مجلة جامعة تشرين للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (39) العدد (3) 2017
Tishreen University Journal for Research and Scientific Studies - Engineering Sciences Series Vol. (39) No. (3) 2017

خوارزمية القائمة السوداء الديناميكية للحماية من هجوم حجب الخدمة الموزع DDoS في شبكة العربات المتنقلة

د. بشرى معلا•
علاء محفوض••

(تاريخ الإيداع 24 / 1 / 2017. قُبِل للنشر في 22/ 6 / 2017)

□ ملخّص □

شبكات العربات المتنقلة هي مجموعة من العربات التي تحتوي على تجهيزات خاصة تمكنها من الاتصال فيما بينها مشكلة شبكة لاسلكية. تعد الهجومات على الشبكة من أخطر التحديات التي تواجه هذه الشبكات، لا سيما تلك التي تستهدف متطلب التوافرية، الذي يعد من أهم متطلبات الأمن في شبكات VANET . من أهم هذه الهجومات هجوما حجب الخدمة DoS وحجب الخدمة الموزع DDoS لأنهما يجعلان الشبكة غير متاحة للمستخدمين الفعليين فيها.

نقدم في هذا البحث اقتراحاً لخوارزمية كشف هجوم DDoS والتصدي له عند حدوثه. تعتمد هذه الخوارزمية على قائمة سوداء تتضمن معرف العربات الخبيثة التي يتم اختيارها بناءً على قيمة عتبة معينة لعدد الرسائل المستقبلة منها. ونقدم تحليلاً لأداء هذه الخوارزمية بالاعتماد على بارامترات الإنتاجية ومعدل وصول الرزم والتأخير نهاية إلى نهاية ومقارنتها مع أداء خوارزمية QLA.لتحقيق هذا الغرض استخدمنا المحاكي NS 2.35 مع استخدام إضافةلدعم اتصالات العربات المتنقلة (WAVE).وقد بينت نتائج المحاكاة أن الخوارزمية المقترحة تخفض تأثير الهجوم بشكل ملحوظ إذ تزيد من الإنتاجية ومعدل الرزم المستلمة.

الكلمات المفتاحية: شبكات العربات المتنقلة، حجب الخدمة الموزع، القائمة السوداء، معدل الرزم الواصلة.

•مدرس، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة تشرين، اللاذقية، سورية.
•• طالب ماجستير، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة تشرين، اللاذقية، سورية.

مجلة جامعة تشرين للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (39) العدد (3) 2017
Tishreen University Journal for Research and Scientific Studies - Engineering Sciences Series Vol. (39) No. (3) 2017

Dynamic Black List (DBL) algorithm to defense against DDoS attack in Vehicular Ad-hoc Network

Dr. Boushra Maala•
Alaa Mahfoud••

(Received 24 / 1 / 2017. Accepted 22 / 6 / 2017)

□ ABSTRACT □

A Vehicular Ad-hoc Network (VANET) is a group of vehicles, which have special equipments enable them to connect with each other as a wireless network .The attacks are considered as the most serious challenge against this network, especially those targeting availability requirement, which is one of the most important security requirements in VANET. The Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks are the most important attacks since they make the network not available for actual users.

In this research, we present an algorithm to detect and face the DDoS attack. This algorithm depends on a black list contains the IDs for malicious vehicles, which are being chosen depending on a certain threshold value for a number of messages received from them. We analyze the algorithm performance depending on throughput, packet delivery ratio, end to end delay parameters, and compare it with the performance of the Queue Limiting Algorithm (QLA) .To achieve this purpose, we use NS2.35 simulator using details to support Wireless Access in Vehicular Environments (WAVE). The simulation results showed that the proposed algorithm reduces the effect of the attack Significantly since it increases the throughput and packet delivery ratio.

Keywords: Vehicular Ad Hoc Network, Distributed Denial of Service, black list, packet delivery ratio.

•Assistant Professor, Department of Communication and Electronics, Faculty of Mechanical and Electrical Engineering, Tishreen University, Lattakia, Syria.
••Postgraduate student, Department of Communication and Electronics, Faculty of Mechanical and Electrical Engineering, Tishreen University, Lattakia, Syria.

مقدمة:

مع تزايد عدد السكان واتساع وتشعب شبكات الطرق، ومع ازدياد عدد حوادث الطرقات وضحايا هذه الحوادث، أصبحت هناك حاجة ملحة لاستخدام تقنية لتخفض قدر الإمكان من الحوادث وتقدم في الوقت ذاته نوعاً من الرفاهية للمتنقلين عبر الطرقات، هكذا ظهر نوع جديد من شبكات Ad Hoc المتنقلة،وتعرف بشبكات (VANET) (Vehicular Ad Hoc Networks). توفر هذه الشبكات بنية تحتية لتطوير أنظمة جديدة لتعزيز السلامة والراحة للسائقين والركاب على شبكات الطرق، تتشكل بين المركبات المتنقلة والمجهزة بأجهزة الاتصالات اللاسلكية. طُّور هذا النوع من الشبكات كجزء من أنظمة التنقل الذكية الـ ITS(Intelligent transportation systems) لتحسين أداء أنظمة النقل .تهدف هذه الشبكات إلى زيادة الأمان على الطرقاتوراحة مستخدمي الطرق. وذلك من خلال تأمين اتصال وتنسيق بين العربات لتفادي حالات الحوادث، والإعلام في حالة حدوث حادث سير ما، وتجنب حالات الازدحام، وضبط السرعة،وتأمين مرور سيارات الطوارئ، وتجنب العقبات غير المرئية، إضافة إلى تطبيقات الأمان. كما تؤمن هذه الشبكات لمستعملي الطريق الحصول على معلومات عن حالة الطقس، الاتصال بالإنترنت وتطبيقات الوسائط المتعددة.

وبما أن الهدف الأساسي لـ VANET هو زيادة الأمان على الطرقات العامة، وبسبب تأثير هذه الشبكة على حياة الناس الذين يعبرون الطريق، فإن توافر الشبكة للمستخدم بشكل متواصل يعد متطلباً أساسياً. كما أنه وبسبب الحاجة إلى تسليم سريع للبيانات الخاصة بالأمان بين العربات يعد متطلب الزمن الحقيقي حرجاً في هذه الشبكات. توجد عدة تحديات تجعل من الصعوبة تحقيق متطلبات الأمن في هذه الشبكات، منها الطوبولوجيا المتغيرة بسرعة والحساسية للتأخير والثغرات الأمنية الناتجة عن الاتصالات اللاسلكية والهجومات على الشبكة.

أهمية البحث وأهدافه:

تعد الهجومات على الشبكة من أخطر التحديات التي تؤثر على توافر الشبكة للمستخدمين الفعليين. يوجد عدة أنواع للهجومات لكن يعد هجوم حجب الخدمة الموزع DDoS من أخطر الهجمات لأنه يجعل الشبكة غير متاحة بشكل كامل. يهدف هذا البحث إلى اقتراح وتطبيق خوارزمية لحماية الشبكة من هذا الهجوم، تعتمد على حساب عدد الرسائل التي تستقبلها العربة من أية عربة أخرى في الشبكة خلال فترة زمنية محددة، عندما يتجاوز عدد هذه الرسائل عتبة محددة يتم تخزين الـ ID الخاص بهذه العربة ضمن قائمة سوداء ديناميكية، بحيث أنه لن تستقبل العربة أية رسالة من هذه العربة المهاجمة في المستقبل. تقدم هذه الخوارزمية حلولاً نسبية لمشكلة عدم توافر الشبكة بسبب الهجوم حيث تزيد من الإنتاجية ومعدل الرزم المستلمة وتقلل من التأخير.

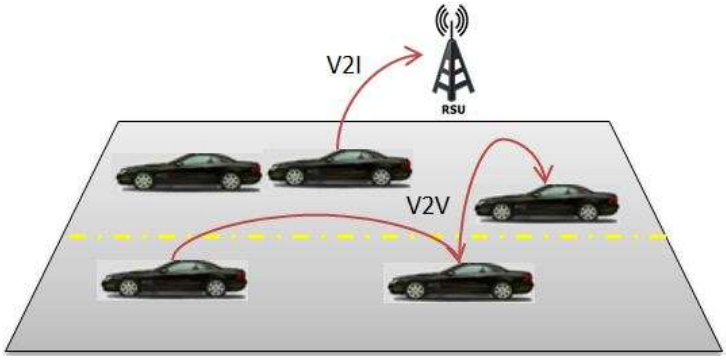
طرائق البحث ومواده:

لاختبار الخوارزمية المقترحة قمنا ببناء سيناريو المحاكاة باستخدام برنامج محاكي الشبكات Network Simulator 2، وهو برنامج محاكاة مفتوح المصدر يعتمد مبدأ محاكاة الأحداث المتقطعة. استخدمنا الإصدار NS2.35 مع الإضافات DSRCAPP التي تجعل البرنامج يدعم الشبكات الخاصة بالمركبات VANET بمعاييرها DSRC,IEEE802.11P و WAVE[1]. يصبح المحاكي بهذه الإضافات قادراً على توليد بيانات تتبع لتطبيق WAVE متضمنة رسائل الأمان الطرقية والتحذيرات (safety message) ورسائل الخدمة service

(message).تستخدم المركبات في الطبقة الفيزيائية التردد 5.9GHz الخاص بالـ WAVE، كما تقسم المجال الترددي إلى سبع قنوات، قناة تحكم CCH(Control Channel) وست قنوات للخدمة SCH(Service Channel). في طبقة MAC(Media Access Control) تم اختيار النوع Mac802_11Ext مع التعديل ليتوافق مع معيار WAVE. بالنسبة للرتل IFQ(Interface Queue) هو رتل ذو أولوية يصنف الرسائل بحسب التطبيق وتكون الأولوية للرزم التابعة لتطبيقات الأمان. سنستخدم تطبيق DSRCApp الذي يحاكي تطبيقات VANET الحقيقية، حيث سيكون لدينا نوعين من الرسائل، رسائل ترسل إلى العقد المجاورة بقفزة واحدة single hop مثل رسائل الترحيب hello ورسائل WSA(WAVE service advertisement) ورسائل تنتقل بوضع تعدد القفزات multihops.

