مجلة جامعة طرطوس للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (٧) العدد(٨) ٢٠٢٣

Tartous University Journal for Research and Scientific Studies - engineering Sciences Series Vol. (٧) No. (٨) 2023

كشف هجوم الثقب الأسود في الشبكات اللاسلكيّة الخاصّة النقّالة باستخدام بروتوكول R-AODV

د. محمد علي عنبر*

م. مرح عيسى كناج**

(تاريخ الإيداع ٢٠٢٣/٧/١٧ . قُبِل للنشر في ٢٠٢٣/١٠/٥)

□ ملخّص□

يُعدّ هجوم الثقب الأسود من أخطر الهجمات الأمنية والأكثر شيوعاً التي تستهدف الشبكات اللاسلكيّة الخاصّة النقّالة MANET بشكل خاص. ونظراً لأهمية شبكات MANET فقد اتجه الباحثون لإيجاد تقنيات لكشف هذا الهجوم، ومن بين هذه التقنيات بروتوكول AODV العكسيّ.

تمّ في هذا البحث دراسة تأثير هجوم الثقب الأسود على أداء الشبكة وذلك في ظل وجود مهاجم واحد ومن ثم مهاجمين، ثم تطبيق بروتوكول AODV العكسيّ (R–AODV) على الشبكة نفسها 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 R-AODV خفّفَ من تأثير هجوم الثقب الأسود، حيث قدّم أفضل النتائج بالنسبة لإنتاجية الشبكة ونسبة تسليم الرزم بنسب تكاد تكون نفسها قبل تطبيق الهجوم، حيث وصلت نسبة تسليم الرزم إلى 97% ولكنّه سبّب زيادة في حمل التوجيه الزائد. كما أظهرت نتائج المحاكاة عدم تأثر قيم معدّل الإنتاجية ونسبة تسليم الرزم بزيادة سرعة حركة العقد في الشبكة، ولكن تناقصت قيمة عبء التوجيه الزائد بشكل واضح.

الكلمات المفتاحية: الشبكات اللاسلكيّة الخاصّة النقّالة، هجوم الثقب الأسود، بروتوكول توجيه شعاع المسافة عند الطلبAODV، بروتوكول AODV العكسيّ.

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

**دارسات عليا (ماجستير) في قسم هندسة تكنولوجيا الاتصالات – كلية هندسة تكنولوجيا المعلومات والاتصالات جامعة طرطوس

مجلة جامعة طرطوس للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (٧) العدد(٨) ٢٠٢٣

Tartous University Journal for Research and Scientific Studies - engineering Sciences Series Vol. (٧) No. (٨) 2023

Detection of Black Hole Attack in MANETs using R-AODV Protocol

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

(Received 17/7/2023 . Accepted 5/10/2023)

□ 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 Reverse AODV Protocol.

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, Reverse AODV Protocol 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 Reverse AODV Protocol reduced the impact of Black Hole Attack, where it presented the best results for Average Throughput and Packet Delivery Ratio with percentages almost the same before the attack, where Packet Delivery Ratio reached to 97%, but the Routing Overhead was increased. The simulation results also showed that the values of Average Throughput and Packet Delivery Ratio weren't affected by increasing the speed of nodes in the network, but the value of Routing Overhead was obviously decreased .

Key Words: MANETs, Black Hole Attack, AODV, R-AODV.

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

** Master in Communication Technology Engineering Department, Information and communication Technology Engineering, Tartous University.

١- مقدّمة

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 ويُعدّ بروتوكول AODV من أشهر هذه البروتوكولات وأكثرها استخداماً [2].

يُعدّ تحقيق الأمن في MANETs من الأمور الصعبة وذلك بسبب بنية الشبكة المتغيرة باستمرار وغياب الإدارة المركزيّة وحركة العقد المستمرّة، حيث يُعرَّف الهجوم عادةً بأنّه محاولة لتدمير أو مقاطعة عمل الشبكة وانتهاك أهداف وقواعد الأمان الأساسية مثل الموثوقيّة Authentication، سلامة البيانات Integrity، السرّية Confidentiality، التوافريّة Availability، عدم التنصّل Non-Repudiation.

تُعدّ عملية التوجيه (Routing) من أهم القضايا في هذه الشبكات والتي تتأثر بالهجمات الأمنية، ويُعدّ هجوم الثقب الأسود (Black Hole Attack) الذي يقوم بإسقاط رزم البيانات ومنعها من الوصول إلى وجهتها المنشودة من الهجمات التي تهدّد عملية التوجيه في هذه الشبكات [3].

يتمثّل 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 R-AODV لكشفها والتخفيف منها.

٢- هدف البحث وأهميته

التخفيف من تأثير هجوم الثقب الأسود في الشبكات اللاسلكيّة النقّالة، وذلك من خلال تطبيق بروتوكول AODV العكسيّ. وتأتي أهمية هذا البحث من ضرورة الحفاظ على استمراريّة عمل شبكات MANET ذات الطبيعة الحساسة حتى في حال حدوث مشاكل أمنيّة.

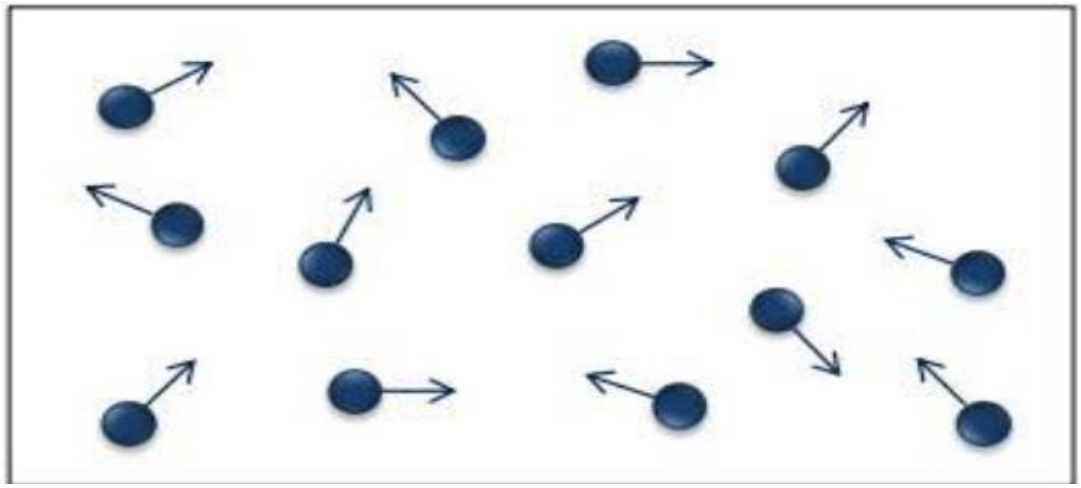
٣- طرائق البحث ومواده

اعتمدَ هذا البحث في تنفيذه على العديد من المراجع والدراسات العلميّة الحديثة [4-13] 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.

