مجلة جامعة طرطوس للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (6) العدد(11) 2022
Tartous University Journal for Research and Scientific Studies - engineering Sciences Series Vol. (6) No. (11) 2022

تخفيف أثر هجوم الثقب الأسود في شبكات MANET بالاعتماد على نظام كشف التسلل لبروتوكول AODV

د. محمد علي عنبر*

م. مرح عيسى كناج**

(تاريخ الإيداع 2022/5/19 . قُبِل للنشر في 2022/11/17)

□ ملخّص□

يعتبر هجوم الثقب الأسود من أخطر الهجمات الأمنية والأكثر شيوعاً. يستهدف هذا النوع من الهجمات الشبكات اللاسلكيّة الخاصّة النقّالة MANET بشكل خاص. ونظراً لأهمية شبكات MANET فقد اتجه الباحثون لإيجاد تقنيات لكشف هذا الهجوم، ومن بين هذه التقنيات نظام كشف التسلل لبروتوكول AODV.

تم في هذا البحث دراسة تأثير هجوم الثقب الأسود على أداء الشبكة وذلك في ظل وجود مهاجم واحد ومن ثم مهاجمين، ثم تطبيق بروتوكول IDSAODV (بروتوكول محسن على بروتوكول AODV ضد هجوم الثقب الأسود) على الشبكة ذاتها بهدف تقييم أدائه ومدى فعاليته في كشف هجوم الثقب الأسود والتخفيف من آثاره، حيث تم اعتماد متوسط الإنتاجية ونسبة تسليم الرزم وحمل التوجيه الزائد كمقاييس للأداء.

أظهرت نتائج المحاكاة أنَّ بروتوكول IDSAODV خفّفَ من تأثير هجوم الثقب الأسود، حيث قدّم أفضل النتائج بالنسبة لإنتاجية الشبكة ونسبة تسليم الرزم بنسب وصلت إلى 100%، وبالنسبة لحمل التوجيه الزائد فقد انخفضت بشكل جيد لتصبح 1%. كما أظهرت نتائج المحاكاة تأثر أداء بروتوكول IDSAODV بزيادة سرعة حركة العقد في الشبكة.

الكلمات المفتاحية: شبكات MANET، هجوم الثقب الأسود، بروتوكول توجيه شعاع المسافة عند الطلبAODV، نظام كشف التسلل لبروتوكول AODV.

*مدرس في قسم هندسة تكنولوجيا الاتصالات – كليّة هندسة تكنولوجيا المعلومات والاتصالات – جامعة طرطوس .

**طالبة دراسات عليا (ماجستير) في قسم هندسة تكنولوجيا الاتصالات – كليّة هندسة تكنولوجيا المعلومات والاتصالات –جامعة طرطوس .

مجلة جامعة طرطوس للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (6) العدد(11) 2022
Tartous University Journal for Research and Scientific Studies - engineering Sciences Series Vol. (6) No. (11) 2022

Mitigating the Impact of Black Hole Attack in MANETs based on the Intrusion Detection System of AODV Protocol

Dr. Mohammad Ali Anbar*
Eng. Marah Essa Knaj**

(Received 19/5/ 2022 . Accepted 17/11/ 2022)

ABSTRACT

Black Hole Attack is one of the most serious and the most common security attacks in MANET networks. Due to the importance of MANETs, researchers have tried to find techniques to discover this attack. One of these techniques is Intrusion Detection System AODV (IDSAODV).

In this research, the effect of Black Hole Attack on network performance, in the presence of one attacker then two attackers, has been studied. After that, IDSAODV (enhanced AODV against Black Hole Attack) has been applied to evaluate its effectiveness in detecting the attack and mitigating its effects. Average Throughput, Packet Delivery Ratio and Routing Overhead parameters have been used for performance evaluation.

The results of the extensive simulation showed that the IDSAODV Protocol reduced the impact of Black Hole Attack, where it presented the best results for Average Throughput and Packet Delivery Ratio with percentages reached to 100%, and Routing Overhead reduced to 1%. The simulation results also showed that the performance of the IDSAODV Protocol was affected by increasing the speed of nodes in network.

Key Words: MANETs, Black Hole Attack, AODV, IDSAODV.

*Teacher, Communication Technology Engineering Department, Information and communication Technology Engineering, Tartous University, Syria.

** Master student, Communication Technology Engineering Department, Information and communication Technology Engineering, Tartous University, Syria

1- المقدمة

تُعرَّف الشبكات اللاسلكيّة الخاصّة النقّالة MANETs بأنها نوع من شبكات Ad-Hoc وتتألف من مجموعة من العقد اللاسلكيّة المُتحرّكة، المُستقلّة والمدارة ذاتياً بدون وجود أية بنية تحتيّة أو نقطة وصول Access Point [1]. تتعاون العقد فيما بينها لإيصال الرسائل إلى أهدافها باستخدام بروتوكولات توجيه مسؤولة عن إيجاد المسارات بين العقد المرسلة والمستقبلة ويعتبر بروتوكول AODV من أشهر هذه البروتوكولات وأكثرها استخداماً [2].

تعد عملية التوجيه Routing من القضايا المهمة في عمل هذه الشبكات والتي تتأثر بالهجمات الأمنية، ويعتبر هجوم الثقب الأسود Black Hole Attack الذي يقوم بإسقاط رزم البيانات ومنعها من الوصول إلى وجهتها المنشودة [3] من الهجمات التي تهدد عملية التوجيه في هذه الشبكات.

