مجلة جامعة دمشق للعلوم الهندسية
المجلد42 العدد (3) – 2026: 155- 165

Damascus University Journal for engineering sciences
Vo 42 number (3) -2026: 155-165

تنفيذ دارة الكترونية لدراسة بارامترات أداء برتوكول MODBUS–RTU والتحقّق من قابلية نمذجته باستخدام المحاكي OPNET

فيدل أحمد ابراهيم*[1]

*[1]. دكتور، مهندس، قسم الهندسة المعلوماتية، كلية الهندسة، جامعة الرشيد الخاصة.
Fidel-Ibrahim@ru.edu.sy

الملخص:

تقوم البرتوكولات الصناعية بإدارة عملية تبادل البيانات بين أجهزة الأتمتة المختلفة بشكل موثوق وفعّال، ويعتبر برتوكول MODBUS أشهر أنواع البرتوكولات الصناعية المُستخدمة.

قدمت هذه الورقة دارة عملية مكونة من وحدتين تتبادل البيانات فيما بينها وفق برتوكول MODBUS-RTU بهدف دراسة بارامترات أداء مثل (تأخير الإطار، ومعدل الأطر) والتحقّق من قابلية النمذجة لمثل هذا النوع من البرتوكولات باستخدام المحاكي OPNET من خلال إجراء عمليات المقارنة بين قيم البارامترات المدروسة.

وأكدت قابلية المحاكي OPNET في توصيف سلوك الشبكات العاملة على البرتوكول المدروس.

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

تاريخ الإيداع: 2023/9/5
تاريخ القبول: 2023/12/13

حقوق النشر: جامعة دمشق – سورية، يحتفظ المؤلفون بحقوق النشر بموجب الترخيص
CC BY-NC-SA 04

http://journal.damascusuniversity.edu.sy/index.php/index/index
ISSN (online): 2789-6854

Damascus University Journal for engineering sciences
Vo 42 number (3) -2026: 155-165

مجلة جامعة دمشق للعلوم الهندسية
المجلد42 العدد (3) – 2026: 155- 165

Implementation of an electronic circuit to study the performance parameters of the MODBUS-RTU protocol and verify its model ability using the OPNET simulation.

Fidel Ahmad Ibrahim*[1]
*[1].Dr. Eng, IT Engineering Department, Faculty of Engineering, Al-Rasheed Private University.
Fidel-Ibrahim@ru.edu.sy

Abstract:
Industrial protocols exchange data between different automation devices. MODBUS is the most widely used industrial protocol.
This paper presented a practical circuit consisting of two units that exchange data with each other according to the MODBUS-RTU protocol in order to study performance parameters such as (frame delay, frame rate) and to verify the model ability of this type of protocol using the OPNET simulator by conducting comparisons between the values of the studied parameters.
The results showed high performance of the MODBUS-RTU protocol in automating industrial processes and confirmed the ability of the OPNET simulator to characterize the behavior of networks operating on the studied protocol.
Keywords: MODBUS protocol, performance analysis of industrial networks, study of factors affecting performance, modeling of the MODBUS protocol using OPNET, modeling of industrial protocols using OPNET.

Received: 5/9/2023
Accepted: 13/12/2023

Copyright: Damascus University- Syria, The authors retain the copyright under a CC BY- NC-SA

http://journal.damascusuniversity.edu.sy/index.php/index/index
ISSN (online): 2789-6854

المقدمة:

يعتبر بروتوكول MODBUS من أشهر أنواع برتوكولات الشبكات الصناعية، بدأ العمل به منذ عام 1979، حيث مكّن ملايين أجهزة الأتمتة الصناعية بالاتصال فيما بينها وبشكل موثوق وفعال (Modbus Application Protocol, 2012)، ويعدّ بروتوكول MODBUS-RTU أحد أشهر أنواع برتوكولات Field-bus ذات الناقل التسلسلي، حيث يستخدم معيار (/ EIA TIA-485) والذي يسمح باتصال متعدد النقاط يصل إلى 247 جهاز تابع (MODBUS, 2016). تأتي دراسة وتحليل سلوك بروتوكولات الاتصال الصناعية من المواضيع الهامة نظراً لارتباطه الوثيق بالأداء العام للشبكة، تمّ تقديم العديد من النماذج الاختبارية لشبكات صناعية الهدف منها دراسة أثر العوامل المختلفة على بارامترات الأداء بهدف تحسينه. تدعم العديد من أدوات النمذجة محاكاة الشبكات الصناعية ومنها المحاكي OPNET والذي يوفر العديد من الأدوات في مكتبته الواسعة لعملية بناء مختلف أنواع الشبكات، ويتيح قابلية لنمذجة العقد على عدة مستويات هرمية وكذلك يُمكن من بناء التطبيقات الخاصة بما يلائم سلوك البرتوكولات المدروسة (Lu Yang, 2012). تقدم النمذجة قدرة على التنبؤ بسلوك برتوكولات الاتصال الشبكية وتتيح إجراء عمليات الاختبار بما يمكن من إجراء عمليات التوسعة والتطوير للشبكات بشكل آمن، لذا كان اختيار أداة النمذجة أمر بالغ الأهمية في نجاح الدراسات المستقبلية للشبكات المُنفذة.

