نمذجة و تحليل أداء شبكات برتوكول MODBUS التسلسلي

طالب الدكتوراه: رضوان صبحي المحمد

كلية الهمك – جامعة البعث

اشراف الدكتور: مسعود الأتاسي

الملخص:

تعتبر الشبكات الصناعيّة التي تستخدم برتوكول MODBUS من أكثر الأنواع انتشاراً و ذلك نتيجة المزايا التي يدعمها هذا البرتوكول و التي تلبي متطلبات الأتمتة الصناعيّة، و ظهرت العديد من اصدارات برتوكول MODBUS لتلبي التطور المُتسارع في منظومات الشبكات الصناعيّة.

لدراسة سلوك برتوكول MODBUS و تحليل أداء الشبكات الصناعية التي يعمل عليها لا بدّ من وضع نماذج تحاكي سلوك البرتوكول و تدعم إجراء عمليات الاختبار و التحليل بحيث تتيح دراسة العوامل المؤثرة في بارامترات الأداء و التنبؤ بسلوك الشبكة المستقبلي في حال الرغبة بتطوير الشبكة الصناعيّة التي يعمل عليها.

في هذا البحث تمّ وضع نموذج لشبكة صناعيّة تستخدم برتوكول MODBUS التسلسلي باستخدام محاكي الشبكات OPNET، و بعد نمذجة جميع الاعتبارات التي يدعمها هذا البرتوكول تمت دراسة مجموعة من بارامترات الأداء مثل (زمن الاستجابة، و تأخير الانتقال للرسائل، و استخداميّة الشبكة) بهدف تحديد أفضل أداء لعمل الشبكة و تحقيق مُتطلبات الزمن الحقيقي.

الكلمات المفتاحية: برتوكول MODBUS ، تحليل أداء الشبكات الصناعية، العوامل المؤثرة في أداء الشبكات، تحليل الأداء باستخدام OPNET.

Modeling And Analysis the Performance of Serial MODBUS Network

Abstract:

Industrial networks that use the MODBUS protocol are considered one of the most common types, because of the advantages supported by this protocol and that meet the requirements of industrial automation, and many versions of the MODBUS protocol have appeared to meet the rapid development in the industrial network system.

To study the behavior of the MODBUS protocol and analyze the performance of the industrial networks on which it operates, it is necessary to develop models that simulate the protocol and support the conduct of analyzes so as to allow studying the factors affecting performance parameters and predicting the future behavior of the network in the event that it is desired to develop the industrial network on which it operates.

In this research, an industrial network using MODBUS protocol was modeled using the OPNET network simulator, and all considerations supported by this protocol were modeled, and then a set of performance parameters such as (response time, delay end to end, utilization) were studied. In order to determine the best performance of the network and achieve the requirements of real time.

The Key words: MODBUS protocol, industrial network performance, performance analysis using OPNET.

1- المقدمة:

يُعتبر برتوكول MODBUS التسلسلي برتوكول اتصال رقمي ثنائي الاتجاه يدير الارسال بين الأجهزة الصناعيّة الذكيّة، ويُعد شبكة محلية مخصّصة للأتمتة المعامل.[1] في شبكات MODBUS ذات الارسال ثنائي الاتجاه من الممكن قراءة البيانات من و إلى الحساسات و المشغلات، و ينتج عن هذا النوع من الاتصال ثنائي الاتجاه للناقل توفيراً كبيراً بعدد الكابلات المُستخدم و بتالي خفض تكاليف الإنتاج، و يجب أن يحتوي كل جهاز يُراد ربطه بالناقل على واجهة للاتصال يتم من خلالها ضبط إعدادات الاتصال بالناقل.[1]

إنّ أداء شبكات MODBUS يتأثر بمجموعة من البارامترات المختلفة لذا لا بدّ من وضع نماذج تحاكي سلوك البرتوكول باستخدام أحد برامج المحاكاة الشبكيّة لدراسة و تحليل العوامل المؤثرة فيها.[2]

يدعم محاكي الشبكات OPNET نمذجة سلوك برتوكولات الاتصال ويتيح توفير بيئة مفتوحة المصدر لنمذجة كافة الاعتبارات التي يدعمها أي نوع من برتوكولات الاتصال، و تمّ الاستفادة من هذه المزايا لنمذجة شبكة صناعية تستخدم ناقل MODBUS التسلسلي و تحليل بارامترات مؤثرة في الأداء لمعرفة سلوك الشبكة المستقبلي بهدف تحسينها و المحافظة على موثوقيتها.[3]

2- مشكلة البحث:

- ❖ صعوبة إجراء عمليات التنبؤ و الاختبار على شبكة صناعيّة واقعيّة.
- ❖ الصعوبة في توسعة و تطوير الشبكة دون التأثير على الأداء العام لها.
- ❖ عدم القدرة على تحديد أهم العوامل المؤثرة في أداء الشبكات الصناعيّة أثناء عملها.
- ❖ مشكلة مادية كبيرة عند عدم تلبية الشبكة لمتطلبات العمل في الأداء المطلوب.

3- هدف البحث:

إنّ الهدف الرئيسي هو بناء نموذج يحاكي سلوك شبكة صناعية تعمل على برتوكول MODBUS التسلسلي آخذين بعين الاعتبار جميع الخصائص التي يدعمها و من ثم إجراء عمليات التحليل و الاختبار بهدف:

- ✓ تحديد أهم العوامل المؤثرة في بارامترات الأداء.
- ✓ المقارنة بين بارامترات الأداء عند كل سيناريو اختباري لتحديد القيم الأفضل.
- ✓ إجراء عمليات التطوير على النموذج قبل تنفيذها على الشبكة الواقعية.
- ✓ دراسة التكلفة المادية و متطلبات التوسعة للشبكة من خلال النموذج المُصمّم.
- ✓ القدرة على التنبّؤ بسلوك الشبكة المستقبلي عند إضافة معدات جديدة على الشبكة.

4- الدراسات المرجعيّة:

اهتم العديد من الباحثين حول العالم بمجال نمذجة الشبكات الصناعيّة و تحليل أدائها و بالأخص التي تستخدم برتوكول MODBUS نظراً لانتشاره الواسع و سنذكر بعض الأبحاث التي تمّ الوقوف عندها و النظر في نتائجها:

- اقترح الباحثان Yao Yuanyuan, Chen Meng خوارزمية محسّنة لطول إطار الاتصال التكيفي استناداً على بروتوكول Modbus لتعديل طول الإطار بهدف تحديد حجم الإطار الأفضل للإرسال وفقاً لمتوسط معدل خطأ الإطار في الفترة الزمنيّة، و تمّ استخدام طريقة "تقليل سريع ، زيادة بطيئة" لضبط طول إطار البيانات عند مستويات مختلفة من FER (Frame Error Rate) معدل خطأ الإطار، لا تعمل هذه الخوارزمية على تحسين معدل الإرسال فحسب بل أيضاً على تحسين استقرار الاتصال و بتالي الأداء.[4]

- الورقة البحثيّة [5] درست العديد من المعايير لتقييم أداء أجهزة الشبكات من نوع Modbus، وتتضمّن: 1) وقت الاستجابة لطلبات Modbus، 2) الحد الأقصى لعدد الطلبات التي يمكن التعامل معها بنجاح بواسطة أجهزة Modbus في فترة زمنيّة

مُحدّدة، و3) مراقبة أجهزة Modbus عند تعرضها لهجوم رفض مُوزّع للخدمة (Distributed Denial of Service)، و تمّ استخدام دارتين الكترونيتين ذات تكلفة منخفضة و هي (ESP8266 و OpenPLC / Raspberry Pi) لتقييم أداء برتوكول Modbus.

– الهدف من المقال [6] هو تقييم أداء ناقل صناعي وآليات تنفيذ دورة الرسائل حيث قدّم نموذجاً يستند على شبكة بتري الملونة لإجرائيات الإرسال و تنفيذ دورة الرسائل (MAC)(Medium Access Control) لطبقة ربط المعطيات للبرتوكولات Fieldbus، وأكدت النتائج على الحاجة لتحديد بارامتر زمن التشغيل وهو معكوس معدل الإرسال (transmission rate)بشكل مناسب من أجل ضمان الأداء الأمثل لشبكة Fieldbus.

