مجلة جامعة طرطوس للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (5) العدد(3) 2021
Tartous University Journal for Research and Scientific Studies - engineering Sciences Series Vol. (5) No. (3) 2021

دراسة تأثير هجوم الثقب الأسود على أداء بروتوكول التوجية التفاعلي AODV في شبكات MANET

د. فادي جودت غصنه*
د. ناجي ابراهيم محمد**
محمد غسان علي***

(تاريخ الإيداع 1 / 12 /2020 . قُبِل للنشر في 4/19 /2021)

□ ملخّص □

تُعتبَر شبكات الـ MANETs نظام اتصال لاسلكي هام جداً يقدم خدمات مستمرة لنقل البيانات بكفاءة عالية في بيئات تغيب فيها أي وجود لبنية تحتية (ذات البنية التحتية المدمرة كالشبكات العسكرية) نظراً للديناميكية التي تتمتع بها العقد من خلال تأسيس الاتصالات المباشرة، والتكيف السريع مع فقدان أي عقدة في الشبكة، يوجد الكثير من الأبحاث التي درست تأثير هجوم الثقب الأسود الأحادي على بروتوكول التوجيه التفاعلي AODV في شبكات ذات كثافة عقد متغيرة.

تم تطبيق هجوم انكار الخدمة على شبكات الـ MANET (Mobile Wireless Ad-hoc Network) حيث تمت دراسة تأثير هجوم الثقب الأسود (black hole attack) على أداء بروتوكول التوجية التفاعلي AODV في شبكات MANET ضمن سيناريوهات متعددة لبيئات عمل متنوعة من حيث كثافة الشبكة وحركة العقد وعدد المهاجمين.

الكلمات المفتاحية: الشبكات النقّالة الخاصّة – الشبكات اللاسلكية متعددة القفزات – هجوم الثقب الأسود – بروتوكول AODV – البروتوكولات التفاعلية .

---

* أستاذ مساعد في قسم هندسة تكنولوجيا الاتصالات – كلية هندسة تكنولوجيا المعلومات والاتصالات – جامعة طرطوس–سوريا
** مدرس في قسم هندسة تكنولوجيا الاتصالات – كليّة هندسة تكنولوجيا المعلومات والاتصالات – جامعة طرطوس– سوريا
***طالب ماجستير– قسم هندسة تكنولوجيا الاتصالات – كليّة هندسة تكنولوجيا المعلومات والاتصالات – جامعة طرطوس– سوريا

مجلة جامعة طرطوس للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (5) العدد(3) 2021
Tartous University Journal for Research and Scientific Studies - engineering Sciences Series Vol. (5) No. (3) 2021

Studying The effect of Black hole attack on The reactive AODV Protocol in MANETs

Dr. Fadi Jawdat Ghosna*
Dr.NAJI Ibrahim Mohammad**
Mohammad Ghassan Ali ***

(Received 1/ 12/ 2020 . Accepted 19/ 4/ 2021)

□ ABSTRACT □

MANETs are considered a very important wireless communication system that provides continuous services to transfer data with high efficiency in environments where there is no presence of any infrastructure (the same as destroyed infrastructure such as military networks) due to the dynamism that the nodes enjoy through establishing direct communications, and quickly adapting to the loss of any node In the network, there is a lot of research examining the effect of a single black hole attack on the AODV interactive routing protocol in networks with variable contract density.

The DOS attack was applied to MANET networks, where the effect of the black hole attack was studied on the performance of the AODV reactive routing protocol in MANET networks within multiple scenarios for a variety of work environments in terms of network density, node traffic and number of attackers.

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

*Assistant Professor , Communication Technology Engineering Department, Information and communication Technology Engineering , Tartous University, Syria .
**Teacher, Communication Technology Engineering Department, Information and communication Technology Engineering , Tartous University, Syria .
*** Student Master, Communication Technology Engineering Department, Information and communication Technology Engineering , Tartous University, Syria.

1- مقدمه:

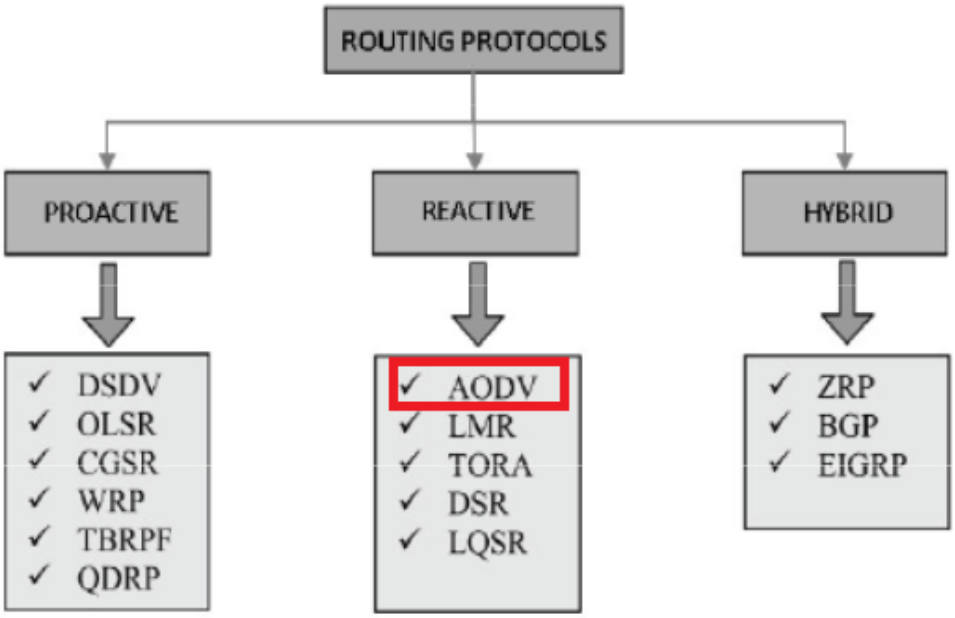
إن شبكات الـ (Ad-Hoc) هي مجموعة من العقد اللاسلكية التي تتصل مع بعضها البعض لاسلكياً باستخدام إشارات لاسلكية بواسطة قناة اتصال مشتركة، وكلمة Ad-Hoc تعني إن الأجهزة يمكن لها أن تُنشيء اتصال في أي وقت وفي أي مكان دون مساعدة بنية تحتية مركزية وهذا هو المميز الأساسي لهذة الشبكات عن غيرها من أنوع الشبكات اللاسلكية، حيث تعمل العقد كموجهات وتكون قادرة على الحركة بحرية وبسرعات مختلفة وتُصنف هذه الشبكات ضمن أربع مجموعات أساسية وهي شبكة MANET (Mobile Wireless Ad Hoc Network) ، وشبكة الحساسات اللاسلكية WSN (Wireless Sensor Network)، وشبكة VANET (Vehicle Ad Hoc Network)، وشبكة WPAN (Wireless Personal Ad Hoc Network)، وتعاني هذه التقنية كغيرها من تقنيات الاتصال اللاسلكية من مشكلة محدودية الأمن الفيزيائي، وتكون الأجهزة المتحركة مسؤوله عن بناء وحفظ اتصالية الشبكة بشكل مستمر، وتتميز هذه الشبكات بعدة مواصفات وهي:

- عدم وجود إدارة مركزية.
- تتصل العقد مع بعضها البعض دون وجود بنية تحتية ثابته.
- يمكن لهذه الشبكات أن تتصل مع شبكات أخرى أو مع شبكة الانترنت.
- العقد ضمنها يمكن أن تكون مرسل أو مستقبل.
- تعمل أغلب هذه الشبكات على الحزمة الترددية المجانية .ISM (Industrial Scientific and Medical)

تجعل هذه الميزات هذه التقنية تؤمن الاتصال بين المستخدمين دون قيود، كما إنها تملك طبولوجيا ديناميكية ومتغيرة باستمرار اذا كانت شبكة MANET لاسلكية متحركة وذلك نتيجة حركة العقد التي تؤدي إلى انقطاع الاتصال بينها وهذا يُعتَبر أمراً اعتيادياً في هذا النوع من الشبكات، وترتبط عناوين العقد بالأجهزة وليس بطبولوجيا الشبكة حيث أن العناوين لا تدل على الموقع، ويُعَد التوجيه قضية هامة جداً ضمن شبكات MANETs وتنقسم بروتوكولات التوجيه إلى عدة أنواع هي البروتوكولات التفاعلية والاستباقية والهجينة [1].

