UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE HOUARI BOUMEDIENE (USTHB)

FACULTE D'ELECTRONIQUE ET D'INFORMATIQUE

MÉMOIRE

Présenté pour l'obtention du grade de:

MAGISTER

Filière: Informatique

Option: Systèmes Informatiques et Ingénierie des Logiciels

Réalisée Par:

Mr. HARBOUCHE Oussama

Sujet:

DÉTECTION ET ÉLIMINATION DES NŒUDS MALICIEUX DANS UN VANET (VEHICULAR AD-HOC NETWORK)

Membres du jury :

Mme M. BOUKALA	**Prof à l'USTHB**	**Présidente**
Mme S. MOUSSAOUI	**M.C/A à l'USTHB**	**Directrice de mémoire**
Mme N. NOUALI	**Maitre de recherche au CERIST**	**Examinatrice**
Mr M. BENCHAIBA	**M.C/A à l'USTHB**	**Examinateur**

2011-2012

Résumé

Notre travail consiste en la conception d'une nouvelle technique de détection et d'élimination des nœuds malicieux pour les réseaux véhiculaires qui répond aux défis imposés par la nature des applications véhiculaires. Notre objectif est double: (a) optimiser les paramètres de sécurité de ces réseaux et (b) améliorer les performances des applications de sécurités pour ces réseaux.

Pour se faire, nous avons étudié dans un premier temps les approches proposées dans ce domaine pour les réseaux véhiculaires. Ces solutions ont étés analysées et critiquées. Elles nous ont permis de concevoir, dans un second temps, un nouveau protocole plus adapté.

Notre contribution a été d'apporter une amélioration aux mécanismes de détection des nœuds malicieux et de compléter les solutions existantes par un outil efficace d'élimination de noeuds malicieux.

Les simulations effectuées ont permis de montrer l'efficacité de notre solution par rapport aux solutions existantes par rapport aux paramètres de performances et de sécurité visés.

Mots clés: VANETs, Sécurité, Détection de nœuds malicieux, Algorithmes distribués, modèles de mobilité.

Abstract

Our work proposes the design of a new method of detection and elimination of the malicious nodes on the vehicular networks. This solution is an answer to the challenges imposed by the nature of the vehicular applications. Our objective is double: (a) to optimize security settings of these networks and (b) to improve the application performances of safety measures for these networks.

To be done, we initially studied the approaches suggested in this field for the vehicular networks. These solutions enabled us to design, in the second time, a new protocol.

Our contribution is an improvement of the detection mechanisms of the malicious nodes and proposes an effective tool for their elimination.

The simulations show the effectiveness of our solution compared to the existing solutions by referring to the parameters of performances and security concerned.

Key words: VANETs, Security, Malicious node detection, distributed Algorithms, mobility models.

