalabilité	Overhead	Traitement	Contraintes temps réel
SRP		Moyenne	Moyenne	Bas	Bas	Bonne
ARIADNE	<i>Basé sur le MAC</i>	Moyenne	Moyenne	Bas	Bas	Bonne
	<i>Basé sur la Signature numérique</i>	Moyenne	Moyenne	Haut	Moyen (Elevé pour le nœud destinataire)	Moyenne
	<i>Basé sur le Tesla</i>	Mauvaise	Moyenne	Moyen	Bas	Mauvaise
SAODV		Moyenne	Moyenne	Haut	Moyen	Moyenne
DSR avec Watchdog et Pathrater		Moyenne	Moyenne	Bas	Bas	Bonne
SPAAR		Moyenne	Bonne	Haut	Elevé	Moyenne

Table 1 : La performance des protocoles de routage ad hoc sécurisés dans les VANETS

3.6.2 Discussion des aspects de sécurité et de confidentialité

Les protocoles SRP et ARIADNE basés sur le MAC ne sont pas recommandés pour les réseaux caractérisés par la haute mobilité et un grand nombre de nœuds; car les opérations de partage de clés seront complexes et difficiles. Le protocole SAODV nécessite l'existence d'un serveur permanent pour la vérification de la signature numérique, mais cette condition ne peut pas être toujours satisfaite dans les réseaux purement ad hoc ou dans les réseaux à grande échelle. Tandis que le protocole SPAAR suppose que l'accès aux serveurs de certificats n'est pas forcément permanent.

Les protocoles de routage sécurisés basés sur le protocole DSR (SRP, ARIADNE et DSR avec Watchdog et Pathrater) sont particulièrement vulnérables aux attaques de manipulations de nombre de sauts, mais tous les protocoles précédents sont vulnérables à l'attaque *Rushing*.

En ce qui concerne la confidentialité, les identités des nœuds peuvent être remplacées par les pseudonymes inclus dans des certificats à court terme. Cependant, la durée de vie de ces derniers est

très courte, et peut influencer la stabilité des routes, notamment, si elles sont très longues. Les protocoles de routage précédents souffrent plus, sachant que les mécanismes de changement de pseudonymes exigent que les nœuds doivent passer par des états de silence où ils ne doivent transmettre aucun paquet pendant un certain délai afin de créer une confusion et éviter le traçage de leurs trajectoires [62].

3.7 Conclusion

Dans ce chapitre nous avons présenté quelques protocoles de routage ad hoc sécurisés, ensuite, nous avons étudié leurs performances dans les réseaux à haute mobilité. Plusieurs aspects de ces protocoles doivent être améliorés afin qu'ils puissent être utilisés dans certains applications des réseaux MANET, notamment, l'aspect de sécurité. En effet, tous ces protocoles n'assurent pas la sécurité des communications à cent pour cent contre les différentes attaques, notamment celles provenant d'attaquants internes (par exemple : l'attaque de modification de compteur du nombre de sauts). Ces derniers peuvent viser la disponibilité du réseau et effectuer des attaques comme le *Rushing*, le *flooding*. Donc, d'autres mécanismes doivent être mis en œuvre afin d'améliorer sécurité de routage et la disponibilité de réseau.

Dans le chapitre suivant, nous proposerons des améliorations à un protocole de routage ad hoc sécurisé afin qu'il s'adapte à l'environnement véhiculaire, puis nous présenterons les techniques utilisés pour améliorer la sécurité des protocoles de routage, Ensuite nous présenterons et nous analyserons les différentes propositions existantes.

Chapitre 4

La protection contre les nœuds malveillants

4.1 Introduction

Nous avons vu que, à cause de l'aspect décentralisé des réseaux ad hoc où chaque nœud a besoin de la collaboration des autres nœuds, la sécurisation d'un protocole de routage ad hoc est un problème délicat et difficile à résoudre; pour cette raison les chercheurs ont proposé d'ajouter d'autres solutions visant à améliorer la sécurité.

Parmi les solutions classiques proposées, l'installation des infrastructures dédiées qui se chargent de délivrer la liste de révocation des certificats, et par la suite les membres du réseau seront capables de déterminer avec qui communiquer, mais cette solution est très lente et nécessite la mise en œuvre d'autres techniques pour collecter les informations à travers les différents nœuds ; quand ces derniers seront en mesure de communiquer avec les infrastructures installées.

Dans ce chapitre, nous présentons les différentes solutions existantes dans la littérature, ensuite, nous en choisissons une pour la discuter en détail, avant d'analyser les différentes propositions et déterminer à quel point elles sont appropriées pour les VANETs.

4.2 La sécurité de routage dans les réseaux VANET

Dans cette section, nous présentons les protocoles de routage dans les VANETs, et particulièrement on s'intéresse aux protocoles de routage ad hoc ayant été adaptés aux réseaux VANET. Puis, nous étudions la possibilité d'adapter ces protocoles de routage sécurisés au contexte VANET.

4.2.1 Les protocoles de routage existants dans les réseaux VANET

Plusieurs protocoles de routage ont été proposés pour les réseaux VANET; la plupart de ces protocoles ont en commun ou l'utilisation de l'information géographique dans le routage ou les informations indiquant des distances géographiques entre les nœuds de manière indirecte (par exemple : les techniques basées sur les mesures d'énergie de signal de trames transmises). Les premières tentatives de définition d'un protocole de routage ont commencé par l'adaptation des protocoles de routage topologiques sur les réseaux VANET, en ajoutant généralement des extensions aux protocoles topologiques, parmi les protocoles destinés aux réseaux VANET, nous citons :

- **AODV+PGB** : afin d'adapter le protocole AODV aux VANETs Naumov et al. [63] ont proposé la stratégie PGB (*Preferred Group Broadcasting*) qui est destinée à être utilisée conjointement avec le protocole AODV pour un double objectif:
 - Eviter le problème de *Broadcast storm*⁷ [64] et réduire la consommation de la bande passante lors de la découverte de routes.
 - Etablir des routes à durée de vie plus longue.

Selon le PGB, en mesurant la quantité d'énergie du signal, les nœuds recevant la requête de découverte de route peuvent connaître s'ils appartiennent ou non au groupe préféré, et qui doit rediffuser cette requête. Comme elle doit être rediffusée seulement par un seul nœud qui n'est

⁷ *Broadcast storm* est causé par une redondance inutile de rediffusion des paquets dans une zone géographique; ce problème entraîne des délais dans l'acheminement des paquets, voire même des collisions qui peuvent éliminer les paquets transitant sur le support sans-fil.

pas nécessairement le plus proche de la destination, les routes construites seront plus stables [65].

- **GPSR+AGF** : Naumov et al. ont aussi proposé la stratégie AGF [63] basée sur le rafraîchissement périodique des informations géographiques dans la table de voisins pour adapter le protocole GPSR aux VANETs. Dans cette stratégie, en utilisant les techniques de localisation, chaque nœud doit intégrer sa vitesse, sa direction et sa position géographique dans les balises afin de permettre à ses voisins de prédire ses futures positions géographiques; donc ces voisins peuvent savoir si ce nœud est dans la portée de leurs zones de couverture radio.
- **CAR(Connectivity-Aware Routing)** [66] : c'est un protocole conçu spécifiquement pour l'environnement véhiculaire, l'avantage principal de ce protocole est qu'il ne se base pas sur un service de localisation indépendant, ce qui lui permet d'optimiser les opérations de découverte de route avec le service de localisation.

4.2.2 Le choix d'un protocole pour les VANETs

A partir de l'étude comparative dans le chapitre précédent, aucun protocole ne peut répondre aux exigences de sécurité et de performance à la fois. Ainsi, l'amélioration de performance d'un protocole ne peut être achevée qu'au détriment de la sécurité.

En effet, nous avons vu que, à cause de l'utilisation des mécanismes de contrôle qui optimisent l'opération de découverte de route, l'attaque *Rushing* peut avoir lieu.

Comme les réseaux VANET sont fortement contraignants en ressource de bande passante et en délai d'acheminement, nous souhaitons l'établissement d'un compromis entre la sécurité et la performance; ainsi SAODV est un très bon candidat. En effet, nous pouvons améliorer la performance de ce protocole avec une technique adaptant ce protocole aux VANETs comme le PGB (voir section 4.2.1).

Comme les réseaux VANET n'assurent pas une communication permanente avec le centre d'autorité, les paquets de protocole SAODV doivent inclure les certificats pour permettre l'authentification des signatures numériques.

Le protocole choisi comme tous les protocoles de routage sécurisés basés seulement sur les techniques cryptographiques reste vulnérable aux attaques visant la disponibilité du réseau comme

le *rushing*, le *flooding* et la modification abusive de compteur du nombre de sauts. De manière générale, il n'y a pas une garantie que les nœuds du réseau appliquent les règles des protocoles de la manière dictée par les concepteurs. Donc, chaque nœud doit être capable de détecter et exclure les nœuds malveillants de l'opération de routage.

4.3 Les protocoles de révocation distribuée

L'opération de routage dans les VANETs exige la rapidité du processus de détection et d'élimination de nœuds malveillants plus que tout autre type de réseaux. Ceci, pour deux raisons :

- premièrement, la durée de connectivité entre les nœuds est très courte.
- deuxièmement, les nouveaux nœuds voisins constituent une part importante des bons candidats pour relayer les paquets, et par conséquent la rapidité de détection amène à avoir plus de routes sécurisées.

La solution qui consiste à utiliser un SDI conjointement avec un protocole de routage présente leurs limites. En effet, la détection avec un SDI distribué pose des problèmes de sécurité ou de consommation de la bande passante, ainsi la détection de certaines attaques avec un SDI autonome ne peut être effectuée qu'après des délais considérables, ce qui ne répond pas aux exigences de routage dans l'environnement VANET.

Ainsi, la révocation globale effectuée par l'AC qui consiste à révoquer les certificats des nœuds malveillants complètement du réseau en se basant éventuellement sur les observations des comportements de véhicules (les observations sont collectées quand les véhicules seront en mesure de communiquer avec les infrastructures installées) est très lente, et ne peut être envisagée comme une solution pour améliorer la sécurité d'un service fortement contraignant en délai comme le routage.

Donc, ni les SDI ni la révocation globale ne peuvent satisfaire les exigences de routage dans les VANETs.

La solution de révocation distribuée est considérée comme la solution la plus rapide et la plus adaptée aux VANETs [5]. Dans cette section, nous allons voir une description détaillée de cette solution et les concepts fondamentaux qui la rendent plus appropriée aux exigences des réseaux

VANET. Puis, nous présentons les propositions les plus connues à ce stade, et nous étudions leurs applicabilités sur les VANETs.

4.3.1 Définition de la révocation distribuée

La révocation distribuée est une approche permettant de détecter et d'éviter rapidement les nœuds malveillants, sans l'intervention du centre d'autorité et par conséquent minimiser leurs impacts sur le réseau dans le cas où une liste de révocation de certificat récente (générée par le centre d'autorité) n'est pas disponible que ce soit à cause de l'absence d'une station de base, ou à cause de la lenteur de processus de révocation globale.

Sachant que les nœuds honnêtes du réseau constituent une majorité, la révocation distribuée vise à décentraliser l'opération de révocation de telle manière où les nœuds du réseau jouent le rôle du centre d'autorité, souvent en s'appuyant sur un processus du vote.

Avant d'éviter ou d'exclure les nœuds malveillants, les nœuds honnêtes doivent être capables de les détecter [67]. A cet effet, les chercheurs proposent que les nœuds doivent utiliser des mécanismes de détection d'intrusion [68] [69] pour en surveiller les activités d'un certain nombre dans le réseau, et échanger les messages entre eux pour voter contre les nœuds suspects (cf. figure 4.1). Le processus de vote permet donc d'avoir une détection plus optimale et plus rapide.

Après la détection d'un nœud malveillant, un mécanisme de sanction doit être employé pour alléger l'impact des attaques sur le réseau.

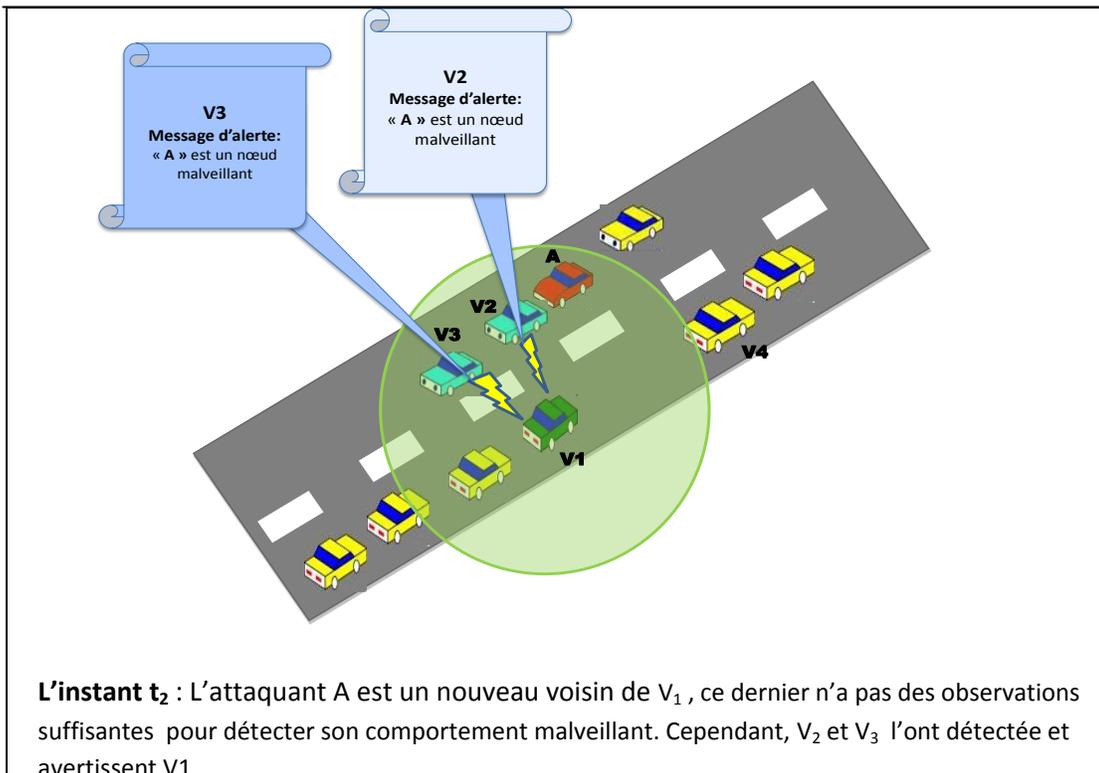
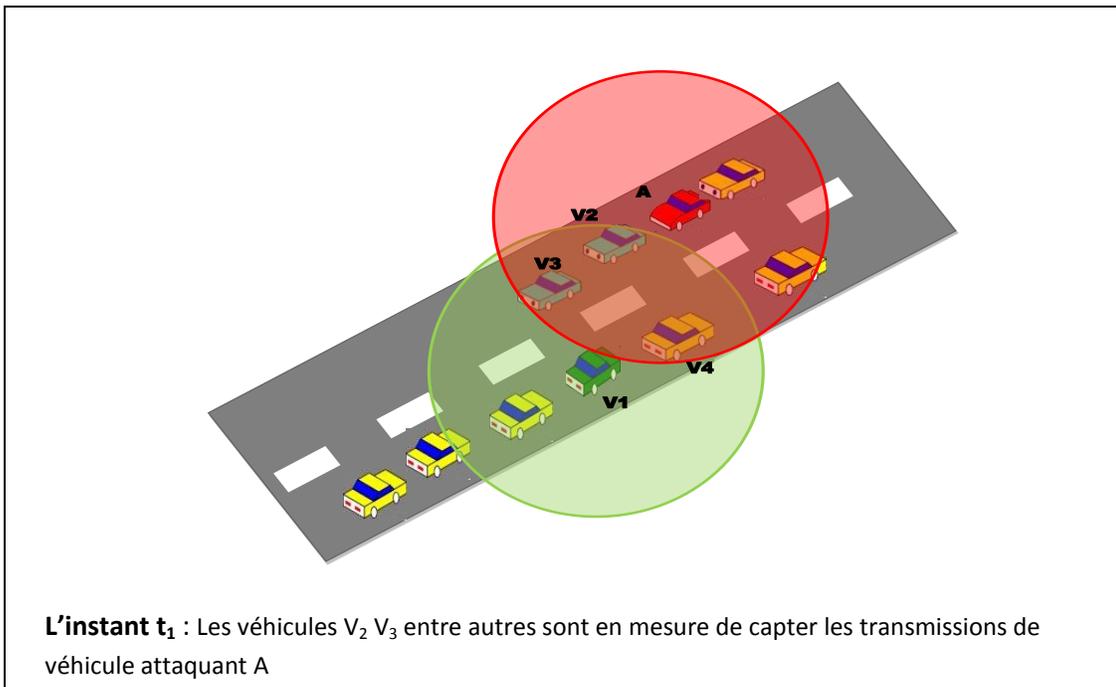


Figure 4.1 : L'importance de la révocation distribuée

4.3.2 L'architecture d'un Protocole de Révocation Distribuée (PRD)

Un PRD n'est qu'un composant logiciel constitué de deux modules (cf. figure 4.2): un système de détection d'intrusion autonome (SDI) et un analyseur des messages d'alerte. Le SDI est généralement un système de détection d'intrusion autonome qui analyse le trafic circulant sur le support sans-fil pour détecter les activités malveillantes. Dans le cas où un nœud malveillant est détecté, le SDI doit ajouter l'identifiant de ce nœud à la liste des nœuds exclus (liste noire du SDI), et ce dernier ne sera plus utilisé comme relai et ses messages seront ignorés ; ensuite le SDI doit diffuser un message d'alerte (un message d'accusation) aux autres nœuds pour les avertir.

