مجلة جامعة تشرين للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (40) العدد (1) 2018
Tishreen University Journal for Research and Scientific Studies - Engineering Sciences Series Vol. (40) No. (1) 2018

Study and analysis the impact of Denial of Service attacks on ZigBee networks (Tree Topology) compared to (Mesh Topology) according to the metrics (delay, load, and Throughput)

Dr. Ahmad Saker Ahmad*
Lujain Saqer**

(Received 19 / 3 / 2018. Accepted 22 / 4 / 2018)

□ ABSTRACT □

ZigBee networks have revolutionized industrial control, remote data collection and intelligent home automation as they rely on ZigBee, a wireless data transmission technology designed to meet the unique needs of wireless sensor networks such as low power consumption and low transmission rates to maintain Battery life is longer, and is based on IEEE 802.15.4

Security is one of the fundamental issues of any network, and the study of attacks and their impact of the important and necessary, The most serious of these attacks Denial of Service Denial of Service, is an attack aimed at denial of service and attempt to make this service unavailable or delayed access to the users concerned.

The aim of this study is to analyze the impact of denial-of-service attacks on ZigBee networks with tree topology and mesh topology, and compare them through criteria: delay, load, and throughput, as they are the most important metrics determining the performance and effectiveness of the network .

The study was carried out using OPNET 14.5 simulation tool, which is one of the most important programs used in the modeling and simulation of wired and wireless networks, and to conduct many experiments and compare them through the mentioned metrics.

The results showed that the attack on ZigBee network lead to different damages depending on the topology, so we have studied and analyzed the impact of denial of service attacks on two different types of topologies, Tree and mixed (Mesh), since these two topologies give certain results in the absence of an attack and different results in case of attack on them.

Key words: ZigBee ، (WSN) ،Denial of Service ،OPNET،Topology.

* **Professor, Department of Computer Networks & System, Faculty of Information Technology, University of Tishreen, Lattakia, Syria.**

** **Postgraduate Student, Department of Computer Networks & System, Faculty of Information Technology, University of Tishreen, Lattakia, Syria.**

مجلة جامعة تشرين للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (40) العدد (1) 2018
Tishreen University Journal for Research and Scientific Studies - Engineering Sciences Series Vol. (40) No. (1) 2018

دراسة وتحليل أثر هجمات الحرمان من الخدمة Denial of Service على شبكات الـZigBee ذات الطوبولوجيا الشجرية (Tree) بالمقارنة مع الطوبولوجيا المختلطة (Mesh) من خلال معايير(التأخير، الحمل، والإنتاجية)

الدكتور أحمد صقر أحمد*
لجين صقر**

(تاريخ الإيداع 19 / 3 / 2018. قُبِل للنشر في 22/ 4 / 2018)

□ ملخّص □

أحدثت شبكات ZigBee تحولاً جذرياً في ميدان التحكم الصناعي، وجمع البيانات عن بعد، وأتمتة المنازل الذكية حيث أنها تعتمد على ZigBee وهي تقنية لنقل البيانات في شبكة لاسلكية، و مصممة لتلبية الاحتياجات الفريدة لشبكات الاستشعار اللاسلكية مثل استهلاك منخفض للطاقة، ومعدلات نقل منخفضة، للحفاظ على عمر البطارية أكبر وقت، وتعتمد على المعيار IEEE 802.15.4 .

الأمن هو من القضايا الاساسية لأي شبكة، ودراسة الهجمات وتأثيراتها من الأمور الهامة والضرورية، ومن أخطر هذه الهجمات هجوم الحرمان من الخدمة Denial of Service، هو هجوم يهدف الى الحرمان من الخدمة و محاولة جعل هذه الخدمة غير متوفرة أو تصل متأخرة إلى المستخدمين المعنيين بها.

إن هدف هذه الدراسة هو تحليل أثر هجمات الحرمان من الخدمة على شبكات الـ ZigBee ذات الطوبولوجيا الشجرية (Tree)، والطوبولوجيا المختلطة (Mesh) ، والمقارنة بينها من خلال المعايير: التأخير، الحمل، والإنتاجية، حيث أنها من أهم المعايير التي تحدد أداء وفعالية الشبكة.

تمت الدراسة باستخدام أداة المحاكاة OPNET 14.5 الذي يعتبر من أهم البرامج المستخدمة في نمذجة ومحاكاة الشبكات السلكية واللاسلكية، والقيام بالعديد من التجارب ومقارنتها من خلال المعايير المذكورة.

حيث أظهرت النتائج أن الهجوم على شبكة الـZigBee يؤدي الى أضرار تختلف باختلاف طوبولوجيتها، لذلك قمنا بدراسة وتحليل أثر هجمات الحرمان من الخدمة على نوعين مختلفين من الطوبولوجيات وهي الشجرية (Tree) والمختلطة (Mesh)، حيث أن هاتين الطوبولوجيتين تعطيان نتائج معينة في حالة عدم وجود هجوم ونتائج مختلفة في حالة الهجوم عليها.

الكلمات المفتاحية: ZigBee ، شبكات الاستشعار اللاسلكية (WSN)، هجمات الحرمان من الخمة، Denial of Service، OPNET، طوبولوجيا.

*أستاذ – قسم النظم والشبكات الحاسوبية – كلية الهندسة المعلوماتية – جامعة تشرين – اللاذقية – سورية.
**طالبة ماجستير – قسم النظم والشبكات الحاسوبية – كلية الهندسة المعلوماتية – جامعة تشرين – اللاذقية – سورية.

مقدمة:

تعتبر شبكات ZigBee ثورة علمية في مجال شبكات الاستشعار اللاسلكية ويعتبر المعيار IEEE 802.15.4 ممثلا" لها، وتتميز تقنية ZigBee لنقل البيانات اللاسلكية بأنها تستغرق وقتا" قليلاً جداً لبدء العمل، وتستهلك قدرا" قليلا" من الطاقة، ومعدل بياناتها منخفض مقارنة بـ Wi-Fi وبلوتوث كما يوضح الجدول (1-1) . مما يساعدها في سرعة اتخاذ القرار، والحفاظ على عمر البطارية أطول وقت ممكن، وهذا ما جعلها مناسبة لأنظمة التحكم بالصناعة [1] .

تستخدم تقنية ZigBee في التطبيقات التي تحتاج الى استهلاك قدر قليل من الطاقة، ومعدل بيانات منخفض، وأجهزة الـ ZigBee لها معدل تأخير منخفض، مما يقلل من متوسط استهلاك التيار الكهربائي، فشبكات الـ ZigBee جزء لا يتجزأ من الاستشعار عن بعد، وجمع البيانات الطبية، والدخان، والإنذار بدخيل، وأتمتة والتشغيل الآلي للمنازل الذكية الخ... [2].

الجدول (1-1) مقارنة ZigBee مع غيرها من تقنيات الشبكة اللاسلكية

	ZigBee	Wi-Fi (802.11n)	Bluetooth
Data Rate	20,40 and 250 Kbps	up to 150Mbps	1Mbps
Range	10-3000m	70-250m	10-100m
Frequency	868MHz, (EU) 900-928MHz, (NA) 2.4GHz (WL)	2.4 & 5 GHz	2.4GHz
Complexity	Low	High	High
Battery Life (days) [3]	100 to > 1000	1 to 5	1 to 7

يوضح الجدول (1-1) مقارنة ZigBee مع غيرها من تقنيات الشبكة اللاسلكية من حيث معدل نقل البيانات، المجال، الترددات، التعقيد، وعمر البطارية [2].

