اكتشاف هجوم الثقب الأسود في الشبكات الخاصة النقالة باستخدام IDSAODV وReverse AODV

د. اناس ليلى [*]

منى محمد [**]

(تاريخ الإيداع 9 / 9 / 2020. قُبِل للنشر في 17/ 2 / 2021)

□ ملخّص □

يعد هجوم الثقب الأسود من أخطر الهجمات الأمنية وأكثرها شيوعاً في شبكات MANET، لذلك توجه الباحثون إلى إيجاد تقنيات لاكتشاف هذا الهجوم، ومن هذه التقنيات نظام كشف التسلل لبروتوكول AODV (IDSAODV) وبروتوكول AODV العكسي (Reverse AODV).

درسنا في هذا البحث تأثير هجوم الثقب الأسود على أداء الشبكة وذلك في ظل وجود مهاجم واحد أو أكثر، ثم طبقنا كل من IDSAODV وReverse AODV في الشبكة بهدف تقييم مدى فعالية كل منهما في كشف هذا الهجوم والتخفيف من آثاره، حيث اعتمدنا الإنتاجية Throughput، ونسبة تسليم الرزم Packet delivery (PDR) Ratio ، وعبء التوجيه الطبيعي Normalized routing load (NRL) كمعايير لتقييم الأداء.

أظهرت نتائج المحاكاة المكثفة أنّ تطبيق IDSAODV خفف من أثر هجوم الثقب الاسود حيث أنه زاد من نسبة تسليم الرزم حتى 68% ، في حين قدم Reverse AODV نتائج أفضل حيث وصلت نسبة تسليم الرزم إلى 100%، إلا أن Reverse AODV سبب زيادة في عبء التوجيه الطبيعي NRL مقارنة ببروتوكول IDSAODV. كما أظهرت نتائج المحاكاة تأثر أداء IDSAODV بموقع العقدة المهاجمة.

الكلمات المفتاحية: الشبكات اللاسلكية الخاصة النقالة ، الثقب الأسود ، IDSAODV، Reverse AODV ، NS2

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

[**] طالب دراسات عليا(ماجستير). قسم النظم والشبكات الحاسوبية–كلية الهندسة المعلوماتية –جامعة تشرين–اللاذقية–سورية .

Detection of Black Hole Attack in MANETS Using IDSAODV and Reverse AODV

Dr. Inas Laila *
Mona Mohammad**

(Received 9 / 9 / 2020. Accepted 17 / 2 / 2021)

□ ABSTRACT □

Black Hole Attack is one of the most dangerous and most common security attacks in MANET networks, so researchers have been directed to find techniques to discover this attack, Intrusion Detection System AODV(IDSAODV) and Reverse AODV are two of these techniques.

In this research, we studied the effect of Black Hole Attack on network performance in the presence of one or more attackers. then we applied IDSAODV and Reverse AODV in network to evaluate their effectiveness in detecting the attack and mitigating its effects. We used Throughput, Packet delivery ratio (PDR) and Normalized routing load(NRL) to performance evaluation .

The results of the extensive simulation showed that the IDSAODV application reduced the impact of the attack ,where it increased the packet delivery rate up to 68%, while Reverse AODV provided better results where the PDR reached to 100 % , but it caused increase in NRL in comparison by IDSAODV.

The simulation results also showed that the performance of the IDSAODV was affected by the location of the attacking node.

Keywords: Mobile wireless networks , Black Hole Attack , IDSAODV, Reverse AODV, NS2.

*** Assistant Professor, Department of System and Networks Computing, Faculty of Informatics Engineering, Tishreen University, Lattakia, Syria**

**** Postgraduate Student (Master), Department of System and Networks Computing, Faculty of Informatics Engineering, Tishreen University, Lattakia, Syria,Email: monamrhg1994@gmail.com.**

مقدمة:

تعرف الشبكات اللاسلكية الخاصة النقالة MANETS بأنها مجموعة من العقد المتحركة المستقلة والمدارة ذاتياً دون وجود بنية تحتية [1]، حيث تتعاون العقد معاً لإيصال الرسائل إلى أهدافها ويتم ذلك باستخدام بروتوكولات التوجيه المسؤولة عن إيجاد المسار بين المصدر والهدف، ويعد بروتوكول AODV من أشهر هذه البروتوكولات وأكثرها استخداماً.

يعد تحقيق الأمن في هذه الشبكات تحدياً يصعب تحقيقه، وذلك لمجموعة من الأسباب منها الطوبولوجيا المتغيرة، عرض الحزمة المحدود، غياب الإدارة المركزية، والحركية المستمرة للعقد Mobility .

وتعد عملية التوجيه Routing عرضة للعديد من المخاطر والهجمات الأمنية، ومن هذه الهجمات هجوم الثقب الأسود Black Hole الذي يقوم بإسقاط الرزم في الشبكة، وبالتالي يمنعها من بلوغ وجهتها المحددة [2].

يتمثل هجوم الثقب الأسود في شبكات MANET بعقدة خبيثة واحدة أو أكثر تعلن بأن لديها المسار الأقصر والأحدث إلى الهدف وذلك عندما تصدر العقدة المصدر رسالة طلب المسار RREQ(Route Request) للعقد الجارة لها لإيجاد هذا المسار.

الدراسة المرجعية:

لقد حظي هجوم الثقب الأسود باهتمام كبير لدى الباحثين حيث بيّنت الدراستين [4] و[3] أنه يؤثر على بروتوكولات التوجيه التفاعلية أكثر من غيرها من البروتوكولات وذلك لأنها تطلب المسار عند الطلب فقط في حين البروتوكولات غير التفاعلية تعتمد على الاحتفاظ بجميع المسارات وصيانتها بشكل دائم قبل إرسال البيانات ، بينما درس الباحثون في [5] تأثير هذا الهجوم على الشبكة التي تستخدم بروتوكول AODV، واستنتجوا أن لهجوم الثقب الأسود أثر كبير على نسبة تسليم الرزم في الشبكة. كما قام آخرون في [6] بدراسة أثر زيادة عدد العقد المهاجمة واستنتجوا تدهور أداء الشبكة بشكل كبير و تناقص في إنتاجيتها عند زيادة عدد المهاجمين. بينما توجه بعض الباحثون إلى إيجاد تقنيات لاكتشاف هذا الهجوم ومحاولة منعه.

