مجلة جامعة تشرين للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (37) العدد (3) 2015
Tishreen University Journal for Research and Scientific Studies - Engineering Sciences Series Vol. (37) No. (3) 2015

دراسة تأثير هجوم حجب الخدمة الموزع على شبكة العربات المتنقلة داخل المدينة

الدكتورة بشرى معلا •

(تاريخ الإيداع 27 / 4 / 2015. قُبِل للنشر في 30/ 6 / 2015)

□ ملخّص □

يعد هجوم حجب الخدمة الموزع على شبكات العربات المتنقلة من أخطر أنواع الهجومات التي يمكن أن تستهدف هذه الشبكات. تكمن خطورة هذا الهجوم في صعوبة اكتشافه كونه ينفذ من خلال التعاون بين أكثر من عقدة مهاجمة ضمن الشبكة، وبسبب تأثيره على استمرار الخدمة التي تقدمها الشبكة، أي انتهاك متطلب التوافرية الذي يعد من أهم متطلبات الأمن المطلوب تحقيقه في شبكة تقدم خدمة في الزمن الحقيقي. يهدف بحثنا إلى دراسة تأثير هذا الهجوم على شبكة عربات متنقلة تعمل داخل المدينة، آخذين بالحسبان حالتين، الأولى عندما يكون الهجوم موجهاً ضد عقد الشبكة والثانية عندما يكون موجهاً ضد الوحدات الجانبية على الطريق (RSU). وقد أظهرت نتائج المحاكاة التأثير الكبير لهذا الهجوم في كلتا الحالتين، وذلك من خلال مقارنة البارامترات الأساسية في الشبكة، مثل نفاذية الدخل/الخرج وعدد الرزم المسقطة، قبل الهجوم وبعده.

الكلمات المفتاحية: شبكات العربات المتنقلة، هجوم، هجوم حجب الخدمة، هجوم حجب الخدمة الموزع، التوافرية.

• مدرسة، قسم هندسة الاتصالات والالكترونيات ، كلية الهندسة الميكانيكية والكهربائية، جامعة تشرين، اللاذقية سورية.

مجلة جامعة تشرين للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (37) العدد (3) 2015
Tishreen University Journal for Research and Scientific Studies - Engineering Sciences Series Vol. (37) No. (3) 2015

Study of DDOS Attack Impact on Vehicular Ad Hoc Network in City

Dr. Boushra Maala •

(Received 27 / 4 / 2015. Accepted 30 / 6 / 2015)

□ ABSTRACT □

Distributed Denial of Service attack (DDOS) on Vehicular Ad Hoc Networks (VANETs) is considered to be one of the most serious types of attacks that can be targeted to those networks. The danger of this attack is in the difficulty of detection because of the cooperation of several attacking nodes in the network, and its impact on the availability requirement that is one of the most important security requirements in a network offering real-time applications .In our research, we study the effect of this attack on VANET network in the city, taking into consideration two cases. In the first case the target of the attack is the nodes, while in the second one, the target is the road side units (RSU). Simulation results have shown that this attack has a significant impact on both cases, by comparing the basic parameters of the network, such as throughput in/out and the number of dropped packets, before and after the attack.

Keywords: VANET, Attack, Denial of Service, Distributed Denial of Service, Availability.

• **Assistant Professor, Departement of Communication and Electronics, Faculty of mechanical and electrical engineering, Tishreen University, Lattakia, Syria.**

مقدمة:

يعد الأمن مطلباً هاماً وحرجاً في الشبكات اللاسلكية ولا سيما الشبكات اللاسلكية المتنقلة، مثل شبكات العربات المتنقلة، بهدف تأمين الاتصال بين العقد المتنقلة، ويعود ذلك أولاً إلى طبيعة الاتصال اللاسلكي المفتوحة والسهلة الانتهاك وثانياً إلى حركية العقد، التي تسبب الانقطاع المستمر في الاتصالات وهذا ينعكس بدوره على طبولوجيا الشبكة مما يجعلها متغيرة باستمرار، الأمر الذي يجعل استخدام تقنيات الأمن التقليدية محدود الفعالية؛ بالنتيجة تكون هذه الشبكات هدفاً سهلاً لكثير من الهجومات . هناك هجومات يكون تأثيرها محدود على الخدمة التي تقدمها الشبكة مثل هجوم التنصت، ولكن توجد هجومات خطرة تتسبب في إفقاد الشبكة فعاليتها من تعطيل الخدمة التي تقدمها هذه الشبكة وهي هجومات حجب الخدمة DoS. تهدف هذه الهجومات بشكل أساسي إلى منع الخدمة من الوصول إلى المشتركين فيها عند الحاجة إليها أي بمعنى آخر انتهاك متطلب التوافرية. تصنف هذه الهجمات من حيث عدد العقد المهاجمة إما من عقدة واحدة أو عدة عقد تتشارك معاً لتنفيذ الهجوم. يعد هجوم حجب الخدمة الموزع أكثر خطورة من الهجوم الذي تقوم به عقدة واحدة، والسبب في ذلك هو صعوبة كشفه لتوزع العقد في عدة مناطق ضمن الشبكة ومهاجمة الشبكة من عدة نقاط. إن خطورة هذا الهجوم دفعتنا إلى القيام ببحثنا هذا بهدف دراسة تأثيره على شبكة العربات المتنقلة التي تعمل داخل المدينة، وذلك في حالتين: الأولى عندما يكون الهجوم على عقد الشبكة، والثانية عندما يكون الهجوم موجهاً إلى الوحدات الجانبية على الطريق (RSU)، وقد تمت مقارنة البارامترات الأساسية في الشبكة قبل الهجوم و بعده، مثل نفاذية الدخل/الخرج وعدد الرزم المسقطة.

أهمية البحث و أهدافه:

تقدم شبكات العربات المتنقلة كثيراً من التطبيقات المفيدة التي ترفع سوية الأمان على الطرقات إضافة إلى الرفاهية التي تقدم إلى مستخدمي هذه الشبكات مثل الوصول إلى الانترنت... لكنها كغيرها من الشبكات اللاسلكية تشكل هدفاً سهلاً لكثير من الهجومات بسبب الطبيعة الخاصة للاتصالات اللاسلكية المفتوحة وسهولة اختراقها والتلاعب بها. سنتطرق في هذا البحث إلى دراسة تأثير هجوم حجب الخدمة الموزع على هذه الشبكات كونها تشكل هدفاً سهلاً له، إضافة إلى خطورة هذا الهجوم، والتي تكمن في صعوبة اكتشافه كونه ينفذ من خلال التعاون بين أكثر من عقدة مهاجمة ضمن الشبكة، الأمر الذي يضعف من إمكانية اكتشافه وتحديد منفذيه بشكل دقيق. يظهر تأثير هذا الهجوم بوضوح من خلال نتائجه السلبية على استمرار عمل الشبكة، بمعنى آخر على فعالية التطبيق الذي تقدمه الشبكة، وانتهاكه الملحوظ لمتطلب التوافرية الذي يعد من أهم متطلبات الأمن المطلوب تحقيقه في شبكة تقدم خدمة في الزمن الحقيقي.

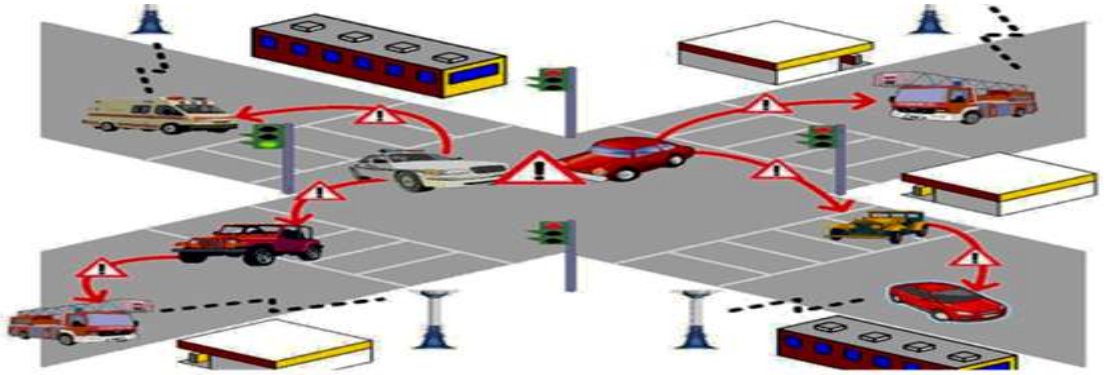
طرائق البحث ومواده

استخدمنا في هذا البحث برنامج المحاكاة NCTUns ، والذي يرمز إلى National Chiao Tung University Network Simulator [1,2]. وهو برمجية مفتوحة المصدر (open source)، تعمل على نظام Linux، إصدار Fedora، مع بيئة GUI متكاملة. يقدم هذا البرنامج عدة مزايا مقارنةً مع بقية برامج المحاكاة مثل توليد حركية شبكات واقعية من قبل تطبيقات الحياة الواقعية لتعطي نتائج محاكاة أقرب للواقع، ويمكن تقييم أداء أي تطبيق حياة واقعية بسهولة تحت شروط مختلفة لمحاكاة الشبكة، كما يمكن لأي برنامج تطبيقي للشبكة مطور من أجل

NCTUns أن يشغِّل مباشرة على نظام حياة واقعية في نظام Linux دون أي تعديل. إضافةً إلى قدرة هذا البرنامج في دعم تنفيذ المعيار IEEE 802.11(p) و 1069 من أجل شبكات العربات المتنقلة (VANET). نستخدم في البحث الإصدار NCTUns 6.0 الذي يشغِّل في واجهة افتراضية تشغِّل Fedora 12. يستطيع NCTUns أن يحاكي الكثير من الشبكات الأخرى مثل IEEE 802.11(b) wireless mesh networks، شبكات IEEE 802.11(e) QoS، شبكات الموبايل الفعالة...إلخ.

