Analyzing the Study of the Effect of Jamming Attack on Ad Hoc Network Performance

Dr. Boushra Maala*
Dr. Haisam alradwan**
Alaa Mahfoud***

(Received 10 / 1 / 2019. Accepted 8 / 10 / 2019)

□ ABSTRACT □

Ad hoc networks are defined as decentralized, self-organization networks that contract with each other without an infrastructure. The applications of these networks in civil and military fields, wireless sensors and intelligent transport systems range to future applications of Internet of Things. These networks suffer from several challenges because of the open environment and lack of infrastructure. Attacks on the network are one of the most serious challenges facing these networks, including the jamming attack that makes the network unavailable to users in the network.

In this paper we present an analytical study of the effect of the jamming attack in Ad hoc networks of various types. To achieve this goal we used the NS 3.11 simulator with the use of additions to support jamming in wireless networks. We have built simulation scenarios that include real-time traffic with different types of jamming. The simulation results showed the impact of the attack on the network performance, where as the result the packet delivery ratio decreased and the delay increased.

Keywords: Network attacks, Jamming attack, packet delivery ratio.

* **Associate Professor, Department of Communication and Electronics, Faculty of Mechanical and Electrical Engineering, Tishreen University, Lattakia, Syria. Boushra.maala@gmail.com**

** **Associate Professor, Department of Communication and Electronics- Faculty of Mechanical and Electrical Engineering, Tishreen University, Lattakia, Syria.haysamradwan@hotmail.com**

*** **PhD Student, Department of Communication and Electronics, Faculty of Mechanical and Electrical Engineering, Tishreen University, Lattakia, Syria. alaa.mahfod@gmail.com**

دراسة تحليلية لتأثير أنواع هجوم التشويش على أداء شبكات Ad Hoc

د. بشرى معلا*

د. هيثم الرضوان**

علاء محفوض***

(تاريخ الإيداع 10 / 1 / 2019. قُبِل للنشر في 8/ 10 / 2019)

□ ملخّص □

تعرف شبكات Ad hoc على أنها شبكات لا مركزية، ذاتية التنظيم، تتصل العقد مع بعضها البعض دون وجود بنية تحتية. تتنوع تطبيقات هذه الشبكات في المجالات المدنية والعسكرية والحساسات اللاسلكية وأنظمة النقل الذكي وصولاً إلى التطبيقات المستقبلية لإنترنت الأشياء. تعاني هذه الشبكات من عدة تحديات بسبب البيئة المفتوحة وعدم وجود البنية التحتية. تعد الهجمات على الشبكة من أخطر التحديات التي تواجه هذه الشبكات، ومنها هجوم التشويش الذي يجعل الشبكة غير متاحة للمستخدمين في الشبكة.

نقدم في هذا البحث دراسة تحليلية لتأثير هجوم التشويش في شبكات Ad hocبأنواعه المختلفة. استخدمنا لتحقيق هذا الغرض المحاكي NS 3.11 مع استخدام إضافاتلدعم التشويش في الشبكات اللاسلكية. قمنا ببناء سيناريوهات المحاكاة التي تتضمن حالة التشويش على إرسال حقيقي باستخدام أنواع التشويش المختلفة. وقد بينت نتائج المحاكاة تأثير الهجوم على أداء الشبكة حيث ينخفض معدل الرزم المستلمة ويزداد التأخير.

الكلمات المفتاحية:الهجمات على الشبكة، هجوم التشويش، معدل الرزم المستلمة.

*استاذ مساعد، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة تشرين، اللاذقية، سورية، boushra.maala@gmail.com

**استاذ مساعد، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة تشرين، اللاذقية، سورية، haysamradwan@hotmail.com

***طالب دكتوراه، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة تشرين، اللاذقية، سورية، alaa.mahfod@gmail.com

مقدمة:

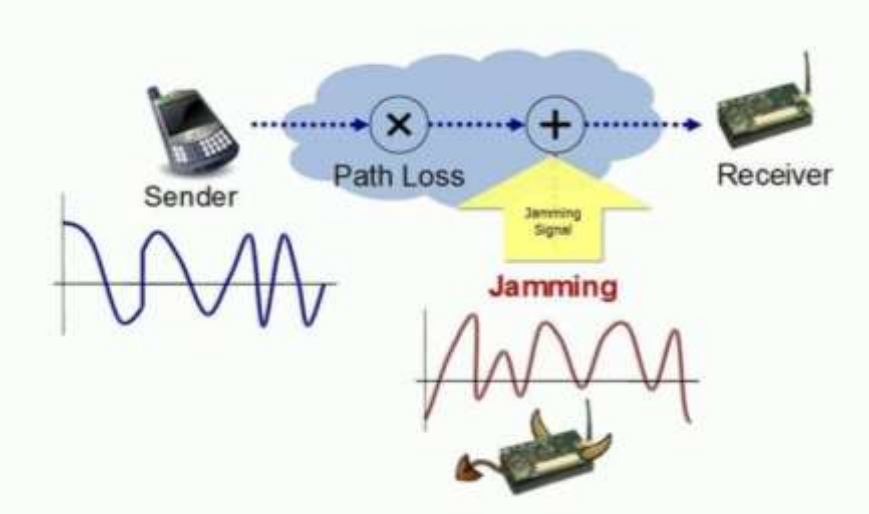
تعد الشبكات اللاسلكية أكثر أنواع الشبكات شيوعاً وانتشاراً في الآونة الأخيرة وذلك نتيجةً لتطور تقنيات الاتصال اللاسلكي وسهولة النشر والتركيب إضافة إلى المرونة والتكلفة المنخفضة. فتح تطور تقنيات الحوسبة والشبكات المجال لظهور أنواع جديدة من الشبكات اللاسلكية مثل شبكات الحساسات اللاسلكية وشبكات النقل الذكيةوغيرها [1,2,3]، وأصبحت الشبكات اللاسلكية والمحمولة جزءاً من حياتنا المعاصرة ونشاطاتنا اليومية. تتنوع الشبكات من حيث الطوبولوجيا وشروط النشر والبيئة المحيطة والتطبيقات الخاصة، يوجد أنواع خاصة من الشبكات اللاسلكية لا تتضمن بنية تحتية وتعتمد في عملها على مبدأ تعدد القفزات، أي أن البيانات تسلك مسارها من المرسل إلى المستقبل مروراً بعدد من العقد.

تتكون الشبكات اللاسلكية متعددة القفزات Wireless Ad Hoc Network من مجموعة من العقد تتصل مع بعضها البعض بمسارات لاسلكية متعددة القفزات كما في الشكل(1)، حيث تقوم العقد بتمرير الرسائل دون وجود بنية تحتية مثل نقاط الوصول. يوجد عدة أنواع لهذه الشبكات مثل بعض تطبيقات شبكات الحساسات اللاسلكية (Wireless Sensor Network)WSN و شبكةMANET (Mobile Wireless Ad Hoc Network) وشبكات العربات المتنقلة (VANET (Ad Hoc NetworkVehicle والشبكات اللاسلكية الشخصية متعددة القفزات (Wireless WPAN (Personal Adhoc Network ...الخ.

الشكل(1) مثال عن شبكة Ad hoc.

تُستخدم هذه الشبكات في العديد من التطبيقات مثل التطبيقات العسكرية والطوارئ وأنظمة النقل وغيرها. تتنافس العقد القريبة من بعضها على مصادر الوسط اللاسلكي مما يخلق مشاكل مثل التنازع والتصادم، وتنشر هذه الشبكات في بيئة مفتوحة ووسط الاتصال اللاسلكي مفتوح مما يؤدي إلى ظهور تحديات أمنية خطيرة يمكن أن تهدد عمل الشبكة على مستوى كل طبقاتها. من هذه التحديات تبرز الهجمات على الشبكة التي تهدف إلى التأثير على الاتصال بين العقد في الشبكة عن طريق استخدام عقد خبيثة. من بين الهجمات على الشبكة لدينا هجوم التشويش jamming attack الذي ينفذ باستخدام أجهزة راديوية بسيطة لكن يمكن أن يسبب مشاكل خطرة تؤدي إلى تخريب الشبكة [4] .