صنف الباحثون تقنيات اكتشاف هجوم الثقب الأسود إلى أصناف كثيرة بعضها يعتمد على التشفير، وآخر يعتمد على تحديد عتبة للرقم الدال على حداثة المسار، وغيرها من التقنيات التي تعتمد على التنصت وتحقيق الثقة بين العقد[7].

قام الباحثون في [8] باقتراح IDSAODV وذلك بإجراء تعديل على بروتوكولAODV بهدف تقليل تأثير هجوم الثقب الأسود. كما قام آخرون في [9] باقتراح Reverse AODV وذلك لمنع هجمات حجب الخدمة (DOS)، واستنتجوا أنه حسَّن بشكل ملحوظ نسبة تسليم الرزم والانتاجية في الشبكة. بينما قام الباحثون في [10] بدمج البروتوكولين المحسنين السابقين وحققوا نتائج جيدة وذلك في شبكات Mesh wireless، إلا أن معظم الباحثين أغفلوا تأثير موقع العقدة المهاجمة على أداء هذه البروتوكولات.

درسنا في هذا البحث أثر تطبيق كل من IDSAODV وReverse AODV في الشبكة في حال وجود مهاجم واحد أو أكثر وتم التركيز على دراسة تكلفة تطبيق هذين البروتوكولين وذلك في حال عدم وجود هجوم ويعود السبب في اختيارهما إلى أن الباحثين في الدراسات السابقة [8] و [9] قد أغفلوا دراسة تكلفة استخدامهما في الشبكة في حال عدم وجود الهجوم، كما درسنا تأثر أداء كل منهما بموقع العقدة المهاجمة بالنسبة للمرسل والمستقبل حيث أن هذه الأفكار لم يتم دراستها مسبقاً.

أهمية البحث وأهدافه:

تأتي أهمية هذا البحث من ضرورة دراسة الهجمات الأمنية وأثرها في الشبكات بشكل عام وفي شبكات MANET بشكل خاص، ودراسة التقنيات المقترحة لكشف هذه الهجمات وتحديد إيجابيات وسلبيات كل منها وذلك في ظل ازدياد الهجمات الأمنية وتنوعها في الوقت الراهن.

يهدف هذا البحث إلى دراسة تأثير هجوم الثقب الأسود على أداء شبكات MANET التي تستخدم AODV كبروتوكول توجيه، ودراسة فعالية البروتوكولين IDSAODV و Reverse AODV في كشف عقدة الثقب الأسود وذلك من خلال محاكاة سيناريوهات مختلفة لشبكة MANET، بهدف تحديد البروتوكول الذي يقدم الأداء الأفضل للشبكة وذلك وفقاً لمجموعة من المعايير كالإنتاجية وعبء التوجيه الطبيعي ونسبة تسليم الرزم.

طرائق البحث ومواده:

أجرينا بدايةً دراسة نظرية عن آلية عمل هجوم الثقب الأسود و كيفية تأثيره على أداء الشبكة، وبحثنا عن الحلول التي اقترحها الباحثون لكشفه والتخفيف من آثاره. ثم استخدامنا محاكي الشبكات NS2 [12] لبناء سيناريوهات مختلفة لدراسة فعّالية بعض هذه الحلول وذلك بوجود مهاجم واحد أو أكثر في الشبكة .

استخدمت الأداة Nam(1.14) لإظهار طوبولوجيا الشبكة وملفات Trace لحساب النتائج ، ثم حللنا النتائج لتحديد البروتوكول الأفضل لكشف هجوم الثقب الأسود في شبكة MANET في ظل قيم مختلفة لبعض بارامترات الشبكة ووفقاً لمجموعة من المقاييس.

1- هجوم الثقب الأسود في MANETS المعتمدة على بروتوكول التوجيه AODV:

يتلخص عمل هجوم الثقب الأسود في شبكات MANETS والتي تستخدم بروتوكول التوجيه AODV لإيجاد المسارات بين العقدة المرسلة والمستقبلة كما يلي :

- عندما تريد العقدة المصدر إرسال رزم البيانات إلى عقدة أخرى، فإنها تقوم باكتشاف المسار من خلال إرسال رسالة طلب المسار. RREQ الى جيرانها.
- تقوم العقدة الخبيثة باستلام هذه الرسالة لترسل بدورها رسالة رد مسار RREP(Route Reply) للمرسل تخبره فيها بأن لديها المسار الأقصر والأحدث نحو العقدة الهدف .
- عندما يستلم المرسل رسالة الرد الاولى RREP من العقدة الخبيثة يتجاهل رسائل RREP القادمة إليه من بقية العقد، ويقوم بإرسال رزم البيانات من خلال المسار المحدد من قبل العقدة الخبيثة.
- تقوم العقد الخبيثة باستلام هذه الرزم وتسقطها، مما يحول دون وصول الرزم إلى هدفها الحقيقي.

2- تقنيات اكتشاف هجوم الثقب الأسود في MANETS:

ظهرت تقنيات كثيرة لاكتشاف هجوم الثقب الأسود وسنركز في هذا البحث على IDSAODV و Reverse AODV.

1-2 نظام كشف التسلل لبروتوكول AODV (IDSAODV):

هو بروتوكول محسن عن بروتوكول AODV اقترحه الباحثون لتحسين أداء شبكات MANETS في ظل وجود هجوم الثقب الأسود، تعتمد فكرته على جعل العقدة المصدر تتجاهل المسار المُنشأ من قبل رزمة الرد الأولى، والاستجابة لرزمة الرد الثانية. إذ يفترض IDSAODV أن الرد الأول(الأسرع) يأتي دوماً من عقدة مهاجمة، لكن هذا الافتراض

غير صحيح دائماً فقد تكون العقدة المهاجمة بعيدة عن العقدة المصدر، وقد تكون العقدة الوجهة بالقرب من العقدة المصدر، في هذه الحالة فإن الرد الأول سيأتي من عقدة الوجهة الحقيقية، ووفقاً لهذا البروتوكول فإنه سيتم تجاهل هذا الرد والاستجابة للرد التالي الذي قد يأتي من عقدة الثقب الأسود [8]. تتلخص خوارزمية IDSAODV كالآتي :

1. ترسل العقدة المصدر رسالة طلب المسار. RREQ بثاً عاماً.
2. تستقبل العقدة المصدر رسائل رد على طلب المسار RREP متعددة .
3. تتجاهل العقدة المصدر رزمة RREP الأولى وتعتبرها قادمة من عقدة خبيثة.
4. تقوم العقدة المصدر بقبول رزمة الرد الثانية وتعتبرها من عقدة موثوقة، ومن ثم تقوم بتحديث جدول توجيهها و تبدأ بإرسال بياناتها وفقاً للمعلومات الواردة في هذه الرزمة.