1. شبكات العربات المتنقلة (VANET (Vehicular Ad-hoc Network

تتكون شبكات العربات المتنقلة من مجموعة من العربات المتنقلة والمجهزة بـ مرسل/مستقبل وبالنظام العالمي لتحديد الموقع GPS(Global Position System) . تصمم هذه الشبكات لتوفير إمكانية الاتصال بين المركبات بعضها ببعض لاسلكياً دون الحاجة إلى بنية تحتية، أو بينها وبين وحدات متواجدة على جانب الطريق والتي تدعى RSU(Road Side Unit). يظهر الشكل (1) مثالاً عن شبكة VANET [3].



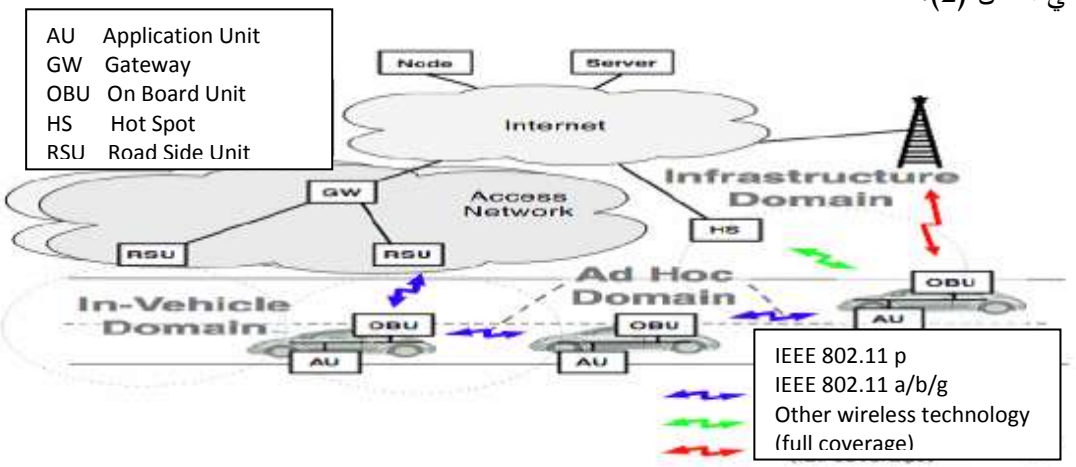
الشكل (1): مثال عن شبكة العربات المتنقلة VANET

تتميز هذه الشبكات عن غيرها من شبكات الـ Ad Hoc بالنقاط الآتية[5-3]:

- ✓ يحدد نموذج التنقل للعربات بمجموعة من العوامل المرتبطة بالطرق مثل الإشارات الضوئية وحدود السرعة وحالة الحركة المرورية وسلوك سائقي العربات ...الخ.
- ✓ تتغير طبولوجيا الشبكة بشكل دائم، وذلك ناتج عن السرعات العالية للسيارات، وهو مايسبب بدوره التقطع المستمر في الاتصال بين العربات حتى أثناء عملية تبادل المعلومات بينها.
- ✓ تتفاقم مشكلة تقطع الاتصال بسبب الكثافة المتغيرة للعقد بين الطرق المزدحمة كطرق السفر، وغير المزدحمة مثل الطرق الفرعية، كما تتفاوت كثافة العقد بين ساعات الازدحام وعدم الازدحام.
- ✓ لا تخضع عقد هذه الشبكات إلى قيود الطاقة وسعات التخزين حيث تملك وفرة في الطاقة وقدرة المعالجة.
- ✓ تعاني هذه الشبكات كغيرها من الشبكات اللاسلكية من الأمن الفيزيائي المحدود إذ يعد تحقيق أمن الشبكات اللاسلكية بشكل عام القضية الأصعب والأعقد مقارنة بالشبكات السلكية، ولاسيما أن الاتصال اللاسلكي يتم في بيئة مفتوحة لذلك تكون أكثر عرضة للهجومات.

2. مكونات الشبكة:

تتكون هذه الشبكة من ثلاث مجالات هي [4] : مجال العربة (in–Vehicle Domain) ومجال الشبكة المتنقلة Ad Hoc (Ad Hoc Domain) ومجال البنية التحتية (Infrastructure Domain). وتظهر هذه المجالات في الشكل (2).

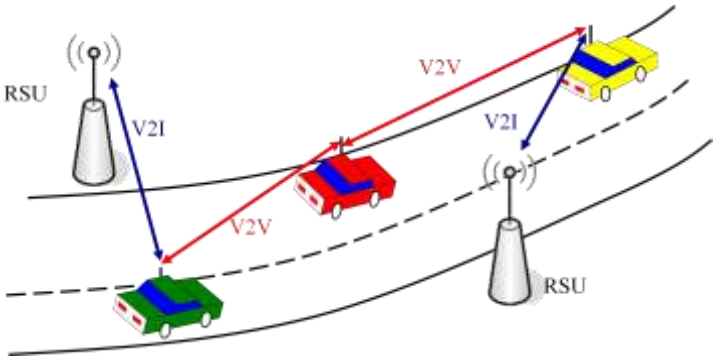


الشكل(2): مكونات شبكة VANET

- **مجال العربة(in–Vehicle Domain):** يخص مكونات العقدة، ويتكون بشكل أساسي من وحدتين هما وحدة الاتصال ووحدة التطبيق Application Unit (AU).
- **وحدة الاتصال:** هي جهاز يعتمد على إرسال واستقبال الأمواج ويتوضع عادة على لوح ضمن العربة ويدعى **On–Board Unit (OBU)**. وظيفتها الاتصال مع وحدة RSU أو وحدات OBU الأخرى في الشبكة من خلال وصلة لاسلكية تعتمد المعيار IEEE 802.11P [6].
- **وحدة التطبيق Application Unit (AU)** : تمثل مجموعة من الحساسات تستخدم لقياس الحالة الخاصة للعربة مثلاً(كمية الوقود)، ومعلومات عن بيئة القيادة مثل (المسافة الآمنة أومعلومات غير معروفة عن طريق ما)، ويمكن تبادل معلومات هذه الحساسات مع العربات الأخرى من أجل زيادة إدراك السائقين ببيئة القيادة لتحقيق ما يسمى "أمن الطريق".

إضافة إلى ذلك تركب لوحة تدعى Trusted platform module(TPM) وظيفتها القيام بعمليات التخزين والحسابات من أجل تحقيق أغراض الأمن تحديداً.

- **مجال الشبكة المتنقلة Ad Hoc (Ad Hoc Domain):** يضم هذا المجال أنواع الاتصال المختلفة بين مكونات الشبكة، و تقسم بشكل أساسي، كما يظهر في الشكل (3)، إلى نوعين اتصال عربة إلى عربة V2V واتصال عربة إلى بنية تحتية V2I.



الشكل (3): مثال عن نوعي الاتصال V2I &V2V

✓ الاتصال عربة إلى عربة Vehicles to Vehicles (OBUs to OBUs) وتكتب اختصاراً (V2V): ويقصد به الاتصال بين العربات مع بعضها مباشرة دون الحاجة إلى المرور بالبنية التحتية للطريق. الهدف من ذلك هو زيادة الأمان بإرسال المعلومات المطلوبة من عربة لأخرى، فمثلاً العربة التي تكتشف طريقاً جليدياً تبلغ العربات التي تسير على الجهة المقابلة على نفس الطريق.

✓ الاتصال عربة إلى بنية تحتية Vehicles to Infrastructure (OBUs to RSUs) وتكتب اختصاراً (V2I) : يتطلب استخدام الوحدات الموجودة على جوانب الطريق (RSUs) لجمع المعلومات. حيث تجمع هذه الوحدات المعلومات المرسلة وتحللها في الزمن الحقيقي، وبالنتيجة تولد معلومات مرورية؛ تتضمن السرعة المتوسطة للعربات، وكثافة العربات، والأحداث مثل الازدحام المروري. ثم تقوم ببث هذه المعلومات للعربات على مسافة قريبة نسبياً، وهذا مناسب لبيئة المدينة. أما العربات فتستخدم هذا الاتصال إما للحصول على معلومات عن العربات الأخرى، أو لاستخدام موارد الشبكة والحصول على الخدمات المتاحة مثل: الوصول إلى شبكة الانترنت.

● **مجال البنية التحتية (Infrastructure Domain)**: يتألف هذا الجزء من الشبكة من عدة كيانات تدير الحركة أو تقدم خدمات إضافية وهي:

1 -المصنع (Manufacture): يمكن أن يعد كجزء من شبكة الـ VANET، ويتمثل بالرقم المميز والخاص الذي يعطى لكل عربة.

2 -المسؤول الشرعي(Legal Authority): له وظيفتان أساسيتان وهما تسجيل العربة والإبلاغ عن الإزعاج.

3 -الجزء الثالث الموثوق (Trust Third Parties TTP): يقدم العديد من الخدمات مثل إدارة الأمن أو الطابع الزمني Timestamping .

