الجمهورية العربية السورية

جامعة البعث

كلية الهندسة المعلوماتية

قسم هندسة النظم و الشبكات الحاسوبية

تحليل الثغرات الأمنية في الشبكات الموائمة للمركبات والإجراءات المقترحة لمعالجتها

دراسة أعدت لنيل درجة الماجستير في هندسة النظم والشبكات الحاسوبية

إعداد: المهندس حسام نظير وسوف

بإشراف الدكتور غسان حمادة

كلية الهندسة المعلوماتية

/جامعة البعث/

١٤٣٨هـ - ٢٠١٧ م

الملخص

شبكات المركبات اللاسلكية هي فئة فرعية من الشبكات اللاسلكية النقالة، تتحرك فيها المركبات بحرية وتتواصل بعضها مع بعض ومع وحدات الطريق (roadside units). تتألف شبكات المركبات اللاسلكية بشكل أساسي من المركبات المتحركة "الوحدات المتحركة "(On Board units) وأبراج الإرسال "وحدات الطريق الثابتة" (On Road units)، وتعد هذه الشبكات لا مركزية حيث تعتمد العقد مبدأ شبكات ad–hoc في الاتصال بين بعضها.

الأمن هو مصدر قلق كبير فيما يتعلق بالمعلومات الحرجة المشتركة بين المركبات، لأنّ المعلومات المرسلة عبر شبكة المركبات حساسة ويمكن أن تؤثر في قرارات أمنية مهمة.

في هذا النوع تحتاج الشبكة أن تكون متاحة بأي وقت، حيث يتعرض توفر الشبكة إلى عدة أنواع من الهجمات والتهديدات، وتشمل هذه الهجمات الأمنية : هجوم سيبيل (Sybil attacks) ،هجوم حجب الخدمة (Denial of Service attacks) ،هجوم حجب الخدمة الموزع (Distributed DOS attacks) ،هجوم الثقب الأسود (Black hole attacks). نقوم في هذا البحث بتقديم دراسة عن الحماية في شبكات الـ VANET، فنقدم دراسة عن أهم الأخطار الأمنية التي تهدد حماية هذه الشبكات وتطبيقاتها و اقتراح بعض الحلول .

في الواقع سندرس الهجمات المتاحة على الشبكة وتحليل أخطارها، بالإضافة لمحاكاة بعض تلك الهجمات، وتحديداً هجوم حجب الخدمة باستخدام أدوات مناسبة، وتصنيف أخطارها بناء على دراسة لمتحولات معينة تصف أداء الشبكة. إضافة إلى ذلك سنقوم باقتراح بعض الحلول الأمنية التي تساعد في الحد من تأثير هذه الهجمات، ومن ثم تطبيق هذه الحلول وتقييمها.

الكلمات المفتاحية: شبكات المركبات اللاسلكية، الثغرات الأمنية ، هجوم حجب الخدمة ، محاكي الشبكة NS2.

ABSTRACT

Vehicles Ad-Hoc networks is a subclass of Mobile ad hoc networks in which the vehicles move freely and communicate with each other and with the roadside units (RSU). VANET networks primaly consist of two parts: moving part “On Board units” and static parts “On Road units”. VANET networks are considered to be non-wired network which apply ad-hoc rules to connect its nodes. Security is the major concern with respect to the critical information shared between the vehicles. The information transmitted over a vehicular network is sensitive and can affect important safety decisions. This kind of network need to be available at any time , Where network availability is exposed to several types of attacks and threads. These security attacks and threats include Sybil attacks, Denial-Of Service (DOS) attacks, Distributed DOS attacks, Black hole attacks. In this search, we provide a study about the security in VANET networks. The most important security flaws of this networks and its applications are studied.

In fact, we study the most important and dangerous attacks that may target VANET networks and analyze its main risks. Furthermore, we simulate some of these attacks specifically Denial-Of Service (DOS) attack using prober tools depending on chosen parameters that characterize the network performance. Moreover, we provide some security solutions to help counter measuring these attacks and minimize this effects, and Finally we apply these solutions and evaluate them.

Keywords: Vehicles Ad-Hoc networks, Security vulnerabilities, DOS Attack, solutions, network simulator NS2