2-2 بروتوكول AODV العكسي (Reverse AODV) :

صمم هذا البروتوكول بدايةً لحل مشكلة ضياع رزمة الرد حيث عالج Reverse AODV مشكلة Unicast Route Reply [13] والتي تعد من نقاط ضعف بروتوكول AODV التي يستخدمها المهاجمون في هجومهم، مما جعله يُستخدم لاحقاً لتخفيف أثر هجوم الثقب الأسود [9]. يعتمد هذا البروتوكول على غمر رسالة الرد في الشبكة وبالتالي إنشاء عدة مسارات توجيه بين المصدر والهدف. و يتلخص عمل بروتوكول Reverse AODV كما يلي:

1- تعمل العقدة المصدر على بث رزمة طلب المسار RREQ بثاً عاماً للعقد الجارة لها والتي بدورها تعيد إرسالها للعقد الجارة لها وهكذا وصولاً للعقدة الهدف.

2- عند استقبال العقدة الهدف لأول رسالة RREQ تُبث إلى جيرانها رزمة تدعى Reverse Route Request (R-RREQ) تتضمن هذه الرزمة معلومات الرد على طلب المسار، وبعدها يقوم الجيران بدورهم بإرسال هذه الرزمة إلى جيرانهم بعد تعديل معلومات جداول توجيههم وتحديثها وهكذا حتى الوصول للعقدة المصدر.

3- عند استقبال العقدة المصدر لرزم R-RREQ تخزن مسارات التوجيه المتاحة لنقل رزم البيانات بين المصدر والهدف وتنتقي المسار الأفضل (الأقصر والأحدث) وتقوم بإرسال رزم البيانات إلى الهدف عبره.

4- في حال فشل المسار المختار يختار مسار بديل من المسارات المخزنة.

بالنتيجة عند وجود مهاجم في الشبكة فإنه سيقوم بإرسال رد على رسالة طلب المسار مباشرةً مبيناً بأنه يملك مساراً إلى الهدف، إلا أن العقدة المصدر لن تستجيب له لأنها تنتظر رسالة الرد العكسية R-RREQ من الهدف، كما أنها ستقوم بعزله وحذفه من جدول توجيهها. إنّ ما يعيب هذا البروتوكول هو تسببه بحمل زائد وتأخير في الشبكة بسبب غمره لرسائل الرد في كامل الشبكة.

3- الدراسة التجريبية:

3-1- بناء نموذج الشبكة:

استخدمنا محاكي الشبكات NS2 لبناء نموذج لشبكة MANET مؤلفة من 20 عقدة متصلة لاسلكياً لها نفس الإمكانيات (متجانسة) ، تنتشر هذه العقد بمواقع ابتدائية عشوائية في منطقة مساحتها 1186m*600 m حيث أنه لم يتم أخذ أي اعتبارات عند اختيار عدد العقد في الشبكة حيث تم اختيار العدد عشوائياً بهدف بناء شبكة MANET ودراسة أثر هجوم الثقب الأسود عليها. ، تتحرك هذه العقد (باستثناء العقد المهاجمة) بسرعة ثابتة 2 m/s وهي متوسط سرعة المشي البشري، تولد بعض هذه العقد رزم بيانات بحجم 1500 bytes وإرسالها الى أهداف محددة بمعدل

0.1Mb/s مستخدمة بروتوكول التوجيه AODV لتحديد المسارات إلى تلك الأهداف. يوضح الجدول (1) بارامترات الشبكة وقيمها.

الجدول(1) : بارامترات الشبكة

البارامتر	القيمة
نوع القناة	لاسلكية
زمن المحاكاة (second)	600
حجم الرزمة (Byte)	1500
بروتوكول طبقة النقل	UDP
معدل تدفق البيانات(Mb/s)	0.1
بروتوكول التوجيه	AODV without BH ,blackholeAODV,IDSAODV,ReverseAODV
عدد العقد الكلي	20
عدد العقد المهاجمة	0,1,2,3
سرعة العقد (m/s)	2
عدد اتصالات CBR	10
منطقة المحاكاة (m^2)	1180*600

2-3 سيناريوهات المحاكاة:

السيناريو الأول:

يهدف هذا السيناريو إلى تقييم أداء شبكة MANET تستخدم بروتوكول AODV تتعرض لهجوم الثقب الأسود من قبل مهاجم واحد أو أكثر وذلك بهدف دراسة تأثر الهجوم على أداء الشبكة.

السيناريو الثاني: يهدف هذا السيناريو إلى تقييم أداء شبكة MANET تتعرض لهجوم الثقب الأسود بمهاجم أو أكثر وذلك عند تطبيق كل من البروتوكولين IDSAODV ، Reverse AODV بهدف دراسة فعالية كل منهما في كشف الهجوم.

السيناريو الثالث: يهدف هذا السيناريو إلى دراسة تأثر أداء كل من البروتوكولين IDSAODV ، Reverse AODV بموقع العقدة المهاجمة بالنسبة للعقدة المرسلة .