1-1 بروتوكولات التوجيه في شبكات الـ MANETs :

تجعل محدودية المصادر في شبكات الـ MANETs تصميم استراتيجية توجيه فعاله وموثوقه تحدياً كبيراً جداً، حيث أن استراتيجية التوجيه الذكية هي الاستراتيجية التي تستخدم المصادر المحدودة للشبكة بشكل فعّال وفي نفس الوقت تكون متكيفة مع ظروف الشبكة المتغيرة مثل حجم الشبكة وكثافة الحركة، وبناءً على ذلك تحتاج هذه البروتوكولات إلى تقديم مستويات مختلفة من الـ QoS تبعاً لنوع التطبيق المستخدم وبذلك تُصنف البروتوكولات وفق الأنواع التالية كما في الشكل (1) [2]:



الشكل (1) الأنواع الرئيسية لبروتوكولات التوجيه في شبكات الـ MANETs

تُصنَف بروتوكولات التوجيه حسب مبدأ عملها إلى ثلاثة أنواع رئيسية:

1. بروتوكولات التوجيه الاستباقية Proactive :

وتُسمى أيضاً بالبروتوكولات المُقادة بالجدول (table driven) حيث يتم تبادل معلومات التوجيه بين جميع عقد الشبكة ويتم اتخاذ قرار التوجيه بغض النظر عن حاجة الشبكة لها، فهي تستهلك حجماً كبيراً من عرض الحزمة إلا إنها تؤمن سهوله في الحصول على معلومات التوجيه بشكل دائم وبشكل أسرع من التوجيه التفاعلي، لكن هناك صعوبة في تعديل جدول التوجيه في حال فشل إحدى العقد، وتُعتبر هذه البروتوكولات مناسبه من أجل شبكات بعدد محدد من العقد وذلك بسبب التحديثات المتكررة التي تسبب حملاً إضافياً على الشبكة [3]، وأهم مميزات هذه البروتوكولات:

- تمتلك كل عقدة جدول توجيه من أجل البث لجميع العقد ضمن الشبكة وتأسيس اتصال مع العقد الأخرى في الشبكة.
- تسجل العقدة كل الوجهات الموجوده ضمن الشبكة، وعدد القفزات المطلوبة للوصول إلى كل وجهه في جدول التوجيه.
- يتم تمييز مدخل جدول التوجيه برقم تسلسلي مولد من قبل العقدة الوجهة.
- يتم تحديث جدول التوجيه كل فترة زمنيه محدده بهدف الحصول على صوره صحيحة عن طبولوجيا الشبكة وذلك تبعاً للبروتوكول المستخدم، أي تُحدِث عقد الشبكة حالة الشبكة وتحافظ على المسار بغض النظر أكان هناك حركة بيانات أم لا.
- أشهر هذه البروتوكولات :DSDV,OLSR,CGSR .

2. بروتوكولات التوجيه التفاعلية Reactive :

وهي بروتوكولات توجيه تقوم بإجراء عمليات التوجيه في الشبكه عند الطلب، أي إن مسارات التوجيه لا تُبنى إلا عند الحاجه فقط، وبالتالي تعمل على توفير عرض الحزمه، لكن هذا الأمر يزيد من التأخير في عملية توجيه الرزم ضمن الشبكة [4]، وتتميز هذه البروتوكولات بما يلي:

- تُحدَد المسارات عند الطلب من قبل المنبع الذي يقوم بعملية اكتشاف المسار.

- يحدث اكتشاف المسارات دائماً عن طريق غمر الشبكة برزم طلب المسار.
- تخفيض الحمل الزائد المُلاحظ في البروتوكولات الاستباقية (Proactive) عن طريق الاحتفاظ بالمسارات الفعالة فقط.
- إن تحديد المسارات والمحافظة عليها مطلوب من أجل إرسال المعلومات إلى الوجهة الفعلية.
- توجد استراتيجيتان أساسيتان تعمل بهما كل البروتوكولات التفاعلية وهما: Source routing, Hop-by-hop ويوضح الجدول التالي الفرق بينهما:

Hop-by-hop routing	Source routing
كل رزمة معلومات تحوي عنوان الهدف وعنوان القفزة التالية فقط	كل رزمة معلومات تحتوي العنوان الكامل من المنبع إلى الهدف
توجه العقد الوسيطة هذه الرزم اعتماداً على جدول توجيهها	توجه العقد الوسيطة هذه الرزم اعتماداً على المعلومات الموجودة في ترويسة كل منها
مناسبة للشبكات الديناميكية لأن العقد ستحدث جداولها بشكل دوري	تقلل من حجم الحمل الزائد لأن العقدة لا تحتاج للاحتفاظ بالاتصالية مع الجيران باستخدام رسائل Hello
يجب أن تحتفظ كل عقدة وسيطة بمعلومات التوجيه حول كل مسار فعال وهذا ما يتطلب منها معرفة جيرانها عن طريق إرسال المزيد من الرسائل	ينخفض أداءها في الشبكات الكبيرة بسبب عدد العقد الوسيطة الكبير الذي يزيد من احتمال حدوث فشل في المسار ويزيد من حجم الحمل الزائد
أشهرها البروتوكول AODV	أشهرها البروتوكول DSR

الجدول (1) مقارنة بين تقنيات البروتوكولات التفاعلية

3. بروتوكولات التوجيه الهجينة Hybrid :

وهي البروتوكولات التي تدمج بين فكرتي البروتوكولات الاستباقية (Proactive) والتفاعلية (Reactive)، حيث أن معظمها بروتوكولات معتمدة على تقسيم الشبكة إلى عدد من المناطق أو من العناقيد أو الأشجار[5]، وتعتمد على الاحتفاظ بالمسارات بشكل مسبق للعقد القريبة من بعضها البعض (داخل نفس المنطقة مثلاً) وتحديد المسارات للعقد البعيدة بشكل تفاعلي، أي أن عملها هجين بين الطريقتين السابقتين حيث تُستخدَم البروتوكولات Proactive عندما نريد تقليل التأثير في الشبكات الصغيرة، وتُستخدَم البروتوكولات Reactive في الشبكات الأكبر لتخفيف عبئ المعالجة الزائدة للبيانات، وأشهرها هما البروتوكولين: ZRP, ZHLS .