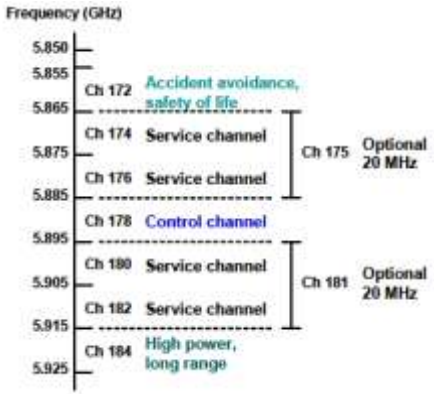
1. معيار IEEE 802.11P

قامت مجموعة IEEE بتعريف معيار الاتصال بين المركبات والذي يسمى 802.11P أو معيار الوصول اللاسلكي في بيئة المركبات WAVE[2]. يؤمن هذا المعيار عدة أنواع من الخدمات التي يتم تزويدها للعربات باستخدام أحد نوعي الاتصالات عربة إلى عربة V2V أو عربة إلى بنية تحتيةV2I كما يبين الشكل (1). تتضمن هذه الخدمات رسائل الأمان مثل تنبيهات الحوادث ومعلومات عن الحركة المرورية الهدف منها المحافظة على حياة الناس وتحسين الحركة على الطريق. أما النوع الثاني فهو رسائل الخدمات مثل الوصول للإنترنت، أخبار الطقس والاستعلام عن مراكز الخدمة [3].يستخدم معيار WAVE مبدأ تعدد القنوات (multi-channels) من أجل تزويد كل من رسائل الأمان ورسائل الخدمة معاً، حيث يصنف الرسائل بأولويات مختلفة بالاعتماد على أصناف وصول مختلفة [2] AC(Access Classes).



الشكل(1) أنماط الاتصالات في شبكة VANET.

يعتمد WAVE على تقنية DSRC التي تتضمن سبع قنوات بعرض حزمة 10MHz لكل قناة تعمل على التردد 5.9GHz. تستخدم هذه القنوات من أجل التأشير والخدمة، لذا لا تكون هذه القنوات متشابهة، فهي تتضمن قناة تحكم CCH وست قنوات خدمة SCH [3]. تقوم العربة بشكل مستمر ودوري بالتبديل بين قناة التحكم وقنوات الخدمة الشكل (2).



الشكل (2) القنوات السبع في معيار DSRC.

تعتمد طبقة MAC في معيار 802.11P على كل من التشغيل متعدد القنوات و 802.11، تُعرف هذه التقنية أربعة أصناف مختلفة (AC_S) لكل قناة، وهذه الأصناف غير متساوية وهي من (AC_0–AC_3). الصنف AC_3 هو الأعلى أولوية. تعد رسائل الأمان ذات أولوية مرتفعة لذلك تأخذ التصنيف AC3 لرسائل التحذيرات المتعلقة بالحياة و AC2 لرسائل تحذيرات الأمان الدورية وتكون باقي الأصناف خاصة برسائل الخدمات [2,3].

2. متطلبات الأمن فيVANET

بما أن الهدف الأساسي من VANET هو ضمان حياة الناس على الطرقات، فإن التطبيقات التي تقدمها وخاصة تطبيقات الأمان يجب أن تزود بشكل مستمر وموثوق. المتطلبات الأساسية للأمن في هذه الشبكات هي [4,5,6]:

- المصادقة (Authentication): تؤكد على ضرورة وجود ترخيص أو هوية للعربة تخولها عبور الطريق بشكل قانوني والتأكد أن العربات التي تنضم للشبكة هي موثوقة بما يضمن للعقد بأنها تستقبل الرسائل من عربات مخول لها الإرسال .
- الموثوقية (Confidentiality): هدفها التأكد من أن البيانات لم تعدل من قبل عقد غير مخولة أو عقد ليست ضمن الشبكة.
- التوافرية(Availability): تضمن أن الشبكة متوفرة عند الحاجة إليها وأن الخدمة تزود للمستخدمين المخولين فقط عندما يتم طلبها.
- عدم التنصل (Non–repudiation): تضمن أن المرسل أو المستقبل لا يستطيع أن يتنصل من أنه قد أرسل أو استقبل الرسالة.
- السرية (privacy): تهدف إلى الحفاظ على المعلومات الخاصة بالسائق بعيداً عن العربات غير الموثوقة، مثل الهوية الحقيقية والوجهة والسرعة.
- ضمان الزمن الحقيقي (Real time constraints): بما أن العربات تتحرك على الطريق بسرعة كبيرة فهي بحاجة إلى استجابة في الزمن الحقيقي بشكل دائم وإلا يمكن أن تحدث فاجعة.

3. الهجومات على VANET

تعد الهجمات على VANET من أهم التحديات التي تعيق تحقيق متطلبات الأمن [5]. توجد عدة أنواع من الهجومات التي تصنف بالاعتماد على الطبقات التي تهاجمها مثل الهجومات على طبقة الشبكة، طبقة التطبيقات أو الطبقة الفيزيائية ومنها:

- هجوم كشف الهوية ID Disclosure: يمكن للمهاجم أن يراقب حركة بيانات العربة الهدف واستخدام هذه المعلومات للحصول على معرف العربة ID بحيث يتأثر متطلب السرية.
- هجوم سايبل(Sybil): في هذا الهجوم يقوم المهاجم بإرسال عدة رسائل بهويات مختلفة، فيظهر المهاجم كأنه أكثر من عربة في الشبكة، يمكن أن يجعل العربات الأخرى تخلي الطريق من أجل مروره.
- هجوم إعادة الإرسال (Replay Attack): يقوم المهاجم بإعادة إرسال معلومات أرسلت في وقت مسبق مما يخلق فوضى في الشبكة.
- هجوم التنكر (Node-Impersonation): يقوم المهاجم بتغيير هويته الحقيقية والتنكر بهوية وهمية يهدف عدم كشف هويته عند القيام بمخالفة ما.
- هجوم حذف الرسالة (Message Suppression Attack): يقوم المهاجم بإسقاط الرسائل المتبادلة في الشبكة، يمكن أن يؤدي هذا إلى عدم وصول رسائل هامة إلى هدفها وتعريض الحياة للخطر.
- هجوم حجب الخدمة Denial of Service وهجوم حجب الخدمة الموزع: سيتم استعراضهما بالتفصيل فيما يلي.

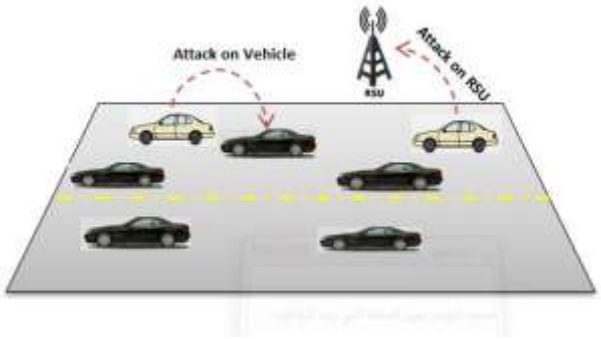
1.3 هجوم حجب الخدمة DoS (Denial of Service)

يهدف إلى منع المستخدمين الفعليين من الوصول إلى الشبكة [7].يمكن أن يحصل بعدة أشكال مثل التشويش على قناة الاتصال من قبل عربة غير مصادقة [8]. وهو أمر خطير في VANET بسبب حساسية التطبيقات التي تزودها مثل تطبيقات الأمان والتحذيرات الطرقية مما يؤدي لتعريض حياة الناس للخطر. يتضمن هذا الهجوم مستويين [9] هما:

- المستوى الأساسي: يقوم المهاجم بتخريب مصادر العقد مما يجعلها غير قادرة على التعامل مع المهام الرئيسية، ويجعل العقد مشغولة بشكل مستمر.
- المستوى الموسع: يقوم المهاجم بالتشويش على قناة الاتصال، بحيث لا تستطيع أي عربة الاتصال مع عربة أخرى أو مع وحدات الاتصال الطرقية في الشبكة.