4- بارامترات تقييم الأداء:

سنعتمد في دراستنا على مجموعة من البارامترات وهي نسبة تسليم الرزم، متوسط الإنتاجية، عبء التوجيه الطبيعي، ويعود السبب في اختيار هذه البارامترات هو أن نسبة تسليم الرزم والإنتاجية تستخدم لتقييم أداء الشبكة حيث أنه كلما كانت قيم هذه المعايير أعلى كان الأداء أفضل في حين يستخدم عبء التوجيه لحساب تكلفة تطبيق بروتوكول التوجيه في الشبكة وذلك من حيث عدد رزم التوجيه التي يولدها لإيجاد المسارات بين المرسل والمستقبل وصيانتها وتعرف هذه البارامترات كما يلي:

نسبة تسليم الرزم packet delivery ratio PDR : طالما أن المهاجم يعمل على إهمال رزم البيانات لذا ستنخفض هذه النسبة في بروتوكول blackhole AODV وهي نسبة عدد الرزم الكلية المستقبلة من قبل العقد الهدف إلى عدد الرزم الكلية المرسلة من العقد المصدر [12] وتعطى بالعلاقة:

$$\text{PDR} = \frac{\sum \text{number of packets received } by\ the\ CBR\ destinations}{\sum number\ of\ packets\ sent\ by\ the\ CBR\ sources} \quad (1)$$

متوسط إنتاجية الشبكة Average Throughput [kbps] : تمثل مقدار البيانات المستقبلة من قبل عقد الشبكة مقدرة بالبت خلال زمن المحاكاة [12]، وستتناقص بوجود الهجوم وذلك لأن المهاجم يمنع وصول الرزم للهدف وتعطى بالعلاقة:

$$\text{Average Throughput} = \frac{\sum \text{number of packets received } by\ the\ CBR\ destinations}{simulation\ time} \quad (2)$$

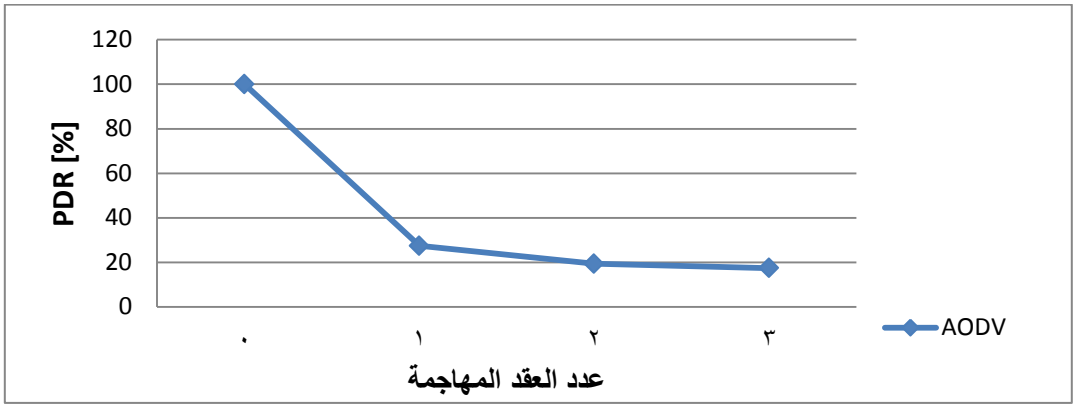
عبء التوجيه الطبيعي Normalized routing load: هو نسبة مجموع عدد رزم التوجيه المستقبلة على عدد رزم البيانات المستقبلة [14]، ويعطى بالعلاقة :

$$NRL = \frac{\sum total\ number\ of\ routing\ packets\ received}{\sum total\ number\ of\ data\ packets\ received} \quad (3)$$

النتائج والمناقشة:

نتائج السيناريو الأول: تبين النتائج الموضحة بالأشكال (1)و(2)و(3) أداء شبكة MANET تستخدم بروتوكول التوجيه AODV في الحالة الطبيعية دون وجود هجوم (عُبّر عن هذه الحالة بعدد عقد مهاجمة يساوي الصفر) وفي حالة التعرض لهجوم الثقب الأسود من قبل عدد من العقد المهاجمة غير المتعاونة (عقدة وعقدتين وثلاث عقد مهاجمة).

تبين النتائج الموضحة في الشكل (1) أن وجود عقدة مهاجمة في الشبكة أدى إلى انخفاض في نسبة تسليم الرزم PDR حيث أصبحت 28% بعد أن كانت 100% في الحالة الطبيعية (مع الأخذ بالاعتبار أنه لا يوجد ضياع بالرزم بسبب ظروف خارجية كالتشويش الذي قد يؤثر على الوصلة)، ويفسر الضياع الكبير في الرزم بأن المهاجم يعمل على إسقاط رزم البيانات جميعها التي تصله بدلاً من إعادة إرسالها إلى هدفها [15] لذا ستصل نسبة تسليم الرزم في بعض الاتصالات للصفر، لكن يوجد في سيناريو العمل أكثر من اتصال CBR بين العقد لذا لا تنخفض قيمة PDR في الشبكة ككل للصفر، كما نلاحظ من الشكل أن هذه النسبة استمرت بالتناقص مع ازدياد عدد العقد المهاجمة حيث وصلت الى 18% عند وجود ثلاث عقد مهاجمة.