المشكلة:

عدم توفر دارة عملية تعمل على بروتوكول MODBUS وتتيح قياس بعض بارامترات الأداء للشبكة الصناعية.

عدم القدرة على استخدام محاكي الشبكات OPNET في نمذجة شبكات صناعية واسعة دون التأكد من قابليته أولا

الهدف:

تنفيذ دارة عملية تدعم الاتصال وفق برتوكول MODBUS الصناعي وقياس بارامترات تخص الأداء وعرضها على واجهة حاسوبية.

التأكد من قابلية OPNET في نمذجة الشبكات الصناعية التي تستخدم برتوكول MODBUS من خلال مقارنة النتائج.

الدراسات المرجعية:

استخدام Mangkalajan وزملاؤه (2019) برنامج LabVIEW في تصميم واجهة تحكم واستحصال بيانات مؤلفة من مجموعة حساسات و مشغلات افتراضية تؤمن إشارات الدخل و الخرج التماثلية، و تم ارسال هذه الاشارات إلى مجموعة متحكمات صغرية ترتبط بدورها مع وحدة تحكم منطقية قابلة للبرمجة PLC من خلال شبكة LAN يدير عملية الاتصال بها برتوكول MODBUS-RTU مع اعتبار أن المتحكمات الصغرية تمثل الأجهزة التابعة في الشبكة و الـ PLC يمثل الجهاز الرئيسي، و أظهرت النتائج اختلافاً بسيطاً بين العملية الافتراضية و الواقعية بمتوسط خطأ مطلق MAPE يُقدر بالقيمة (5.24%). كما درس Gamess وزملاؤه (2020) العديد من المعايير لتقييم أداء أجهزة الشبكات الصناعية التي تستخدم برتوكولModbus/TCP، ومن المعايير التي تم دراستها (زمن الاستجابة لطلبات Modbusوالحد الأقصى لعدد الطلبات التي يمكن التعامل معها بنجاح بواسطة أجهزة Modbus في فترة زمنية محددة ومراقبة أجهزة Modbus عند تعرضها لهجوم رفض مُوزّع للخدمة Distributed Denial of Service)، وتمّ استخدام دارتين عمليتين ذات تكلفة منخفضة لتقييم أداء Modbus/TCP.

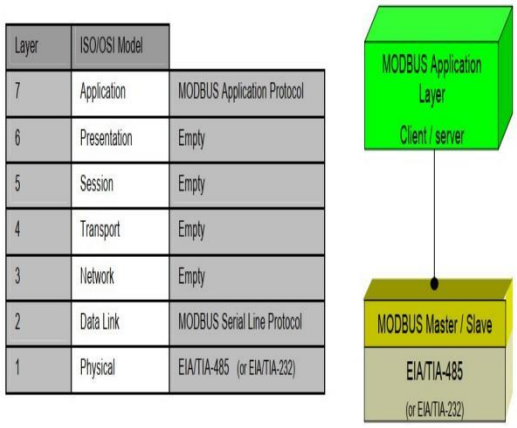
وتناول Ferrari وزملاؤه (2007) طريقة مُبسطة لتقدير أداء أنظمة الأتمتة الصناعية في الزمن الحقيقي مُستخدماً برتوكول PROFINET IO الصناعي حيث تمّ استخدام المحاكي الشبكات OPNET لتقديم نموذجين الأول لوحدات التحكم PROFINET IO والثاني لأجهزة الإدخال والإخراج، وأظهرت