يعرف التشويش بأنه عملية توجيه طاقة كهرومغناطيسية باتجاه نظام اتصالات بهدف تعطيل الاتصالات ضمن النظام [5]، كما في الشكل (2).



الشكل (2) مبدأ عمل التشويش.

يعد هجوم التشويش مستوى خاص من هجوم حجب الخدمة DoS (Denial of Service)، والذي يعمل على التأثير على الإرسال ضمن الشبكة عن طريق إغراق الشبكة بمعلومات غير مفيدة [4]. يمكن للهجوم أن يستهدف طبقات MAC أو الشبكة أو التطبيقات مما يجعل من الصعب كشفه أو التصدي لهُ [6] . نسمي العقدة التي تشن الهجوم بالمهاجم أو المشوش jammer بينما نسمي المنطقة التي يحدث فيها الهجوم بمنطقة التشويش jammed region.

أهمية البحث وأهدافه:

تعد الهجومات على الشبكة من أخطر التحديات التي تؤثر على توافر الشبكة للمستخدمين الفعليين. يوجد عدة أنواع للهجومات لكن يعد هجوم التشويش jamming attack من أخطر الهجمات لأنه يجعل الشبكة غير متاحة بشكل كامل. يهدف هذا البحث إلى دراسة الأنواع المختلفة لهذا الهجوم من ناحية طريقة عملها وآلية تنفيذ الهجوم على الشبكة، ومن ثم دراسة تأثير كل نوع من أنواع التشويش على الشبكة وفق عدة سيناريوهات مقترحة وترتيب الأنواع حسب قوة التأثير. يهدف البحث أيضاً إلى دراسة تأثير الهجوم على بارامترات الشبكة وذلك بهدف اختيار البارامترات الأكثر تأثراً بالهجوم من أجل استخدامها لاحقاً في كشف الهجوم والتصدي له. تكمن أهمية البحث في كونه يعطي تصوراً واضحاً لعمل الهجوم وتأثيره على الشبكة، إضافة لتحديد العلاقة بين الهجوم وبارامترات الشبكة. ويهدف البحث أيضاً إلى دراسة تأثير زيادة عدد المهاجمين أي زيادة فعالية الهجوم على أداء الشبكة.

طرائق البحث ومواده:

من أجل نمذجة وتحليل أنواع هجمات التشويش سوف نقوم ببناء سيناريوهات المحاكاة باستخدام برنامج محاكي الشبكات الإصدار الثالث Network Simulator 3مع إضافات ليدعم التشويش ودراسة بارامتراته[7]، وهو عبارة عن

محاكي شبكات مفتوح المصدر يدعم عدداً كبيراً من بروتوكولات الشبكات المختلفة مع إمكانية إجراء التعديلات ودراسة البارامترات المختلفة وإظهار النتائج وتحليلها. قمنا ببناء عدة سيناريوهات لشبكات Ad hoc مع دراسة البارامترات الآتية بشكل تجريبي باستخدام المحاكي السابق:

a) معدل الرزم المستلمة Packet Delivery Ratio(PDR): وهو نسبة عدد الرزم التي تصل بشكل صحيح بالنسبة لعدد الرزم المرسلة وهو بارامتر مهم لتحديد حالة الشبكة وتأثير التشويش عليها (يقوم البرنامج بقياسها عند كل وصول لرزمة جديدة).

b) قوة الإشارة المستقبلة RSS(Received Signal Strength): استطاعة الإشارة المستقبلة من قبل العقد وتحسب بالواط وهي مقياس لوجود التشويش (تقاس للرزم المرسلة والمستقبلة).

c) التأخير Delay: هو الزمن الذي تحتاجه الرزمة للانتقال من المرسل إلى المستقبل (يقوم البرنامج بقياسها عند كل وصول لرزمة جديدة).

d) الطاقة المستهلكة Energy Consumed: هي كمية الطاقة التي تستهلكها العقد أثناء عمل الشبكة، تتضمن الإرسال والاستقبال والمعالجة وغيرها.

1. هجمات التشويش في الشبكات اللاسلكية وتأثيراتها:

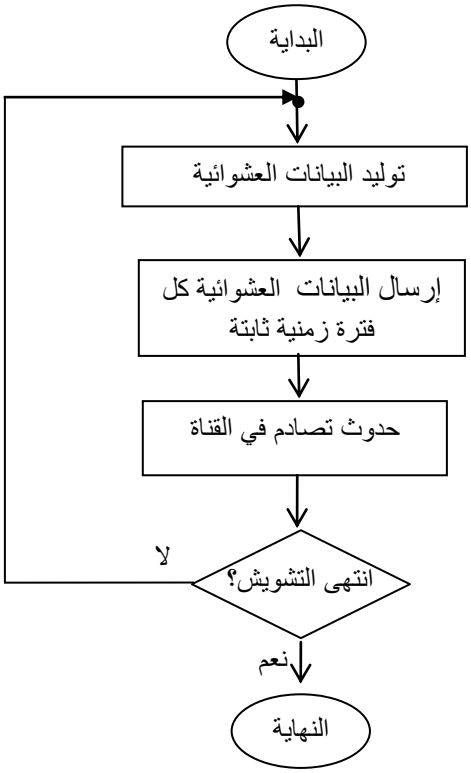
يستخدم المهاجم أو المشوش تداخلاً راديوياً متعمداً من أجل تخريب الاتصال اللاسلكي عن طريق إبقاء وسط الاتصال مشغولاً وهذا يؤدي إلى فشل الاتصالات الحقيقية بين العقد. يمكن أن يتم ذلك عن طريق التأثير على الإشارة المستقبلة بتقليص نسبة الإشارة إلى الضجيج SNR أو دفع المرسل للدخول في حيز انتظار بسبب انشغال الوسط اللاسلكي[8] . يوجد عدة استراتيجيات لهجوم التشويش ويمكن تقسيمها إلى أصناف متعددة تبعاً لعدة نماذج زمنياً وترددياً وحسب الطبقة وغيرها.

1.1. هجمات التشويش في المجال الزمني:

تُقسم الأنواع الرئيسية للتشويش إلى أربعة أصناف[9] هي:

1.1.1.التشويش الثابت Constant jammer:

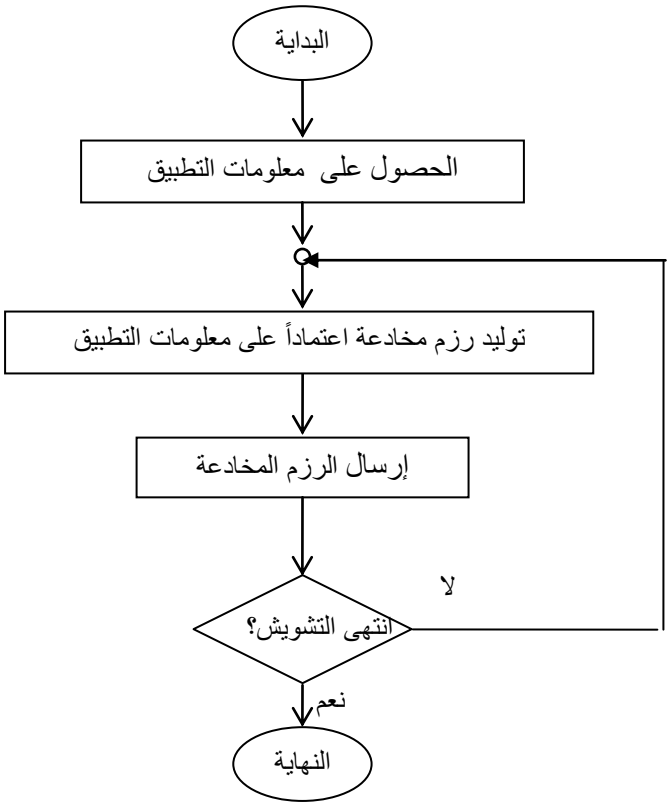
هو عبارة عن إشارات راديوية مستمرة وهي دائماً عشوائية. لا تتبع لبروتوكول MAC محدد وإنما هي تسلسل بتات عشوائي[10]. يقوم المهاجم بتوليد البيانات العشوائية وتشكيل الرزم وبثها بشكل مستمر في القناة، لا يراعي موضوع مشغولية القناة وإنما يتم الإرسال خلال فواصل زمنية ثابتة. بعد إرسال البيانات في القناة تتصادم مع البيانات الحقيقية مما يؤدي إلى فقدها، ولا تصل إلى هدفها. يمثل الشكل (3) خوارزمية عمل التشويش الثابت.