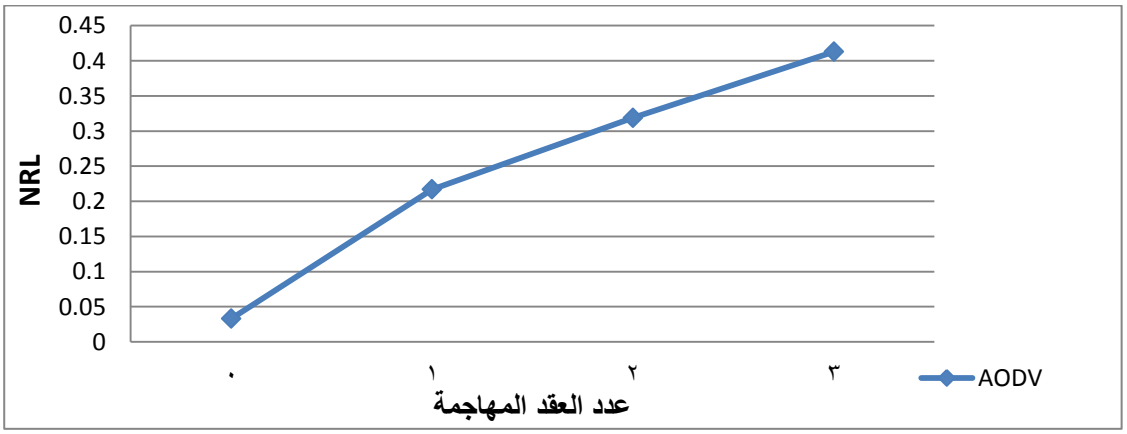


الشكل (1):العلاقة بين نسبة تسليم الرزم وعدد العقد المهاجمة في شبكة MANET

كما يبين الشكل (2) أن وجود عقدة مهاجمة في الشبكة أدى إلى انخفاض إنتاجية الشبكة حيث أصبحت 23 kbps بعد أن كانت 68 kbps في الحالة الطبيعية، ويفسر ذلك بأن المهاجم يعمل على إسقاط رزم البيانات التي تصله بدلاً من إعادة إرسالها إلى أهدافها ، كما نلاحظ من الشكل أن الانتاجية استمرت بالتناقص مع ازدياد عدد العقد المهاجمة حيث وصلت الىkbps 15 عند وجود ثلاث عقد مهاجمة.

الشكل (2):العلاقة بين متوسط الإنتاجية وعدد العقد المهاجمة في شبكة MANET

كما ويوضح الشكل (3) أن عبء التوجيه الطبيعي NRL ازداد حتى 0.22 بوجود عقدة مهاجمة مقارنة بـ 0.033 بدون وجود هجوم، وأنه استمر بالتزايد مع زيادة عدد المهاجمين حيث وصل الى 0.41 عند وجود ثلاث عقد مهاجمة، ويفسر ذلك بتناقص عدد رزم البيانات الواصلة الى أهدافها بسبب إهمال المهاجم لرزم البيانات مع بقاء عدد رزم التحكم الخاصة بالتوجيه كما هو.



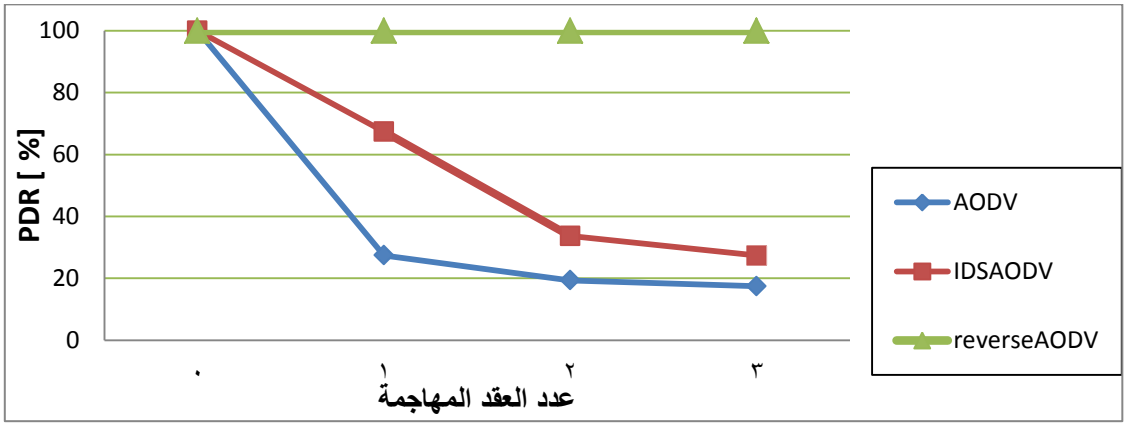
الشكل (3):العلاقة بين عبء التوجيه الطبيعي وعدد العقد المهاجمة في شبكة MANET

وتؤكد النتائج السابقة على الأثر الضار لهجوم الثقب الأسود على أداء الشبكة.

<u>نتائج السيناريو الثاني:</u>

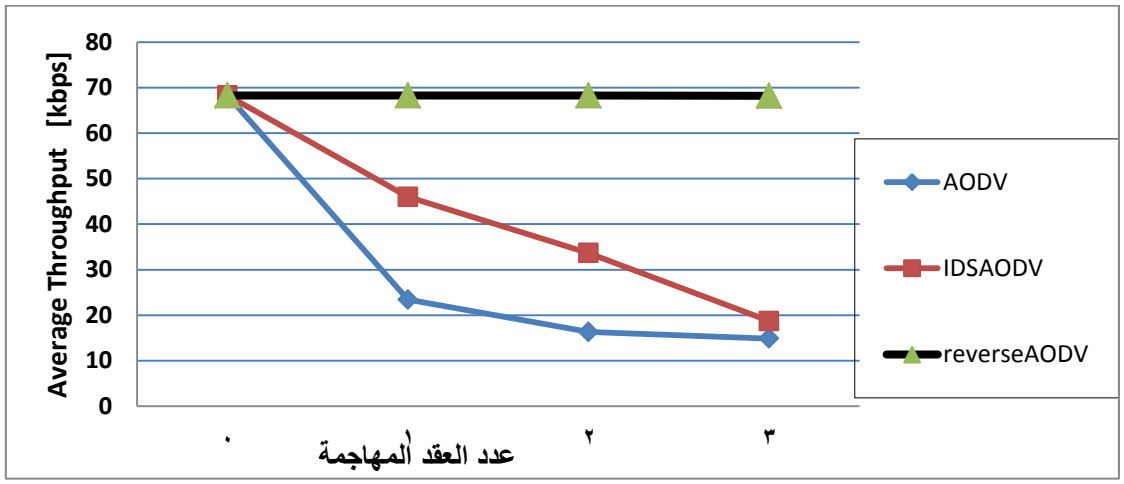
أظهرت نتائج المحاكاة بعد تطبيق كل من البروتوكولين IDSAODV, Reverse AODV في الشبكة ، أن كل من البروتوكولين حسّن من أداء الشبكة لكن بنسب مختلفة. يبين الشكل (4) أن البروتوكول IDSAODV زاد نسبة تسليم الرزم حتى 68% عند وجود عقدة مهاجمة مقارنة بـ 28% في نفس الشبكة عند استخدم بروتوكول AODV. كما أنه حسّن من نسبة تسليم الرزم عند وجود عقدتين أو ثلاث عقد مهاجمة، إلا أنه لم يمنع تأثير الهجوم بشكل كلي حيث يعالج الرد الأول الخاطئ المرسل من العقدة المهاجمة الأولى ويقبل الرد التالي والذي قد يكون قادم من العقدة المهاجمة الثانية أو الثالثة وبالتالي لن يستطيع كشف العقد المهاجمة الثلاث. كما نلاحظ من نفس الشكل أن البروتوكول ReverseAODV رفع نسبة تسليم الرزم حتى 100 % من أجل عقدة مهاجمة أو أكثر، ويفسر ذلك بأن هذا

البروتوكول لا يسمح للعقدة المهاجمة بالإعلان عن نفسها بأنها تملك المسار الصحيح والاحدث إلى الهدف وينتظر الرد من الهدف الحقيقي. كما أنه يستبدل المسار الحالي المستخدم لنقل البيانات بمسار آخر عند ملاحظته عدم وصول الرزم الى هدفها وفقاً لهذا المسار.



