مجلة جامعة تشرين للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (39) العدد (1) 2017
Tishreen University Journal for Research and Scientific Studies - Engineering Sciences Series Vol. (39) No. (1) 2017

دراسة تأثير هجوم الثقوب السوداء على أداء بروتوكولات التوجيه AODV وOLSR في شبكات AD-HOC ذات الحمل المرتفع

الدكتور محمد ياسين صبيح*

(تاريخ الإيداع 9 / 10 / 2016. قُبِل للنشر في 14/ 2 / 2017)

□ ملخّص □

إن شبكات الـ MANETs (Mobile Ad-Hoc Networks) اللاسلكية عبارة عن مجموعة من العقد اللاسلكية القادرة على الاتصال مع بعضها خلال الحركة والثبات، دون الحاجة إلى وجود أية نقاط دخول مركزية، أو بنية تحتية ثابتة. تعمل هذه العقد كموجهات قادرة على الحركة بحرية وبسرعات مختلفة. من مشاكل هذه التقنية، الضعف الأمني وحمايتها من الاختراق والهجمات، نتيجة عدم وجود نقطة تحكم مركزية قادرة على إدارة الاتصالات. هجمات الثقب الأسود هي واحدة من الهجمات الخطيرة التي تستهدف شبكات AD_HOC اللاسلكية من خلال نقطة مزيفة تستطيع امتصاص البيانات وارسالها إلى مكان آخر أو إهمالها. من هنا سندرس تأثير الثقب الأسود على أداء بروتوكول التوجيه التفاعلي AODV وعلى بروتوكول التوجيه غير التفاعلي OLSR من اجل عدد متغير من العقد المتحركة بسرعات مختلف في بيئة ذات حمل عال.

الكلمات المفتاحية : الشبكات اللاسلكية Manets (Mobile Ad-Hoc Networks)– هجوم الثقب الأسود .Black Hole Attack –بروتوكول AODV –بروتوكول OLSR.

* مدرس –قسم النظم والشبكات الحاسوبية– كلية الهندسة المعلوماتية– جامعة تشرين– اللاذقية– سورية .

مجلة جامعة تشرين للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (39) العدد (1) 2017
Tishreen University Journal for Research and Scientific Studies - Engineering Sciences Series Vol. (39) No. (1) 2017

A Study of the Effect of Black Holes Attacks on the Performance of Routing Protocols: AODV and OLSR in High-Load AD-HOC Networks.

Dr. Mohammad Yassin Sobeih *

(Received 9 / 10 / 2016. Accepted 14 / 2 / 2017)

□ ABSTRACT □

MANET is a set of wireless nodes that can communicate with each other through movement and stability, without the need for the existence of any central entry points, or fixed infrastructure. These nodes operate as routers, which are able to move freely with different speeds. These networks suffer from weaknesses such as poor security and protection against intrusion attacks because a central control point that manages communications among nodes does not exist.

Black hole attack is one of the most serious attacks that target Ad-HOC networks through a false point that can neglect or absorb the data and send it to another place

Hence, we investigate the influence of the black hole attack on the performance of interactive routing protocol AODV and the non-interactive OLSR for a variable number of nodes moving with different speeds in a high load environment.

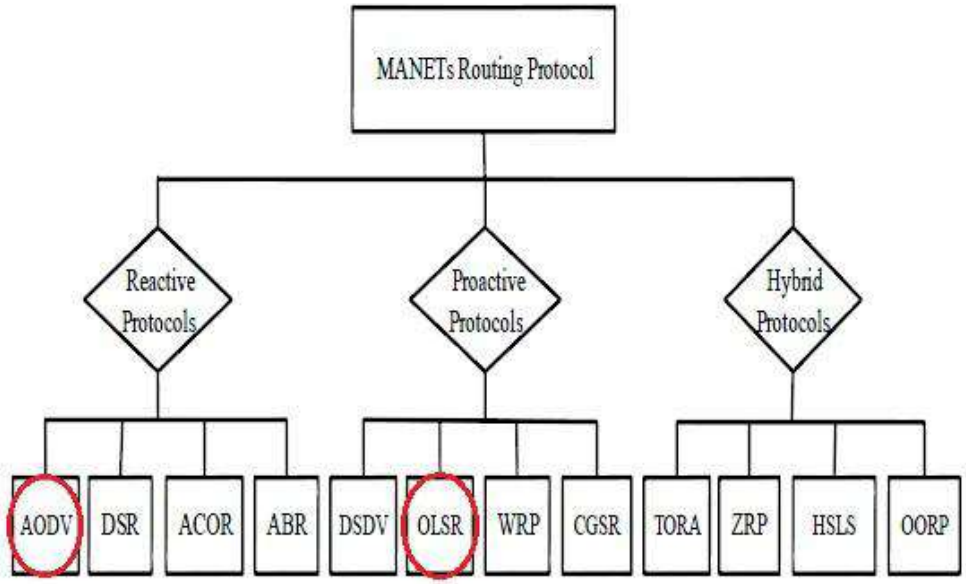
Key Words: MANETs (Mobile Ad-Hoc Networks). Protocol (AODV), Protocol (OLSR) - Black Hole Attack.

* **Assistant Professor- System and Network Computing Department-Faculty of Information Engineering- Lattakia-Tishreen University- Lattakia- Syria.**

مقدمة

ان شبكة MANETs اللاسلكية، عبارة عن مجموعة من الأجهزة المحمولة، التي يمكنها التواصل مع بعضها، دون وجود أية إدارة محددة مسبقاً، ودون وجود بنية تحتية ثابتة، أو رقابة مركزية، مما يجعلها توفر الاتصال بين المستخدمين دون قيود. حيث تعمل العقد (الحواسيب) كموجه، ومضيف، وتعيد توجيه الرزم إلى العقد المرئية بالنسبة لها. كما أنها تملك طوبولوجيا متغيرة باستمرار، نتيجة انقطاع الاتصال بين العقد، وهذا يعتبر أمراً اعتيادياً في هذه الشبكات، كما ترتبط عناوين العقد بالأجهزة وليس بطوبولوجيا الشبكة (لأن العناوين لا تدل على الموقع).

يوجد العديد من بروتوكولات التوجيه في شبكات ال MANETs اللاسلكية، وتنقسم إلى ثلاثة أنواع كما في الشكل (1) [1].



الشكل (1) أنواع بروتوكولات التوجيه في شبكات ال MANETs

- **تصنف بروتوكولات التوجيه بحسب مبدأ عملها إلى ثلاثة أنواع رئيسة:**

1-بروتوكولات التوجيه التفاعلية Reactive:

هي بروتوكولات توجيه تقوم بإجراء عمليات التوجيه في الشبكة عند الطلب. أي ان مسارات التوجيه لا تبنى إلا عند الحاجة فقط بالتالي تعمل على توفير عرض الحزمة. لكن هذا يزيد من التأخير في عملية توجيه الرزم ضمن الشبكة.

مثل بروتوكولات: AODV & DSR

2-بروتوكولات التوجيه غير التفاعلية Proactive:

في هذه البروتوكولات يتم تبادل معلومات التوجيه بين جميع عقد الشبكة ويتم اتخاذ قرار التوجيه بغض النظر عن حاجة الشبكة لها.

-تستهلك الكثير من عرض الحزمة، إلا أنها تؤمن سهولة في الحصول على معلومات التوجيه بشكل دائم وبشكل اسرع من التوجيه التفاعلي، لكن هناك صعوبة في تعديل جداول التوجيه في حال فشل احدى العقد.

مثل بروتوكولات: DSDV & OLSR.