٣-١ الشبكات اللاسلكيّة الخاصّة النقّالة (MANETs (Mobile Ad-Hoc Networks

إنّ 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). يوضّح الشكل (١) الحركة العشوائية للعقد في شبكة MANET.



الشكل (١): الحركة العشوائية للعقد في شبكة MANET

تُعرَّف 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.

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

٣-٢ التوجيه في MANETs

يُعدّ التوجيه من القضايا المهمة في عمل شبكاتMANET [16]، و يُقصَد بالتوجيه إرسال الرسالة من العقدة المصدر إلى عقدة تالية حتى الوصول إلى العقدة الهدف عن طريق بناء جداول التوجيه. وبما أنّ بنية شبكات MANET تتغير باستمرار نتيجة انضمام عقد جديدة وخروج عقد أخرى، وكذلك حركيّة 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.

٣-٢-١ خوارزميات التوجيه

يوجد العديد من الخوارزميات التي استُخدِمَت لعمليّة التوجيه منها:

١) خوارزمية التوجيه بشعاع المسافة Distance Vector Algorithm:

تُعدّ المسافة لكل عقدة هي المقياس الذي يجب أن يكون أصغر ما يمكن لاتخاذ المسار الأفضل، والمسافة غالباً ما تحدد على أساس عدد القفزات اللازمة للوصول للعقدة الهدف. حيث يُحدَّد في جدول التوجيه المعلومات الآتية:

العقدة الآتية للوصول للهدف والمسافة للهدف. ويتم تبادل معلومات جدول التوجيه بين الجيران لإيجاد أفضل مسار للهدف.

٢) خوارزمية حالة الوصلات Link-State Algorithm:

تتشارك كل العقد بمعلومات وصلاتها لذلك تستطيع جميعها تشكيل خريطة عن طوبولوجيا الشبكة. ويتم تحديث معلومات الوصلة عندما يطرأ أي تعديل في الشبكة من إنشاء أو حذف وصلات.

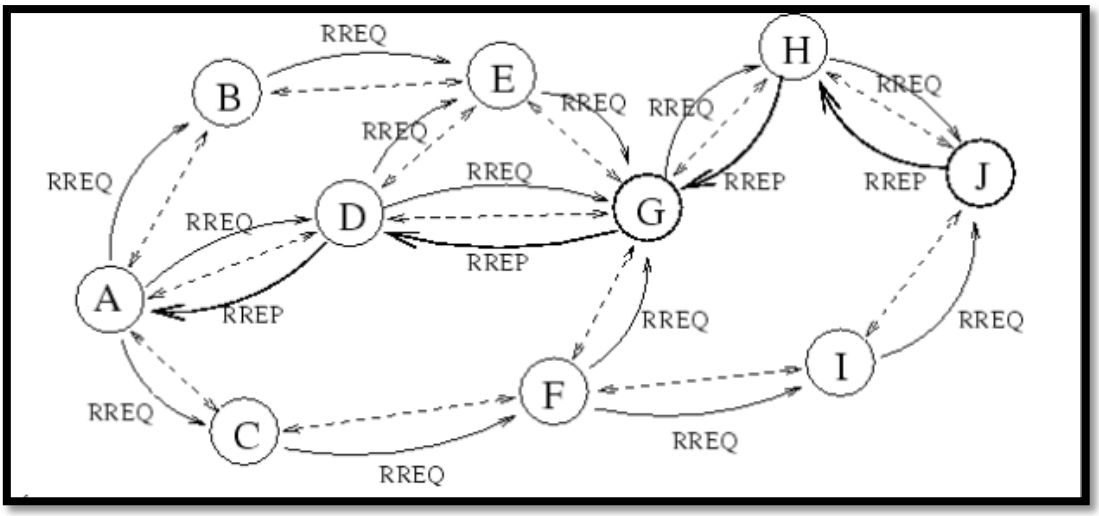
٣-٣ بروتوكول توجيه شعاع المسافة عند الطلب Ad hoc On-demand Distance (AODV)

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:

١. رسالة طلب المسار Route Request Message (RREQ)
٢. رسالة الرد على طلب المسار Route Reply Message (RREP)
٣. رسالة الخطأ في المسار Route Error Message (RERR)
٤. رسالة الترحيب Hello Message .

يوضّح الشكل (٢) هذه الرسائل:



الشكل (٢): نظرة عامّة عن عمل بروتوكول AODV

٣-٤ القضايا الأمنية وهجمات الثقوب في شبكات MANET

يُشكّل موضوع الأمن في شبكات MANET تحدياً كبيراً [17]، وذلك بسبب حركة العقد المستمرة والبنية 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.

٣-٤-١ هجوم الثقب الأسود في MANETs التي تستخدم بروتوكول التوجيه AODV

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

يمكن تلخيص عمل هذا الهجوم بالمراحل التالية [4]:

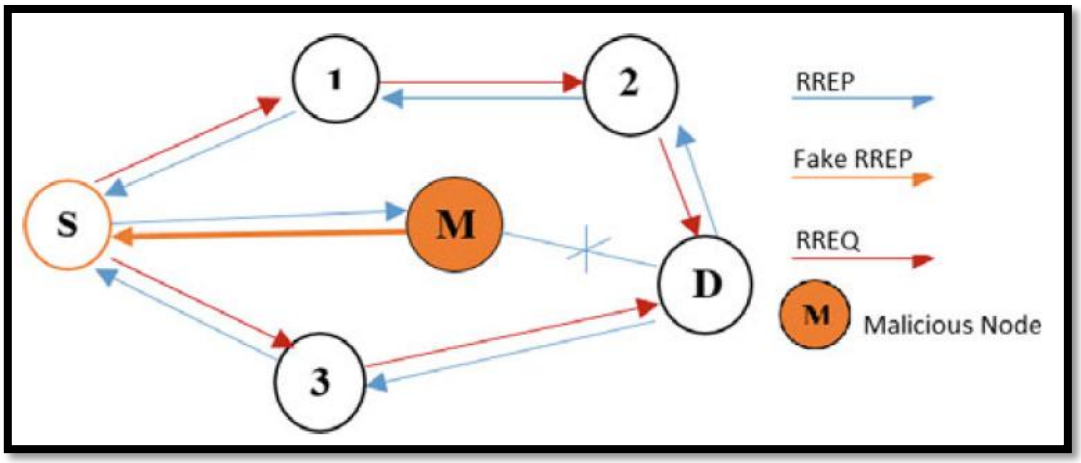
❖ عندما تريد العقدة المصدر إرسال رزم البيانات إلى عقدة أخرى، فإنها تقوم بعملية اكتشاف المسار من خلال إرسال رسالة طلب المسار RREQ إلى العقد الجيران لها.