Lorsqu'un nœud reçoit un message d'alerte, l'analyseur des messages d'alerte doit garder celui-ci sur une liste spécifique appelée la liste d'accusation pour une durée déterminée; cette liste ne sera utilisée que dans le cas où il y a un nœud candidat à être utilisé comme relai (spécifié par le protocole de routage). A cet effet un algorithme spécifique est utilisé pour attribuer une note (ou un taux d'accusation τ , $0 \leq \tau \leq 1$) à ce nœud sur la base des messages d'alerte inclus dans la liste d'accusation. Cette note est ensuite comparée à un seuil pour décider d'ajouter ou non l'identifiant de ce nœud à une liste noire spécifique généralement différente de celle de SDI. Cette distinction est très importante car la détection réalisée par le SDI (une détection basée sur les informations de première main) est plus sûre que celle réalisée par l'analyseur des messages d'alerte (une détection basée sur les informations de deuxième main). Il est donc recommandé d'employer un mécanisme de sanction moins rigoureux sur les nœuds détectés par l'analyseur. Par exemple: un nœud existant sur la liste noire de l'analyseur sera exclu que pour une durée limitée.

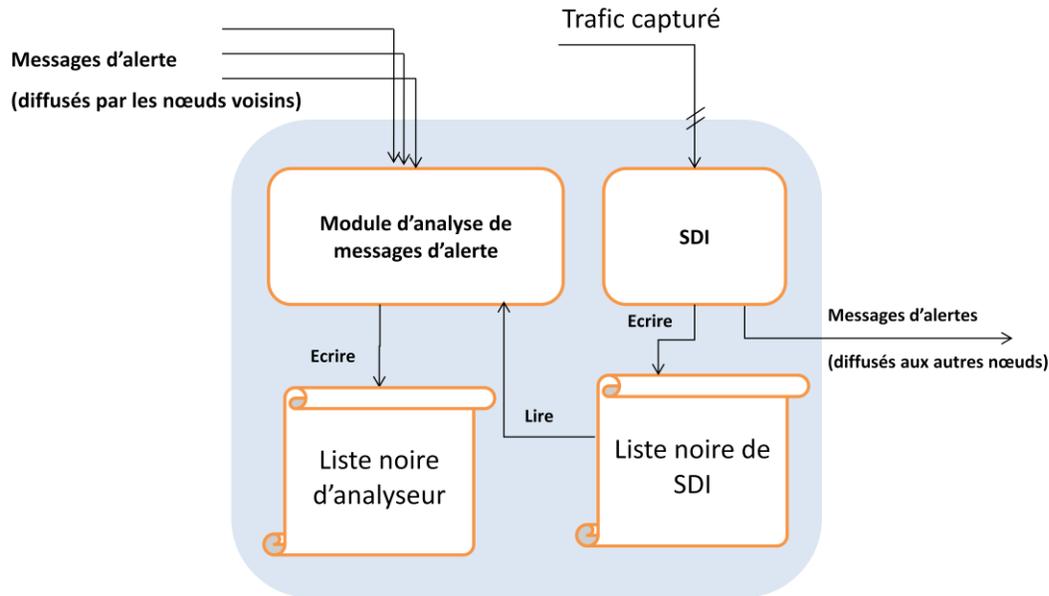


Figure 4.2 L'architecture d'un protocole de révocation distribuée

A partir de l'architecture précédente une description d'un protocole de révocation distribuée doit au minimum fournir les réponses à chacune des questions suivantes :

-Comment le SDI détecte les attaques ?

Le concepteur doit au minimum identifier les fonctionnalités à sécuriser et la nature de l'adversaire, ensuite il doit décrire le modèle de détection à utiliser.

-Lorsqu'un SDI d'un nœud détecte un attaquant, quels sont les nœuds à avertir et comment le faire?

Avant de répondre à cette question, le concepteur doit identifier la liste de contraintes imposées par l'environnement sur lequel le protocole sera déployé; par exemple: la bande passante et la densité des nœuds dans le réseau. Ensuite, il peut identifier le rayon de la zone de diffusion des messages d'alerte; exemple: choisir une valeur appropriée pour le champ TTL; ces messages peuvent être retransmis plusieurs fois dépendamment du modèle de mobilité caractérisant les nœuds du réseau.

-Quel est l’algorithme à utiliser par l’analyseur des messages d’alerte pour calculer le taux d’accusation?

L’algorithme utilisé par l’analyseur constitue le défi majeur des concepteurs, car il décide de la décision finale de révocation; si le SDI n’est pas en mesure d’identifier un comportement malveillant, l’algorithme conçu doit être performant tout en minimisant les risques des messages d’alerte falsifiés.

-Quelle est le mécanisme de sanction infligée sur les nœuds jugés comme malveillants?

La sanction infligée aux nœuds malveillants détectés peut être choisie selon le type d’application (l’environnement) et le problème envisagé; par exemple: dans les VANETs pour quoi les nœuds refusent-ils les messages liés à la sécurité (des messages authentifiables) alors qu’ils peuvent en vérifier la source et la fraîcheur.

4.3.3 Les critères de performance d’un protocole de révocation distribuée

Un protocole de révocation distribuée sera considéré comme performant généralement s’il ne consomme pas les ressources et vérifie les conditions suivantes:

- **Une fenêtre de vulnérabilité minimale** : comme les protocoles de routage préfèrent les relais les plus éloignés et les nouveaux nœuds voisins constituent une part importante des nœuds candidats pour acheminer les paquets (les protocoles de routage préfèrent les relais les plus éloignés), un protocole de révocation doit minimiser le temps nécessaire pour détecter un nœud malveillant, et tout retard de détection augmente significativement le risque et l’impact de ce dernier sur l’acheminement du paquet.
- **Un taux de détection élevé** : cette condition assure qu’une partie importante d’attaques ne réussissent pas, et par conséquent le réseau peut être considéré plus sécurisé dans une certaine mesure. Généralement les auteurs, dans la littérature, envisagent un taux de détection élevé sans se soucier des capacités de détection de SDI, car ils proposent souvent des solutions génériques pour les réseaux ad hoc, et la performance d’un SDI dépend de l’environnement de déploiement et des fonctionnalités à sécuriser.

- **Un taux minime de faux positifs** (fausse détection) : les nœuds malveillants ne doivent pas être capables d'exclure un nombre important des nœuds honnêtes par la génération des fausses alertes (les accusations falsifiées).

4.3.4 Le graphe d'accusation

Un graphe d'accusation permet de modéliser les messages d'accusations reçus par un nœud N pendant une durée donnée.

Le graphe d'accusation d'un nœud N est un graphe orienté où les nœuds représentent un certain ensemble de nœuds d'un réseau, et les arcs représentent leurs accusations. Par exemple: l'existence de l'arc (x, y) signifie que le nœud N a reçu un message envoyé par x qui accuse y dans son contenu.

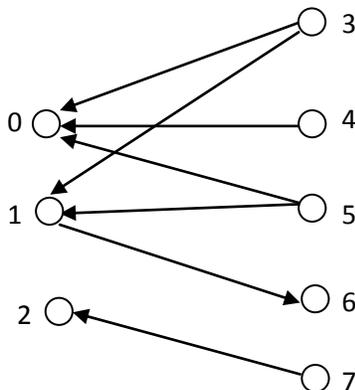


Figure 4.3: Exemple d'un graphe d'accusation d'un nœud N

La figure 4.3 montre un exemple de graphe d'accusation d'un nœud N; ce graphe montre que le nœud 0 a été accusé par les nœuds 3,4 et 5, il montre aussi que N a reçu un message dans lequel le nœud 7 accuse le nœud 2.

Il faut souligner qu'on ne peut rien déduire directement à partir de l'arc (x, y) , il se peut que le nœud x soit honnête et accuse y car il a détecté son comportement malveillant, comme il se peut que y soit malveillant et accuse arbitrairement le nœud x. Pour cette raison, le graphe d'accusation peut être aussi représenté sous forme d'un graphe non-orienté et l'ensemble A est défini alors par des arêtes de la forme $\{x, y\}$ et signifie que l'un de ces deux nœuds accuse l'autre.

Le but de ce graphe est généralement de faciliter la tâche d'analyse et de conception des protocoles de révocation distribuée.

4.3.5 Les protocoles de révocation distribuée basés sur le vote existants

Dans cette section, nous présentons quelques solutions existantes dans le contexte réseaux ad hoc.

a- Le protocole de révocation distribuée basé sur la cryptographie à seuil

Ce protocole a été proposé par Chan et al. [69] pour l'exclusion des nœuds malveillants dans un réseau de capteurs. Le protocole est très générique et un message d'alerte n'est diffusé qu'une seule fois aux nœuds voisins à travers un certain nombre de sauts, donc la mobilité n'est pas prise en compte par ce protocole.

Dans ce protocole, chaque paire de nœuds partage une clé utilisée pour l'authentification des messages. En plus, chaque nœud doit au début générer une autre clé secrète (appelée clé de révocation), il doit diviser cette clé en n portions en utilisant le mécanisme de partage de clé secrète de Shamir [70]. L'obtention de k de n ($k \leq n$) portions sont suffisantes pour reconstruire la clé de révocation. Ensuite chaque nœud doit distribuer ces portions sur les n nœuds voisins de telle manière que chaque nœud voisin ait avec lui une portion partagée. Cette portion sera diffusée dans un message d'alerte par un voisin seulement lorsqu'il pense que le nœud qui partage avec lui cette portion est malveillant. Par la suite, chaque nœud doit enregistrer les portions diffusées, et lorsqu'il reçoit k portions concernant le même nœud, il peut reconstruire la clé de révocation secrète qui doit être diffusée une seule fois à travers le réseau. L'obtention de la clé de révocation d'un nœud exige la suppression de la clé partagée avec lui et par conséquent tous ses messages seront ignorés; donc ce protocole maintient seulement une seule liste noire puisque tous les nœuds détectés par le SDI ou par l'analyseur seront définitivement exclus.

Parmi les inconvénients de ce protocole; on constate la consommation de la bande passante engendrée par la gestion des arbres d'hachage utilisés pour l'authentification des voix de vote, et les messages ne sont diffusés qu'une seule fois; donc, le protocole ne peut pas être utilisé dans les réseaux à connectivité sporadique. En plus, ce protocole ne prend pas en considération la densité des nœuds et le seuil est exprimé en terme d'un certain nombre d'accusateurs, d'où l'existence de

groupe des nœuds malveillants en coalitions (des attaquants sophistiqués) en nombre suffisant capables d'exclure tous les nœuds du réseau et causer un déni de service.

b- La révocation par l'attaque suicide

Les procédures d'exclusion des nœuds malveillants seront plus faciles lorsqu'un seul nœud est responsable de la décision de révocation. Dans le protocole de révocation par l'attaque suicide proposé par Clulow et al. [71], lorsqu'un nœud A détecte un comportement malveillant de M, A doit diffuser un message d'alerte " $\text{Suicide}_{a,M}$ " signé par sa clé publique qui contient l'identifiant des deux nœuds A et M. Les autres nœuds recevant le message doivent mettre ces derniers sur leurs listes noires. Il est clair que le fait de sacrifier de futures participations dans le réseau est une démonstration de la véracité de ce message.

Dans le cas de la diffusion de plusieurs messages d'accusations simultanés accusant le même nœud, ceux ayant reçu ces messages ne doivent considérer que le dernier message reçu, et éliminer les anciens accusateurs de leurs listes noires.

Parmi les inconvénients de ce protocole, nous constatons que les concepteurs supposent que le réseau est soit statique, soit complètement connecté, et lorsqu'un message est diffusé à travers le réseau, alors un seul nœud honnête est exclu pour chaque nœud malveillant. Dans le cas des VANETs où la topologie du réseau est très dynamique et sous forme d'îlots non connectés, la diffusion d'un message d'alerte à travers ce réseau pendant une petite durée, n'est pratiquement pas possible.

c- Le protocole de révocation de Crépeau

Crépeau et al. [72] ont proposé un protocole de révocation pour les réseaux ad hoc sans-fil. Dans ce protocole chaque nœud doit diffuser périodiquement son certificat à tous les membres du réseau; ainsi, il diffuse une requête pour l'obtention de leurs tables d'accusation (tables profiles). Ces dernières sont envoyées dans des messages de tailles variables et chacune d'elles contient au minimum la liste des accusateurs du nœud spécifié par la requête; l'émetteur du message doit indiquer les nœuds qu'il accuse inclus dans la liste précédente. Les tables profils sont analysées par les SDI pour détecter les anomalies, ces dernières peuvent être identifiées s'il y a inconsistance entre

une table et la majorité des autres tables. L'algorithme de l'analyseur se base sur le principe que les accusations suspectes sont celles émises par des nœuds générant un nombre élevé des accusations ou ceux ayant été accusés par un nombre élevé des nœuds, pour calculer le paramètre de sécurité, les auteurs ont défini:

- Le nombre des accusations contre le nœud i (A_i): le nombre total des accusations émises (seulement une accusation est comptée pour chaque nœud accusateur) contre le nœud i [72].
- Le nombre des accusations additionnelles émises par i (α_i): le nombre total des accusations émises par i (une seule accusation est possible par i contre un autre nœud) moins un [72].
- L'indice du comportement du nœud i (β_i): l'indice du comportement du nœud i (β_i) est un nombre tel que $0 < \beta_i \leq 1$. Il s'agit d'une mesure de comportement du nœud par rapport aux autres membres du réseau, et il est calculé de la manière suivante [72] :

$$\beta_i = 1 - \lambda A_i$$

$\lambda = \frac{1}{2N-3}$, où N est le nombre des nœuds dans les réseaux [72].

- Le poids d'une accusation d'un nœud i (ω_i): le poids d'une accusation d'un nœud dépend de l'indice de comportement (β_i) et du nombre des accusations additionnelles du nœud i (α_i). ω_i est un nombre tel que $0 \leq \omega_i \leq 1$, il est calculé de la manière suivante [72]:

$$\omega_i = \beta_i - \lambda \alpha_i$$

- Le paramètre de sécurité (R_j): c'est un nombre qui permet de déterminer si un certificat doit être révoqué ou non, il est calculé de la manière suivante [72]:

$$R_j = \sum_{i=1}^N \sigma_{ij} \omega_i$$

Si un graphe d'accusation a été construit, $\sigma_{ij} = 1$ s'il y un arc partant du nœud i vers le nœud j , sinon $\sigma_{ij} = 0$.

Finalement, le certificat du nœud j sera révoqué, si R_j est supérieur ou égal à un seuil prédéfini R_S ; la valeur $N/2$ a été spécifiée par les auteurs comme un seuil typique.

Il faut souligner que la valeur R_j et R_S peuvent être normalisés et représentés sous forme des taux, en divisant leurs valeurs sur le nombre total des nœuds N .