ونلاحظ من الجدول السابق ان معدل نقل البيانات في ZigBee منخفض مقارنة" بباقي التقنيات، ومجال ZigBee أوسع ، ويدعم ترددات اتصال متعددة، وتعقيده أقل من باقي التقنيات، وأهم صفة فيه أن عمر البطارية يدوم لسنوات.

تعمل شبكات الـ ZigBee في النطاقات الراديوية الصناعية والعلمية والطبية industrial, scientific and medical (ISM) التالية:

- 2.4 GHz في معظم الولايات في جميع أنحاء العالم
- 784 MHz في الصين
- 868 MHz في أوروبا
- 915 MHz في الولايات المتحدة وأستراليا

وتتراوح معدلات البيانات من 20 kbps الى 250 kbps.

تتكون تقنية ZigBee من أربع طبقات وهي [3] :

- الطبقتين العلويتين: طبقة التطبيقات، وطبقة الشبكة .
- والطبقتين السفليتين: طبقة الولوج للوسط الفرعية Media Access Control (MAC) ، والطبقة الفيزيائية.

أجهزة شبكات ZigBee:

الاجهزة في شبكة ZigBee لها ثلاث أنواع [3] :

- **منسق ZigBee (ZC)ZigBee Coordinator** : الجهاز الأكثر قدرة، وهو الذي يشكل جذر الشبكة و ربما جسر إلى شبكات أخرى. هناك على وجه التحديد منسق واحد ZC في كل شبكة لأنه يقوم ببدء عمل الشبكة ويخزن المعلومات عن الشبكة، بما في ذلك العمل كمركز الثقة ومستودع لمفاتيح الأمن.
- **موجه ZigBee (ZR)ZigBee Router** : مسؤول عن عمليات التوجيه في الشبكة، وحفظ جداول التوجيه، ويعمل كوسيط لتمرير البيانات من الأجهزة الأخرى عند استخدامه لتوسعة الشبكة.
- **عقد النهاية ZigBee (ZED)ZigBee End devices** : تقوم بالتواصل مع العقدة الرئيسية (المنسق ZC أو الموجهZR)؛ لأنه لا يمكنها تمرير البيانات من الأجهزة الأخرى. وهذا ما يجعلها غير نشطة لفترة طويلة من الزمن مما يزيد من عمر البطارية ، ZED .يتطلب أقل قدر من الذاكرة، وبالتالي، يمكن أن تكون أقل تكلفة بالنسبة للمكونات المادية من ZR أو ZC.

يجب أن يكون في كل طوبولوجيا منسق واحد فقط مكلف بإنشائها والسيطرة على معالمها والصيانة الاساسية.

تتوزع هذه الأجهزة على أكثر من طوبولوجيا مثل:

- **الطوبولوجيا الشجرية (Tree):** وتتكون الشبكة من عقدة مركزية هي المنسق والعديد من أجهزة التوجيه وأجهزة النهاية ترتبط ببنية شجرية، بحيث يكون المنسق فيها هو جذر الشبكة.
- **والطوبولوجيا المختلطة (Mesh):** وميزتها هي أنه إذا فشل أي جهاز توجيه، عندها يمكن اكتشاف طرق بديلة واستخدامها.

من أكثر المشاكل التي تعاني منها الشبكات هي مشاكل الأمن والتعرض للهجمات، ومن أخطر هذه الهجمات هجوم الحرمان من الخدمة (DoS).

هجوم إيقاف الخدمة Denial of Service :

هجوم إيقاف الخدمة أو الحرمان من الخدمة هو محاولة لجعل الخدمة غير متوفرة أو تصل بشكل متأخر الى المستخدمين المعنيين بها. كما أن وسائل وأسباب وأهداف هذا النوع من الهجوم متعددة، ولكن بالعموم تتألف من تأثيرات مشتركة لشخص أو أشخاص لمنع الخدمة من أن تعمل بشكل صحيح أو فعال أو أن تتأخر بالوصول لهدفها بالوقت المطلوب الذي يحتاجها في موعد محدد، وذلك بشكل مؤقت أو يدوم لفترة غير محددة [4] .

أهمية البحث وأهدافه:

تأتي اهمية البحث من أهمية شبكات الـ ZigBee في الوقت الحالي ودورها الكبير في مجال التحكم بالصناعة و الأتمتة والتشغيل الآلي للمنازل الذكية، وجمع المعلومات الطبية، والإنذار بدخيل وغيرها الكثير، ومن خطر هجوم الحرمان من الخدمة و دراسة تأثيرات هذا الهجوم عليها.

يهدف البحث إلى دراسة وتحليل أثر هجوم الحرمان من الخدمة على هذه الشبكات بنوعين مختلفين من الطوبولوجيات وهي الشجرية (Tree) والمختلطة (Mesh).

طرائق البحث ومواده:

- **المحاكي المستخدم:**

اعتمدنا في دراستنا على استخدام المحاكي OPNET Modeler version 14.5 وهو اختصار لـ Optimized Network Engineering Tools أي أداة هندسة الشبكة المحسنة ، وهو برنامج معروف عالميا" في مجال محاكاة الشبكات و يعتبر من أهم البرامج المستخدمة في نمذجة ومحاكاة الشبكات السلكية واللاسلكية ومن أكثر البرامج انتشارا" لدى الباحثين في المجال الأكاديمي[5] .

- **السيناريوهات المدروسة**[6,7] :

تمت نمذجة ومحاكاة الطوبولوجيتين لشبكة Zigbee بالوضع الطبيعي للشبكة، أي بدون وجود هجوم عليها. و الطوبولوجيات هي: الشجرية (Tree)، والمختلطة (Mesh)، وقمنا بنمذجة هجوم الحرمان من الخدمة حيث يقوم المهاجم باستهداف الشبكة.

- **المعايير**[8,9] :

تمت دراسة وتحليل أثر هجوم الحرمان من الخدمة من خلال المعايير:

1. **التأخير(Delay)**: هو أحد مقاييس الأداء المهمة في الشبكات، وهو متوسط التأخير اللازم لانتقال رزم البيانات من المصدر الى الهدف عبر شبكة الاتصال، ويقاس التأخير بالثانية، وكلما كانت قيمة التأخير أكبر كان أداء الشبكة أضعف، كما أن زيادة التأخير بالشبكة قد يسبب ازدحام فيها .
2. **الحمل(Load)**: يستخدم هذا المقياس لقياس العبء على الشبكة، ويقدر هذا المقياس غالبا بعدد الرزم التي ترسل بالشبكة في واحدة الزمن(pkts/sec)، أو بعدد البتات المرسلة خلال الشبكة في واحدة الزمن (bits/sec)، وكلما كانت هذه الأرقام أكبر كان استخدام عرض الحزمة المتاح أكبر.
3. **الإنتاجية (Throughput)**: هي معدل الرزم أو البتات الواصلة بنجاح الى هدفها خلال واحدة الزمن، وتقدر الانتاجية بـ (bits/sec)، وتعد انتاجية الشبكة من المعايير الهامة التي يجب اخذها بعين الاعتبار عند تقييم اداء الشبكة .