– قام الباحثان Beata Krupanek and Ryszard Bogacz بإجراء بحث [7] باستخدام المحاكي OPNET لدراسة أداء الأنظمة اللاسلكية متعددة العقد، وتمَ من خلال هذا البحث نمذجة شبكة مؤلفة من عدة عقد لاسلكية باستخدام برنامج OPNET و دراسة جودة الخدمة و الأداء للشبكة من حيث تلبيتها لمُحدّدات الزمن الحقيقي و دراسة التأخيرات في عملية نقل البيانات.

– في الدراسة المرجعيّة [8] قدّم الباحثون تحليلاً لأداء بروتوكول الاتصال Modbus الذي يتم تنفيذه باستخدام محاكي الشبكات (NS–3)، و يُركّز البحث على تقييم الأداء من خلال زمن الاستجابة مرتبطاً بعدد العقد والطوبولوجيا، و أظهرت النتائج أن طول الحزمة ليس له تأثيراً كبيراً على وقت الاستجابة في كلا النوعي للطوبولوجيا (الناقل و النجمي) و بتالي ليس له أثراً كبيراً على الأداء.

– في البحث [9] ناقش الباحثون أداة لتحليل وقت الاستجابة والجدولة لاتصالات برتوكول Modbus عبر ناقل RS–485، حيث يتم جمع أزمنة استجابة مجموعة الرسائل بواسطة جهاز Modbus مُتخصّص ثم إرسالها إلى البرنامج حيث يتم التحليل، ثم يتم نشر تطبيق Modbus عبر شبكة RS–485 بشكل يتناسب مع الأداء.

– قدم الباحثون Jia Hao, Jiechang Wu, Chaoyou Guo بحثاً [10] تمّ من خلاله نمذجة و تحليل أداء برتوكول CAN ، حيث تم بالبداية نمذجة الناقل بشكل هرمي انطلاقاً من نموذج الشبكة و من ثم نموذج العقدة و من ثم نموذج العمليّة مع الأخذ بعين

الاعتبار كلاً من وظائف معالجة الأخطاء و تحسس حالة القناة و أولويّة العقد لتفادي التصادم، و بعد الانتهاء من بناء النموذج تمّ دراسة بعض العوامل المؤثرة في الأداء مثل أولوية العقدة و حجم الإطار و الأزمنة الفاصلة بين عمليات الإرسال.

– تمّ في البحث [11] دراسة بعض العوامل المؤثرة في تصميم الشبكات الصناعية Fieldbus من خلال المحاكاة باستخدام برنامج Opnet و أثر هذه العوامل عل أداء الشبكات، و تم اختيار ثلاث عوامل وهي معدل الإرسال (إما 2.5Mbps أو 1.5Mbps) و طبولوجيا الشبكة (إما حلقي أو نجمي) و نوع مجمّع الشبكة المركزي (إما hub أو switch) مما يقود إلى اختبار ثمانية سيناريوهات (2^3) في المحاكي OPNET، و تم في كل سيناريو تشغيلي حساب مجموع عدد الرزم المرسلة بالمقارنة مع عدد الرزم المستقبلة و تقسيم المجموعين للحصول على نسب تعكس أداء كل حالة اختبار.

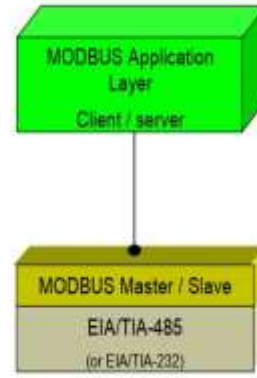
– قام الباحث العراقي قتيبة علي بنشر مقال [12] لدراسة و تحليل أداء شبكات إثرنيت الصناعية باستخدام برنامج المحاكاة أوبنيت ، ففي البداية تمّ التأكد من قابلية برنامج أوبنيت في نمذجة الشبكات الصناعيّة من خلال مقارنة نتائج تجارب شبكة عمليّة مع نتائج المحاكاة و من ثمّ تم دراسة تأثير عدد من العوامل على الأداء مثل طول الحزمة و عدد العقد و معدل إنتاجية العقد و حمل FTP مُوجه لعقدة محددة، وأظهرت النتائج أنه يمكن استخدام برنامج OPNET بكفاءة لمحاكاة الشبكات الصناعيّة.

5– برتوكول MODBUS التسلسلي:

هو بروتوكول Fieldbus ذو نظام ارسال (Master/Slave)، فالعقدة "الرئيسية" تُصدر أوامر صريحة إلى إحدى العقد "التابعة" وتقوم بمعالجة الاستجابات، ولا تقوم العقد التابعة عادةً بنقل البيانات دون طلب من العقدة الرئيسيّة، ولا تتواصل مع العقد التابعة الأخرى إلا عن طريقها.[2]

يُعطي الشكل (1) تمثيلاً عاماً لطبقات برتوكول MODBUS مقارنة بالطبقات السبع لنموذج (OSI) حيث يُلاحظ وجود ثلاث طبقات و هي (الطبقة الفيزيائية و طبقة ربط المعطيات و طبقة التطبيق).[2]

Layer	ISO/OSI Model	
7	Application	MODBUS Application Protocol
6	Presentation	Empty
5	Session	Empty
4	Transport	Empty
3	Network	Empty
2	Data Link	MODBUS Serial Line Protocol
1	Physical	EIA/TIA-485 (or EIA/TIA-232)



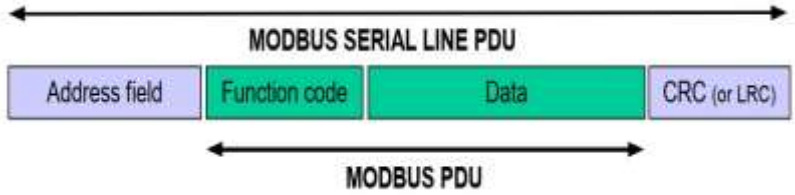
الشكل (1): طبقات برتوكول MODBUS مقارنة بطبقات (OSI).

5-1 إطار برتوكول MODBUS التسلسلي:

يُحدد بروتوكول MODBUS وحدة بيانات بروتوكول بسيطة (PDU) مستقلة عن طبقات الاتصال الأساسية، و تتألف من حقل البيانات و حقل الوظيفة كما يظهر في الشكل(2).

الشكل (2): وحدة البيانات في برتوكول MODBUS.

يقوم بروتوكول MODBUS على الناقل بإضافة بعض الحقول على وحدة بيانات البروتوكول، ويُظهر الشكل (3) إطار MODBUS التسلسلي المُرسل من العقدة الرئيسيّة.



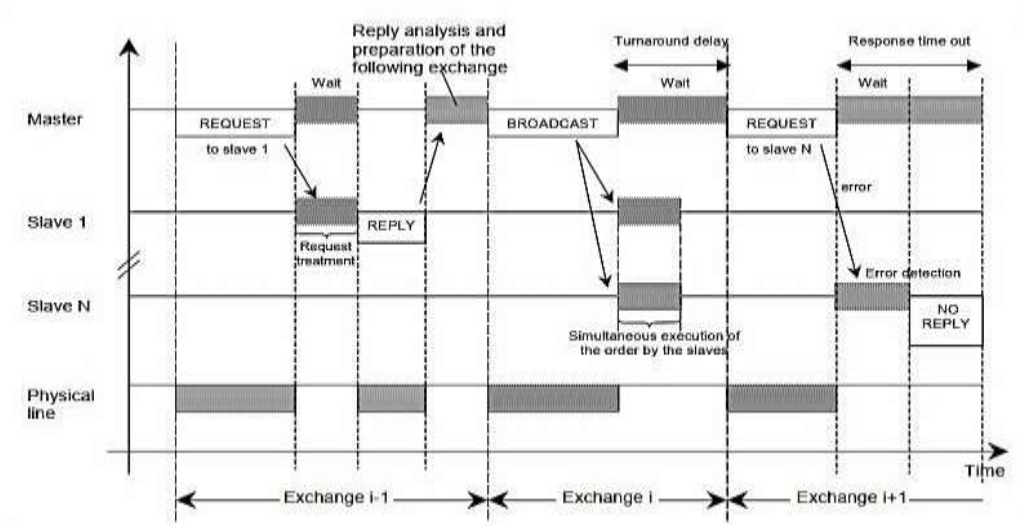
الشكل (3): إطار MODBUS التسلسلي.