❖ 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 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 وجهتها الحقيقية بالتالي تعطل العقدة المهاجمة عمل الشبكة وتحقق هدفها المنشود.

يوضّح الشكل (٣) مثالاً عن آلية عمل هجوم الثقب الأسود في شبكة بسيطة، حيث أنّ العقدة S هي العقدة المصدر التي تريد الإرسال إلى العقدة الهدف D، والعقدة M هي العقدة المهاجمة [20].



الشكل (٣): مثال عن تطبيق هجوم الثقب الأسود على برتوكول AODV في شبكة بسيطة

٣-٤-٢ آلية عمل بروتوكول R-AODV

صُمّمَ هذا البروتوكول بدايةً لحل مشكلة ضياع رزمة الرّد Route Reply حيث عالج مشكلة Unicast Route Reply [21] والتي تُعدّ من نقاط ضعف بروتوكول AODV التي يستخدمها المهاجمون في هجومهم، مما جعله يُستخدم لاحقاً للتخفيف من أثر هجوم الثقب الأسود [22].

ويعتمد هذا البروتوكول على غمر رسالة الرّد في الشبكة بالتالي إنشاء عدة مسارات توجيه بين المصدر والهدف.

٣-٤-٢-١ المخطط التدفّقي لآلية عمل R-AODV

يعمل بروتوكول R-AODV وفق المراحل الآتية [21]:

١) تعمل العقدة المصدر على بث رزمة طلب المسار RREQ بثاً عاماً للعقد الجارة لها والتي بدورها ترسلها للعقدة الجارة لها وهكذا وصولاً للعقدة الهدف وهي ذاتها العمليّة الابتدائية لعمل برتوكول AODV.

٢) عند استقبال العقدة الهدف لأول رسالة RREQ تُبث إلى جيرانها رزمة تدعى Reverse Route Request (R-RREQ). يوضّح الشكل (٤) بنية رسالة R-RREQ حيث تتضمن الرزمة معلومات الرّد على

طلب المسار، وبعدها يقوم الجيران بدورهم بإرسال هذه الرزمة إلى جيرانهم بعد تعديل معلومات جداول توجيههم وتحديثها وهكذا حتى العقدة المصدر.

Type	Reserved	Hop Count
Broadcast ID		
Destination IP Address		
Destination Sequence Number		
Source IP Address		
Reply Time		

الشكل (٤): بنية رزمة طلب المسار العكسيّ R-RREQ

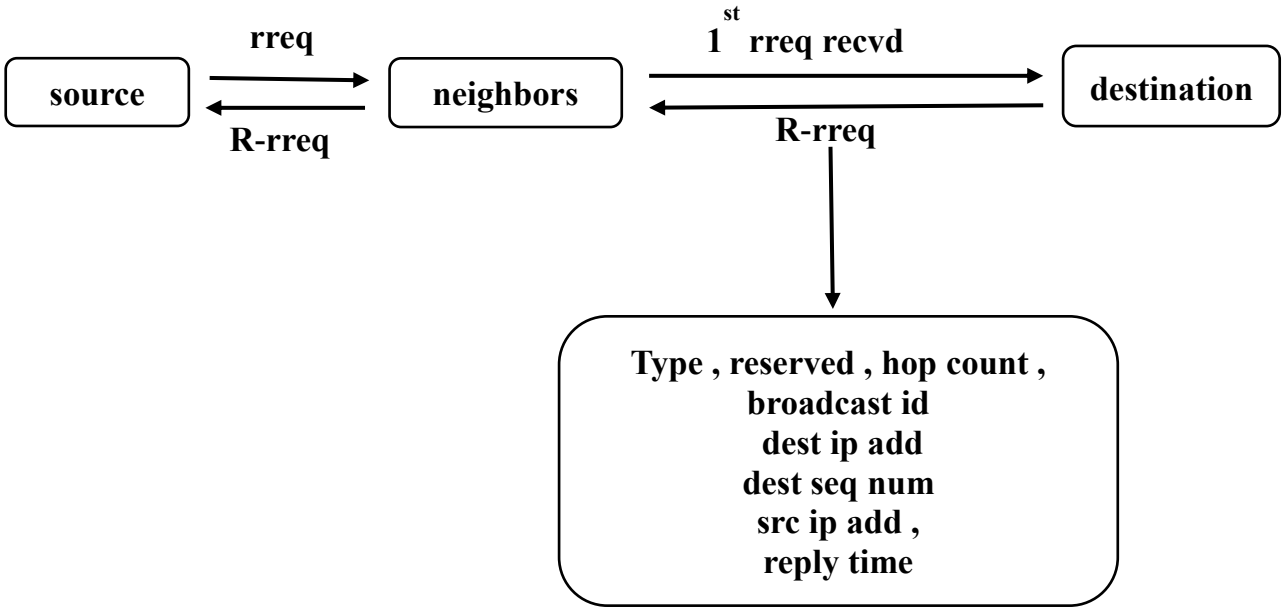
٣) عند استقبال العقدة المصدر لرزم R-RREQ تخزّن مسارات التوجيه المتاحة لنقل رزم البيانات بين المصدر والهدف وتنتقي المسار الأفضل وتقوم بإرسال رزم البيانات إلى الهدف عبره.

٤) في حال إخفاق المسار المختار يتم اختيار مسار بديل من المسارات المخزّنة.

بالتالي عند وجود هجوم الثقب الأسود كعقدة مهاجمة في الشبكة فإنها ستقوم بإرسال رد على رسالة طلب المسار مباشرة مبينةً بأنها تملك مساراً إلى الهدف، إلّا أن العقدة المصدر لن تستجيب لها لأنها تنتظر رسالة الرّد العكسيّة R-RREQ من العقدة الهدف، كما أنها ستقوم بعزلها وحذفها من جدول توجيهها.

- ما يعيب هذا البروتوكول هو ما يسبّبه من حمل زائد وتأخير في الشبكة.