3-بروتوكولات التوجيه الهجينة Hybrid:

هي البروتوكولات التي تجمع بين البرتوكولات التفاعلية وغير التفاعلية حيث تقسم الشبكة إلى عدة مناطق تمرير، ويستخدم أحد البرتوكولات ضمن مناطق التمرير وبرتوكول آخر للتوجيه بين مناطق تمرير البيانات.

مثال: ZRP (Zone Routing Protocol) وغيرها.

ويعتبر عملها هجين بين الطريقتين السابقتين، بحيث يُستخدم البروتوكولات proactive عندما نريد تقليل التأثير في الشبكات الصغيرة ويُستخدم البروتوكولات reactive في الشبكات الأكبر لتخفيف عبئ المعالجة الزائدة للبيانات.

-البروتوكول التفاعلي AODV

ان البروتوكول Ad hoc On-demand Distance Vector (AODV) هو عبارة عن برتوكول توجيه تفاعلي[2].

يتكيف هذا البروتوكول مع تغيرات الوصلات، في حال فشل الوصلة، يتم إرسال رسائل الإعلام بالفشل إلى العقد المتأثرة فقط في الشبكة، مما يسمح لهذه العقد بتحويل مسارات التوجيه عن الوصلات الفاشلة إلى العقد الفعالة في الشبكة، وبالتالي ضمان موثوقية الشبكة.

- **آلية عمله:**

يستخدم بروتوكول AODV أربع أنماط من الرسائل من اجل تحقيق عملية الاتصال بين العقد، هذه الرسائل هي:

1-رسائل طلب التوجيه Route Request (RREQ)

2-رسائل إجابة التوجيه Route Reply (RREP)

وتستخدمان من أجل عملية تحقيق مسارات التوجه.

3-رسائل الترحيب HELLO messages

4-رسائل خطأ التوجيه Route Error (RERR) messages

وتستخدمان من أجل عملية صيانة مسارات التوجيه.

- تستخدم عادة رسائل الترحيب من أجل بناء الوصلات بين العقد المتجاورة، ويتم ارسال هذه الرسائل بشكل دوري خلال فترات محددة ولذلك عند عدم استلام العقدة عدة رسائل ترحيب من عقدة جارة ما تعتبر الوصلة إلى هذه العقدة فاشلة.
- في حال كان لدى العقدة المنبع بيانات وتريد ارسالها إلى هدف ما، تقوم باكتشاف المسار الافضل باستخدام رسائل RREQ التي ترسلها ببث عام إلى كل عقد الشبكة.
- في حال لم تستلم العقدة الوسيطة رسالة RREQ من قبل، وفي حال لم تكن هي العقدة الهدف أو ليس لديها أي مسار نحو العقدة الهدف، تقوم هذه العقدة ايضاً بإعادة بث هذه الرسالة إلى عقد الشبكة.
- أما في حال كانت هذه العقدة هي الهدف أو لديها مسار توجيه إلى العقدة الهدف فإنها تنشئ رسالة RREP ويتم إرسال هذه الرسالة عبر المسار العكسي إلى العقدة المنبع.

- عندما تصل رسالة RREP إلى العقدة المنبع، تسجل هذه العقدة مسار التوجيه إلى العقدة الهدف لديها ثم تبدأ بإرسال البيانات عبره.
- في حال وصول عدة رسائل RREP إلى العقدة المنبع، يتم أخذ المسار ذي عدد القفزات الأقل.

-البروتوكول غير التفاعلي (OLSR) (Optimized Link State routing):

ان بروتوكول توجيه حالة الرابط (OLSR) هو بروتوكول استباقي، يؤمن التوجيه الآني في الشبكة اللاسلكية عند الحاجة، وفي حالة ظهور أية تغييرات على طبولوجيا الشبكة، فانه يرسل معلومات عن هذه التغيرات بطريقة البث العام إلى كل العقد المضيفة المتاحة في الشبكة، وبهذه الطريقة يمكن ي إنقاص الزمن الأعظمي لفترة ارسال الرسائل الدورية المنقولة في البروتوكول OLSR، وعند حدوث تغيرات على طوبولوجيا الشبكة التفاعلية. فإن هذا البروتوكول يحتفظ بجداول التوجيه إلى كل الأهداف المتاحة في الشبكة.

أهمية البحث وأهدافه

تكمن اهمية البحث في اختيار البروتوكول المناسب لنقل البيانات عبر الشبكة اللاسلكية AD-HOC، وذلك عندما تتعرض إلى هجوم من نوع الثقوب السوداء، حيث ننطلق في هذا البحث من دراسة تأثير هذه الثقوب السوداء على عمل بروتوكول التوجيه التفاعلي Reactive AODV وغير التفاعلي OLSR Proactive، من خلال دراسة تأثير الهجمات على كفاءة نقل البيانات الكبيرة في الشبكة، من خلال تغير عدد العقد في الشبكة ومن خلال حركية العقد الدائمة وسرعتها الكبيرة التي قد تتجاوز 70 م/ث، وبالتالي تقييم هذه البروتوكولات واختيار الأفضل.

طرائق البحث ومواده

اعتمدنا في هذا البحث على استخدام برنامج المحاكاة OPNET 14.5 الذي يعتبر أحد أهم برامج نمذجة ومحاكاة الشبكات الحاسوبية نظراً لدقته وسرعته في اظهار النتائج. و الذي يتيح محاكاة الشبكات اللاسلكية مع استخدام عقد الثقوب السوداء، وبالتالي على القيام بعمل العديد من السيناريوهات التي تحقق المطلوب، لأجل البروتوكولات AODV و OLSR.

النتائج والمناقشة

تعتبر شبكات ال MANETs كنظام اتصالات لاسلكي يقدم خدمات مستمرة، نظراً للديناميكية التي تتمتع فيها العقد، من خلال تأسيس الاتصالات المباشرة، وخاصة في حالة فقدان اية عقدة في الشبكة، يوجد الكثير من الأبحاث التي درست تأثير هجوم الثقوب السوداء، على بروتوكولات التوجيه اللاسلكية AODV و OLSR. حيث تم دراسة تأثير هجوم الثقب السود على هذه البروتوكولات في شبكة من 20 إلى 30 عقدة [3] [5] [6] [7] [8].

انواع الهجمات في شبكات MANET:

- تصنف الهجمات في شبكات الـ MANET إلى:

1-هجوم سلبي /نشط

الهجوم السلبي: يهدف الى سرقة المعلومات الهامة في كامل الشبكة ومن انواعه الشائعة هجمات التنصت وهجمات تحليل حركة المرور.

الهجوم النشط: يقوم المهاجم بتعديل البيانات بهدف عرقلة سير العمليات في الشبكة المستهدفة.

2- هجوم داخلي / خارجي:

الهجوم الخارجي: يبقى المهاجم خارج الشبكة وليس لديه وصول مسموح إلى داخل الشبكة، ويهدف من هجومه الى منع وصول المصرح لهم الدخول الى الشبكة (مثل حركة مرور الـ HTTP) من خلال إبقاء الشبكة تحت ضغط المشغولية العظمى التي تسبب الازدحام الذي يعطل عمل الشبكة.

الهجوم الداخلي: يتم الهجوم من داخل الشبكة وهو أكثر خطورة في منع الوصول المصرح فيه الى الشبكة، وبإمكان المهاجم المشاركة في النشاطات العادية للشبكة، ومن ثم العمل على ضياع بعض البيانات.

3-هجمات التوجيه

الهجمات الخاصة في شبكات MANET:

- **هناك أربع انواع مختلفة من هذه الهجمات تنقسم على النحو التالي:**

1-الهجوم باستخدام التعديل:

يقوم المهاجم بتعديل حقول برتوكول التوجيه في الرسائل وهذا يسبب تغيير مسارها واعادة توجيها الى مكان آخر.