النتائج والمناقشة:

1-المرحلة الأولى:

قمنا بنمذجة ومحاكاة نوعين من الطوبولوجيات لشبكة Zigbee بالوضع الطبيعي للشبكة، أي بدون وجود هجوم عليها. و الطوبولوجيات هي :الشجرية (Tree)، والمختلطة (Mesh). الجدول (4-1)

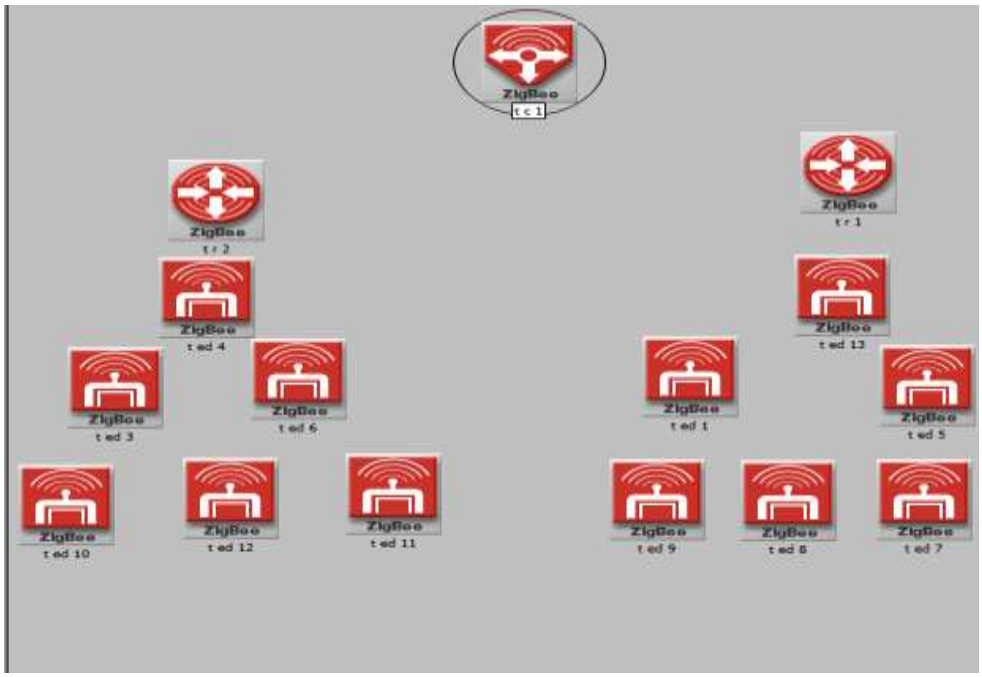
الجدول (4-1) طوبولوجيات شبكة Zigbee المدروسة:

شكل الطوبولوجيا	عدد العقد بالشبكة	انواع الأجهزة الموجودة	زمن المحاكاة
Tree	15	منسق، موجه، عقد نهاية	ساعة
Mesh	15	منسق، موجه، عقد نهاية	ساعة

1-1-السيناريو الأول:

في هذه السيناريو:

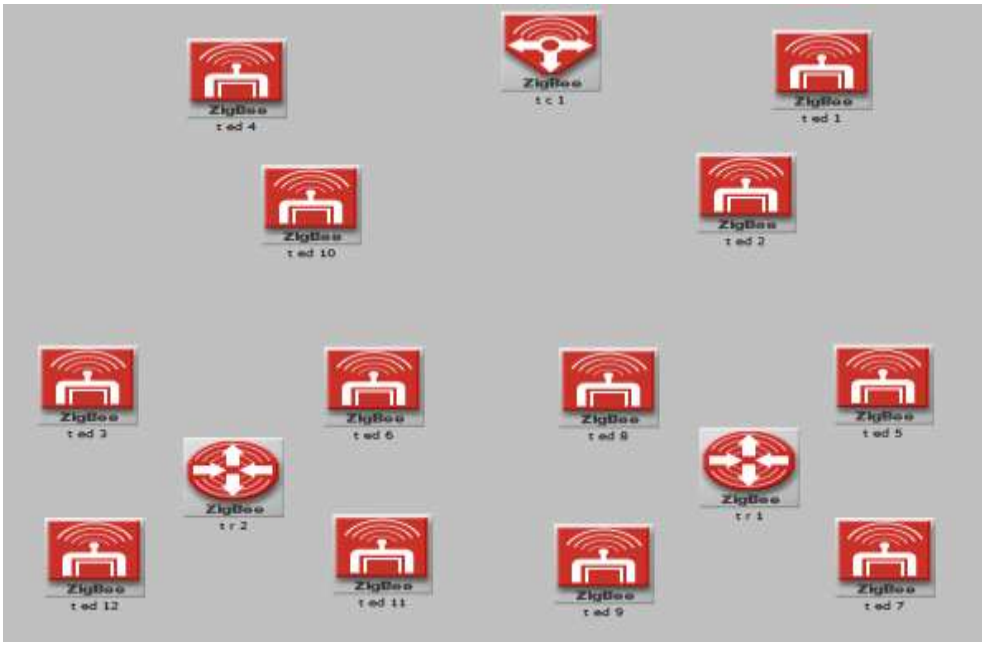
1. قمنا بنمذجة شبكة Zigbee بطوبولوجيا شجرية (Tree) الشكل(4-1).



الشكل(4-1) شبكة Zigbee بطوبولوجيا شجرية

يوضح الشكل(4-1) شبكة Zigbee بطوبولوجيا شجرية (Tree) مكونة من خمسة عشر عقد، وهي عبارة عن منسق واحد، وموجهين، اثنتا عشرة عقدة نهاية.

2. تمت نمذجة شبكة Zigbee بطوبولوجيا مختلطة (Mesh) الشكل(4-2)

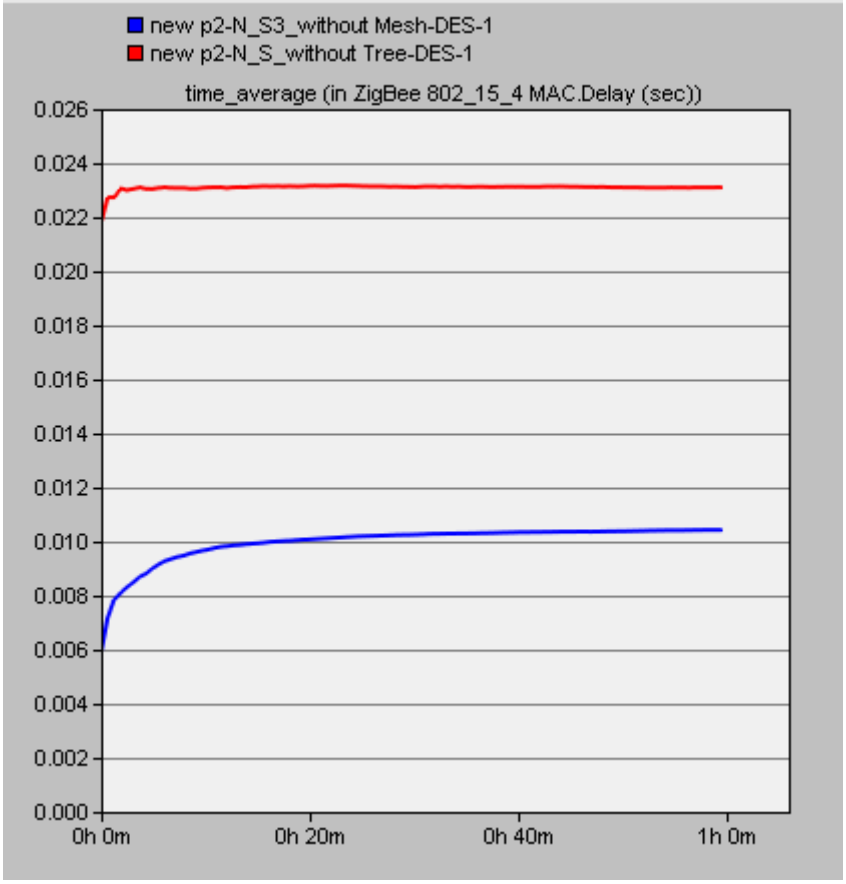


الشكل(4-2)شبكة Zigbee بطوبولوجيا مختلطة

يوضح الشكل(4-2) شبكة Zigbee بطوبولوجيا مختلطة (Mesh) مكونة من خمسة عشر عقد، وهي عبارة عن منسق واحد، وموجهين، واثنتا عشرة عقدة نهاية.