ويعبّر الشكل (٥) الآتي عن المخطط التدفقي وآلية عمل R-AODV:



الشكل (٥): المخطط التدفقي لآلية عمل R-AODV

3-٤-٢-٢ مقاييس الأداء المُتّبعة لتقييم عمل الخوارزميّة

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]:

١. متوسط إنتاجية الشبكة Average Throughput:

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

$$\text{إنتاجية الشبكة [كيلو بت/ثانية]} = \frac{\text{عدد البيانات المستقبلة}}{\text{زمن المحاكاة}} \quad (1)$$

٢. 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 (٢)**:

$$\text{نسبة تسليم الرزم [\%]} = \frac{\text{عدد رزم اليانات الكلية المستقبلة}}{\text{عدد رزم البيانات المرسلة}} \quad (٢)$$

٣. حمل التوجيه الزائدRouting Overhead (RH)

هو النسبة بين رزم التوجيه الكلية إلى عدد رزم البيانات الكلية المستقبلة من قبل العقد الهدف ويعطى **بالعلاقة (٣)**:

$$\text{حمل التوجيه الزائد} = \frac{\text{عدد رزم التوجيه الكلية}}{\text{عدد رزم البيانات الكلية المستقبلة}} \quad (٣)$$

٤- النتائج والمناقشة

قمنا بدراسة أداء البروتوكول Reverse AODV لكشف هجوم الثقب الأسود والتخفيف من آثاره، وذلك وفق السيناريوهات الآتية:

السيناريو الأول: الهدف منه دراسة أداء شبكة لاسلكيّة نقّالة MANET تستخدم بروتوكولAODV، تتعرض لهجوم الثقب الأسود من قبل مهاجم واحد أو أكثر، وذلك بهدف دراسة تأثير الهجوم على أداء الشبكة.

السيناريو الثاني: والغاية منه دراسة أداء شبكة لاسلكيّة نقّالة MANET تتعرض لهجوم الثقب الأسود من قبل مهاجم أو أكثر، وذلك عند تطبيق بروتوكول Reverse AODV بهدف دراسة فعاليّته في كشف الهجوم.

السيناريو الثالث: الغاية منه دراسة تأثر أداء بروتوكول Reverse AODV بزيادة سرعة حركة العقد في الشبكة.

٤-١ نموذج المحاكاة المُقترَح

تمّ بناء شبكة MANET مؤلفة من (٢٥) عقدة متصلة لاسلكيّاً لها نفس الإمكانيات، وتنتشر بمواقع بدائية عشوائية في منطقة مساحتها (1000*800 m) وتتحرك بسرعة مبدئية (5 m/s). 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. ويوضّح الجدول (٥-١) بارامترات الشبكة التي تم اعتمادها.

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, Reverse AODV
عدد العقد	25
عدد العقد المهاجمة	0 (before Black Hole attack), 1 Malicious Node, 2 Malicious Nodes
سرعة العقد (متر/ثانية)	٥-١٠(m/s)
CBRعدد اتصالات	٥
نمط حركة البيانات	UDP
مساحة منطقة المحاكاة	(1000 * 800)

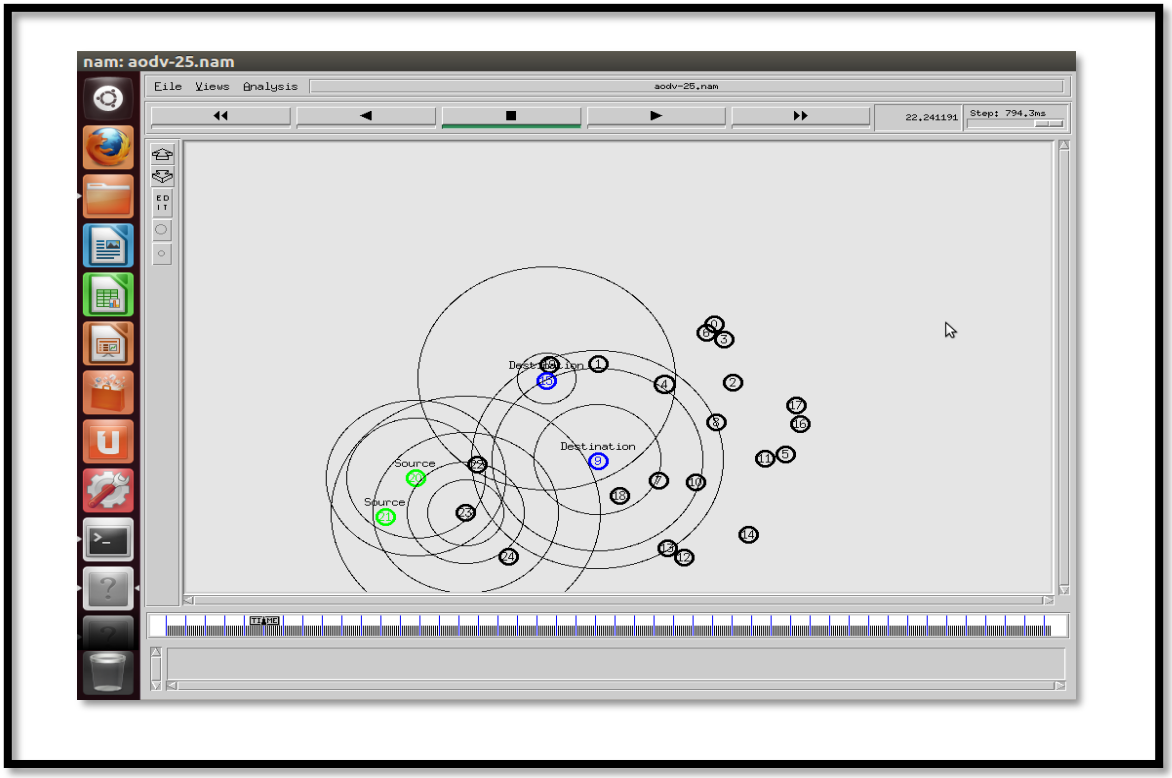
الجدول (١): بارامترات الشبكة

يوضّح الشكل (٦) شبكة MANET المراد محاكاتها وكذلك مواقع العقد المهاجمة التي تم اختيارها بشكل عشوائي. تم توليد نموذج الحركية العشوائية للعقد RWP (Random WayPoint) Mobility Model في سيناريوهات الشبكة باستخدام الخاصية setdest. ويتم ذلك باستخدام لغة TCL حيث يُحدَّد الزمن الذي تتوضع فيه العقد في مكانها والسرعة التي تتحرك بها من أجل برنامج NAM كما هو موضح في الأمر البرمجي التالي:

```
$ns_ at time "$node_ (i) setdest next_Xcoord next_Ycoord next_speed"
```

فمثلاً عند الزمن (1 sec) تتحرك العقدة رقم (٣) نحو الموقع ذي الإحداثيات (X=680, Y=458) وبسرعة (5 m/sec).

```
$ns at 1.0 "$n3 setdest 680.0 458.0 5.0"
```



الشكل (٦): التوضّع العشوائي للعقد في الشبكة

٤-٢ نتائج السيناريو الأوّل

يظهر الجدول (٢) نتائج مقاييس الأداء عندما تكون سرعة حركة العقد 5 m/s (االسرعة الافتراضية) قبل تطبيق هجوم الثقب الأسود، ثم في ظل وجود الهجوم بعقدة مهاجمة واحدة (1-BlackHoleAODV Attack) ثم في حال وجود عقدتي هجوم (2-BlackHoleAODV Attack)، حيث أنّ تنفيذ الهجوم سبّب تناقصاً في قيم إنتاجية الشبكة وقيم نسبة تسليم الرزم وبحمل توجيه زائد.