النتائج توافق بين نتائج المحاكاة والنتائج العملية بنسبة خطأ لا تتجاوز 3%. ونشر بحث يُظهر عملية تنفيذ منظومة عملية تستخدم بروتوكول MODBUS في الزمن الحقيقي، وتتألف المنظومة من ثلاث عقد تتصل عبر ناقل RS485 إحدى هذه العقد Master في حين أنّ العقدتين الباقيتين هما Salves، تم برمجة وظائف العمليات لبرتوكول MODBUS والتأكد من تلبيتها لمتطلبات الزمن الحقيقي دون إجراء عمليات تحليل لبارامترات الأداء (Shukla et al., 2017). عانت جميع الدراسات المرجعية التي تم عرضها سابقاً من الضبابية وعدم الوضوح في طريقة تنفيذ الدارات العملية والتي تم الاستناد عليها في النتائج باستثناء الدراسة (Shukla et al., 2017) والتي وضّحت ذلك إلا أنها لم تهتم بدراسة بارامترات الأداء واختبار قابلية النمذجة.

بروتوكول MODBUS-RTU:

أحد أنواع برتوكولات MODBUS ذات الناقل التسلسلي (MODBUS Serial Line)، وهو بروتوكول Master-Slave، ويتوضّع هذا البروتوكول في المستوى الثاني من نموذج (OSI)، كما يظهر في الشكل 1 (MODBUS, 2016)، يحتوي نظام Master-Slave المُستخدم على عقدة واحدة "رئيسية" تصدر أوامر صريحة إلى إحدى العقد "التابعة" وتقوم بمعالجة الاستجابات، ولن تقوم العقد التابعة عادةً بنقل البيانات دون طلب من العقدة الرئيسية.

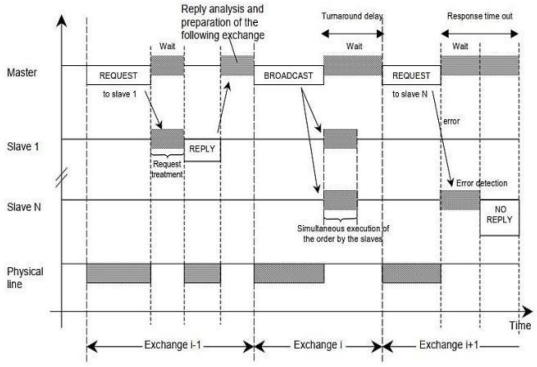
على المستوى الفيزيائي يستخدم MODBUS لأنظمة الناقل التسلسلي خطوط نقل مختلفة مثل (RS485، RS232)، ويُعتبر (RS485) ثنائية الأسلاك الأكثر شيوعا (MODBUS, 2016).



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

المخطط الزمني للاتصال (Master/Slave):

يوضح الشكل 2 الرسم البياني الزمني لثلاثة سيناريوهات نموذجية لاتصالات (Master/Slave). (MODBUS, 2016)



الشكل (2) المخطط الزمني للإرسال (Master/Slave)

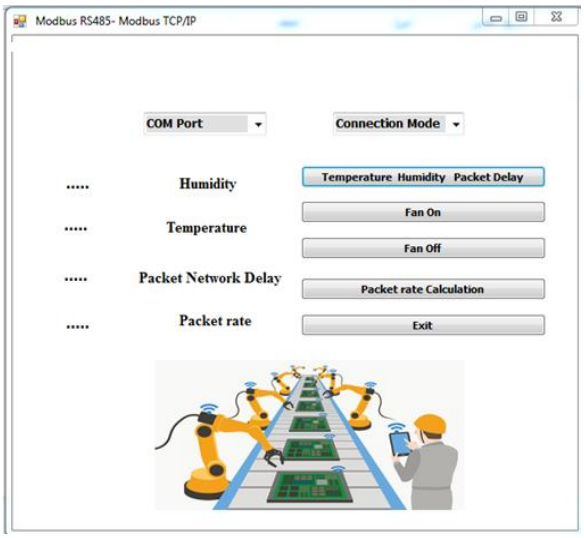
السيناريو الأول: يقوم فيه الجهاز الرئيسي "Master" بإرسال طلب "REQUEST" للعقدة التابعة "Salve1" والتي تستجيب بإرسال "REPLY" بعد فترة زمنية محددة " REQUEST TREATMENT" ويكون الناقل "Physical Line" خلال عملية ارسال كلاً من "REQUEST " و "REPLY " مشغولاً.