2-الهجمات التي تستخدم الانتحال:

هي عبارة عن عقد خبيثة تنتحل عنوان عقدة أخرى ضمن الشبكة، وتغير في طبولوجيا الشبكة.

3-الهجمات التي تستخدم التلفيق:

في هذا النوع يستخدم المهاجم عقد خبيثة لحقن رسائل خاطئة ورزم توجيه وهمية في الشبكة من أجل تعطيل عملية التوجيه.

4-الهجمات الخاصة

هناك عدة انواع منها، وتستهدف فقط برتوكولات التوجيه مثل ال DSR/ AODV .

الهجمات الخاصة في شبكات MANET:

يوجد عدة أنواع للهجمات في شبكات MANET حسب نوع العقد الخبيثة [4]

❖ **Worm hole Attack:**

يعتبر من أحد الانواع الخطيرة للهجمات الخاصة، والتي يستخدم فيه المهاجمون عقدتين خبيثتين في شبكة ال MANET وذلك لنقل الرزم عبر نفق خاص، حيث يهدف هذا النفق الى تسجيل بيانات حركة المرور وارسالها إلى مكان آخر في الشبكة بهدف استبعادها.

❖ **Gray hole attack:**

في هذا النوع من الهجوم، يعمل المهاجمين في بداية عمل الشبكة بشكل طبيعي ودون أي يتسبب المهاجم بإسقاط أية رزمة، ويرسل المهاجم رسالة RREP صحيحة الى العقدة التي ارسلت رسالة RREQ ولكن عندما يستلم المهاجم الرزم يقوم بإسقاطها.

❖ **Black hole attack:**

هو أكثر انواع الهجمات التي تشغل خبراء الامن في شبكات ال MANE في الوقت الحالي، حيث يستخدم فيه المهاجمون واحدة أو أكثر من العقد الخبيثة، والتي تعلن عن نفسها في الشبكة كعقد تمتلك مسار صحيح الى كل الوجهات وهذا يجعل جميع العقد توجه رزم البيانات الى هذه العقد الخبيثة .

يعتبر البرتوكولين AODV و DSR أكثر عرضة لهذا الهجوم بسبب عدم وجود الخاصية المركزية في التوجيه، لأن جميع العقد تقوم بعملية التوجيه وتتبادل معلومات التوجيه. كما هو واضح في الجدول (1). [5].

الجدول (1) مقارنة بين الهجمات الخاصة بشبكات ال MANET

Attack	Required Knowledge	Cost	Detectability
Black-hole Single Cooperative	 Low Low	 Low Low	 High Low
Worm hole	High	High	Low
Gray hole	Medium	Medium	Low

فإن هجوم الثقب الاسود هو المفضل لدى المهاجمين، لأنه يمكّن من تحقيق الهجوم بالحد الادنى من الكلفة وكمية المعلومات التي يحتاجها المهاجم حول الشبكة ، وان امكانية كشف هجوم الثقب الاسود المنفرد تعتبر أعلى من الهجمات الاخرى ولكن يوجد شكل آخر أكثر تعقيداً من هجوم الثقب الأسود، وهو هجوم الثقب الاسود التعاوني والذي يعتبر صعب الكشف والايقاف.

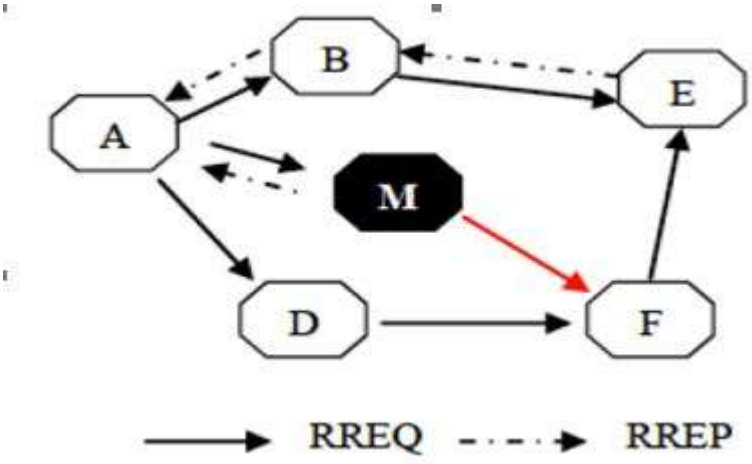
كيف يعمل هجوم الثقب الاسود

يتضمن هذا الهجوم عقدة خبيثة واحدة أو أكثر ويتم كما يلي:

- عندما تريد العقدة المصدر ارسال رزم البيانات الى عقدة أخرى، فإنها تقوم باكتشاف المسار من خلال إرسال رسالة RREQ الى جيرانها.
- تقوم العقدة الخبيثة باستلام هذه الرسالة ثم ترسل رسالة RREP وهمية للمرسل تظهر فيها بان لديها مسار صحيح نحو العقدة الهدف.
- عندما يستلم المرسل رسالة ال RREP سيعتقد بأن العقدة الخبيثة هي عقدة حقيقية وبعدها يقوم بإرسال رزم البيانات خلال المسار المحدد من قبل العقدة الخبيثة
- تستلم العقد الخبيثة هذه الرزم ولا ترسلها الى وجهتها بل تقوم بخلق حلقات توجيه وازدحام في الشبكة وبذلك يعطل المهاجمون أداء الشبكة.

هجوم الثقب الاسود المنفرد

يمكن تنفيذ هجوم الثقب الأسود باستخدام عقدة خبيثة واحدة مع شبكة صغيرة الحجم كما يبين الشكل (2) [5]، فعندما تريد العقدة المنبع A الاتصال مع عقد أخرى لإيصال الرزم إلى العقدة الهدف F . فإنها ترسل رسالة RREQ إلى العقد الجيران لتتعرف على المسار الصحيح إلى الهدف، وعند وجود عقدة خبيثة (ثقب أسود)، فإنها تستقبل الرسالة RREQ وترسل رسالة RREP مما يجعل العقدة المصدر تعتقد بأن العقدة الخبيثة حقيقة وترسل لها البيانات والتي بدورها تسقطها، يتميز التعامل مع هذه الشبكة بصعوبة كشف الهجوم لتصرف العقدة الخبيثة كما العقد النظامية.



الشكل (2) شبكة لاسلكية مع عقدة ثقب اسود واحدة

هجوم الثقب الاسود التعاوني

- يستخدم المهاجم عدة عقد خبيثة تعمل بالتعاون مع بعضها.
- امكانية كشف الهجوم منخفضة.

تمت دراسة هجوم الثقب الأسود بالاعتماد على البروتوكولات AODV وOLSR. في ظل وجود عقد ثقوب سوداء في البحث [6]. والذي اعتمد على وجود عقدة خبيثة مع 16 إلى 30 عقدة في الشبكة اللاسلكية، وبحمل منخفض نسبياً قيمته: 1024 bits ، وهذا لا يغطي إمكانية استخدام الشبكة بكامل طاقتها، حيث تبين في البحث تفوق البروتوكول AODV في نسبة ارسال الرزم وفي وجود تأخير زمني أقل لوصولها. ومن أفضل الأبحاث التي تمت على البروتوكولين البحث [7]. حيث قام الباحثون بدراسة شبكة مؤلفة من 40 عقدة، وبسرعات مختلفة من 10 الى 70 متر في الثانية، لكن الحمل كان منخفضاً، ولم نعرف تصرف البروتوكولات في ظروف الحمل العالي. بينما في البحث [8] استخدم الباحثون شبكة مؤلفة من 30 عقدة، بسرعة 10 متر بالثانية فقط. وهكذا نرى ان الكثير من الأبحاث التي أجريت درست تأثير هجوم الثقوب السوداء على بروتوكولات التوجيه اللاسلكية AODV وOLSR في حالات التأخير الزمني ونسبة وصول الرزم ولكنها لم تلحظ تغير عدد العقد إلى شبكة كبيرة فوق 40 عقدة، والى سرعات تفوق ال 70 متر بالثانية، وكذلك لم تلحظ ظروف نقل حمولة عالية. من هنا سنقوم بدراسة تأثير تغير عدد العقد مع تغيير حركيتها على أداء الشبكة اللاسلكية من خلال البروتوكولات AODV وOLSR. في ظل وجود حمولة عالية وشبكة متغيرة العقد والسرعة.

