

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE HOUARI  
BOUMEDIENE (U.S.T.H.B)

Faculté d'Electronique et d'Informatique



## MEMOIRE

Présenté pour l'obtention du diplôme de MAGISTER

En INFORMATIQUE

*Option : Informatique Mobile*

*Par : M<sup>elle</sup> MEKLICHE Kenza*

# *Les attaques Sybil dans les réseaux véhiculaires*

Jury

ZAFOUNE Y.

MC. A

Président

MOUSSAOUI S.

MC. A

Directrice de mémoire

NOUALI N.

M/R

Examinatrice

KHEROUA L.

MA. A

Invitée

## Table des matières

Table des Figures	vii
Table des tableaux	ix
Remerciements	x
Résumé	xi
Introduction générale	1
Chapitre 1 : Les Réseaux Véhiculaires	5
1. Introduction	6
2. Réseaux Mobiles Ad hoc (MANETs)	6
2.1. Caractéristiques des MANETs	6
2.2. Applications MANET	7
3. Réseaux Véhiculaire Ad hoc (VANETs)	7
3.1. Définition	7
3.2. Types de communications	10
3.2.1. Communication véhicule à véhicule (V2V)	10
3.2.2. Communication véhicule à infrastructure ou infrastructure à véhicule (V2I/I2V)	10
3.3. Caractéristiques	10
3.2.1. Topologie du réseau dynamique	10
3.2.2. Partitionnement du réseau	10
3.2.3. Modèle de mobilité	10
3.2.4. Modèle de propagation	11
3.2.5. Energie et stockage illimités	11
3.3. Taxonomie des applications dans les réseaux véhiculaires	11
3.3.1. Applications de sécurité routière	11
3.3.2. Applications de confort	12
4. Technologies d'accès dans les VANETs	12
4.1. Standard IEEE 802.11p	12
4.2. Dedicated Short Range Communication (DSRC)	14
5. Routage dans les VANETs	15
5.1. Protocoles de routage basé topologie	17
5.1.1. Protocoles proactifs	17

5.1.2. Protocoles réactifs	18
5.2. Protocoles de routage Géographique	19
5.2.1. Protocoles de réseaux non tolérants aux délais (non DTN)	20
5.2.2. Protocoles de réseaux tolérants aux délais (DTN)	21
5.2.3. Protocoles hybrides	23
6. Consortiums et projets récents	23
7. Conclusion	25
Chapitre 2 : Sécurité des réseaux véhiculaires	26
1. Introduction	27
2. Sécurité	27
2.1. Authentification	28
2.2. Intégrité	28
2.3. Confidentialité et anonymat	28
2.4. Non répudiation	28
2.5. Vérification de cohérence des données	28
2.6. Disponibilité	29
2.7. Minimum overhead	29
2.8. Contrôle d'accès	29
2.9. Contraintes de temps réel	30
3. Types d'attaques dans les réseaux véhiculaires	30
3.1. Attaques basiques	30
3.1.1. Fausses informations	30
3.1.2. Falsification des informations des capteurs	31
3.1.3. Divulgateion d'ID	31
3.1.4. Déni de services	31
3.1.5. Masquerading	32
3.2. Attaques sophistiquées	32
3.2.1. Véhicule caché	32
3.2.2. Tunnel	32
3.2.3. Wormhole (trou de ver)	33
3.2.4. Bush telegraph	34

