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 était à mes cotés

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 contribués 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 للمركباتVANETs 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 الاشارة 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