اعداد بيئة المحاكاة

تم اجراء محاكاة لتقييم أداء بروتوكولين من بروتوكولات التوجيه في الشبكات المخصصة (Ad Hoc) هما AODV و OLSR تحت تأثير هجوم الثقب الأسود. حيث تم استخدام المحاكي OPNET 14.5 لإجراء المحاكاة.

تم تشغيل المحاكاة لمدة ساعة واحدة، بمساحة شبكة تبلغ (1000 m x1000 m) وتوضع عقد عشوائي، كما تم انشاء 12 سيناريوه لدراسة أداء البروتوكولين في حالة الشبكات الصغيرة والمتوسطة والكبيرة وبسرعة عقد صغيرة وكبيرة، حيث تم اختيار 20 عقدة في حالة الشبكات الصغيرة و 50 عقدة في حالة الشبكات المتوسطة و100 عقدة في حالة الشبكات الكبيرة، كما أن العقد تتحرك بسرعة 10 m/s في حالة السرعات الصغيرة وبسرعة تبلغ 70 m/s في حالة السرعات الكبيرة. تم اختيار تطبيق نقل ملفات كبيرة الحجم (5Mb)، للعمل ضمن الشبكة ليحقق لنا حمل كبير على الشبكة.

في البداية قمنا بإنشاء 4 سيناريوهات لدراسة أداء البروتوكولين في حالة الشبكات الصغيرة وبسرعة عقدة صغيرة وكبيرة، ثم قمنا بإنشاء 4 سيناريوهات اخرى لدراسة أداء البروتوكولين في حالة الشبكات المتوسطة وبسرعة عقد صغيرة وكبيرة، وفي النهاية قمنا بإنشاء 4 سيناريوهات لدراسة أداء البروتوكولين في حالة الشبكات الكبيرة وبسرعة عقد صغيرة وكبيرة. يبين الجدول رقم (2) البارامترات المستخدمة في المحاكاة.

الجدول (2) بارامترات المحاكاة

Simulator	OPNET Modeler 14.5
Examined protocols	AODV and OLSR
Simulation time	3600 seconds
Simulation area (m x m)	1000m X 1000m
Number of Nodes	20 – 50 – 100
Number of Black Hole Node	1
Performance Parameter	Throughput, delay, Data Dropped , Load
Mobility (m/s)	10 m/s – 70 m/s
File size (bytes)	5Mb
Transmit Power(W)	0.005
Mobility Model	Random waypoint
Date Rate (Mbps)	11 Mbps

مقاييس الأداء

التأخير في الشبكة (Delay): هو متوسط الزمن اللازم لانتقال رزم البيانات من المصدر إلى الهدف عبر شبكة الاتصال، متضمناً التأخير الناتج عن اكتشاف المسار والتأخير الناتج عن عمليات التخزين المؤقت والمعالجة في العقد الوسيطة، وكذلك التأخير الناتج عن عمليات إعادة الإرسال في طبقة الـ MAC وغيرها.

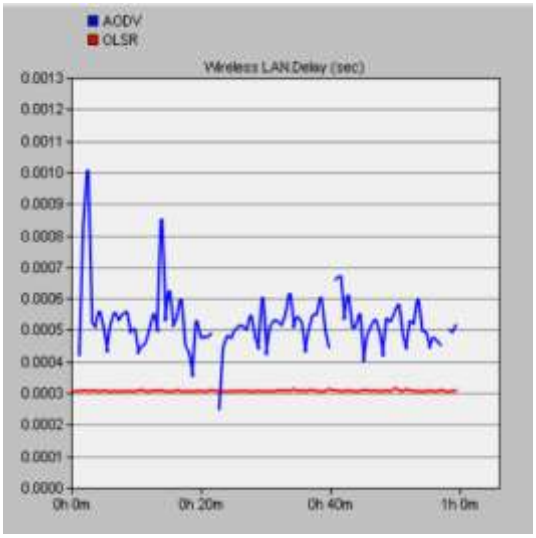
الانتاجية (Throughput): هي معدل الرزم أو البتات التي تستطيع الشبكة نقلها بنجاح خلال واحدة الزمن، وتقدر الإنتاجية بـ (bits/sec)، ويوجد العديد من العوامل التي تؤثر على إنتاجية الشبكة منها عرض الحزمة المتاح والازدحام وعمليات إعادة الإرسال والتأخير.

الحمل على الشبكة (Network load): المقدار الكلي للبيانات المنقولة عبر الشبكة ويقدر بواحدة (bits/sec).

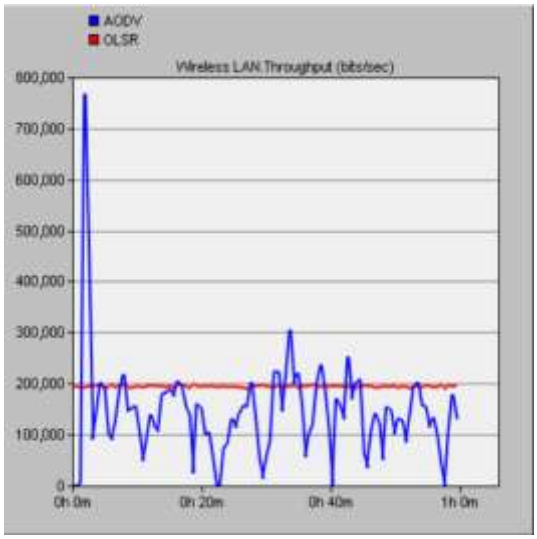
الضياع في الشبكة (data dropped): مقدار البيانات التي تم اسقاطها ولم تصل الى وجهتها بنجاح في الشبكة وتقدر بواحدة (bits/sec).

المناقشة وتحليل النتائج

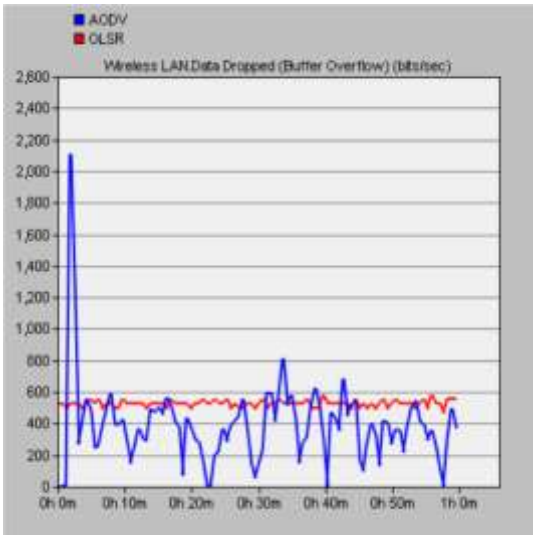
تظهر الأشكال (3 الى 6) مقارنة أداء البروتوكولين في حالة الشبكات الصغيرة 20 عقدة وسرعة العقد صغيرة 10 m/s



