



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

## 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