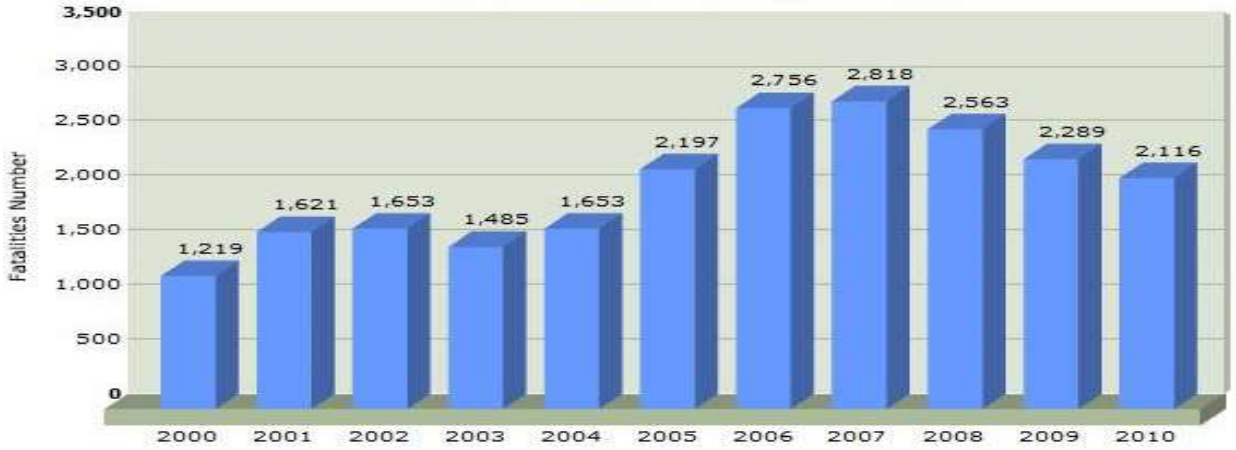
4 -مزودات الخدمة (Service Provider): والتي تقدم خدمات متعددة في شبكة الـ VANET، على سبيل المثال الخدمات المعتمدة على الموقع (LBS location based service) وبث الفيديو الرقمي ، ويمكن أن تستخدم العربات أيضاً شبكات الخليوي (3G/4G) و WiFi.

3. تطبيقات شبكات العربات المتنقلة:

تتيح هذه الشبكات تنوعاً كبيراً من التطبيقات تفيد الإدارة، والشركات، والسائقين ومستخدمي العربات وكذلك المجالات المتعلقة بالأمن والسلامة، والتحكم بالمرور، والتسلية والترفيه. تصنف هذه التطبيقات حسب منتجي العربات إلى صنفين رئيسين هما: تطبيقات الأمان وتطبيقات الترفيه.

3-1. تطبيقات الأمان (Safety Applications):

هي التطبيقات الأكثر أهمية بين تطبيقات العربات المتحركة، وتهدف إلى تخفيض الإصابات والوفيات الناجمة عن حوادث المرور وتحسين السلامة العامة. خصوصاً أن الإحصائيات التي أجريت على أعداد الوفيات من جراء حوادث السير أعطت أعداداً كبيرة في مختلف أنحاء العالم، ففي سوريا مثلاً وفقاً لإحصائيات وزارة النقل بين عامي 2000 و2010 كما يبين الشكل (4)، نلاحظ مثلاً أن عدد الوفيات في عام 2007 وصل إلى 2818 شخصاً.



الشكل (4) إحصائية وزارة النقل عن الوفيات الناتجة عن حوادث السير بين عامي 2000-2010

وتصنف هذه التطبيقات بدورها إلى صنفين هما تطبيقات الأمان الحرج (Safety-critical) والتطبيقات المتعلقة بالأمان (Safety-related). يشمل الصنف الأول كل التطبيقات التي تستخدم في الحالات الخطرة والمتعلقة بحالات الحياة الحرجة مثل تطبيقات تجنب الاصطدام وتحذيرات الطرق المتجمدة، إضافة إلى الحالات الأقل خطورة مثل تحذيرات السرعة عند المنعطفات وتحذيرات منطقة عمل . أما الصنف الثاني فيشمل تطبيقات تحقيق أفضلية المرور والخدمات المتعلقة بالموقع. أحد أشهر أنواع هذه التطبيقات هو **خدمة e-call** [7] وهو مشروع طرحته المفوضية الأوروبية، ويهدف إلى تقديم المساعدة السريعة للسائقين عن طريق التشارك في حادث التصادم في أي مكان في دول الاتحاد الأوروبي. في حالة التعطل، تقوم العربة المجهزة بـ e-call باستدعاء أقرب مركز طوا رئ، ولو كان الركاب غير قادرين على الاتصال؛ بسبب إصابات تعرضوا لها خلال الحادث.

3-2. تطبيقات غير مرتبطة بالأمان (Non- Safety Applications):

تهدف هذه التطبيقات [8] إلى تأمين معلومات المرور وتحسين راحة القيادة بشكل رئيسي، وتتدرج معظم أنواع هذه التطبيقات تحت نوعين هما تطبيقات الرفاهية والتطبيقات الإدارية. من تطبيقات الرفاهية إعطاء معلومات عن حالة المرور الحالية وحالة الطقس، الاتصالات التفاعلية، الألعاب على الانترنت وخدمات المراسلة، خدمات الإعلان التجارية، ومعلومات عن محطات الوقود،..الخ. بينما تعد خدمة تحديد هوية العربات من أهم التطبيقات الإدارية؛ لأنها توفر وسيلة آمنة وسريعة لتوفير المعلومات من المركبات دون الحاجة لإيقافهم. ستساعد هذه الخدمة الشرطة في العديد من النواحي، مثل: التحقق من امتلاك السيارات الأوراق المطلوبة، اكتشاف المخالفات، وفي حال حدوثها، يتم إعطاء السائقين تقريراً عنها بشكل تلقائي.

4. متطلبات الأمن في شبكات العربات المتنقلة:

تشكل شبكات العربات المتنقلة كغيرها من الشبكات اللاسلكية هدفاً للكثير من الهجمات، لكن تعد هذه الشبكة آمنة إذا حققت متطلبات الأمن الآتية [8]:

1) التوافرية (Availability): وتعني توافر الخدمة لأية عقدة في الشبكة وفي أي وقت من زمن التطبيق.

2) المصادقة (Authentication): تعني أن مصدر الرسالة يجب أن يكون موثوقاً وكذلك المعلومات المتضمنة.

3) عدم التنصل (Non-Repudiation): تعني ضمان عدم إمكانية إنكار أي كيان لقيامه بإرسال أو استقبال رسالة ما، و يسهل إمكانية تحديد المهاجم بعد حدوث الهجوم وهو مايمنعه من التنصل من هجومه.

4) تكاملية الرسالة (Message Integrity): هو المتطلب الذي يكفل وصول الرسالة إلى الهدف دون أية تعديلات غير شرعية من قبل موجه وسيط غير مخول له ذلك أثناء عملية الإرسال.

5) الموثوقية (Confidentiality): يضمن تحقيق هذا المتطلب أن تبقى المعلومات المتبادلة ضمن الشبكة سرية وبعيدة عن متناول المستخدمين غير المخول لهم الوصول إليها.

إن تحقيق هذه المتطلبات في شبكة ما يجعل منها شبكة آمنة قادرة على تقديم الخدمة بالشكل الأفضل. إن الاعتماد على الاتصالات اللاسلكية في بيئة مفتوحة يجعل تحقيق الأمن واحدة من أكثر القضايا الحرجة في شبكات العربات المتنقلة، لذلك من الضروري حماية البيانات المرسلة من التعديل أو الإضافة التي قد تتم لتحقيق أغراض الدخلاء. وسنستعرض فيما يأتي تصنيفاً للهجومات التي تتعرض لها شبكات العربات المتنقلة.

5. أصناف الهجومات التي تتعرض لها شبكات العربات المتنقلة:

كما ذكرنا، يعد تحقيق أمن شبكات العربات المتنقلة واحداً من القضايا الهامة، لأن المعلومات تنتشر عبر وسط لاسلكي يكون عرضة للاختراق مما قد يؤدي إلى تغير في المعلومات المرسلة، وهذا ما ينعكس سلباً على أداء الشبكة. في هذا البحث يهمنا الهجومات التي تستهدف الرسالة تحديداً [9] ويصنف هذا النوع من الهجومات إلى الهجومات المشروحة تالياً.

5-1. هجوم إعادة الإرسال (Replay Attack) :

في هذا الهجوم يقوم المهاجم بإعادة إرسال معلومات تم إرسالها في وقت سابق بهدف الاستفادة من الحالة التي تخلقها هذه الرسالة. هدف هذا الهجوم أن يخلق تضارباً في الصلاحيات، ويمنع تحديد هويات العربات في الحوادث. لم تأخذ تقنيات الأمن في النسخة الأساسية للمعيار 802.11 بالحسبان هذا الهجوم إذ لم يتم استخدام رقم تسلسلي أو timestamps للرسائل والتي تعد من التقنيات الأساسية للحماية من هذا الهجوم.

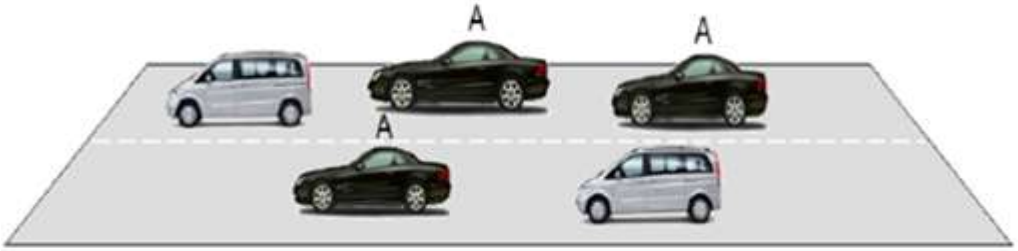
5-2. هجوم التعديل (Alteration Attack) :

يحدث هذا الهجوم عندما يقوم المهاجم بتعديل المعلومات الموجودة. ويتضمن هذا الهجوم تأخيراً في إرسال المعلومات أو إعادة إرسالها أو بالتعديل الفعلي في المعلومات.