1.1.3 المستوى الأساسي (تخريب مصادر العقد):

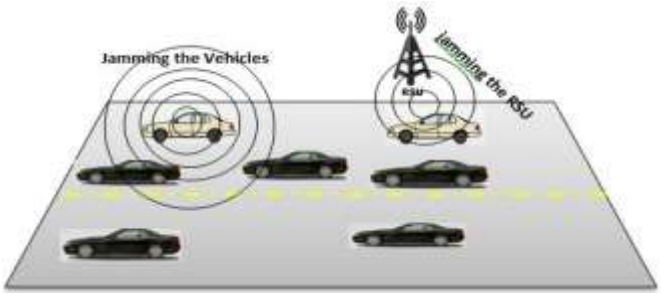
يقوم المهاجم في هذا المستوى باستهلاك مصادر العقد بحيث تصبح عاجزة عن إنجاز المهام الأساسية، كمثال عنها يقوم المهاجم بإرسال عدد كبير من الرسائل إلى العقدة الهدف بحيث تنشغل العقدة بشكل مستمر في معالجة الرسائل، ويحدث تأخير في معالجة الرسائل الهامة الأخرى [9,10]. يمكن للمهاجم شن هجومه على عربة أخرى كما في الشكل (3)، فيؤثر على الاتصالات بين المركبات (V2V)، أو يمكن أن يشن هجومه على وحدات الاتصال الطرقية (RSU(Road Side Unite، حيث يؤثر على الاتصالات V2I.



الشكل (3) هجوم DoS على كل من العربات ووحدات الاتصال الطرقية.

2.1.3 المستوى الموسع (التشويش على قناة الاتصال):

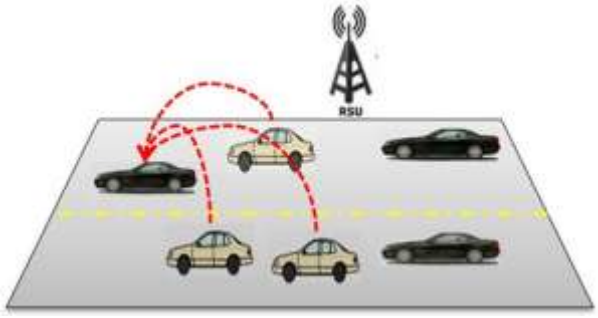
يقوم المهاجم بالتشويش على القناة عن طريق بث إشارة بتردد عالي، بحيث لا تستطيع العقد الأخرى الوصول إلى الشبكة. يمكن للمهاجم أن يقوم بالتشويش على قناة الاتصال بين العربات بحيث تصبح العربة غير قادرة على الاتصال بجيرانها ضمن مجال التشويش [10]، ويمكن أن يقوم بالتشويش على قناة الاتصال بين العربات ووحدات الاتصال الطرقية ،كما يظهر في الشكل (4). يعد هذا الهجوم من أخطر الهجومات حيث يقود الشبكة إلى الانهيار.



الشكل (4) هجوم التشويش على العربات ووحدات الاتصال الطرقية.

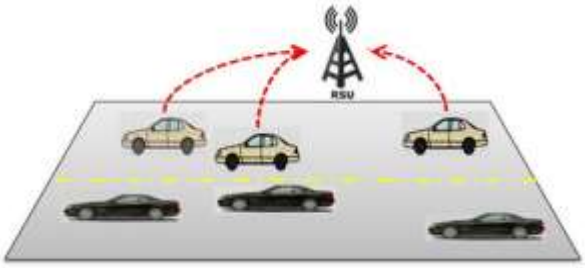
2.3 هجوم حجب الخدمة الموزع DDoS

يعد أخطر الهج ومات في بيئة العربات [8,9]، ويعتمد هذا الهجوم على عدة مهاجمين من مواقع جغرافية مختلفة بشكل متزامن، بحيث لا تستطيع العربة تحديد مكان العربة المهاجمة. يمكن للمهاجمين استخدام عدة حيزات زمنية (time slots) أو استخدام رسائل مختلفة من مهاجم لمهاجم [8]، بحيث تصبح العربة المستهدفة غير قادرة على الاتصال مع غيرها بشكل كامل،يبين الشكل (5) هذا الهجوم.



الشكل (5) هجوم DDoS على عربة

كما يمكن للمهاجم شن هجومه على وحدات الاتصال الطرقية من عدة مواقع [8,9] جغرافية بحيث تصبح العقد عاجزة عن الاتصال مع RSU، الشكل(6).



الشكل(6) هجوم DDoS على وحدة الاتصال الطرقي

الدراسات المرجعية:

هناك عدة أبحاث تناولت هجوم DoS في شبكة VANET. في [11] قدم الباحث طريقة للحد من الهجوم تعتمد على تغيير القناة المستخدمة في حال حدوث الهجوم ولكن لم يختبر هذه الطريقة. في[12] اقترح الباحثون طريقة فعالة للحد من هجوم DDoS المعتمد على التزامن، لكن هذه الطريقة تعتمد على RSU بشكل أساسي لكشف وعزل العربات المهاجمة، فهي غير فعالة في البيئات التي لا تحوي RSU. استعرض الباحثون في [13] آلية لكشف هجوم حجب الخدمة الذي يعتمد على التشويش على قناة الاتصال وذلك عن طريق مراقبة معدل خطأ البت من قبل العربات، ولكن لم يقدم حلاً فعالاً للحد من الهجوم، واعتمد على كشف الهجوم من أجل تنبيه السائق للابتعاد عن مكان الهجوم. أجرى الباحثون في[14] دراسة ومقارنة لتأثير الهجوم على الشبكة مع استخدام بروتوكولات توجيه مختلفة ودراسة بروتوكول التوجيه الأقل تأثراً بالهجوم ووجد اختلاف في النتائج عند تغيير بروتوكول التوجيه. بينما في [15] تم اقتراح خوارزمية QLA التي تعتمد على تقليص طول الرتل للحد من تأثير الهجوم على العربة وتجنب تخريب مصادر العقدة، تقلص هذه الطريقة عدد رسائل الأمان التي يمكن أن يتضمنها الرتل قبل معالجتها، أي تحسن الإنتاجية ومعدل الرزم الواصلة، لكن هذه الخوارزمية تؤثر على أداء الشبكة في حال عدم وجود هجوم. و تضمن البحث [16] دراسة لتأثير خوارزمية QLA على أداء بروتوكول التوجيه Dynamic Source Routing (DSR)، حيث وجد أن DSR يتأثر بشكل كبير بهجوم حجب الخدمة، ووجد أنه عند استخدام الخوارزمية يتحسن أداء الشبكة من ناحية الإنتاجية ومعدل الرزم الواصلة. كما تم اقتراح خوارزمية [17]Neighbor Trust Algorithm (NTA) للتصدي لهجوم DoS الذي يعتمد إرسال عدد كبير من الرسائل مع هجوم التزييف لإخفاء ID المركبة، تعتمد الخوارزمية على حساب عدد الرسائل المرسلة من العربة المهاجمة وتقليص طول الرتل في نفس الوقت، تزيد الخوارزمية معدل الرزم الواصلة بنسبه من 3-6%، لكن اعتمد الباحثون على تقليص طول الرتل عند حصول الهجوم ولم يعتمد عزل العربة المرسلة كما ولم يعتمد نموذج VANETحقيقي، وإنما طبقت الخوارزمية على نموذج MANETمعدل ليشابه شبكة VANET.

4 خوارزمية العمل المقترحة:

تهدف الطريقة المقترحة إلى حماية الشبكة من هجوم حجب الخدمة الموزع DDoS، الذي يمكن أن تنفذه مجموعة من المهاجمين باستخدام رسائل الأمان الطرقية أو رسائل الترحيب HELLO الدورية. يقوم المهاجم بإرسال عدد كبير من الرسائل عبر قناة التحكم إلى العربة الهدف، التي تستقبل الرسائل وترتبها ضمن رتل ذو أولوية وتعالجها بشكل متتالي، وبما أن الرسائل التي يرسلها المهاجم ذات أولوية عالية فسوف توضع في أول الرتل، ويقوم معالج العربة

بمعالجتها بشكل متتالي. لكن عدد الرسائل التي يرسلها المهاجم كبير جداً، لذا ستستهلك العربة كل مصادرها من أجل معالجة هذه الرسائل، وعندما ترسل عربة موثوقة رسالة أمان إلى العربة الهدف ستدخل الرتل ويحدث تأخير في معالجتها بسبب انشغال العربة. ربما يكون هذا خطير جداً لما يمكن أن تتضمنه الرسالة من معلومات خطرة عن حالة الطريق أو وجود حوادث وغيرها. مع استمرار الهجوم تحجب الخدمة عن العربة المستهدفة وتصبح غير قادرة على الاتصال مع غيرها أو الاستفادة من خدمات الشبكة.