الجدول (٢): قيم مقاييس الأداء قبل وبعد تطبيق هجوم الثقب الأسود

مقياس الأداء Measured Metric	متوسط الإنتاجية Average Throughput (Kbps)	نسبة تسليم الرزم Packet Delivery Ratio (%)	عبء التوجيه الزائد Routing Overhead
AODV without Blackhole Attack	٣٨.٢١	97.50	1.0267
Blackhole AODV	25.10	14.79	6.7615

٤-٣ نتائج السيناريو الثاني

يوضح الجدول (٣) قيم مقاييس الأداء وذلك عند تطبيق بروتوكول AODV العكسيّ في ظل وجود عقدة ثقب أسود واحدة (1-malicious node) في الشبكة ثم في ظل وجود عقدتي ثقب أسود (2-malicious nodes)، حيث أنّ تطبيق بروتوكول Reverse AODV حسّن من قيم مقاييس الأداء بالمقارنة مع بروتوكول AODV وذلك عند تطبيق هجوم الثقب الأسود.

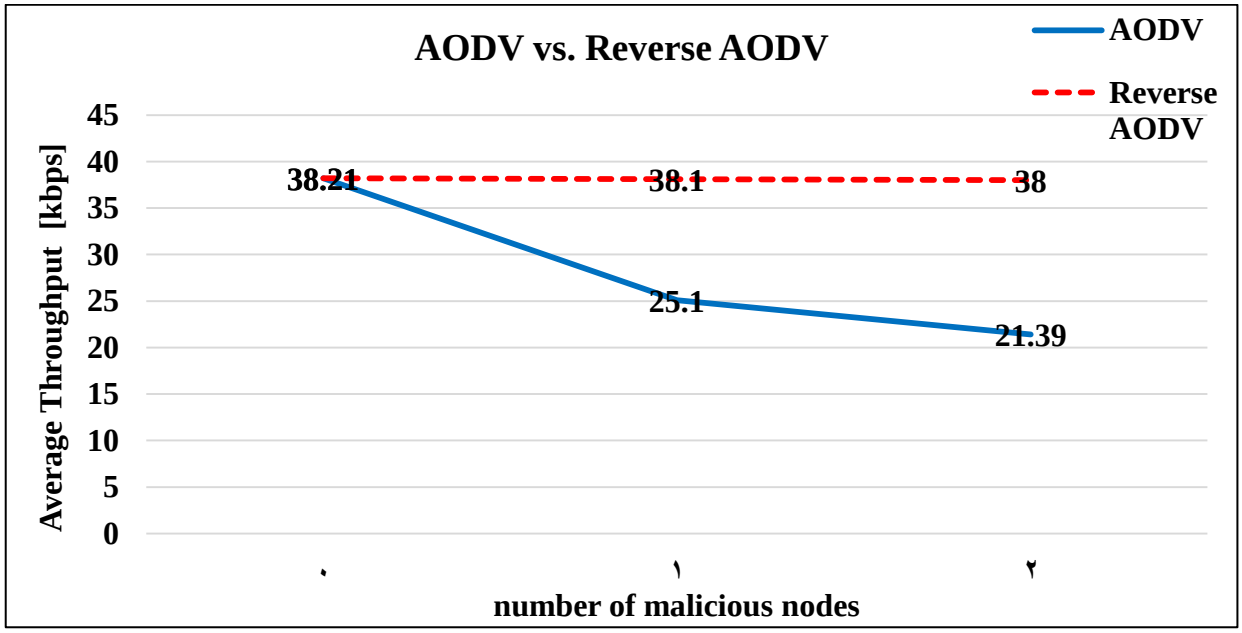
الجدول (٣): قيم مقاييس الأداء عند تطبيق بروتوكول AODV العكسيّ (Reverse AODV)

عبء التوجيه الزائد Routing Overhead	نسبة تسليم الرزم Packet Delivery Ratio (%)	متوسط الإنتاجية Average Throughput (Kbps)	مقياس الأداء Measured Metric
29.29	97.3	38.1	Reverse AODV (1-malicious node)
31.38	97.0	38.0	Reverse AODV (2-malicious node)

تبيّن النتائج الموضحة في الأشكال (٧) و (٨) و (٩) أداء شبكة لاسلكيّة خاصّة نقّالة MANET تستخدم برتوكول التوجيه AODV في الحالة الطبيعية بدون وجود هجوم، ثم في حالة التعرض لهجوم الثقب الأسود من قبل عدد من العقد المهاجمة غير المتعاونة (عقدة مهاجمة ثم عقدتين مهاجمتين)، ثم عند تطبيق بروتوكول Reverse AODV المستخدم لكشف والتخفيف من أثر الهجوم، وبالسرعة الافتراضيّة لحركة عقد (5m/s).

تُظهر النتائج الموضّحة في الشكل (٧) أنّ وجود عقدة مهاجمة في الشبكة أدى إلى انخفاض في متوسط إنتاجية الشبكة (Average Throughput) حيث كانت (38.2 kbps) في الحالة الطبيعية ثم تناقصت إلى (25.1 kbps) واستمرت القيمة بالتناقص حيث أصبحت (21.4 kbps) في ظل وجود عقدتي هجوم. ويُفَسَّر ذلك بأن المهاجم يهمل رزم البيانات التي تصله بالتالي فإن معدل وصول الرزم للعقد الهدف قليل بالتالي فإن معدّل الإنتاجية قليل.

وعند تطبيق البروتوكول المُقتَرَح Reverse AODV على الشبكة السابقة تحسّنت قيم متوسط الإنتاجية حيث أنّه رفع الإنتاجية حتى (٣٨.١kbps) مهما اختلف عدد المهاجمين وهي نفسها إنتاجية الشبكة في حالة عدم وجود هجوم.

