

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique



Centre de Recherche en Information Scientifique et Technique CERIST

Mémoire en vue de l'obtention du diplôme de Post-Graduation Spécialisée
PGS en Sécurité Informatique

Thème

**Vers une Approche Efficace pour
l'Acheminement et la Sécurité de
l'Information dans les Réseaux VANETs**

Dirigé par :

Dr. NECIBI Khaled

Réalisé par :

MAAKOUF Nedjib
KHALDI Fares

- Promotion 2015-2016 -

Dédicace

Je dédie ce modeste travail à ...

*Mes chers parents pour leur patience, leur amour,
leur soutien et leur encouragement.*

*Mes frères et ma sœur qui n'ont cessé d'être pour
moi des exemples de persévérance, de courage et
de générosité*

Ma chère femme qui a toujours été à mes côtés

Mes collègues

Tous ceux qui m'aiment

Nedjib

Remerciement

Tout d'abord, nous remercions le Dieu, notre créateur de nos avoir donné les forces, la volonté et le courage afin d'accomplir ce travail modeste.

Ce travail a été réalisé sous la direction du Docteur NECIBI khaled, Maître de conférences à l'université de Constantine 2. Nous tenons à le remercier vivement pour ses conseils, son aide, sa disponibilité ainsi que son soutien tout au long de ce travail. Qu'il trouve ici, notre sincère reconnaissance et notre profonde gratitude.

Nous remercions nos responsables de la Sûreté Nationale pour nous avoir donné l'occasion de suivre cette formation.

Aussi, Nous tenons également à remercier Messieurs les membres de jury pour l'honneur qu'il nous fait en acceptant de siéger à notre soutenance, qu'ils trouvent ici l'expression de notre profonde gratitude.

Finalement, Nous remercions les enseignants du CERIST, le Chef du département formation continue et audiovisuel et tous ceux qui ont contribué de près ou de loin à la réalisation de ce travail.

Résumé

Un réseau Ad hoc de véhicules ou VANET (Vehicular Ad Hoc NETwork) est constitué de véhicules capables d'échanger des informations via leurs interfaces de communication sans fil. Par rapport à un réseau Ad hoc classique, un réseau VANET se différencie par une forte mobilité des nœuds rendant la topologie du réseau fortement dynamique. Le problème dans ces réseaux consiste à déterminer la stratégie de routage la plus adaptée, et ensuite à la sécurisée dans le but d'assurer un acheminement de données plus sécurisé.

Dans ce travail nous allons commencer par étudier la faisabilité de construire des attaques sur le protocole de routage open source GPSR (avec service de localisation). Tout fois, ce dernier n'est pas disponible sur la plateforme NS2, donc il nous a fallu d'intégrer ce protocole de routage dans le simulateur NS2. Nous commencerons cette étude de faisabilité par quelques expérimentations d'attaque mené sur le protocole de routage AODV, ensuite nous allons effectuer des attaques sur le protocole de routage GPSR et essayer ensuite de le sécurisé contre les attaques de type blackhole en employant une méthode de chiffrement par substitution de données géographique.

Mots clés : routage géographique, données géographique, attaque sur les données géographique, blackhole, chiffrement par substitution de donnée géographique.

Abstract

An Ad hoc vehicle network or VANET (Vehicular Ad Hoc NETWORK) consists of vehicles capable of exchanging information via their wireless communication interfaces. Compared to a traditional ad hoc network, the VANET is distinguished by a high degree of mobility of the nodes, making the topology of the network highly dynamic. The problem in these networks is to determine the most appropriate routing strategy, and then to secure it in order to ensure a more secure routing of data. In this work, we will start by studying the feasibility of building attacks on the open source GPSR routing protocol (with location service). It should be noted that this protocol is not available on the NS2 platform, so we had to integrate it under the NS2 simulator. We will begin this feasibility study with some experiments of attack conducted on the AODV routing protocol, then we will carry out attacks on the GPSR routing protocol and then try to secure it against blackhole attacks using an encryption by substitution mechanism.