5-3. هجوم سايبل (Sybil Attack):

وهو يتمثل بإرسال عدة رسائل من قبل المهاجم لكن بعدة هويات مختلفة [10]، هكذا يظهر المهاجم وكأنه أكثر من عقدة في الشبكة. يكون هذا الهجوم فعالاً إذا كان النظام يعتمد في توليد هويات العقد على آلية بسيطة، وإذا لم يستخدم هذا النظام طريقة موثوقة للتأكد من ربط الهويات بالكيانات المعرفة لها في الشبكة. يبين الشكل (5) كيفية

ظهور العقدة المهاجمة بأكثر من هوية ويقوم بإيهام العربات الأخرى بأن الطريق آمن عن طريق إرسال بعض الرسائل الكاذبة في تطبيق حالة المرور، رغم أن الصحيح هو وجود اختناق مروري.



الشكل(5) : هجوم سايبل

4 5. هجوم حذف الرسالة (Message Suppression Attack):

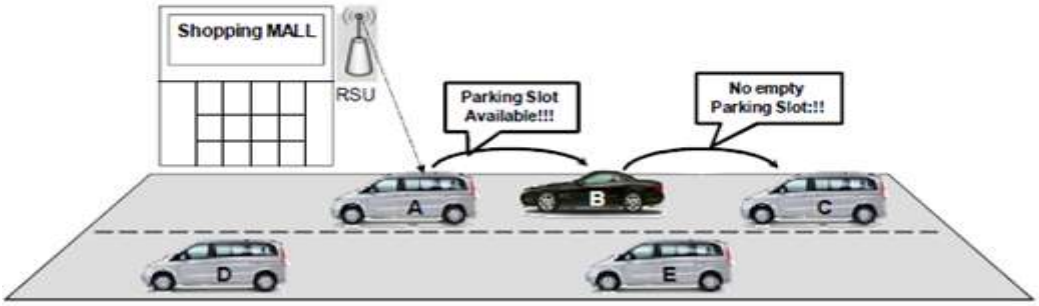
يقوم المهاجم بإسقاط الرسائل ضمن الشبكة، وقد يتسبب هذا الحذف بمنع وصول معلومات حرجة وهامة جداً إلى المستقبل. هدف هذا الهجوم هو منع تسجيل حالات التصادم الحاصلة على الطريق، أو منع وصول تقارير حدوث اصطدام إلى الوحدات على جانب الطريق، وهذا ما قد يتسبب بنتائج كارثية.

5 5. هجوم التزييف (Fabrication Attack):

يرسل المهاجم في هذا الهجوم معلومات مزيفة أو يدعي بأنه شخص آخر. ويتضمن هذا الهجوم تزييف رسائل أو تحذيرات أو شهادات أو هويات. فكما نعلم، تعد رسائل التحذير من الرسائل المهمة المستخدمة في تطبيقات الأمان؛ في حال حدوث خلل ما على الطريق، وإذا قام أحد المهاجمين بتغيير رسائل التحذير التي سترسل للتنبيه عن هذا الخلل، فإن العديد من الحوادث ستقع على الطريق [11]. يظهر الشكل (6) مثالاً عن هذا الهجوم، يستهدف فيه المهاجم (B) تطبيق الأمان، إذ يستقبل المهاجم (B) رسالة تحذير "منطقة عمل"، من عربة ما قريبة، فيقوم بتغيير مضمون هذه الرسالة، ويرسل رسالة "الطريق خالي"، للعربة (C).

الشكل (6): سيناريو هجوم المعلومات المزيفة على اتصال V2V

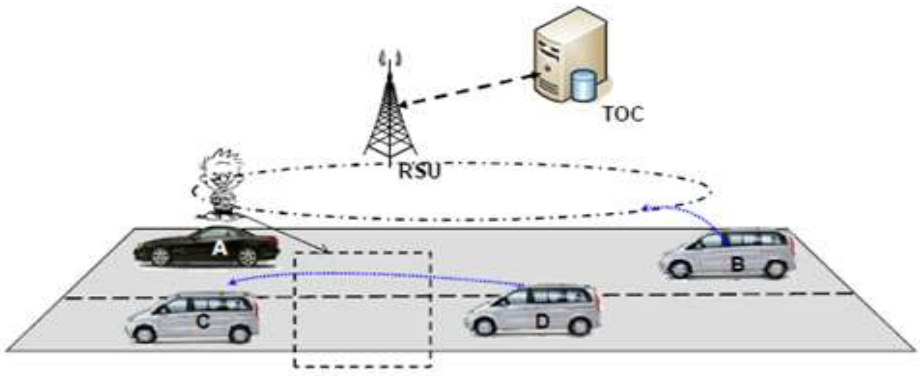
يستهدف هذا الهجوم أيضاً الرسائل المرسلة من الـRSU, والتي تؤمن راحة الركاب وتحسين نظام المرور [12] , بتزويدهم بمعلومات حول توافر مواقف السيارات في مراكز التسوق والمجمعات الرياضية. ويبين الشكل (7) هذا الهجوم، حيث يستقبل المستخدم (A) رسالة "موقف متاح للسيارات" من أحد وحدات جوانب الطريق بالقرب من مركز التسوق، فيرسل هذه الرسالة إلى السيارة المهاجمة (B)، والتي تقوم بتغيير محتوى الرسالة إلى "لا يوجد مكان لوقوف السيارة"، وتمررها إلى سيارة أخرى (C).



الشكل (7) : هجوم المعلومات المزيفة على الاتصال V2I

5-6. هجوم حجب الخدمة (Denial of Service) DoS:

يعد هذا الهجوم أحد أخطر الهجومات التي تتعرض لها الشبكة [13-15] ، لذا سنهتم في هذا البحث بدراسة هذا النوع من الهجومات. يحدث هذا الهجوم عندما يملك المهاجم القدرة على التحكم بمصادر العربة أو القدرة على التشويش على قناة الاتصال المستخدمة ضمن الشبكة، ليمنع بذلك المعلومات من الوصول. أي يعمل المهاجم على تعطيل وسط الاتصال الرئيسي مما يؤدي إلى عدم توفر الشبكة بعد ذلك للمستخدمين الشرعيين، وحرمانهم من الوصول إلى خدمات الشبكة. من أبسط الأمثلة على هذا الهجوم إذا كان المهاجم يريد أن يخلق حالة اختناق على الطريق، فإنه يفتعل حادثاً مع عربة أخرى و ينفذ هجوم DoS لمنع وصول رسالة الإنذار من الحادث إلى العقد القادمة باتجاه المنطقة التي وقع فيها الحادث. يظهر الشكل (8) سيناريو عن هذا الهجوم؛ يطلق المهاجم A هجوم DoS على الشبكة ويعطل كل أوساط الاتصال V2V و V2I، ونتيجةً لذلك لا يمكن للمستخدمين الشرعيين B-C-D التواصل مع بعضهم البعض ولا مع البنية التحتية.



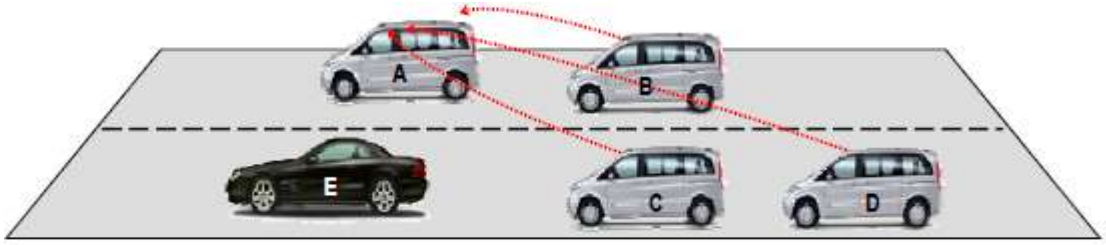
الشكل(8): هجوم حجب الخدمة

يمكن أن تشترك أكثر من عقدة في إطلاق هذا الهجوم وهو ما يسمى هجوم حجب الخدمة الموزع DDoS (Distributed Denial of Service). وسيكون دراسة تأثير هذا الهجوم هو تحديداً هدف بحثنا.

5-6-1. هجوم حجب الخدمة الموزع (Distributed Denial of Service):

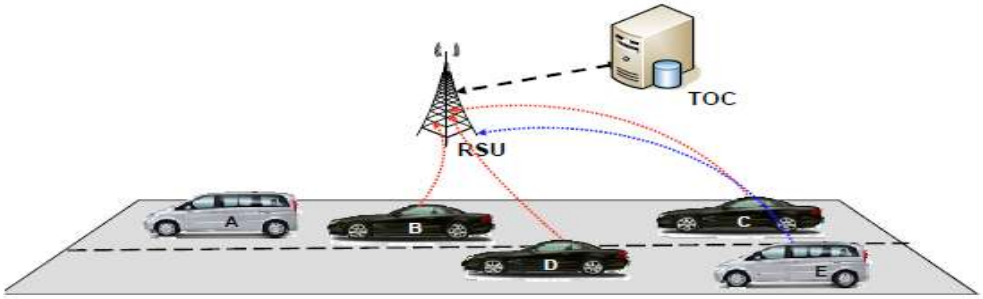
تعد الهجومات الأكثر حدة في بيئة العربات لأن آلية الهجوم تكمن في طريقة توزيعها [16]. إذ يطلق المهاجم في هذه الحالة الهجوم من مواقع مختلفة وقد يستخدم فترات مختلفة لإرسال الرسائل. تختلف طبيعة الرسالة وفترتها

الزمنية من عربة مهاجمة لأخرى. ويشرح الشكل (9) هجوم DDoS على مجموعه من العربات، حيث تطلق العربات المهاجمة (B,C,D) الهجوم على العقدة (A).