يتمثل هجوم الثقب الأسود في شبكات MANET بعقدة خبيثة " Malicious node " 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. بالتالي فإن جميع العقد ستوجه رزم البيانات إلى هذه العقد الخبيثة. تم في هذا البحث استخدام محاكي الشبكات NS2 لبناء نموذج لشبكة MANET ومحاكاتها في حال استخدامها لبروتوكول التوجيه AODV ودراسة سلوكها وأدائها تحت تأثير وجود عقد الثقب الأسود داخل الشبكة وفي حال تطبيق بروتوكول IDSAODV لكشفها والتخفيف منها.

2- هدف البحث وأهميته

يهدف هذا البحث إلى اكتشاف هجوم الثقب الأسود والتخفيف من آثاره على الشبكة وذلك من خلال تطبيق بروتوكول IDSAODV. وتأتي أهمية البحث من ضرورة الحفاظ على استمرارية عمل شبكات MANET ذات الطبيعة الحساسة حتى في حال حدوث ثغرات أمنية.

3- طرائق البحث ومواده

اعتمد هذا البحث في تنفيذه على العديد من المراجع والدراسات العلميّة الحديثة [13-4] المختصّة بمجال الشبكات اللاسلكيّة الخاصّة النقّالة وأمنها، والمعنيّة بدراسة هجوم الثقب الأسود والتقنيات المستخدمة للتخفيف من آثاره. وتمت الدراسة العمليّة بالاعتماد على محاكي الشبكات الشهير NS-2.35 لمحاكاة هجوم الثقب الأسود وللتخفيف من آثاره على الشبكة.

3-1 الشبكات اللاسلكيّة الخاصّة النقّالة (Mobile Ad-Hoc Networks) MANETs

إن الهدف الأساسي من الشبكات اللاسلكيّة هو التخلص من الحاجة إلى الربط السلكي وتحقيق إمكانية الاتصال في أي مكان وبأي وقت. كما أن إنشاء شبكة ذات بنية تحتية سلكيّة يترتّب عليه كلفة أعلى من الشبكة اللاسلكيّة [15]، مما يجعل الشبكات اللاسلكيّة خياراً مناسباً. حالياً يوجد العديد من أنواع الشبكات اللاسلكيّة المتاحة مثل شبكات الحساسات اللاسلكيّة Wireless Sensor Networks(WSNs) والشبكات الخاصّة النقّالة Mobile Ad hoc Networks (MANET).

تعرف الشبكات اللاسلكيّة الخاصّة النقّالة بأنها نوع من الشبكات التي تنشأ بشكل آني من مجموعة من العقد المتحركة والمتصلة فيما بينها، إذ بإمكان كل عقدة التحرك بشكل عشوائي وبسرعة معينة في أي اتجاه والاتصال مع غيرها من العقد دون الحاجة لأي نوع من الوصلات أو التهيئة المسبقة و دون الاعتماد على عقدة مركزية.

العقد يمكن أن تعمل كمضيف أو كموجه لكشف المسار وإرسال رزم البيانات إلى العقد الأخرى في الشبكة [14].

3-2 التوجيه في شبكات MANET

يعد التوجيه من القضايا المهمة في عمل شبكاتMANET، و يقصد بالتوجيه إرسال الرسالة من العقدة المصدر إلى عقدة تالية (next hop) حتى الوصول إلى العقدة الهدف عن طريق بناء جداول التوجيه. وبما أن طوبولوجيا شبكات MANET تتغير باستمرار نتيجة انضمام عقد جديدة وخروج عقد أخرى، وكذلك حركية العقد نفسها بالتالي تغير مناطق تغطية كل عقدة باستمرار، فإن عملية التوجيه تصبح أكثر تعقيداً مما دفع الباحثين إلى اقتراح عدة برتوكولات لتعالج عملية التوجيه في شبكات MANET.

3-3 بروتوكولات التوجيه في شبكات MANET

إن الهدف الأساسي من استخدام بروتوكول التوجيه هو إنشاء المسار الصحيح و الفعال بين زوج من العقد بحيث يمكن تسليم الرسائل في الوقت المناسب.

تقسم برتوكولات التوجيه في شبكات MANET وفقاً لاستراتيجية التوجيه إلى ثلاث أنواع [16] وهي:

- البرتوكولات التفاعلية Reactive Protocols
- البرتوكولات الاستباقية Proactive Protocols
- البرتوكولات الهجينة Hybrid Protocols

1) بروتوكولات التوجيه التفاعلية

هي بروتوكولات توجيه تقوم بإيجاد مسارات التوجيه في الشبكة عند الطلب. أي أن مسارات التوجيه لا تبنى إلا عند الحاجة لها فقط وبالتالي فهي توفر عرض الحزمة، لكن هذا يزيد من التأخير في عملية توجيه الرزم ضمن الشبكة. كما أن استخدام هذا النوع من البرتوكولات يؤدي إلى تبادل أقل لمعلومات التحكم مقارنة مع برتوكولات النمط Proactive. ومن الأمثلة على هذه البرتوكولات بروتوكول توجيه شعاع المسافة عند الطلب Ad-hoc On Demand Distance Vector (AODV) .

2) بروتوكولات التوجيه الاستباقية

في هذه البروتوكولات يتم تبادل معلومات التوجيه بين جميع عقد الشبكة واتخاذ قرار التوجيه بغض النظر عن حاجة العقد لها، ويتم الاحتفاظ بمعلومات التوجيه في عدد من الجداول المختلفة ويتم تحديث هذه المعلومات بشكل دوري مما يجعل هذه البرتوكولات تستهلك الكثير من عرض الحزمة. ويعد برتوكول OLSR (Optimized Link State Routing)من أهم برتوكولات التوجيه الاستباقية.

3) بروتوكولات التوجيه الهجينة

تجمع هذه البروتوكولات 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. وكمثال عنها بروتوكول توجيه المنطقة (ZRP(Zone Routing Protocol .