2- هدف البحث وأهميته:

تكمن أهمية البحث نتيجة تزايد الهجمات الأمنية على الشبكات والعمل في البيئات المختلفة بشكل غير مرخص أو غير مشروع، ولذلك هناك ضرورة للتأثير على تبادل المعلومات في الشبكات المعادية ومحاولة حجبه بشكل كامل، حيث ننطلق في هذا البحث من دراسة تأثير هجوم الثقب الأسود على عمل بروتوكول التوجيه التفاعلي Reactive AODV من خلال تطبيق هجوم الثقب الأسود سواء الأحادي أو التعاوني على شبكة MANET ودراسة تأثير هذا الهجوم على كفاءة نقل البيانات الكبيرة في الشبكة من خلال تغيير في عدد المهاجمين أو تغيير عدد العقد في الشبكة (كثافة الشبكة) ومن خلال حركية العقد أيضاً وذلك ضمن سيناريوهات متعددة ودراسة تغير الإنتاجية وتقليلها قدر الإمكان.

3-طرائق البحث ومواده:

تم في هذا البحث استخدام برنامج المحاكاة **NS2 2.35** الذي يُعتبَر أحد أهم برامج نمذجة ومحاكاة الشبكات اللاسلكية المخَصصة Ad Hoc وذلك نظراً لدقته العالية في اظهار النتائج، حيث تم تعديل البنية البرمجية للبروتوكول AODV وتطبيق هجوم الثقب الأسود التعاوني (Cooperative Black-hole Attack)، وتم تنفيذ العديد من السيناريوهات التي تحقق المطلوب لأجل البروتوكول التفاعلي AODV علماً أن نظام التشغيل المستخدم هو Linux Ubuntu .

3-1 البروتوكول التفاعلي AODV (Ad Hoc On-demand Distance Vector Protocol):

إن البروتوكول AODV (Ad Hoc On-demand Distance Vector Protocol) هو عبارة عن بروتوكول توجيه تفاعلي (Reactive) [6]، يعتمد على استراتيجية Hop by hop Routing حيث إنه لا حاجة لتضمين كامل المسار ضمن الرزمة، ويتكيف هذا البروتوكول مع تغّير 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، ويمكن تقسيم العمليات التي ينجزها إلى:

- اكتشاف المسارات (Route Discovery)
- صيانة المسارات (Route Maintenance)

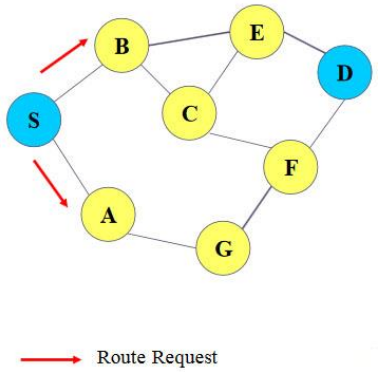
يستخدم البروتوكول AODV أربعة أنماط من الرسائل من أجل تحقيق عملية الاتصال بين العقد وهذه الرسائل هي:

1. رسائل طلب المسار Route Request (RREQ): وتُرسل من أجل عملية بناء المسار نحو الهدف .
2. رسائل إجابة المسار Route Reply (RREP): ترسلها العقدة الهدف المعنية بالاستقبال من أجل عملية تحقيق مسار التوجيه.
3. رسائل الترحيب (HELLO messages): وتُستخدَم من أجل بناء الوصلات بين العقد المتجاورة، ويتم ارسال هذه الرسائل بشكل دوري خلال فترات محدده، ولذلك عند استقبال العقدة عدة رسائل ترحيب من عقدة جاره ما تعتبر الوصلة إلى هذه العقدة فاشلة.
4. رسائل خطأ التوجيه Route Error (RERR): وتُستخدَم من أجل عملية صيانة مسارات التوجيه عند حدوث فشل بالوصلة.

3-1-1 آلية عمل البروتوكول AODV :

1. إنشاء المسار (AODV – Route Discovery):

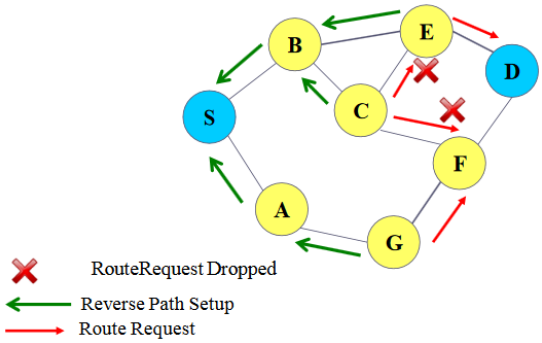
- تبدأ عملية اكتشاف المسار عندما تدرك العقدة المصدر أنها لا تملك مساراً إلى العقدة الهدف ضمن جدولها.
- تقوم العقدة المصدر ببث رزمة طلب مسار (RREQ) كما هو موضح بالشكل (2).
- تتميز رزمة طلب المسار بعنوان المصدر وعنوان الهدف والرقم التسلسلي للهدف.



الشكل (2) إرسال رسالة طلب المسار "RREQ" للبروتوكول AODV

- عند استقبال رزمة طلب مسار من قبل العقدة نميز حالتين:

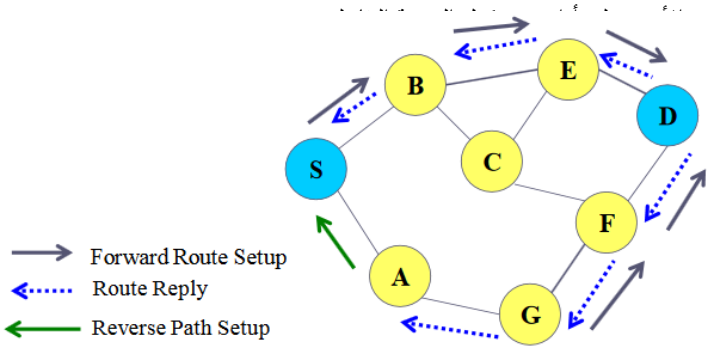
1. **اذا لم تكن العقدة هي الهدف أو كان المسار نحو الهدف مجهولاً لديها:** هنا تدفع العقدة رزمة طلب المسار المستلمة إلى العقد المجاورة وتسجل ضمن جدولها المعلومات التالية: عنوان المصدر، عنوان الهدف، الرقم التسلسلي للهدف، عدد القفزات بعد زيادتها واحد، وهكذا يتشكل المسار العكسي (Reverse Path) كما هو موضَح بالشكل (3)، علماً أن كل عقدة تستقبل الرزمة الأولى فقط (الخاصة بمصدر وهدف محددين) وكل نسخة أخرى يتم إهمالها.



الشكل (3) بناء المسار العكسي "Reverse Path" للبروتوكول AODV

2. **في حال كانت العقدة هي العقدة الهدف:** هنا تقوم هذه العقدة بإرسال رزمة إجابة (RREP) إلى المصدر بعملية (unicast) كما هو مُوضَح بالشكل (4)، علماً أنها تتضمن المعلومات التالية: الرقم التسلسلي للهدف (SN)، عدد القفزات (بعد تصفيرها)، زمن حياة المسار.

- عندما تستقبل العقدة الوسيطة رزمة الإجابة تقوم بتسجيل المعلومات التالية: عنوان الهدف، العقدة المجاورة التي تلقت منها الرزمة، عدد القفزات، زمن الحياة، وبذلك يتشكل المسار الأمامي (Forward Route) كما هو مُوضَح بالشكل (4).
- تبدأ العقدة المصدر بإرسال رزم البيانات عند تلقيها لأول رزمة إجابة.
- تقوم العقدة المصدر بتعديل المسار عند تلقيها لرزمة إجابة تحتوي عدد قفزات أقل.
- تحتفظ كل عقدة بعداد زمن الحياة بحيث تقوم بحذف تسجيل المسار بعد انقضاء زمن محدد من عدم استخدام هذا المسار (300 s).
- الغاية من استخدام الرقم التسلسلي هو تحديد المسار الأحدث.