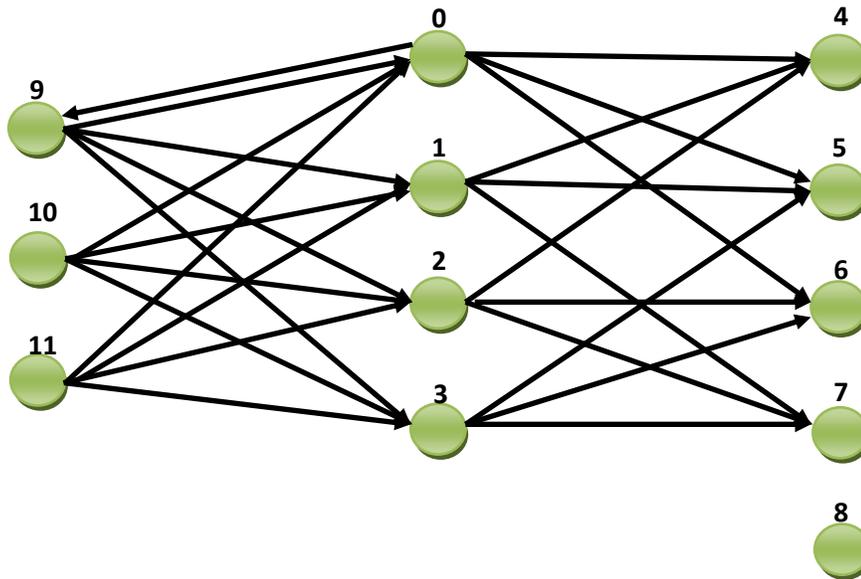


Figure 4.4 : Un graphe d'accusation illustratif

La figure 4.4 montre un graphe d'accusation qui sera utilisé pour calculer les taux d'accusation à l'aide de l'algorithme de Crépeau. Le tableau suivant illustre les nœuds exclus par cet algorithme avec un seuil égal à 0.25 :

Nœud	A_i	β_i	α_i	ω_i	R_j	R_j/N	Exclu(≥ 0.25)?
0	3	0,857	3	0,714	2,952	0,246	Non
1	3	0,857	2	0,762	2,952	0,246	Non
2	3	0,857	2	0,762	2,952	0,246	Non
3	3	0,857	2	0,762	2,952	0,246	Non
4	3	0,857	0	0,857	2,238	0,187	Non
5	3	0,857	0	0,857	2,238	0,187	Non
6	3	0,857	0	0,857	2,238	0,187	Non
7	3	0,857	0	0,857	2,286	0,190	Non
8	0	1,000	0	1,000	0,000	0,000	Non
9	1	0,952	3	0,810	0,714	0,060	Non
10	0	1,000	3	0,857	0,000	0,000	Non
11	0	1,000	3	0,857	0,000	0,000	Non

Table 2: Les taux d'accusation en utilisant l'algorithme de Crépeau

L'avantage :

- L'algorithme de ce protocole prend en considération les accusations malicieuses, et limite le nombre de faux positifs.

L'inconvénient:

- Ce protocole n'est pas recommandé pour les réseaux larges et dynamiques comme les VANETs, car il entraîne des échanges fréquents d'un grand nombre de messages comportant les tables d'accusation, ainsi les messages contenant les certificats des nœuds qui sont diffusés périodiquement à travers le réseau par chaque nœud.

Adaptation du protocole aux réseaux VANET

Comme le SDI d'un nœud peut détecter efficacement les nœuds malveillants voisins, nous proposons que les nœuds dans le protocole de Crépeau doivent échanger les messages seulement avec leurs voisins les plus proches (les voisins à-un-saut dans les autoroutes). Ces messages doivent être rediffusés périodiquement afin d'avertir les nouveaux voisins.

d- Le protocole LEAVE (Local Eviction of Attackers by Voting Evaluators)

Raya et al. [30], proposent un protocole de révocation distribuée destiné aux réseaux VANET. Ce protocole est similaire à celui de Chan (le protocole de révocation distribuée basé sur la cryptographie à seuil) mais avec les modifications suivantes :

- La signature numérique est utilisée à la place des clés partagées.
- Un nœud A qui veut voter contre un nœud M, doit diffuser périodiquement aux nœuds voisins (à un saut) un message d'alerte "WARN_M".
- Chaque nœud enregistre les messages "WARN" reçus sur une liste d'accusation pour une durée limitée.
- Lorsque le nœud exécutant le protocole veut évaluer un autre nœud quelconque, il utilise un algorithme spécifique pour calculer le taux d'accusation. Si ce dernier dépasse un seuil prédéfini Q_T (0.5 est utilisé dans l'article), il doit exclure ce nœud et ignorer ses messages temporairement. Ensuite un message "DISREGARD_M" est diffusé pour avertir les autres nœuds non voisins; ce message comporte un certain nombre de signatures de

nœuds qui ont voté contre M, pour donner plus de crédibilité au contenu du message. Les nœuds récepteurs de ce message doivent cesser de diffuser les messages "WARN_M"

- Les nœuds existants sur la liste noire seront exclus pour une durée limitée seulement, mais les messages liés à la sécurité reçus de la part de ces nœuds seront acceptés.

L'algorithme de calcul du taux d'accusation de LEAVE :

Contrairement au protocole de Chan, LEAVE ne calcule pas le nombre d'accusations pour exclure un nœud, mais il associe des poids pour chaque accusation émise contre ce dernier, puis il calcule le taux d'accusation sur la base de la moyenne pondérée. Le but de cette pondération est de minimiser l'influence des accusations des nœuds qui sont eux mêmes accusés par d'autres nœuds.

Malheureusement les nœuds malveillants générant des accusations falsifiées ne sont pas nécessairement détectés par les SDI et par conséquent l'influence de leurs accusations demeure importante.

Dans le protocole LEAVE le taux d'accusation est calculé suivant la formule donnée ci-dessous :

Soit v un nœud exécutant l'algorithme LEAVE pour calculer τ_j le taux d'accusation d'un nœud j.

$$\tau_j = \frac{1}{P_j} \sum_{i=1}^{P_j} \sigma_{ij} \cdot \omega_i \quad \text{avec} \quad \omega_i = 1 - \alpha_i.$$

σ_{ij} est égale à 1 si le nœud i accuse le nœud j, et égale à 0 autrement.

P_j est le nombre de voisins communs à j et v.

α_i représente la proportion des nœuds voisins communs à i et v qui ont accusé i.

A titre d'exemple, nous supposons que les nœuds ont la même liste de voisin, et leurs accusations sont modélisées par le graphe d'accusation de la figure 4.4. Le tableau suivant illustre les nœuds exclus par cet algorithme avec un seuil égal à 0.25 :

Nœud	α_i	ω_i	τ_j	Exclu(≥ 0.25)
0	0.250	0.750	$0.243=(0.917+1.000+1.000)/12$	Non
1	0.250	0.750	$0.243=(0.917+1.000+1.000)/12$	Non
2	0.250	0.750	$0.243=(0.917+1.000+1.000)/12$	Non
3	0.250	0.750	$0.243=(0.917+1.000+1.000)/12$	Non
4	0.250	0.750	$0.187=(0.750+0.750+0.750)/12$	Non
5	0.250	0.750	$0.187=(0.750+0.750+0.750)/12$	Non
6	0.250	0.750	$0.187=(0.750+0.750+0.750)/12$	Non
7	0.250	0.750	$0.187=(0.750+0.750+0.750)/12$	Non
8	0.000	1.000	0.000	Non
9	0.083	0.917	$0.062=0.750/12$	Non
10	0.000	1.000	0.000	Non
11	0.000	1.000	0.000	Non

Table 3 : Les taux d'accusation en utilisant le protocole LEAVE

Les avantages :

- En utilisant LEAVE le processus de révocation d'un nœud ne concerne que ceux situant dans une petite zone géographique, donc ce protocole est efficace dans les réseaux à haute densité.
- Les messages "WARN" et "DISREGARD" sont diffusés périodiquement, et par conséquent les nouveaux voisins peuvent être avertis rapidement.

Les inconvénients :

- L'algorithme utilisé dans LEAVE ne contient aucun mécanisme pour diminuer les poids des accusations falsifiées des attaquants indétectable par les nœuds honnêtes (attaquants sophistiqués).
- Le nombre de signatures à inclure dans un message disregard pose des problèmes en termes de sécurité et de consommation de bande passante. A cet effet, les auteurs proposent d'inclure quatre signatures ; cependant, ce nombre n'est pas coûteux quant à la consommation de la bande passante d'une part mais réduit le nombre minimum d'attaquants sophistiqués pouvant causer un déni de service d'autre part.
- le protocole requiert une très bonne observabilité.

Amélioration du protocole LEAVE

Nous proposons d'éliminer la procédure de dissémination des messages DISREGARD, et au lieu de générer et rediffuser les messages WARN pour chaque nœud malveillant, les nœuds rediffusent seulement un seul message WARN incluant la liste de tous les nœuds accusés.

4.4 Conclusion

Dans ce chapitre, nous avons adapté le protocole de routage ad hoc sécurisé SAODV aux réseaux VANET, et nous avons montré que, à cause de l'aspect décentralisé des réseaux ad hoc, les techniques cryptographiques seules ne sont pas suffisantes pour assurer la sécurité des protocoles de routage. A cet effet, nous avons présenté les PRD qui permettent aux nœuds du réseau de détecter les nœuds malveillants de manière rapide, voire même avant l'interaction avec eux. Cependant, nous avons vu que ces protocoles sont vulnérables aux problèmes de fausses accusations générées par les nœuds malveillants qui visent à exclure une partie importante de nœuds honnêtes du réseau, et mettre en péril la disponibilité de ce dernier. Donc, nous avons proposé des améliorations sur quelques PRD afin d'être utilisés de manière efficace pour exclure les nœuds malveillants de l'opération de routage dans les VANETs.

Dans le chapitre suivant, nous présenterons notre propre protocole de révocation distribuée qui prend en considération les propriétés spécifiques des réseaux VANET tout en minimisant l'impact de fausses alertes sur la disponibilité du réseau.

Chapitre 5

Notre nouveau protocole **SEDIREP** (SEcure DIstributed REvocation Protocol)

5.1 Introduction

Malgré que les PRD permettent la détection des nœuds malveillants de manière rapide par rapport aux autres solutions, ces protocoles, à cause des algorithmes utilisés par les analyseurs, restent vulnérables aux quelques attaques effectuées par un certain ensemble de nœuds malveillants qui sont en coalition.

De toute façon, la détection effectuée par un SDI ne peut être considérée comme parfaite; ainsi les attaquants peuvent présenter un comportement bienveillant, coopératif, d'une part, et générer de fausses alertes afin de causer un déni de service d'une autre part. Ce dernier type d'attaque qu'on a appelé attaque sophistiquée est très difficile à y faire face, car il concerne le PRD lui-même et non pas le système à sécuriser. Malheureusement, tous les PRD existants sont vulnérables à ce type d'attaques et ne prennent pas les contres mesures nécessaires; ainsi l'augmentation de la valeur du seuil de taux d'accusation minimise le risque de cette attaque d'une part, et augmente les risques d'avoir d'autres types d'attaques (car dans ce cas les nœuds doivent avoir une très bonne observabilité) d'une autre part.

Dans ce contexte, nous proposons notre propre protocole **SEDIREP**. Ce dernier peut être utilisé conjointement avec n'importe quel protocole de routage sécurisé destiné aux réseaux VANET. SEDIREP minimise l'impact de l'attaque précédente sur le réseau, mais pas au détriment d'augmentation du risque d'avoir d'autres attaques.

Dans ce chapitre, nous commençons d'abord par une description de l'adversaire, puis nous présentons notre protocole SEDIREP, ensuite nous discutons de la sécurité apportée, enfin, nous analysons la performance de notre protocole avec les différentes simulations.

5.2 Le modèle d'adversaire

Nous supposons l'existence de plusieurs attaquants coopérants et capables d'échanger les messages entre eux; ces attaquants ayant un accès légitime au réseau et possédant leurs propres certificats, ils ont le droit de communiquer avec les autres membres du réseau.

Nous supposons aussi que les nœuds visent à causer un déni de service par la génération de fausses alertes.

Dans le réseau, un ensemble de nœuds peut être séparé en deux sous-ensembles (l'un des deux est éventuellement vide) : un sous-ensemble comprenant des nœuds honnêtes, et un autre comprenant des nœuds malveillants. La figure 5.1 illustre ces deux sous-ensembles dans un graphe d'accusation dont les nœuds verts représentent les nœuds honnêtes, tandis que les nœuds rouges représentent les nœuds malveillants. A partir de ce graphe nous pouvons donc distinguer les types d'accusations suivantes:

1. Une accusation émise par un nœud honnête contre un nœud malveillant (représenté par l'arc vert), est généralement due aux attaques simples détectables par le SDI.
2. Une accusation émise par un nœud malveillant contre un nœud honnête: il s'agit d'une attaque contre le protocole de révocation lui-même afin de causer un déni de service. L'attaque doit comprendre un ensemble d'attaquants coopérants indétectables par les SDI pour qu'elle soit efficace.
3. Une accusation émise pas un nœud malveillant contre un autre nœud malveillant, il s'agit d'une attaque éventuelle contre le PRD utilisé, si ce dernier ne prend pas en considération ce type d'actions qui vise à dérouter les observateurs.

On peut constater que dans le graphe d'accusation nous n'avons pas présenté une accusation d'un nœud honnête émise contre un autre nœud honnête, car ce type d'action est rare et il concerne un faux positif dû seulement aux imperfections du SDI.

Enfin, nous pouvons déduire que l'identification de l'ensemble des nœuds malveillants à partir du graphe d'accusation n'est pas une tâche facile. Les attaquants peuvent utiliser toutes les combinaisons d'accusations afin d'exclure un nombre élevé des nœuds honnêtes et mettre en péril la disponibilité du réseau.

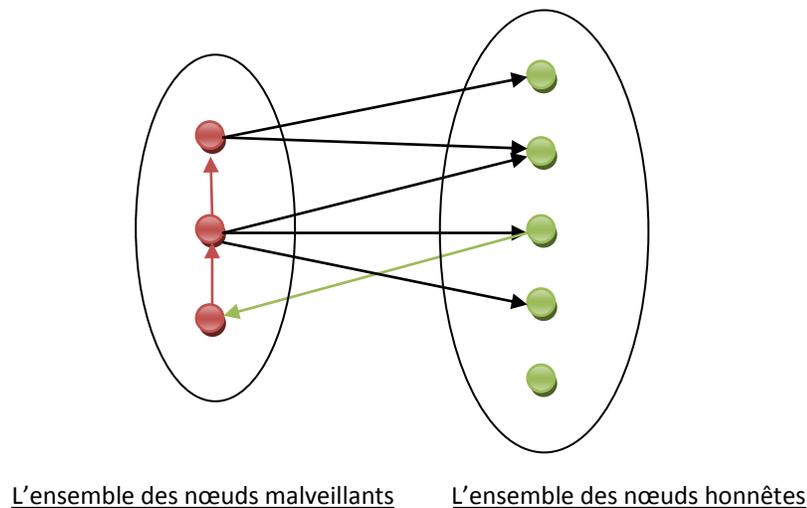


Figure 5.1: Les types d'accusations dans un graphe d'accusation

5.3 Le protocole SEDIREP (SEcure DIstributed REvocation Protocol)

5.3.1 Les hypothèses de conception du protocole SEDIREP

Nous supposons que le réseau est de type VANET dont les nœuds sont équipés d'antennes omnidirectionnelles ayant la même portée de transmission, et que les nœuds honnêtes constituent la majorité des nœuds du réseau. De plus, dans la conception de notre protocole nous n'avons pas pris en compte le cas où les nœuds malveillants constituent une majorité locale, car il est impossible d'avoir un PRD efficace traitant ce cas à cause de l'aspect distribué de ces protocoles.

5.3.2 Le mécanisme de détection d'intrusion

Puisque SEDIREP sera utilisé pour améliorer la sécurité de routage dans les VANETs, le SDI utilisé doit prendre en considération les caractéristiques des protocoles de routage dans cet environnement. Dans le protocole SEDIREP, chaque nœud doit activer le mode *promiscuous* afin de capturer les paquets émis par ses voisins ou destinés à ses voisins à un saut, et les analyser suivant le modèle présenté dans la section 2.6.3. Comme nous avons veillé à rendre notre protocole indépendant de protocole de routage sécurisé à utiliser, nous n'avons pas exigé toutes les vérifications à effectuer pour la détection de malveillance, mais nous en avons sélectionnées quelques-unes qui sont importantes.