Keywords: geographic routing, geographic data, geographic data attack, blackhole, geographic data substitution encryption.

ملخص

الشبكة اللاسلكية للمركبات VANETs تتكون من مركبات قادرة على تبادل المعلومات عبر واجهات الاتصالات اللاسلكية، الشبكة اللاسلكية للمركبات تختلف مقارنة بالشبكات اللاسلكية الكلاسيكية، انها تتميز بحركية عالية للعقد مما يجعل طوبولوجيا الشبكة تمتاز بديناميكية عالية. المشكلة في هذه الشبكات هي تحديد استراتيجية التوجيه الجغرافي الأكثر ملائمة، ثم ضمان نقل البيانات بشكل آمن.

في هذا العمل سنبدأ بدراسة جدوى هجمات على بروتوكول توجيه مزود بخدمة تحديد الموقع. ولابد الإشارة ان هذا الاخير غير متوفر في منصة برنامج محاكاة الشبكات NS2، لذلك كان علينا ادماجه. نبدأ هذه دراسة، ببعض التجارب الرائدة التي أجريت على بروتوكول التوجيه AODV ، ثم اجراء هجوم الثقب الأسود على بروتوكول GPSR، بالمقابل انشاء طريقة جديدة للحماية ضد هذا الهجوم..

كلمات البحث: التوجيه الجغرافي، والبيانات الجغرافية، والهجوم على البيانات الجغرافية، الثقب الأسود، وتشفير البيانات الجغرافية، استبدال الشفرات.

Table de matière

Dédicace	i
Remerciement.....	ii
Résumé	iii
Abstract	iv
ملخص	v
Table des Matières.....	vi
Table des figures.....	x
Introduction Générale	1
Motivation.....	1
Objectif.....	2
Organisation du mémoire	2
Chapitre 01 : les réseaux sans fil	3
1.Les réseaux sans fil	4
1.1.Introduction	4
1.2.Définition	4
1.3.Classification des réseaux sans fil.....	5
1.3.1.Classification selon le mode opératoire du réseau	5
1.3.1.1.Réseau avec infrastructure	5
1.3.1.2.Réseau sans infrastructure.....	7
1.3.2.Classification selon la zone de couverture	7
1.3.2.1.Les réseaux personnels sans fil (WPAN).....	7
1.3.2.2.Les réseaux locaux sans fil (WLAN).....	8
1.3.2.3.Les réseaux métropolitains sans fil (WMAN).....	8
1.3.2.4.Les réseaux étendus sans fil (WWAN)	9
1.4.La norme IEEE 802.11	9
1.4.1.La couche physique	10
1.4.2.La sous-couche MAC.....	10
1.5.Les réseaux mobiles Ad hoc (MANETs)	11
1.5.1.Présentation des réseaux MANETs.....	11