تعتمد الخوارزمية المقترحة والتي أسميناها القائمة السوداء الديناميكية DBL(Dynamic Black List) على تقنية حماية ذاتية تتم ضمن العربة دون تدخل البنية التحتية المتمثلة بوحدات الاتصال الطرقية RSU، تعمل الخوارزمية على كشف العربات الخبيثة التي تنفذ الهجوم ووضع معرف العربة ID ضمن قائمة سوداء (Black List) BL. عملية التصدي للهجوم تعتمد على عدم استقبال أية رسالة من أية عربة موجودة ضمن القائمة السوداء.

تعتمد عملية التحديد فيما إذا كانت العربة هي عربة مهاجمة أم لا على البارامترات الآتية:

- زمن المؤقت (t_0): يمثل الفترة الزمنية التي يتم خلالها اختبار عدد الرسائل التي تصل للعربة. تُحدد قيمة هذا البارامتر بالاعتماد على كثافة الشبكة والمتمثلة بـ n أي عدد العربات الموجودة ضمن الجدول الخاص بالعربات، حيث أنه عند زيادة الكثافة تزيد مدة المؤقت وذلك تفادياً للتأخير الذي يمكن أن يحصل عند حساب عدد الرسائل الواردة من كل عربة خلال فترات زمنية قصيرة، المسمى جدول ID.حيث أنه عند زيادة الكثافة تزيد مدة المؤقت وذلك تفادياً للتأخير الذي يمكن أن يحصل عند حساب عدد الرسائل الواردة من كل عربة خلال فترات زمنية قصيرة. تم ضرب عدد العربات بالثابت 100 الذي تم اختياره من خلال دراسة احصائية لعدة قيم كما في الجدول (1). الواحدة بالميلي ثانية لأن أكبر تأخير مسموح لرسائل الأمان هو 100 ميلي ثانية [1]، وتم اختيار هذه القيمة كأصغر فتره للمؤقت في حال n=1.

الجدول (1) حساب الثابت الخاص بعلاقة زمن المؤقت.

قيمة الثابت	عدد العربات التي تم تمييزها كعربة مهاجمة		
	حالة عربة مهاجمة واحدة مع n=1	حالة 10 عربات مهاجمة مع n=50	حالة 20 عربة مهاجمة مع n=50
50	0	3	6
75	0	5	9
90	0	8	15
100	1	10	19
105	1	10	21
110	1	11	22
120	1	13	24

العلاقة التي تحدد قيمة هذا البارامتر هي :

$$t_0 = 100 * n \ (msec) \qquad (1)$$

- **قيمة العتبة (a)**: تحدد الحد الأعظمي الذي إذا تجاوزه عدد الرسائل ضمن الفترة الزمنية t_0تعد العربة المرسلة خبيثة، وبذلك يرسل الـ ID الخاص بها إلى القائمة السوداء. يتم حساب العتبة بالاعتماد على قيمة t_0 وعلى التأخير

الأعظمي المسموح للرسالة والذي بدوره يعتمد على نوع التطبيق. بما أن أغلب الرسائل تصل بزمن أصغر من زمن التأخير الأعظمي للتطبيق، تم ضرب الكسر بـ 1.2 لتجنب حالة عربة ترسل رسالة واحدة كل 100 ميلي ثانية فهي ليست حالة هجوم أما إذا تجاوزت حد 1.2 رسالة كل 100 ميلي ثانية تعد مهاجمة. تم اختيار القيمة 1.2 بناء على دراسة إحصائية لعدة قيم وتم اختيار القيمة التي تحقق أعلى أداء كما يبين الجدول (2).

الجدول (2) حساب الثابت الخاص بعلاقة العتبة.

قيمة الثابت	عدد العربات التي تم تمييزها كعربات مهاجمة		
	حالة10=n و 5 عقد مهاجمة	حالة 50=n و 20 عربة مهاجمة	حالة 80=n و 40 عربة مهاجمة
1	6	24	52
1.05	6	23	47
1.1	5	22	44
1.15	5	22	41
1.2	5	20	40
1.25	4	16	36

$$a = 1.2 * t_0 / \max d \qquad (2)$$

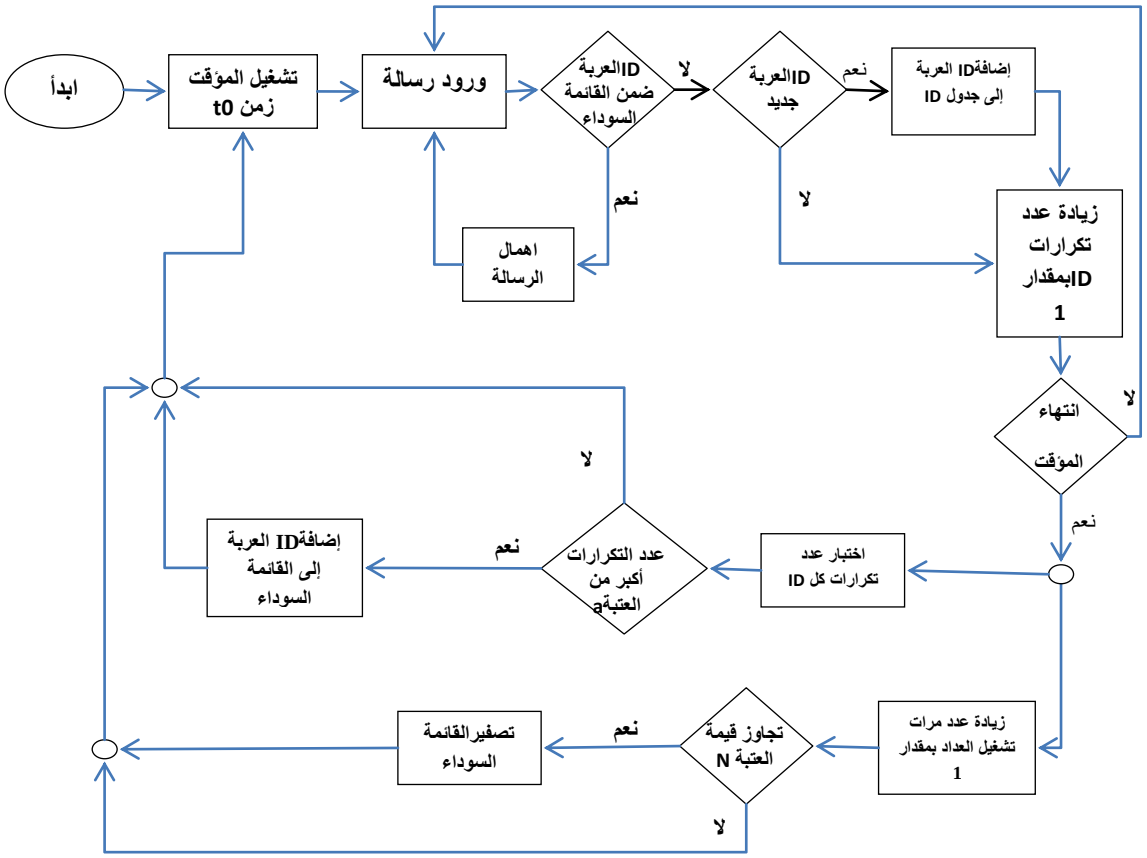
d: التأخير المسموح للتطبيق.

- **عتبة القائمة السوداء:** هي قيمة تحدد متى يتم تصفير القائمة السوداء، الغرض منها عدم الاحتفاظ بمعرف العربات في القائمة السوداء للأبد لأن العربات في الشبكة متبدلة بشكل دائم، فليس من المجدي الاحتفاظ بالمّعرف لزمن طويل، وكذلك من أجل تجنب هجومات التزييف التي تعتمد على تزييف المعرف الخاص بالعربة حيث من غير المجدي الاحتفاظ بمعرف غير صحيح. سنعتمد في حساب هذه العتبة على سرعة تغير العقد المحيطة بالمركبة التي تعتمد على سرعة حركة المركبة على الطريق والتي تتناسب عكساً مع عدد مرات تشغيل المؤقت N. تم اختيار الثابت 20000 من أجل الحالة الدنيا عربة تسير بسرعة 1 كيلو متر بالساعة بهذا الشكل سيكون تغير طوبولوجيا الشبكة محدود فيتم الاحتفاظ بالقائمة السوداء 20000 دورة، أما في حال سرعة متوسطة 100 سيتم الاحتفاظ بمحتوى القائمة السوداء 200 دورة فقط وهكذا. نعتمد في حساب الثابت السابق على دراسة إحصائية لعدة قيم كما في الجدول(3).

الجدول (3) حساب الثابت الخاص بعلاقة عتبة القائمة السوداء.