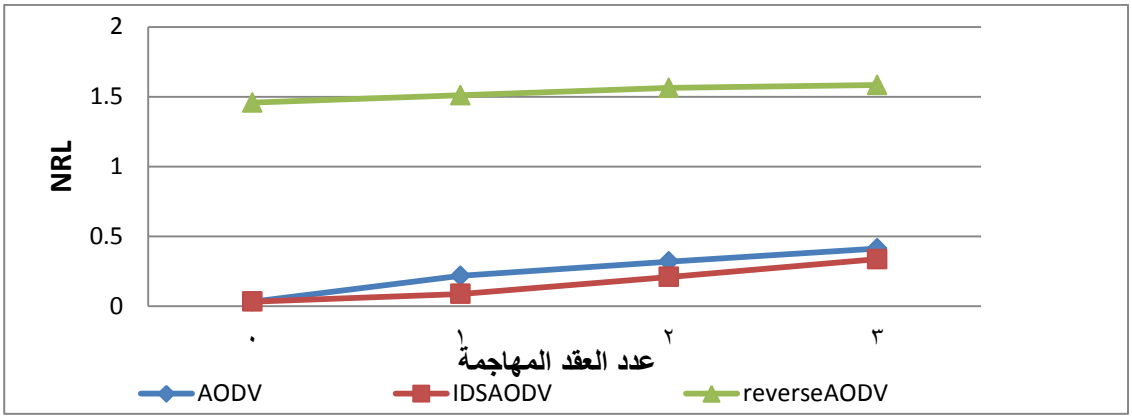
الشكل (4):العلاقة بين نسبة تسليم الرزم وعدد العقد المهاجمة عند استخدام AODV, IDSAODV, ReverseAODV

ويبين الشكل (5) أن البروتوكول IDSAODV زاد انتاجية الشبكة حتى 46 kbps عند وجود عقدة مهاجمة مقارنة بـ 23 kbps- في نفس الشبكة المعرضة للهجوم والتي تستخدم بروتوكول AODV ، كما أنه حسّن من انتاجية الشبكة عند وجود عقدتين مهاجمتين، بينما كان التحسن طفيفاً عند وجود ثلاث عقد مهاجمة بسبب توقعه الخاطئ لرزمة الرد التالية . بينما نلاحظ من نفس الشكل أن البروتوكول ReverseAODV رفع الانتاجية حتى 68 kbps مهما اختلف عدد المهاجمين وهو نفسه انتاجية الشبكة في حالة عدم وجود هجوم في الشبكة ويعود تفسير ذلك الى انخفاض عدد الرزم المستقبلة عند الهدف بالتالي تناقص معدل الإنتاجية .



الشكل (5):العلاقة بين إنتاجية الشبكة وعدد العقد المهاجمة عند استخدام AODV, IDSAODV, ReverseAODV

كما يتضح من الشكل (6) أن الـ IDSAODV لم يسبب أي عبء توجيه إضافي، لأنه لم يستخدم أية رزمة تحكم إضافية، بينما تسبب ReverseAODV بزيادة في حمل التوجيه الطبيعي وذلك بسب عمله الذي يعتمد على غمر رزمة الـ R-RREQ في الشبكة، أما AODV فانه يرسل رزمة رد واحدة على طول المسار العكسي، ويزداد هذا العبء بشكل نسبي بازدياد المهاجمين.



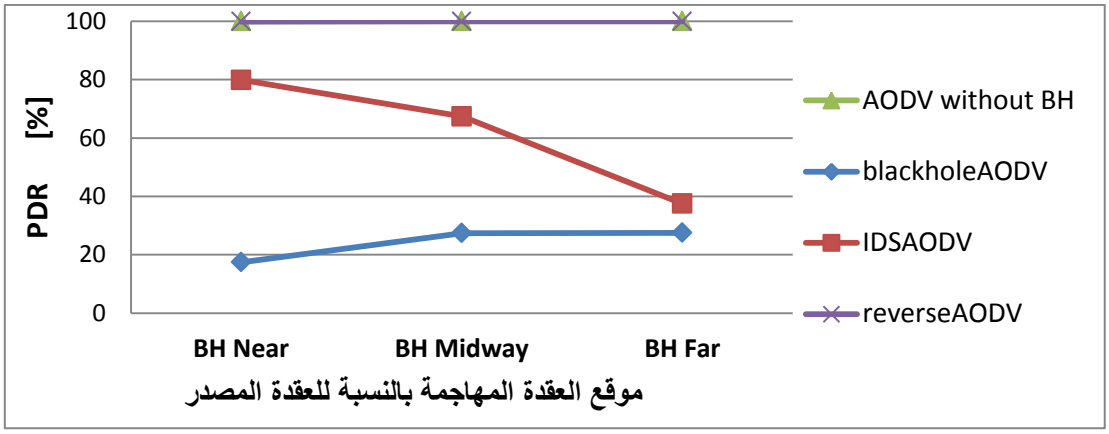
الشكل (6):العلاقة بين عبء التوجيه الطبيعي وعدد العقد المهاجمة في ظل AODV, IDSAODV, ReverseAODV

<u>نتائج السيناريو الثالث:</u> يهدف هذا السيناريو إلى دراسة مدى تأثر أداء كل من البروتوكولين IDSAODV، ReverseAODV بموقع العقدة المهاجمة.