3. بعد ان قارنا الطوبولوجيات الشجرية (Tree)، والمختلطة (Mesh) بالوضع الطبيعي للشبكة، أي بدون وجود هجوم عليها بالنسبة للمقاييس : التأخير، الحمل، والانتاجية، وقمنا بتحليل النتائج بعد زمن محاكاة للشبكة لمدة ساعة واحدة وتم تسجيل النتائج التالية:

أولا": مقارنة الشبكة ذات طوبولوجيا مختلطة مع الشبكة ذات الطوبولوجيا الشجرية بدون وجود هجوم بالنسبة **للتأخير** الشكل (4-3).

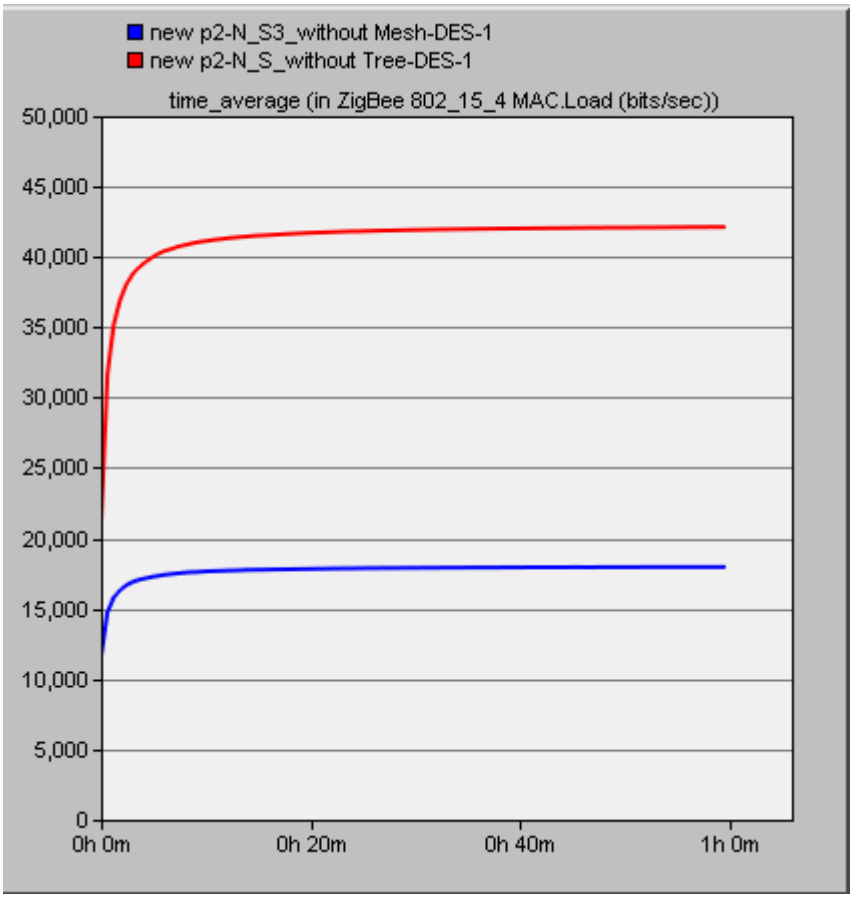


الشكل (4-3) مقارنة الشبكة ذات طوبولوجيا مختلطة مع الشبكة ذات الطوبولوجيا الشجرية بدون وجود هجوم بالنسبة للتأخير

يوضح الشكل (4-3) مقارنة الشبكة ذات طوبولوجيا مختلطة مع الشبكة ذات الطوبولوجيا الشجرية بدون وجود هجوم بالنسبة للتأخير، نلاحظ أن متوسط التأخير في الطوبولوجيا الشجرية هو حوالي (sec) 0.023 أما متوسط التأخير في الطوبولوجيا المختلطة (Mesh) هو حوالي (sec) 0.009 .

إن التأخير في الطوبولوجيا الشجرية (Tree) هو الأعلى مقارنة" بالطوبولوجيا المختلطة، ويرجع ذلك لوجود عدة مستويات، بالتالي المسار أطول، حيث تأخذ الرسالة وقتا" أطول للوصول الى الهدف. اما في الطوبولوجيا المختلطة (Mesh) توجد عدة طرق بديلة والرسالة تحتاج وقت أقصر للوصول الى الهدف .

ثانيا": مقارنة الشبكة ذات طوبولوجيا مختلطة مع الشبكة ذات الطوبولوجيا الشجرية بدون وجود هجوم بالنسبة **للحمل** الشكل (4-4).

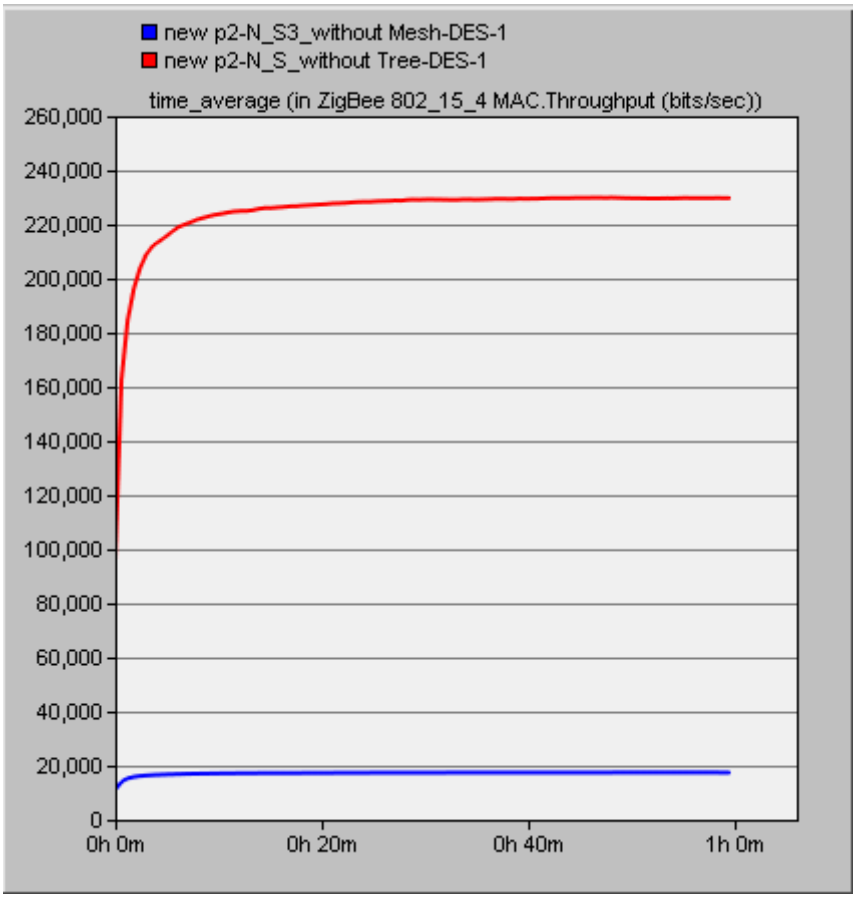


الشكل (4-4) مقارنة الشبكة ذات طوبولوجيا مختلطة مع الشبكة ذات الطوبولوجيا الشجرية بدون وجود هجوم بالنسبة للحمل