يتألف مما يلي:

- حقل العنوان: يحتوي على عنوان الجهاز التابع فقط، و تقع عناوين العقد التابعة في نطاق العشري (247–0)، و يُخاطب الجهاز الرئيسي الجهاز التابع من خلال وضع عنوانه في حقل عنوان الرسالة، وعندما يُرجِع الجهاز التابع استجابته فإنه يُكرّر وضع عنوانه في حقل العنوان للاستجابة للسماح للجهاز الرئيسي معرفة وصول البيانات إلى عنوانها المطلوب و بشكل صحيح.
- حقل الوظيفة: يشير إلى رمز الوظيفة للجهاز التابع أي نوع الإجراء الذي يجب القيام به.
- حقل تدقيق الأخطاء: هو نتيجة حساب "التحقق من التكرار" الذي يتم إجراؤه على محتويات الرسالة، يتم استخدام نوعين من طرق الحساب اعتماداً على نمط الإرسال المستخدم (RTU أو ASCII).

2-5 المخطط الزمني لبرتوكول MODBUS التسلسلي:

يوضح الشكل (4) الرسم البياني الزمني لثلاثة سيناريوهات نموذجية لاتصالات (Master / Slave).[2]



الشكل (4): المخطط الزمني للإرسال (Master / Slave) لناقل MODBUS.

السيناريو الأول: يقوم فيه الجهاز الرئيسي "Master" بإرسال طلب "REQUEST" للعقدة التابعة "Salve1" و التي تستجيب برسال "REPLY" بعد فترة زمنية محددة "REQUEST TREATMENT" و يكون الناقل "Physical Line" خلال عملية ارسال كلاً من "REQUEST " و "REPLY " مشغولاً كما هو مُوضح بالشكل(4).

السيناريو الثاني: يقوم فيه الجهاز الرئيسي "Master" بإرسال طلب عام "BROADCAST" لجميع الأجهزة التابعة "Salves" و التي تستجيب فيها للطلب المُرسل دون إرسال رد و يكون الناقل"Physical Line " خلال عملية ارسال "BROADCAST" مشغولاً كما هو مُوضح بالشكل(4).

السيناريو الثالث: يقوم فيه الجهاز الرئيسي "Master" بإرسال طلب "REQUEST" للعقدة التابعة "Salve N" و يعاني هذا الطلب من حدوث خطأ تقوم العقدة التابعة باكتشافه "Error Detection" فلا تقوم بإرسال طلب إجابة و عندما يتجاوز تأخير الاستجابة مهلة زمنية "Response Time Out" يعود الجهاز الرئيسي"Master" بإعادة الارسال لنفس الطلب و يكون الناقل "Physical Line "مشغولاً خلال عملية ارسال الطلب"REQUEST" كما هو موضح بالشكل(4).

5-3 أنماط برتوكول MODBUS التسلسلي:

يوجد نمطين مختلفين لبرتوكول MODBUS التسلسلي هما : (RTU) و (ASCII) وهي تحدد محتويات بتات حقول الرسالة المرسلة بشكل تسلسلي على الناقل، و يُحدد كيفية تعبئة المعلومات في حقول الرسالة وفك تشفيرها.

يجب أن يكون وضع الإرسال هو نفسه لجميع الأجهزة على ناقل MODBUS التسلسلي، و يجب على المستخدمين إعداد الأجهزة على وضع الإرسال المرغوب (RTU) أو (ASCII)، علماً أنّ الوضع الافتراضي للأجهزة هو (RTU).

5-3-1 نمط الارسال (RTU):

عندما تتواصل الأجهزة على ناقل MODBUS التسلسلي باستخدام وضع (RTU)، فإن كل بايت (8) بت في الرسالة يحتوي على حرفين سداسي عشريين (hex) بطول (4) بت، و تسمح هذه الميزة أن تكون كثافة الأحرف أكبر ممّا يعني إخراج بيانات أفضل لنفس معدل النقل مقارنةً مع النمط (ASCII)، و يجب إرسال كل رسالة بسلسلة من الأحرف.[2]

- التنسيق (11) بت لكل بايت في وضع (RTU): بت التكافؤ (parity) بطول (1) بت، و يكون وضع التكافؤ الافتراضي (even)، و في حال عدم وضع بت تكافؤ سنقوم بوضع (2 bits) للتوقف، و يتم نقل الأحرف بالتسلسل، حيث يُرسل كل حرف أو بايت بهذا الترتيب من اليسار إلى اليمين، أي من الأقل أهمية (LSB) إل الأكثر أهمية (MSB) كما يظهر في الشكل (5).

Start	1	2	3	4	5	6	7	8	Par	Stop

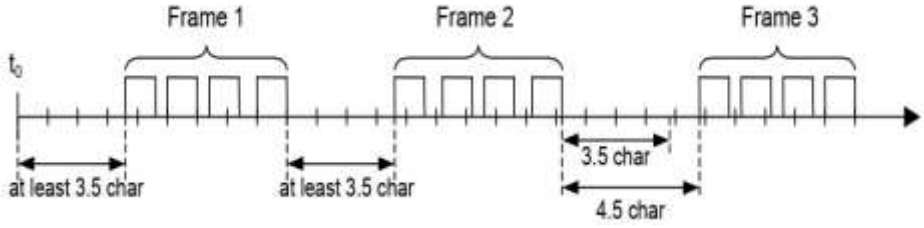
الشكل (5): تسلسل البتات لبرتوكول MODBUS-RTU.

- **إطار MODBUS-RTU:** يُظهر الشكل (6) حقول إطار MODBUS-RTU ، بحجم (256 Byte) كحد أقصى.

Slave Address	Function Code	Data	CRC
1 byte	1 byte	0 up to 252 byte(s)	2 bytes CRC Low, CRC Hi

الشكل (6): إطار MODBUS RTU.

- **<u>تأطير رسائل MODBUS RTU:</u>** يتم وضع رسالة MODBUS بواسطة جهاز الإرسال في إطار له نقطة بداية ونهاية معروفة، و يسمح هذا للأجهزة التي تتلقى إطاراً جديداً معرفة وقت اكتمال الرسالة، وفي وضع (RTU) يتم فصل إطارات الرسائل بفاصل زمني لا يقل عن (3.5 character) كما في الشكل (7)، و يتوضّع الفاصل الزمني في بداية و نهاية الإطار.



الشكل (7): آلية ارسال الأطر في MODBUS-RTU.

<u>ملاحظة:</u> بالنسبة لمعدلات الارسال التي تزيد عن (19200) بت في الثانية يُوصى باستخدام قيمة (750) ميكرو ثانية للمهلة بين الأحرف (1.5 char) وقيمة (1.750) ميلي ثانية للفاصل الزمن (3.5 char).[2]

6- ناقل (RS485) لبرتوكول MODBUS التسلسلي:

على المستوى الفيزيائي يستخدم MODBUS التسلسلي نواقل مختلفة مثل (RS485، RS232)، و يعتبر الناقل (RS485) ثنائي الأسلاك الأكثر شيوعاً، و سنذكر فيما يلي أهم مُتطلبات ناقل "RS458 " [2]:

a) **<u>عدد الأجهزة:</u>** بالنسبة لأي نظام متعدد النقاط (EIA / TIA-485) ، سواء في تكوين 2 سلك أو 4 أسلاك ، يكون عدد الأجهزة التي يمكن وصلها بدون مكرّر (Repeater) هو (32) جهاز.

b) **الطوبولوجيا:** يحتوي تكوين RS485-MODBUS بدون مكرر على كابل (trunk) واحد، يتم على طوله توصيل الأجهزة بشكل مباشرة (daisy chaining) أو بواسطة كابلات اشتقاق قصيرة (derivation cables)، و يجب توصيل طرفي الناقل الرئيسي عند انتهاء الخط بمقاومات.

c) **طول الناقل:** يجب أن يكون طول الناقل (trunk) محدوداً، و يعتمد الحد الأقصى للطول على معدل الارسال بالبت، فالحد الأقصى لمعدل ارسال ([bps] 9600) مثلاً هو (1) كيلومتر و طول كابلات الاشتقاق قصير نسبياً و لا يتجاوز (20) متر.

