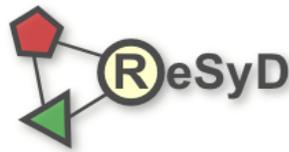


RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE  
Ministère de l'Enseignement Supérieure et de la Recherche Scientifique  
Université Mira Abderrahmene de Béjaia

# ÉTUDE DE L'ATTAQUE DU TROU DE VER AVEC LE ROUTAGE PROACTIF DANS LES RÉSEAUX AD HOC



PAR  
ATTIR AZEDDINE

PRÉSENTÉE À LA FACULTÉ DES SCIENCES ET SCIENCES DE L'INGÉNIEUR  
DÉPARTEMENT D'INFORMATIQUE, ÉCOLE DOCTORALE D'INFORMATIQUE

ReSyD

(Réseaux et Systèmes Distribués)

POUR L'OBTENTION DU GRADE DE MAGISTÈRE EN INFORMATIQUE

À

L'Université Mira Abderrahmene

Béjaia, 06000

---

Acceptée sur proposition du jury

**Président :** M. Ahmed Aït Saidi, Maître de Conférences, Université de Béjaia.  
**Rapporteur :** M. Farid Naït-Abdesselam, Maître de Conférences, Université de Lille 1.  
**Examineurs :** M. Nadjib Badache, Professeur, USTHB de Alger.  
M. Ali Mellit, Maître de Conférences, Université de Jijel.

UNIVERSITÉ MIRA ABDERRAHMENE  
École doctorale d'informatique, ReSyD.

Date: **Décembre 2006**

Nom : **ATTIR Azeddine.**  
Titre : **Étude de l'attaque du trou de ver avec le routage proactif  
dans les réseaux ad hoc.**  
Département : **Informatique.**  
Grade : **Magistère en informatique.**

*A mes parents,  
A mes frères et sœurs  
A toute la famille,  
A la mémoire de mes grand-pères : Moussa, Slimane, Ezehra, Allah Yarahmhoum.*

# Table des Matières

Table des matières	iv
Liste des Tableaux	vii
Liste des Figures	viii
Remerciements	x
Résumé	xi
Abstract	xii
Introduction Générale	1
<b>1 Le routage dans les réseaux ad hoc</b>	<b>4</b>
1.1 Introduction . . . . .	4
1.2 Définition . . . . .	5
1.3 Les caractéristiques des réseaux ad hoc . . . . .	5
1.4 Routage . . . . .	6
1.5 Les différentes familles de protocoles de routage MANET . . . . .	7
1.5.1 Classification du groupe MANET . . . . .	7
1.5.1.1 Les protocoles proactifs . . . . .	7
1.5.1.2 Les protocoles réactifs . . . . .	9
1.5.1.3 Les protocoles hybrides . . . . .	11
1.6 Optimized Link State Routing Protocol (OLSR) . . . . .	13
1.6.1 Vue d'ensemble . . . . .	13
1.6.2 Les relais multipoint . . . . .	13
1.6.3 Fonctionnement du protocole . . . . .	15
1.6.3.1 Détection de voisinage . . . . .	15
1.6.3.2 Sélection des relais multipoints . . . . .	16
1.6.3.3 Heuristique de calcul des relais multipoints . . . . .	16
1.6.3.4 Gestion de la topologie . . . . .	18
1.6.3.5 Déclaration des interfaces multiples . . . . .	20
1.6.3.6 Gestion des sous réseaux . . . . .	20
1.6.3.7 Le calcul de la route . . . . .	20
1.7 Sécurité pour OLSR . . . . .	23
1.8 Conclusion . . . . .	23

<b>2</b>	<b>La Sécurité pour le protocole OLSR</b>	<b>24</b>
2.1	Introduction . . . . .	24
2.2	Protocoles proactifs de routage de MANET et les vulnérabilités d'OLSR . . . . .	25
2.2.1	Brouillage (Jamming) . . . . .	26
2.2.2	Génération incorrecte du trafic . . . . .	26
2.2.2.1	Génération incorrecte de message HELLO . . . . .	26
2.2.2.2	Génération incorrecte de message TC . . . . .	27
2.2.3	Relayage incorrect du trafic . . . . .	28
2.2.3.1	Relayage incorrect du trafic de contrôle . . . . .	28
2.2.3.2	Replay attack . . . . .	29
2.2.3.3	L'attaque Wormhole . . . . .	29
2.3	Sécuriser OLSR . . . . .	30
2.3.1	Sécuriser le protocole OLSR . . . . .	31
2.3.1.1	Signature pour OLSR . . . . .	31
2.3.1.2	L'estampillage . . . . .	32
2.3.2	Sécuriser OLSR en utilisant la localisation des nœuds . . . . .	32
2.3.2.1	L'ajout de la position du nœud dans le message de la signature . . . . .	33
2.3.2.2	Spécification . . . . .	33
2.3.2.3	Vérification de l'originalité du message HELLO . . . . .	34
2.3.2.4	Procédure de la création des messages de contrôle . . . . .	35
2.3.2.5	Procédure à la réception des messages de contrôle . . . . .	35
2.3.3	Un système de signature avancée pour OLSR . . . . .	35
2.3.3.1	Protocole d'échange des messages ADVSIG . . . . .	36
2.3.4	OLSR sécurisé . . . . .	37
2.3.4.1	Détection de voisin sécurisée . . . . .	38
2.3.4.2	Routage sécurisé des paquets . . . . .	39
2.3.5	Système de detection des intrusions pour OLSR . . . . .	39
2.3.5.1	Propriétés intrinsèques du protocole OLSR . . . . .	39
2.3.6	Table récapitulative . . . . .	40
2.4	Autres propositions . . . . .	41
2.5	Conclusion . . . . .	42
<b>3</b>	<b>L'attaque Wormhole dans les réseaux ad hoc</b>	<b>43</b>
3.1	Introduction . . . . .	43
3.2	Caractéristiques du MANET et leur impact sur la sécurité . . . . .	44
3.3	Attaques contre les protocoles de routage dans les réseaux ad hoc sans fil . . . . .	45
3.4	L'attaque Wormhole . . . . .	49
3.4.1	L'attaque Wormhole et les protocoles réactifs . . . . .	49
3.4.2	L'attaque Wormhole et les protocoles proactifs . . . . .	50
3.5	Sécurisation du réseau ad hoc contre l'attaque Wormhole . . . . .	52
3.5.1	Propositions générales . . . . .	52
3.5.1.1	" <i>Packet Leashes</i> " : Défense contre l'attaque du trou de ver dans les réseaux sans fil . . . . .	52
3.5.1.2	" <i>SECTOR</i> " : Trace sécurisée des périodes de rencontre des nœuds dans les réseaux sans fil multi-sauts . . . . .	54