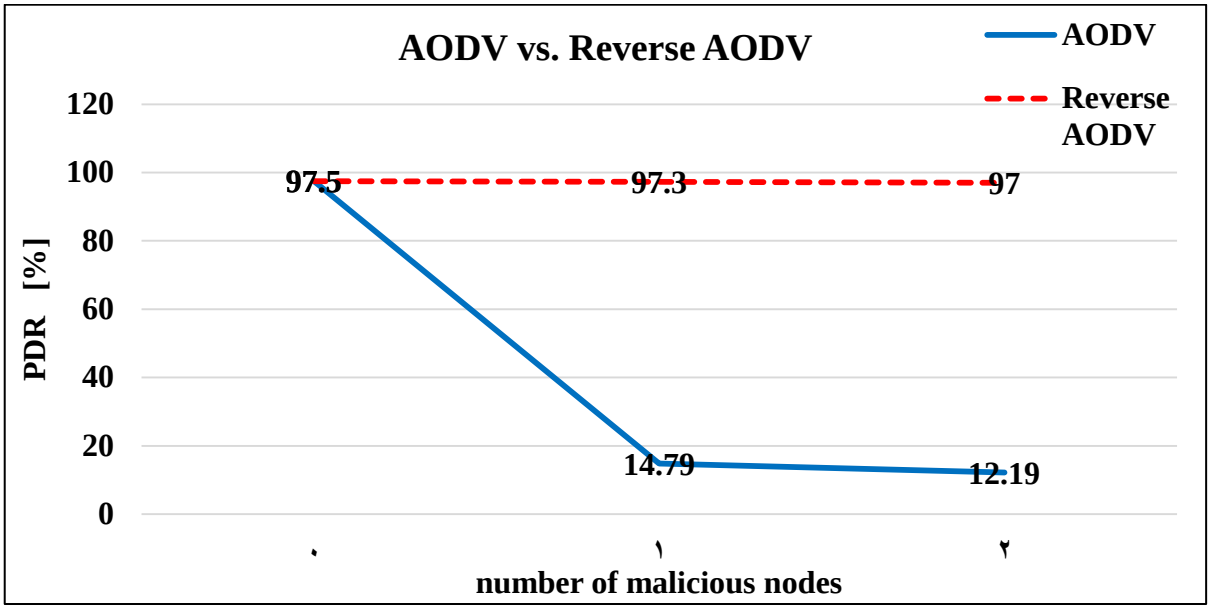


الشكل (٧): العلاقة بين إنتاجية الشبكة وعدد العقد المهاجمة عند استخدام AODV وReverse AODV

ويبين الشكل (٨) أنّ وجود عقدة مهاجمة أدى لانخفاض في نسبة تسليم الرزم Packet Delivery Ratio (PDR) حيث أصبحت (15%) بعد أن كانت (٩٨%) 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.

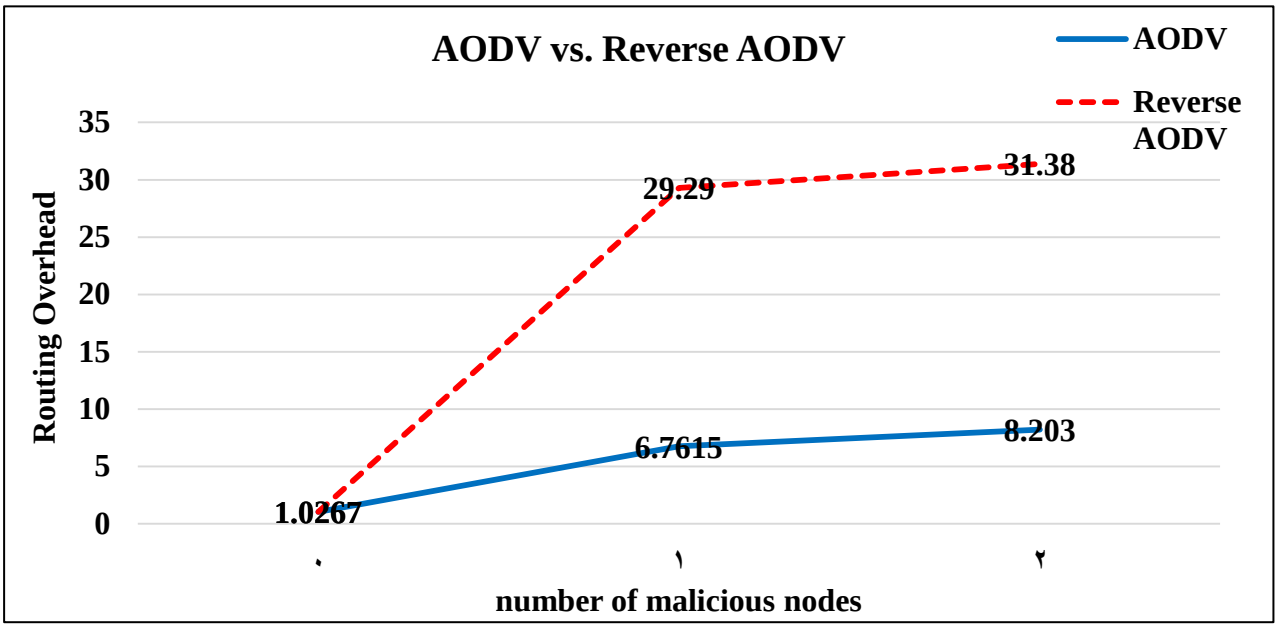
وبتطبيق البروتوكول Reverse AODV فقد ازدادت نسبة تسليم الرزم حتى (٩٧.٣%) من أجل عقدة مهاجمة أو أكثر، ويُفَسَّر ذلك بأن هذا البروتوكول لا يسمح للعقدة المهاجمة بالإعلان عن نفسها بأنها تملك المسار الصحيح والأحدث إلى الهدف وينتظر الرّد من الهدف الحقيقي. كما أنه يستبدل بالمسار الحالي المستخدم لنقل رزم البيانات مساراً آخر عند ملاحظته عدم وصول الرزم إلى هدفها وفقاً لهذا المسار.



الشكل (٨): العلاقة بين نسبة تسليم الرزم وعدد العقد المهاجمة عند استخدام AODV وReverse AODV

كما يوضّح الشكل (٩) 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 فقد تسببّ بزيادة في عدد رزم التوجيه بالتالي زيادة في عبء التوجيه الزائد، حيث أصبحت (٢٩.٣) بعد أن كانت (١.٠٣) في الحالة الطبيعية، وذلك بسبب عمله الذي يعتمد على غمر رزمة الرد على طلب المسار R-RREQ في الشبكة، ويزداد هذا العبء بازدياد عدد المهاجمين.