3-4 بروتوكول توجيه شعاع المسافة عند الطلب Ad hoc On-demand Distance (AODV)

هو بروتوكول تفاعلي يتكيف مع تغيرات الوصلات حيث أنه في حال اكتشاف فشل الوصلة، يتم إرسال رسائل الإعلام بالفشل إلى العقد المتأثرة فقط في الشبكة.

يستخدمAODV أربعة أنماط من الرسائل من أجل تحقيق عملية الاتصال بين العقد وهي كالآتي:

1. رسالة طلب المسار Route Request Message (RREQ)
2. رسالة الرد على طلب المسار Route Reply Message (RREP)
3. رسالة الخطأ في المسار Route Error Message (RERR)
4. رسالة الترحيب Hello Message

4- القضايا الأمنية وهجمات الثقوب في شبكات MANET

يشكل موضوع الأمن في شبكات MANET تحدياً كبيراً، وذلك بسبب حركة العقد المستمرة والطبولوجيا المتغيرة للشبكة باستمرار ومجال التغطية المحدود للعقد، لذلك تعتبر شبكات MANET عرضة للاختراق والتعرض للهجمات بشكل كبير والتي يمكن تنفيذها بسهولة على عكس الشبكات السلكية.

4-1 المتطلبات الأمنية لشبكات MANET

من أجل الحفاظ على بيئة موثوقة و أمنة في شبكات MANET لا بد من توفر خمسة أهداف أمان رئيسية [17]:

1) سرية البياناتConfidentiality
2) استمرارية الشبكة (Availability التوافرية)
3) موثوقية البياناتAuthentication
4) سلامة البياناتIntegrity
5) عدم الإنكار Non Repudiation

4-2 هجوم الثقب الأسود في شبكات MANET التي تستخدم بروتوكول التوجيهAODV

يصنف هجوم الثقب الأسود كنوع من هجوم رفض الخدمة DOS (Denial Of Service) [13] والذي يحدث في طبقة الشبكة [18]، ويعتبر هجوماً شهيراً ومعروفاً في AODV [19].

يمكن تلخيص عمل هذا الهجوم بالمراحل التالية [4]:

- عندما تريد العقدة المصدر إرسال رزم البيانات إلى عقدة أخرى، فإنها تقوم بعملية اكتشاف المسار من خلال إرسال رسالة طلب المسار RREQ إلى العقد الجيران لها.

- تقوم العقدة الخبيثة باستلام هذه الرسالة لترسل بدورها رسالة رد على طلب المسار RREP(Route Reply) للمرسل تخبره فيها بأن لديها المسار الصحيح نحو العقدة الهدف.
- عندما يستلم المرسل رسالة الرد الأولى RREP من العقدة الخبيثة يتجاهل رسائل RREPالقادمة 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 وجهتها الحقيقية بالتالي تعطل العقدة المهاجمة عمل الشبكة وتحقق هدفها المنشود.

4-3 نظام كشف التسلل لبروتوكولAODV: IDSAODV (Intrusion Detection System AODV)

هو بروتوكول محسن عن بروتوكول AODV [6] تم اقتراحه من قبل عدد من الباحثين لتحسين أداء شبكات MANET في حال وجود هجوم الثقب الاسود ويتم تطبيقه من خلال إجراء تعديل في عملية التوجيه ضمن بروتوكول AODV من خلال جعل العقدة المصدر (المرسلة) Source Node تتجاهل المسار المنشأ من قبل رزمة الرد الأولى والاستجابة لرزمة الرد الثانية، حيث أن هذا البروتوكول يفترض أن الرد الأول والأسرع سيكون دائماً من عقدة مهاجمة، لكن هذا الافتراض قد يكون غير صحيح فقد تكون العقدة المهاجمة بعيدة عن العقدة المصدر وقد تكون العقدة الهدف Destination Node بالقرب من العقدة المصدر، في هذه الحالة سيكون الرد الأول قادماً من عقدة الهدف الحقيقية وسيتم تجاهل هذا الرد والاستجابة للرد التالي الذي قد يأتي من العقدة المهاجمة. من مساوىء هذا البروتوكول أنه في حال كان الرد الأول من عقدة الهدف الحقيقية (غير المهاجمة) سيتم اعتبارها عقدة خبيثة وبالتالي سيتم ضياع كل رزم البيانات.