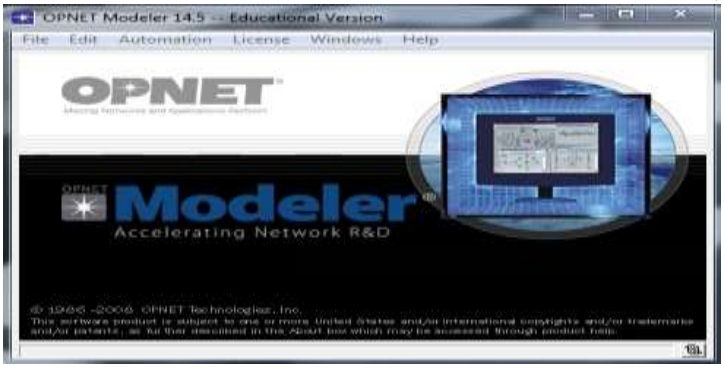
d) **التأريض:** يجب توصيل السلك المشترك "Common" مباشرة بالأرض ويفضل عند نقطة واحدة فقط للناقل بأكمله، و بشكل عام تكون هذه النقطة عند الجهاز الرئيسي"Master".

e) **إنهاء الناقل:** الانعكاس في الناقل هو نتيجة لانقطاع الممانعة الذي تعانيه الموجة المتنقلة أثناء انتشارها في الناقل، و لتقليل الانعكاسات من نهاية ناقل (RS485) يلزم وضع نهاية خط (LT)، و يتم وضع مقاومتي انهاء عند طرفي الناقل تصل بين السلكين (D0) و (D1)، و تكون قيمة المقاومة (150 ohm) و باستطاعة (0.25 watt)، و يتم وصل مكثف قطبي (1) نانو فاراد (10) فولط.

7- محاكي الشبكات OPNET:

إنّ OPNET عبارة عن أداة من شركة MIL3 طوّرها الطالب Alain Cohen في عام 1986 وهو اختصار لـOptimized Network Engineering Tools أي أدوات هندسة الشبكات المُحسّنة، وهو أحد أشهر المحاكيات الشبكيّة وأكثرها شعبية بسبب استخدامه الكبير والواسع في مجالي الصناعة والأبحاث الشبكية، وهو نظام هندسي قادر على محاكاة شبكات الاتصال الضخمة مع نمذجة تفصيليّة للبروتوكولات والتطبيقات

والأجهزة وتحليل الأداء، و تمّ استخدام نسخة OPNET الأكاديمية ذات الاصدار (14.5) في بحثنا هذا و تظهر واجهة البرنامج بالشكل(8).[3]



الشكل (8): واجهة برنامج OPNET اصدار (14.5) المُستخدم.

7-1 أهم خصائص برنامج OPNET:

a) دورة النمذجة والمحاكاة: إنّ OPNET يُوفر أداة فعالة لمساعدة المستخدم في تحقيق المراحل الثلاث الأولى من طور التصميم وهي: بناء نموذج، تنفيذ المحاكاة، تحليل الخرج.

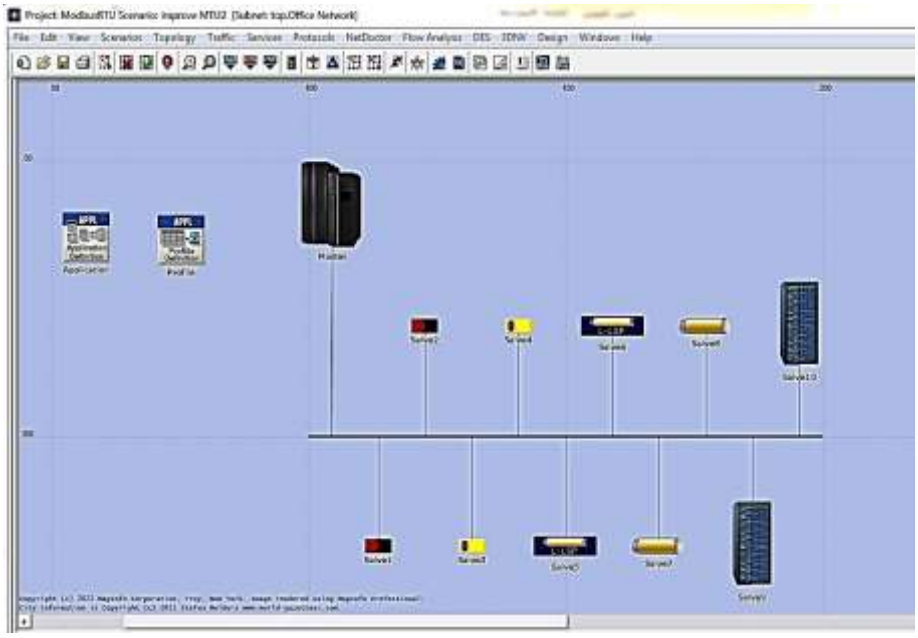
b) النمذجة الهرمية: إنّ OPNET يوظف بنية هرميّة من أجل النمذجة وكل مستوى من الهرميّة يصف مفاهيم مختلفة من النموذج الكامل الذي يتم مُحاكاته، حيث أنّ النماذج فيOPNET تُبنى بشكل هرمي، النماذج يمكن أنْ تُبْنَى إما من الأعلى للأسفل أَو من الأسفل للأعلى وكُلّ مستوى يمثّل التركيب الداخلي ووظيفة المستوى الأعلى، و هي (مستوى الشبكة و مستوى العقدة و مستوى العمليّة).[3]

c) تُخصص لشبكات الاتصال: OPNET يملك مكتبات مُفصّلة تزود دعم كبير لبروتوكولات الاتصال ويتيح للباحثين بتعديل النماذج الموجودة أو تطوير نماذج جديدة خاصة بهم.

d) توليد المحاكاة بشكل أوتوماتيكي: إنّ نموذج OPNET يترجَم إلى شيفرة مصدريّة قابلة للتنفيذ وهذه الشيفرة الخاصة بمحاكاة الأحداث المُتقطّعة، يتم تنفيذها ببساطة والحصول على نتائج الخرج.

8- نمذجة مكونات شبكة صناعية لبرتوكول MODBUS التسلسلي:

نقوم بإنشاء شبكة ذات طوبولوجيا ناقل تسلسلي مُكوّنة من (11) عقدة قابلة للاختبار، واحدة منها هي "Master" و الأخرى من النوع "Salves" و تمّ وضع عدة أنواع من العقد التابعة مثل (الحساسات الرقمية والتماثلية و المشغلات الرقمية والتماثلية و أجهزة التحكم المنطقية PLC التابعة) تتبادل البيانات وفق نمط الارسال MODBUS-RTU كما يظهر في الشكل (9).



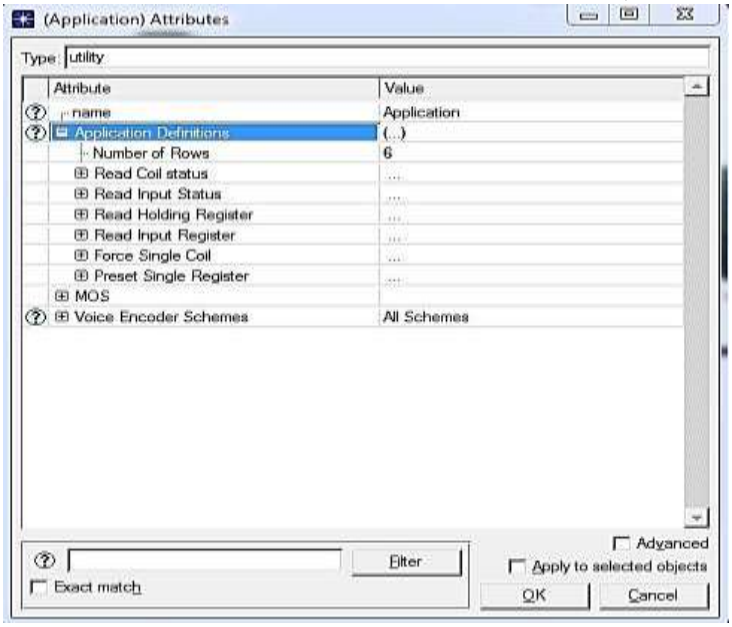
الشكل (9): شبكة برتوكول MODBUS التسلسلي باستخدام برنامج OPNET.

ملاحظة هامة جداً: لا تحتوي مكتبة OPNET ناقل برتوكول MODBUS بمختلف أنواع العقد المتصلة به من حساسات و مشغلات و أجهزة تحكم منطقيّة PLC و ناقل RS485 لنقل أُطر البيانات ذات النمط RTU المُستخدم، لذلك قمنا من خلال هذا

البحث بنمذجة هذه المكونات من خلال عملية تعديل خصائص العقد المُختارة لتتناسب مع خصائص شبكة ناقل MODBUS التسلسلي، مُقدمين نموذج لشبكة MODBUS قابلة لعمليات التحليل و الاختيار.