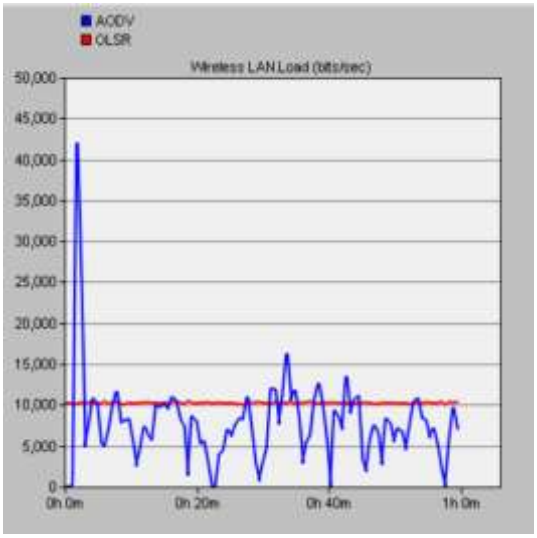
الشكل (3): التأخير في الشبكة



الشكل (4): الانتاجية في الشبكة

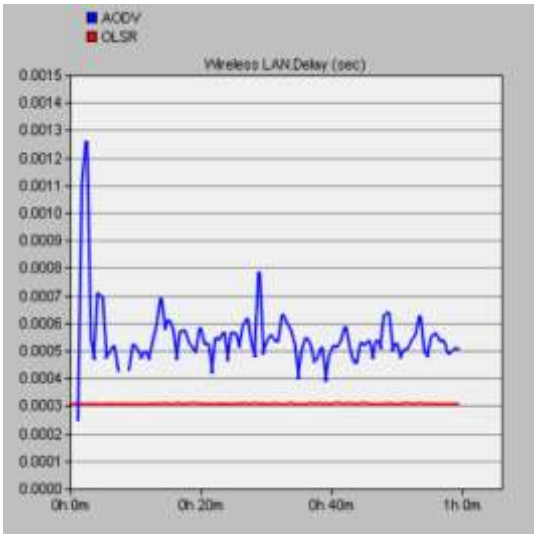


الشكل (5): الضياع في الشبكة

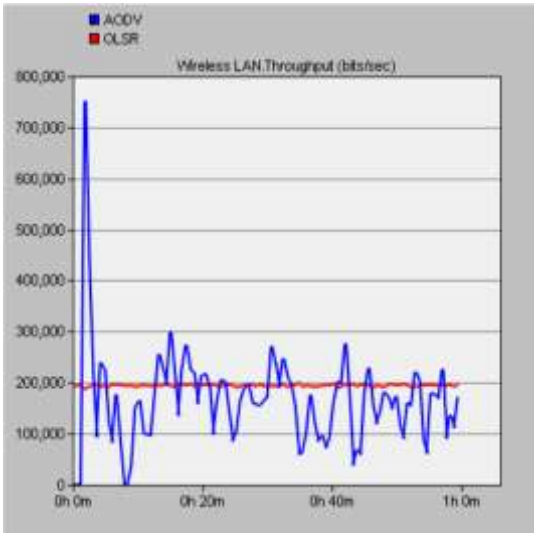


الشكل (6): الحمل في الشبكة

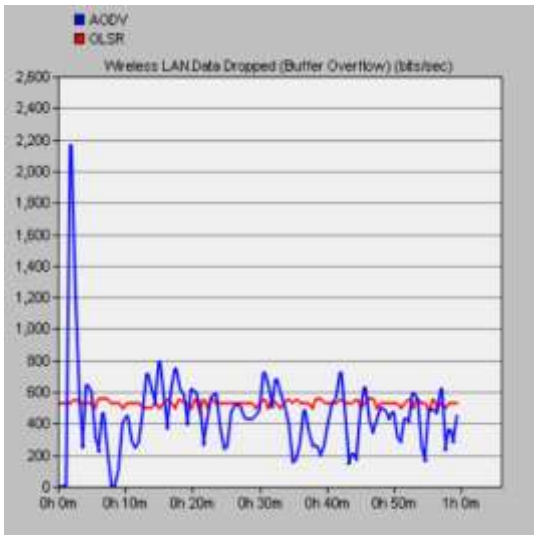
تظهر الأشكال (7 الى 10) مقارنة أداء البروتوكولين في حالة الشبكات الصغيرة 20 عقدة وسرعة العقد كبيرة 70 m/s.



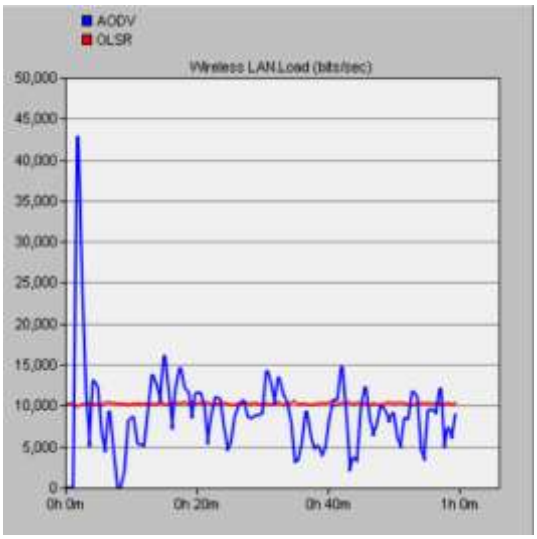
الشكل (7): التأخير في الشبكة



الشكل (8): الانتاجية في الشبكة

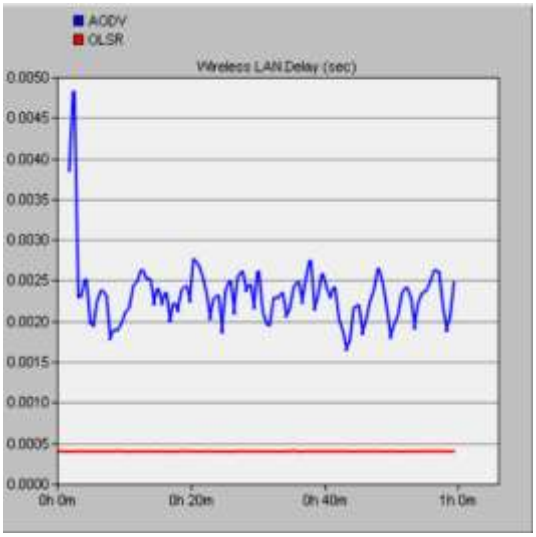


الشكل (9): الضياع في الشبكة

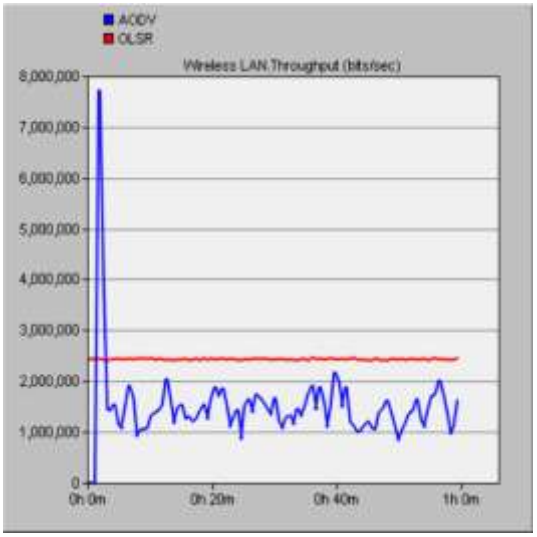


الشكل (10): الحمل في الشبكة

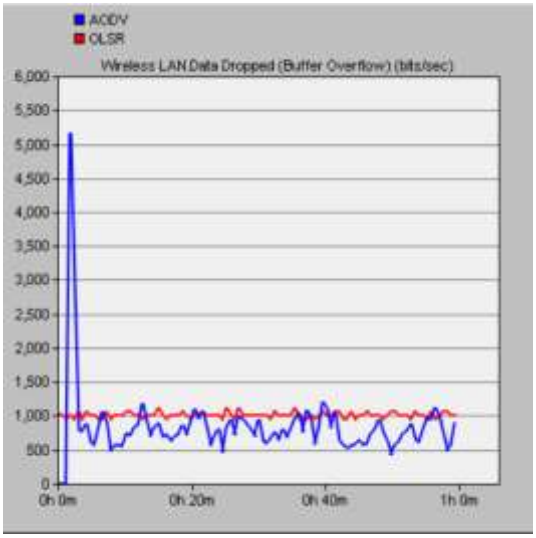
تظهر الأشكال (11 الى 14) مقارنة أداء البروتوكولين في حالة الشبكات المتوسطة 50 عقدة وسرعة العقد صغيرة 10 m/s