يوضح الشكل (4-4) مقارنة الشبكة ذات طوبولوجيا مختلطة مع الشبكة ذات الطوبولوجيا الشجرية بدون وجود هجوم بالنسبة للحمل، نلاحظ أن متوسط الحمل على الطوبولوجيا الشجرية هو حوالي (bits/sec) 41238 أما متوسط الحمل على الطوبولوجيا المختلطة (Mesh) هو حوالي (bits/sec) 17693 .

ويعود ذلك إلى أن الطرق والمسارات في الطوبولوجيا الشجرية (Tree)، أطول. أما الحمل في الطوبولوجيا المختلطة (Mesh) كان أقل من الطوبولوجيا الشجرية (Tree)، حيث أن الرسالة يمكنها سلوك أي طريق متاح للوصول الى الهدف دون اللجوء الى المنسق أو الموجه، حيث يمكن لأي عقدتين نهائيتين التواصل مباشرة" دون وجود المنسق والموجه فيما بينهما وهذا يقلل الحمل على الشبكة.

ثالثا": مقارنة الشبكة ذات طوبولوجيا مختلطة مع الشبكة ذات الطوبولوجيا الشجرية بدون وجود هجوم بالنسبة **للإنتاجية** الشكل (4-5).



الشكل (4-5) مقارنة الشبكة ذات طوبولوجيا مختلطة مع الشبكة ذات الطوبولوجيا الشجرية بدون وجود هجوم بالنسبة للإنتاجية

يوضح الشكل (4-5) مقارنة الشبكة ذات طوبولوجيا مختلطة مع الشبكة ذات الطوبولوجيا الشجرية بدون وجود هجوم بالنسبة للإنتاجية، نلاحظ أن متوسط الإنتاجية في الطوبولوجيا الشجرية هي حوالي (bits/sec) 224410 أما متوسط الإنتاجية في الطوبولوجيا المختلطة (Mesh) هي حوالي (bits/sec) 17206

ويرجع ذلك الى ان المسار أطول في الطوبولوجيا الشجرية (Tree)، اذ يتم التواصل من المنسق الى الموجهات وصولا" الى العقد النهائية، وهذا يتيح ارسال رسائل عبر الشبكة وبالتالي تحقيق انتاجية أفضل.

لوحظ في هذه المرحلة أن الطوبولوجيا الشجرية تفوقت على الطوبولوجيا المختلطة تأخيرا"، حملا"، وإنتاجية"، بدون وجود أي هجوم على كلتا الطوبولوجيتين: الشجرية (Tree)، و مختلطة (Mesh).

2-المرحلة الثانية:

لاحظنا من المرحلة السابقة أن الطوبولوجيا الشجرية فاقت الطوبولوجيا المختلطة تأخيرا"، حملا"، وإنتاجية"، ولكن كان ذلك بدون وجود أي هجوم على شبكة Zigbee في كلا الطوبولوجيتين: الشجرية (Tree)، و المختلطة (Mesh).

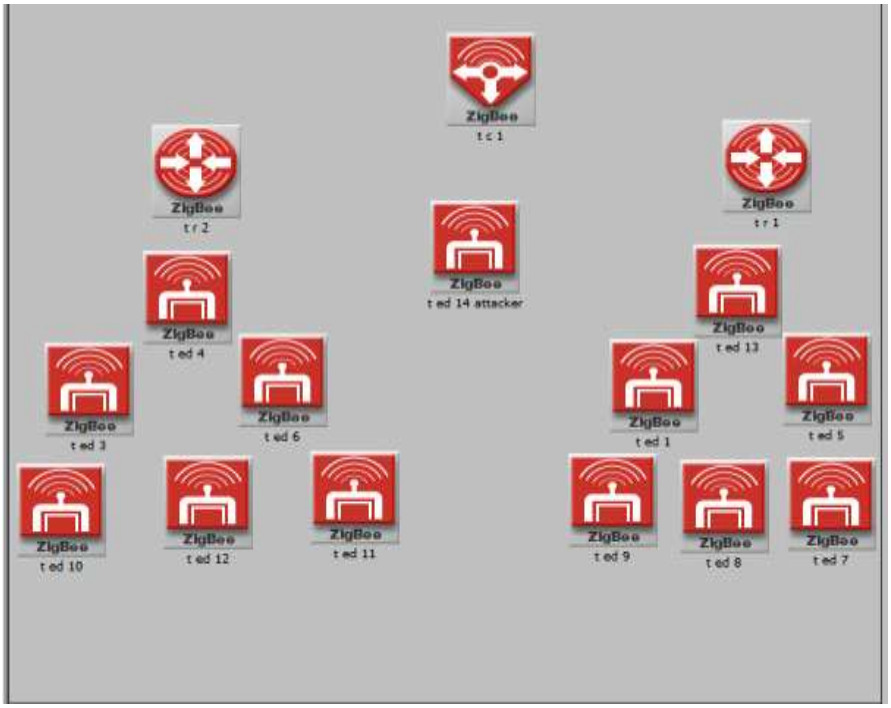
لكن ماذا ستكون نتائج المقارنة في حال تم الهجوم على الطوبولوجيتين: الشجرية (Tree)، و المختلطة (Mesh)؟

للإجابة على هذا التساؤل قمنا في هذه المرحلة بنمذجة هجوم حرمان من الخدمة وفيه يستهدف المهاجم شبكة Zigbee ذات طوبولوجيا الشجرية (Tree) الشكل (4-6) ومقارنتها مع هجوم حرمان من الخدمة وفيه يستهدف المهاجم شبكة Zigbee ذات طوبولوجيا مختلطة (Mesh) الشكل(4-7).

تجدر الإشارة إلى أن أهم الصعوبات والتحديات التي واجهتنا واستوقفتنا خلال المرحلة العملية ودراسة هجوم الحرمان من الخدمة على شبكات Zigbee هي مرحلة نمذجة هجوم الحرمان من الخدمة على هذه الشبكات في برنامج المحاكاة OPNET الذي يقدم امكانية نمذجة شبكة الZigbee بشكل سهل ويسير، ولكنه لا يقدم امكانية نمذجة هجوم عليها ، فكان من الصعب جدا" اختراع نموذج هجوم على هذه الشبكات يحاكي هجوم الحرمان من الخدمة الحقيقي على هذه الشبكات في الواقع، حيث أن الدراسات المرجعية لم تقدم ولم توضح كيفية نمذجة عقدة مهاجم تستهدف شبكات Zigbee في برنامج المحاكاة OPNET، فكان علينا ان نقوم بإيجاد نموذج لهجوم الحرمان من الخدمة على شبكة Zigbee وأن نبدأ من الصفر نظرا" لعدم توفر ابحاث ودراسات مرجعية تساعدنا في معرفة كيفية نمذجة مثل هذا الهجوم في برنامج المحاكاة OPNET.