الشكل (3) خوارزمية عمل التشويش الثابت

2.1.1.التشويش المخادع Deceptive jammer:

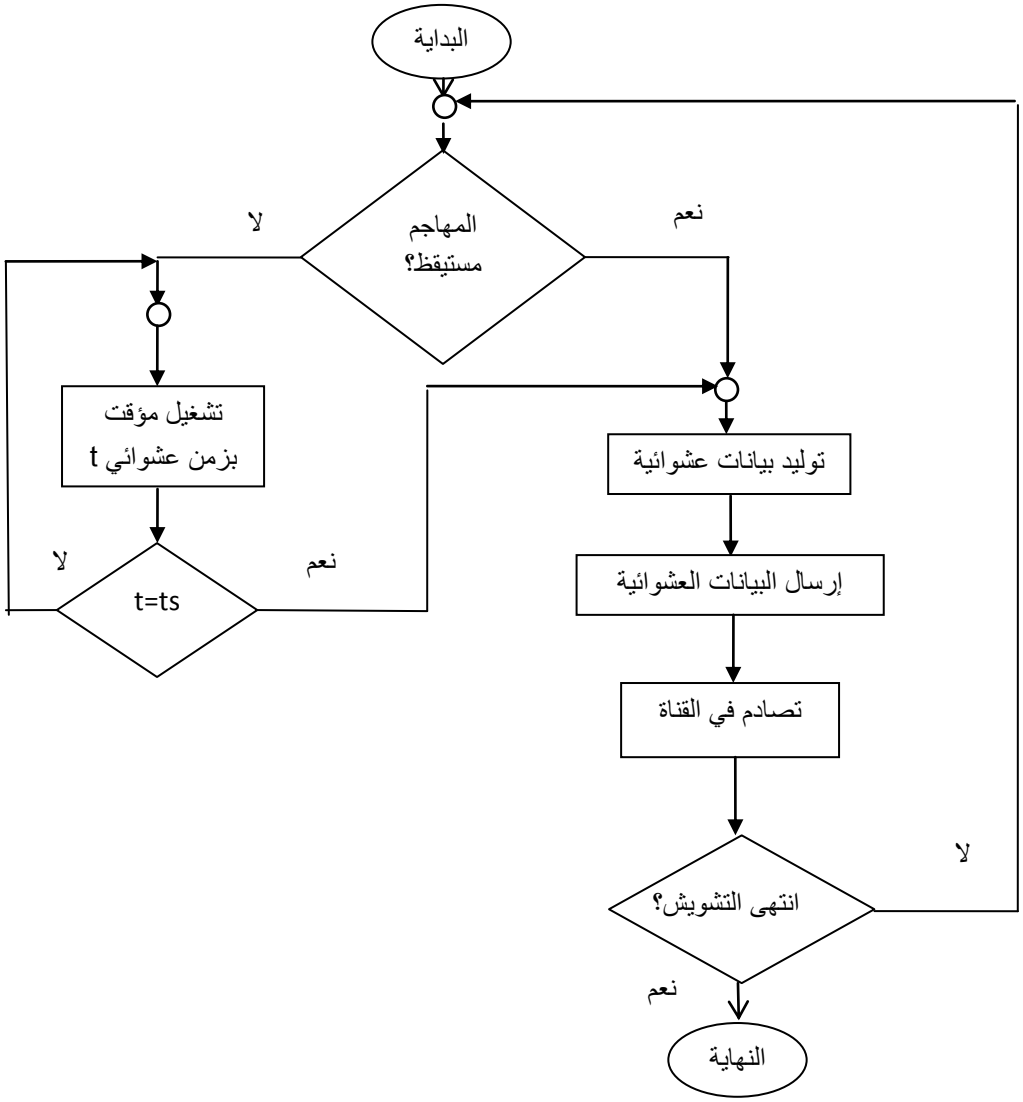
يعمل على حقن رزم حقيقية في القناة دون أي فاصل بين تسلسل الرزم المرسلة (أي بث رزم مشابهة تماماً للرزم الحقيقية المرسلة بين العقد). بالنتيجة سوف يتم خداع الاتصال الحقيقي وستعتقد العقد أن الرزم حقيقية وتقوم باستقبالها[11]. يجب أن يكون للمهاجم قدرة على معرفة المرسل والمستقبل ونوع البيانات المرسلة من أجل توليد الرزم المخادعة وبثها في قناة الاتصال. عندما تصل الرزم المخادعة مع الرزم الحقيقية إلى الهدف سوف تستهلك العقدة مواردها في معالجة الرزم وتمييز البيانات المزيفة.يمثل الشكل (4) خوارزمية عمل التشويش المخادع.



الشكل (4) خوارزمية عمل التشويش المخادع

3.1.1.التشويش العشوائي Random jammer:

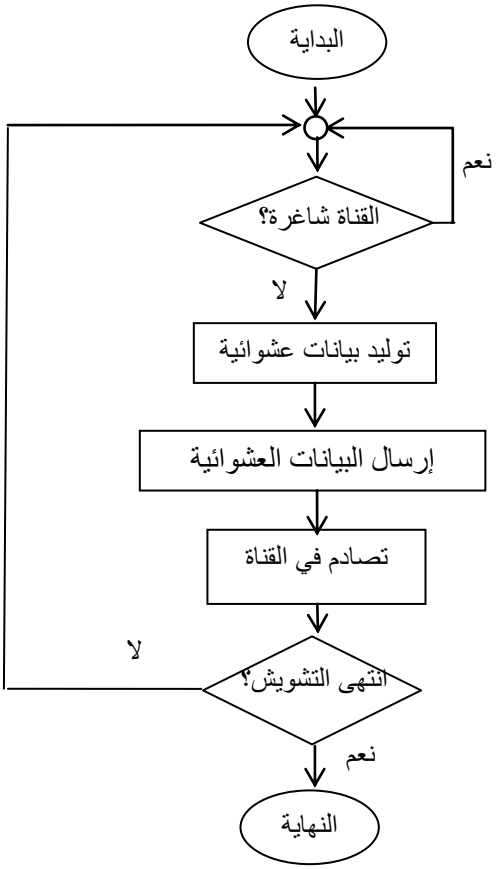
يعتمد هذا النوع من التشويش على التناوب بين النوم والاستيقاظ. أي بعد أن يقوم المهاجم بالتشويش لفترة زمنية tj ، يقوم بإطفاء وحدتهِ الراديوية ويدخل في وضع النوم لزمن ts، وهكذا. الهدف من تطبيق النوم والاستيقاظ هو المحافظة على طاقة المشوش وعدم هدرها. يتم تحديد فترتي النوم والاستيقاظ بشكل عشوائي[12].يمثل الشكل (5)خوارزمية عمل التشويش العشوائي.