الشكل (٩): العلاقة بين حمل التوجيه الزائد وعدد العقد المهاجمة عند استخدام AODV وReverse AODV

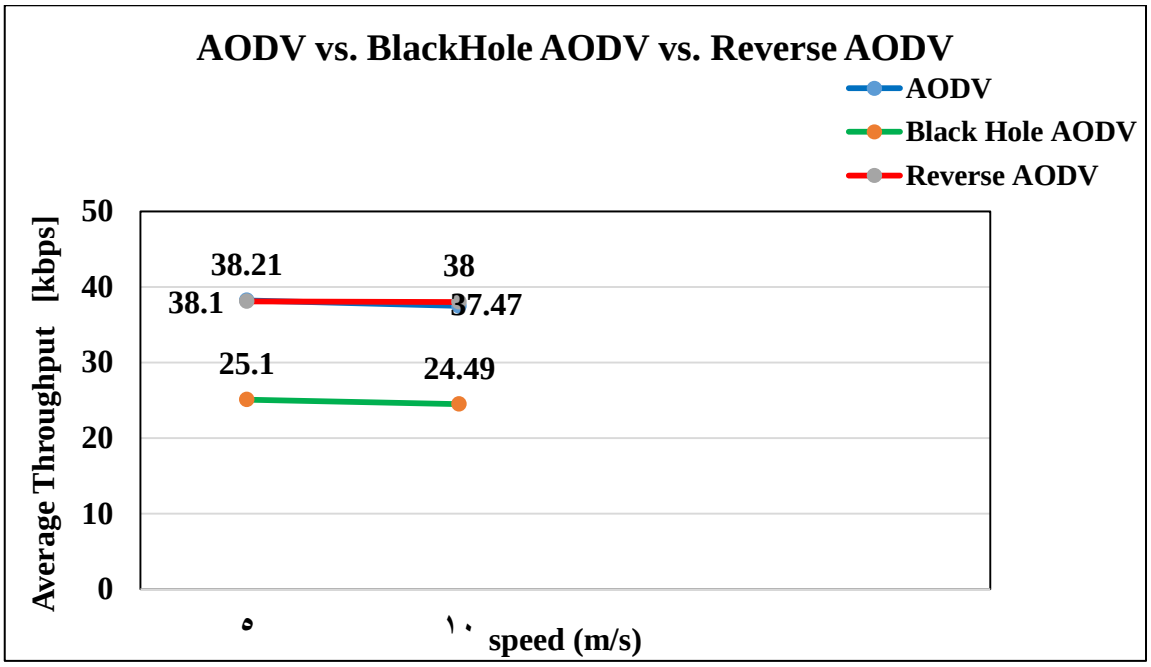
٤-٤ نتائج السيناريو الثالث

عند زيادة سرعة حركة العقد في الشبكة يُقدّم البروتوكول Reverse AODV نسبة تسليم الرزم وإنتاجية جيدتين، وبعبء توجيه كبير نسبياً، لكنه يبدأ بالانخفاض مع زيادة سرعة حركة العقد في الشبكة. يمكن تلخيص النتائج في الجدول (٤):

الجدول (٤): قيم مقاييس الأداء عند تطبيق بروتوكول AODV العكسيّ وبتغيير سرعة حركة العقد

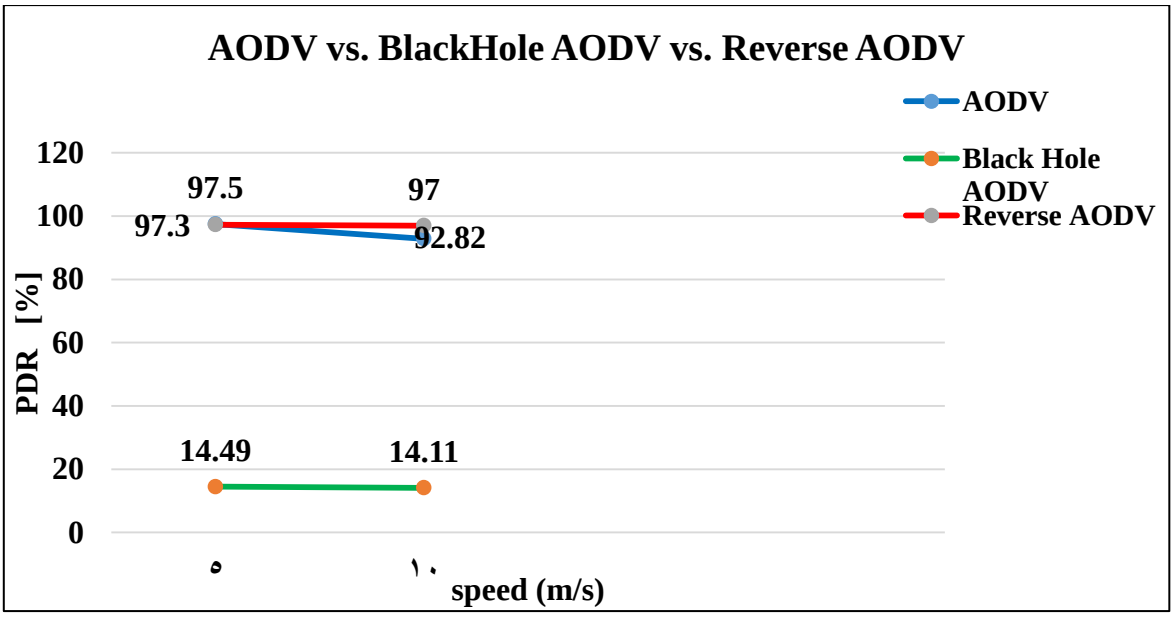
مقياس الأداء Measured Metric		متوسط الإنتاجية Average Throughput (Kbps)	نسبة تسليم الرزم Packet Delivery Ratio (%)	عبء التوجيه الزائد Routing Overhead
Reverse AODV	5m/s	38.1	97.3	29.29
	10m/s	38.0	97.0	25.94

تبيّن النتائج الموضحة في الأشكال (١٠) و (١١) و (١٢) قيم مقاييس الأداء عند تطبيق بروتوكول AODV العكسيّ وبزيادة سرعة حركة العقد في الشبكة، حيث يبيّن الشكل (١٠) أنّه عند تطبيق البروتوكول Reverse AODV لم تتأثر إنتاجية الشبكة بسرعة حركة عقد الشبكة، والسبب في ذلك أنه عند إخفاق الوصلات نتيجة السرعات العالية تقوم العقدة المرسلة باختيار مسار بديل من المسارات المحتفظة ضمن جدول توجيها وهي إحدى ميزات هذا البرتوكول.