الشكل (4) تلقي رسالة الإجابة "RREP" للبروتوكول AODV

2. صيانة المسار (AODV – Route Maintenance):

- عند اكتشاف عقدة لفشل في وصلة مرتبطة بها (غياب رسائل Hello القادمة عبر هذه الوصلة) ترسل رسالة reply مع عدد قفزات لا نهائي.
- تصل الرسالة إلى المصدر الذي يقوم ببدء عملية اكتشاف مسار جديد.

3-2 تصنيفات الهجمات في شبكات MANETs :

تُصنف الهجمات الأمنية في شبكات MANETs وفق عدة تصنيفات أساسية كما يلي:

1. هجوم سلبي / نشط (Active / Passive Attack):

- الهجوم السلبي Passive: هدفة الحصول على نسخه من البيانات المتبادلة عبر الشبكة ومن أنواعه الشائعة هجمات التنصت وهجمات تحليل حركة المرور [7]
- الهجوم الفعال Active : يقوم المهاجم بتعديل البيانات بهدف عرقلة سير العمليات في الشبكة المُستهدَفه.

2. هجوم داخلي / خارجي (Internal / External Attack):

- الهجوم الداخلي Internal : يتم الهجوم من داخل الشبكة وهو أكثر خطورة في منع الوصول المُصرَح فيه إلى الشبكة، وبإمكان المهاجم المشاركة في النشاطات العادية للشبكة، ومن ثم العمل على ضياع بعد البيانات.
- الهجوم الخارجي External : يبقى المهاجم خارج الشبكة وليس لديه سماحية وصول إلى الشبكة، ويهدف من هجومه إلى منع وصول المُصرَح لهم الدخول إلى الشبكة من خلال إبقاء الشبكة تحت ضغط المشغولية العظمى التي تسبب الازدحام الذي يعطل عمل الشبكة.

3. هجمات التوجيه (Routing Attacks):

a) **Worm hole Attack** : يُعتبَر أحد الأنواع الخطيرة للهجمات الخاصة، والتي يستخدم فيها المهاجمون عقدتين خبيثتين ضمن شبكة الـ MANET وذلك لنقل الرزم عبر نفق خاص،

حيث يهدف هذا النفق إلى تسجيل بيانات حركة المرور وارسالها إلى مكان آخر في الشبكة بهدف اسبعادها [8] .

b) Gray hole Attack : في هذا النوع من الهجوم يعمل المهاجمين في بداية عمل الشبكة بشكل طبيعي ودون أن يتسبب المهاجم باسقاط أي رزمة، ويرسل رسالة إجابة RREP صحيحة إلى العقدة التي أرسلت رسالة طلب المسار RREQ ولكن عندما يستلم المهاجم الرزم يقوم باسقاطها [8] .

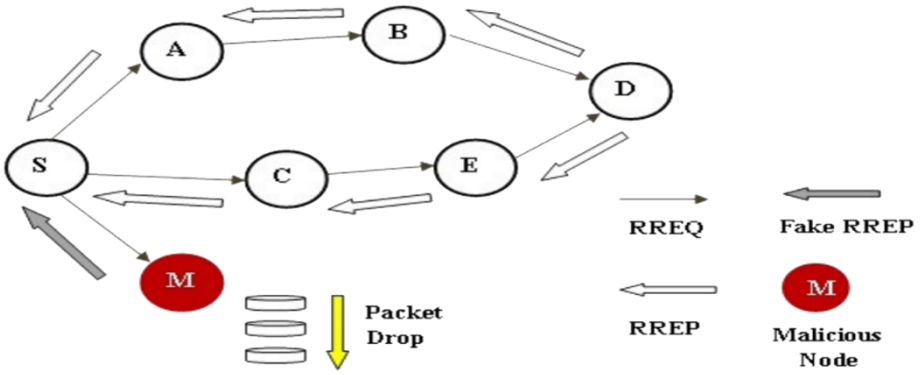
c) Black hole Attack : وهو أكثر الهجمات التي تشغل خبراء الأمن في شبكات MANETs في الوقت الحالي، وينتمي هذا الهجوم إلى الطبقة الثالثة (طبقة الشبكة Network Layer) في النموذج OSI، علماً أنه يمكن أن يُنفَذ هذا الهجوم بواسطة عقدة مهاجمة واحدة فقط أو عدة عقد خبيثة تعمل معاً بشكل تعاوني، حيث تدّعي العقد الخبيثة في الشبكة أنها عقد تملك المسار الأفضل ذو التكلفة الأقل إلى كل الوجهات المُراد الإرسال إليها مما يجعل جميع العقد توجه البيانات إلى هذه العقد الخبيثة [9]، وإن امكانية كشف هجوم الثقب الأسود المنفرد تُعتبَر أعلى من الهجمات الأخرى لكن هناك شكل أكثر تعقيداً من هجوم الثقب الأسود وهو هجوم الثقب الأسود التعاوني والذي يُعتبَر صعب الكشف والإيقاف.

3-3 آلية عمل هجوم الثقب الأسود:

يمكن تنفيذ الهجوم من قبل عقدة واحدة أو أكثر ويتم كما يلي:

- عندما تريد العقدة المصدر إرسال رزم البيانات إلى عقدة أخرى فإنها تقوم بتفعيل عملية بحث عن مسار للهدف وذلك من خلال ارسال رسالة طلب مسار RREQ على شكل بث عام Broadcast إلى كل جيرانها.
- تقوم العقدة الخبيثة باستلام هذه الرسالة ثم ترسل رسالة إجابة RREP وهمية للمرسل تُظهر من خلالها أنها تملك أفضل مسار باتجاه الهدف (المسار ذو عدد القفزات الأقل والرقم التسلسلي الأعلى).
- عندما يستلم المرسل رسالة الإجابة RREP يطلع على محتواها ثم يقوم بإرسال رزم البيانات عبر المسار المُحدد من قبل العقدة الخبيثة.
- تستلم العقدة الخبيثة الرزم ولا تقوم بتوجيهها إلى وجهتها، بل تقوم إما بحذفها أو تقوم بخلق حلقات توجيه وازدحام في الشبكة.

3-3-1 هجوم الثقب الأسود المنفرد: كما ذكرنا فإنه يمكن تنفيذ هجوم الثقب الأسود باستخدام عقدة مهاجمه واحدة فقط كما في الشكل (5) [10]، حيث تريد العقدة المصدر S إرسال بيانات إلى العقدة الهدف D فتقوم بإرسال RREQ على شكل بثّ عام إلى الجيران من أجل البحث عن أفضل مسار للهدف، وعندما تستقبل العقدة المهاجمة M الرسالة RREQ فإنها تقوم مباشرة بإرسال رسالة إجابة RREP (باقل عدد قفزات وأعلى رقم تسلسلي) مما يجعل المصدر S يعتقد أنها حقيقية فيرسل لها البيانات لتقوم بإسقاطها لاحقاً ويتميز التعامل مع هذه الشبكة بصعوبة كشف الهجوم كون العقدة الخبيثة تسلك سلوك عقدة نظامية.