Elles comprennent :

- **La vérification de la position géographique signalée:** comme les protocoles de routage géographiques, sont préconisés à être utilisés dans les réseaux VANET [73] [74], alors la vérification de la position géographique est une nécessité pour la sécurité du routage.

Dans la littérature, il existe plusieurs mécanismes proposés par les auteurs des articles [75] [76] [77] [78], mais dans notre protocole, nous avons choisi d'en utiliser deux mécanismes proposés dans [78] :

- Le premier mécanisme (cf. figure 5.2) suppose que tous les nœuds ont la même portée de la zone de couverture, et par conséquent peuvent détecter la position géographique falsifiée annoncée par le nœud, si cette position est hors de leurs zones de couverture.
- Le deuxième mécanisme concerne la mobilité des nœuds: comme les véhicules ont une vitesse limite maximale exigée par les lois physiques ou par le code de la route, alors un nœud ne doit pas annoncer dans deux balises consécutives, deux positions contradictoires.

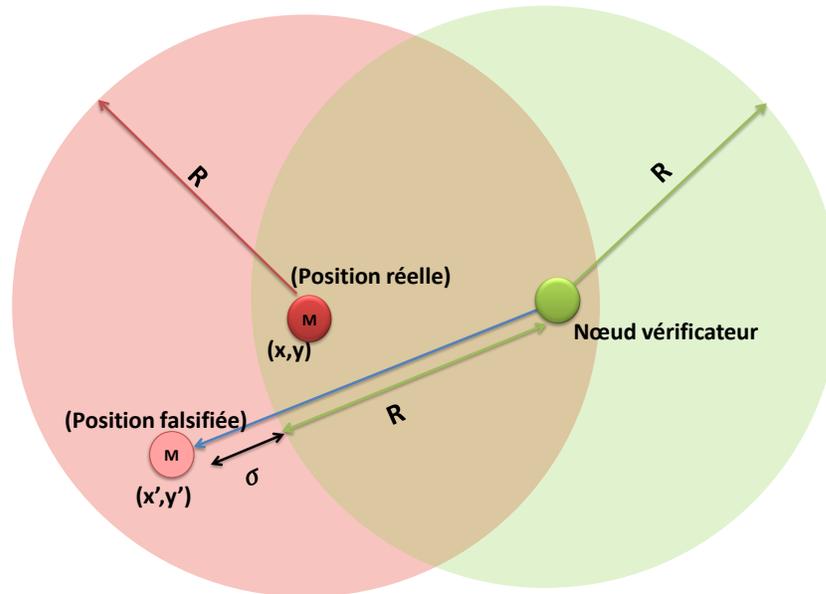


Figure 5.2 : Vérification de localisation en utilisant la zone de couverture

- **La vérification de la fonction d’acheminement de paquets** : elle consiste en l’utilisation par le nœud vérificateur d’un *WATCHDOG* (voir 3.5.5) pour déterminer le taux de paquets correctement acheminés (retransmis) par le nœud dont il a la charge; pendant une durée définie.
- **La vérification du nombre de paquets transmis pendant une durée** : afin de préserver la bande passante et éviter la congestion dans le réseau, il est indispensable de définir une limite pour le nombre de paquets possibles à transmettre par un nœud en une durée déterminée.
- **La vérification du processus d’accès au canal** : chaque nœud doit vérifier que ses voisins respectent les règles d’accès au médium spécifiées par la couche MAC. Les nœuds malveillants peuvent modifier leurs Backoff pour avoir plus de chance que leurs voisins à accéder au canal partagé. Ce type de vérification peut être aussi effectué au niveau de la couche réseau si le protocole de routage utilisé spécifie des mécanismes de contrôle similaires sur les requêtes d’établissement de routes.

5.3.3 La description du protocole SEDIREP

SEDIREP est un PRD conçu pour améliorer la sécurité des protocoles de routage dans les réseaux VANET. A cet effet, nous veillons à ce que notre protocole prenne en considération le modèle de mobilité et les exigences de routage dans cet environnement comprenant la rapidité de détection ainsi que la disponibilité du réseau.

Pour que le protocole s'adapte à la nature de cet environnement, nous avons conçu SEDIREP en considérant les dimensions suivantes :

- **Le modèle de mobilité:** comme ces réseaux ont une topologie très dynamique, les nouveaux voisins doivent détecter le nœud malveillant le plus rapidement possible. A cet effet, dans notre protocole, les nœuds doivent périodiquement transmettre les messages d'accusations, alors que les pseudonymes (dorénavant, nous utilisons le mot « pseudonyme » au lieu d'identifiant) des nœuds sur la liste d'accusation ne sont gardés que pour une durée déterminée (d'environ une minute) afin d'en limiter la longueur. Ainsi, les nœuds malveillants ont tendance à attaquer de façon continue.
- **La densité des nœuds et la bande passante :** les nœuds concernés par la révocation d'un nœud, sont ceux se situant dans sa zone de couverture; donc chaque nœud doit se charger de ne contrôler que les activités de ses voisins à un saut, et lors de détection d'un nœud malveillant, il diffuse un message d'accusation destiné seulement à ses voisins à un saut. Nous avons adopté cette démarche pour la raison suivante : puisque ce type de réseau est généralement caractérisé par une haute densité de nœuds, il convient de limiter le nombre des observateurs aux nœuds voisins afin que ceux recevant les messages d'accusations puissent bien vérifier le comportement de leurs correspondants d'une part, et de préserver la bande passante en minimisant le nombre des messages d'accusations diffusés d'autre part.

Dans le cas où un nœud a plusieurs accusations à signaler, nous avons choisi qu'il les diffuse toutes à la fois dans un seul message. A cet effet, nous avons adopté le format de message illustré dans la figure 5.3. Avec ce format de message d'accusation ce dernier doit inclure le pseudonyme de l'accusateur ainsi que celui des nœuds accusés (dénnotés par PSD_1, \dots, PSD_n , respectivement) et leur nombre, l'horodateur pour assurer la fraîcheur du message, le certificat et la signature pour l'authentifier.

PSD de L'accusateur	Nombre des nœuds accusés	Horodateur	Signature Numérique	PSD ₁	PSD _n	Certificat Numérique
---------------------	--------------------------	------------	---------------------	------------------	-------	------------------	----------------------

Figure 5.3: Le format de message du protocole SEDIREP

- **Les exigences de sécurité:** comme il peut s'agir du routage d'un message lié à la sécurité, assurer la disponibilité de réseau est une préoccupation primordiale. A cet effet, nous avons proposé un algorithme permettant de mitiger l'impact des nœuds malveillants indétectables par le SDI sur la disponibilité du réseau. De plus, notre mécanisme de sanction exclut les nœuds dans la liste noire de l'analyseur définitivement (au minimum pendant une durée égale à la durée de vie du certificat à court terme), mais les messages liés à la sécurité (ceux qui sont signés par l'autorité de certification) reçus de leur part sont acceptés.

a- L'algorithme de l'analyseur :

Nous rappelons que le but de l'analyseur est l'attribution d'une note ou un taux d'accusation à un nœud sur la base duquel il sera sanctionné ou non. Dans toutes les propositions précédentes, tous les messages d'accusations reçus contre un nœud sont utilisés par l'algorithme de l'analyseur pour en calculer le taux. Mais dans notre algorithme nous avons introduit une opération de filtrage qui permet d'ignorer une accusation contre un nœud si l'accusateur est moins crédible que l'accusé.

Cette opération de filtrage est inspirée de notre comportement social: dans le cas d'un nombre de personnes accusées par d'autres, on tend à croire en premier lieu celles qui ne sont pas accusées par nous mêmes, puis en celles qui sont plus nombreuses. Les personnes malveillantes peuvent aussi cependant créer une confusion: l'une d'entre elles en accuse une autre. Cette situation réclame à faire une investigation par un spécialiste (un juge à titre d'exemple). Celui-ci appelle les accusateurs pour témoignages, ensuite si le nombre de témoins est suffisant, il vérifie les antécédents de chacun avant d'accepter sa version.

Il en est de même dans notre algorithme : au début, un nœud vérificateur v doit vérifier sur ses listes noires, si le nœud à vérifier c n'a pas été exclu auparavant; v consulte ensuite sa liste d'accusation afin d'établir celle des accusateurs de c ; nous pouvons donc distinguer trois cas :

Si le nombre de nœuds accusant c est plus grand que la moitié de celui des nœuds voisins communs à c et v **NVN** (Nombre de Voisins Communs), alors c est ajouté immédiatement sur la liste noire de l'analyseur car la majorité de ses observateurs l'accusent.

Si le taux d'accusation qui est égal au rapport du nombre des accusateurs de c sur **NVN** est plus petit que la valeur du seuil (sa valeur est prédéfinie et a une valeur entre 0 et 1), alors c ne sera pas ajouté à la liste noire.

Si les deux cas précédents ne sont pas vrais, alors v doit effectuer l'opération de filtrage sur la liste des accusateurs de c en éliminant ceux qui sont moins crédibles que c . Ensuite, v calcule le taux d'accusation en divisant le nombre d'éléments de la liste filtrée par **NVN**; si le taux d'accusation est plus grand que la valeur du seuil, alors c est ajouté à la liste noire de l'analyseur.

L'opération de filtrage:

Nous avons indiqué dans notre algorithme qu'un nœud vérificateur v peut effectuer l'opération de filtrage sur les accusateurs de c ; en éliminant ceux qui sont moins crédibles que c . La notion de crédibilité ici concerne deux éléments: l'état et le comportement d'un nœud accusateur, dont voici un ensemble de définitions formelles les concernant que nous utiliserons plus tard afin de déterminer une fonction appropriée pour mesurer la crédibilité des nœuds :

Soit $G(X, A)$ un graphe d'accusation construit par le nœud v , où X est l'ensemble des nœuds voisins communs à c et v , et A l'ensemble des accusations effectuées par les nœuds appartenant à X .

Définition 1:

Soit x un nœud quelconque appartenant à X , on définit par \mathcal{A}_x l'ensemble des accusations effectuées par ce nœud comme suit:

$$\mathcal{A}_x = \{(x, y) \in A / y \in X\}.$$

Définition 2:

On définit par \mathcal{A} l'ensemble des accusations possibles qui peuvent être effectuées par un nœud quelconque appartenant à X de la manière suivante :

$$\mathcal{A} = \{(x, y)/x, y \in X\}$$

$$\text{Donc } \forall x \in X, \mathcal{A} = \mathcal{A}_x \cup \overline{\mathcal{A}_x} \quad \text{et } |\mathcal{A}| = |X|$$

Définition 3:

Le comportement d'un nœud accusateur x ressemble à celui d'un autre nœud y s'il y a un grand nombre de nœuds appartenant à X , accusés (ou non) par les deux nœuds sus énoncés à la fois ; et la valeur de cette similarité est calculée par la fonction de similarité comportementale f_c définie comme suit :

$$f_c(x, y) = |\mathcal{A}_x \cap \mathcal{A}_y| + |\overline{\mathcal{A}_x} \cap \overline{\mathcal{A}_y}|$$

Définition 4:

Nous définissons la fonction comportementale globale de la manière suivante :

$$f_{cg}(x) = \frac{1}{|X|} \sum_{y \in X - \{x\}} f_c(x, y)$$

Définition 5:

L'état d'accusation d'un nœud x est similaire à celui d'un autre nœud y s'il y a un grand nombre de nœuds appartenant à X accusant (ou non) les deux nœuds à la fois. La valeur de cette similarité est calculée par la fonction suivante :

$$f_e(x, y) = |\{z \in X/(z, x), (z, y) \in A\} \vee \{z \in X/(z, x), (z, y) \notin A\}|$$

$$\Rightarrow f_e(x, y) = |\{z \in X/(z, x), (z, y) \in A\}| + |\{z \in X/(z, x), (z, y) \notin A\}|$$

Puisqu'on considère qu'une seule accusation possible du nœud z contre un autre nœud, alors :

$$f_e(x, y) = |\{(z, y) \in A/(z, x) \in A \wedge z \in X\}| + |\{(z, y) \notin A/(z, x) \notin A \wedge z \in X\}|$$

Définition 6:

Nous définissons la fonction de similarité d'état globale de la manière suivante :

$$f_{eg}(x) = \frac{1}{|X|} \sum_{y \in X - \{x\}} f_e(x, y)$$

$$f_{eg}(x) = \frac{1}{|X|} \sum_{y \in X - \{x\}} (|\{(z, y) \in A/(z, x) \in A \wedge z \in X\}| + |\{(z, y) \notin A/(z, x) \notin A \wedge z \in X\}|)$$

$$\Rightarrow f_{eg}(x) = \frac{1}{|X|} \left[\sum_{y \in X - \{x\}} \left| \bigcup_{z \in X} \{(z, y) \in A/(z, x) \in A\} \right| + \sum_{y \in X - \{x\}} \left| \bigcup_{z \in X} \{(z, y) \notin A/(z, x) \notin A\} \right| \right]$$

Puisque les ensembles $\{(z, y_i) \in A / (z, x) \in A\}$ pour tout $y_i \in X - \{x\}$ sont disjoints deux à deux alors :

$$f_{eg}(x) = \frac{1}{|X|} \left[\left| \bigcup_{y \in X - \{x\}, z \in X} \{(z, y) \in A / (z, x) \in A\} \right| + \left| \bigcup_{y \in X - \{x\}, z \in X} \{(z, y) \notin A / (z, x) \notin A\} \right| \right]$$

$$f_{eg}(x) = \frac{1}{|X|} \left[\left| \bigcup_{y \in X - \{x\}, z \in X, (z, x) \in A} \{(z, y) \in A\} \right| + \left| \bigcup_{y \in X - \{x\}, z \in X, (z, x) \notin A} \{(z, y) \notin A\} \right| \right]$$

$$f_{eg}(x) = \frac{1}{|X|} \left[\left| \bigcup_{y \in X, z \in X, (z, x) \in A} \{(z, y) \in A\} \right| - \left| \bigcup_{y=x, z \in X, (z, x) \in A} \{(z, y) \in A\} \right| + \left| \bigcup_{y \in X, z \in X, (z, x) \notin A} \{(z, y) \notin A\} \right| - \left| \bigcup_{y=x, z \in X, (z, x) \notin A} \{(z, y) \notin A\} \right| \right]$$

$$f_{eg}(x) = \frac{1}{|X|} \left[\left| \bigcup_{y \in X, z \in X, (z, x) \in A} \{(z, y) \in A\} \right| - \left| \bigcup_{z \in X} \{(z, x) \in A\} \right| + \left| \bigcup_{y \in X, z \in X, (z, x) \notin A} \{(z, y) \notin A\} \right| - \left| \bigcup_{z \in X} \{(z, x) \notin A\} \right| \right]$$

$$f_{eg}(x) = \frac{1}{|X|} \left[\left| \bigcup_{y \in X, z \in X, (z, x) \in A} \{(z, y) \in A\} \right| + \left| \bigcup_{y \in X, z \in X, (z, x) \notin A} \{(z, y) \notin A\} \right| - \left| \bigcup_{z \in X} \{(z, x) \notin A \vee (z, x) \in A\} \right| \right]$$

$$f_{eg}(x) = \frac{1}{|X|} \left[\left| \bigcup_{y \in X, z \in X, (z, x) \in A} \{(z, y) \in A\} \right| + \left| \bigcup_{y \in X, z \in X, (z, x) \notin A} \{(z, y) \notin A\} \right| - |X| \right]$$

$$f_{eg}(x) = \frac{1}{|X|} \left[\left| \bigcup_{z \in X, (z, x) \in A} \mathcal{A}_z \right| + \left| \bigcup_{z \in X, (z, x) \notin A} \overline{\mathcal{A}_z} \right| - 1 \right]$$

Donc la valeur de la fonction d'état global d'un nœud x est égale au nombre d'éléments des ensembles \mathcal{A}_z (concernant les nœuds accusateurs de x), plus le nombre d'éléments des ensembles $\overline{\mathcal{A}_z}$ (concernant les nœuds qui n'ont pas accusé x), divisé sur $|X|$, moins un.

Dans le cas où l'observabilité est minimale et où il y a déni de service généré par les fausses alertes, nous pouvons distinguer ce qui suit :

Premièrement : l'observabilité des nœuds honnêtes est minime, donc chaque nœud honnête h n'a pas une tendance à adresser les accusations (donc ils ont le même comportement), et la valeur de $|\overline{\mathcal{A}_h}|$ sera plus grande.