4-3-1 مراحل عمل خوارزمية بروتوكول IDSAODV

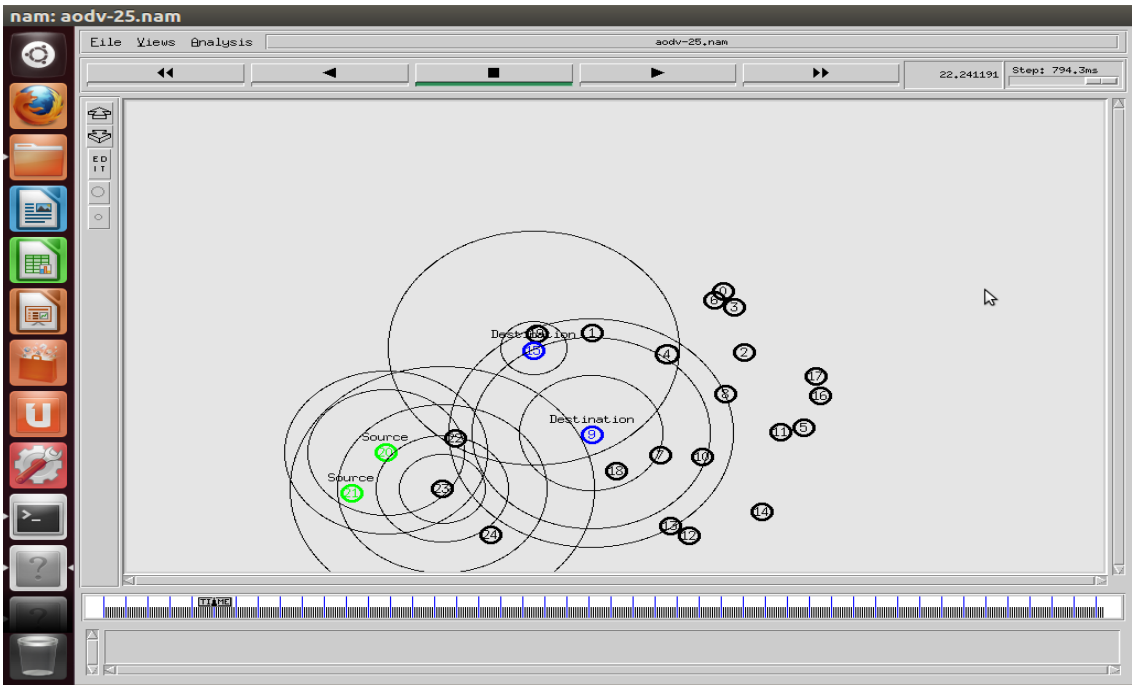
يمكن تلخيص مراحل عمل بروتوكول نظام كشف التسلل لبروتوكول AODV كما يلي [6]:

1-ترسل العقدة المصدر رسالة طلب مسار Route Request (RREQ) عبر بث عام Broadcast.
2-تستقبل العقدة المصدر رسائل الرد على طلب المسار المتعددة Route Reply (RREP).
3-تخزن العقدة المصدر رزمة RREP الأولى وتعتبرها قادمة من عقدة مهاجمة Malicious Node.
4-تقوم العقدة المصدر بقبول رزمة الرد الثانية وتعتبر أنها من عقدة موثوقة Trusted Node.
5-عندها تقوم العقدة المصدر بتحديث جدول توجيهها وتبدأ بإرسال البيانات.

5- النتائج والمناقشة

5-1 بيئة المحاكاة:

يوضح الشكل (1) نموذج لشبكة MANET المراد محاكاتها، حيث تتوضع العقد بشكل عشوائي ضمن مساحة محددة.



الشكل (1): التوضع العشوائي للعقد في الشبكة

الخطوة الأولى:

تم في هذه الخطوة بناء شبكة MANET مؤلفة من 25 عقدة متصلة لاسلكياً لها نفس الإمكانيات وتنتشر بمواقع بدائية عشوائية في منطقة مساحتها 1000*800 m وتتحرك بسرعة مبدئية 5 m/s (تمت زيادة السرعة لاحقاً ودراسة أداء الشبكة). تقوم بعض هذه العقد بتوليد رزم بيانات بحجم 1500 Bytes وإرسالها إلى أهداف محددة بمعدل 0.1 Mb/s مستخدمة بروتوكول AODV لتحديد المسارات إلى تلك الأهداف. ويوضح الجدول (1) بارامترات الشبكة التي تم اعتمادها.

الجدول (1): بارامترات الشبكة

البارامتر	القيمة
محاكي الشبكات	NS-2.35
نوع القناة	Wireless
زمن المحاكاة (ثانية)	200(s)
حجم الرزمة (بايت)	1500 (Bytes)
معدل تدفق البيانات (ميغا بت/ثانية)	0.1 (Mb/s)
بروتوكول التوجيه	AODV(without attack), BlackHoleAODV, IDSAODV
عدد العقد	25
عدد العقد المهاجمة	0 , 1 , 2
سرعة العقد (متر/ثانية)	5-10(m/s)
عدد اتصالاتCBR	4
نمط حركة البيانات	UDP
مساحة منطقة المحاكاة	(1000 * 800)

الخطوة الثانية:

تهدف إلى دراسة أداء شبكة MANET تستخدم بروتوكول AODV وتتعرض لهجوم الثقب الأسود من قبل مهاجم واحد ثم من قبل مهاجمين وذلك بهدف دراسة تأثير الهجوم على أداء الشبكة، حيث تم تطبيق بروتوكول هجوم الثقب الأسود على الشبكة السابقة ودراسة مقاييس الأداء الآتية (متوسط الإنتاجية – نسبة تسليم الرزم – حمل التوجيه الزائد) لدراسة تأثير الهجوم على الشبكة السابقة.

الخطوة الثالثة:

تهدف إلى تقييم أداء شبكة MANET تتعرض لهجوم الثقب الأسود من قبل مهاجم واحد ثم من قبل مهاجمين وذلك عند تطبيق بروتوكول IDSAODV بهدف دراسة فعالية هذا البروتوكول في كشف الهجوم والتخفيف من آثاره على أداء الشبكة، حيث تم تطبيق بروتوكول IDSAODV الذي يهدف للكشف عن هجوم الثقب الأسود والتخفيف من آثاره. تم تنفيذ العمل باستخدام أداة المحاكاة NS–2.35.

ملاحظة: القيمة (0) تعني قبل تطبيق الهجوم (الحالة الطبيعية بالاعتماد على بروتوكول التوجيه AODV).

أما القيمتان (1–2) للدلالة على عدد العقد المهاجمة.