متوسط السرعة/ Km/h	التأخير الإجمالي لرسائل الأمان عند العربة التي تستخدم DBL بالنسبة لقيمة الثابت في حال وجود هجوم				
	الثابت 10000	الثابت 15000	الثابت 20000	الثابت 25000	الثابت 30000
1	0.085	0.071	0.041	0.051	0.062
50	0.099	0.086	0.052	0.073	0.081
100	0.101	0.098	0.059	0.087	0.962
150	0.119	0.113	0.062	0.094	0.103
200	0.123	0.121	0.088	0.102	0.109

$$N = 20000 / ((\max speed - \min speed)/2) \qquad (3)$$



الشكل (7) مخطط خوارزمية العمل المقترحة

5.المحاكاة والنتائج

قمنا بتطبيق الخوارزمية المقترحة، ومن خلال المحاكاة اختبرنا الخوارزمية وقارناها مع خوارزمية QLA. يعتمد تحليل الخوارزمية المقترحة ومقارنتها على أهم ثلاث بارامترات وهي التأخير نهاية إلى نهاية ومعدل وصول الرزم والإنتاجية.

1.5 سيناريو المحاكاة

قمنا بإجراء المحاكاة على شبكة مؤلفة من 20 عربة تتحرك على طريق باتجاه واحد ثنائي المسار بطول 1000m بحيث مساحة العمل هي $(1000 \times 500)m^2$. وقد تم اختيار نموذج التنقل بحيث تتحرك العربات بسرعات مختلفة تتراوح بين 40Km/h و 120Km/h. قمنا باختيار إحدى العربات وهي العربة 5 لتكون العربة المستهدفة بالهجوم، أما العربات المهاجمة سنقوم باختيارها وفق عدة حالات. تم اختيار بروتوكول توجيه AODV(Ad hoc On–Demand Distance Vector) لأنه الأكثر استخداماً في هذه الشبكات وهو مناسب لهذا الحجم من الشبكات. القيم المستخدمة في المحاكاة موضحة في الجدول (1):

الجدول (4) بارامترات المحاكاة.

Parameters(البارامتر)	Values(القيمة)
Simulation Time(زمن المحاكاة)	150Sec
Environment Size (حجم بيئة المحاكاة)	1000m X 500m
Number of nodes(عدد العقد)	20
Packet Size(حجم الرزمة)	512 bytes serves message 300 bytes safety message
Traffic-Type(نوع البيانات)	DSRCApp
Transmit power(استطاعة الإرسال)	0.0046 W
Transmit rang(مجال الإرسال)	250m
Data rate of each node(معدل البيانات)	3 Mbps with BPSK
MAC Protocol (MAC بروتوكول طبقة)	IEEE 802.11p
Routing protocol(بروتوكول التوجيه)	AODV
Vehicle speed(سرعة العربة)	40-120 Km/hr
Visualization Tool(أداة الإظهار)	NAM

2.5سيناريوهات المحاكاة

لتقييم أداء الخوارزمية المقترحة فقد قمنا باعتماد السيناريوهات الآتية:

1.2.5السيناريو 1

شبكة VANET مؤلفة من 20عربة. نختار إحدى العربات لتكون عربة خبيثة تهاجم العربة المدروسة أي السيناريو يمثل حالة DoS. ترسل العربة المهاجمة رسائل أمان طرقية إلى العربة المستهدفة بغرض استهلاك مصادر العقدة. تزيد العربة المهاجمة عدد الرسائل المرسلة بشكل تدريجي من 50 إلى 250 رسالة بالثانية.

الغاية: تقييم أداء خوارزمية DBL في حالة هجوم DoS ومقارنتها مع الخوارزمية الأخرى ودراسة تأثير زيادة عدد الرسائل عمل الخوارزمية.

2.2.5السيناريو 2

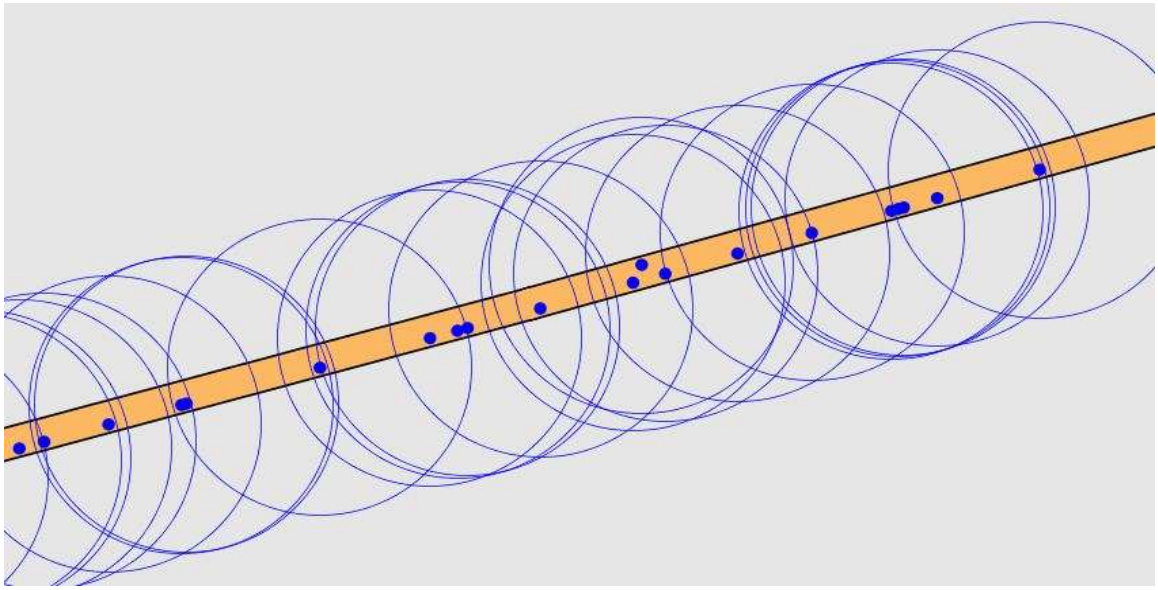
في السيناريو 1 سنزيد عدد العربات التي تهاجم العربة المدروسة إلى ثلاث عربات. سترسل العربات المهاجمة رسائل أمان طرقية إلى العربة المستهدفة. تمثل هذه الحالة هجوم DDoS تنفذه عدة عربات من مواقع جغرافية مختلفة خلال زمن المحاكاة.

الغاية: تقييم أداء خوارزمية DBL في حالة هجوم DDoS ومقارنتها مع الخوارزمية الأخرى .

3.2.5السيناريو 3

في السيناريو 1 سنزيد عدد العربات التي تهاجم العربة المدروسة **بشكل تدريجي**. سترسل العربات المهاجمة رسائل أمان طرقية إلى العربة المستهدفة. تمثل هذه الحالة هجوم DDoS بتفذه عدة عربات من مواقع جغرافية مختلفة.

الغاية: تقييم أداء خوارزمية DBL في حالة هجوم DDoS وتأثير زيادة عدد العربات المهاجمة على عمل الخوارزمية.



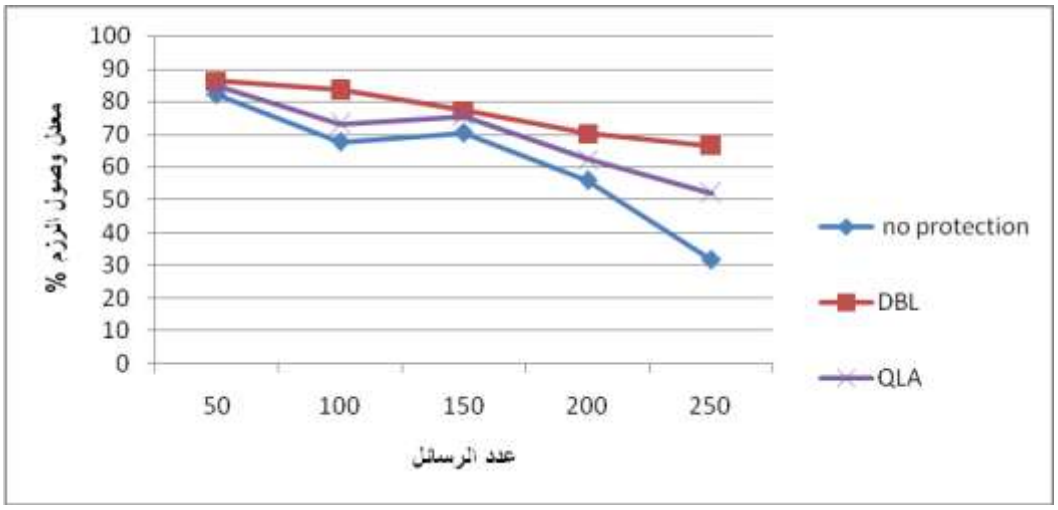
الشكل(9) سيناريو الشبكة على برنامج VANETSIM

النتائج والمناقشة

يمثل الشكل (9) سيناريو الشبكة المستخدم.