الجدول (1) المكونات الالكترونية للدارة المُنفذة.

م	المُكون الالكتروني للشبكة الصناعية	العدد
1	المتحكم الصغرى (ATMEGA328p)	2
2	وحدة الاتصال التسلسلي (MAX 485)	2
3	حساس حرارة ورطوبة (DHT11)	1
4	مروحة	1
5	ترانزستور (BC337)	1
6	وحدة اتصال مع الحاسوب (CP2102)	1
7	لد مؤشر	6

واجهة التحكم بالدارة العملية:

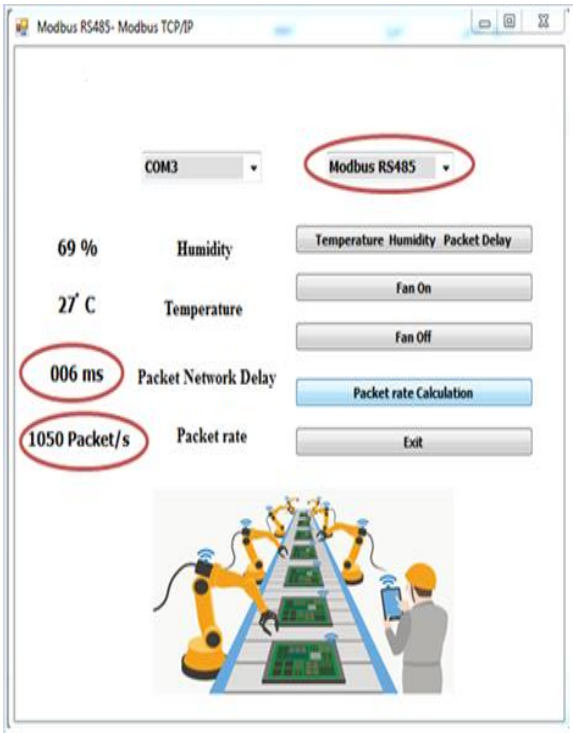
يُظهر الشكل 7 واجهة تحكم بالمنظومة المصممة، حيث تم تنفيذ هذه الواجهة باستخدام برنامج Visual BASIC، تتيح الواجهة اختيار منفذ الاتصال التسلسلي مع المنظومة و الذي تم تعيينه على القيمة (COM3)، كما تتيح الواجهة اختيار برتوكول الاتصال من خلال القائمة المنسدلة " Connection Mode"، و كذلك تتيح المنظومة إظهار كلاً من درجة الحرارة و الرطوبة و زمن تأخير الإطار من خلال النقر على الزر "Temperature Humidity Packet Delay"، و يمكن تشغيل و إطفاء المروحة من خلال الزرين "Fan On" و "Fan Off"، و يمكن حساب عدد الرزم في الثانية من خلال " Packet rate Calculation" و يمكن الخروج من البرنامج من خلال الزر "Exit".



الشكل (7) واجهة تحكم بالمنظومة المصممة

النتائج للشبكة العملية المنفذة:

الحالة الأولى: تم ارسال أمر لتشغيل حساس (الحرارة / الرطوبة)، و أظهرت النتائج الخاصة بالأداء أنّ زمن تأخير الإطار بشكل وسطي يتراوح حول القيمة (Packet Delay = 0.06 [MS]) و أنّ قيمة معدل الأطر في الثانية بشكل وسطي (Packet rate = 1050 [Packet/s])، تُظهر النتائج أداء عالي نتيجة صغر زمن التأخير و معدل الإرسال العالي للأطر كما هو موضح بالشكل8.



الشكل (8) تشغيل الدارة العملية وأخذ قراءات بعض بارامترات الأداء.

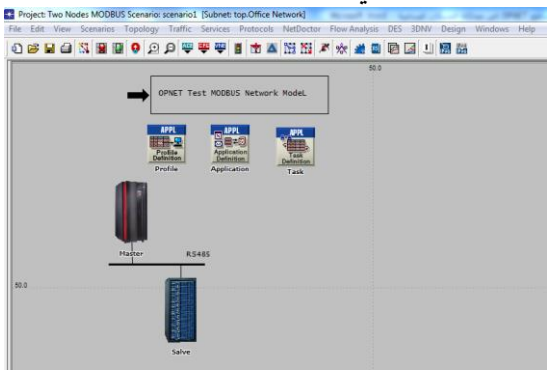
التحقّق من قابلية برنامج OPNET في محاكاة الشبكات الصناعية:

يُعتبر محاكي الشبكات OPNET بيئة مناسبة جداً في بناء الشبكات الحاسوبية كونه يحتوي جميع المكونات اللازمة في بناء هذه الشبكات ويدعم أيضاً جميع البرتوكولات والخدمات والتطبيقات المطلوبة في توصيف آلية نقل البيانات بين تلك المكونات.