الشكل(9) : هجوم DDOS على الاتصال V2V

تقوم هذه العربات بإشغال القناة بشكل كامل مما يحجب جميع الخدمات عن العقدة A و يجعلها غير قادرة على استقبال أية رسالة. هذا ولا تنجو البنى التحتية من هذا الهجوم أيضاً، فقد يستهدف الهجوم إحداها ليمنع المستخدمين الشرعيين من الحصول على الخدمات، ويشرح الشكل (10) هجوم DDOS على البنية التحتية، حيث يطلق المهاجمون (B–C–D) الهجوم على البنية التحتية (RSU) من مواقع مختلفة، عندما تريد المركبات الأخرى (A–E) الوصول إلى الشبكة تكون الـ RSU في حالة حمل إضافي (overload). فيما يأتي قمنا بدراسة أداء الشبكة في حال عدم وجود هذا الهجوم ومن ثم قمنا بإطلاق هذا الهجوم، و قد طبقنا هذا الهجوم على سيناريوهين.



الشكل (10) : هجوم DDoS على الاتصال V2I

6. المحاكاة وإظهار النتائج

6-1. منطقة العمل:

تم اختيار منطقة العمل في مدينة جبلة بحيث يمتد المسار على كل المسارات المحيطة بين الكراجين القديم والجديد ويتخلل المسار دوار العمارة ودوار العلبي كما هو موضح بالشكل (11). يتضمن البرنامج أربع نقاط عمل وهي:

- **الأولى** : تنفيذ اتصال V2V في الحالة الطبيعية دون وجود هجوم .
- **الثانية** : يحوي عدة عقد مهاجمة على العربة التي تقوم بالإرسال .
- **الثالثة** : تنفيذ اتصال V2I في الحالة الطبيعية مع وجود هجوم.
- **الرابعة** : يتضمن عقد تقوم بالهجوم على وحدة الطريق.

الشكل (11) : البيئة المدروسة

سنقوم في هذه السيناريوهات بمقارنة النتائج بين الحالة الطبيعية وحالة الهجوم. لتحقيق هذا الهدف قمنا بإنشاء شبكة مكونة من 40 عقدة مع مساراتها وقمنا بتطبيق البروتوكول AODV كبروتوكول توجيه. حيث سندرس الاتصال V2V في السيناريوهين الأول والثاني، والاتصال V2I في السيناريوهين الثالث والرابع. ستتم دراسة تأثير هذا الهجوم من خلال عدد الرزم المرسلة والمستقبلة خلال واحدة الزمن والتي تمثل هنا بنفاذية الدخل (الاستقبال) IN Throughput وبنفاذية الخرج (الإرسال) OUT Throughput . وبالنتيجة حساب الرزم المسقطة (Drop packets) التي تشير بشكل واضح لتأثير هذا الهجوم على الخدمة كونها تدل على عدم وصول المعلومات المفترض وصولها للعقد المعنية بها من خلال هذه الشبكة.

6-2. نتائج المحاكاة

6-2-1 السيناريو الأول: اتصال V2V دون وجود هجوم

يبين الشكل (12) السيناريو المدروس.

الشكل (12) : سيناريو اتصال V2V المدروس

ويظهر الشكلان (13) و (14) عملية تبادل البيانات بعد المحاكاة. ويظهر الشكل (15) ملف الحركية الخاص بالسيناريو الأول .

الشكل (13) : إرسال البيانات

الشكل (14) : رسالة الإفادة بالاستلام ACK

```
802.11p RX   46977129 1740 QoS_DATA   <2 6> <2 6 6> 2015702 100 0 NONE   174
802.11p TX   46979189 640 ACK   <0 0> <6 2 2> 2015703 14 0 NONE   174
802.11p RX   46979268 590 ACK   <0 0> <6 2 2> 2015757 14 0 NONE   174
802.11p TX   46981088 1840 QoS_DATA   <2 6> <2 6 6> 2007350 100 0 NONE   174
802.11p RX   46981217 1740 QoS_DATA   <2 6> <2 6 6> 2015863 100 0 NONE   174
802.11p TX   46983277 640 ACK   <0 0> <6 2 2> 2015864 14 0 NONE   174
802.11p RX   46983356 590 ACK   <0 0> <6 2 2> 2015918 14 0 NONE   174
802.11p TX   46984916 1840 QoS_DATA   <2 6> <2 6 6> 2007511 100 0 NONE   174
802.11p RX   46985045 1740 QoS_DATA   <2 6> <2 6 6> 2016024 100 0 NONE   174
802.11p TX   46987105 640 ACK   <0 0> <6 2 2> 2016025 14 0 NONE   174
802.11p RX   46987184 590 ACK   <0 0> <6 2 2> 2016079 14 0 NONE   174
802.11p TX   46988744 1840 QoS_DATA   <2 6> <2 6 6> 2007672 100 0 NONE   174
802.11p RX   46988873 1740 QoS_DATA   <2 6> <2 6 6> 2016237 100 0 NONE   174
802.11p TX   46990933 640 ACK   <0 0> <6 2 2> 2016238 14 0 NONE   174
802.11p RX   46991012 590 ACK   <0 0> <6 2 2> 2016292 14 0 NONE   174
802.11p TX   46992182 1840 QoS_DATA   <2 6> <2 6 6> 2007832 100 0 NONE   174
802.11p RX   46992311 1740 QoS_DATA   <2 6> <2 6 6> 2016398 100 0 NONE   174
802.11p TX   46994371 640 ACK   <0 0> <6 2 2> 2016399 14 0 NONE   174
802.11p RX   46994450 590 ACK   <0 0> <6 2 2> 2016401 14 0 NONE   174
802.11p TX   46995750 1840 QoS_DATA   <2 6> <2 6 6> 2007993 100 0 NONE   174
802.11p RX   46995879 1740 QoS_DATA   <2 6> <2 6 6> 2016559 100 0 NONE   174
802.11p TX   46997939 640 ACK   <0 0> <6 2 2> 2016560 14 0 NONE   174
802.11p RX   46998018 590 ACK   <0 0> <6 2 2> 2016562 14 0 NONE   174
802.11p BTX   47140580 2560 BCON   <0 0> <2 0 0> 2022699 156 0 NONE   178
802.11p BRX   47140665 2480 BCON   <0 0> <2 3 0> 2022857 156 0 NONE   178
```

الشكل(15) : جزء ملف حركية السيناريو الأول

لنأخذ سطراً منه، وليكن السطر المشار إليه:

802.11p TX 46984916 1840 QoS_DATA <2 6> <2 6 6 > 2007511 100 0 NONE 174

Field : 1 2 3 4 5 6 7 8 9 10 11 12

1. الحقل الأول <protocol> : البروتوكول المستخدم وهو 802.11p
2. الحقل الثاني <event type>: نوع الحدث وهو هنا ارسال بيانات TX.
3. الحقل الثالث <time (unit: tick) at which the event is started>: يدل هذا الحقل على الزمن الذي يبدأ فيه الحدث وهنا يدل على بدء الإرسال بالزمن 46984916 ميكرو ثانية.
4. الحقل الرابع <duration (unit: tick) of this vent>: يدل على زمن استمرار الحدث هنا 1840 ميكرو ثانية.
5. الحقل الخامس <packet type>: نوع رزمة البيانات المرسله وهي هنا QoS_DATA.
6. الحقل السادس <source/destination node IDs based on the IP addresses>: يدل هذا الحقل على المصدر و الوجهة اعتماداً على عنوان الـ IP وهي هنا < 6 2> أي المصدر هو العقدة 2 والوجهة هي العقدة (6).

7. الحقل السابع <transmitted/received node IDs based on the MAC addresses>: يدل هذا الحقل على كل من العقدة المرسلة (المصدر) والمستقبلة (الوجهة) اعتماداً على عنوان الـ MAC وهي هنا <6 6 2> أي تم الإرسال من العقدة (2) إلى العقدة (6)، وتم الاستقبال الفعلي في العقدة (6). مثلاً في حال وجود عقدة وسيطة بين العقدتين (2 و 6)، وفرضاً هي العقدة(1)، لكانت البيانات <6 1 2> أي تم الإرسال من العقدة (2) إلى العقدة (6) بعد المرور بالعقدة (1).

8. الحقل الثامن <packet's ID>: معرف الرزمة وهي هنا 2007511.

9. الحقل التاسع<packet's length (unit: byte)>: يدل هذا الحقل على طول رزمة البيانات وهي هنا 100.