– فيما يلي سوف نوضّح خصائص كل عقدة مستخدمة في هذا النموذج:

خصائص الجهاز (Application): هو جهاز يتيح نمذجة التطبيقات وفق الشبكة المدروسة و برتوكول الاتصال MODBUS المُستخدم، وتمّ نمذجة ستة تطبيقات فقط علماً أنه يوجد العديد من التطبيقات التي يدعمها برتوكول MODBUS و تختلف عن بعضها بحجم و عنوان و وظيفة الطلب المرسل من العقدة الرئيسية إلى إحدى العقد التابعة كما يظهر في الشكل(10):



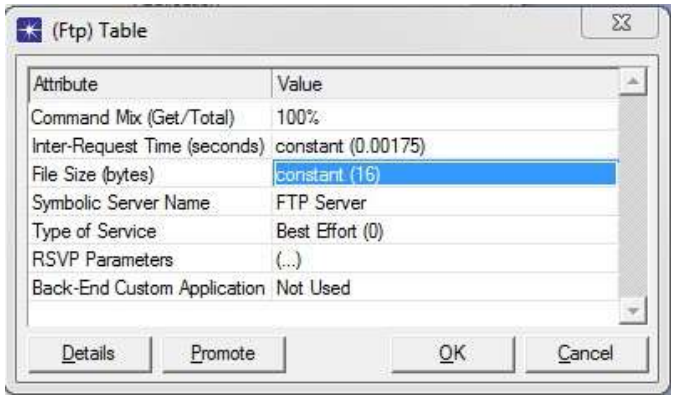
الشكل (10) : تعريف التطبيقات الستة المستخدمة في شبكة MODBUS.

حيث أنّ:

1. التطبيق (Read Coil Status): يدل على إرسال طلب من العقدة الرئيسية للعقدة التابعة لقراءة حالة خرج رقمي و يُرمز للوظيفة بالعنوان (01) بشكل ستة عشري بطول واحد بايت.

2. التطبيق (Read Input Status): يدل على إرسال طلب من العقدة الرئيسية للعقدة التابعة لقراءة حالة دخل رقمي و يُرمز للوظيفة بالعنوان (02) بشكل ستة عشري بطول واحد بايت.
3. التطبيق (Read Holding Register): يدل على إرسال طلب من العقدة الرئيسية للعقدة التابعة لقراءة حالة خرج تماثلي و يُرمز للوظيفة بالعنوان (03) بشكل ستة عشري بطول واحد بايت.
4. التطبيق (Read Input Register): يدل على إرسال طلب من العقدة الرئيسية للعقدة التابعة لقراءة حالة دخل تماثلي و يُرمز للوظيفة بالعنوان (04) بشكل ستة عشري بطول واحد بايت.
5. التطبيق (Force Single Coil): يدل على إرسال طلب من العقدة الرئيسية للعقدة التابعة لكتابة أمر لخرج رقمي و يُرمز للوظيفة بالعنوان (05) بشكل ستة عشري بطول واحد بايت.
6. التطبيق (Preset Single Register): يدل على إرسال طلب من العقدة الرئيسية للعقدة التابعة لكتابة أمر لخرج تماثلي و يُرمز للوظيفة بالعنوان (06) بشكل ستة عشري بطول واحد بايت.

تمّ تعيين كل تطبيق وفق الخصائص المُوضّحة بالشكل(11):



الشكل (11): ضبط خواص التطبيق المُعرف في برنامج OPNET.

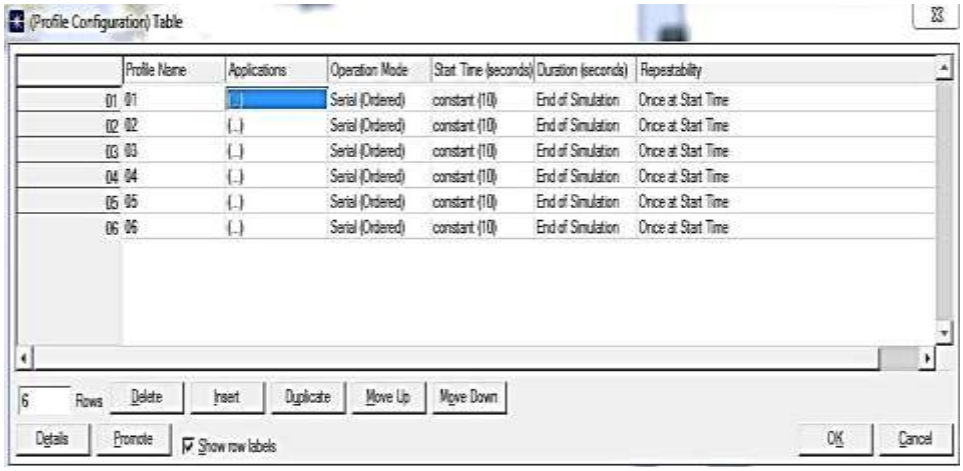
- ❖ الخاصية "Inter-Request Time" تدل على الفترة الزمنية التي تفصل بين الأطر المرسلة و تم تحديدها بالقيمة (1.750) ميلي ثانية لتناسب خصائص برتوكول MODBUS.
- ❖ الخاصية "File Size" تدل على حجم الإطار المرسل مقدراً بالبايت و يُمكن تحديد حجمه ضمن المجال (8 Byte) إلى القيمة (256 Byte) آخذين بعين الاعتبار حجم ترويسة إطار MODBUS-RTU و التي تُقدر بـ ([Byte] 4).

خصائص الجهاز(Profile): يتم بالبداية تعيين ستة ملفات تعريف حسب الرمز المُعتمد لترميز الوظائف في شبكات MODBUS حيث يحصل كل تطبيق على رمز مُؤلف من خانتين بشكل ستة عشري، ويتم ضبط ملف التعريف الأول (01) على التطبيق (Read Coil Status) و يتم تحديد السمات كتالي:

- ❖ السمة (Start Time Offset) على القيمة ([s]1=Constant): هذه السمة تُحدد الفترة الزمنية بين نهاية أحد التطبيقات وبداية التطبيق التالي.
- ❖ السمة (Duration) على القيمة (End of the Profile): تُعبّر عن الحد الأقصى من الزمن المسموح به لجلسة التطبيق قبل أن يتم إحباطها.
- ❖ السمة (Start Time) على القيمة ([s]10=Constant): تُحدد زمن التأخير لبداية المحاكاة.

ملاحظة: بالاعتماد على السمة الأولى و الثالثة سوف تحتاج كل عقدة تعمل على مثل هذا النوع من التطبيقات لزمن تأخير يُقدر بـ (11) ثانية.

يتم تحديد ملفات تعريف باقي التطبيقات بنفس الطريقة كما في الشكل (12):



الشكل (12): ملفات تعريف تطبيقات شبكة MODBUS الستة.

خصائص الجهاز الرئيسي (Master): يمثل هذا الجهاز العقدة الرئيسيّة في الشبكة و التي تدير عمليات الارسال و الاستقبال في شبكات MODBUS و تمّ ضبط خصائصها كالتالي:

- السمة (wkatn): يتيح هذا النوع من الأجهزة تعريف تطبيقات مختلفة تدعمها العقدة الرئيسية، حيث لم يتم بناء هذه العقدة وفق مستويات برنامج OPENT الهرميّة، وإنّما تمّ تعديل بعض الخصائص بما يلائم مزايا العقد المُستخدمة في الشبكة المدروسة، و إضافة بعض السمات على مستوى العقدة مثل السمة "Type" التي تحدد نوع الجهاز المُستخدم و تم إضافة السمة "Device" لتحديد نوع الوظيفة التي تدعمها العقدة.
- السمة (Application Supported Profile): تُحدد أسماء جميع ملفات التعريف التي تمّ تمكينها على هذه العقدة لدعم جميع أنواع التطبيقات المُتاحة في نموذج MODBUS.

- ❖ السمة (Application Supported Services): تتيح هذه السمة للعقدة استقبال جميع أنواع التطبيقات المتاحة من العقدة الأخرى و قد تمّ ضبطها على القيمة (ALL).

خصائص العقدتين (Salve1+Salve2): تمّ تعيين هاتين العقدتين كحساسيين رقميين و بتالي سيتم ضبط السمات كالآتي:

- ❖ السمة (Application Supported Profile): على ملف التعريف (02) الذي يعبر عن تطبيق (Read input status).
- ❖ السمة (Application Supported Services): على القيمة ALL.
- ❖ السمة (Type Device): على القيمة (digital sensor).