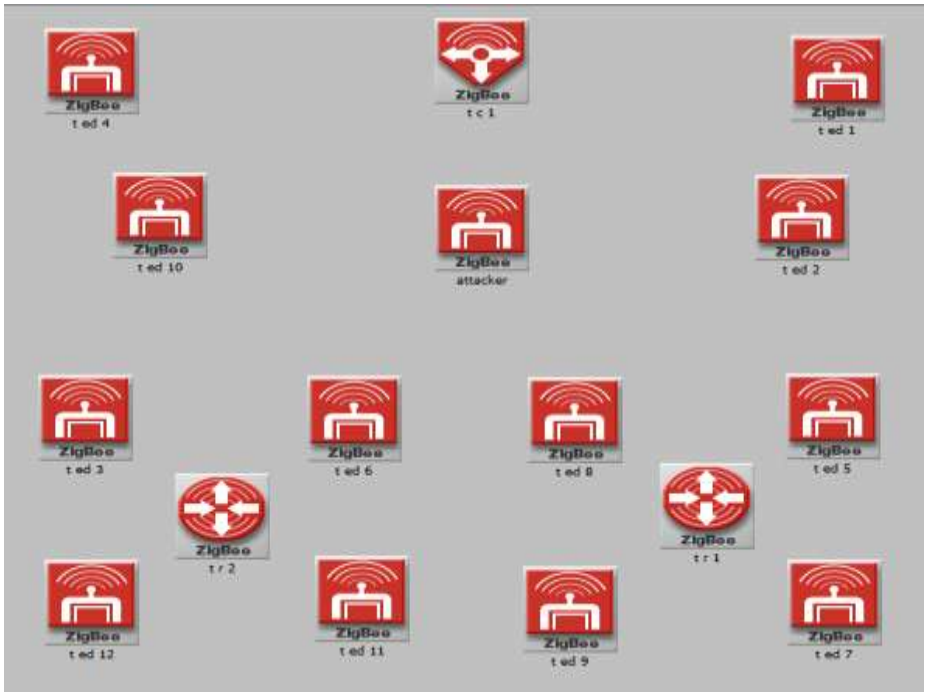
بعد البحث والتجربة توصلنا إلى طريقة تمكننا من نمذجة هجوم الحرمان من الخدمة على شبكات الـ Zigbee في برنامج المحاكاة OPNET.

وكان التحدي تجربة هذا المهاجم الذي قمنا بنمذجته بجعله يستهدف أجهزة الشبكة المختلفة وتشغيل الشبكة بوجود المهاجم ومراقبة تأثيراته والتأكد أنه قد شكل خطراً حقيقياً على اداء الشبكة المدروسة، وإن هذا الخطر يصنف كحرمان من الخدمة.



الشكل(4-6) عقدة مهاجم تستهدف شبكة Zigbee ذات طوبولوجيا شجرية (Tree)

يوضح الشكل (4-6) هجوم الحرمان من الخدمة على شبكات الـ Zigbee ذات طوبولوجيا شجرية (Tree) وفيه يستهدف المهاجم منسقها.



الشكل (4-7)مهاجم يستهدف منسق شبكة Zigbee ذات طوبولوجيا مختلطة (Mesh)

يوضح الشكل (4-7) شبكة Zigbee ذات طوبولوجيا مختلطة (Mesh) تحوي على خمسة عشرة عقدة، ومهاجم يستهدف منسقها.

2-1-السيناريو الثاني:

قمنا بنمذجة هجوم حرمان من الخدمة وفيه يستهدف المهاجم المنسق في شبكة Zigbee ذات الشجرية (Tree)، و طوبولوجيا مختلطة (Mesh) وتمت دراسة وتحليل تأثيراته من خلال مقارنة تأثيره على الطوبولوجيتين من خلال المعايير: التأخير والحمل والإنتاجية حسب معطيات الجدول (4-2).

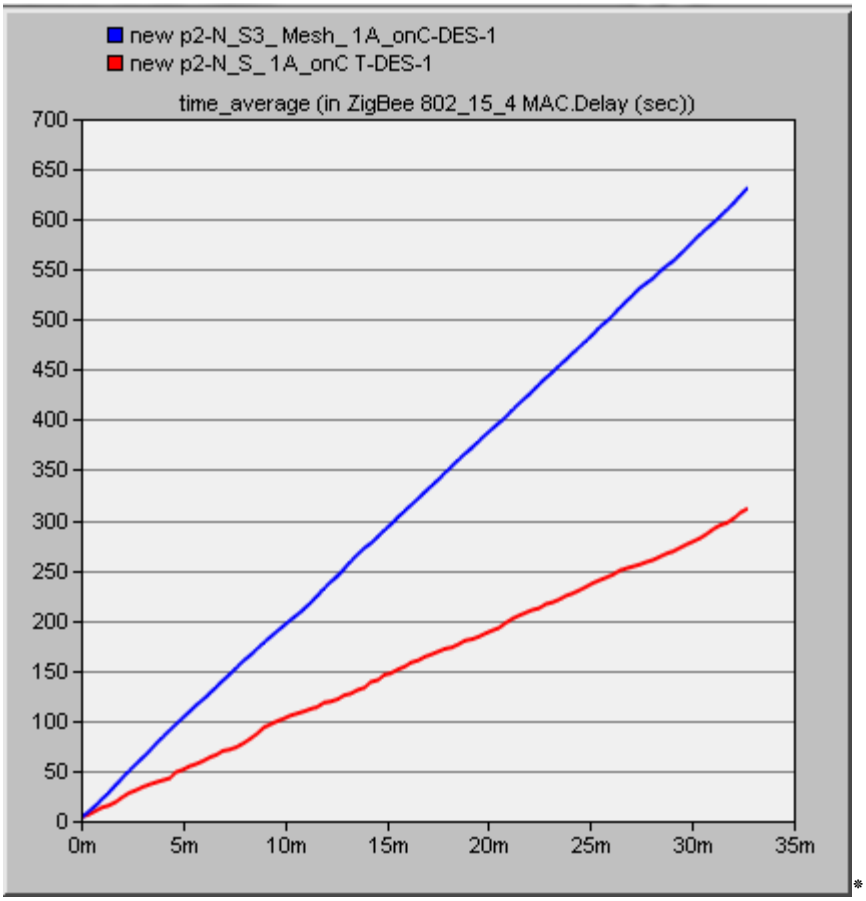
الجدول(4-2) صفات شبكات Zigbee ذات طوبولوجيا شجرية (Tree)، طوبولوجيا مختلطة (Mesh) والمهاجم الذي يستهدفها

الطوبولوجيا	عدد العقد	عدد المهاجمين	أنواع الأجهزة	المقارنة	الاجهزة المستهدفة	زمن المحاكاة	صفات المهاجم
Tree	15	واحد	منسق واحد، موجهين، واثنتا عشرة عقد نهاية	Tree مع Mesh	المنسق	33 دقيقة*	**Interval Time=1 ms** Packet size=10 KByte
Mesh	15	واحد	منسق واحد، موجهين، واثنتا عشرة عقد نهاية	Tree مع Mesh	المنسق	33 دقيقة*	**Interval Time=1 ms** Packet size=10 KByte

قمنا بتجريب فواصل زمنية أكبر وأصغر من الفاصل الطبيعي، وتبين ان تأثير الهجوم من حيث الاضرار بالشبكة يكون أوضح عند 1 ms، واعتمدنا حجم الحزمة 1 Kbyte في حالة الهجوم وتمت مقارنته مع حجم الرزمة الطبيعي في حالة عدم وجود هجوم.