الشكل (5) خوارزمية عمل التشويش العشوائي

4.1.1.التشويش التفاعلي Reactive jammer:

يعتمد مبدأ عمله على أن لا ضرورة للتشويش على القناة عندما لا يوجد أية عقدة متصل. يبقى المهاجم خامداً طالما القناة شاغرة ويبدأ إرسال الإشارة الراديوية عندما يتحسس لوجود نشاط في القناة وهكذا يؤثر على عمل القناة[13].يحتاج المشوش في هذا الهجوم إلى مراقبة القناة بشكل دائم، وبذلك يستهلك الطاقة بشكل فعال. يمثل الشكل (6) خوارزمية عمل التشويش التفاعلي.



الشكل (6)خوارزمية عمل التشويش التفاعلي

2. الدراسات المرجعية:

تناولت عدة أبحاث موضوع هجمات التشويش وتأثيرها على شبكات Ad Hoc، في المرجع [14] قام الباحثون بإجراء مقارنة لتأثير أنواع التشويش المختلفة من ناحية الانتاجية والتأخير وكمية الطاقة المستهلكة ووجدوا أن التشويش التفاعلي هو الأكثر خطراً، حيث يزداد التأخير بمعدل 10% وتنقص الإنتاجية حوالي 18% مقارنة مع التشويش العشوائي. في [15] قام الباحثون بدراسة شبكة من عقدتين مع تطبيق أنواع التشويش المختلفة عليها، ولكن الدراسة تمت من ناحية الانتاجية فقط، حيث يخفض تطبيق التشويش التفاعلي الإنتاجية 8% تقريباً. قدم الباحثون [16] تحليلاً لأداء شبكة Ad Hoc تحت تأثير الانواع المختلفة لهجوم التشويش وتمت الدراسة من ناحية معدل الرزم المرسلة ومعدل الرزم المستلمة، وجد الباحث أن التشويش التفاعلي الأكثر خطراً يليه التشويش العشوائي. قام الباحثون في [17] بدراسة تأثير هجوم التشويش التفاعلي على الشبكة مع دراسة تأثير تغيير بارامترات الشبكة وفعالية الهجوم. قدم الباحثان في [18] دراسة لأداء شبكة Ad Hoc تحت تأثير هجوم التشويش دون مراعاة نوع الهجوم ووجدوا أن تطبيق الهجوم يقلل من الإنتاجية حوالي 15% ويزيد من التأخير من ثلاثة إلى تسعة أضعاف. قدم الباحثون في [19] بمقارنة أنواع التشويش من ناحية الزمن الفاصل بين وصول كل رزمتين متتاليتين Packet inter-arrival time، أظهرت النتائج زيادة البارامتر السابق في حالة التشويش التفاعلي بحوالي 0.004 ثانية. يمكن تلخيص الدراسات المرجعية بالنقاط الآتية:

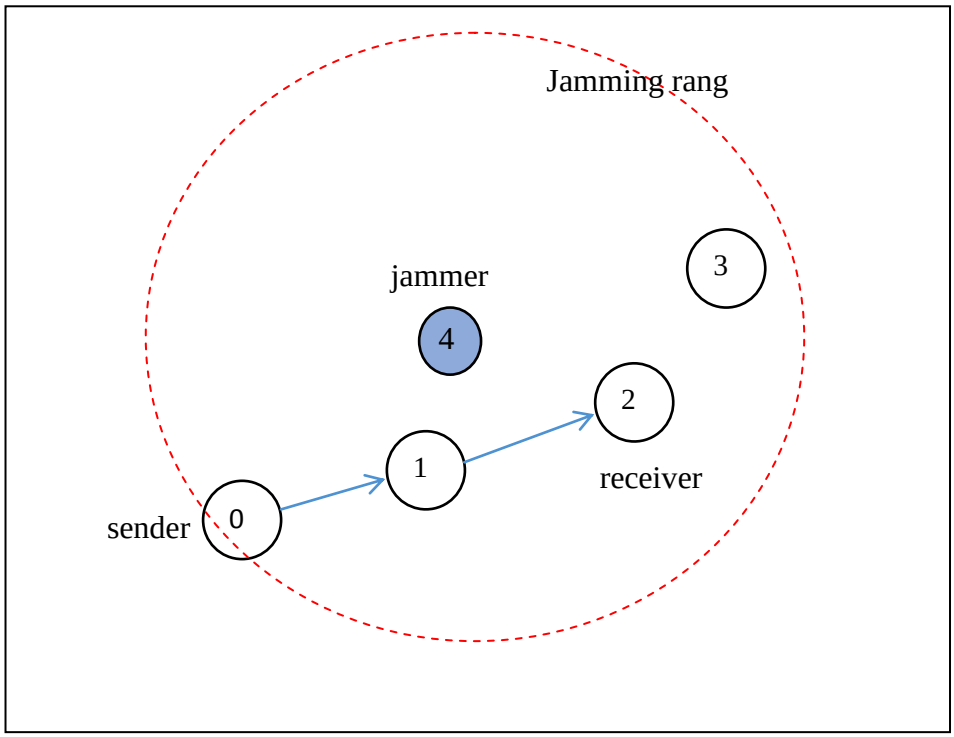
- اعتمدت معظم الدراسات المرجعية على قياس بارامتر واحد أو أكثر من بارامترات الشبكة.
- لم تراع أي من الدراسات المرجعية قضية قوة الإشارة المستقبلة.

- اعتمدت بعض الدراسات على قياس بارامتر واحد فقط لتحليل الهجوم وهذا غير كاف.
- قام الباحثون في بعض الدراسات بدراسة نوع واحد من أنواع التشويش فقط مع إهمال دراسة باقي الأنواع.

النتائج والمناقشة:

1. السيناريو الأول:

قمنا ببناء شبكة Ad hoc مؤلفة من أربع عقد تتبادل البيانات فيما بينها وعقدة تشويش واحدة، تستطيع التشويش على كامل الشبكة، كما في الشكل (7). ترسل العقدة 0 بيانات للعقدة رقم 2 والعقدة 4 هي المشوش.



الشكل (7) الشبكة المدروسة

بهدف دراسة تأثير هجوم التشويش على الشبكة دون تأثر النتائج بأي عوامل أخرى مثل الازدحام أو التصادم صممنا التطبيق بحيث لا يحدث أي ازدحام أو تصادم في الحالة الطبيعة،وكذلك اعتمدنا تقنية DirectSequence Spread Spectrum (DSSS) في الطبقة الفيزيائية لأنها التقنية الأعلى مقاومة للضجيج والتداخل والخفوت في الشبكة. كما اخترنا اللحظة 7 ثانية لبداية التشويش وليس لحظة البداية لكي يتسنى لنا مراقبة حالة الشبكة قبل وبعد تطبيق الهجوم. أخذنا مساحة الشبكة 500x500 متر مربع كي تتناسب مع شبكة Ad hoc وتكون العقد قادرة على الاتصال مع بعضها. قمنا باختيار عدد العقد 4 لكي نتجنب حالة ازدحام الشبكة مع حجم رزمة 200 بايت وعدد رزم 10000 ومعدل نقل 1Mbps لنفس الغاية.

تم اختيار استطاعة الارسال 40mw وهي كافية كي تتصل العقدة مع جيرانها فقط لضمان الاتصال متعدد القفزات. بارامترات المحاكاة المستخدمة موضحة في الجدول (1).