خصائص العقدتين (Salve3+Salve4): تمّ تعيين هاتين العقدتين كحساسيين تماثليين و بتالي سيتم ضبط السمات كالتالي:

- ❖ السمة (Application Supported Profile): على ملف التعريف (04) الذي يعبر عن تطبيق (Read input register.
- ❖ السمة (ApplicationSupported Services): على القيمة ALL.
- ❖ السمة (Type Device): على القيمة (analog sensor).

خصائص العقدتين (Salve5+Salve6): تمّ تعيين هاتين العقدتين كمشغلين رقميين و بتالي سيتم ضبط السمات كتالي:

- ❖ السمة (Application Supported Profile): سيتم ضبطها على ملفي التعريف (01) و (05) أي (Read Coil Status) و (Force Single Coil) بالترتيب.
- ❖ السمة (Application Supported Services): على القيمة ALL.
- ❖ السمة (Type Device): على القيمة (Digital Actuator).

خصائص العقدتين (Salve7+Salve8): تمّ تعيين هاتين العقدتين كمشغلين تماثليين و بتالي سيتم ضبط السمات كتالي:

- السمة (Application Supported Profile): سيتم ضبطها على ملفي التعريف (03) و (06) أي (Read Holding Registers) و (Preset Single Registers) بالترتيب.
- السمة (ApplicationSupported Services): على القيمة ALL.
- السمة (Type Device): على القيمة (Analog Actuator).

خصائص العقدتين (Salve9+Salve10): تمّ تعيين هاتين العقدتين كمتحكمين منطقيين قابلين للبرمجة (PLC) و بتالي سيتم ضبط السمات كتالي:

- السمة (Application: Supported Profile): سيتم ضبطها على ملفات التعريف الستة.
- السمة (Application Supported Services): على القيمة ALL تتيح هذه القيمة استقبال كافة طلبات التطبيقات المستخدمة في شبكة MODBUS– RTU المدروسة.

خصائص الناقل (RS485): هو الناقل الرئيسي في شبكة MODBUS–RTU، و تمّ تحديد نوعه "coax–adv" و هذا النوع يُتيح عدة سمات نستطيع من خلالها رصد العديد من البارامترات الهامة مثل (حالة حصول تصادم بين الأطر و كذلك يمكن معرفة فيما إذا تم قبول الإطار و يمكن حساب عدد الأخطاء في بتات الإطار و يمكن أيضاً مراقبة زمن تأخير الارسال و الانتشار للإطار عبر الناقل) و غيرها من البارامترات الهامة، و لقد تمّ ترك السمات على القيم الافتراضية باستثناء البعض منها و نذكر فيما يلي السمات التي تم ضبطها ليُمثل هذا الناقل خصائص ناقل RS485 المُستخدم في شبكات MODBUS– RTU الصناعية.

- السمة(ber): تمّ ضبطها على القيمة (10^{-6}).

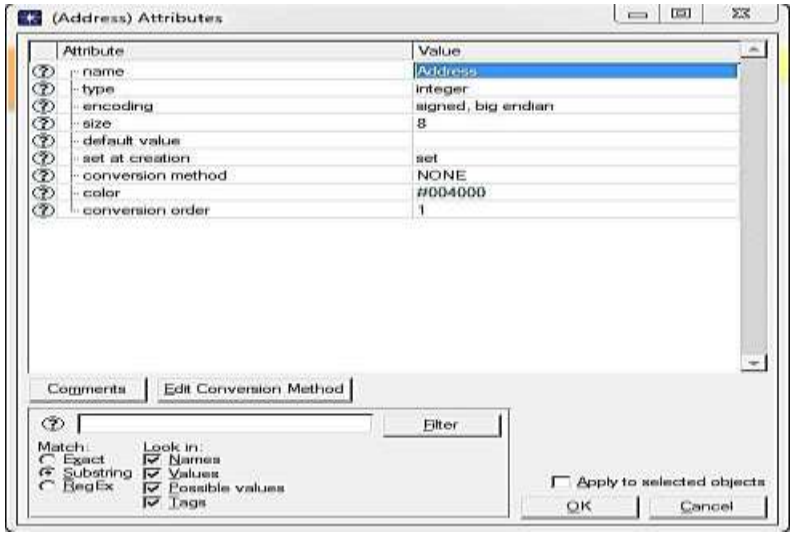
- السمة(data rate): تمّ ضبطها على القيمة (19200 bps).
- السمة(delay): تمّ ضبطها على القيمة (0.001) ثانية.
- السمة(packet format): تمّ ضبطها على القيمة (Modbus-RTU).
- السمة(thickness): تمّ ضبطها على القيمة (2) ملم.

إطار MODBUS-RTU: يُتيح برنامج OPNET بناء إطار برتوكول اتصال معين، و تمّ تشكيل إطار MODBUS-RTU وفق الخطوات الآتية:

- من قائمة "File" نختار "New" و من ثمّ نختار محرر الأطر " Packet Format"، من النافذة نختار "Create New Field".
- نقوم بإنشاء إطار MODBUS-RTU المؤلف من أربعة حقول كما في الشكل (13).

الشكل (13): حقول إطار MODBUS-RTU الأربعة في برنامج OPNET.

- نقوم بتحرير أربعة حقول ومن ثم نحدد خصائص كل حقل "attribute" كما في الشكل (14) و الذي يُظهر خصائص الحقل "Address".



الشكل (14): خصائص حقل "Address" في إطار MODBUS-RTU.

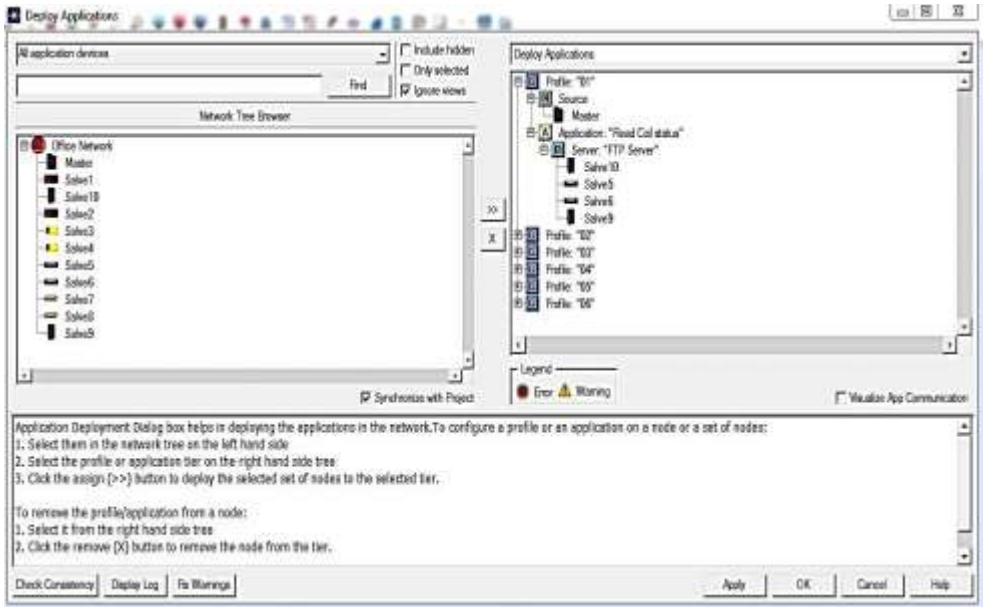
ملاحظة : تتشابه كل من الحقول "Address" و "Function Code" و "CRC" بنوع الخاصية فجميعها من النوع "integer" و تختلف فقط بالحجم حسب خصائص برتوكول MODBUS-RTU.

- حقل "Data" يتم ضبط خاصية "Type" على النوع "Packet" ومن ثم اختيار "Inherited" ،حيث يتيح خيار "Inherited" تعيين حجم الحقل على حجم البيانات الفعلي وفق التطبيق المستخدم، و يتم ضبط الترميز "encoding" على النوع "singed.big endian" الذي يحافظ على تسلسل البيانات المُرسل بجهة الاستقبال.
- نقوم بحفظ الإطار باسم "ModbusRTU" و من ثم نعود إلى خصائص ناقل RS485 ونقوم بضبط الخاصية "Packet Formats" على الوضع "ModbusRTU" حيث نقوم بجعلها "supported".