أولا": تأثير هجوم الحرمان من الخدمة : وفيه يستهدف المهاجم المنسق على شبكة الـ Zigbee ذات طوبولوجيا شجرية مقارنة مع مهاجم يستهدف المنسق على شبكة الـ Zigbee ذات طوبولوجيا مختلطة بالنسبة **للتأخير** الشكل(4-8)

*** قمنا بمحاكاة للشبكة لمدة 33 دقيقة في حالة الهجوم بدلا" من ساعة وذلك لأننا لاحظنا ان الشبكة تنهار بعد الدقيقة 34 من بداية المحاكاة بسبب ضغط المهاجم الكبير عليها.**

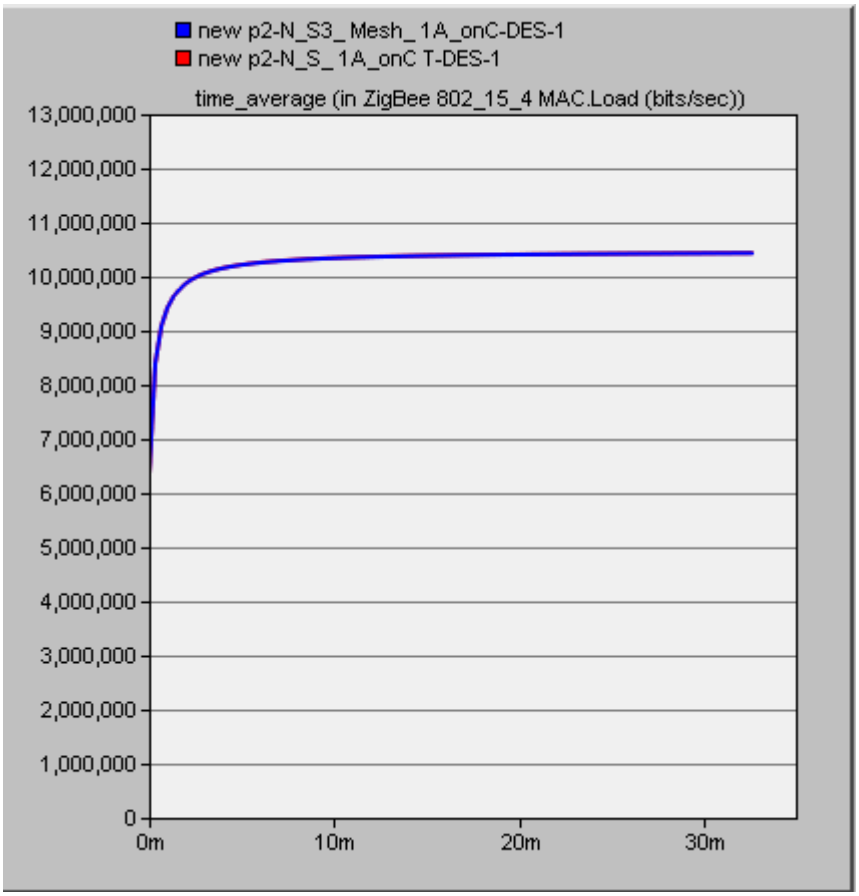


الشكل(4-8) يستهدف المهاجم المنسق في شبكة الـ Zigbee ذات طوبولوجيا شجرية مقارنة مع مهاجم يستهدف المنسق في شبكة الـ Zigbee ذات طوبولوجيا مختلطة بالنسبة للتأخير

يوضح الشكل(4-8) أن متوسط التأخير **ارتفع** في الطوبولوجيا المختلطة حيث أصبح لدينا 318.1 sec في حين أنه كان 156.4 sec في الطوبولوجيا الشجرية بعد الهجوم على المنسق بفاصل زمني 0.001 sec، أي أنه ارتفع تقريبا الضعف في الطوبولوجيا المختلطة عن الطوبولوجيا الشجرية، ووصل التأخير بعد الهجوم على المنسق إلى قيمة أقصاها 630.8 sec بعد زمن محاكاة نصف ساعة.

إن التأخير في الطوبولوجيا الشجرية (Tree) هو الأعلى مقارنة" بالطوبولوجيا المختلطة في الوضع الطبيعي بدون وجود هجوم، ولكن الأمر اختلف في حالة الهجوم، حيث أن الرسائل في الطوبولوجيا الشجرية تصل اسرع منها في الطوبولوجيا المختلطة في حالة الهجوم، لأنه في الطوبولوجيا المختلطة لا يوجد مسار محدد للرسائل التي يبثها المهاجم في الشبكة وهذا ما يجعل الرسائل تستغرق وقتا" أطول للوصول الى هدفها.

ثانيا": تأثير هجوم الحرمان من الخدمة: وفيه يستهدف المهاجم المنسق على شبكة الـ Zigbee ذات طوبولوجيا شجرية مقارنة مع مهاجم يستهدف المنسق على شبكة الـ Zigbee ذات طوبولوجيا مختلطة (Mesh) بالنسبة **للحمل** الشكل(4-9).

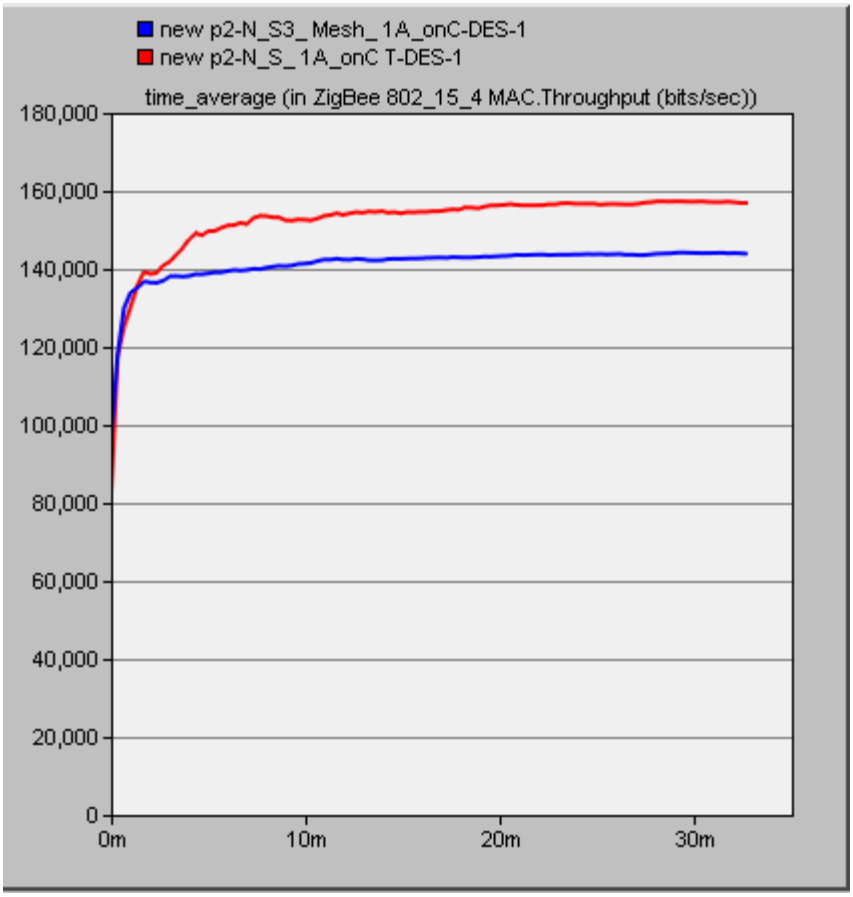


الشكل(4-9)يستهدف المهاجم المنسق في شبكة الـ Zigbee ذات طوبولوجيا شجرية مقارنة مع مهاجم يستهدف المنسق في شبكة الـ Zigbee ذات طوبولوجيا مختلطة بالنسبة للحمل