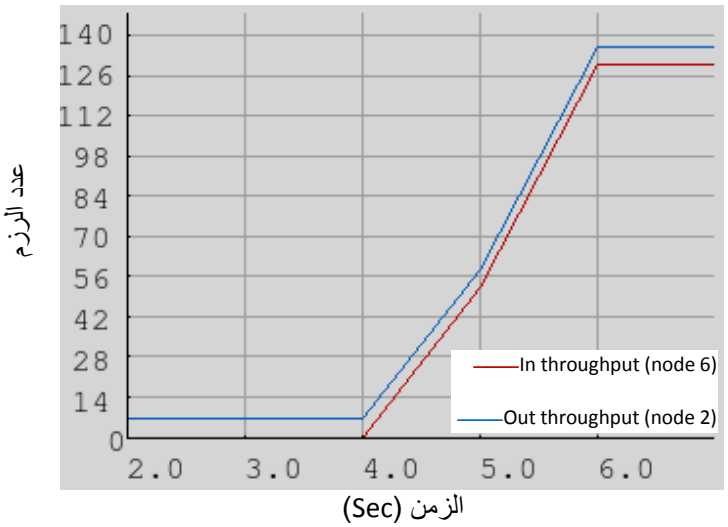
10. الحقل العاشر< count of successive retransmissions>: يدل على عدد الرسائل التي تم إعادة إرسالها بنجاح وهي هنا 0، وهذا يعني بأننا لم نحتج أصلاً لإعادة إرسال الرسالة.

11. الحقل الحادي عشر <drop reason>: سبب إسقاط الرسالة وهنا none لأن الرسالة استقبلت بنجاح ولم يتم إسقاطها.

12. الحقل الثاني عشر <frequency channel (for 802.11/OPHY/GPRS protocol)>: يدل على تردد القناة وهي هنا 174.

سنقوم بدراسة البارمترات الآتية :

1- In\out throughput: سندرس في هذا السيناريو بارامتر **out throughput** للعقدة المرسلة وهي(2)، وبارامتر **in throughput** للعقدة المستقبلة وهي(6). تظهر نتائج المحاكاة المخطط البياني الآتي:



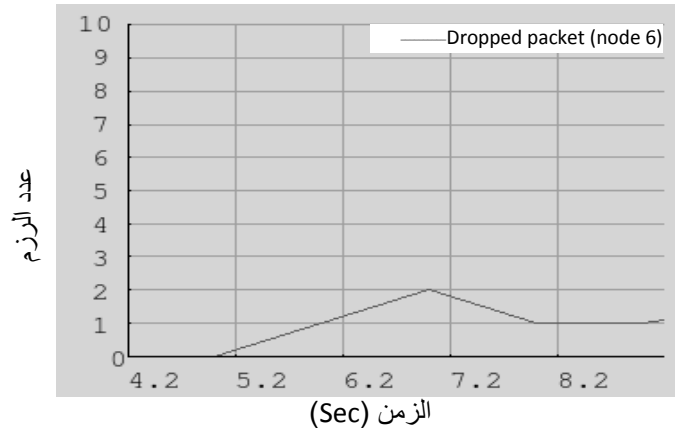
الشكل (16) : حركية المرسل والمستقبل في السيناريو الأول

نلاحظ أن عدد الرسائل المرسلة خلال الزمن (0 -4 sec) يكون ثابتاً، وعند هذا الزمن (4 sec) تبدأ العقدة (6) بالاستقبال فيأخذ كل من البارامترين نافذية الدخل/الخرج **in\out throughput** بالازدياد مع الزمن حتى اللحظة (6sec) يبدأ عندها البارامترين بالثبات، ونلاحظ من الشكل السابق أن عدد الرسائل المرسلة في لحظة ما

أكبر بقليل من عدد الرسائل المستقبلة، ففي اللحظة (5sec) نلاحظ أن عدد الرسائل المرسلة (56 رسالة)، بينما كان عدد الرسائل المستقبلة (50 رسالة) تقريباً، وبالتالي يوجد لدينا إسقاط بسيط لبعض الرزم المستقبلة وهذا محتمل الحدوث في الشبكات اللاسلكية بشكل طبيعي.

2- عدد الرزم المسقطة (Number of drop packet):

من دراسة البارمتر الأول وجدنا أنه حدث إسقاط لبعض رزم البيانات وتعطي نتائج المحاكاة المخطط البياني الآتي.



الشكل (17) : الرزم المهملة في السيناريو الأول للعقدة (6)

هذه الرزم المهملة هي السبب في الاختلاف بين البارامترين in-out throughput .

6-2-2 السيناريو الثاني: اتصال V2V بعد تنفيذ الهجوم

في هذا السيناريو قمنا بتطبيق الهجوم من خلال أربع عقد هي (7، 8، 3، 1)، حيث تقوم هذه العقد بإرسال بيانات للعقدة (2) على نفس المنفذ وفي فتَرات زمينة متقاربة جداً (أجزاء من الميللي ثانية) فتؤدي إلى الضغط على العقدة (2) التي تقوم بإرسال بيانات للعقدة (6)، يؤدي هذا الضغط إلى إهمال الرسائل المرسلة من (2) إلى (6) في هذه الفترة الزمنية. تعطي محاكاة هذا السيناريو ملف الحركية الموضح بالشكل (18).

```
802.11p TX  18506567 1840 QoS_DATA  <3 2> <3 2 2> 209 100 0 NONE  174
802.11p TX  18506567 1840 QoS_DATA  <7 2> <7 2 2> 103 100 0 NONE  174
802.11p DROP  18506568 1840 QoS_DATA  <8 2> <8 2 2> 4813214 216 0 COLL  174
802.11p DROP  18506568 1840 QoS_DATA  <8 2> <8 3 2> 4813214 216 0 RXERR  174
802.11p DROP  18506570 1840 QoS_DATA  <8 2> <8 7 2> 4813214 216 0 RXERR  174
802.11p DROP  18506570 1840 QoS_DATA  <7 2> <7 2 2> 4813215 216 0 COLL  174
802.11p DROP  18506571 1840 QoS_DATA  <3 2> <3 7 2> 4813216 216 0 RXERR  174
802.11p DROP  18506571 1840 QoS_DATA  <3 2> <3 8 2> 4813216 216 0 RXERR  174
802.11p DROP  18506571 1840 QoS_DATA  <7 2> <7 3 2> 4813215 216 0 RXERR  174
802.11p DROP  18506572 1840 QoS_DATA  <7 2> <7 1 2> 4813215 216 28704 COLL  174
802.11p DROP  18506572 1840 QoS_DATA  <3 2> <3 2 2> 4813216 216 0 RXERR  174
802.11p DROP  18506573 1840 QoS_DATA  <7 2> <7 8 2> 4813215 216 0 RXERR  174
802.11p DROP  18506575 1840 QoS_DATA  <8 2> <8 1 2> 4813214 216 28704 COLL  174
802.11p DROP  18506576 1840 QoS_DATA  <3 2> <3 1 2> 4813216 216 28704 RXERR  174
802.11p TX  18509001 1840 QoS_DATA  <1 2> <1 2 2> 6 100 0 NONE  174
802.11p RX  18509107 1740 QoS_DATA  <1 2> <1 2 2> 4814311 100 0 NONE  174
802.11p TX  18511167 640 ACK  <0 0> <2 1 1> 4814312 14 0 NONE  174
802.11p RX  18511223 590 ACK  <0 0> <2 1 1> 4814632 14 0 NONE  174
802.11p TX  18512653 1840 QoS_DATA  <1 2> <1 2 2> 7 100 0 NONE  174
802.11p RX  18512759 1740 QoS_DATA  <1 2> <1 2 2> 4815259 100 0 NONE  174
802.11p TX  18514819 640 ACK  <0 0> <2 1 1> 4815260 14 0 NONE  174
802.11p RX  18514875 590 ACK  <0 0> <2 1 1> 4815580 14 0 NONE  174
```

الشكل(18) : ملف حركية السيناريو الثاني

802.11p DROP 18506575 1840 QoS_DATA <8 2> <8 1 2> 4813214 216 28704 COLL 174

802.11p DROP 18506576 1840 QoS_DATA <3 2> <3 1 2> 4813216 216 28704 RXERR 174

بالمقارنة مع سطر من ملف الحركية للسيناريو الاول:

802.11p TX 46984916 1840 QoS_DATA <2 6> <2 6 6 > 2007511 100 0 NONE 174

نلاحظ: اختلاف ملف الحركية في حالة الهجوم عن ملف الحركية في الحالة الطبيعية حيث يختلف السطران السابقان من ملف الحركية للهجوم بالحقول الآتية:

1. الحقل الثاني <event type>: حيث هنا نوع الحدث هو **DROP**، أي حدوث إهمال لرزم البيانات (إسقاطها).

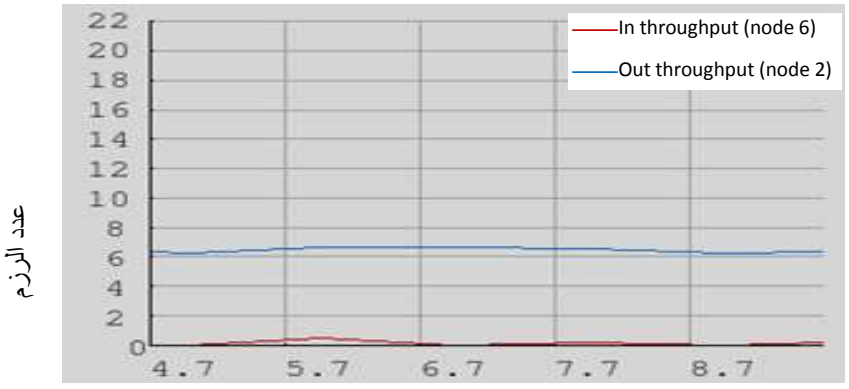
2. الحقل العاشر < count of successive retransmissions>: حيث هنا كان عدد الرسائل المعاد إرسالها هو 28704، بينما كان في السيناريو الأول صفر؛ وذلك لأننا في حالة الهجوم احتجنا إلى عمليات إعادة إرسال كثيرة بسبب إهمال رزم البيانات أو عدم وصولها بشكل ناجح وعمليات إعادة الإرسال هذه سوف تضغط على الشبكة مؤدية إلى الازدحام والذي هو هدف الهجوم.