5–2 مقاييس الأداء Performance Metrics

اعتُمد في دراسة هجوم الثقب الأسود وتقنية التخفيف من آثاره على مجموعة من مقاييس أداء الشبكات وهي متوسط الإنتاجية، نسبة تسليم الرزم، حمل التوجيه الزائد، وتُعرّف هذه المقاييس كما يلي [12]:

- متوسط إنتاجية الشبكةِ Average Throughput:

يعرّف بعدد البيانات المستقبلة من قبل عقد الشبكة مقدرة بالبت خلال الثانية ويعطى **بالعلاقة (1):**

العلاقة (1) $$\text{Average Throughput [kbps]} = \frac{\Sigma\, number\ of\ \text{packets}\ received\ by\ the\ CBR\ destinations}{Simulation\ Time}$$

- نسبة تسليم الرزم Packet Delivery Ratio (PDR):

هي نسبة الرزم الكلية المستقبلة من قبل العقد الهدف إلى عدد الرزم الكلية المرسلة من قبل العقد المرسلة وتعطى **بالعلاقة (2):**

العلاقة (2) $$\text{Packet Delivery Ratio [\%]} = \frac{\Sigma\, number\ of\ packets\ received\ by\ the\ CBR\ destinations}{number\ of\ packets\ sent\ by\ the\ CBR\ Sources}$$

- حمل التوجيه الزائد Routing Overhead (RH):

هو النسبة بين رزم التوجيه الكلية إلى عدد رزم البيانات الكلية المستقبلة من قبل العقد الهدف ويعطى **بالعلاقة (3):**

العلاقة (3) $$\text{Routing Overhead} = \frac{\Sigma\, number\ of\ Total\ routing\ packets}{\Sigma\, number\ of\ packets\ received\ by\ the\ CBR\ destinations}$$

نتائج الخطوة الأولى:

يظهر الجدول (2) نتائج مقاييس الأداء عندما تكون سرعة حركة العقد 5 m/s (االسرعة الافتراضية) قبل تطبيق هجوم الثقب الاسود (في الحالة الطبيعية بالاعتماد على بروتوكول AODV):

الجدول (2): قيم مقاييس الأداء قبل تطبيق هجوم الثقب الأسود

مقياس الأداء	AODV without BlackHole Attack
متوسط الإنتاجيةAverage Throughput (kbps)	38.21
نسبة تسليم الرزم Packet Delivery Ratio (%)	97.40
حمل التوجيه الزائد Routing Overhead	1.0267

نتائج الخطوة الثانية:

تبين النتائج في الجدول (3) قيم مقاييس الأداء عندما تكون سرعة حركة العقد في الشبكة هي 5 m/s (الافتراضية) في ظل وجود هجوم ثقب أسود بعقدة مهاجمة واحدة (BlackHoleAODV Attack–1) ثم في حال وجود عقدتي هجوم (BlackHoleAODV Attack–2)، حيث أنّ تنفيذ الهجوم سبّب تناقصاً في قيم إنتاجية الشبكة وقيم نسبة تسليم الرزم وبحمل توجيه زائد.

الجدول (3): قيم مقاييس الأداء عند تطبيق هجوم الثقب الأسود وبسرعة 5m/s

مقياس الاداء	1 – BlackHoleAODV Attack	2–BlackHoleAODV Attack
متوسط الإنتاجية (kbps)	25.10	21.39
نسبة تسليم الرزم (%)	14.79	12.19
حمل التوجيه الزائد	6.7615	8.2030

نتائج الخطوة الثالثة:

يوضح الجدول (4) قيم مقاييس الأداء وذلك عند تطبيق بروتوكول IDSAODV في ظل وجود عقدة ثقب أسود واحدة (IDSAODV – 1) في الشبكة ثم في ظل وجود عقدتي ثقب أسود (IDSAODV–2)، حيث أنّ تطبيق بروتوكول IDSAODV حسّن من قيم مقاييس الأداء بالمقارنة مع بروتوكول AODV وذلك عند تطبيق هجوم الثقب الأسود.

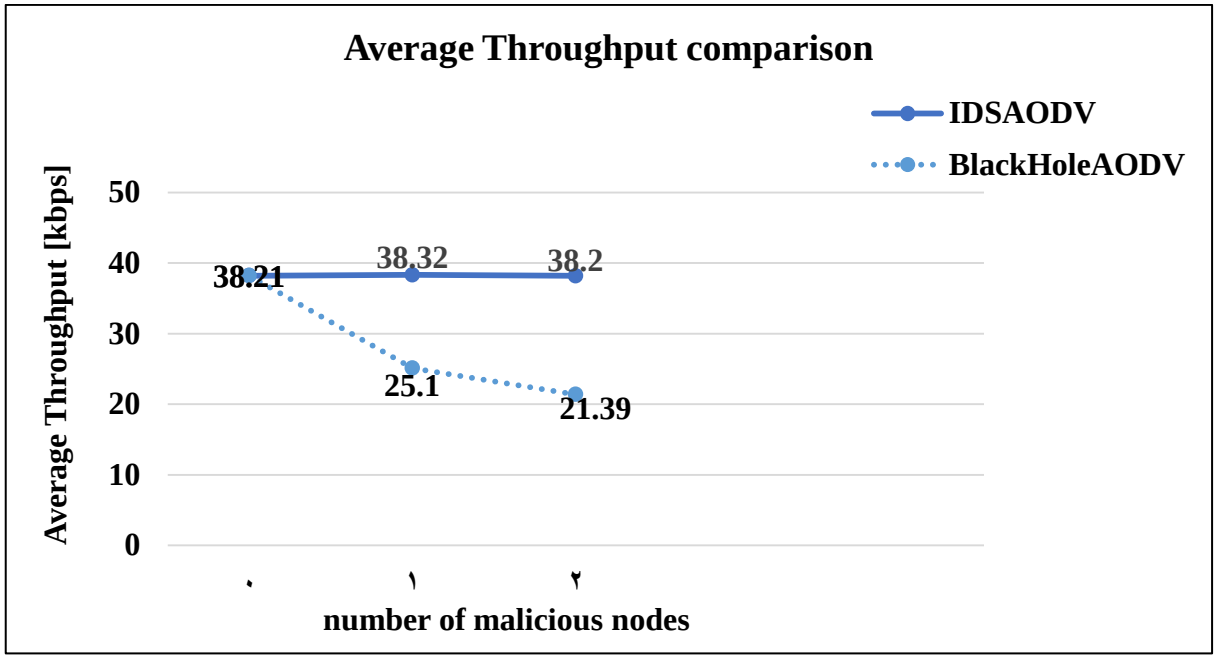
الجدول (4): قيم مقاييس الأداء عند تطبيق بروتوكول IDSAODV وبسرعة 5m/s