ما يُميّز برنامج OPNET أنّهُ بيئة مفتوحة المصدر أي يمكن إضافة مكونات شبكيّة جديدة لمكتبته الخاصة المُعدة للاستخدام، كما ويدعم إجراء عمليات التعديل على خصائص العقد الموجودة بشكل يتناسب مع الحالة المدروسة. (3)

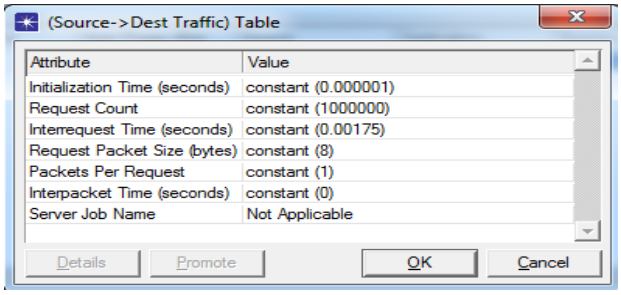
نموذج شبكة OPNET الاختبارية:

يُظهر الشكل 9 نموذج الشبكة الصناعية الاختباريّة والتي تتكون من عقدتين (Salve & Master) يربط بينهما ناقل RS458 ويدير عملية تبادل البيانات برتوكول MODBUS الصناعي والذي تمّ تعريف خواصه من خلال المكونات (Profile & Application &Task)، وسنذكر فيما يلي خصائص كل مكون في الشبكة المُصمّمة:



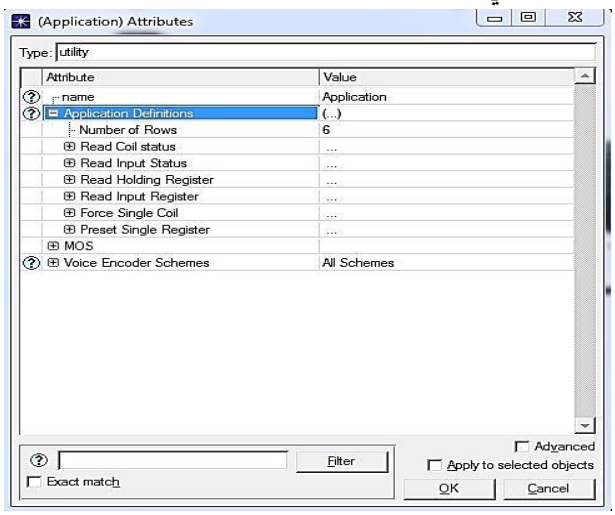
الشكل (9) الشبكة الصناعية الاختبارية باستخدام OPNET.

– خصائص الأيقونة Task: يتيح برنامج OPNET بناء التطبيقات الخاصة "Custom" عبر هذه أيقونة و من خلال الولوج إلى خصائصها "Attributes" يمكن وضع توصيف كامل للتطبيق المرغوب و بشكل يدوي من خلال " Manual Configration"، حيث تم ضبط خصائص الأطر المتبادلة بين العقد بشكل يتوافق مع خصائص برتوكول MODBUS كما يظهر في الشكل10 حيث نلاحظ أن حجم الأطر المرسلة 8 بايت و الزمن الفاصل بين الأطر يُقدر (1.75 MS)، و غيرها من القيم التي حددتها "The Modbus Organization". (1)



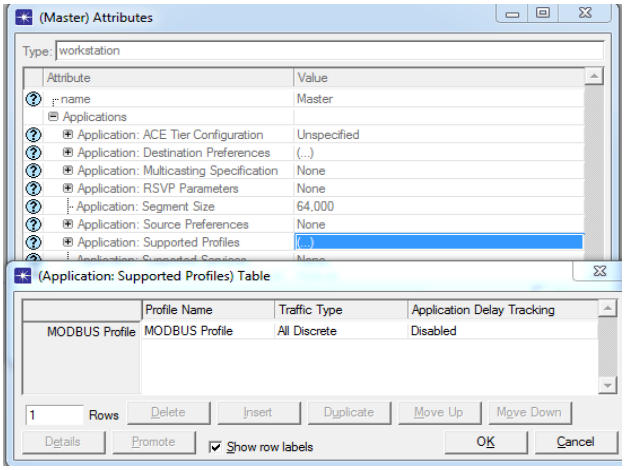
الشكل (10) خصائص الأطر المتبادلة وفق برتوكول MODBUS.