ملاحظة هامة: قبل تشغيل الشبكة المُصمّمة لا بدّ من جعل العقدة الرئيسية هي التي تقوم بإرسال جميع أوامر التطبيقات للعقد التابعة الأخرى وفق نمط الارسال

(Master\Salve) المُعتمد في برتوكول MODBUS-RTU و تم ضبط ذلك بالخطوات التالية:

- من تبويبه (Protocols) نختار (Applications) و من ثم (Deploy Defined Application) و نقوم بضبط خواص العقد كما في الشكل (15).



الشكل (15): ضبط خواص عقد شبكة MODBUS لتحديد "Master" و "Salves".

9- بارامترات أداء شبكة MODBUS التسلسلي:

يرتبط مفهوم أداء الشبكات الصناعيّة بعدد كبير من البارامترات نذكر منها (الاستخدامية للشبكة "Utilization"، و مقدار الخطأ في البت "BER"، و نسبة عدد البتات المرسلة إلى المستلمة، و زمن تأخير الأطر في الشبكة "End To End Delay"، وعدد التصادمات للأطر "Collisions"، و زمن الاستجابة "Time Response"، و الانتاجية "Throughput") و غيرها.

يتيح برنامج OPNET دراسة الكثير من الإحصائيات المرتبطة بالأداء حيث تُقسم إلى ثلاثة أنواع رئيسية:

1. (Global Statistics): تتيح دراسة بارامترات تؤثر على كامل الشبكة.

2. (Node Statistics): يمكن من خلالها دراسة بارامترات تؤثر في العقدة المرتبطة بالشبكة.
3. (Link Statistics): يمكن من خلالها دراسة بارامترات تؤثر في خطوط النقل التي تربط بين عقد الشبكة.

ملاحظة : أثناء اختيار بارامترات الأداء المرتبطة بالشبكة المدروسة لا بدّ من توخي الحذر لأنّ البرنامج يتيح حرية اختيار الاحصائيات من قبل المُستخدم بشكل عام لذلك قد لا تظهر أية نتائج مرتبطة بالإحصائيات المختارة نتيجة عدم ارتباطها بخصائص الشبكة المدروسة، لذا لا بد من اختيار الاحصائيات المرتبطة بأداء الشبكة بشكل دقيق.

العوامل المؤثرة في بارامترات الأداء : يوجد العديد من العوامل المؤثرة في بارامترات أداء الشبكات الصناعية ذات الناقل MODBUS تمّ دراستها في العديد من الأبحاث المرجعيّة نذكر منها (طوبولوجيا الشبكة ، عدد العقد في الشبكة ، طول و نوعية الناقل) و غيرها من العوامل الأخرى، و تمّ اختيار العامل (MTU) في دراستنا و الذي هو اختصار للعبارة (Maximum Transmission Unit) و يُعرّف بوحدة الارسال العظمى أي حجم أكبر بيانات مرسلة في حقل الـ (Data) للإطار و هو مُرتبط بالقيمة الأعظمية لحجم الإطار المُرسل وفق برتوكول MODBUS–RTU، و يرتبط العامل (MTU) بمجموعة عوامل أخرى بالعلاقة الرياضيّة الآتية:

$$T_{transmission} = \frac{D\ (H + MTU)}{MTU * R}$$

حيث أنّ:

- ($T_{transmission}$): زمن الارسال اللازم لإرسال المعلومات بشكل كامل من المنبع.
- (D): عدد البيانات الكلي أو حجم (Data).
- (H): حجم الترويسة للبرتوكول المستخدم.
- (R): معدّل الارسال.

نلاحظ من العلاقة الرياضيّة السابقة وجود العامل (MTU) في البسط و المقام و بتالي لا بد من إجراء اختبار دقيق لتحديد قيمة مناسبة له، فالقيمة الصغيرة نسبياً تنعكس سلباً على الأداء نتيجة زيادة حجم الترويسات للأطر المرسلة مما يؤدي إلى انخفاضه، و كذلك زيادة حجمه نسبياً سيزيد من طول الإطار و بتالي سيؤثر على بارامترات أخرى مرتبطة بالأداء و بتالي انخفاضه أيضاً، لذا لا بدّ من اختيار قيمة وسط للمقدار (MTU) تحقّق أفضل أداء للشبكة.

البارومترات المرتبطة بأداء ناقل MODBUS الصناعي نذكر منها:

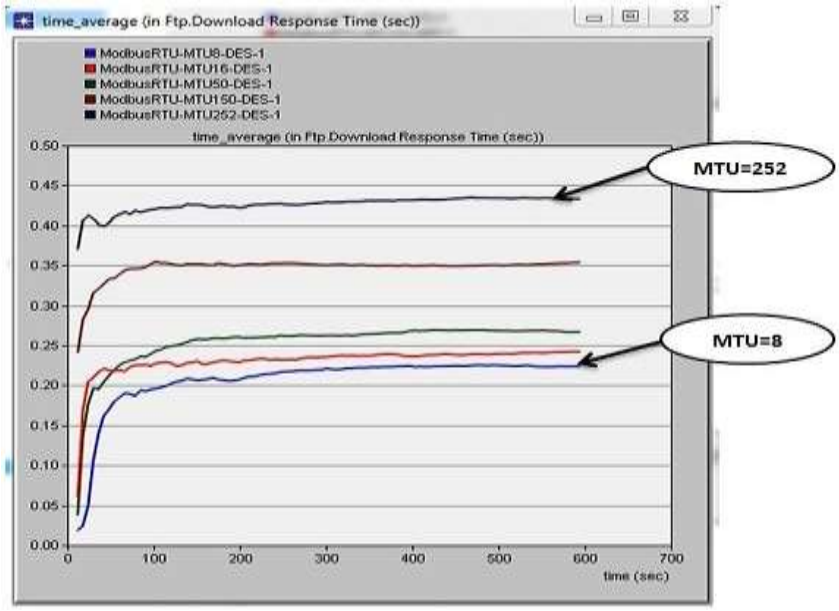
1. (Response Time): و هو من النوع (Global Statistics) و يُمثل الزمن اللازم لإرسال الطلب واستلام الاستجابة، حيث يتم قياس زمن التأخير بين لحظة ارسال العقدة الرئيسية (Master) الطلب إلى العقدة التابعة (Salve1) ولحظة تلقي الاستجابة و يُقاس هذا التأخير الزمني بالثانية و يتناسب عكساً مع أداء الشبكة فبنقصانه يزداد الأداء.
2. (End To End Delay): و هو من النوع (Global Statistics) و يُمثل الزمن التأخير (end to end) الفاصل بين لحظة ارسال الرسالة من المنبع إلى لحظة استقبالها من قبل الوجهة، و من أجل الحصول على أداء أفضل لا بد من تخفيضه قدر الإمكان.
3. (Utilization): و هي من النوع (Link Statistics) و تمثل النسبة المئوية المُستهلة لعرض النطاق الترددي للنقال الرئيسي و بازدياد النسبة يزداد الأداء.

10- دراسة و تحليل النتائج المرتبطة ببارامترات شبكة MODBUS التسلسلي:

تمّ تشغيل عملية المحاكاة على خمسة سيناريوهات مختلفة ، تمّ فيها زيادة قيمة العامل MTU بالترتيب (252-150-50-16-8) بايت، و تمّ تحديد زمن المحاكاة بمقدار (10) دقائق.