1.5.2.Modélisation d'un réseau MANET	11
1.5.3.Caractéristiques des réseaux MANETs.....	13
1.5.4.Domaines d'applications	14
1.5.5.Les inconvénients des réseaux MANETs.....	15
1.6.Les réseaux Ad hoc de véhicules (VANETs).....	16
1.6.1.Présentation des réseaux VANETs	16
1.6.2.Services et applications des réseaux VANETs	17
1.6.3.Architecture des réseaux VANETs	17
1.6.3.1.La communication de véhicule à véhicule (V2V).....	18
1.6.3.2.La communication de véhicule à infrastructure (V2I)	19
1.6.3.3.La communication hybride.....	19
1.6.4.Propriétés et applications dans les réseaux VANETs	19
1.6.4.1.Propriétés des réseaux VANETs	19
1.6.4.2.Applications des réseaux VANETs.....	20
1.6.4.3.Quelques exemples d'applications	20
1.7.Les réseaux VANETs VS les réseaux MANETs	21
1.8.Conclusion.....	23
1.9.Références	24
Chapitre 02 : Le routage dans les réseaux MANETs et VANETs	25
2.1.Introduction	26
2.2.Le routage dans les réseaux Ad hoc	27
2.2.1.Les protocoles proactifs	28
2.2.2.Les protocoles réactifs.....	28
2.2.3.Les protocoles hybrides.....	28
2.2.4.Les protocoles de routage indépendant de la localisation	29
2.2.5.Les protocoles de routage basés sur la localisation (géographiques).....	29
2.3.Quelques protocoles de routage géographiques pour les réseaux MANETs	30
2.3.1.Le protocole DREAM (Distance Routin Effect Algorithm for Mobility).....	32
2.3.2.Le protocole GPSR (Greedy Perimeter Stateless Routing).....	33
2.3.2.1.L'organigramme du protocole GPSR.....	38
2.4.Le routage dans les réseaux VANETs.....	39
2.5.Quelques protocoles de routage pour les réseaux VANETs	39
2.5.1.Le protocole GSR (Geographic Source Routing).....	39

2.5.2. Le protocole GPCR (Greedy Perimeter Coordinator Routing)	40
2.5.3. Le protocole VADD (Vehicle-Assisted Data Delivery)	40
2.6. Conclusion	41
2.7. Références	42
Chapitre 03 : Sécurité appliquée aux données de routage	44
3.1. Introduction	45
3.2. Sécurité d'une manière générale	45
3.2.1. Objectifs généraux de sécurité	45
3.2.1.1. La confidentialité	45
3.2.1.2. L'authentification	46
3.2.1.3. L'intégrité	46
3.2.1.4. Non-répudiation	47
3.2.1.5. Disponibilité	47
3.2.1.6. Gestion de la vie privée	48
3.2.1.7. Contrôle d'accès	48
3.3. Sécurité appliquée aux données de routage	48
3.3.1. Les raisons de la nécessité des mécanismes de sécurité de données de routage dans les réseaux VANETs	48
3.3.1.1. La mobilité	48
3.3.1.2. Interface sans fil partagée	49
3.3.1.3. Manque de serveurs centraux	49
3.3.1.4. Manque de coopération	49
3.3.1.5. Nœuds compromis	49
3.3.2. Les mécanismes de sécurité	50
3.3.2.1. L'interception des messages	50
3.3.2.2. Modification des paquets	51
3.3.2.3. Suppression des paquets de routage	51
3.4. Les modèles d'attaques	51
3.4.1. Actif vs Passif	51
3.4.2. Interne vs Externe	51
3.4.3. Individuelle vs Distribuée	52
3.5. Les attaques spécifiques aux réseaux Ad hoc	52
3.5.1. L'attaque Blackhole	52
3.5.2. L'attaque Grayhole	53

3.5.3. L'attaque Wormhole	53
3.6. Classification des attaques selon les techniques de routage.....	54
3.7. Conclusion.....	54
3.8. Références	56
Chapitre 4 : Implémentation, simulation et analyse des résultats	57
4.1.Introduction	58
4.2.Présentation du Network Simulator NS2	58
4.2.1.Installation	59
4.2.2.Principe de fonctionnement de NS2.....	61
4.2.2.1.Langage de programmation dans NS2	61
4.2.2.2.Outils de traitement des résultats de simulation.....	62
4.3.Langages de programmation utilisés.....	63
4.4.Etude de l'attaque blackhole sur le protocole AODV.....	63
4.5.L'ajout du protocole GPSR dans NS2.....	66
4.6.La simulation du protocole GPSR.....	68
4.7.Simulation d'un scénario d'attaque sur le protocole GPSR.....	70
4.8.GPSR sécurisé : Simulation du protocole de routage & résultats	73
4.9.Conclusion.....	76
4.10. Références	78
Conclusion générale et perspectives	79