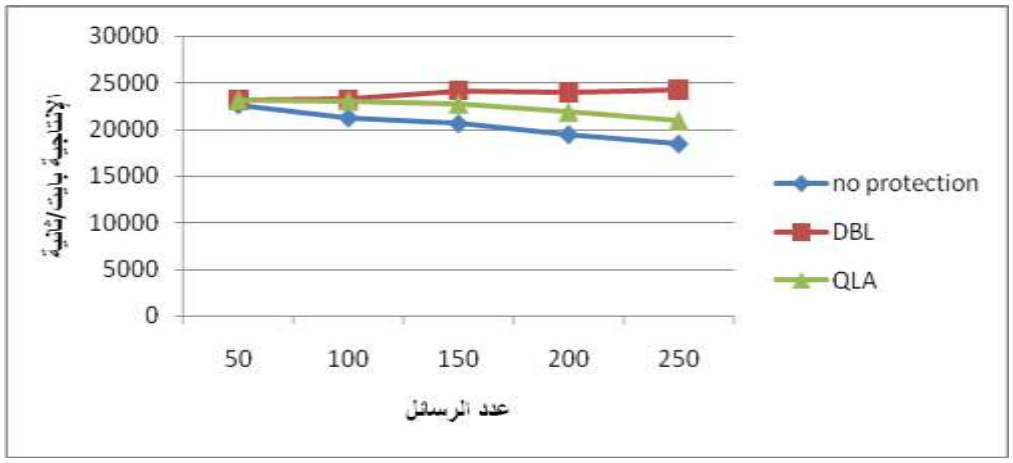
1. نتائج السيناريو 1

عند دراستنا لأداء الخوارزمية في حالة هجوم DoS، أي عربة مهاجمة واحدة مع زيادة عدد الرسائل التي تولدها العربة بشكل تدريجي، حصلنا على النتائج الآتية، حيث زمن المحاكاة 2.5 دقيقة، والنتائج مدروسة على العربة المستهدفة فقط وهي العربة 5:



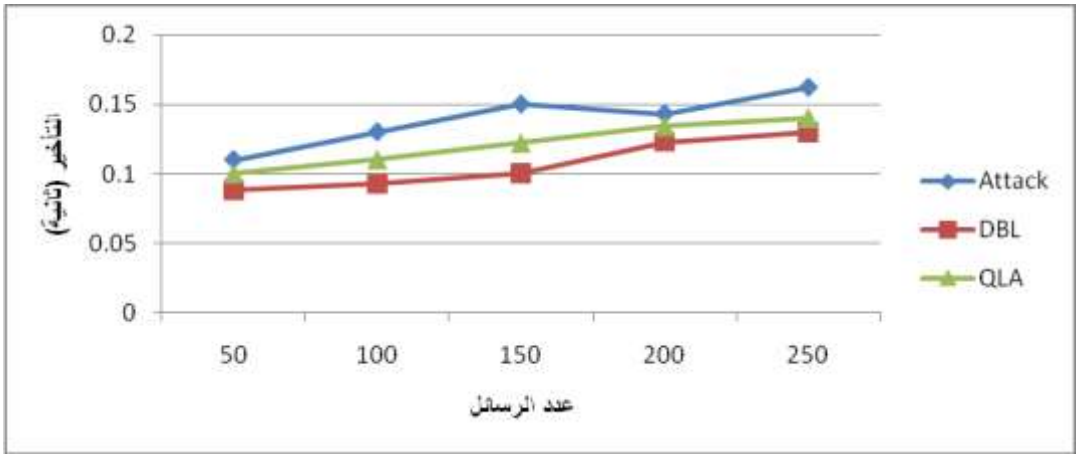
الشكل (10) معدل الرزم الواصلة في حالة هجوم DoS.

يوضح الشكل (10) مخطط لمعدل الرزم الواصلة إلى العربة المستهدفة أثناء الهجوم بحيث يتضمن ثلاث حالات هي حالة عدم تطبيق حماية وحالة الخوارزمية المقترحة DBL وحالة الخوارزمية السابقة QLA. نلاحظ من الشكل أنه بشكل عام ينخفض معدل الرزم الواصلة بتأثير زيادة فعالية الهجوم. لاحظنا أنه في حال عدم تطبيق تقنية حماية يكون تأثير الهجوم كبير حيث ينخفض PDR ليصل لحوالي 32% عندما يكون عدد الرسائل 250 رسالة بالثانية. تحسن خوارزمية QLA معدل الرزم الواصلة بنسبة بين 5-20% مقارنة بالحالة السابقة. لاحظنا أن الخوارزمية المقترحة DBL تزيد معدل الرزم الواصلة بنسبة 7% وسطياً عن خوارزمية QLA، فمثلاًمن أجل عدد الرسائل 200 يكون معدل وصول الرزم لـ QLA هو 63%بينما يرتفع في DBLإلى 70.1%، والسبب في ذلك أن خوارزمية QLA تقوم بتقليص حجم الرتل، مما يؤدي إلى حذف جزء كبير من رسائل العربة المهاجمة، ولكن بنفس الوقت وبسبب كون العربة المهاجمة تنفذ هجومها باستخدام رسائل ذات أولوية عالية، يتم حذف بعض الرسائل الحقيقية المرسلة من عربات موثوقة. أما في خوارزمية DBL عندما تتجاوز عدد الرسائل المرسلة من العربة المهاجمة قيمة العتبة a تضاف العربة إلى القائمة السوداء وبعدها سيتم حذف أية رسالة تحمل ID العربة المهاجمة فيرتفع PDR مقارنة مع خوارزمية QLA.



الشكل (11) الإنتاجية عند العقدة المستهدفة مقارنة مع عدد رسائل العربة المهاجمة في الثانية .

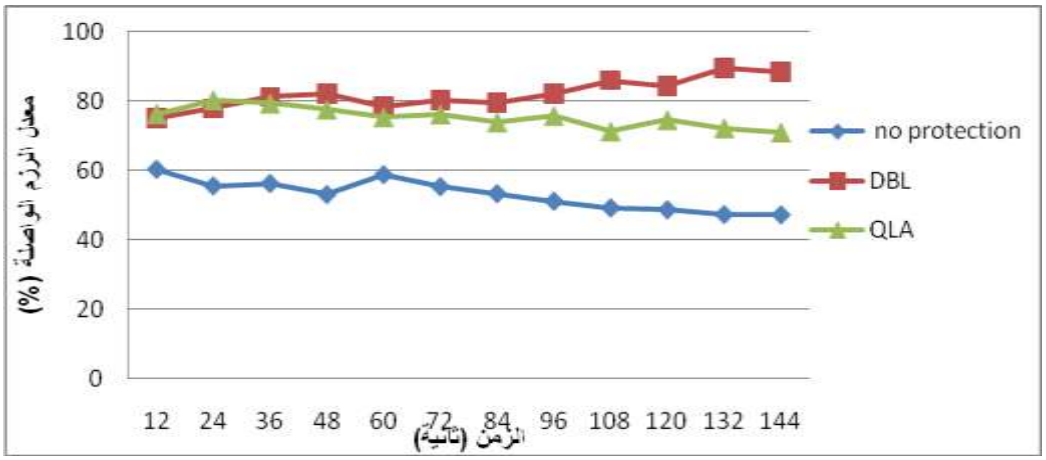
يوضح الشكل (11) إنتاجية العقدة 5 عند الحالات الخمس لعدد الرسائل التي ترسلها العقدة المهاجمة في الثانية. نلاحظ أن الإنتاجية في حال استخدام DBL أعلى منها عند استخدام QLA، حيث نلاحظ أن الإنتاجية أعلى بمعدل وسطي 9%، يزداد الفرق مع زيادة فعالية الهجوم، مثلا عند عدد رسائل 150 نلاحظ الإنتاجية عند استخدام QLA هي 22.741KB/sec أما عند استخدام DBL هي 24.201KB/sec.