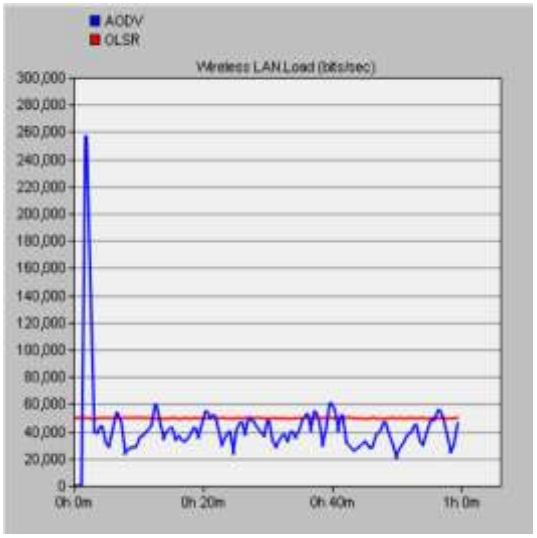
الشكل (11): التأخير في الشبكة



الشكل (12): الانتاجية في الشبكة

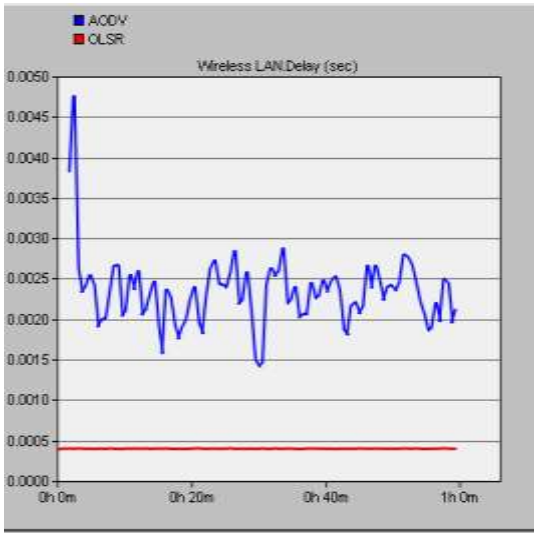


الشكل (13): الضياع في الشبكة

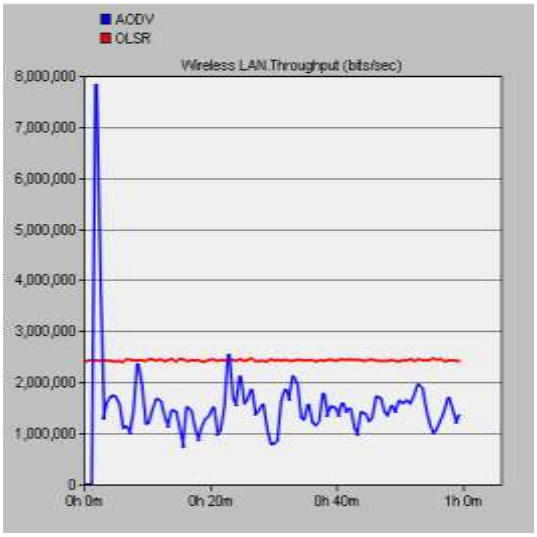


الشكل (14): الحمل في الشبكة

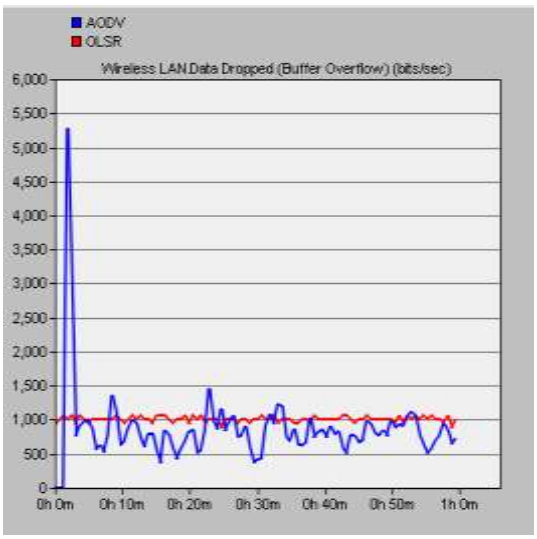
تظهر الأشكال (15 الى 18) مقارنة أداء البروتوكولين في حالة الشبكات المتوسطة 50 عقدة وسرعة العقد كبيرة 70 m/s