مقياس الاداء	1 – IDSAODV	2–IDSAODV
متوسط الإنتاجية (kbps)	38.32	38.20
نسبة تسليم الرزم (%)	100.00	89.42
حمل التوجيه الزائد	1.0000	1.1183

تظهر الأشكال (1)، (2)، (3) قيم مقاييس الأداء (متوسط الإنتاجية – نسبة تسليم الرزم – حمل التوجيه الزائد) في حالة سرعة حركة العقد 5 m/s والعقد المهاجمة على الترتيب (2–1–0) وذلك قبل وعند تطبيق هجوم الثقب الأسود وعند تطبيق بروتوكول IDSAODV المستخدم للتخفيف من أثر الهجوم.

يبيّن الشكل (1) أنّ وجود عقدة مهاجمة في الشبكة أدى إلى انخفاض في متوسط إنتاجية الشبكة Avgerage Throughput حيث كانت 38.2kbps في الحالة الطبيعية ثم تناقصت إلى 25.1 واستمرت القيمة بالتناقص حيث أصبحت 21.4 في ظل وجود عقدتي هجوم. ويُفَسَّر ذلك بأن المهاجم يهمل رزم البيانات التي تصله بالتالي فإن معدل وصول الرزم للعقد الهدف قليل بالتالي فإن معدل الإنتاجية قليل.

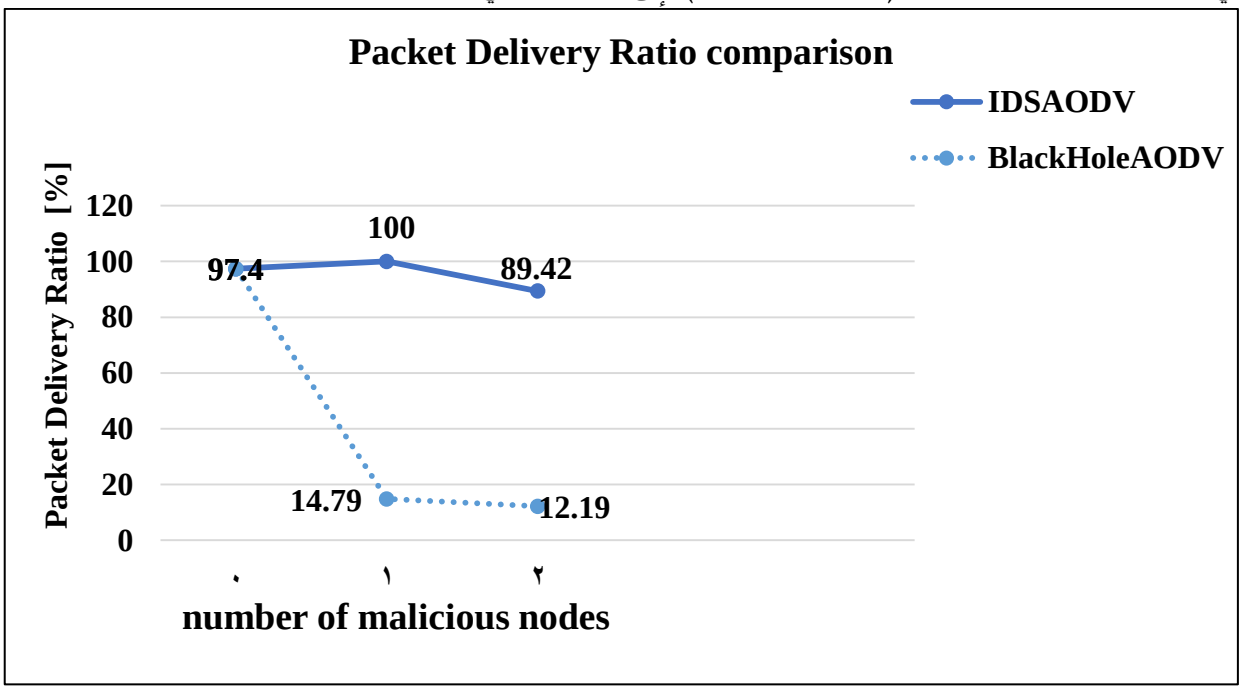
وعند تطبيق البروتوكول المُقتَرَح IDSAODV على الشبكة السابقة تحسّنت قيم متوسط الإنتاجية حيث وصلت إلى 38.32 وذلك في ظل وجود عقدة مهاجمة واحدة (IDSAODV – 1) كما أنه أعطى نفس القيمة تقريباً عند وجود عقدتين مهاجمتين.