الشكل(12) التأخير نهاية إلى نهاية مقارنة مع عدد الرسائل التي ترسلها العربة المهاجمة

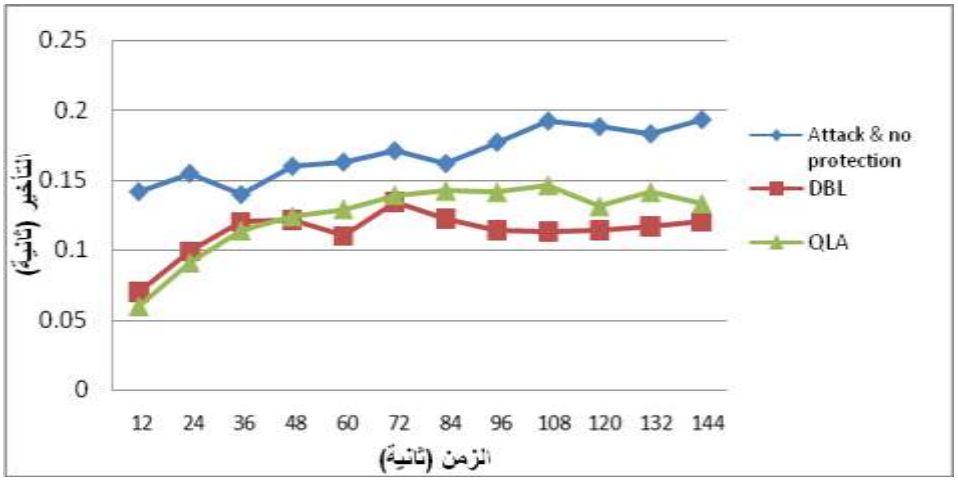
يبين الشكل(12) قيمة التأخير نهاية لنهاية عند الحالات الخمس لعدد الرسائل الخبيثة في الثانية. نلاحظ أن التأخير عند استخدام الخوارزمية المقترحة أقل من التأخير عند استخدام QLA بمعدل وسطي 20 ميلي ثانية،فمثلاً عند حالة عدد الرسائل 200 نجد التأخير عند استخدام QLA هو 0.133 ثانية، أما التأخير عند استخدام DBL فكان 0.122 ثانية. يكون التأخير أكبر في QLA بسبب عمليات إعادة الإرسال للرزم التي تسقط من الرتل وتتبع لتطبيقات غير مزيفة. نلاحظ أنه كلما زاد عدد الرسائل يزداد التأخير وتقل الإنتاجية،وذلك بسبب الزمن المستغرق للتأكد من ID الخاص بالرسالة واتخاذ القرار باستقبالها من عدمه.

2.3.5نتائج السيناريو 2



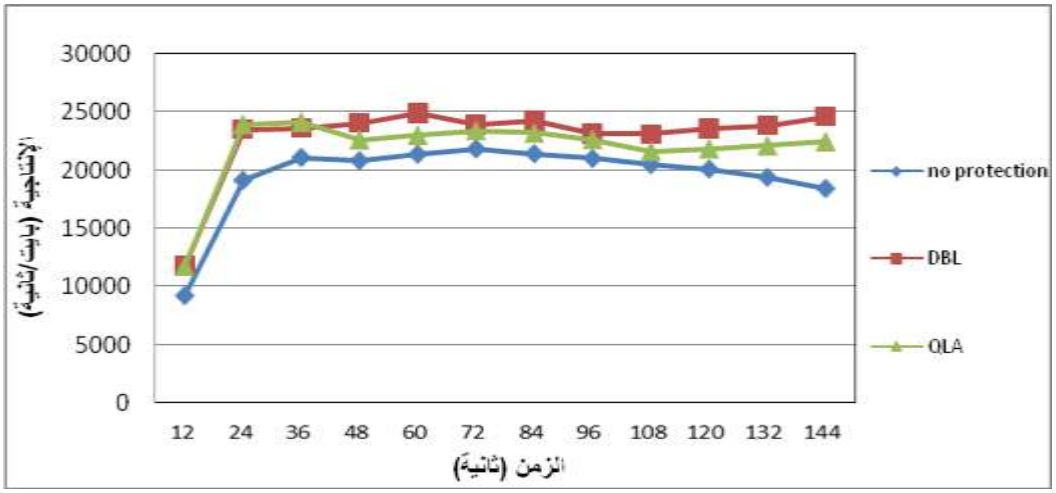
الشكل(13) معدل الرزم الواصلة خلال زمن المحاكاة.

دراسة حالة هجوم DDoS تنفذه ثلاث عربات على العربة الهدف وهي العربة 5 ، وحددنا مدة المحاكاة 2.5 دقيقة. حصلنا على الشكل (13). يبين الشكل معدل الرزم الواصلة خلال المحاكاة إلى العقدة المستهدفة. من الشكل نلاحظ أنه في بداية المحاكاة يكون معدل الرزم الواصلة أعلى عند استخدام خوارزمية QLA منه عند استخدام خوارزمية DBL بنسبة صغيرة حوالي 1.5%. مع سير المحاكاة يصبح معدل الرزم الواصلة عند استخدام DBL أعلى منه عند استخدام QLA بمعدل وسطي 15%فمثلاً عند الزمن 108ثانية يكون هذا المعدل 71% عند استخدام QLA و 85% عند استخدامDBL.



الشكل (14) التأخير نهاية إلى نهاية عند تطبيق هجوم DDOS.

يبين الشكل (14) التأخير نهاية إلى نهاية عند العربة المستهدفة خلال زمن المحاكاة. نلاحظ أنه في بداية المحاكاة يكون التأخير في حال استخدام QLA أقل منه عند استخدام DBL، ولكن مع سير المحاكاة نلاحظ أن التأخير يزداد عند QLA عن حالة استخدام DBL بمعدل وسطي 20 ميلي ثانية.



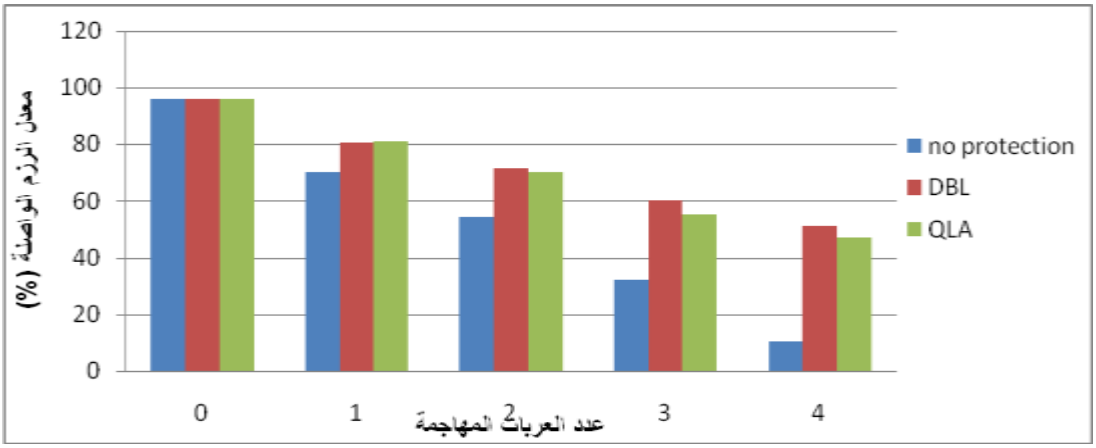
الشكل (15) الإنتاجية عند العقدة المستهدفة في حال تطبيق هجوم DDOS.

يبين الشكل (15) قيمة الإنتاجية عند العربة المستهدفة خلال الزمن. نلاحظ أنه في بداية المحاكاة تكون الإنتاجية أعلى عند استخدام QLA من استخدام DBL، وكنا قد وجدنا أن التأخير عند هذا الزمن أقل في حال استخدام QLA. والسبب يعود إلى كون خوارزمية QLA تعمل بشكل دائم عن طريق تقليص حجم الرتل، حيث أنه في بداية المحاكاة وقبل امتلاء الرتل لا يحدث أي إسقاط للرزم لذلك تكون الإنتاجية مرتفعة، أما خوارزمية DBL ففي بداية

المحاكاة يتم استقبال الرسائل الخبيثة ومن ثم حساب عددها، عندما يتجاوز هذا العدد قيمة العتبة يتم إضافة العربة إلى القائمة السوداء، وبعدها يتم حذف كل الرسائل الواردة من العربات المهاجمة فينخفض التأخير وتزداد الإنتاجية.

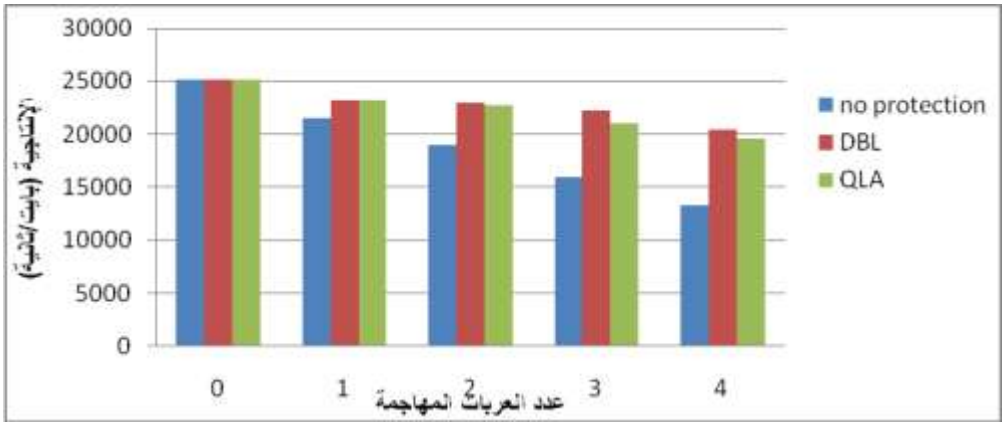
3.3.5نتائج السيناريو 3

دراسة حالة هجوم DDoS مع زيادة عدد العربات المهاجمة من0إلى4 عربات.