يوضح الشكل(4-9) أن متوسط الحمل انخفض بشكل طفيف جدا" في الطوبولوجيا المختلطة من bits/sec 10430679 عن bits/sec 10436779 في الطوبولوجيا الشجرية بعد الهجوم على المنسق بفاصل زمني 0.001 sec، ووصل الحمل بعد الهجوم على المنسق إلى قيمة أقصاها bits/sec 10485781 بعد زمن محاكاة نصف ساعة.

يكون الحمل في حالة الهجوم متطابق تقريبا" وذلك لأن عدد العقد في الطوبولوجيتين هو نفسه فعندما يقوم المهاجم بالهجوم يؤدي الى تأثير متشابه بالحمل على الطوبولوجيتين لأن عدد وحجم وتواتر الرسائل التي يبثها بالشبكة متشابهة فيكون الازدحام (traffic) نفسه في كلا الطوبولوجيتين.

ثالثا": تأثير هجوم الحرمان من الخدمة: وفيه يستهدف المهاجم المنسق على شبكة الـ Zigbee ذات طوبولوجيا شجرية مقارنة مع مهاجم يستهدف المنسق على شبكة الـ Zigbee ذات طوبولوجيا مختلطة بالنسبة **للإنتاجية** الشكل(4-10).



الشكل(4-10) يستهدف المهاجم المنسق في شبكة الـ Zigbee ذات طوبولوجيا شجرية مقارنة مع مهاجم يستهدف المنسق في شبكة الـ Zigbee ذات طوبولوجيا مختلطة بالنسبة للإنتاجية

يوضح الشكل(4-10) أن متوسط الإنتاجية **انخفض** في الطوبولوجيا الشجرية من 152170 bits/sec إلى 141218 bits/sec في الطوبولوجيا المختلطة بعد الهجوم على المنسق بفاصل زمني 0.001 sec، ووصلت الإنتاجية بعد الهجوم على المنسق إلى قيمة أقصاها 143318 bits/sec بعد زمن محاكاة نصف ساعة.

لوحظ أن الإنتاجية في الطوبولوجيا الشجرية أعلى ويرجع ذلك إلى بنيتها و وجود عدة مستويات فيها، حيث يتم التواصل من المنسق الى الموجهات وصولا" إلى العقد النهائية، فعدد الرسائل المرسلة بالشبكة أكبر وبالتالي تحقق إنتاجية أفضل.

الجدول(4-3) نتائج مقارنة الهجوم على الطوبولوجيا الشجرية بالهجوم على الطوبولوجيا المختلطة

	متوسط التأخير (sec)	متوسط الحمل (bits/sec)	متوسط الانتاجية (bits/sec)
المختلطة (Mesh)	318.1	10430679	141218
الشجرية (Tree)	156.4	10436779	152170

الاستنتاجات و التوصيات:

تناولنا في هذا البحث أثر هجمات الحرمان من الخدمة (DoS) على شبكات الـ ZigBee ذات الطوبولوجيا الشجرية (Tree) بالمقارنة مع الطوبولوجيا المختلطة (Mesh) وحللنا النتائج من خلال المعايير: التأخير، والحمل، والإنتاجية، ولاحظنا أن تأثير هجوم الحرمان من الخدمة (DoS) يختلف من شبكة لأخرى ومن طوبولوجيا لأخرى وتتعدد أشكال هذا الهجوم واضراره.

حيث أظهرت النتائج التي حصلنا عليها أن هجوم الحرمان من الخدمة (DoS) يكون أخطر عندما يستهدف المهاجم شبكة ZigBee ذات الطوبولوجيا المختلطة (Mesh) بالمقارنة مع استهداف نفس المهاجم لشبكة ZigBee ذات الطوبولوجيا الشجرية (Tree)، حيث أن التأخير في الطوبولوجيا المختلطة (Mesh) كان أكبر من التأخير في الطوبولوجيا الشجرية (Tree) بشكل ملحوظ، ولم يقتصر الامر على التأخير الذي ارتفع بشكل واضح، بل إن إنتاجية الشبكة تأثرت أيضا" وانحدرت، حيث لاحظنا ان الإنتاجية في الطوبولوجيا المختلطة (Mesh) انخفضت عن الإنتاجية في الطوبولوجيا الشجرية (Tree) بشكل كبير وهذا ما أكدته المخططات والرسوم البيانية التي حصلنا عليها بعد نمذجة الطوبولوجيات والهجوم عليها.

من الممكن تطوير الدراسة السابقة من خلال:

1) زيادة عدد العقد في الشبكة المدروسة.
2) دراسة تأثير هجمات الحرمان من الخدمة على أنواع أخرى من الطوبولوجيات.
3) إيجاد حلول مناسبة لتفادي هجمات الحرمان من الخدمة (DoS) أو التخفيف من أضرارها.

المراجع:

[1] Ankur Tomar. *Introduction to Zigbee Technology* . Global Technology Center,2011.

[2] Meng-Shiuan Pan ;Yu-Chee Tseng. *ZigBee Wireless Sensor Networks and Their Applications*. National Chiao Tung University, 2008.

[3] G. Shi; K. Li.*Fundamentals of ZigBee and Wi-F.i.* Springer International Publishing,2017.

[4] Sunil Ghildiyal; Amit Kumar Mishra; Ashish Gupta;Neha Garg. *ANALYSIS OF DENIAL OF SERVICE (DOS) ATTACKS IN WIRELESS SENSOR NETWORKS*. IJRET: International Journal of Research in Engineering and Technology ,2014.

[5] Vasil Hnatyshin. *OPNET Modeler simulations of performance for multi nodes wireless systems*. Rowan University ,2016.

[6] Doddapaneni.krishna Chaitanya; Ghosh.Arindam. *Analysis of Denial-of-Service attacks on Wireless Sensor Networks Using Simulation.* Middlesex University, 2010.

[7] Sanchari Saha. *ZIGBEE OPNET Modeler: An Efficient Performance Analyzer for Wireless Sensor Networks*. International Journal of Engineering Sciences & Research Technology, 2013.

[8] Nischay Bahl ; Ajay K. Sharma; Harsh K. Verma.*On Denial of Service Attacks for Wireless Sensor Networks*. International Journal of Computer Applications (0975 – 8887) Volume 43– No.6, April 2012.

[9] Radosveta Sokullu; Ilker Korkmaz; Orhan Dagdeviren. *GTS Attack: An IEEE 802.15.4 MAC Layer Attack in Wireless Sensor Networks. International Journal On* Advances in Internet Technology, vol 2 no 1, 2009.