الشكل (1): العلاقة بين متوسط الإنتاجية وعدد العقد المهاجمة عند تطبيق BlackHoleAODV, IDSAODV

كما يبيّن الشكل (2) أنّ وجود عقدة مهاجمة أدى لانخفاض في نسبة تسليم الرزم Packet Delivery Ratio حيث أصبحت 15% بعد أن كانت 97% في الحالة الطبيعية واستمرت هذه النسبة بالتناقص مع زيادة عدد العقد المهاجمة إلى عقدتين حيث وصلت إلى 12%. ويُفَسَّر ذلك بأن المهاجم يعمل على إسقاط رزم البيانات الواصلة إليه بدلاً من إعادة توجيهها وإرسالها إلى هدفها.

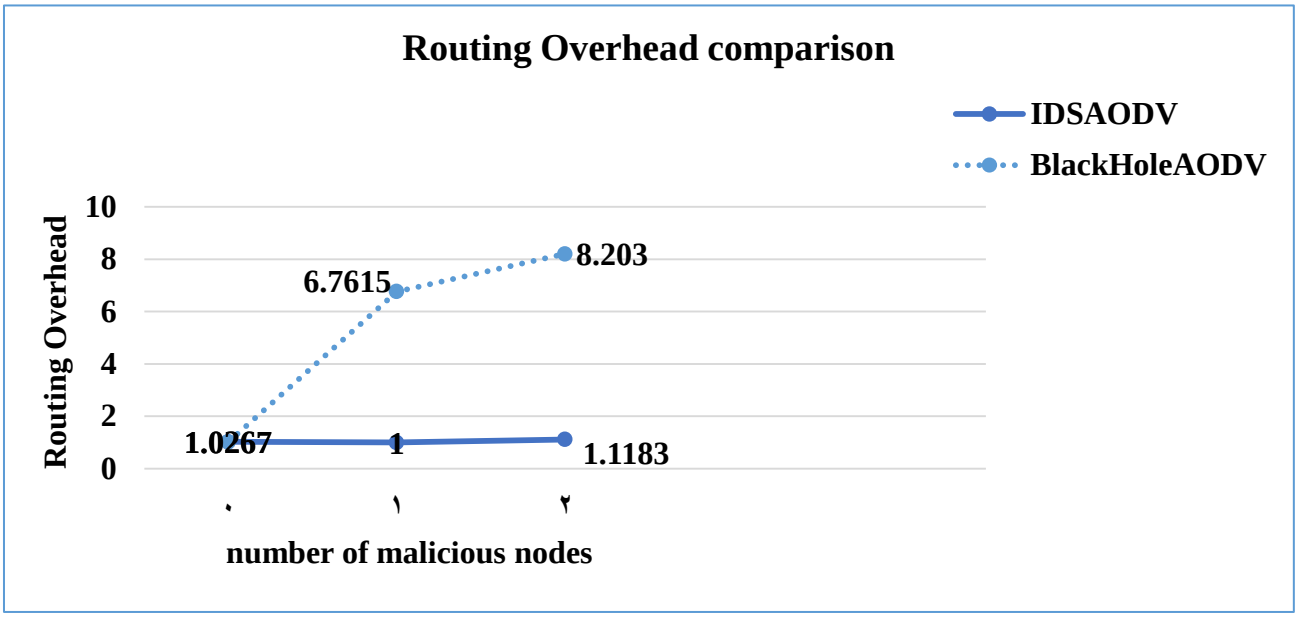
وبتطبيق البروتوكول IDSAODV فقد حسّن من نسبة تسليم الرزم بنسبة كبيرة وصلت إلى 100% حتى وذلك في ظل وجود عقدة مهاجمة واحدة (IDSAODV – 1) وإلى 89.42% في ظل وجود عقدتين مهاجمتين.



الشكل (2): العلاقة بين نسبة تسليم الرزم وعدد العقد المهاجمة عند تطبيق BlackHoleAODV, IDSAODV

كما يوضّح الشكل (3) أنّ قيم حمل التوجيه الزائد Routing Overhead زادت حتى 6.8 بوجود عقدة مهاجمة مقارنة بالقيمة 1 بدون وجود هجوم، واستمرت القيمة بالتزايد مع زيادة عدد العقد المهاجمة إلى عقدتين حيث وصل إلى القيمة 8.2، ويُفَسَّر ذلك بتناقص عدد رزم البيانات الواصلة إلى أهدافها بسبب إهمال المهاجم لرزم البيانات.

وعند تطبيق البروتوكول المُقتَرَح IDSAODV فقد حسَّنَ من قيم حمل التوجيه الزائد حيث انخفضت بشكل طفيف إلى القيمة 1 بعد أن كانت 1.0267 وذلك في ظل وجود عقدة مهاجمة واحدة (IDSAODV – 1) ولكنها ازدادت إلى القيمة 1.1183 عند وجود عقدتين مهاجمتين.



الشكل (3): العلاقة بين حمل التوجيه الزائد وعدد العقد المهاجمة عند تطبيق BlackHoleAODV, IDSAODV

يبين الجدول (5) استمرار تناقص قيم مقاييس الأداء مع زيادة سرعة حركة العقد من 5m/s إلى 10 m/s في ظل وجود كل من هجوم الثقب الأسود والبروتوكول المقترح للتخفيف من أثر الهجوم.