Deuxièmement : puisque les nœuds malveillants accusateurs constituent une minorité, chaque nœud malveillant m essaye d'accuser un nombre important de nœuds honnêtes afin de pouvoir en exclure un grand nombre, donc ces nœuds malveillants ont le même comportement, et leurs $|\mathcal{A}_m|$ sera plus grand.

A partir de la description précédente, dans le cas d'un déni de service les nœuds honnêtes ont des $|\overline{\mathcal{A}_h}|$ plus grands, et les nœuds malveillants des $|\mathcal{A}_m|$ plus grands, et puisque seuls les nœuds malveillants ont tendance à accuser les nœuds honnêtes, alors les valeurs de la fonction d'état de ces derniers seront plus grandes (voir la formule de la définition 6).

Dans le cas où l'observabilité des nœuds est bonne, il y a plus de chance qu'une partie importante des nœuds honnêtes détectent le comportement malveillant de manière efficace, donc, il est attendu que ces nœuds honnêtes détectant de manière efficace soient nombreux et aient le même comportement, et par conséquent ils ont des grandes valeurs pour la fonction comportementale globale.

Ainsi, dans le cas où l'observabilité est bonne, la fonction comportementale globale est un très bon indicateur de la crédibilité des nœuds honnêtes, tandis que dans le cas où l'observabilité est mauvaise la fonction d'état globale des nœuds malveillants sera l'indicateur le plus approprié pour la crédibilité des nœuds honnêtes. Comme il est difficile de prévoir la nature des éventuels attaquants, il convient de prendre les deux cas précédents en considération, et pour mesurer la crédibilité des nœuds, utiliser les deux fonctions f_{eg} et f_{cg} à la fois, en leurs associant les mêmes poids; par conséquent, on définit la fonction de crédibilité qui permet de la mesurer pour un nœud x quelconque de la manière suivante :

$$f_{cr}(x) = f_{cg}(x) + f_{eg}(x)$$

Enfin, la fonction comportementale globale permet à l'analyseur de SEDIREP de détecter la malveillance lorsque les SDI détectent de manière efficace, et la fonction d'état global permet d'éviter l'exclusion d'un nombre important de nœuds honnêtes par la génération de fausses alertes.

Voici la procédure SEDIREP exécutée par le nœud vérificateur v :

```

Fonction SEDIREP(c: nœud, NVC: ensemble_de_nœuds, A: ensemble_accusations,
liste_noire_SDI, liste_noire_analyseur: ensemble_de_nœuds) : booléen ;
// NVC est l'ensemble de voisins communs entre c et v
VAR
  Trusted : booléen ;
  Y : ensemble_de_nœuds;
  Taux: réel ;
DEBUT
  Si c ∈ liste_noire_SDI ou c ∈ liste_noire_analyseur alors Trusted =faux ;
  Sinon
    Y=LISTE_ACCUSATEURS (NVC,A,c) ;
    Taux =|Y|/ |NVC | ;
    Si Taux ≥ 0.5 alors Trusted= faux ;
    Sinon
      Y=FILTRE ( Y,c);
      Taux =|Y|/ |NVC | ;
      Si Taux ≥ SEUIL alors Trusted= faux ;
      Sinon
        Trusted= vrai ;
      Fin_Si
    Fin_Si
  Fin_Si
  Si non Trusted alors liste_noire_analyseur= liste_noire_analyseur ∪ {c} ; Fin_Si
  return Trusted ;
FIN

```

```

Fonction Filtrer(NVC: ensemble_de_nœuds,
c: nœud) : ensemble_de_nœuds ;
VAR
x : nœud ;
DEBUT
  Pour tout x ∈ NVC faire
    Debut
      Si  $f_{cr}(x) < f_{cr}(c)$  alors
        NVC=NVC-{x}
      Fin_Si
    Fin
  return NVC ;
FIN

```

```

Fonction LISTE_ACCUSATEURS (NVC: ensemble_de_nœuds,
A: ensemble_accusations, c: nœud): ensemble_de_nœuds;
VAR
x : nœud ;
DEBUT
  Pour tout x ∈ NVC faire
    Debut
      Si (x, c) ∉ A alors
        NVC=NVC-{x}
      Fin_Si
    Fin
  return NVC ;
FIN

```

- **Procédures pour calculer la fonction de crédibilité**

$$f_{cg}(x) = \frac{1}{|X|} \sum_{y \in X - \{x\}} f_c(x, y)$$

$$f_{cg}(x) = \frac{1}{|X|} \sum_{y \in X - \{x\}} (|\mathcal{A}_x \cap \mathcal{A}_y| + |\overline{\mathcal{A}}_x \cap \overline{\mathcal{A}}_y|)$$

Comme $|\mathcal{A}_x \cap \mathcal{A}_y| + |\overline{\mathcal{A}}_x \cap \overline{\mathcal{A}}_y|$ peut être obtenu si on modélise le comportement du nœud x de la manière suivante :

Soit A une matrice qui modélise le graphe d'accusation de la manière suivante :

$$A[i, j] = \begin{cases} 1 & \text{Si le nœud } i \text{ accuse } j \\ 0 & \text{Sinon} \end{cases}$$

Soit $A[i]$ un vecteur qui représente la ligne i de la matrice A , i l'indice qui correspond au nœud x et j l'indice qui correspond au nœud y .

Donc, $A[i]$ modélise \mathcal{A}_i et $\overline{\mathcal{A}}_i$ (les accusations émises/ non par i), par conséquent $A[i] \oplus A[j]$ qui représente le nombre d'éléments similaires entre $A[i]$ et $A[j]$, est égal à $|\mathcal{A}_x \cap \mathcal{A}_y| + |\overline{\mathcal{A}}_x \cap \overline{\mathcal{A}}_y|$, alors la fonction comportementale globale est donnée comme suit :

$$f_{cg}(i) = \frac{1}{|X|} \sum_{j=1; i \neq j}^{|X|} A[i] \oplus A[j] = \frac{1}{|X|} \sum_{j=1; i \neq j}^{|X|} \sum_{k=1}^{|X|} A[i, k] \oplus A[j, k]$$

Nous avons défini la fonction d'état globale de la manière suivante :

$$f_{eg}(x) = \frac{1}{|X|} \sum_{y \in X - \{x\}} (|\{(z, y) \in A / (z, x) \in A \wedge z \in X\}| + |\{(z, y) \notin A / (z, x) \notin A \wedge z \in X\}|)$$

1. $|\{(z, y) \in A / (z, x) \in A \wedge z \in X\}|$ est égal au nombre des nœuds accusant x et y simultanément.
2. $|\{(z, y) \notin A / (z, x) \notin A \wedge z \in X\}|$ est égal au nombre des nœuds n'accusant pas les nœuds x et y simultanément.

Sachant que $A'[j]$ désignant la colonne j de la matrice A , alors $A'[j]$ modélise les accusations contre le nœud j , alors $A'[i] \oplus A'[j]$ est aussi égal au nombre des nœuds accusant/non les nœuds i et j simultanément, alors :

$$f_{eg}(i) = \frac{1}{|X|} \sum_{j=1; i \neq j}^{|X|} A'[i] \oplus A'[j] = \frac{1}{|X|} \sum_{j=1; i \neq j}^{|X|} \sum_{k=1}^{|X|} A[k, i] \oplus A[k, j]$$

5.4 Analyse de performance de l'algorithme utilisé par SEDIREP

Dans cette section, nous analysons la performance de notre protocole SEDIREP.

5.4.1 Simulation

5.4.1.1 L'environnement de simulation

Pour analyser la performance de notre protocole nous avons utilisé l'outil NS2, ce dernier est un simulateur open source utilisé dans les recherches liées aux réseaux de communication d'ordinateurs [79]. Il est très populaire car il est à accès libre et la majorité des protocoles de réseaux ont été implémenté sous ce simulateur ; la documentation sur le NS-2 est largement disponible sur les différents sites WEB, nous citons "The ns Manual" [80], et " NS by Example " [81]. Pour le modèle de mobilité, nous avons particulièrement étudié le cas des autoroutes, car ces derniers sont plus contraignants en terme de durée de connectivité à cause de haute mobilité. A cet effet, nous avons utilisé l'outil « IMPORTANT » [82] pour générer les fichiers traces définissant des scénarios de mobilité, cet outil a été proposé par l'université de Californie du Sud afin que les simulations liées aux réseaux véhiculaires soient plus réalistes; la documentation et le code source sont téléchargeables depuis le site web [83].

Les propriétés de l'environnement de simulation sont données dans la table suivante :

Simulateur	NS-2 version 2.30
La portée des antennes	300m
Le nombre de nœuds	300
Le générateur de la mobilité	IMPORTANT
Le modèle de mobilité	Freeway
Les caractéristiques de l'autoroute	5Km/4 voies pour chaque sens
La nature des antennes	Omnidirectionnelle
L'intervalle de temps minimum entre deux messages d'accusations pour chaque nœud	1 seconde

Table 4 : Environnement de simulation

5.4.1.2 Les métriques et paramètres de simulations

Nous avons utilisé comme métrique le taux de détection de nœuds malveillants et le taux de faux positifs (le taux de fausse détection), ce dernier représente le taux des nœuds honnêtes qui ont été exclus à cause de messages d'accusations falsifiés générés par les nœuds malveillants. Comme la plupart des protocoles de révocation distribuée ne spécifient pas les SDI utilisés, alors ces deux métriques ne concernent que la révocation effectuée par l'analyseur. Pour l'analyse, nous avons défini deux taux de nœuds malveillants 20% et 30% des nœuds qui sont distribués aléatoirement dans le l'environnement de simulation, chacun de ces nœuds génère des messages d'accusations malicieux (falsifiés) contre tous ses voisins, tandis que chacun des nœuds honnêtes génère les messages d'accusations contre un nœud malveillant, seulement si la distance qui les sépare (on appelé cette distance : «Distance maximum de détection de malveillance ») est moins que certaines limites qui varie entre 0 et 300m, la variation de cette distance exprime dans une certaine mesure le nombre des messages d'accusations émis contre les nœuds malveillants .

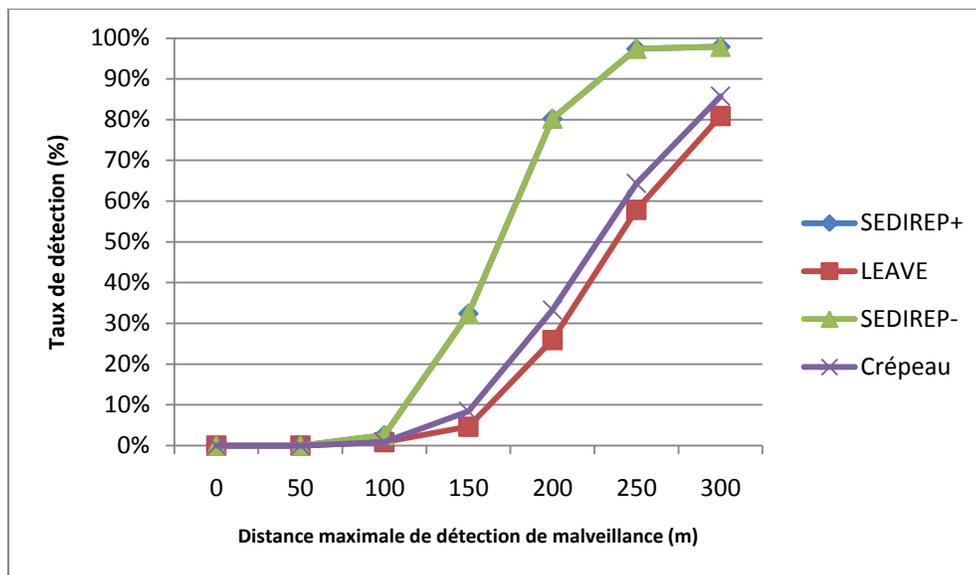
Pour comparer la performance de notre protocole avec d'autres, nous avons choisi le protocole de révocation de Crépeau et le protocole LEAVE, avec chaque protocole nous avons envisagé deux valeurs pour le seuil : 0.25 et 0.5 respectivement. En ce qui concerne notre protocole, nous avons retenu les mêmes paramètres, et les mêmes scénarios de mobilité.

Pour bien analyser le protocole SEDIREP, nous avons défini deux variantes de ce protocole : la variante SERIDIP- qui représente notre protocole de révocation distribuée sans l'opération de filtrage et la variante SERIDIP+ qui représente notre protocole de révocation distribuée avec l'opération de filtrage tel qu'il est défini dans la section précédente.

Nous rappelons que la stratégie du protocole de Crépeau et de protocole LEAVE sont basés sur la réduction des poids des accusations suspectes d'être malicieuses, et la stratégie de SERIDIP+ se base sur leur élimination. Donc, la variante SERIDIP- doit assurer des taux de détection plus élevés tant que aucune des accusations ne sera éliminée ni son poids sera réduit.

5.4.2 Résultats et discussions

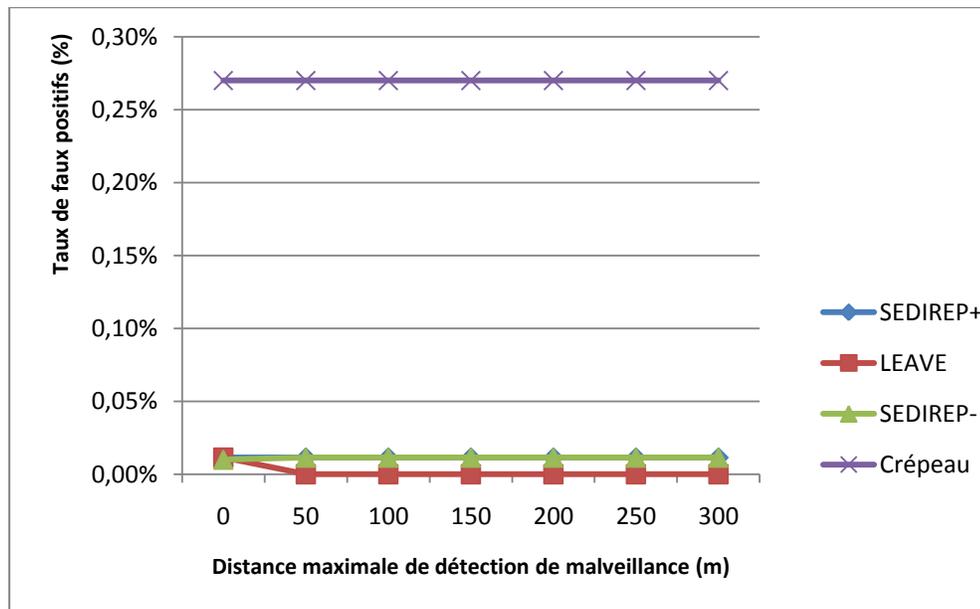
Dans cette partie, nous présentons et nous analysons les résultats de simulation que nous avons obtenus à travers les scénarios précédemment définis.