3.2.5. Attaque Sybil	34
4. Conclusion	34
Chapitre 3 : Méthodes & Protocoles de sécurité	35
1. Introduction	36
2. Méthodes et techniques de sécurité dans les VANETs	36
2.1. Protocole de détection des attaques Sybil	36
2.1.1. Modèle d'environnement	36
2.1.2. Solution proposée	37
2.2. Protocole P-SRLD	41
2.2.1. Modèle d'environnement	41
2.2.2. Solution proposée	42
2.3. Protocole de sécurité basé sur la détection active de position	46
2.3.1. Modèle d'environnement	46
2.3.2. Solution proposée	47
2.4. Protocole P <sup>2</sup> DAP	50
2.4.1. Modèle d'environnement	50
2.4.2. Solution proposée	50
2.5. Protocole timestamp series	53
2.5.1. Modèle d'environnement	53
2.5.2. Solution proposée	54
2.6. Mécanisme de défense contre les attaques Sybil	55
2.6.1. Modèle d'environnement	55
2.6.2. Solution proposée	55
2.7. Protocole de détection et de localisation des nœuds Sybil	57
2.7.1. Modèle d'environnement	57
2.7.2. Solution proposée	57
2.8. Protocole TACK	60
2.8.1. Modèle d'environnement	60
2.8.2. Solution	60
3. Synthèse	61
4. Conclusion	66

Chapitre 4 : Protocoles de détection d'attaques Sybil dans les VANETs	67
1. Introduction	68
2. Environnement du système	68
2.1. Architecture VANET	68
2.2. Modèle d'adversaire	68
3. Motivations	69
4. Protocole Location-based Privacy Preserving Detection of Sybil Attack	69
4.1. Initialisation	69
4.2. Détection des attaques au niveau du RSU	70
4.2.1. Etape d'écoute et de détection préliminaire	70
4.2.2. Etape de vérification des suspicions d'attaques	71
4.3. Vérification du DMV	72
4.4. Discussion	73
5. Protocole Historic-based Privacy Preserving Detection of Sybil attack	73
5.1. Environnement du système	73
5.1.1. Architecture VANET	73
5.1.2. Modèle d'adversaire	74
5.2. Mécanisme de détection H-P2DSA	74
5.2.1. Initialisation	74
5.2.2. Détection des attaques au niveau du RSU	74
5.2.3. Vérification du DMV	78
6. Conclusion	78
Chapitre 5 : Test de Simulation et Analyse des performances	79
Analyse de performance du protocole L-P2DSA	80
1. Simulation	80
1.1. Environnement de simulation	80
1.2. Métriques et paramètres de simulation	81
2. Résultats et discussion	81
3. Conclusion	88
Conclusion générale et perspectives	89
Perspectives	90



## Résumé

Les réseaux véhiculaires (VANET pour Vehicular Ad hoc NETwork) sont des réseaux constitués de véhicules et d'infrastructures appelés communément nœuds.

Créés initialement pour répondre à un souci de sécurité routière, les VANETs offrent aujourd'hui différents services aux utilisateurs tels que les services d'info-traffic en temps réel ou de localisation de service.

Cette évolution des fonctionnalités a permis de mettre en évidence certaines vulnérabilités liées à la sécurité. Ces vulnérabilités peuvent être exploitées par un certain nombre d'attaques telles que les attaques Sybil qui peuvent avoir de très graves conséquences sur le fonctionnement et l'intégrité de ces réseaux. Ces menaces ont poussé les chercheurs à mettre en place un certain nombre de protocoles de sécurité permettant la détection ou la prévention de ces attaques.

C'est dans ce contexte que s'insèrent les travaux de cette thèse qui étudie les différents protocoles de sécurité permettant la détection ou la prévention des attaques Sybil dans les réseaux véhiculaires.

Cette étude permettra de proposer deux protocoles de détection des attaques Sybil utilisant les infrastructures routières nommé L-P2DSA (Location based Privacy Preserving Detection of Sybil Attacks) et H-P2DSA (Historic-based Privacy Preserving Detection of Sybil Attacks). Nos propositions (L-P2DSA et H-P2DSA) introduisent un filtre supplémentaire au niveau des infrastructures (RSUs) permettant de diminuer la charge sur l'autorité centrale en alliant la vérification des pseudonymes des véhicules à la vérification de la position des nœuds pour L-P2DSA, ou la vérification des pseudonymes à la cohérences de l'historique du mouvement des nœuds pour H-P2DSA. Les résultats de simulation de L-P2DSA montrent un taux de détection élevé et un faible taux de faux positifs.

Mots clés : Attaque Sybil, VANET, degré de distinction, sécurité, anonymat.