الجدول (5): قيم مقاييس الأداء عند استخدام BlackHoleAODV, IDSAODV وبزيادة سرعة العقد

مقياس الأداء Performane Metric	BlackHoleAODV		IDSAODV	
	5 m/s	10 m/s	5 m/s	10 m/s
Average Throughput (kbps)	25.10	24.49	38.32	37.90
Packet delivery Ratio (%)	14.79	14.11	100.00	98.58
Routing Overhead	6.7615	7.0877	`1.0000	1.0144

6- الاستنتاجات والتوصيات

- إنّ وجود هجوم الثقب الأسود في شبكة MANET تعتمد على بروتوكول التوجيه التفاعلي AODV تسبّبَ في تناقص قيم كل من متوسط إنتاجية الشبكة Average Throughput ونسبة تسليم الرزم Packet Delivery Ratio كما تسبب بزيادة في حمل التوجيه الزائد Routing Overhead.
- إن بروتوكول IDSAODV ساعد في تخفيف أثر هجوم الثقب الأسود حيث أنه حسن من قيم مقاييس الأداء بشكل جيد تحسنت قيم متوسط الإنتاجية بنسبة 100% (عادت إلى قيمها الطبيعية قبل تطبيق الهجوم). وبالنسبة لقيم نسبة تسليم الرزم فقد ارتفعت بشكل كبير فكانت 14%عند تطبيق الهجوم وارتفعت لتصبح 100% عند تطبيق IDSAODV. كذلك الأمر بالنسبة لقيم حمل التوجيه الزاذد فقد انخفضت بعد أن كانت 6.76% لتعود وتصبح 1%.
- إن أداء بروتوكول IDSAODV في الشبكات ذات السرعات المنخفضة أفضل مما هو عليه في الشبكات ذات السرعات الأعلى.
- عند تطبيق هجوم الثقب الأسود BlackHoleAODV وزيادة السرعة إلى (10m/s) انخفضت قيم الإنتاجية ونسبة تسليم الرزم بشكل بسيط وارتفع حمل التوجيه الزائد بشكل بسيط أيضاً، بالتالي نستنتج عدم تأثر الشبكة المدروسة بزيادة سرعة حركة العقد من 5m/s إلى 10 m/s.
- نفس الأمر ينطبق على بروتوكول IDSAODV (بزيادة سرعة حركة العقد كان تأثر مقاييس الأداء قليلاً أيضاً).

من التوصيات المستقبلية

- دراسة أداء الشبكة في ظل حركة عشوائية للعقد بشكل مستمر ودائم.
- دراسة أثر الهجوم على شبكات تستخدم بروتوكولات توجيه من أنواع أخرى (استباقية – هجينة).
- مقارنة نتائج هذا البحث مع نتائج أبحاث سابقة لإظهار التحسين الذي قدمته هذه التقنية.
- دراسة تقنيات أخرى مقتَرحة لاكتشاف هجوم الثقب الأسود والتخفيف من آثاره.

7- المراجع

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

[2] MAURYA. P. K; SHARMA. G; SAHU.V;ROBERTS.A; SRIVASTAVA. M, *An Overview of AODV Routing Protocol* , International Journal of Modern Engineering Research (IJMER),Vol 2, Issue 3. 2012, pp -728-732.

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

[4] 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, issue 1.2017, p197-213

[5] DING,Y;QU,H;LI,G. *Black hole Attack Model and simulation for mobile ad hoc network*.International Journal of Innovative Computing ,Information and Control(ICIC),2015 , P203-211.

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

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

[8] THACHIL, F; SHET, C.K. *A trust based approach for AODV protocol to mitigate black hole attack in MANET.* International Conference on Computing Sciences, 2012. PP 281-285.

[9] SHEOKAND, R; GUPTA, M. *Detection and Prevention of Black-Hole Attack in MANET*. International Journal of Computer Science and Mobile Computing (IJCSMC), Vol. 8, Issue. 5, 2019, pg.239 – 251.

[10] SINGH, A; HASAN, M. *An Improved Mechanism to Prevent Blackhole Attack in MANET,* Springer Nature Singapore Pte Ltd. 2018.

[11] PATEL, R; PATEL, M. *Preventing DSR Protocol against Black Hole Attack for MANET.* International Research Journal of Engineering and Technology (IRJET) Vol. 03, Issue.06, 2016, PP 448-454.

[12] CHAVAN, A. A; KURULE, D. S; DERE, P. U. *Performance Analysis of AODV and DSDV Routing Protocol in MANET and Modifications in AODV against Black Hole Attack.* Procedia Computer Science 79 (2016) 835-844.

[13] DORRI, A.; VASEGHI, S.; GHARIB, O. *DEBH: detecting and eliminating black holes in mobile ad hoc networks.* Springer Science + Business Media. New York 2017.

[14] Ranjeet Suryawanshi & Sunil Tamhankar., (2012) "Performance analysis and minimization of balck hole attack in MANET" , International Journal Of Engineering Research and Applications (IJERA), ISSN: 2248-9622, Vol. 2, Issue 4, pp.1430-1437.

[15] HIJAZIEH,M;YOUNES,M;ABBAS.M.*Effect of proactive, reactive and hybrids protocol on the performance of wireless network (MANET).* Tishreen University Journal for Research and Scientific Studies - Engineering Sciences Series Vol. 38,No. 4 , 2016. P235-254.

[16] MEGHNA CHHABRAL, BRIJ GUPTA, AMMAR ALMOMANI. *A Novel Solution to Handle DDOS Attack in MANET*. Journal of Information Security. Vol 4, July 2013, P 165-179.

[17] KUMAR,K.R;PRASANNA,S.*COMPLETE ANALYSIS OF VARIOUS ATTACKS IN MANET*. International Journal of Pure and Applied Mathematics.Vol. 119, No. 15, 2018, 1721-1727.

[18] KALAKAR, V. K; ALI, S. T; CHACK, H. *Performance Analysis of Black Hole Attack in MANET using OPNET.* IJIRT. Volume 6 Issue 10, March 2020, ISSN: 2349-6002.

[19] TRIVEDI,M.C;MALHOTRA,S.*Identification and Preventioin of Joint Gray Hole and Black Hole Attacks.*International Journal of Ambient Computing and Intelligence.Vol. 10, Issue 2. April-June 2019, P(80-90).