الشكل (5) شبكة MANET مع عقدة ثقب أسود واحدة

3-3-2 هجوم الثقب الأسود التعاوني: وهنا يستخدم المهاجم عدة عقد خبيثة تعمل معاً، ويكون الهجوم أكثر تعقيداً وتكون إمكانية كشفه منخفضة جداً.

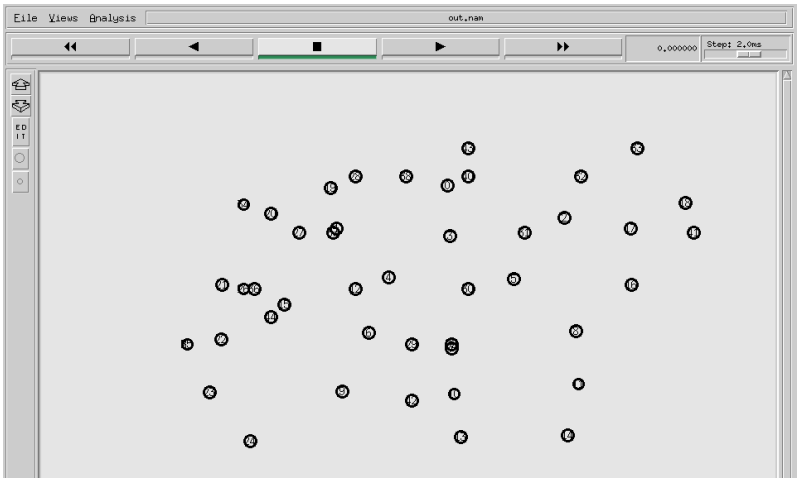
قام الباحثون في الدراسة [11] بدراسة هجوم الثقب الأسود في شبكة MANET لكن عدد العقد الخبيثة كان عقدة واحدة فقط أي أنه هجوم ثقب اسود فردي، وفي بحث آخر [12] قام الباحثون بدراسة شبكة ذات عدد عقد (كثافة) متغيّر من 10-50 عقدة ولكن الحمل في الشبكة كان منخفض وبالتالي لم نحصل على معرفة أداء البروتوكول AODV في ظل وجود حمل عالي ضمن الشبكة، وفي دراسة أخرى [13] تمت دراسة هجوم الثقب الأسود التعاوني ولكن عدد العقد المهاجمة لم يزد عن أربع عقد ولم توجد حركية للعقد ضمن الشبكة بالإضافة إلى أن الشبكة كانت ذات حمل منخفض، وبذلك نجد أن الكثير من الأبحاث التي أُجريَت درست تأثير هجوم الثقب الأسود على البروتوكول التفاعلي AODV لم تلحظ تغيّر حجم الشبكة إلى شبكة كبيرة ولم تلحظ أيضاً وجود حركية للعقد سواءً العقد النظامية أو المهاجمة، بالإضافة إلى أن الحمل في الشبكة كان منخفضاً، وهنا سنقوم بدراسة تأثير تغير كثافة العقد على أداء الشبكة اللاسلكية وذلك مع وجود حركية لهذه العقد ضمن ظروف وجود حمل عالي ضمن الشبكة، بالإضافة إلى دراسة سلوك البروتوكول عند وجود هجوم ثقب اسود تعاوني (تغير عدد العقد الخبيثة) ووجود حركية وذلك تحت كثافة معينة للشبكة.

4- المحاكاة والنتائج:

4-1 إعداد بيئة المحاكاة:

تم اجراء المحاكاة لدراسة سلوك البروتوكول AODV في الشبكات المخصصة اللاسلكية (Ad Hoc) وتحديداً شبكات الـ MANETs تحت تأثير هجوم الثقب الأسود التعاوني (Cooperative Black hole attack) حيث اعتمدت الدراسة على استخدام المحاكي NS2 2.35 مع نظام التشغيل Linux Ubuntu حيث تم بتعديل البنية البرمجية للبروتوكول AODV من خلال تعديل الملفين البرمجيين aodv.cc & aodv.h، وبذلك تم تطبيق الهجوم المطلوب وفق سيناريوهات متعددة من حيث تغيير عدد المهاجمين وتغيير كثافة الشبكة وحركية العقد.

تُمثِل الشبكة المدروسة مجموعة من أجهزة الحاسب التي تشكل شبكة "MANET" بدون بنية تحتية في مهرجان ثقافي.
تم تحديد تموضع العقد بشكل مُحدد، وبعض العقد تتحرك وفق مسارات محددة ضمن حدود الشبكة، كما هو موضح في الشكل(6).