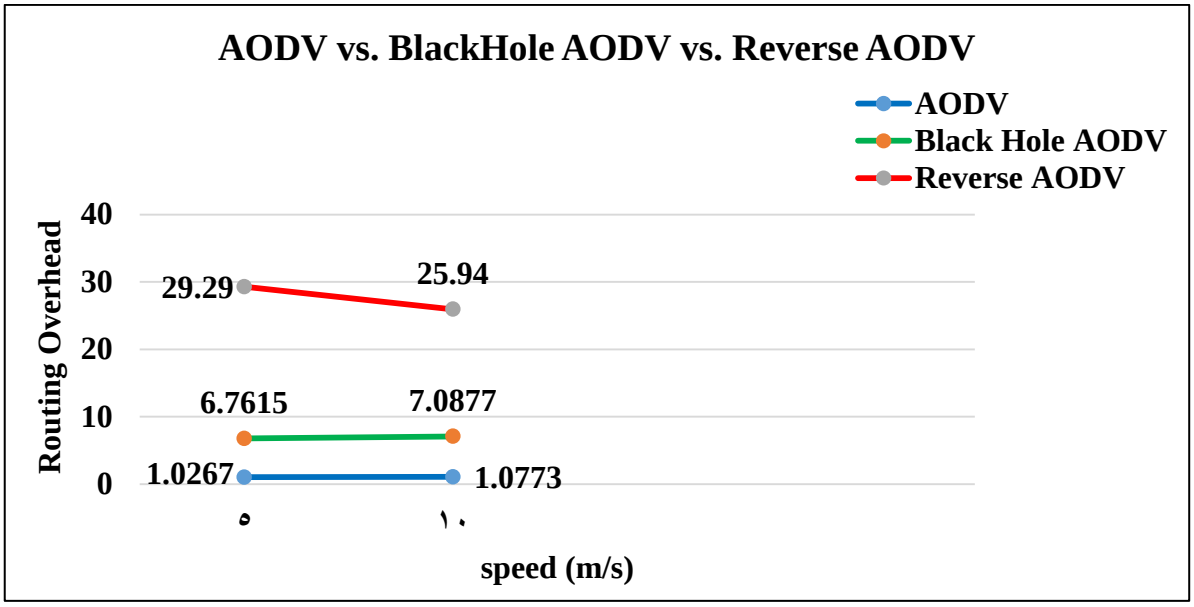
الشكل (١٠): العلاقة بين إنتاجية الشبكة وسرعة حركة العقد عند استخدام AODV وReverse AODV

ويوضّح الشكل (١١) عدم تأثُّر نسبة تسليم الرزم بزيادة سرعة حركة العقد، وذلك لنفس التفسير السابق (انتقاء مسار بديل عند إخفاق المسار الحالي نتيجة زيادة سرعة حركة العقد).



الشكل (١١): العلاقة بين نسبة تسليم الرزم وسرعة حركة العقد عند استخدام AODV وReverse AODV

كما نلاحظ تناقصاً في قيمة عبء التوجيه الزائد عند تطبيق برتوكولReverse AODV وبزيادة سرعة حركة العقد، والسبب في ذلك أنه عند تغير طبولوجيا الشبكة بسبب زيادة سرعة حركة العقد فإن المرسل يستخدم أحد المسارات البديلة مباشرة كما في الشكل (١٢).



الشكل (١٢): العلاقة بين عبء التوجيه الزائد وسرعة حركة العقد عند استخدام AODV وReverse AODV

٥- الاستنتاجات والتوصيات

بناءً على نتائج السيناريوهات السابقة يمكننا استنتاج ما يأتي:

- **إنّ تطبيق هجوم الثقب الأسود (المنفرد) في شبكة لاسلكيّة خاصّة نقّالة MANET تستخدم بروتوكول توجيه شعاع المسافة عند الطلب AODV:**

١. تسبّبَ في تناقص قيم كل من معدّل إنتاجية الشبكة Average Throughput ونسبة تسليم الرزم Packet Delivery Ratio وبالتالي عبء توجيه عالٍ Routing Overhead.

٢. مع زيادة عدد العقد المهاجمة أصبح أداء الشبكة أسوأ، حيث استمرّت قيم إنتاجية الشبكة ونسبة تسليم الرزم بالتناقص كما استمرّت قيمة عبء التوجيه الزائد بالتزايد.

٣. مع زيادة سرعة حركة العقد في الشبكة استمرّت قيم مقاييس الأداء بالتناقص ولكن بشكل بسيط نسبيّاً.

- **إنّ تطبيق بروتوكول توجيه شعاع المسافة عند الطلب العكسي Reverse AODV:**

١. قدّم نتائج جيدة جدّاً من حيث إنتاجية الشبكة ونسبة تسليم الرزم تكاد تكون نفسها تقريباً في حالة عدم وجود هجوم في الشبكة، ولكنّه تسبّبَ بعبء توجيه كبير نسبياً مقارنةً بأداء الشبكة عند تطبيق هجوم الثقب الأسود.

٢. لم تتأثر قيم معدّل الإنتاجية ونسبة تسليم الرزم مهما اختلف عدد العقد المهاجمة في الشبكة.

٣. مع زيادة سرعة حركة العقد في الشبكة لم تتأثر قيم معدّل الإنتاجية ونسبة تسليم الرزم، ولكن تناقصت قيمة عبء التوجيه الزائد بشكل واضح.

٤. يُعدّ بروتوكول AODV العكسي مناسباً للتطبيق في الشبكات اللاسلكيّة النقّالة التي تتعرّض لهجوم الثقب الأسود وتتطلّب تحقيق نتائج جيّدة فيها من حيث إنتاجية الشبكة ونسبة تسليم الرزم مهما اختلف عدد العقد المهاجمة ومهما ازدادت سرعة حركة العقد في الشبكة،

٥. كما يعدّ بروتوكول AODV العكسي مناسباً للتطبيق في الشبكات التي تتعرّض لهجوم الثقب الأسود وتتطلّب قياس حمل التوجيه بحيث تتحرك العقد بسرعات عالية مع أقل عدد عقد مهاجمة.

من التوصيات المستقبلية

- تحقيق البيئة المتكيّفة في الشبكة وذلك من خلال تصميم لوحة تحكم تُستَخدم للانتقال مباشرة إلى بروتوكول التوجيه المُحَسّن، والمُستخَدم للتخفيف من أثر كل هجوم جارٍ في الشبكة، ومن ثمّ إظهار نتائج قياس البارمترات على شاشة اللوحة.
- 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.

٦- المَراجِع

[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.

[٤] 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

[٥] 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.

[٦] 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.

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

[٨] 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.

[٩] 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.

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

[١١] 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.

[١٢] 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.

[١٣] 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] Murthy C. S. R.; Manoj B. S. *Ad Hoc Wireless Networks: Architectures and Protocols*, 2004.

[17] Mahendra Dhole, Anand Gadwal, *Wormhole Attack Detection Techniques: A Review*. International Journal of Computer Science and Technology. 2016.

[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).

[20] DUTTA, D.; MANDAL, S; KAR, R; DEBNATH, S. *Gray Hole Attack in Mobile Ad Hoc Networks*. RCC INSTITUTE OF INFORMATION TECHNOLOGY, 2015.

[21] BABU.B; NAGARAJU. C; 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, Issue 9, 2013, p 691-695.

[22] KIM.CH, TALIPOV. E; AHN. B. *A Reverse AODV Routing Protocol in Ad Hoc Mobile Networks*. IFIP International Federation for Information Processing LNCS 4097, 2006, p 522 – 531.