اخترنا في هذا السيناريو عقدة مرسلة واحدة وأخرى مستقبلة في الشبكة وحددنا موقع العقدة المهاجمة وفقاً لثلاث حالات، الأولى: المهاجم قريب من العقدة المرسلة BH near، الثانية: المهاجم يقع بمنتصف المسافة بين المرسل والمستقبل BH midway ، الثالثة: المهاجم بعيد عن العقدة المرسلة BH far وذلك بهدف دراسة مدى تأثر أداء كل من البروتوكولين IDSAODV ، ReverseAODV بموقع العقدة المهاجمة حيث قمنا بتمثيل حالات موقع العقدة الثلاث على المحور الأفقي. ننوه في هذا السيناريو أننا اخترنا العقد المرسلة والمستقبلة التي تتحرك بذات الاتجاه وبذات الخطوة(إلى مواقع قريبة منها أيضاً) وبالتالي المسافة من العقدة المهاجمة للعقدة المرسلة مساوياً بشكل تقديري للمسافة بين العقدة المستقبلة والعقدة المهاجمة في حالة المهاجم في المنتصف. .

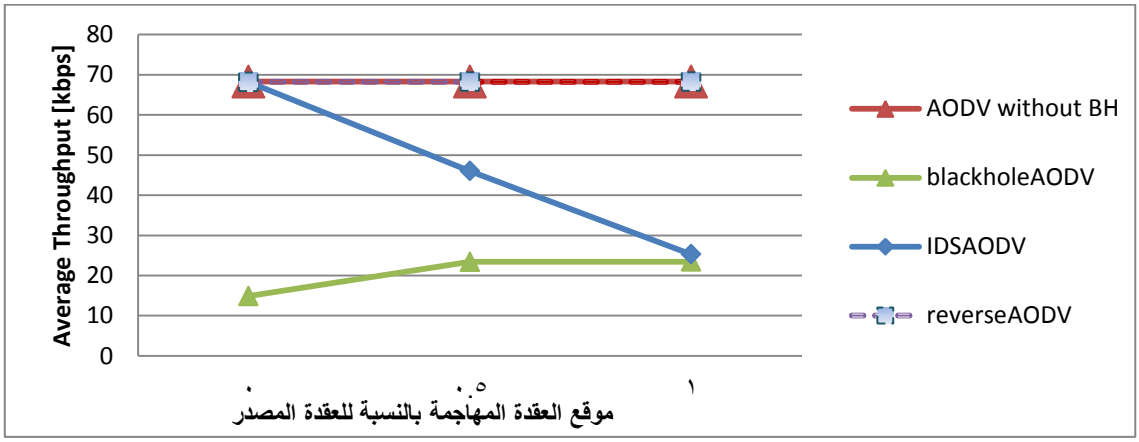
يبين الشكل(7) أن نسبة تسليم الرزم عند استخدام IDSAODV تكون أفضل عندما يكون المهاجم بالقرب من العقدة المرسلة، بينما نلاحظ انخفاض نسبة تسليم الرزم كلما ابتعد المهاجم عن المرسل ويعود السبب في ذلك الى أن البروتوكول IDSAODV يعمل على إهمال رزمة الرد الأولى متوقعاً بأنها قادمة من مهاجم ويعتمد على رزمة الرد الثانية، فكلما كان المهاجم أقرب إلى المرسل سيكون الرد القادم منه أسرع وبالتالي سيكون توقع البروتوكول صحيحاً إلا أن توقعه قد يكون خاطئاً وقد يتسبب بنتائج عكسية عندما يكون المهاجم بعيداً عن المرسل مما يتسبب برفض رسالة الرد الحقيقية وقبول رسالة رد المهاجم مما يؤدي لانخفاض نسبة تسليم الرزم.

كما نلاحظ من نفس الشكل أن نسبة تسليم الرزم التي قدمها ReverseAODV لم تتأثر بموقع العقدة المهاجمة في الحالات الثلاث، ويعود ذلك الى عدم استجابة هذا البروتوكول لأي رد قادم من عقدة مهاجمة أياً كان موقعها وانتظاره للرد القادم من المستقبل الحقيقي.



الشكل (7): العلاقة بين نسبة تسليم الرزم وموقع العقدة المهاجمة عند استخدام AODV, IDSAODV, ReverseAODV

كما ويوضح الشكل(8) أن إنتاجية الشبكة عند استخدام IDSAODV تكون أفضل عندما يكون المهاجم بالقرب من العقدة المرسلة، بينما نلاحظ انخفاض نسبة تسليم الرزم كلما ابتعد المهاجم عن المرسل، كما يظهر من الشكل أن الانتاجية التي قدمها ReverseAODV لم تتأثر بموقع العقدة المهاجمة في الحالات الثلاث ويعود سبب ذلك إلى إهمال الرد القادم من العقدة الخبيثة واستخدام مسار توجيه آخر وبالتالي معدل وصول عالي للرزم عند الهدف.



الشكل (8): العلاقة بين متوسط الإنتاجية وموقع العقدة المهاجمة عند استخدام AODV, IDSAODV, ReverseAODV

نستنتج من السيناريوهين السابقين ، أن البروتوكول Reverse AODV حقق نتائج أفضل من حيث الإنتاجية ونسبة تسليم الرزم عند وجود هجوم بمهاجم واحد أو أكثر في الشبكة، إلا أنه تسبب بزيادة في عبء التوجيه الطبيعي، لذا يعتبر الأنسب لاكتشاف هجوم الثقب الأسود كما أنه لم يتأثر بموقع العقدة المهاجمة في الشبكة.

ويلخص الجدول(2) النتائج التي توصلنا اليها في هذا البحث.