	SEDIREP+	LEAVE	SEDIREP-	Crépeau
0	0,00%	0,00%	0,00%	0,00%
50	0,00%	0,00%	0,00%	0,00%
100	2,56%	0,87%	2,56%	0,87%
150	32,41%	4,66%	32,41%	8,40%
200	80,24%	25,92%	80,24%	33,27%
250	97,40%	57,87%	97,40%	64,35%
300	97,90%	80,92%	97,90%	85,76%

Figure 5.4 : Taux de détection des nœuds malveillants (cas 20% de nœuds sont malveillants et seuil=0. 5)

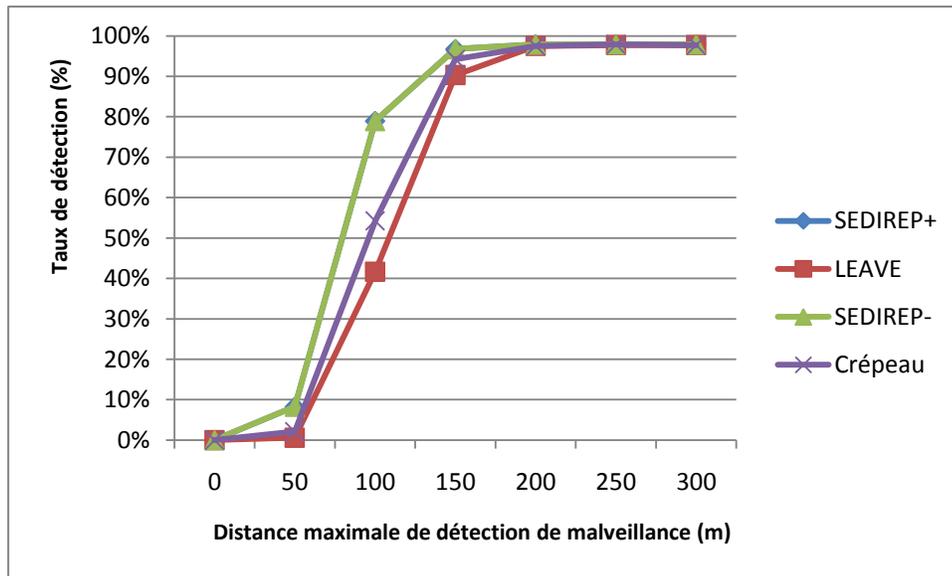
La figure 5.4 illustre les taux de détection de nœuds malveillants, avec le scénario où 20% des nœuds du réseau sont malveillants et un seuil égale à 0.5. Nous remarquons que la détection des nœuds malveillants croît à l'augmentation de distance de détection, car cette dernière influe sur le nombre des messages d'accusations contre les nœuds malveillants. Avec ce scénario, les deux variantes de protocoles SEDIREP présentent les meilleurs des cas avec des taux de détection égaux ; cela signifie que l'opération de filtrage n'a pas affecté la détection des nœuds malveillants. Nous remarquons ainsi que SEDIREP - (comme SEDIREP +) n'ont pas assuré un taux de détection égale à 100% même si la distance maximale de détection de malveillance est égale à 300m (observabilité optimale), cela signifie qu'il y a des situations où la majorité des voisins d'un nœud honnête sont des nœuds malveillants ou il y a des pertes de messages d'accusations.



	SEDIREP+	LEAVE	SEDIREP-	Crépeau
0	0,01%	0,01%	0,01%	0,27%
50	0,01%	0,00%	0,01%	0,27%
100	0,01%	0,00%	0,01%	0,27%
150	0,01%	0,00%	0,01%	0,27%
200	0,01%	0,00%	0,01%	0,27%
250	0,01%	0,00%	0,01%	0,27%
300	0,01%	0,00%	0,01%	0,27%

Figure 5.5 : Taux des nœuds faux positifs (cas 20% de nœuds sont malveillants et seuil=0.5)

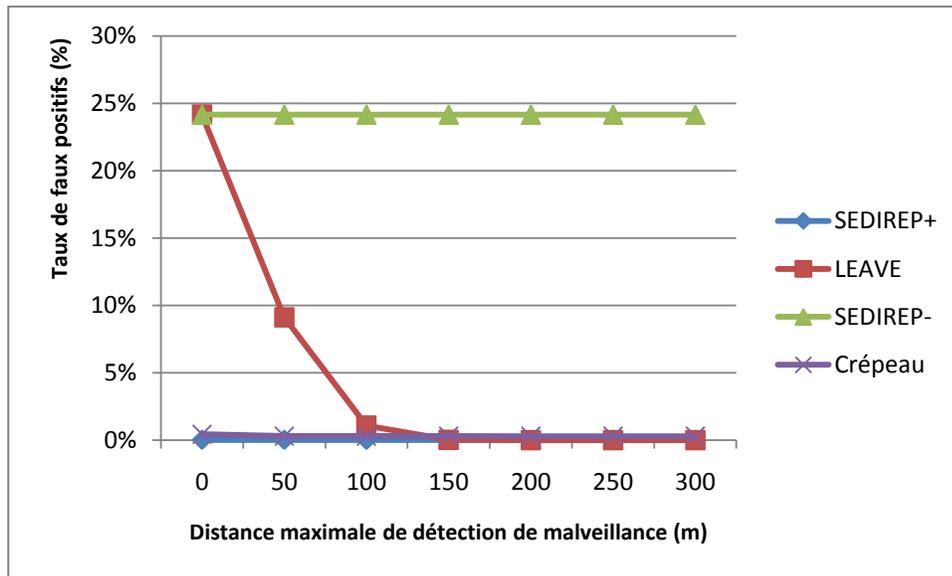
La figure 5.5 illustre le taux de faux positifs avec le scénario où 20% des nœuds du réseau sont malveillants et un seuil égal à 0.5. Avec le protocole SEDIREP- le taux de faux positifs est fixe et égal à 0.01%, cela signifie qu'il y a au minimum 0.01 % de situations où les nœuds malveillants constituent une majorité locale. Comme le protocole SEDIREP-, le taux de faux positifs avec le protocole SEDIREP+ est fixe et égal à 0.01%, cela signifie que le filtrage n'a pas pu éliminer les accusations des nœuds malveillants lorsque les nœuds honnêtes ne constituent pas une majorité locale. Avec le protocole LEAVE lorsque la distance de détection maximale est égale à 0m; le taux de faux positifs égale à 0.01% car dans ce cas les accusations contre les nœuds malveillants n'existent pas(seulement les nœuds malveillants qui envoient les messages d'accusations), et par conséquent les taux calculés en utilisant l'algorithme de LEAVE seront égaux aux taux calculés en utilisant SEDIREP- ; à partir de distance de détection supérieure à 50m le taux de faux positifs avec le protocole LEAVE est nul, car les accusations des nœuds honnêtes adressées aux nœuds malveillants ont diminué les taux d'accusation. Le taux de faux positifs avec le protocole de Crépeau reste inchangé quelle que soit la distance de détection, cela signifie que les accusations des nœuds honnêtes n'influent pas sur le taux de faux positifs, donc il est probable que ces nœuds soient exclus dans des cas où les nœuds malveillants constituent une majorité locale.



	SEDIREP+	LEAVE	SEDIREP-	Crépeau
0	0,00%	0,00%	0,00%	0,00%
50	8,26%	0,59%	8,26%	2,10%
100	78,96%	41,67%	78,96%	54,22%
150	96,76%	90,32%	96,76%	94,20%
200	97,90%	97,54%	97,90%	97,54%
250	97,90%	97,72%	97,90%	97,90%
300	97,90%	97,72%	97,90%	97,72%

Figure 5.6 : Taux de détection des nœuds malveillants (cas 20% de nœuds sont malveillants et seuil=0.25)

La figure 5.6 représente le taux de détection des protocoles sus énoncés avec un scénario de 20% des nœuds du réseau sont malveillants et un seuil égal à 0.25. Nous remarquons que les taux de détection ont augmenté de façon spectaculaire au-delà d'une distance de détection de 50m car, à partir de cette distance les messages d'accusations contre les nœuds malveillants seront en nombre suffisant pour que le taux d'accusation excède le seuil. Nous pouvons remarquer ainsi que la réduction de la valeur du seuil (de 0.5 à 0.25) n'a pas augmenté le taux de détection de la variante de SERIDIP- avec une observabilité optimale (distance de détection de malveillance égale à 300m), ce qui indique que l'opération du filtrage n'a pas une influence négatif sur la détection des nœuds.



	SEDIREP+	LEAVE	SEDIREP-	Crépeau
0	0,01%	24,16%	24,15%	0,43%
50	0,01%	9,12%	24,16%	0,30%
100	0,01%	1,07%	24,16%	0,30%
150	0,01%	0,02%	24,16%	0,30%
200	0,01%	0,00%	24,16%	0,29%
250	0,01%	0,00%	24,16%	0,29%
300	0,01%	0,00%	24,16%	0,29%

Figure 5.7 : Taux de faux positifs (cas 20% de nœuds sont malveillants et seuil=0.25)

La figure 5.7 illustre le taux de faux positifs avec un scénario de 20% des nœuds du réseau sont des nœuds malveillants et un seuil égal à 0.25. Nous remarquons qu'avec le protocole de Crépeau et le protocole SEDIREP+ les taux de faux positifs sont bas, mais avec le protocole LEAVE le taux de faux positifs croît lorsque les distances de détection sont inférieures à 100m, car il y a peu d'accusations contre les nœuds malveillants. Avec SEDIREP- le taux de faux positifs est égal à peu près à 24% quelle que soit la distance de détection de malveillance, car les nœuds malveillants émettent les mêmes accusations indépendamment des capacités de détection des nœuds honnêtes, et dans ce protocole le calcul des taux d'accusation des nœuds dépend seulement des accusations émises contre les nœuds concernés.

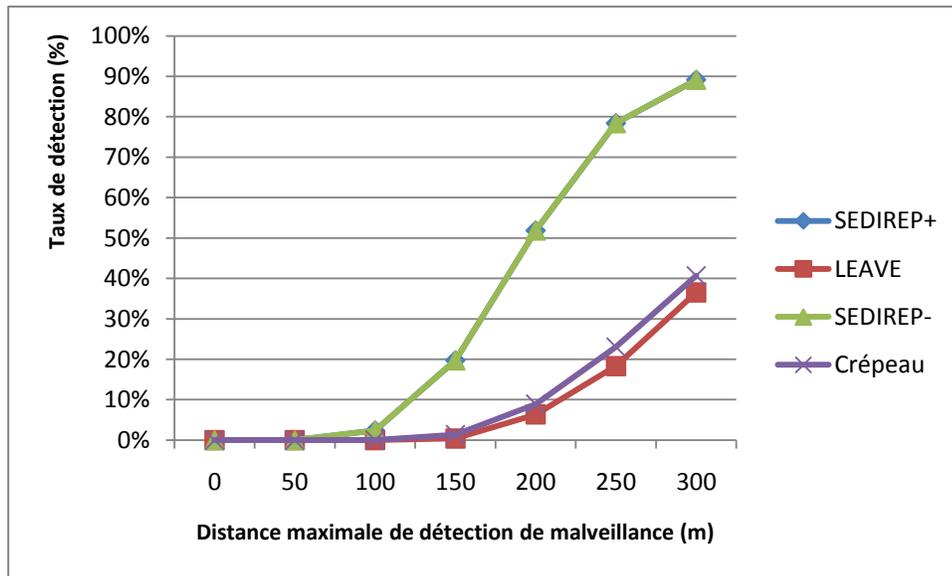
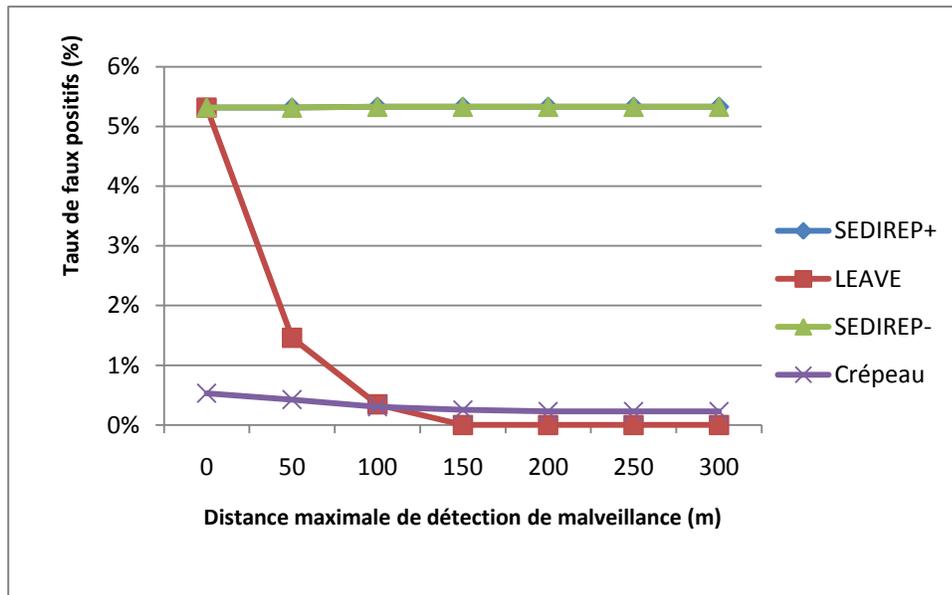


Figure 5.8 : Taux de détection des nœuds malveillants (cas 30% de nœuds sont malveillants et seuil=0.5)

La figure ci-dessus illustre les taux de détection de nœuds malveillants, avec le scénario où 20% des nœuds du réseau sont malveillants et un seuil égale à 0.5. Nous remarquons que les deux variantes de protocole SEDIREP toujours donnent des meilleurs résultats, même en présence du nombre élevé de nœuds malveillants ; tandis que le protocole de Crépeau et le protocole LEAVE ont échoué de détecter la majorité des nœuds malveillants, même dans le cas où l’observabilité est parfaite.



	SEDIREP+	LEAVE	SEDIREP-	Crépeau
0	5,32%	5,32%	5,32%	0,53%
50	5,32%	1,46%	5,32%	0,42%
100	5,33%	0,34%	5,33%	0,30%
150	5,33%	0,00%	5,33%	0,25%
200	5,33%	0,00%	5,33%	0,23%
250	5,33%	0,00%	5,33%	0,23%
300	5,33%	0,00%	5,33%	0,23%

Figure 5.9 : Taux de faux positifs (cas 30% de nœuds sont malveillants et seuil=0.5)

La figure 5.9 illustre le taux de faux positifs avec 30% des nœuds de réseau sont des nœuds malveillants et un seuil égal à 0.5. Nous remarquons que l'augmentation de la proportion des nœuds malveillants dans le réseau a augmenté les taux de faux positifs. Cependant, ces taux peuvent être considérés bas avec les trois protocoles de manière générale.

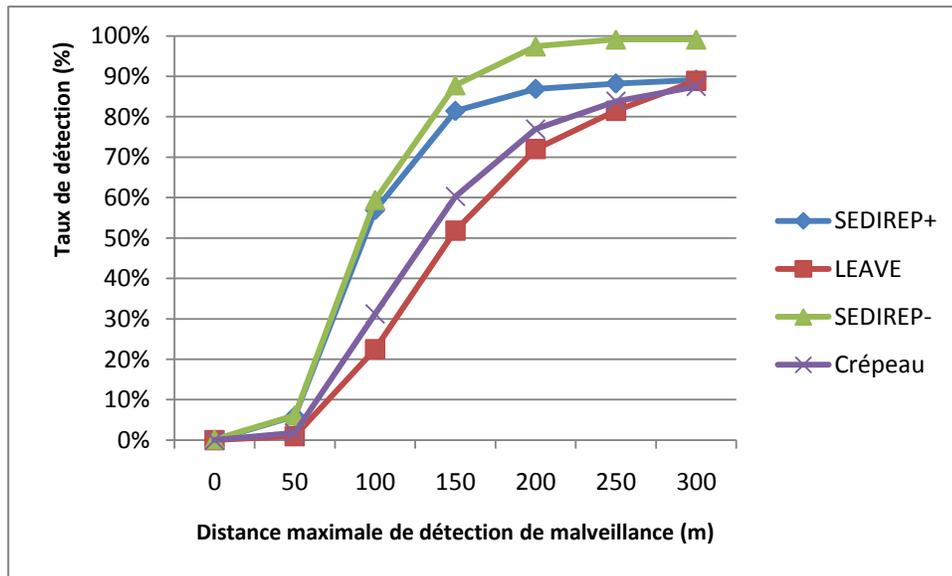


Figure 5.10 : Taux de détection des nœuds malveillants (cas 30% de nœuds sont malveillants et seuil=0.25)

La figure 5.10 représente les taux de détection des protocoles sus énoncés avec le scénario 30% des nœuds sont malveillants et un seuil égal à 0.25. Nous constatons que la variante SEDIREP- présente les meilleurs résultats avec un taux de détection allant jusqu'à 99.12%; tandis que la variante SEDIREP+ présente de meilleures performances que les deux protocoles LEAVE et de Crépeau avec un taux de détection allant jusqu'à 89.12%. A la différence des résultats obtenus dans la figure 5.8 (Taux de détection cas 30% de nœuds sont malveillants et seuil égale à 0.5) SEDIREP+ n'a pas assuré les mêmes taux de détection avec SEDIREP+, car il y a des situations où la proportion des nœuds malveillants voisins d'un nœud honnête dépasse 25%.