– خصائص الأيقونة Application: تتيح نمذجة التطبيقات وفق الشبكة الصناعية المدروسة وبرتوكول الاتصال MODBUS المُستخدم، وتمّ نمذجة ستة يدعمها برتوكول MODBUS وتختلف عن بعضها بعنوان وظيفة الطلب المرسل من العقدة الرئيسية "Master" إلى إحدى العقد التابعة "Salve" كما يظهر في الشكل 11:



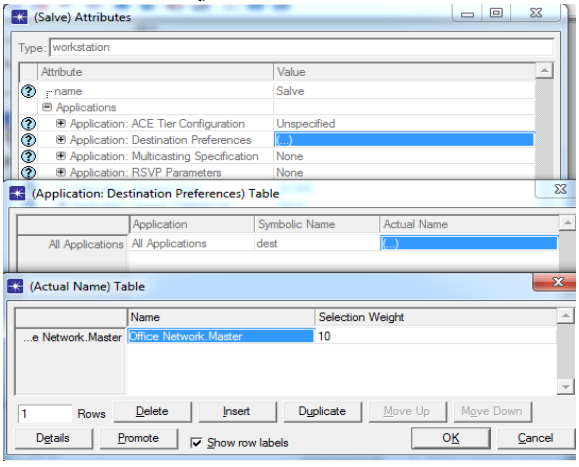
الشكل (11) التطبيقات المستخدمة في شبكة MODBUS الصناعية.

خصائص العقدة (Master): وهي من النوع "workstation" وهذا النوع يتيح للعقدة تحديد ملف التعريف المرغوب ومن خلال خصائصها "Attributes" تم تحديد ملف التعريف "Modbus" المحدد في الأيقونة "Profile"، وتم وضع الخاصية "Application: Supported Profiles" على " MODBUS Profile" كما يظهر في الشكل12.



الشكل (12) خصائص العقدة Master في OPNET.

خصائص العقدة (Salve): وهي من النوع "workstation" أيضاً وهذا النوع يتيح للعقدة تحديد ملف التعريف المرغوب ومن خلال خصائصها "Attributes" تم تحديد ملف التعريف "Modbus" المحدد في الأيقونة "Profile"، وتم وضع الخاصية " Applicastion: Supported Services" على MODBUS Profile"، كما وتم ضبط الخاصية " Application: Destination Preferences" على الوضع Office Network: "Master" ليكون الجهاز الرئيسي هو وجهة الارسال للجهاز التابع عند الرد على الطلب كما يظهر في الشكل 13.



الشكل (13) خصائص العقدة Salve في OPNET.

خصائص الناقل (RS485): هو الناقل الرئيسي في شبكة MODBUS، وتمّ تحديد نوعه "Coax-adv" وهذا النوع يُتيح عدة سمات نستطيع من خلالها رصد العديد من البارامترات الهامة مثل (زمن تأخير انتقال الأطر، والانتاجية، والاستخدامية) وغيرها من البارامترات الهامة المرتبطة بالأداء العام للشبكة، ونذكر فيما يلي السمات التي تم ضبطها ليُمثل هذا الناقل خصائص ناقل RS485 المُستخدم في شبكات MODBUS الصناعيّة.

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

السمة (data rate): تمّ ضبطها على القيمة (19200 bps).

السمة (delay): تمّ ضبطها على القيمة (0.0001) ثانية.

السمة (packet format): تمّ ضبطها على القيمة (Modbus).

السمة (thickness): تمّ ضبطها على القيمة (2) ملم.