الجدول (2): ايجابيات وسلبيات البروتوكولين IDSAODV و ReverseAODV

البروتوكول	استخدام رزم توجيه إضافية	المزايا	المساوئ
IDSAODV	لم يستخدم أي رزم تحكم إضافية	حسّن من نسبة تسليم الرزم ومن الإنتاجية وبعبء توجيه قليل	تأثره بموقع العقدة المهاجمة على المسار بين المصدر والهدف وعدم عمله بالشكل الصحيح عندما تكون بعيدة عن المصدر.
Reverse AODV	استخدم رزمة الرد العكسي R-RREQ	حسّن من نسبة تسليم الرزم حتى 100% تقريباً وقدم متوسط إنتاجية عالٍ	يسبب زيادة بعبء التوجيه الطبيعي مقارنة بـ AODV

الاستنتاجات والتوصيات:

بالاستناد إلى نتائج السيناريوهات السابقة يمكن استنتاج ما يلي:

- إن وجود هجوم الثقب الأسود في شبكة MANET تستخدم بروتوكول التوجيه AODV يتسبب في تناقص كل من الإنتاجية ونسبة تسليم الرزم كما يسبب NRL عالٍ، ويسوء أداء الشبكة بزيادة عدد العقد المهاجمة.
- إن بروتوكول IDSAODV قادر على التخفيف من أثر هجوم الثقب الأسود ويحسن نسبة تسليم الرزم ومتوسط الانتاجية ، لكن أداءه يسوء عند ازدياد عدة مهاجمين.
- إن موقع العقدة المهاجمة بالنسبة للعقدة المرسلة تؤثر على أداء الشبكة، حيث ينخفض أداء الشبكة كلما اقترب المهاجم من المرسل.
- يستطيع بروتوكول IDSAODV تحسين أداء الشبكة عندما تكون العقدة المهاجمة قريبة من المصدر بشكل أكبر مما هي عليه عندما تكون بعيدة عن المصدر.
- إن بروتوكول ReverseAODV يقدم نتائج أفضل من IDSAODV من ناحية نسبة تسليم الرزم والإنتاجية لكنه يتسبب بعبء توجيه كبير نسبياً مقارنة بـ IDSAODV .
- اختبر هذا البحث من أجل عقد مهاجمة ثابتة، لذا نوصي بدراسة أداء الشبكة في حالة عقد مهاجمة متحركة.
- هناك العديد من الخوارزميات المقترحة لاكتشاف هجوم الثقب الأسود غيرIDSAODV , ReverseAODV منها ما يعتمد على التعلم الآلي ومنها ما يعتمد على الثقة، لذلك نوصي بدراسة هذه التقنيات واختيار التقنية الأفضل والأقل تكلفة. كما يمكن دراسة الهجمات التي تستهدف بروتوكولات التوجيه الأخرى.

References:

[1] WANG,X. *MOBILE ADHOC NETWORK S:APPLICATIONS*, 2011, p 524.

[2] ULLAH, I and SHOAIB.U.R, *Analysis of Black Hole attack On MANETS Using different MANET Routing Protocols*, 2010, p41.

[3] SOBEIH, M. YASSIN . *Study of performance AODV and OLSR Routing Protocols Under the influence of the Black Hole Attack in AD-HOC Networks with High Traffic Load.* Tishreen University Journal for Research and Scientific Studies - Engineering Sciences Series, Vol.39, Iss.1.2017, pp.197-213.

[4] ARORA.N and BARWAR. N.C, *Evaluation of AODV, OLSR and ZRP Routing Protocols under Black hole attack*. International Journal of Application or Innovation in Engineering & Management (IJAIEM), Vol.3 Iss 4, 2014, pp. 285-288.

[5] DOKURER,S. *Simulation of Back hole attack in wireless ad-hoc networks.* 2006, p66.

[6] SIMRANJIT ,N.K and ARORA, S. K. *Analysis of Black Hole Effect and Prevention through IDS in MANET*. American Journal of Engineering Research (AJER), Vol.2 Iss.10, 2013, pp. 214-220.

[7] GURUNG, SH and CHAUHAN, S. *A survey of black-hole attack mitigation techniques in MANET: merits, drawbacks, and suitability*. Springer Science , 2019, p31.

[8] TAN.D.N, HIEU,T and TAN.V.L. *IMPLEMENTATION OF BLACK HOLE ATTACK ON AODV ROUTING PROTOCOLS IN MANET USING NS2.* Journal of Science and Technology, ISSN 2354-0575, 2020, pp.45-51.

[9] BABU.B; NAGARAJU.C and PRASAD.K.M. *An Implementation and Performance Evaluation Study of AODV, MAODV, RAODV in Mobile Ad hoc Networks*. International Journal of Scientific & Engineering Research, Vol .4,Iss. 9, 2013, pp. 691-695.
[10] SHREE.O and OGWU.F. *A Proposal for Mitigating Multiple Black Hole Attack in Wireless Mesh Networks*. Wireless Sensor Network (SciRes), Vol.5, 2013, pp. 76-83.
[11] MAALA, B. *Study of DDOS Attack Impact on Vehicular Ad Hoc Network in City* . Tishreen University Journal for Research and Scientific Studies - Engineering Sciences Series,Vol.37,Iss.2, 2015, pp.211-230.
[12] FALL,K and VARADHAN,K . *The ns Manual,* pp.1-434.
[13] KIM.CH,TALIPOV.E and AHN.B. *A Reverse AODV Routing Protocol in Ad Hoc Mobile Networks.* IFIP International Federation for Information Processing LNCS 4097, 2006, pp. 522 – 531.
[14] THAKUR, B; PATEL, SH ;VERMA, Ashok and DUBEY ,SH. *Simulation of Black hole Nodes and Prevention Using IDS for MANET Reactive Routing Protocol AODV*. International Journal of Computer Sciences and Engineering(IJCSE) Vol.2, Iss.12, 2014, pp.114-120.
[15] Ahmed,A; Hanan,A and Osman.I. *Description of Black Hole Attack Behaviour in MANET*. International Journal of Computer Networks and Communications Security, VOL. 4 NO. 12, DECEMBER 2016, pp.322–329
[16] GOSWAMI,M; SHARMA,P and BHARGAVA,A. Black Hole Attack Detection in MANETS using Trust Based Technique. International Journal of Innovative Technology and Expioring Engineering (IJITEE) Vol.9 Iss.4 ,2020, pp. 1447-1451.
[17] YASSEIN. B,M; HMEIDI,I ;KHAMAYSE,Y ; AL-ROUSAN,M AND ARRABI,D. *BLACK HOLE ATTACK SECURITY ISSUESCHALLENGES & SOLUTION IN MANET*. Faculty of Computer & Information Technology, University of Science and Technology CS & IT-CSCP, Irbid, Jordan, 2018, pp. 199–207.