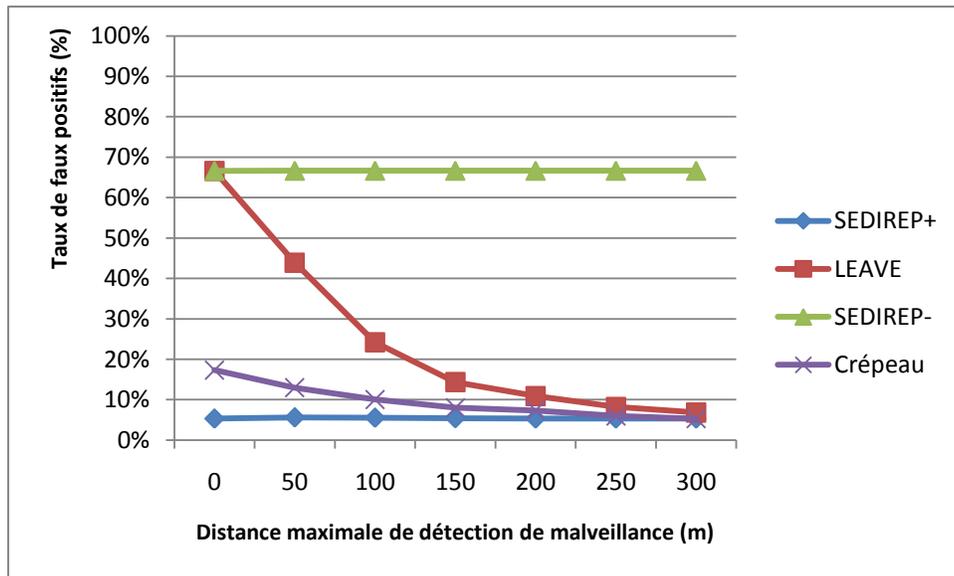


Figure 5.11 : Taux de faux positifs (cas 30% de nœuds sont malveillants et seuil=0.25)

La figure 5.11 illustre le taux de faux positifs avec le scénario 30% des nœuds sont malveillants et un seuil égal à 0.25. Nous remarquons que l’algorithme SEDIREP- présente toujours le pire des cas avec un taux de faux positifs allant jusqu’à 66.64%, tandis que SEDIREP+ assure les plus faibles taux de faux positifs, la distance de détection 50m représente le plus pire des cas avec un taux de 5.61%, car les valeurs de la fonction comportementale globale de nœuds malveillants sont plus grande que celles de certain nombre des nœuds honnêtes. Le protocole de Crépeau présente de meilleures performances que LEAVE notamment lorsque les distances de détection de malveillance sont très courtes, car les nœuds malveillants accusent tous les nœuds honnêtes et ce protocole se base sur la réduction de poids des accusations de nœuds accusateurs.

5.4.3 Analyse de la complexité de l'algorithme utilisé

En ce qui concerne la complexité de l'algorithme de SEDIREP, de LEAVE et celle de Crépeau, elle est de l'ordre de $O(n^2)$, tel que n est le nombre des nœuds voisins à un saut au nœud exécutant le protocole, cette complexité correspond seulement aux situations avec un nombre élevé de nœuds malveillants et une observabilité faible. Tandis que les autres situations la complexité de l'algorithme est de l'ordre $O(n)$. Cependant nous pouvons alléger le temps d'exécution si n est très élevé en choisissant un certain nombre des nœuds aléatoirement afin de construire le graphe d'accusation. Cela va permettre à notre algorithme de prendre place avec les algorithmes connus.

5.5 Conclusion

Dans ce chapitre, nous avons présenté notre protocole de révocation distribuée SEDIREP, il a été conçu pour qu'il s'adapte à un environnement avec une topologie dynamique et fortement contraignante notamment en termes de sécurité et de bande passante. Les résultats de simulation ont montré que SEDIREP a de meilleures performances par rapport aux autres PRD. En effet, la réduction du seuil dans les autres PRD augmente le taux de détection d'une part, et augmente le taux de faux positifs d'une autre part. Cependant, avec un seuil réduit SEDIREP assure un très bon taux de détection tout en minimisant le taux de faux positifs, ce qui permet d'améliorer la sécurité et la disponibilité du réseau.

Conclusion générale et perspectives

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

Les réseaux véhiculaires sont vulnérables aux attaques menaçant la vie des usagers et les biens, et donc la sécurité de ces réseaux est un pré-requis pour leurs déploiements. Les techniques cryptographiques peuvent assurer les objectifs de l’authentification, l’intégrité et la confidentialité dans une certaine mesure, mais la disponibilité est difficile à assurer car l’aspect décentralisé des réseaux VANET donne la possibilité d’avoir plusieurs attaques.

Le service du routage est responsable de l’acheminement des messages entre les véhicules. Ces messages sont souvent acheminés avec un protocole de routage multi-sauts, ce qui donne lieu à la possibilité d’avoir plusieurs types d’attaque.

Outre les techniques cryptographiques, les protocoles de routage sécurisés doivent avoir des mécanismes de détection afin d’éviter les nœuds malveillants et minimiser leurs impacts sur la performance du réseau.

Dans la littérature, les chercheurs souvent proposent l’utilisation des SDI et des systèmes de réputation ; mais, à cause de l’aspect temps réel de certaines applications dans les VANETs, ils ne peuvent pas être utilisés afin de sécuriser le routage.

Les protocoles de révocation distribuée peuvent détecter les nœuds malveillants même avant l’interaction avec eux. Cependant, ils sont vulnérables aux attaques de fausses alertes visant à exclure un nombre important de nœuds honnêtes, et donc la disponibilité du réseau.

Dans ce travail, nous avons proposé un protocole de routage sécurisé adapté à l’environnement véhiculaire, nous avons proposé des améliorations aux protocoles LEAVE et une adaptation de protocole de Crépeau au contexte du VANET afin d’être utilisés conjointement avec les protocoles de routage dans les VANETs. Enfin nous avons aussi proposé un nouveau protocole de révocation distribuée appelé « SEDIREP ». A la différence des autres protocoles, SEDIREP est conçu pour qu’il prenne en considération le cas où les nœuds malveillants sont indétectables, et par conséquent il accepte les alertes seulement lorsqu’il n’y a pas des risques d’avoir un déni de service. Les résultats de simulation montrent que SEDIREP surpasse les autres protocoles de révocation

distribuée. En effet, il assure un taux de détection élevé et minimise le risque d'avoir un déni de service causé par les fausses alertes, même en présence d'un grand nombre des nœuds malveillants en coalition.

Comme extensions futures à notre travail nous proposons :

- L'implémentation du protocole de routage ad hoc sécurisé proposé SAODV modifié+PBR.
- La proposition d'un SDI approprié pour le protocole de routage proposé, et l'application de notre protocole SEDIREP avec eux.
- Simuler notre protocole avec d'autres modèles de mobilité.

Bibliographie

- [1] L. Buttyan and J.-P. Hubaux, *Security and cooperation in wireless networks: Thwarting Malicious and Selfish Behavior*. Cambridge University Press, 2007.
- [2] E. J. Caballero, "Vulnerabilities of Intrusion Detection Systems in Mobile Ad-hoc Networks - The routing problem," in *Seminar on Network Security*, Helsinki, 2006.
- [3] A. Studer, F. Bai, B. Bellur, and A. Perrig, "Flexible, Extensible, and Efficient VANET Authentication," in *Proceedings of the 6th Annual Conference on Embedded Security in Cars (escar 2008)*, 2008.
- [4] B. Liu, J. T. Chiang, and Y.-C. Hu, "Limits on Revocation in VANETs," in *Pre-proceedings of the 8th International Conference on Applied Cryptography and Network Security (ACNS 2010)*, Beijing, China, 2010, pp. 38-52.
- [5] M. Raya, M. H. Manshaei, M. Félegyház, and J.-P. Hubaux, "Revocation Games in Ephemeral Networks," in *ACM Conference on Computer and Communications Security*, 2008, pp. 199-210.
- [6] C. BURGOD, "Contribution à la sécurisation du routage dans les réseaux ad hoc," Université de Limoges Thèse de doctorat, 2009.
- [7] J.-P. Hubaux. (2004, Nov.) The Security and Privacy of Smart Vehicles. Presentation at ZISC Information Security Colloquium.
- [8] M. Burmester, E. Magkos, and V. Chrissikopoulos, "Strengthening Privacy Protection in VANETs," in *IEEE International Conference on Wireless and Mobile Computing, Networking and Communications(WIMOB)*, Avignon, 2008.
- [9] J. Choi, S. Jung, Y. Kim, and M. Yoo, "A Fast and Efficient Handover Authentication Achieving Conditional Privacy in V2I Networks," in *Proceedings of the 9th International Conference on Smart Spaces and Next Generation Wired/Wireless Networking and Second Conference on Smart Spaces*, St. Petersburg, Russia, 2009, pp. 291-300.
- [10] Q. Xu and D. Jiang, "Design and analysis of highway safety communication protocol in 5.9 GHz dedicated short range communication spectrum," *Vehicular Technology Conference, 2003. VTC 2003-Spring. The 57th IEEE Semiannual*, vol. 4, pp. 2451-2455, Apr. 2003.

- [11] J. Santa, A. F. Gómez-Skarmeta, and M. Sánchez-Artigas, "Architecture and evaluation of a unified V2V and V2I communication system based on cellular networks," *Computer Communications*, vol. 31, no. 12, pp. 2850-2861, Jul. 2008.
- [12] M. JERBI, "Protocoles pour les communications dans les réseaux de véhicules en environnement urbain : Routage et GeoCast basés sur les intersections," UNIVERSITE D'EVRY VAL D'ESSONNE thèse de doctorat, 2008.
- [13] X. Zhuo, J. Hao, D. Liu, and Y. Dai, "Removal of misbehaving insiders in anonymous VANETs," in *Proceedings of the 12th ACM international conference on Modeling, analysis and simulation of wireless and mobile systems*, Tenerife, 2009, pp. 106-115.
- [14] M. Fiore, J. Harri, F. Filali, and C. Bonnet, "Vehicular Mobility Simulation for VANETs," in *Proceedings of the 40th Annual Simulation Symposium*, Norfolk, VA , 2007, pp. 301-309.
- [15] S. N. Pathak and U. Shrawankar, "Secured Communication in Real Time VANET," in *Proceedings of the 2009 Second International Conference on Emerging Trends in Engineering & Technology*, Nagpur , 2009, pp. 1151-1155.
- [16] F. Kargl, "Inter-Vehicular Communication," Ulm University Habilitation Thesis, 2008.
- [17] C. TCHEPNDA, "Authentification dans les Réseaux Véhiculaires Opérés," Ecole Nationale Supérieure des Télécommunications Thèse de doctorat, 2008.
- [18] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, vol. 15, p. 39-68, 2007.
- [19] A. Burg, "Ad hoc network specific attacks," in *Seminar Ad hoc networking: concepts, applications, and security*, Technische Universität München, 2003.
- [20] A. Yger and J.-A. Weil, *Mathématiques appliquées L3*, P. Education, Ed. 2009.
- [21] http://fr.wikipedia.org/wiki/Infrastructure_à_clés_publicques. consulté le : 22/02/2010.
- [22] S. Mahajan and A. Jindal, "Security and Privacy in VANET to reduce Authentication Overhead for Rapid Roaming Networks," *International Journal of Computer Applications*, vol. 1, no. 20, 2010.
- [23] P. Papadimitratos, et al., "Secure Vehicular Communication Systems: Design and Architecture," *IEEE Communication Magazine*, vol. 46, no. 11, pp. 100-109, Nov. 2008.
- [24] E. Schoch, F. Kargl, T. Leinmüller, S. Schlott, and P. Papadimitratos, "Impact of Pseudonym Changes on Geographic Routing in VANETs," in *Third European workshop, ESAS 2006*, Hamburg, 2006, pp. 43-57.

- [25] P. Ning and S. Jajodia, "Intrusion detection techniques," in *The Internet Encyclopedia*, J. W. & Sons, Ed. hobokenon, New Jersey, USA, 2006, pp. 355-367.
- [26] Y. Li, N. Wu, S. Wang, and S. Jajodia, "Enhancing profiles for anomaly detection using time granularities," *Journal of Computer Security*, vol. 10, pp. 137-157, 2002.
- [27] S. Kumar, "Classification and detection of computer intrusions," PhD thesis, Purdue University, 1995.
- [28] D. E. DENNING, "An intrusion-detection model," *IEEE TRANSACTIONS ON SOFTWARE ENGINEERING*, vol. SE-13, no. 2, pp. 222-232, Feb. 1987.
- [29] F. Kargl, Z. Ma, and E. Schoch, "Security Engineering for VANETs," in *proceedings of the Workshop on Embedded Security in Cars (ESCAR) 2006*, Berlin, Germany, 2006.
- [30] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J. -P. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks," *IEEE Journal on Selected Areas in Communication*, vol. 25, no. 8, p. 155768, M. Raya, P. Papadimitratos, I. Aad, D. Jungels, J.-P. Hubaux, 2007.
- [31] J. Hu, "Cooperation in Mobile Ad Hoc Networks," Computer Science Department, Florida State University, Technical report, 2005.
- [32] A. Trivedi, et al., "Ad Hoc Networks: Vulnerabilities and Issues in Intrusion Detection," in *Encyclopedia of Information Science and Technology*, 2006.
- [33] F. Anjum and P. Mouchtaris, *Security for Wireless Ad Hoc Networks*, Wiley-Interscience, Ed. 2007.
- [34] S. Buchegger and J.-Y. Le Boudec, "Performance analysis of the CONFIDANT," in *Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing*, Lausanne, Switzerland , 2002, pp. 226-236.
- [35] P. Michiardi and R. Molva, "A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in *Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security*, 2002, pp. 107-121.
- [36] S. Bansal and M. Baker, "Observation-based Cooperation Enforcement in Ad Hoc Networks," Stanford University, Technical report 0307012, 2003.
- [37] L. K. Qabajeh, L. M. Kiah, and M. M. Qabajeh, "A qualitative comparison of position-based routing protocols for ad-Hoc networks," *International Journal of Computer Science and Network Security*, vol. 9, no. 2, pp. 131-140, Feb. 2009.
- [38] A. G. DLUDLA, N. NTLATLAPA, T. Nyandeni, and M. ADIGUN, "Towards designing energy-efficient

- routing protocol for wireless mesh networks," in *Southern Africa Telecommunication Networks and Applications Conference (SATNAC 2009)*, Swaziland, 2009.
- [39] L. K. Qabajeh, L. M. Kiah, and M. M. Qabajeh, "A scalable and secure position-based routing protocol for ad-hoc networks," *Malaysian Journal of Computer Science*, vol. 22, no. 2, pp. 99-120, 2009.
- [40] C. Perkins, E. M. Royer, and S. Das, "Ad Hoc on-demand distance vector (AODV) routing," *IETF internet draft (work in progress), Internet Engineering Task Force*, 2002.
- [41] D. Johnson, D. Maltz, Y. Hu, and J. Jetcheva, "The dynamic source routing protocol for mobile Ad Hoc networks," *IETF internet draft Internet Engineering Task Force*, 2002.
- [42] V. Park and M. S. Corson, "Temporally-ordered routing algorithm," *IETF MANET Working Group Internet Draft*, 2000.
- [43] P. Jacquet and T. Clausen, "Optimized link state routing protocol (OLSR)," *RFC 3626*, 2003.
- [44] C. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers," *ACM SIGCOMM Computer Communication Review*, vol. 24, no. 4, pp. 234-244, Oct. 1994.
- [45] Z. Haas, M. Pearlman, and P. Samar, "The zone routing protocol (zrp) for Ad Hoc networks," *Internet Draft: draft-ietf-manet-zone-zrp-04.txt*, 2002.
- [46] S. C. a. A. Yasinsac, S. Carter, and A. Yasinsac, "Secure position aided ad hoc routing," in *Proceedings of The IASTED International Conference on Communications and Computer Networks(CCN02)*, Cambridge, 2002, pp. 329-334.
- [47] E. AMAR and S. Boumerdassi, "A location service for position-based routing in mobile ad hoc networks," in *Proceedings of the 8th international conference on New technologies in distributed systems*, Lyon, France , 2008.
- [48] Y.-B. Ko and N. H. Vaidya, "Location-aided routing (LAR) in mobile Ad Hoc," in *Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking*, Dallas, Texas, United States, 1998, pp. 66-75.
- [49] S. Basagni, I. Chlamtac, V. R. Syrotiuk, and B. A. Woodward, "A distance routing effect algorithm for mobility (DREAM)," in *Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking*, Dallas, Texas, United States, 1998, pp. 76-84.
- [50] B. Karp and H. T. Kung, "GPSR: Greedy perimeter stateless routing for wireless networks," in *Proceedings of the 6th annual international conference on Mobile computing and networking*, Boston,