Table des matières

Chapitre1 :Définition et caractéristiques 3

1 Introduction 4

2 Réseau véhiculaire: définition 5

3 Architectures et caractéristiques des réseaux de véhicules 6

3.1 Architectures des réseaux véhiculaires 6

3.2 Scénarios possibles de déploiement pour les réseaux véhiculaires 8

3.3 Caractéristiques des réseaux véhiculaires 9

3.4 Environnements routiers 10

4 Applications des réseaux véhiculaires 11

4.1 Applications de sécurité (safety-related) 11

4.2 Applications de confort (comfort-related) 11

5 Technologies d'accès dans les VANETs 12

5.1 Caractéristiques du MAC VANET 13

5.2 Technologies d'accès véhiculaires 14

5.3 Histoire de standardisation du WAVE 16

5.4 Fonctionnement de WAVE et du protocole MAC 17

5.5 MAC P1609.4/IEEE 802.11p 18

6 Projets existants 19

6.1 USA: Vehicle-Infrastructure Integration (VII) 20

6.2 Europe: European Commission's Cooperative Vehicle-Infrastructure System (CVIS) 20

6.3 Japon: SmartWay 21

7 Conclusion 21

Chapitre2: Sécurité des VANETs 23

1 Introduction 24

2 Caractéristiques applicatives 25

3 Attaques dans les réseaux véhiculaires 26

3.1 Taxonomie des attaques 26

3.2 Exemples d'attaques 27

3.3 Exigences et défis de sécurité 31

4 Solutions et contributions 36
5 Discussion 38
6 Conclusion 39
Chapitre3:Détection Et Elimination Des Nœuds Malicieux Dans Un VANET 41
1 Introduction 42
2 Détection Des Nœuds Malicieux 43
2.1 Solution de Philippe Golle et al(2004) 43
2.1.1 Modèle d'environnement 44
2.1.2 Exemple 46
2.2 Solution de Bin Xiao et al(2006) 50
2.2.1 Modèle d'environnement 51
2.2.2 Solution 53
2.2.3 Technique d'élimination des témoins Sybil 55
2.3 Solution de Jonathan Van Eenwyk (2007) 57
2.3.1 Modèle D'environnement 57
2.3.2 Solution 58
2.4 Solution de Soyoung Park et al.(2009) 62
2.4.1 Modèle D'environnement 62
2.4.2 Solution 63
2.5 Discussion 65
3 Elimination des nœuds malicieux 66
3.1 Environnement de travail 67
3.1.1 Model du système 67
3.1.2 Modèle d'attaque 68
3.2 LEAVE 69
3.3 Stinger 70
3.4 Discussion 75
4 Conclusion 76
Chapitre4:Une Nouvelle Solution Pour La Détection Et L'élimination des Nœuds Malicieux Dans Un VANET 77
1 Introduction 78
2 Modèle d'environnement 79

2.1 Modèle du système 79
2.2 Modèle d'attaque 81
3 Détection de nœuds malicieux 82
3.1 Paramètres de synchronisation 83
3.2 Construction modèle 84
4 S-LEAVE (Stinged-LEAVE) 87
4.1 Les structures utilisées 89
4.2 Les messages utilisés 90
4.3 Les fonctions utilisées 90
5 CONCLUSION 94
Chapitre5:Évaluation des Performances de S-LEAVE 95
1 Introduction 96
2 Les techniques d'évaluation des performances: 96
2.1 La mesure (émulation): 97
2.2 La modélisation: 97
2.3 La simulation: 97
3 Environnement de simulation: 97
3.1 Le Network Simulator NS2: 98
3.1.1 Les modèles de mobilité sous NS2 [03]: 99
3.1.2 Le langage TCL/OTCL: 100
3.2 Générateurs de mobilité: 101
3.3 Le simulateur MOVE: 102
3.4 Mise en œuvre de la simulation: 105
3.4.1 génération des scénarios de mobilité: 105
3.4.2 Codification des cartes routières: 108
3.4.3 Direction de mouvement 110
3.4.4 Les coordonnées et vitesses des véhicules 110
3.4.5 Les feux de signalisation 111
4 Mise en œuvre comparative des protocoles 111
4.1 Les paramètres de simulation 112
4.2 Les métriques d'évaluation de performances 113
5 Résultats 114

5.1 Impact de la variation des capacités de détection des nœuds 115
5.2 Impact de la variation des capacités et stratégies adverses 116
5.3 Impact de la variation des conditions de trafic 118
6 Conclusion 120
Conclusion générale 121
Bibliographie 123

Table des figures

Figure 1. Trois catégories d'architectures pour les réseaux de véhicules [1] 6

Figure 2.Architecture ad-hoc hybride C2C-CC [6] 8

Figure 3.La pile de protocole WAVE 15

Figure 4.Standards de communication DSRC 16

Figure 5.Les canaux de transmission WAVE 17

Figure 6.Configurations des paramètres pour les différentes catégories d'application selon IEEE 802.11p 18

Figure 7.Processus d'accès au canal IEEE P1609.4/IEEE 802.11p MAC 19

Figure 8. Identification non autorisée 28

Figure 9. Injection d'informations de trafic erronées 28

Figure 10. Fausses déclarations de localisation 29

Figure 11. Usurpation d'identité 29

Figure 12. Déni de service par brouillage du canal radio 30

Figure 13. Extraction du mot de passe d'une transaction commerciale 30

Figure 14. Principaux défis et exigences de sécurité des réseaux véhiculaires 36