الشكل (16) معدل وصول الرزم بالنسبة لعدد العربات المهاجمة

يبين الشكل (16) أن معدل الرزم الواصلة عند عدم وجود هجوم متساوية تقريباً، الاختلاف ناتج عن التأخير عند تطبيق الخوارزميات. في الحالة التي يكون فيها عربة مهاجمة واحدة أي هجوم DoS نلاحظ أن PDRأعلى عند تطبيق QLA منه عند تطبيق DBL بفارق 2%. مع زيادة عدد العربات المهاجمة نجد أن معدل وصول الرزم عند استخدام DBL أعلى منه عند استخدام QLA بنسبه من 3–5%.



الشكل(17) الإنتاجية بالنسبة لعدد العربات المهاجمة.

يبين الشكل (17) الإنتاجية عند العربة المستهدفة، نلاحظ أنها تكون متساوية تقريباً عند عدم وجدود هجوم. في حالة هجوم DoS نجد أنها أعلى عند استخدام QLA لكن مع زيادة عدد العربات المهاجمة تصبح الإنتاجية في حال استخدام DBL أعلى وسطياً بـ 2000 بايت، يعود سبب الزيادة إلى أنه عند زيادة عدد العربات المهاجمة تزداد الرسائل التي تصل إلى العربة المستهدفة. في حال استخدام QLA تزداد عدد الرسائل التي تسقط من الرتل، فتنخفض الإنتاجية أما عند استخدام DBL فعند تجاوز عدد الرسائل قيمة العتبة، تضاف العربة للقائمة السوداء ولا تستقبل منها أية رسالة، فتبقى الإنتاجية مرتفعة لكن تنخفض تدريجياً بسبب التأخير اللازم لاختبار مصدر كل رسالة وحذفها.

الاستنتاجات والتوصيات:

قمنا في هذا البحث بتطبيق خوارزمية جديدة أطلقنا عليها القائمة السوداء الديناميكية DBL، من أجل حماية شبكة VANET من هجوم DDoS. وقارنا أداء هذه الخوارزمية مع أداء خوارزمية تحديد طول الرتل QLA. أجرينا المحاكاة في بيئة شبكة VANET واقعية، تتضمن تطبيقات أمان طرقية وتطبيقات خدمية في بيئة المحاكاة NS2 التي أعطتنا إمكانية واسعة لتطبيق الخوارزمية والتعديل عليها بلغة C++، وأثبتنا من خلال المحاكاة أنه:

1. يؤثر هجوم DDoS بشكل كبير على شبكة VANET حيث بتأثير الهجوم في حال عدم وجود طريقة لحماية العربات من الهجوم، يزداد التأخير وتنخفض الإنتاجية ومعدل الرزم الواصلة. بما أن تطبيقات الأمان في شبكات VANET حساسة للتأخير وضياع الرزم، فإن هذا الأثر قد يكون خطر جداً على حياة الناس لما يمكن أن تحمله هذه الرسائل من معلومات خطيرة.
2. عند تطبيق الخوارزمية المقترحة DBL لاحظنا انخفاض التأخير الإجمالي وزيادة كل من الإنتاجية وPDR، حيث أنه بعد زمن من بدء الهجوم تضاف العربة المهاجمة بشكل تلقائي إلى القائمة السوداء وتتوقف العربة المستهدفة عن الاستقبال منها.
3. عند مقارنة أداء الخوارزمية المقترحة مع QLA في حال هجوم من عربة واحدة DoS، يكون أداء الخوارزميتين متقارباً في حال كان الهجوم محدوداً ، ولكن عند زيادة فعالية الهجوم وجدنا أداء الخوارزمية المقترحة أفضل من ناحية التأخير والإنتاجية و PDR.
4. في حالة هجوم DDoS وجدنا أن أداء QLA أفضل في بداية عمل الشبكة، ولكن مع سير المحاكاة وجدنا أن أداء DBL أفضل بمعدل وسطي من 10%-5 من حيث التأخير ومن 15%-10 بالنسبة للإنتاجية.
5. تساهم الخوارزمية المقترحة في الحماية الذاتية للعربات من الهجوم بغض النظر عن وجود وحدات الاتصال الطرقية.

بالنتيجة نوصي باستخدام الخوارزمية المقترحة DBL،لأنها تحقق الأداء الأفضل في حماية العربة من الهجوم. وكذلك نوصي باختبار استخدام الخوارزميتين معاً لتأمين أعلى مستوى من الحماية. ونقترح أن يتم تبادل رسائل بين العربات تتضمن محتويات القائمة السوداء لكل عربة، وبذلك نضمن أن تعرض عربة للهجوم سيحمي باقي العربات في الشبكة من الهجوم.

المراجع:

[1] GHANDOUR, A. FELICE, M. BONONI,L and ARTAIL, H. "*Modeling and simulation of WAVE 1609.4-based multi-channel vehicular ad hoc networks*". In Proceedings of the 5th International ICST Conference on Simulation Tools and Techniques, Desenzano del Garda, Italy, March 2012, 148-156.

[2] EICHLER, S. *"Performance Evaluation of the IEEE 802.11p WAVE Communication Standard".* Vehicular Technology Conference,30 Sept.-3 Oct. 2007.

[3] QIAN, Y. LU, K and MOAYERI, N, "*A SECURE VANET MAC PROTOCOL FOR DSRC APPLICATIONS*", Global Telecommunications Conference,30 Nov.-4 Dec. 2008.

[4] LA, V, H. and CAVALLI, A. "*SECURITY ATTACKS AND SOLUTIONS IN VEHICULAR AD HOC NETWORKS: A SURVEY*". International Journal on AdHoc Networking Systems (IJANS),Vol. 4, No. 2, April 2014, 1-20.

[5] MOKHTAR, B. and AZAB, M. "*Overview of security issues in Vehicular Ad-hoc Networks* ", Alexandria Engineering Journal, Vol. 54, No. 4,December 2015, 1115-1126.

[6] SAMARA, GH.AL-SALHI, W. and SURES, R. "*Security Analysis of Vehicular Ad Hoc Networks (VANET)*". In Proceedings Second International Conference on Network Applications, Protocols and Services, 2010, 55-60.

[7] SAHARE, K. and MALIK, L. " *Review - Technique for Detection of Attack in VANET*", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, No. 2, February 2014, 580-584.

[8] SELVA,T. SUBRAMANIAN, K. and RAJENDIRAN, R. *"A Holistic Protocol for Secure Data Transmission in VANET"* International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, No. 6,December 2013, 8840-8846.

[9] PATHRE, A. AGRWAL,C.and JAIN, A. "*IDENTIFICATION OF MALICIOUS VEHICLE IN VANET ENVIRONMENT FROM DDOS ATTACK*," Journal of Global Research in Computer Science, Vol. 4, No. 6, June 2013, 30-34.

[10] MALLA, A. and SAHU, R. *"Security Attacks with an Effective Solution for DOS Attacks in VANET" International Journal of Computer Applications*. Vol. 66, No.22, March 2013, 45-49.

[11] HASBULLAH, H. SOOMRO, I. and MANAN, J. "*Denial of Service (DOS) Attack and Its Possible Solutions in VANET*," International Science, Vol.4, No.5,2010, 348-352.

[12] PATHRE, A. AGRAWAL, CH. and GAIN, A. ''*A Novel Defense Scheme against DDoS Attack in VANET*'' Wireless and Optical Communications Networks (WOCN), Tenth International Conference, IEEE 2013.

[13] LYAMIN, N. VINEL, A. and LOO, J. "*Real-Time Detection of Denial-of-Service Attacks in IEEE 802.11p Vehicular Networks*" IEEE COMMUNICATIONS LETTERS, VOL. 18, NO. 1,JANUARY 2014,110-113.

[14] SHARMA, G. and NARULA, T. *"Comparative Analysis of DDOS Attack on MANET and VANET using various Protocols*," International Journal of Research in Information Technology (IJRIT),Vol.2, No. 5, May 2014, 140-147.

[15] SINHA, A. and MISHRA, S. "*Queue Limiting Algorithm (QLA) for Protecting VANET from Denial of Service (DoS) Attack"*. International Journal of Computer Applications. Vol. 86,No .8, January 2014, 14-17.

[16] RANI, K. and MEENAKSHI. "*PREVENTION OF DENIAL OF SERVICE ATTACK ON DYNAMIC SOURCE ROUTING VANET PROTOCOL*," IJRET: International Journal of Research in Engineering and Technology, Vol. 04,No. 09, September2015,251-255.

[17] RAGHUWANSHI, V. and LILHORE, U. "*Neighbor Trust Algorithm (NTA) to Protect VANET from Denial of Service Attack (DoS).*" International Journal of Computer Applications, Vol.140 ,No.8 , April 2016, 8-12.