3. الحقل الحادي عشر<drop reason>: يدل هذا الحقل على سبب حدوث الفشل (إسقاط رزم البيانات) وفي السيناريو الأول كان محتوى هذا الحقل هو (NONE) حيث دل على عدم وجود فشل (إسقاط لرزم البيانات)، بينما في سيناريو الهجوم فإن سبب الفشل هنا هو إما تصادم البيانات المعبر عنها بمحتوى الحقل (COLL) أو بسبب عمليات إعادة الإرسال المتكررة المعبر عنها بالمحتوى (RXERR).

وسنقوم في هذا السيناريو بدراسة البارمترات المدروسة في السيناريو السابق ، لنقوم لاحقاً بمقارنتها.

1- IN\OUT throughput:

تعطي محاكاة السيناريو الثاني المخططات البيانية الآتية:



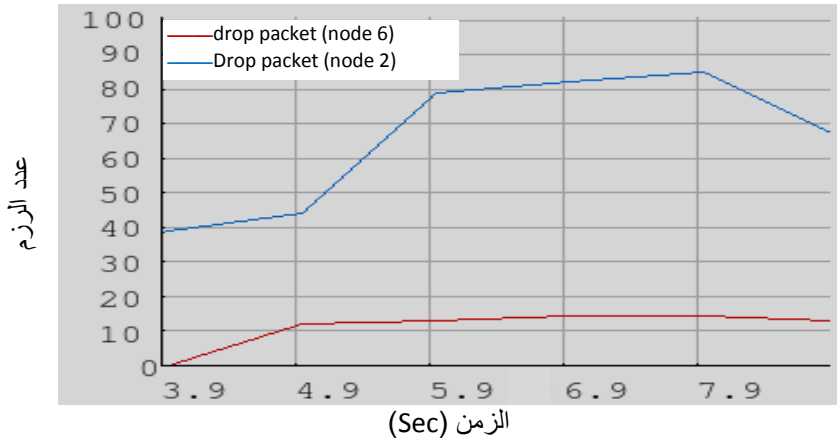
الشكل (19) : حركية المرسل والمستقبل في السيناريو الثاني

نلاحظ من المخطط البياني أن عدد الرسائل المرسلة من العقدة (2) (in throughput)، وعدد الرسائل المستقبلة في العقدة (6) (out throughput) قد انخفض بشكل ملحوظ نتيجة تطبيق الهجوم الذي أدى إلى الضغط على الشبكة بالمقارنة مع السيناريو الأول، وبمقارنة الشكل (19) مع الشكل(16) نلاحظ مايلي: أخذ البارامتران (in\out throughput) في السيناريو الأول بالثبات بعد الزمن (6sec) على القيم (128\138) على الترتيب، بينما

في السيناريو الثاني الذي طبق فيه الهجوم انخفض البارامتر out throughput للعقدة (2) إلى القيمة(6) وذلك بدءاً من الزمن (4sec)، وأخذ بالثبات على هذه القيمة.

أما البارامتر in throughput للعقدة (6) فانخفاضه كان أكبر بكثير وكاد يصل إلى القيمة صفر في بعض اللحظات (عدم وجود أي استقبال) وأخذ قيم لاتزيد عن (1) وذلك بسبب تأثير الهجوم على الإرسال والاستقبال.

2- Number of drop Packet عدد رزم البيانات التي تم اسقاطها : يدل هذا البارامتر على عدد رزم البيانات التي تم إسقاطها وقمنا بدراسته في هذا السيناريو لأنه من تأثير تطبيق الهجوم هو حدوث هذا الإسقاط لرزم البيانات. ويبين تنفيذ المحاكاة في الشكل (20) هذا البارامتر.



الشكل (20) : الرزم التي تم اسقاطها في الشبكة نتيجة وجود الهجوم

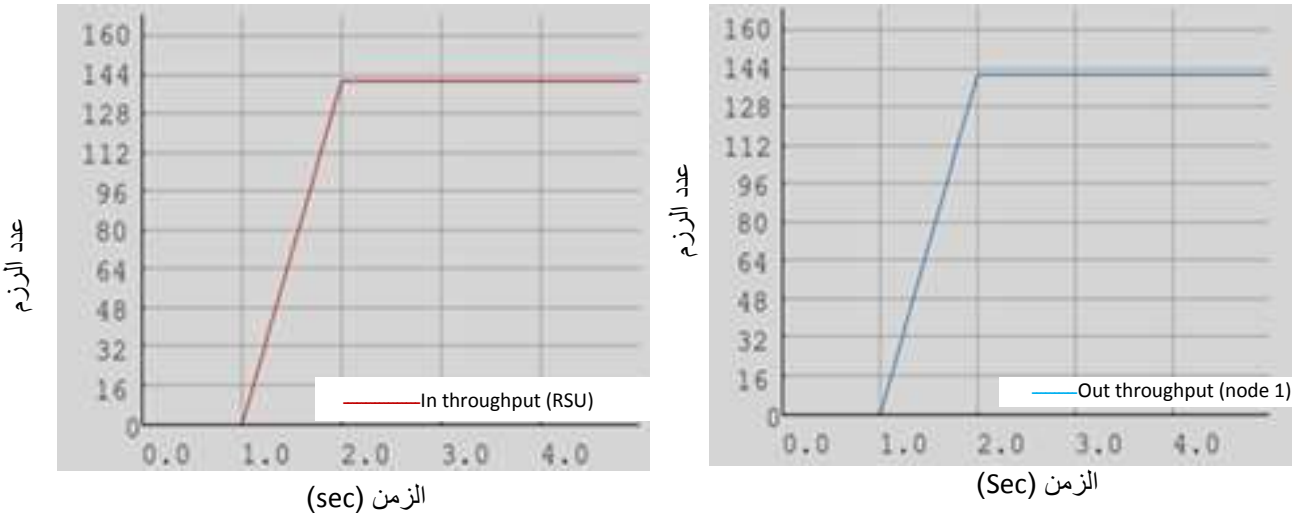
يظهر المخطط السابق أن الهجوم سبب ازدياداً في الرزم المهملة بشكل ملحوظ للعقدة المرسلة والتي تعرضت للهجوم مع الزمن حيث وصل عدد الرزم المهملة إلى (88 رزمة تقريباً) عند اللحظة (7.9sec) .

6-2-3 السيناريو الثالث: اتصالV2I دون وجود هجوم

الشكل (21) : سيناريو اتصال V2I المدروس

في هذا السيناريو تقوم العقدة (1) بطلب خدمة من وحدة الطريق الجانبية وتقوم وحدة الطريق الجانبية بتزويدها بالخدمة المطلوبة دون أية مشاكل . يظهر الشكلان (22)، (23) الحركية المتبادلة بين الـ RSU والعربة (1).

نلاحظ من الشكل أن عدد الرسائل المرسلة خلال الزمن (out throughput) من العقده (1) مساوية لعدد الرسائل المستقبلة (in throughput) في وحدة الطريق الجانبية. ذلك يدل على إرسال واستقبال سليم دون وجود أية مشاكل ولا يوجد أي رسائل مهملة حيث وصلت قيمة كل من البارمترين إلى 144 باللحظة (2 sec) وأخذت بالثبات، أما ملف الحركية فيظهر آلية تبادل البيانات التي تتم بشكل طبيعي جداً كما في الشكل(24). حيث تدل القيم الموجودة في الملف أن الإرسال تم من العقدة (1) والاستقبال الفعلي تم في العقدة (3) والتي هي وحدة الطريق الجانبية بدون وجود حاجة لإعادة الإرسال (الحقل العاشر= 0) ودون وجود أي رزم مهملة (الحقل 11= NONE).



الشكل (22) : In Throughput لوحدة الطريق الجانبية **الشكل (23) : Out Throughput للعقدة 1**