3.5.1.3	Utilisation des antennes directionnelles pour empêcher l'attaque du trou de ver . . . . .	55
3.5.1.4	Vérification de la présence physique des voisins contre l'attaque de re- joue dans les réseaux ad hoc sans fil . . . . .	55
3.5.1.5	" <i>LITEWORP</i> " : Une légère contre-mesure pour l'attaque du trou de ver dans les réseaux sans fil multi-sauts . . . . .	58
3.5.1.6	Prévention de l'attaque du trou de ver dans les réseaux ad hoc sans fil : l'approche de théorie des graphes . . . . .	60
3.5.1.7	Détection de l'attaque du trou de ver dans les réseaux ad hoc sans fil : l'approche d'analyse statistique . . . . .	62
3.5.1.8	Défense contre l'attaque du trou de ver dans les réseaux mobiles ad hoc	63
3.5.1.9	"DelPHI" : Mécanisme de détection du trou de ver pour les réseaux ad hoc sans fil . . . . .	64
3.5.2	Propositions pour le protocole AODV . . . . .	65
3.5.3	Propositions pour le protocole OLSR . . . . .	66
3.6	Table synthétique . . . . .	66
3.7	Conclusion . . . . .	68
<b>4</b>	<b>Light Extension for OLSR MANET Protocol Defending Against Logical Wormhole Attack</b>	<b>70</b>
4.1	Introduction . . . . .	70
4.2	Spécification du Wormhole logique dans le protocole OLSR . . . . .	71
4.3	Hypothèses . . . . .	74
4.4	Description de LWPOLSR . . . . .	74
4.5	Simulation et analyse . . . . .	78
4.6	Conclusion . . . . .	82
	<b>Conclusion &amp; perspectives</b>	<b>83</b>
	<b>Bibliographie</b>	<b>85</b>

# Liste des tableaux

1.1	Table des voisins du nœud <b>C</b> . . . . .	16
1.2	Table topologique du nœud <b>C</b> . . . . .	19
1.3	Exemple de la table de routage du nœud <b>C</b> . . . . .	22
3.1	Classification de l'attaque Wormhole . . . . .	58
3.2	Wormholes détectés par LITEWORP . . . . .	60
3.3	Table synthétique . . . . .	67
4.1	Paramètres de simulation . . . . .	79

# Table des figures

1.1	Le changement de la topologie des réseaux ad hoc . . . . .	5
1.2	Principe de fonctionnement des protocoles proactifs . . . . .	8
1.3	Optimisation des relais multipoints . . . . .	9
1.4	Principe de fonctionnement des protocoles réactifs . . . . .	9
1.5	Procédure de découverte de la route et la réponse avec AODV . . . . .	10
1.6	Le mécanisme d'entretien des routes avec AODV . . . . .	11
1.7	Principe de fonctionnement du protocole ZRP . . . . .	12
1.8	Relais multipoints . . . . .	14
1.9	Réseau ad hoc . . . . .	15
1.10	Construction de la route à partir des informations topologiques . . . . .	21
2.1	Usurpation d'identité des messages HELLO . . . . .	27
2.2	Usurpation d'identité des messages TC . . . . .	28
2.3	Intrus $X$ entre le nœud $A$ et $B$ . . . . .	29
2.4	Wormhole Attack : les intrus $X$ et $Y$ créent un lien artificiel entre $A$ et $B$ . . . . .	30
2.5	Format de la signature pour OLSR . . . . .	31
2.6	Format du SIGLOC . . . . .	33
2.7	Teste d'existence de lien quand le message HELLO est reçu . . . . .	34
2.8	Format du message ADVSIG . . . . .	36
2.9	Format du paquet d'extension pour sécuriser OLSR . . . . .	39
2.10	Table récapitulative . . . . .	41
3.1	L'attaque Wormhole . . . . .	50
3.2	Étapes de NVP . . . . .	56
3.3	Les nœuds $M$ , $N$ , $X$ sont des gardiens du lien de $X$ vers $A$ . . . . .	59
3.4	Classification de l'attaque Wormhole . . . . .	63
3.5	Wormhole caché et exposé . . . . .	64
3.6	Classification des propositions . . . . .	68
4.1	Format générique du paquet OLSR . . . . .	71
4.2	Le Wormhole Logique . . . . .	72
4.3	Topologie incorrecte due au Wormhole logique . . . . .	73
4.4	Délai généré par le Wormhole logique . . . . .	74

4.5	Format de message Worm_Delay . . . . .	75
4.6	Réseau de simulation . . . . .	79
4.7	Le délai généré par le Wormhole logique . . . . .	80
4.8	Messages HELLOs Acceptés par les nœuds 13 et 25 . . . . .	81