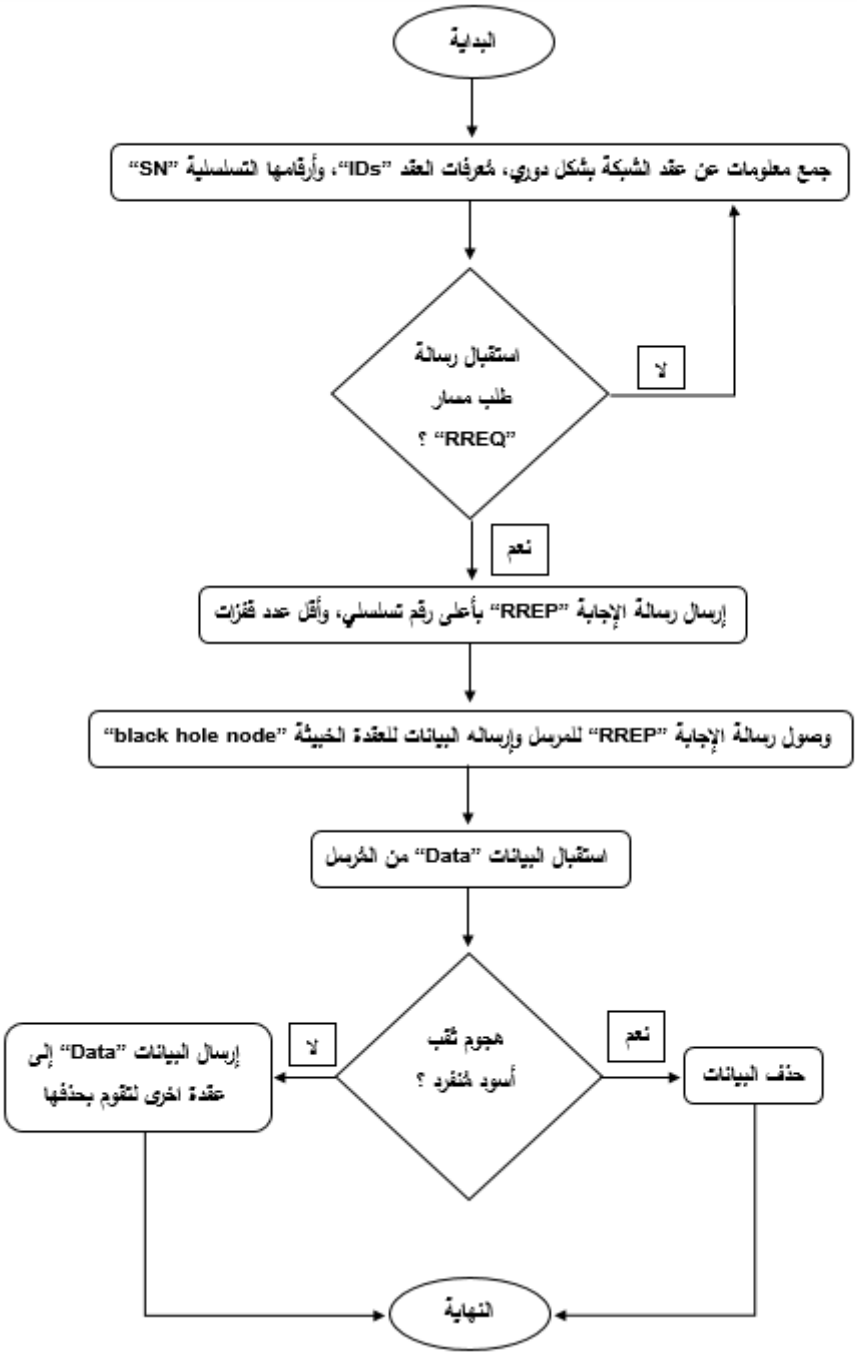
الشكل (6) شبكة MANET بحجم 45 عقدة

تم تشغيل المحاكاة لمدة 100 sec بمساحة شبكة تبلغ 584m * 1186m وتوضع عقد بدائي عشوائي، حيث تم إنشاء عدة سيناريوهات لدراسة أداء البروتوكول في حالة الشبكات الصغيرة والمتوسطة والكبيرة وبحركية للعقد حيث كانت العقد تتحرك بسرعة 40 m/sec، تم اختيار تطبيق نقل ملفات كبيرة بحجم 3Mb من أجل تحقيق حمل كبير ضمن الشبكة، ويبين الجدول التالي البارامترات المستخدمة في المحاكاة:

Simulation Properties	Valus
Antenna Model	Omni Antenna
Radio Propagation	Two Ray Ground
Node Distribution	Random
MAC Type	IEEE 802.11 (2.4 GHZ)
Band width	11Mbps
Application Traffic	CBR
Topology	1186 X 584
Channel Type	Wireless Channel
No of Mobile Nodes	15 – 25 – 35 – 45 –55
CBR Packet Size	1500 Byte
Routing Protocol	AODV
Time Of Simulation	100 Seconds
NS Version	NS – allinone – 2.35
Traffic Pattern	CBR Sessions
PauseTime	1 second
No Of Black hole Nodes	0 – 1 – 2 – 3 – 4
Maximum Speed Of Nodes	40 m/sec

الجدول (2) بارامترات المحاكاة

- بعد تعديل البنية البرمجية للبروتوكول AODV من خلال تعديل الملفين البرمجيين aodv.cc و aodv.h، يكون سلوك العقدة المهاجمة مُوضّح بالشكل(7) التالي:



الشكل(7) المخطط الصندوقي لعمل العقدة المُهاجِمة

4-2 مقياس الأداء :

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

وقد اعتمدنا في هذه الدراسة على حساب بارامتر متوسط الإنتاجية (Average Throughput) وذلك لأنه يقدم نظرة أدق وأكثر شمولية عن سلوك بروتوكول التوجيه AODV تحت تأثير هجوم الثقب الأسود في شبكة MANET ذات توضع عقد بدائي بشكل عشوائي.

حيث تُعطى علاقة الإنتاجية كما يلي: $\frac{\text{حجم البيانات المستقبلة بشكل صحيح}}{\text{الزمن}}$، ويمكن حسابها بـ bits/sec، أو Bytes/sec.

بما أن الهجوم يقوم بحذف رزم البيانات فلن تصل كل الرزم إلى أهدافها، مما يؤدي إلى انخفاض حجم الرزم المستقبلة، وبالتالي تنخفض الإنتاجية وفق العلاقة السابقة.

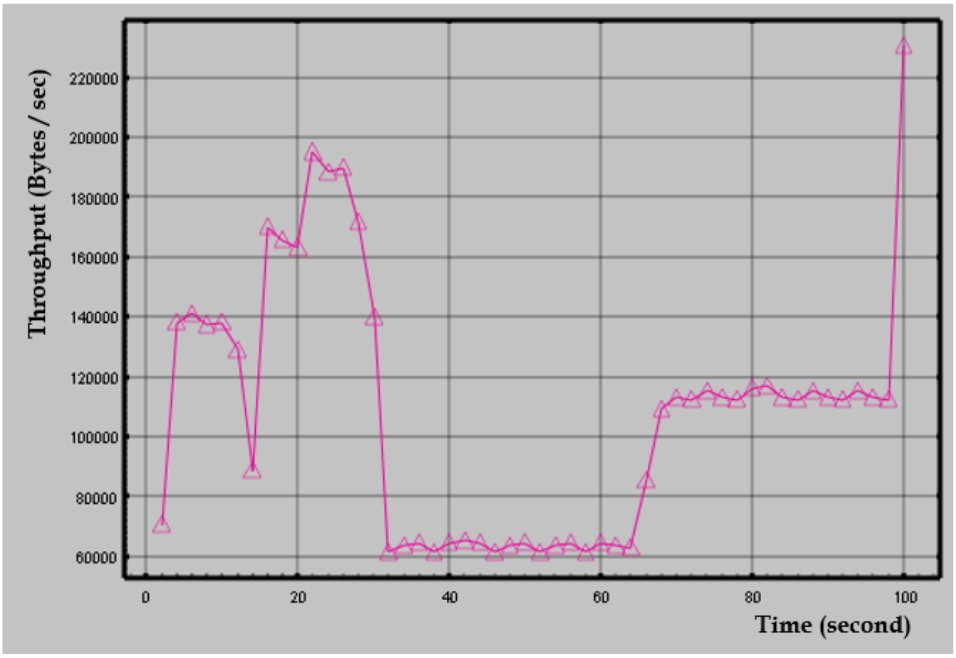
عند زيادة عدد العقد المهاجمة تزداد فعالية الهجوم، أي يقل عدد الرزم التي تصل إلى أهدافها، فينخفض حجم البيانات المُستقبَلة مع كل زيادة في عدد العقد المهاجمة وبالتالي تقل الإنتاجية تدريجياً.

4-3 المناقشة وتحليل النتائج:

لقد قمنا بدراسة حالة الشبكة ضمن ثلاث سيناريوهات حيث كان السيناريو الأول يقارن بين حالتي عدم وجود هجوم ووجود هجوم بعقدة خبيثة واحده فقط ثم عقدتين وذلك لشبكة بكثافة متوسطة مؤلفة من 25 عقدة، أما في السيناريو الثاني فقد قمنا بتطبيق هجوم ثقب أسود تعاوني مكون من 4 عقد مهاجمة تعمل معاً وذلك في شبكة ذات كثافة عقد متغيرة 55 – 45 – 35 – 25 – 15 عقدة، وفي السيناريو الثالث تم تطبيق هجوم ثقب أسود تعاوني أيضاً ولكن بعدد عقد خبيثة متزايد 0 – 1 – 2 – 3 – 4 – 5 عقدة، وذلك تحت كثافة ثابتة للشبكة (25 عقدة)، علماً أنه في السيناريو الأول تم قياس الإنتاجية أما في السيناريوهين الثاني والثالث تم قياس متوسط الإنتاجية للحصول على توصيف أكثر دقة لسلوك البروتوكول AODV وذلك كما يلي:

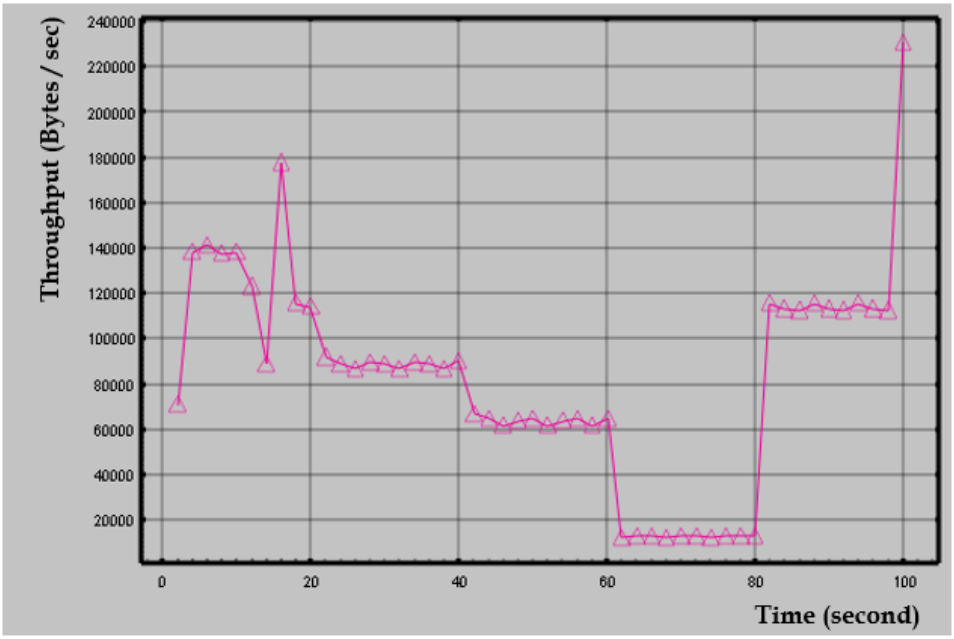
السيناريو الأول :

A. شبكة مؤلفة من 25 عقدة، ومدة المحاكاة 100 sec، ولا توجد أي عقدة خبيثة كما يلي:



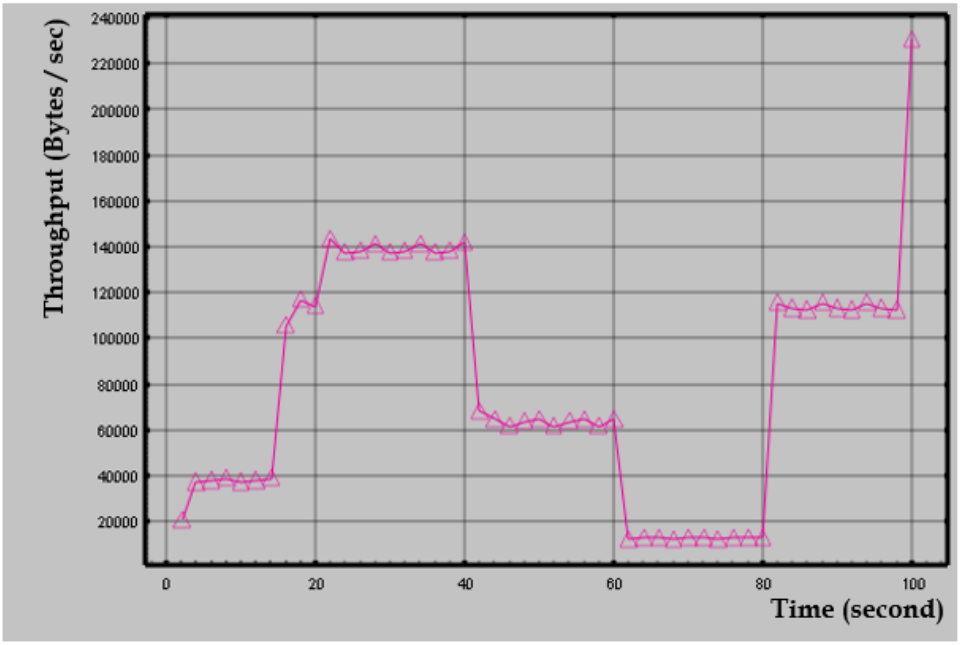
الشكل(8) الإنتاجية دون وجود هجوم

B. شبكة مؤلفة من 25 عقدة، ومدة المحاكاة 100 sec، وعقدة خبيثة واحدة فقط كما يلي:



الشكل(9) الإنتاجية مع وجود هجوم بعقدة خبيثة

C. شبكة مؤلفة من 25 عقدة، ومدة المحاكاة 100 sec، وعقدتين خبيثتين كما يلي:



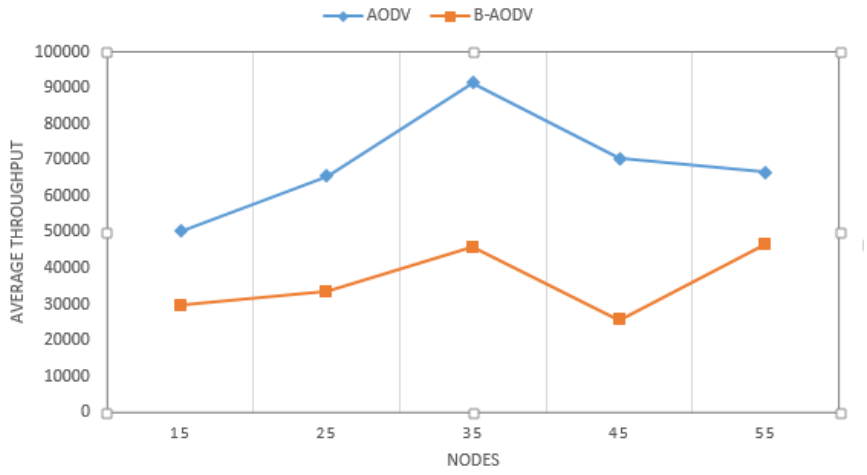
الشكل(10) الإنتاجية مع وجود هجوم بعقدتين خبيثتين

تبين لدينا في السيناريو الأول الحالة الأولى A وبالمقارنة بين الشكلين(8) و(9) حدوث انخفاض في الإنتاجية بالمجمل على طول فترة المحاكاة عند تطبيق الهجوم بعقدة خبيثة واحدة، وكذلك الأمر في الحالة C حيث

يظهر الشكل (10) انخفاض إضافي في الإنتاجية عن الحالة الأولى وذلك نتيجة تطبيق هجوم تعاوني بعقدتين خبيثتين تعملان معاً، ولكن بالرغم من ذلك لم يتم الحصول على سلوك واضح للبروتوكول AODV من هذه الحالة الفردية فقط، ولذلك تم حساب بارامتر متوسط الإنتاجية والذي يعطي فكرة أكثر وضوحاً وشمولية ويتم ذلك من خلال تغيير كثافة الشبكة وتغيير عدد العقد المشتركة بالهجوم التعاوني حيث تتحول كل من المخططات السابقة إلى نقطة واحدة فقط، وتم توضيح ذلك في السيناريوهين الثاني والثالث.