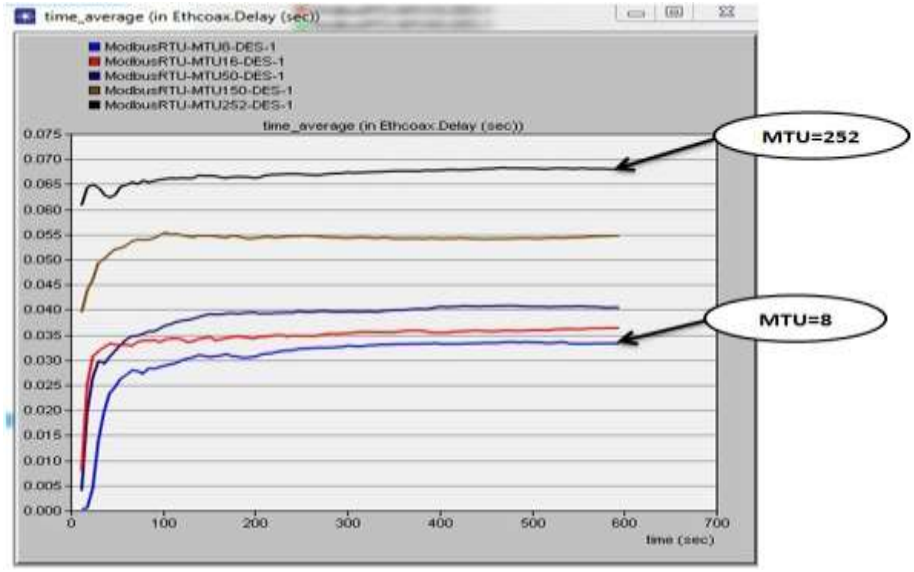
-البارامتر (Response Time): نلاحظ أنّه مع ازدياد حجم (MTU) يزداد زمن

الاستجابة فعند القيمة (MTU=8 [Byte]) سجل قيمة (0.2) ثانية و ازدادت بشكل طفيف مع ازدياد الحجم لتصل للقيمة (0.45) ثانية عند (MTU=252 [Byte])، كما هو مُوضح بالشكل(16).



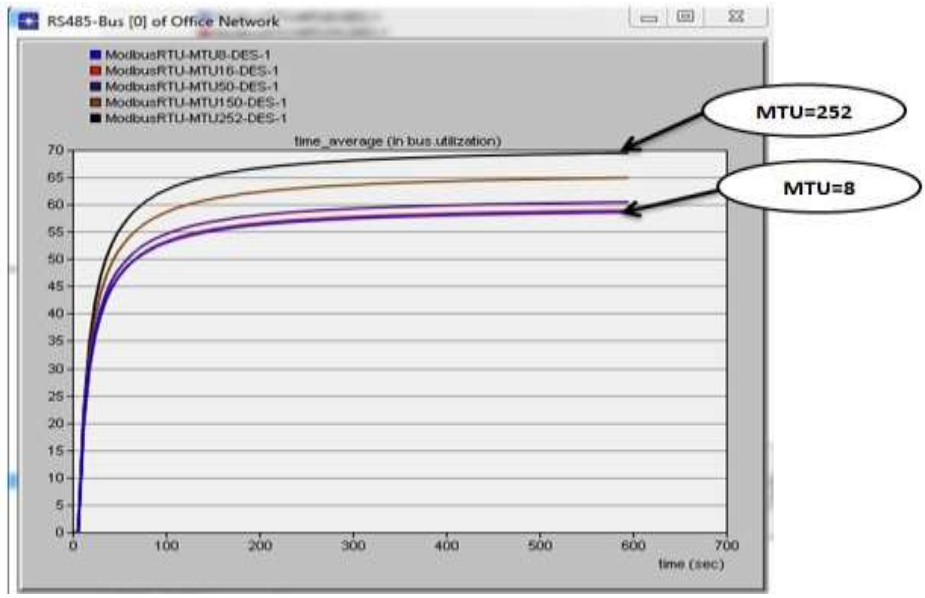
الشكل (16): مقارنة قيم البارامتر "Response Time " عند احجام MTU مختلفة.

- البارامتر(End To End Delay): بشكل مشابه لبارامتر زمن الاستجابة سجل تزايداً طفيفاً بدأ من القيمة (30) ميلي ثانية عند (MTU=8 [Byte]) و وصل للقيمة (70) ميلي ثانية عند (MTU=252 [Byte])، كما يظهر في الشكل(17).



الشكل (17): مقارنة قيم البارامتر "End To End Delay" عند احجام MTU مختلفة.

– البارامتر (**Utilization**): شهد هذا البارامتر ازدياد مع ازدياد حجم (MTU) فسجل قيمة (55%) عند أول سيناريو و قيمة (70%) عند خامس سيناريو كما يظهر في الشكل (18).



الشكل (18): مقارنة قيم البارامتر "Utilization" عند احجام MTU مختلفة.

11- النتائج و الاستنتاجات:

على الرغم من ازدياد أزمنة التأخير بازدياد حجم الإطار المُرسل نتيجة زيادة العامل MTU إلا أنّه يبقى في مستويات مقبولة بالنسبة لمتطلبات الزمن الحقيقي في الشبكات الصناعية و الذي يُحدد قيمة عظمى لتأخير زمن الاستجابة بمقدار (0.5) ثانية، من جهة أخرى لاحظنا ارتفاع في استخدامية الناقل بقدار (15%) و بتالي رفع أداء الشبكة الصناعية لبرتوكول MODBUS التسلسلي.

إنّ استخدام حساسات و مشغلات صناعية ذات دقة عالية نسبياً و بحجم معلومات من رتبة ([Byte] 200) لن يخل بمُتطلبات الزمن الحقيقي بل له أثر إيجابي في زيادة استخدامية الناقل و بتالي رفع أداء الشبكات الصناعية MODBUS ، و على الرغم من عدم تأثر الناقل بأقصى حجم للإطار عند (MTU = 252 [Byte]) إلا أنه لا يُنصح بالوصول لهذه القيمة نتيجة الاقتراب الكبير من القيمة الحديّة التي تخل بشروط العمل في الزمن الحقيقي للشبكات الصناعية فتبقى نماذج المحاكاة مثاليّة من ناحية التصميم و لا يظهر فيها عيوب الوصلات و الاسلاك التي تُسبب تأخير لا بدّ منه في الشبكات الصناعية الواقعية.

مما سبق يُنصح بضبط أحجام الأطر للعقد المتصلة بالشبكة ضمن المجال من (150) إلى (200) بايت بحيث تُسبب زيادة في استخدامية الناقل و بتالي الأداء و بشكل لا يزيد من أزمنة التأخير لتبقى في مستويات مقبولة لعمل الشبكات الصناعية في الزمن الحقيقي.

12- التوصيات و الآفاق المستقبلية:

- ✓ يمكن استخدام نموذج الشبكة المصمّم لدراسة عوامل أخرى مُؤثرة في بارامترات الأداء.
- ✓ إجراء نماذج لشبكات MODBUS/TCP و تحليل أدائها.
- ✓ نمذجة شبكات صناعية واقعية باستخدام برنامج OPNET و اختبار أدائها.
- ✓ تصميم منظومة عملية للمقارنة بين أنماط ارسال MODBUS و اختبار أدائها.

المراجع:

[1] KUMER SEN, S2014-Fieldbus and Networking in Process Automation. CRC Press, New York ,439p.

[2] MODBUS.Org,2006-MODBUS over Serial Line Specification and Implementation Guide. US,44p.

[3] LU YANG,H2012-Unloking The Power of OPNET Modeler. CAMBRIDGE, UK, 253p.

[4] Yunyuan.Y, Meng.C,2020-An Improved Algorithm for Adaptive Communication Frame Length Based on Modbus Protocol. IEEE, Shenyang Institute of Technology, China,8p.

[5] Gamess.E, Smith.B, and Francia.G,2020 - PERFORMANCE EVALUATION OF MODBUS TCP IN NORMAL OPERATION AND UNDER A DISTRIBUTED DENIAL OF SERVICE ATTACK. IJCNC, Florida,US, Vol.12, No.2,21p.

[6] Mnaouer.A, Fujii.Y, Sekiguch.T,2017- Colored Petri Nets Based Evaluation of Transmission Procedures at a Fieldbus Data Link Layer Protocol.IEEE, Yokohama University,Brazil,12p.

[7] Krupanek.B , Bogacz.R,2016- OPNET Modeler simulations of performance for multi nodeswireless systems. Silesian University of Technology, Poland,10p.

[8] Kim.B, Lee.D, Choi.T,2015- Performance Evaluation for Modbus/TCP Using Network Simulator NS3.IEEE, Kyungpook National University, Korea,10p.

[9] Künzel.G, Ribeiro.C, Pereira.C,2014- A Tool for Response Time and Schedulability Analysis in Modbus Serial Communications. IEEE, Federal Institute of Education, Brazil,12p.

[10] Hao.J, Wu.J, Guo.C,2011- Modeling and Simulation of CAN Network Based on OPNET. IEEE, Naval University, China,10p.

[11] Oh.E,2009- Study of Network Design Factors That Influence Industrial Fieldbus Network-Based System Integration . The Ohio State University, Korea,84p.

[12] Ali.Q,2007- Measurements and Performance Analysis of Industrial Ethernet. IEEE, University of Mosul, Iraq,16p.