الجدول (1) بارامترات المحاكاة

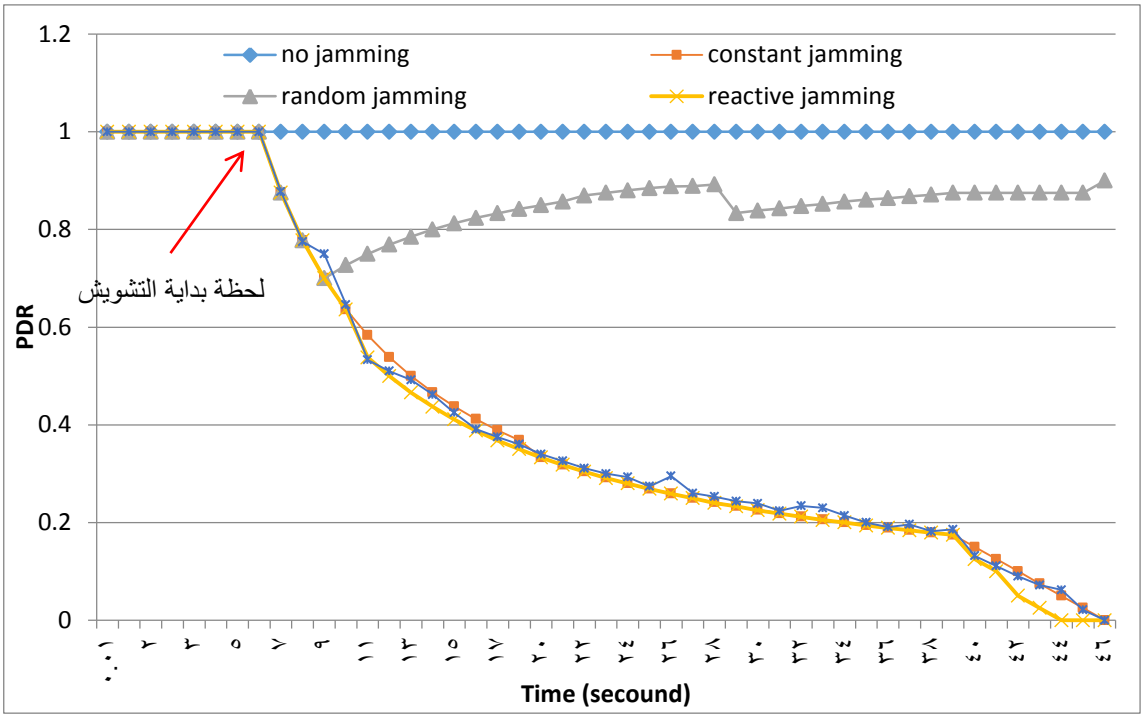
نوع الشبكة	Ad hoc
مساحة الشبكة	$500x500m^2$
عدد العقد	4
زمن المحاكاة	50s
عدد الرزم	10000
حجم الرزمة	200 byte
معدل النقل	1Mbps
بروتوكول الطبقة الفيزيائية	802.11b–DSSS
استطاعة الإرسال	40mw
طاقة العقد	0.1J
زمن بداية التشويش	7s

أجرينا المحاكاة وفق خمس حالات تشمل حالة عدم وجدود التشويش إضافة حالات تطبيق الأنواع الأربعة للتشويش:

a. عدم وجود تشويش No jamming.
b. تشويش ثابت Constant jamming.
c. تشويش مخادع Deceptive jamming.
d. تشويش عشوائي Random jamming.
e. تشويش تفاعلي Reactive jamming.

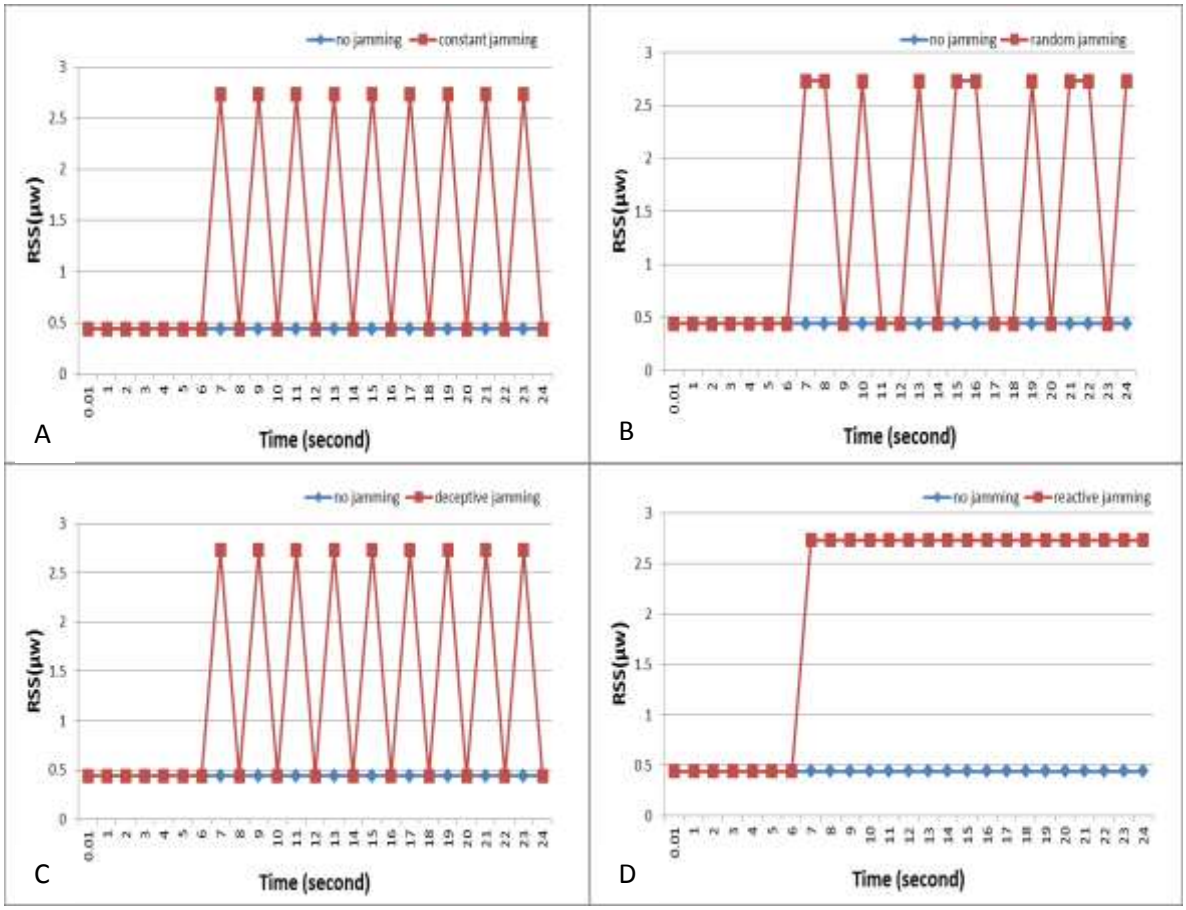
1.1. نتائج السيناريو الأول:

يظهر المخطط (8) قيم معدل الرزم المستلمة عند تطبيق السيناريو الأول مع الحالات الخمسة السابقة، نلاحظ أن قيم معدل الرزم المستلمة من بداية المحاكاة في اللحظة0 وحتى اللحظة التي يبدأ فيها المشوش jammer بث رزم التشويش أي اللحظة7، ثابتة وتساوي الواحد، وهذا يعني أن جميع الرزم التي يتم إرسالها تصل إلى المستقبل (لا يوجد ازدحام في الشبكة قبل بدء التشويش).