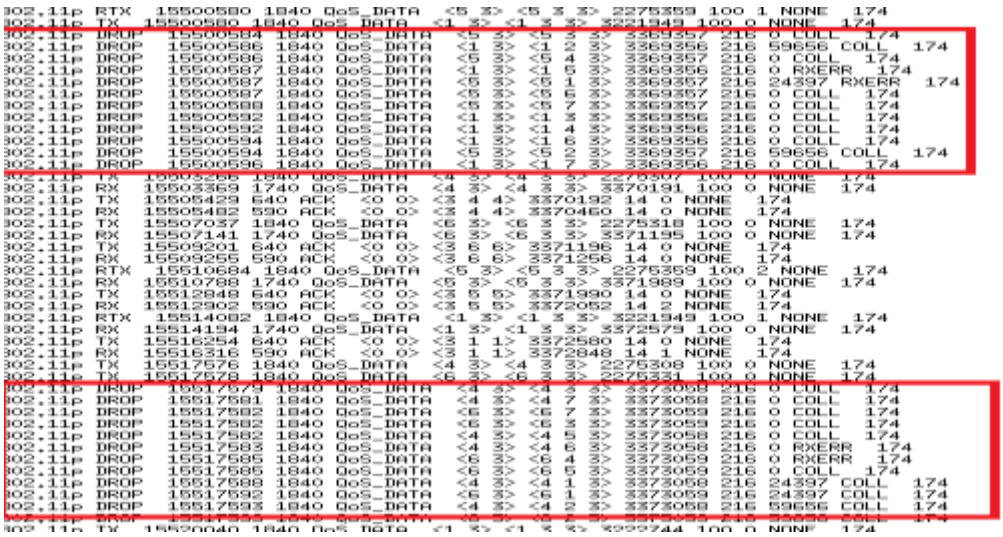
```
802.11p RX  10557637 1740 QoS_DATA  <1 3> <1 3 3> 915365 100 0 NONE  174
802.11p TX  10559697 640 ACK  <0 0> <3 1 1> 915366 14 0 NONE  174
802.11p RX  10559756 590 ACK  <0 0> <3 1 1> 915370 14 0 NONE  174
802.11p TX  10561056 1840 QoS_DATA  <1 3> <1 3 3> 910037 100 0 NONE  174
802.11p TX  10563225 640 ACK  <0 0> <3 1 1> 915687 14 0 NONE  174
802.11p RX  10563284 590 ACK  <0 0> <3 1 1> 915691 14 0 NONE  174
802.11p TX  10564714 1840 QoS_DATA  <1 3> <1 3 3> 910038 100 0 NONE  174
802.11p RX  10564823 1740 QoS_DATA  <1 3> <1 3 3> 916007 100 0 NONE  174
802.11p TX  10566883 640 ACK  <0 0> <3 1 1> 916008 14 0 NONE  174
802.11p RX  10566942 590 ACK  <0 0> <3 1 1> 916012 14 0 NONE  174
802.11p TX  10568112 1840 QoS_DATA  <1 3> <1 3 3> 910039 100 0 NONE  174
802.11p RX  10568221 1740 QoS_DATA  <1 3> <1 3 3> 916224 100 0 NONE  174
802.11p TX  10570281 640 ACK  <0 0> <3 1 1> 916225 14 0 NONE  174
802.11p RX  10570340 590 ACK  <0 0> <3 1 1> 916333 14 0 NONE  174
802.11p TX  10571640 1840 QoS_DATA  <1 3> <1 3 3> 910040 100 0 NONE  174
802.11p RX  10571749 1740 QoS_DATA  <1 3> <1 3 3> 916545 100 0 NONE  174
802.11p RX  10573868 590 ACK  <0 0> <3 1 1> 916654 14 0 NONE  174
```

الشكل(24) : ملف حركية السيناريو الثاني

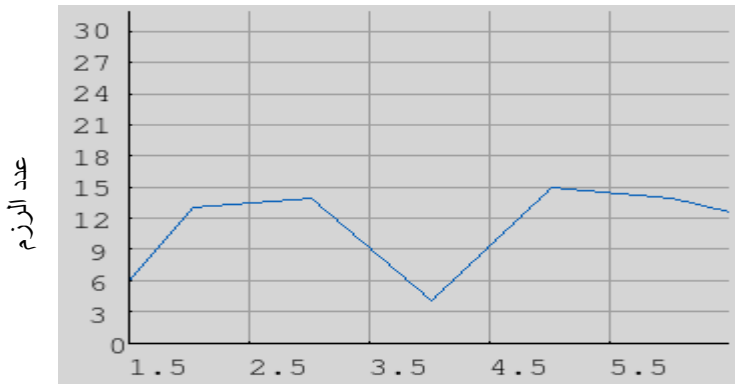
6-2-4 السيناريو الرابع : اتصال V2I بعد تنفيذ الهجوم

في هذا السيناريو تقوم العربات (4، 5، 6، 7) بمهاجمة وحدة الطريق الجانبية (node 3) من خلال إرسال البيانات لها في فترات زمنية متقاربة جداً على نفس المنفذ فتضغط على الشبكة لتمنع وحدة الطريق الجانبية من استقبال رسالة طلب العقدة (1) وتقوم بإسقاط هذه الرسالة. بعد المحاكاة نحصل على ملف الحركية الموضح في الشكل (25). يظهر ملف الحركية إهمال الرزم المرسلة من عقدة الى أخرى (field 6 = < * ** >) بسبب حدوث تصادم ووجود تكرار للرسائل (إعادة إرسال) (field 11 = COLL\RXERR). ويظهر الشكل (26) البارمتر المدروس في هذا السيناريو وهو عدد الرزم المسقطة **NUMBER OF DROP BACKCET**، حيث نلاحظ أن عدد الرزم

المسقطة أخذ بالارتفاع من الثانية الأولى ليصل إلى أعلى قيمه له بالثانية (5 Sec) حيث وصل إلى (15) ثم عاد للانخفاض والارتفاع حسب تأثير السيارات المهاجمة والضغط الذي تؤديه على الشبكة.



الشكل (25) : ملف الحركية للسيناريو الرابع



الشكل (26) : الرزم المهملة لـ RSU

الاستنتاجات والتوصيات

قمنا في هذا البحث بدراسة تأثير هجوم حجب الخدمة الموزع على شبكة VANET ضمن مدينة وهذه الدراسة شملت تأثير الهجوم في حال كان هدف الهجوم عربة وفي حالة كان هدف الهجوم هو الوحدة الموجودة على جانب الطريق، وأثبتنا من خلال إجراء المحاكاة باستخدام بيئة المحاكاة NCTUns مايلي:

1. يؤثر الهجوم بشكل ملحوظ على عدد الرزم الواصلة بشكل صحيح أي يتسبب بزيادة عدد الرزم المهملة مسبباً انقطاع الخدمة عن العربة الضحية.
2. يتسبب الهجوم على RSU بمنعها من استقبال رسالة طلب العقد للخدمة وبالتالي إسقاط هذه الرسالة.

وبالنتيجة نجد أنّ هذا الهجوم يجعل الشبكة غير فعالة كونه يتسبب في منع وصول العقد للخدمة التي تريدها و يمنع وحدات جانب الطرق من القيام بدورها بتقديم الخدمة لعقد الشبكة.نتيجة لهذا التأثير الملحوظ للهجوم ينصح باستخدام تقنيات تسمح بتقليص فعالية هذا الهجوم من خلال استخدام تقنيات تبديل القنوات التي تسمح باستبدال القناة المستخدمة للإرسال الأمر الذي يسمح بالحصول على الخدمة في حال التعرض للهجوم.

المراجع:

[1] S-Y Wang and C-C Lin, "*NCTUns 5.0: A Network Simulator for IEEE 802.11(p) and 1609 Wireless Vehicular Network Researches*," Vehicular Technology Conference, 2008. VTC2008-Fall. IEEE 68th, pp.1-2, 21-24 Sept.

[2] S.Y Wang, C.L Chou,. C. C Lin, and C.H. Huang "*The Protocol Developer Manual for the NCTUns 6.0 Network Simulator and Emulator*", National Chiao Tung University, Tajwan 2010.

[3] Karim Rizwanul, "*Security issues in VANET*", Master's Thesis, BRAC University, Dhaka, Bangladesh, 16 April, 2010.

[4] J. M. de Fuentes, A. I. González-Tablas, and A. Ribagorda, "*Overview of security issues in Vehicular Ad-hoc Networks*", Handbook of Research on Mobility and Computing: Evolving Technologies and Ubiquitous Impacts,Ch-56, 2011.

[5] Y. Gadkari, and B. Sambre, "*VANET: Routing Protocols, Security Issues and Simulation Tools*", In IOSR Journal of Computer Engineering (IOSRJCE), Vol 3, PP 28-38, July-Aug. 2012.

[6] F. Neves, A. Cardote, R. Moreira, S. Sargento,"*Real-world evaluation of IEEE 802.11p for vehicular networks*" Eighth ACM International Workshop on Vehicular Inter-Networking (2011), pp. 89–90

[7] Digital Agenda for Europe, http://ec.europa.eu/digital-agenda/en/ecall-time-saved-lives-saved. last access date 20/4/2015

[8] P. Yadav, and D. Chaurse , "*Survey and analysis of security issues in Vehicular AdHoc network*", International Journal of Electronics and Communication Engineering & Technology (IJECET), ISSN 0976 –6464(Print), ISSN 0976 – 6472(Online), Volume 5, Issue 3, March (2014), pp. 70-78

[9] A. Rawat, S. Sharma, and R. Sushil," *VANET: Security Attacks and its possible solutions*" , In Journal of Information and Operations Management, Vol 3, pp:301-304, 2012.

[10] G. Guette and B. Ducourthial,"*On the sybil attack detection in VANET*", IEEE International Conference on Mobile Adhoc and Sensor Systems, 2007.

[11] T. Leinmuller, E. Schoch, F. Kargl and C. Maihofer, "*Improved security in Geographic ad hoc routing through autonomous Position Verification*", Proceedings of the 3rd international workshop on Vehicular ad hoc networks, 2006.

[12] I. A. Soomro, H.B.Hasbullah and J.lb.Ab Manan,"*User requirements model for vehicular ad hoc network applications*", International Symposium on Information Technology 2010 (ITSim 2010), Malaysia.

[13] I.A. Soomro, H.B.Hasbullah, and J.lb.Ab Manan, "*Denial of Service (DOS) Attack and Its Possible Solutions in VANET*",WASET issue 65, april 2010 ISSN 2070-3724.

[14] Kevin J. Houle and George M. Weaver, "*Trends in Denial of Service Attack Technology*", CERT® Coordination Center 2001.

[15] B. Parno and A. Perrig, "*Challenges in Securing Vehicular Networks*", Hot Topics in Networks (HotNets-IV), 2005

[16] V. Paxson. "*An analysis of using reflectors for distributed denial-of-service attacks*". ACM Computer Communications Review (CCR), 31(3), July 2001.