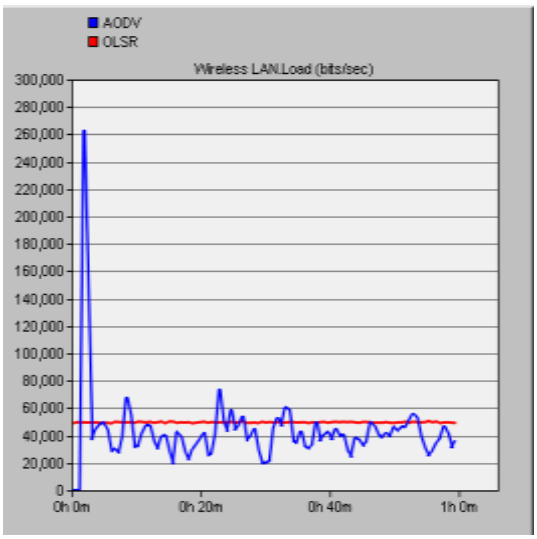
الشكل (15): التأخير في الشبكة



الشكل (16): الانتاجية في الشبكة

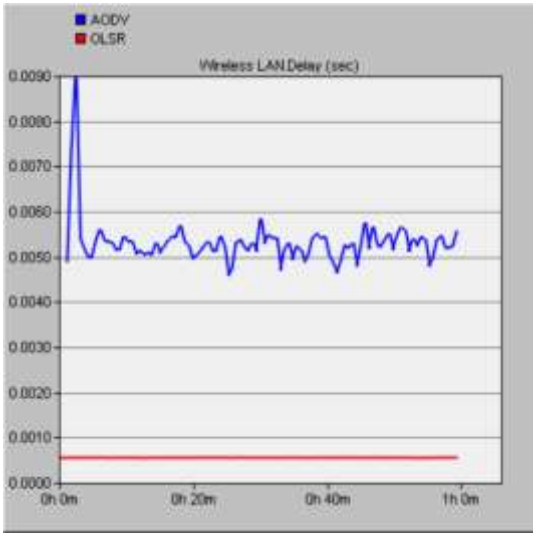


الشكل (17): الضياع في الشبكة

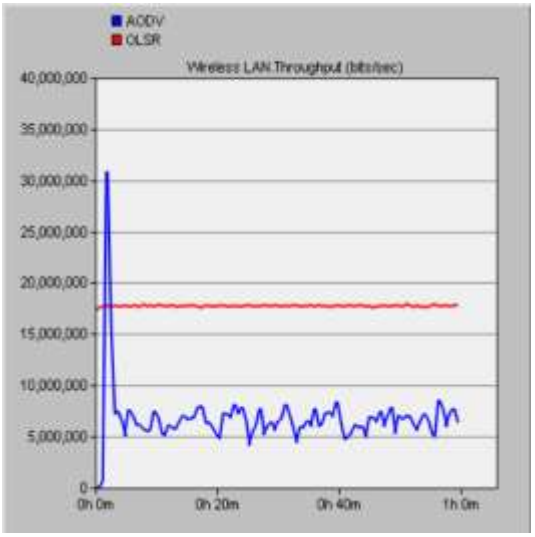


الشكل (18): الحمل في الشبكة

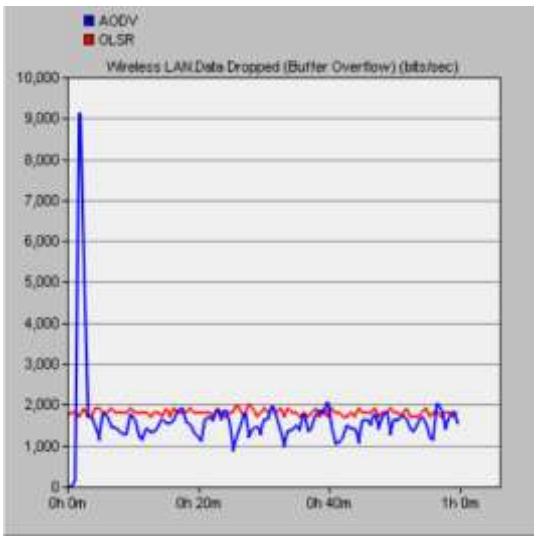
تظهر الأشكال (19 الى 22) مقارنة أداء البروتوكولين في حالة الشبكات الكبيرة 100 عقدة وسرعة العقد صغيرة 10 m/s



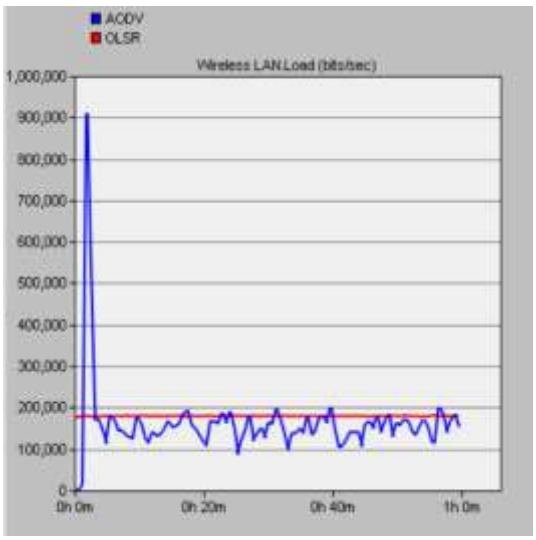
الشكل (19): التأخير في الشبكة



الشكل (20): الانتاجية في الشبكة

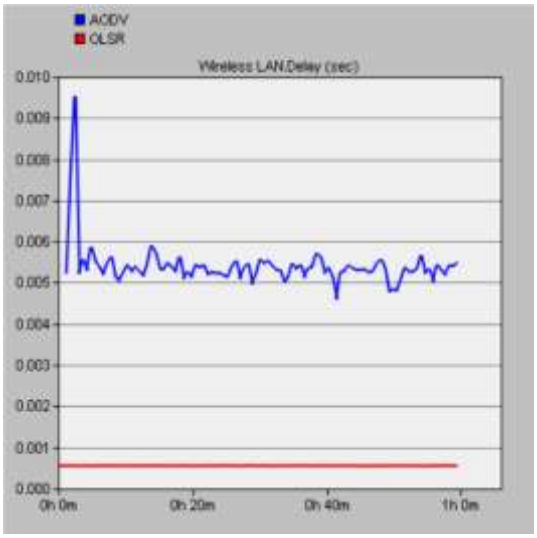


الشكل (21): الضياع في الشبكة

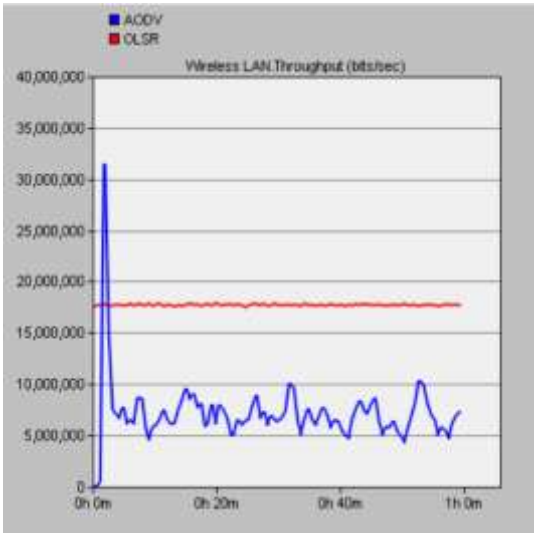


الشكل (22): الحمل في الشبكة

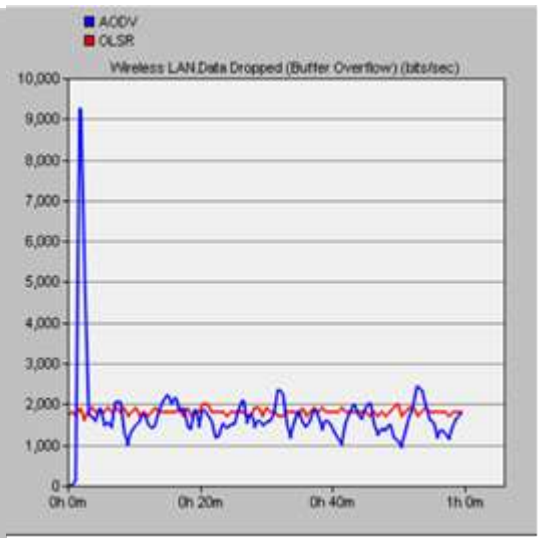
تظهر الأشكال (23 الى 26) مقارنة أداء البروتوكولين في حالة الشبكات الكبيرة 100 عقدة وسرعة العقد كبيرة 70 m/s



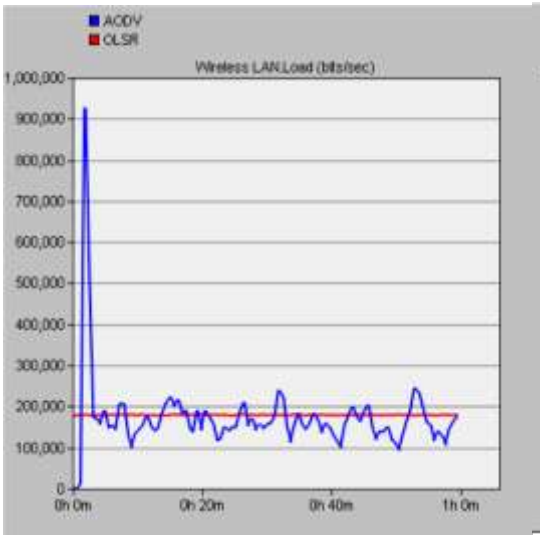
الشكل (23): التأخير في الشبكة



الشكل (24): الانتاجية في الشبكة



الشكل (25): الضياع في الشبكة



الشكل (26): الحمل في الشبكة

جميع السيناريوهات السابقة تعمل ضمن حمل مرتفع بقيمة (5 Mb) على الشبكة، وبوجود عقدة خبيثة واحدة، وبالتالي من نتائج المحاكاة نلاحظ في حالة الشبكة الصغيرة ب 20 عقدة، وسرعة العقد الصغيرة البالغة 10متر بالثانية، أن البروتوكول OLSR هو البروتوكول الأقل تأخيراً لأنه يقوم بحساب جميع المسارات في الشبكة بشكل مسبق وصيانتها بشكل دائم، مما يؤدي الى انخفاض التأخير وزيادة الحمل على الشبكة الشكل (3)، بينما يقوم البروتوكول AODV بحساب المسارات عند طلبها فقط مما يؤخر عملية النقل ويجعل زمن التأخير يرتفع عند طلب مسار لم يتم اكتشافه مسبقاً، وهذا يفسر ارتفاع التأخير عند استخدام البروتوكول AODV.