- Massachusetts, United States, 2000, pp. 243-254.
- [51] M. N. Lima, H. W. da Silva, A. L. dos Santos, and G. Pujolle, "A Security Management Architecture for Supporting Routing Services on WANETs," Federal University of Parana, Curitiba, Parana, Brazil, Technical Report, 2010.
- [52] E. Fonseca and A. Festag, "A Survey of Existing Approaches for Secure Ad Hoc Routing and Their Applicability to VANETS," NEC Network Laboratories, Technical Report, 2006.
- [53] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Rushing attacks and defense in wireless ad Hoc network routing protocols," in *Proceedings of the 2nd ACM workshop on Wireless security*, San Diego, CA, USA, 2003, pp. 30-40.
- [54] P. Papadimitratos and Z. Haas, "Secure routing for mobile ad hoc networks," in *Proceedings of the SCS communication networks and distributed systems modeling and simulation conference (CNDS 2002)*, San Antonio, USA, 2002.
- [55] Y.-C. Hu, A. Perrig, and D. B. Johnson, "ARIADNE: A secure on-demand routing protocol for ad hoc networks," in *Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking (MobiCom 2002)*, Atlanta, Georgia, USA, 2002, pp. 12-23.
- [56] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "Efficient Authentication and Signing Multicasts Streams over Lossy Channels," in *IEEE Symposium on Security and Privacy*, Berkeley, CA , USA, 2000, pp. 56-73.
- [57] M. G. Zapata and N. Asokan, "Securing ad hoc routing protocols," in *Proceedings of the 1st ACM workshop on Wireless security*, Atlanta, GA, USA , 2002, pp. 1-10.
- [58] S. Carter and A. Yasinsac, "Secure position aided ad hoc routing," in *Proceedings of The IASTED International Conference on Communications and Computer Networks*, 2002, pp. 329-334.
- [59] T. Leinmüller, E. Schoch, F. Kargl, and C. Maihöfe, "Influence of falsified position data on geographic ad-hoc routing," *Lecture notes in computer science*, 2005.
- [60] S. Marti, K. Lai, and T. J. Giuli, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proceedings of the 6th annual international conference on Mobile computing and networking*, Boston, Massachusetts, United States , 2000, pp. 255-265.
- [61] H. ABIOD, *Réseaux mobiles ad hoc et réseaux de capteurs sans fil*. 2006.
- [62] L. Buttyan, T. Holczer, A. Weimerskirch, and W. Whyte, "SLOW: A Practical pseudonym changing scheme for location privacy in VANETs," in *IEEE Vehicular Networking Conference (VNC)*, Tokyo, Japan , , 2009.

- [63] V. Naumov, R. Baumann, and T. Gross, "An evaluation of inter-vehicle ad hoc networks based on realistic vehicular traces," in *Proceedings of the 7th ACM international symposium on Mobile ad hoc networking and computing*, Florence, Italy, 2006, pp. 108-119.
- [64] S.-Y. Ni, Y.-C. Tseng, Y.-S. Chen, and J.-P. Sheu, "The broadcast storm problem in a mobile ad hoc network," in *Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking*, Seattle, Washington, United States, 1999, pp. 151-162.
- [65] K. C. Lee, U. Lee, and M. Gerla, "Survey of Routing Protocols in Vehicular Ad Hoc Networks," in *Advances in Vehicular Ad-Hoc Networks: Developments and Challenges*, IGI Global, I. S. Reference, Ed. 2010, ch. 8, pp. 149-170.
- [66] V. Naumov and T. R. Gross, "Connectivity-Aware Routing (CAR) in Vehicular Ad-hoc Networks," in *INFOCOM 2007. 26th IEEE International Conference on Computer Communications*, Anchorage, AK , 2007, pp. 1919-1927.
- [67] T. Moore, "Cooperative attack and defense in distributed networks," University of Cambridge, Cambridge, Technical Report ISSN 1476-2986, 2008.
- [68] D. S. Kim, M. G. Sadi, and J. S. Park, "A Key Revocation Scheme for Mobile Sensor Networks," in *International Workshop on Security and Survivability in Distributed Sensor Networks*, Niagara Falls, Ontario, Canada, 2007.
- [69] H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks," *IEEE Symposium on Security and Privacy (S&P)*, pp. 197-213, 2003.
- [70] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, 1979.
- [71] J. Clulow and T. Moore, "Suicide for the common good: a new strategy for credential revocation in self-organizing systems," *ACM SIGOPS Operating Systems Review*, vol. 40, no. 3, pp. 18-21, 2006.
- [72] C. Crépeau and C. R. Davis, "A certificate revocation scheme for wireless ad hoc networks," in *Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks*, Fairfax, Virginia, 2003, pp. 54-61.
- [73] J. Luo and J.-P. Hubaux, "A Survey of Inter-Vehicle Communication," School of Computer and Communication Sciences, EPFL, Lausanne, Switzerland, Technical Report IC, 2004.
- [74] J. Choi, Y. Khaled, M. Tsukada, and T. Ernst, "IPv6 support for VANET with geographical routing," *8th International Conference on Intelligent Transport System Telecommunicaitons*, Oct. 2008.
- [75] J.-H. Song, V. W. S. Wong, and V. C. M. Leung, "Secure Location Verification for Vehicular Ad-Hoc

- Networks," in *IEEE Global Communications Conference, (Globecom)*, New Orleans, LO, 2008, pp. 1-5.
- [76] S. Capkun and M. Cagalj, "Secure Location Verification with Hidden and Mobile Base Stations," *IEEE TRANSACTIONS ON MOBILE COMPUTING*, vol. 7, no. 4, Apr. 2008.
- [77] L. Lazos and R. Poovendran, "Secure Localization for Wireless Sensor Networks using Range-Independent Methods," in *Secure Localization and Time Synchronization for Wireless Sensor and Ad Hoc Networks*. USA: Springer, 2007, pp. 185-214.
- [78] T. Leinmüller, E. Schoch, F. Kargl, and C. Maihofer, "Decentralized position verification in geographic ad hoc routing," *Security and Communication Networks*, Wiley and Sons, 2008.
- [79] T. Issariyakul and E. Hossain, *Introduction to Network Simulator NS2*, 1^èèth ed. New York, USA: Springer, 2008.
- [80] The ns Manual, <http://www.isi.edu/nsnam/ns/ns-documentation.html>. consulté le : 14/04/2010.
- [81] NS by Example, <http://nile.wpi.edu/NS/>. consulté le : 14/04/2010.
- [82] F. Bai, N. Sadagopan, and A. Helmy. (2004,) User Manual for IMPORTANT Mobility Tool Generators in ns-2 Simulator. Document.
- [83] <http://nile.cise.ufl.edu/important/software.htm>. consulté le : 20/04/2010.

Annexe

Calcul de taux d'accusation avec SEDIREP

Dans cette partie, nous voulons montrer comment SEDIREP exclut les nœuds malveillants, et pour cela nous avons envisagé le graphe d'accusation illustré dans la figure 6.1.

A la différence de tous les PRD précédents, nous remarquons que seulement les nœuds 0,1,2 et 3 qui sont exclus par SEDIREP avec un seuil égal à 0.25. En effet, analytiquement, ces nœuds sont suspects d'être des nœuds malveillants en coalition, car ils ont à peu près le même comportement d'accusation ; ainsi, si on suppose que la majorité des nœuds sont honnêtes, alors il est clair que l'ensemble des nœuds 4,5,6 et 7 et l'ensemble des nœuds 9,10 et 11 ne sont pas en coalition avec 0,1,2 et 3 comme le comportement d'accusation le montre.

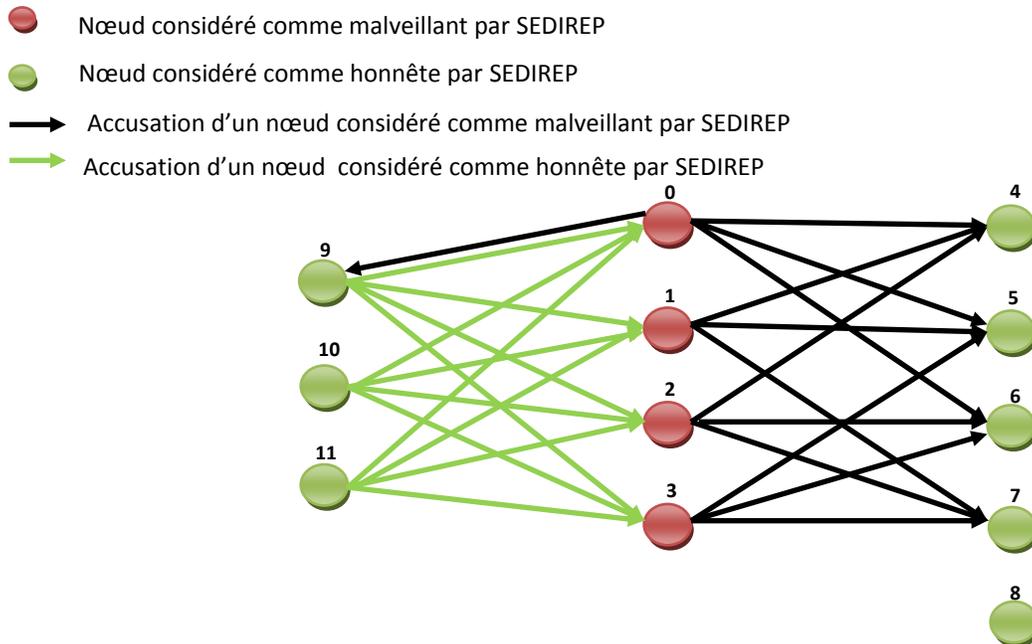


Figure 6.1 : Exemple illustrant les nœuds exclus par SEDIREP

Les valeurs de différentes fonctions de SEDIREP utilisées pour l'exclusion des nœuds dans la figure précédente sont présentées dans les tableaux ci-dessous.

Voici la matrice A modélisant le graphe d'accusation précédent :

	0	1	2	3	4	5	6	7	8	9	10	11
0	0	0	0	0	1	1	1	0	0	1	0	0
1	0	0	0	0	1	1	0	1	0	0	0	0
2	0	0	0	0	1	0	1	1	0	0	0	0
3	0	0	0	0	0	1	1	1	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0
9	1	1	1	1	0	0	0	0	0	0	0	0
10	1	1	1	1	0	0	0	0	0	0	0	0
11	1	1	1	1	0	0	0	0	0	0	0	0

Le tableau suivant illustre les valeurs de fonction comportementale entre chaque paire de nœuds, ainsi la fonction comportementale globale de chacun entre eux :

x	0	1	2	3	4	5	6	7	8	9	10	11	$f_{cg}(x)$
0	0	9	9	9	8	8	8	8	8	4	4	4	$79/12=6,58$
1	9	0	10	10	9	9	9	9	9	5	5	5	$89/12=7,42$
2	9	10	0	10	9	9	9	9	9	5	5	5	$89/12=7,42$
3	9	10	10	0	9	9	9	9	9	5	5	5	$89/12=7,42$
4	8	9	9	9	0	12	12	12	12	8	8	8	$107/12=8,92$
5	8	9	9	9	12	0	12	12	12	8	8	8	$107/12=8,92$
6	8	9	9	9	12	12	0	12	12	8	8	8	$107/12=8,92$
7	8	9	9	9	12	12	12	0	12	8	8	8	$107/12=8,92$
8	8	9	9	9	12	12	12	12	0	8	8	8	$107/12=8,92$
9	4	5	5	5	8	8	8	8	8	0	12	12	$83/12=6,92$
10	4	5	5	5	8	8	8	8	8	12	0	12	$83/12=6,92$
11	4	5	5	5	8	8	8	8	8	12	12	0	$83/12=6,92$

Le tableau suivant illustre la matrice transposé A' :

	0	1	2	3	4	5	6	7	8	9	10	11
0	0	0	0	0	0	0	0	0	0	1	1	1
1	0	0	0	0	0	0	0	0	0	1	1	1
2	0	0	0	0	0	0	0	0	0	1	1	1
3	0	0	0	0	0	0	0	0	0	1	1	1
4	1	1	1	0	0	0	0	0	0	0	0	0
5	1	1	0	1	0	0	0	0	0	0	0	0
6	1	0	1	1	0	0	0	0	0	0	0	0
7	0	1	1	1	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0
9	1	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0

Le tableau suivant illustre les valeurs de fonction d'état entre chaque paire de nœuds, ainsi la valeur de la fonction d'état globale de chacun entre eux :

x	0	1	2	3	4	5	6	7	8	9	10	11	$f_{eg}(x)$
0	0	12	12	12	6	6	6	6	9	8	9	9	$95/12=7,92$
1	12	0	12	12	6	6	6	6	9	8	9	9	$95/12=7,92$
2	12	12	0	12	6	6	6	6	9	8	9	9	$95/12=7,92$
3	12	12	12	0	6	6	6	6	9	8	9	9	$95/12=7,92$
4	6	6	6	6	0	10	10	10	9	10	9	9	$91/12=7,58$
5	6	6	6	6	10	0	10	10	9	10	9	9	$91/12=7,58$
6	6	6	6	6	10	10	0	10	9	10	9	9	$91/12=7,58$
7	6	6	6	6	10	10	10	0	9	8	9	9	$89/12=7,42$
8	9	9	9	9	9	9	9	9	0	11	12	12	$107/12=8,92$
9	8	8	8	8	10	10	10	8	11	0	11	11	$103/12=8,58$
10	9	9	9	9	9	9	9	9	12	11	0	12	$107/12=8,92$
11	9	9	9	9	9	9	9	9	12	11	12	0	$107/12=8,92$

X	$f_{cg}(x)$	$f_{eg}(x)$	$f_{cr}(x)$	Liste des accusateurs	Liste des accusateurs après le filtrage	Nombre de voisins	Taux d'accusation	Seuil	x est exclu ?
0	6,58	7,92	14,5	{9,10,11}	{9,10,11}	12	0,25	0,25	OUI
1	7,42	7,92	15,34	{9,10,11}	{9,10,11}	12	0,25	0,25	OUI
2	7,42	7,92	15,34	{9,10,11}	{9,10,11}	12	0,25	0,25	OUI
3	7,42	7,92	15,34	{9,10,11}	{9,10,11}	12	0,25	0,25	OUI
4	8,92	7,58	16,5	{0,1,2,3}	{0,1,2,3}	12	0	0,25	NON
5	8,92	7,58	16,5	{0,1,2,3}	{}	12	0	0,25	NON
6	8,92	7,58	16,5	{0,1,2,3}	{}	12	0	0,25	NON
7	8,92	7,42	16,34	{0,1,2,3}	{}	12	0	0,25	NON
8	8,92	8,92	17,84	{}	{}	12	0	0,25	NON
9	6,92	8,58	15,5	{}	{}	12	0	0,25	NON
10	6,92	8,92	15,84	{}	{}	12	0	0,25	NON
11	6,92	8,92	15,84	{}	{}	12	0	0,25	NON

Table 5 : Illustration des valeurs de différentes fonctions de SEDIREP

Glossaire

AC Autorité de Certification

AODV Ad hoc On Demand Distance Vector

CAR Connectivity-Aware Routing

DSDV Destination-Sequenced Distance Vector

DoS Denial of Service

DREAM Distance Routing Effect Algorithm for Mobility

DSR Dynamic Source Routing

GPSR Greedy Perimeter Stateless Routing

HSM Hardware Security Module

LAR Location-Aided Routing

LEAVE Local Eviction of Attackers by Voting Evaluators

LRC Liste de Révocation de Certificats

MAC Message Authentication Code

MANET Mobile Ad-hoc NETWORKs

OLSR Optimized Link State Routing

P2P Peer-to-Peer

PGB Preferred Group Broadcasting

PKI Public Key Infrastructure

PRD Protocole de Révocation Distribuée

SAODV Secure Ad hoc On-Demand Distance Vector

SEDIREP SEcure DIstributed REvocation Protocol

SDI Systèmes de Détection d’Intrusion

SPAAR Secure Position Aided Ad hoc Routing

SRP Secure Routing Protocol

STI Système de Transport Intelligent

TORA Temporally-Ordered Routing Algorithm

TPD Tamper-Proof Device

V2I Véhicule-à-Infrastructure

V2V Véhicule-à-Véhicule

VANET Vehicular Ad-Hoc Network

ZRP Zone Routing Protocol