السيناريو الثاني:

قياس متوسط الإنتاجية عند تغيير كثافة الشبكة مع ثبات حجم الشبكة وعدد المهاجمين، حيث تم تغّيير كثافة الشبكة 15 – 55 عقدة، وذلك تحت شروط ثابتة لهجوم ثقب أسود تعاوني مكون من أربع عقد خبيثة، وحجم ثابت للشبكة وتم قياس متوسط الإنتاجية لكل حالة، وكانت النتائج كما هو مُوضَح في الشكل(11)، حيث تم التعبير عن البروتوكول AODV المُعدَل لنتمكن من تطبيق الهجوم بالرمز "B–AODV"، والبروتوكول AODV بحالتة الطبيعة بالرمز "AODV":

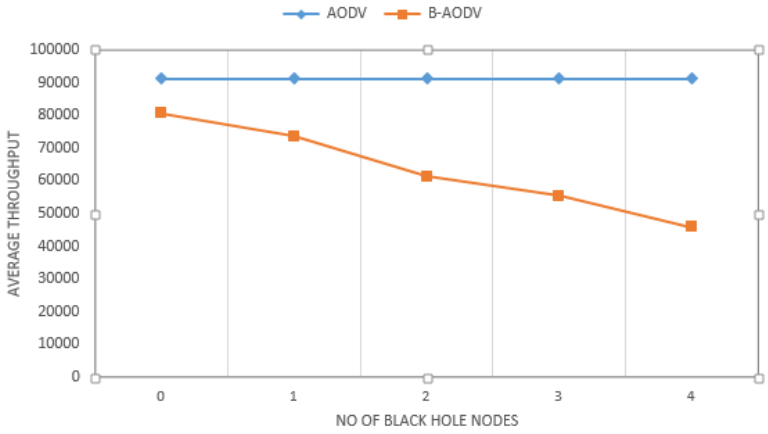


الشكل(11) متوسط الإنتاجية مع تغير عدد العقد

- نلاحظ من المخطط أن زيادة عدد العقد ضمن الشبكة (كثافة الشبكة) يؤدي إلى تقليل تأثير الهجوم وذلك حتى حد معين لكثافة الشبكة 35 عقدة وذلك تبعاً لزيادة عمليات الارسال والاستقبال، وبعد ذلك تنخفض الإنتاجية بشكل واضح، وذلك بسبب أن الكثافة العالية للعقد تؤدي إلى حصول ازدحام وهذا يزيد عدد مرات إعادة الارسال واسقاط الرزم وبالتالي تنخفض إنتاجية الشبكة عند كثافة عقد 45 عقدة وما فوق عند عدم وجود هجوم، ونلاحظ عند كثافة 45 عقدة في حالة وجود هجوم زيادة تأثير الهجوم (انخفاض الانتاجية) حيث إن كل عقدة مهاجمة تؤثر على عدد أكبر من العقد نتيجة الكثافة العالية للشبكة في نفس مساحة العمل المحددة.

السيناريو الثالث:

قياس متوسط الإنتاجية عند تغير عدد العقد الخبيثة 4 – 3 – 2 – 1 – 0 عقدة، تحت شروط ثابتة لكثافة الشبكة بـ 35 عقدة كما هو مُوضَح في الشكل(12):



الشكل(12) متوسط الإنتاجية مع تغير عدد العقد الخبيثة

تبين لدينا أن زيادة عدد العقد الخبيثة ضمن الشبكة يؤدي بشكل واضح إلى زيادة فعالية هجوم الثقب الأسود التعاوني حيث تستمر الإنتاجية بالانخفاض مع هذه الزيادة في عدد المهاجمين، وهذا يوضح أن هجوم الثقب الأسود التعاوني أكثر فعالية وأشد تعقيداً من هجوم الثقب الأسود المنفرد.

5- الاستنتاجات والتوصيات:

وُجِدَ من خلال الدراسة والمحاكاة أن هجوم الثقب الأسود يؤثر بشكل واضح على نقل البيانات في شبكات MANETs العاملة مع بروتوكول التوجيه AODV، حيث أظهرت النتائج أن هجوم الثقب الأسود التعاوني هو أكثر فعالية وأشد تأثيراً من هجوم الثقب الأسود المنفرد، علماً أن فعالية هذا الهجوم تتغير حسب كثافة الشبكة.

تم اقتراح حل لهذا الهجوم وذلك من خلال تزويد كل عقدة نظامية من عقد الشبكة بمفتاح خاص"private key"، تستخدمه العقد لفك تشفير رسائل طلب المسار القادمة لها والمُشفَرة مسبقاً بالمفتاح العام"public Key"، وبذلك لن تستطيع أي عقدة مُهاجِمة دخيلة على الشبكة التعامل مع رسائل طلب المسار وإرسال رسائل الإجابة عليها، نظراً لعدم امتلاكها مفتاحاً خاصاً لفك التشّفير.

6- المراجع:

[1] Mohapatra, P., & Krishnamurthy, S. (Eds.). (2004). *AD HOC NETWORKS: technologies and protocols*. Springer Science & Business Media.

[2] Lalar, S., & Yadav, A. (2017). Comparative study of routing protocols in MANET. *OJCST*, *10*, 174.

[3] Shenbagapriya, R., & Kumar, N. (2014, November). A survey on proactive routing protocols in MANETs. In 2014 International Conference on Science Engineering and Management Research (ICSEMR) (pp. 1-7). IEEE.

[4] Patel, D. N., Patel, S. B., Kothadiya, H. R., Jethwa, P. D., & Jhaveri, R. H. (2014, February). A survey of reactive routing protocols in MANET. In International Conference on Information Communication and Embedded Systems (ICICES2014) (pp. 1-6). IEEE.

[5] Raheja, K., & Maakar, S. K. (2014). A survey on different hybrid routing protocols of MANET. IJCSIT) International Journal of Computer Science and Information Technologies, 5(4), 5512-5516.

[6] Jiang, F., & Hao, J. (2010, February). Simulation of an improved AODV algorithm for ad hoc network. In 2010 The 2nd International Conference on Computer and Automation Engineering (ICCAE) (Vol. 1, pp. 540-543). IEEE.

[7] Mistry, M., Tandel, P., & Reshamwala, V. (2017, May). Mitigating techniques of black hole attack in MANET: A review. In Trends in Electronics and Informatics (ICEI), 2017 International Conference on (pp. 554-557). IEEE.

[8] Arya, N., Singh, U., & Singh, S. (2015, September). Detecting and avoiding of worm hole attack and collaborative blackhole attack on MANET using trusted AODV routing algorithm. In Computer, Communication and Control (IC4), 2015 International Conference on (pp. 1-5). IEEE.

[9] Rathiga, P., & Sathappan, S. (2016, October). Hybrid detection of Black hole and gray hole attacks in MANET. In Computation System and Information Technology for Sustainable Solutions (CSITSS), International Conference on (pp. 135-140). IEEE.

[10] Deshmukh, S. R., & Chatur, P. N. (2016, March). Secure routing to avoid black hole affected routes in MANET. In Colossal Data Analysis and Networking (CDAN), Symposium on (pp. 1-4). IEEE.

[11] Saurabh, V. K., Sharma, R., Itare, R., & Singh, U. (2017, April). Cluster-based technique for detection and prevention of black-hole attack in MANETs. In *Electronics, Communication and Aerospace Technology (ICECA), 2017 International conference of* (Vol. 2, pp. 489-494). IEEE.

[12] Nitnaware, D., & Thakur, A. (2016, February). Black hole attack detection and prevention strategy in DYMO for MANET. In *2016 3rd International Conference on Signal Processing and Integrated Networks (SPIN)* (pp. 279-284). IEEE.

[13] Sharma, N., & Bisen, A. S. (2016, March). Detection as well as removal of black hole and gray hole attack in MANET. In *Electrical, Electronics, and Optimization Techniques (ICEEOT), International Conference on* (pp. 3736-3739). IEEE.