الشكل (8) معدل الرزم المستلمة خلال زمن المحاكاة عند العقدة المستقبلة (2)

يبدأ التشويش في اللحظة 7 حيث تنخفض قيمة PDR عند كل فقدان لرزمة وعدم وصولها إلى هدفها. تختلف قيمة PDR عند كل حالة لحالات التشويش الأربعة وتختلف عن حالة عدم وجود تشويش والتي تبقى فيها قيمة PDR ثابتة وتساوي الواحد. نلاحظ أن قيمة PDR تكون أعلى عند تطبيق التشويش العشوائي والسبب أنه يخضع لاحتمال عشوائي لأنه يتم بث التشويش في نفس وقت إرسال الرزم الحقيقية، أما في التشويش الثابت فيتم إرسال الرزم بشكل دائم فينخفض عدد الرزم الحقيقية المستلمة وتنخفض قيمة PDR تدريجياً حتى تقارب الصفر في اللحظة46 ثانية. نلاحظ أن التشويش المخادع الذي يعتمد على إعادة توليد رزم حقيقية وإرسالها إلى الهدف يخفض قيمة PDR بشكل تدريجي حتى تقارب الصفر في اللحظة45.3 ثانية، وأخيراً فإن قيمة PDR عند تطبيق التشويش التفاعلي ستكون بأدنى قيمها، والسبب أن هذا النوع من التشويش يعتمد على حقن رزم التشويش في القناة عندما يكتشف أي نشاط فيها أي سيؤثر على كل عملية إرسال فينخفض عدد الرزم المستلمة وتنخفض قيمة PDR حتى تصل الصفر عند اللحظة43.9 ثانية.

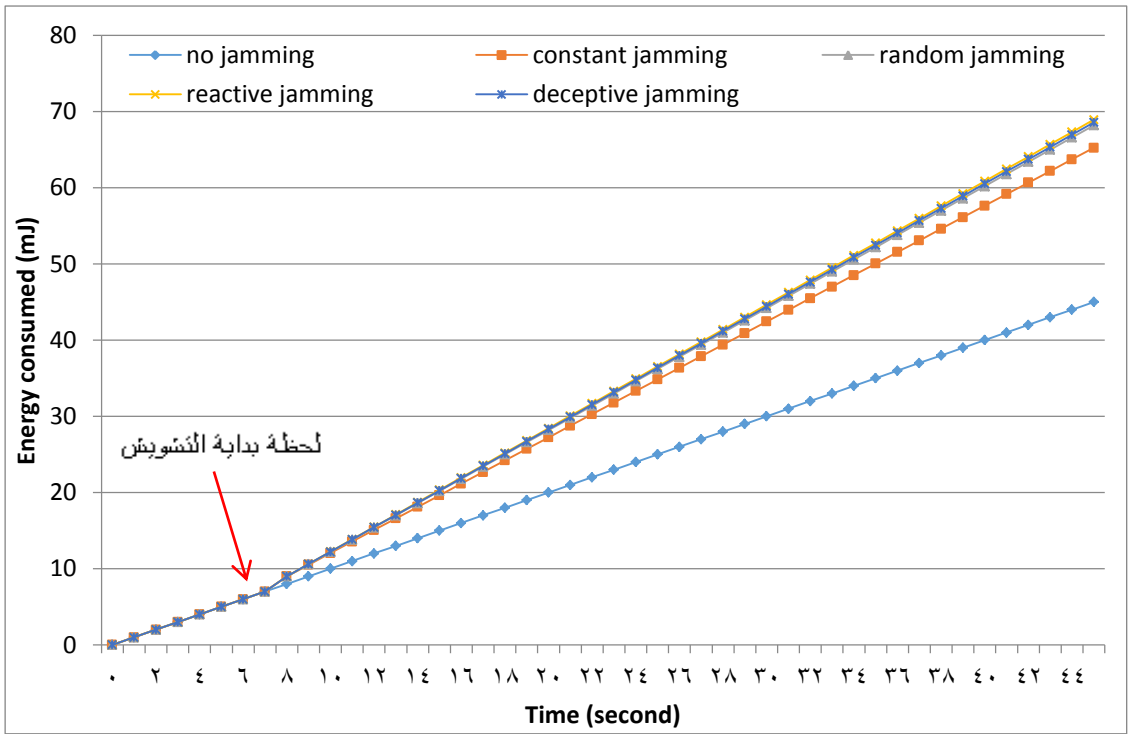


الشكل (9) مخطط قوة الإشارة المستقبلة في حالة عدم وجود تشويش ومقارنة مع حالات التشويش الأربعة: A: تشويش ثابت، B: تشويش عشوائي، C: تشويش مخادع، D: تشويش تفاعلي.

يظهر الشكل (9) (A) مخططاً لقوة الإشارة المستقبلة RSS عند العقدة المستقبلة في حالة تطبيق تشويش ثابت مقارنة مع حالة عدم تطبيق تشويش. نلاحظ أن قيمة قوة الإشارة RSS تبقى ثابتة في بداية المحاكاة (المسافة بين العقد ثابتة ولا يوجد ضجيج) وقيمتها 0.44µW. في لحظة بدء التشويش 7 ثانية ترتفع قيمة RSS لتصل إلى 2.7µW وهي إشارة التشويش التي تتناوب بتواتر ثابت حتى نهاية المحاكاة لأنه في التشويش من النوع الثابت، يترافق التشويش مع إرسال الرزم الحقيقية. يظهر الشكل (9) (B) مخططاً لقوة الإشارة المستقبلة RSS عند تطبيق التشويش العشوائي ونلاحظ تناوب العمل بين وضعي النوم والاستيقاظ لفترات عشوائية. يظهر الشكل (9) (C) مخططاً لقوة الإشارة المستقبلة RSS عند تطبيق التشويش المخادع ونلاحظ أنه مشابه لحالة التشويش الثابت، يقوم المهاجم بقراءة البيانات الحقيقية وتوليد بيانات مشابهه للبيانات الحقيقية وبثها في القناة، وأخيراً يظهر الشكل (9) (D) مخططاً لقوة الإشارة المستقبلة RSS عند تطبيق التشويش التفاعلي، يبدأ المهاجم ببث إشارات التشويش في القناة عند اكتشاف أي نشاط بالقناة ويستمر بالبث طالما القناة نشطة.

يوضح الشكل (10) مخططاً لكمية الطاقة المستهلكة في العقدة المستقبلة عند حالة عدم وجود تشويش وعند الحالات الأربعة للتشويش. نلاحظ أن الطاقة المستهلكة عند عدم وجود تشويش تتزايد بشكل خطي من القيمة 0حتى تصل إلى 45 ميلي جول. عند تطبيق أنواع التشويش الأربعة نلاحظ زيادة الطاقة المستهلكة بشكل متقارب، وسبب الزيادة هو الطاقة المستهلكة في استقبال رزم التشويش إضافة إلى عمليات إعادة إرسال الرزم. تعتمد العقد في أغلب تطبيقات

شبكات Ad hoc على بطاريات محدودة الطاقة لذلك فإن المحافظة على طاقة العقد من أخطر التحديات التي تواجه هذه الشبكات.