ومع زيادة سرعة العقد نلاحظ عدم تأثر البروتوكول OLSR بهذه الزيادة في حين يتأثر البروتوكول AODV بزيادة سرعة العقد ويزداد الضياع في البيانات الأشكال (7،15، 19).

ومع زيادة عدد العقد في الشبكات المتوسطة والكبيرة، نلاحظ ازدياد التأخير بشكل كبير في البروتوكول AODV لأن الشبكة تعمل ضمن حمل مرتفع (5 Mb)، وبالتالي على البروتوكول AODV ارسال عدد كبير من طلبات

اكتشاف المسار ، أما البروتوكول OLSR فلا يتأثر كثيراً بزيادة عدد العقد في حالة الحمل المرتفع لأنه يقوم بشكل مستمر بصيانة المسارات.

بالنسبة لبارمترات الانتاجية والضياع والحمل، نرى ان الشبكة ذات ال 20 عقدة ومع سرعة 10 م/ث تكون متوازنة بين البروتوكولين لصالح البروتوكول OLSR قليلاً، ولكن عندما نزيد من سرعة العقد إلى 70 م/ث نرى التوازن واضح في إنتاجية الشبكة وفي الضياع بين البروتوكولين، ولكن الاختلاف الواضح يظهر عندما نعتمد شبكة كبيرة نوعا ما ب 50 عقدة، وعند سرعة العقد ب 10 م/ث، نرى إنتاجية البروتوكول OLSR تتفوق بشكل واضح على البروتوكول AODV، وأفضل أيضاً من ناحية الضياع والحمل، الأشكال (15-18).

وفي حالة الشبكات الكبيرة ذات الحمل الكبير وب 100 عقدة متحركة بسرعة 10 م/ث، فنرى الإنتاجية عند البروتوكول OLSR عالية جداً الشكل (24)، بينما يبقى الضياع والحمل في حالة توازن بين البروتوكولين، مع أفضلية نسبية لصالح البروتوكول OLSR، الأشكال (24-26).

ومن خلال دراسة السيناريوهات السابقة والنتائج الواضحة، وجدنا أن البروتوكول OLSR هو البروتوكول الأقل تأثراً بهجوم الثقب الأسود في حالة الشبكات ذات الحمل المرتفع وذلك باختلاف سرعة العقد أو عددها. من خلال انتاجيته الأفضل، وتأخيره الزمني الأقل كما وجدنا أيضا أن ضياع البيانات فيه نسبياً أفضل، وكل ذلك ناتج عن أن البروتوكول يقوم دائما بصيانة ذاتية وحاضرة، مع معرفته المسبقة للمسارات التي توفر عليه كمية بيانات، وتأخير زمني قليل، يعوضه عن البيانات الضائعة.

الاستنتاجات والتوصيات

وجدنا بعد الدراسة والمحاكاة، أن البروتوكول OLSR هو البروتوكول الأقل تأثراً بوجود هجوم الثقب السود، وذلك في بيئة حمل مرتفع، من خلال اختلاف عدد العقد في الشبكة ومن خلال اختلاف سرعتها إلى السرعة القصوى 70m/s. وان البروتوكول AODV هو البروتوكول الأكثر تأثراً بهجوم الثقب الأسود في نفس بيئة المحاكاة السابقة، ويزداد هذا التأثر بزيادة عدد العقد وزيادة سرعتها.

في المستقبل يمكن القيام بمحاكاة عمل البروتوكولين AODV وOLSR في الشبكات التي تعمل بحركة بيانات منخفضة، مع زيادة عدد العقد في الشبكة، ومقارنة النتائج مع نتائج هذا البحث والتي حصلنا عليها بمحاكاة الشبكات التي تعمل ضمن حركة بيانات مرتفعة (تتجاوز 3Mb). كما يمكن دراسة سلوك البروتوكولين بوجود أكثر من عقدة خبيثة، وفي ظروف وجود حمل كبير، ضمن الشبكة لاكتشاف البروتوكول الأقل تأثراً بزيادة عدد العقد الخبيثة الممثلة بعقد الثقب الأسود. وكذلك يمكن القيام بمقارنة عمل البروتوكول OLSR مع أحد البروتوكولات الهجينة، في ظل وجود حمل كبير على الشبكة يتجاوز 3Mb وسرعة تحرك كبيرة للعقد، مع وجود عدد عقد كبير إلى حدود 100 عقدة.

المراجع

[1] - SHAMEKH, KARIM. ELFAKHARANY, ESSAM ELDEN. *Comparative Study of AODV and OLSR Protocols in MANET Network under the Impact of Black Hole Attack*, International Journal of Computer Science and Telecommunications. Vol 4, N^{o} 9, 2013, p. 14-19.

[2] -)ADE, S, A., TIJARE P, A. ” *Performance Comparison of AODV, DSDV, OLSR and DSR Routing Protocols in Mobile Ad Hoc Networks*”, International Journal of Information Technology and Knowledge Management, Vol 2, N^{o}. 2, 2010, p. 545-548.

[3] – SIJO, CHERIAN. ANJALY, GOY. *BLACK HOLE ATTACK AND ITS MITIGATION TECHNIQUES IN AODV AND OLSR*، -International Journal of Computer Science & Engineering Technology ,IJCSET, Vol. 4, N^{o}. 6, 2013, p. 740-745.

[4] – MANINDERPAL SINGH. MANMOHAN SHARMA. *Enhanced Multipath Approach for Prevention and Elimination of Black Hole Attack in Mobile Ad-Hoc Networks considering the Enhancement of Network Throughput.* International Journal of Engineering Sciences & Research Technology, Vol. 3, N^{o}.5, 2014, P.798-808.

[5] - EHSAN KAMAL AMIN MOHEBI, Prof.Dr.SIMON SCOTT. *Simulation and Analysis of AODV and DSR Routing Protocol under Black Hole Attack*. I.J.Modern Education and Computer Science. Vol. 10, P. 19-26.

[6] – IRSHAD ULLAH. SHAHZAD ANWAR**.** *Effects of Black Hole Attack on MANET Using Reactive and Proactive Protocols*. International Journal of Computer Science issues. Vol. 10, N^{o}. 1, 2013, p. 152-159.

[7] - HUMYUN, RASHID. ISLAM, RASHEDUL. *Performance measurement of MANET routing protocols under Blackhole security attack*, IOSR Journal of Computer Engineering (IOSR-JCE), Vol. 17, N^{o}. 2, 2015. P. 89-93.

[8] - RUPINDER KAUR. OARMINDER SINGH. *REVIEW OF BLACK HOLE AND GREY HOLE ATTACK*. The International Journal of Multimedia & Its Applications (IJMA). Vol.6, N^{o}.6, 2014, P. 35-45.