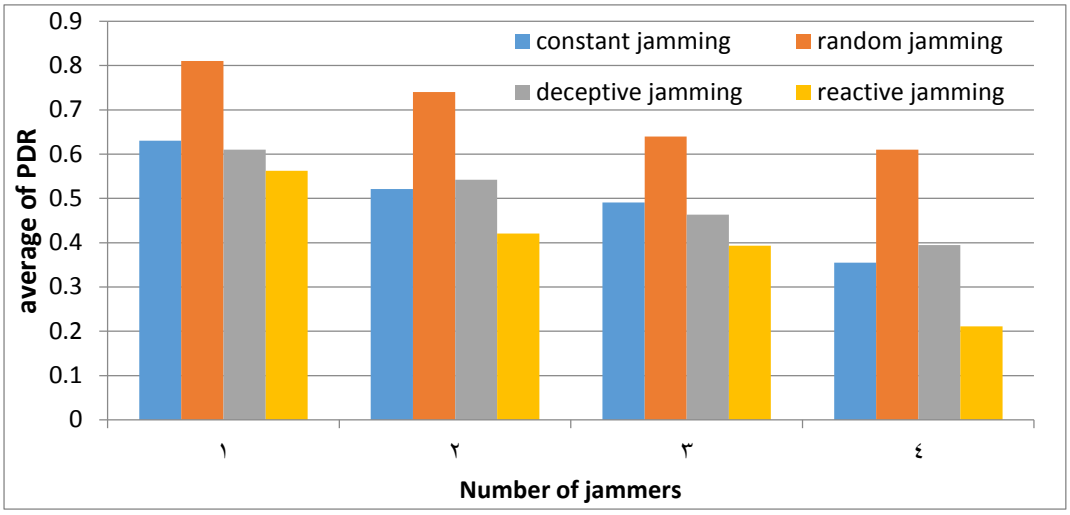


الشكل (10) مقدار الطاقة المستهلكة في العقد خلال الزمن لأنواع التشويش المختلفة

2.1. السيناريو الثاني:

في هذا السيناريو حافظنا على الفرضيات التي تتعلق ببناء الشبكة في السيناريو الأول لكن مع زيادة عدد العقد المهاجمة (المشوش) من عقدة واحدة إلى4 عقد، ودرسنا بارامترات متوسط معدل الرزم المستلمة ومتوسط التأخير والطاقة الإجمالية المستهلكة، وقياس البارامترات السابقة عند العقدة المستقبلة.

يبين الشكل (11) مخطط متوسط PDR عند زيادة عدد المهاجمين في الشبكة. نلاحظ أن معدل الرزم المستلمة ينخفض مع زيادة عدد العقد المهاجمة، وهذا ناتج عن زيادة فعالية التشويش أي اشتراك أكثر من مهاجم في بث رزم التشويش وبالنتيجة فشل أكبر في وصول الرزم الحقيقية إلى هدفها.



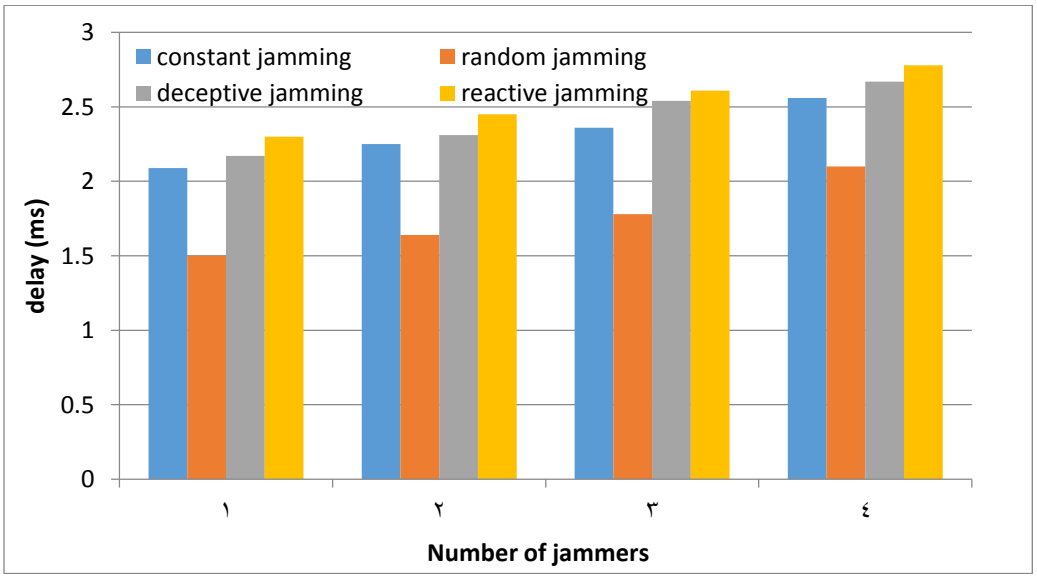
الشكل (11) مخطط متوسط معدل الرزم المستلمة بالنسبة لعدد العقد المهاجمة

نلاحظ أن قيمة متوسط PDR أعلى في حالة التشويش العشوائي لأن الفترات التي يحدث فيها التشويش عشوائية ولا تتعلق بالبيانات الحقيقية. في حالة التشويش المخادع والتشويش الثابت تقل قيمة PDR حوالي 20% مقارنةً مع التشويش العشوائي، أما حالة التشويش التفاعلي فهي الأعلى خطورة وينخفض فيها متوسط PDR بين 25% إلى 50% مقارنة بالتشويش العشوائي لأنه يعمل عند كل نشاط للقناة.

يظهر الشكل (12) مخطط التأخير الإجمالي للرزم من نهاية إلى نهاية محسوبة عند العقدة المستقبلة مع زيادة عدد العقد المهاجمة.

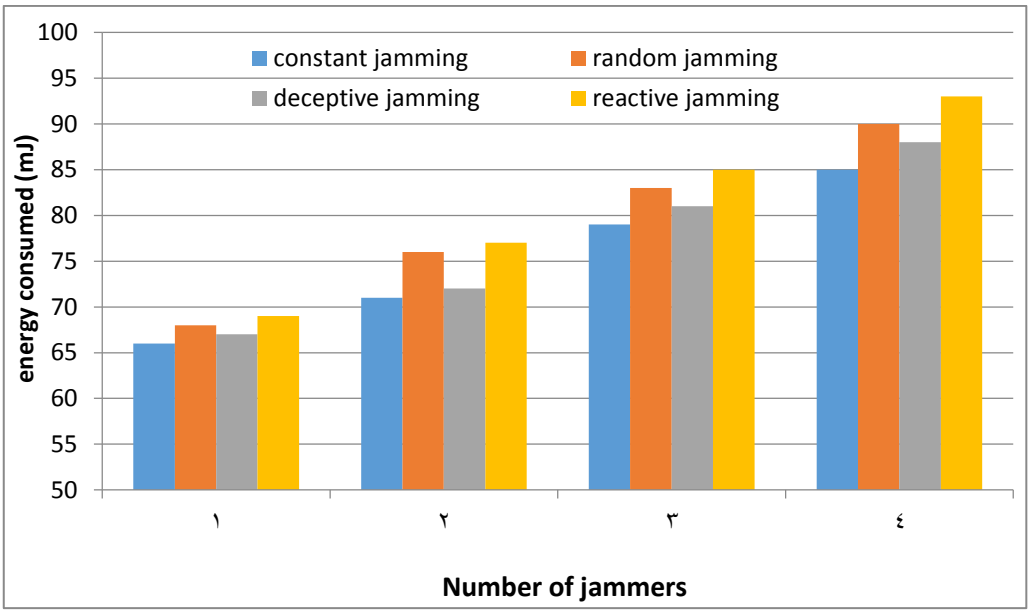
نلاحظ من المخطط أن قيمة التأخير تزداد بزيادة عدد المهاجمين، بسبب زيادة الزمن اللازم لوصول الرزم إلى هدفها.

نلاحظ أن قيمة التأخير في حالة التشويش التفاعلي تملك القيمة الأعلى وتزيد بمقدار 0.9 إلى 1.2 ميلي ثانية مقارنة بالتشويش الثابت ذو القيمة الأدنى.



الشكل (12) مخطط تأخير الرزم المستلمة بالنسبة لعدد العقد المهاجمة

يوضح الشكل (13) مخططاً لكمية الطاقة المستهلكة في العقدة 2 خلال زمن المحاكاة مع زيادة عدد المهاجمين. نلاحظ أن قيمة الطاقة المستهلكة تزداد بازدياد عدد المهاجمين، وذلك بسبب زيادة رزم التشويش المستقبلة وزيادة عمليات المعالجة لتمييز الرزم الصحيحة. نجد أن قيم الطاقة المستهلكة عند الحالات الأربعة للتشويش متقاربة وتختلف عن بعضها من 1 إلى 3 ميلي جول تقريباً.



الشكل(13) مخطط الطاقة المستهلكة في العقدة بالنسبة لعدد المهاجمين

الاستنتاجات والتوصيات:

قدمنا في هذا البحث دراسة تحليلية لتأثير هجوم التشويش على شبكاتAd hoc آخذين بالحسبان الحالات الأربعة للتشويش، حيث قارنا تأثير التشويش على بارامترات الشبكة عند الحالات الأربعة باستخدام بيئة المحاكاة NS3، يمكننا تلخيص النتائج التي تم الحصول عليها في النقاط الآتية:

1. يؤثر هجوم التشويش على شبكات Ad hoc بحيث ينخفض معدل الرزم المستلمة ويزداد التأخير واستهلاك الطاقة.
2. ينخفض أداء الشبكة التي يطبق عليها تشويش عشوائي مقارنةً مع حالة عدم وجود تشويش بنسبة من 10–20% بالنسبة لـ PDR، لأن المهاجم يولد اشارة التشويش بشكل عشوائي ومستقل عن حالة القناة.
3. ينخفض أداء الشبكة التي يطبق عليها تشويش ثابت مقارنةً مع حالة تشويش عشوائي بنسبة من 5–30% بالنسبة لـ PDR، وزيادة استهلاك طاقة حوالي 5 ميلي جول.
4. عند تطبيق التشويش المخادع تستهلك العقدة المستقبلة مصادرها في معالجة الرزم الخاطئة فينخفض معدل الرزم المستلمة بمقدار 2% مقارنة مع التشويش الثابت.
5. يعد التشويش التفاعلي الأخطر بين أنواع التشويش لأنه مرتبط بحالة القناة، لذا تنخفض قيمة معدل الرزم المستلمة بنسبة من 2–5% مقارنة مع التشويش المخادع.

6. يزداد تأثير الهجوم على الشبكة بزيادة عدد العقد المهاجمة (زيادة فعالية الهجوم)، فتنخفض قيمة PDRويزداد التأخير واستهلاك الطاقة مع كل زيادة في عدد العقد المهاجمة.

7. يزيد هجوم التشويش من استهلاك الطاقة في العقد وكما نعلم أن قضية حفظ الطاقة من أهم التحديات التي تواجه شبكات Ad hoc.

8. نلاحظ أن البارامترات المدروسة تتأثر بمستويات مختلفة بالتشويش. وجدنا أن بارامتر معدل الرزم المستلمة PDR يتغير بشكل سريع بتأثير الهجوم، بسبب أنه يتغير مع كل وصول لرزمة جديدة أو عدم وصولها.

بعد تحليل النتائج السابقة نوصي بالعمل على تجنب التأثيرات السلبية لهجوم التشويش على الشبكة من خلال اتخاذ عدة إجراءات حماية (تبديل القناة، استخدام مسارات بديلة للبيانات،....)، كما نوصي بالعمل في مجال كشف التشويش من أجل تمييز حالة حصول التشويش (مثل الحالات التي تم دراستها سابقاً)، من الحالات الأخرى لانخفاض أداء الشبكة مثل الازدحام والضجيج ومشكلة العقد المخفية والبعد بين العقد، وذلك عن طريق الاستفادة من تغير قيم البارامترات المدروسة بتأثير الهجوم.

المراجع

[1] LU, Z. WANG, C and WEI, M. *On detection and concealment of critical roles in tactical wireless networks*, in Military Communications Conference. MILCOM - IEEE, Oct 2015, 909–914.

[2] OSANAIYE, O. ALFA, A and HANCKE, G. *A Statistical Approach to Detect Jamming Attacks in Wireless Sensor Network*, Sensors (Basel). May 2018.

[3] بشرى معلا، علاء محفوض. خوارزمية القائمة السوداء الديناميكية للحماية من هجوم حجب الخدمة الموزع DDoS في شبكة العربات المتنقلة. سلسلة العلوم الهندسية، مجلة جامعة تشرين للبحوث والدراسات العلمية، المجلد (39)، العدد (3)، 2017.

[4] ANWAR, A. ATIA, G. and GUIRGUIS, M. *Adaptive topologies against jamming attacks in wireless networks: A game-theoretic approach.* Journal of Network and Computer Applications, Vol. 121, November 2018, 44-58.

[5] JAIN, A. BHUSHANWAR, K and MALVIYA, V. *A Survey on Jamming Attacks and Its Types in Wireless Networks*. International Journal of Technology Research and Management, Vol. 4, no.6, June 2017, 1-8.

[6] LU, Z. WANG, C and WANG, M. *Modeling, evaluation and detection of jamming attacks in time-critical wireless applications*. Mobile Computing IEEE Transactions, vol. 13, no. 8, 2014, 1746–1759.

[7] Ns3. Portal. [Online]. Available: http://www.nsnam.org, LAST VISITE 20/12/2018.

[8] SIVANESHSAN, B and THARMALINGAM, A. *Impacts and prevention techniques of jamming attacks in Wireless ad hoc networks*. SSRG International Journal of Mobile Computing & Application (SSRG-IJMCA) ,vol. 4, Issue1, 2017, 13-18.

[9] XU, W. TRAPPE, W. ZHANG, Y and WOOD, T. *The feasibility of launching and detecting jamming attacks in wireless networks*. in ACM International Symposium on Mobile Ad Hoc Networking & Computing, 2005, 46-57.

[10] WILHELM, M. MARTINOVIC, I. SCHMITT, J and LENDERS, V. *Short paper: Reactive jamming in wireless networks: How realistic is the threat.* The fourth ACM conference on Wireless network security, 2011, 47-52.

[11] NEHA, T. and ARUNA, S. *Introduction to Jamming Attacks and Prevention Techniques using Honeypots in Wireless Networks*. IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), Vol. 3, No.2, April 2013, 202-207.

[12] MAHESWARI, R. RALESWARI, S. and PHIL, M. *A Review on Types of Jamming Attack InMobile Ad-Hoc Network.* Proceedings of the UGC Sponsored National Conference on Advanced Networking and Applications, March 2015, 84-86.

[13] RUPANI, P and TADA, N. *Literature Survey on Jamming Attack in Wireless Adhoc Network.* International Journal of Engineering Development and Research, Vol. 5, N. 2, 2017 , 434-443.

[14] BABAR, S. PRASAD, N. and PRASAD, R. *Jamming Attack: Behavioral Modelling and Analysis.* Wireless VITAE 2013, IEEE October 2013.

[15] BAYRAKTAROGLU, E. KING, C. LIU, X. NOUBIR, G and RAJMOHAN, A . *Performance of IEEE 802.11 under Jamming.* Mobile Networks and Applications, Volume 18, Issue 5, pp. 678–696, August 2011.

[16] YU, B and ZHANG, L. *An Improved Detection Method for Different Types of Jamming Attacks in Wireless Networks.* 2014 2nd International Conference on Systems and Informatics, IEEE 2014, 553-558.

[17] SHINE, I. SHEN,Y. XUAN, Y. THAI, M and ZNATI, T. *A Novel Approach Against Reactive Jamming Attacks.* Ad Hoc & Sensor Wireless Networks, Vol. 0, June 14, 2010, 1-25.

[18] POPLI, P. and RAJ, P. *Effect of Jamming Attack in Mobile Ad Hoc Environment*. International Journal of Science, Engineering and Technology Research (IJSETR), Volume 5, Issue 5, May 2016, 1521-1526.

[19] OSANAIYE, O. ALFA, A. and HANCKE, G. *A Statistical Approach to Detect Jamming Attacks in Wireless Sensor Networks.* Sensors 2018, 18, 1691, 24 May 2018, 1-15.