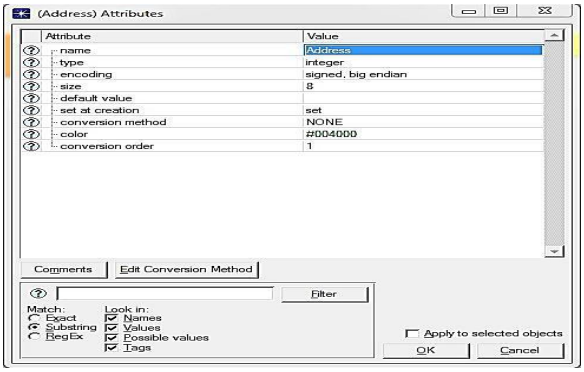
إطار MODBUS: يُتيح برنامج OPNET بناء إطار برتوكول اتصال معين، وتمّ تشكيل إطار MODBUS وفق الخطوات الآتية:

من قائمة "File" نختار "New" ومن ثمّ نختار محرر الأطر "Packet Format"، من النافذة نختار "Create New Field".

نقوم بإنشاء إطار MODBUS المؤلف من أربعة حقول كما في الشكل 14.

الشكل (14) حقول إطار MODBUS الأربعة في برنامج OPNET.

نقوم بتحرير أربعة حقول ومن ثم نحدد خصائص كل حقل "attribute" كما في الشكل 15 والذي يُظهر خصائص الحقل "Address".



الشكل (15) خصائص حقل "Address" في إطار MODBUS-RTU.

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

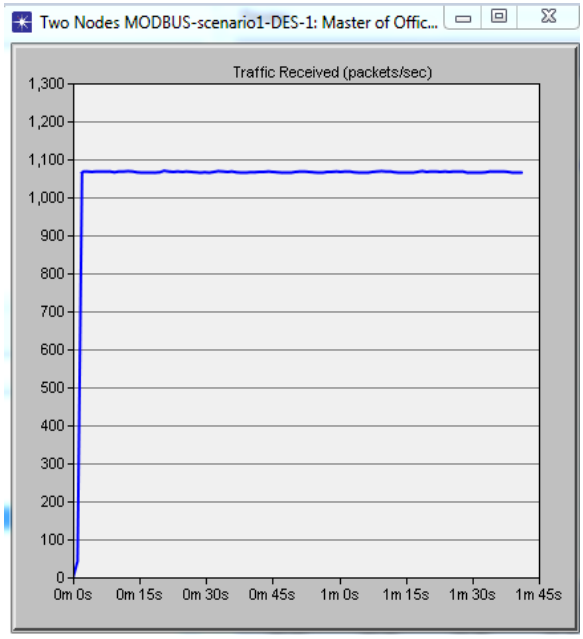
حقل "Data" يتم ضبط خاصية "Type" على النوع "Packet" ومن ثم اختيار "Inherited"، حيث يتيح خيار "Inherited" تعيين حجم الحقل على حجم البيانات الفعلي وفق التطبيق المستخدم، ويتم ضبط الترميز "encoding" على النوع "singed. Big endian" الذي يحافظ على تسلسل البيانات المُرسل بجهة الاستقبال.

نقوم بحفظ الإطار باسم "Modbus" ومن ثم نعود إلى خصائص ناقل RS485 ونقوم بضبط الخاصية " Packet Formats" على الوضع "Modbus" حيث نقوم بجعلها "supported".

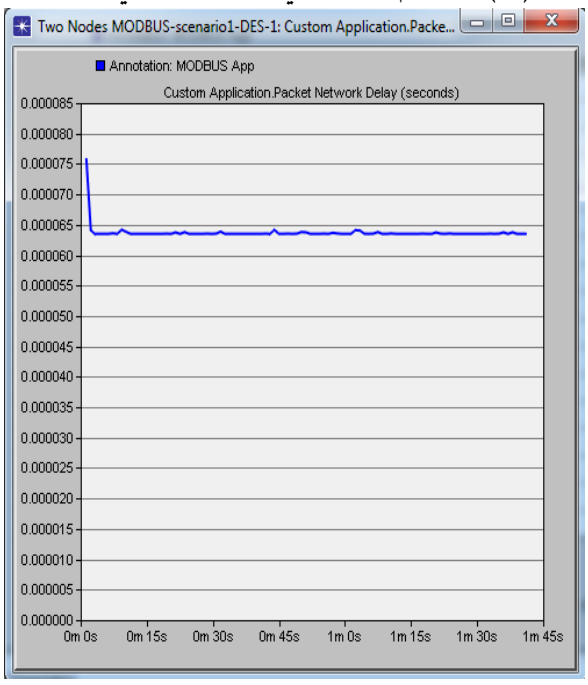
البارومترات المرتبطة بأداء الشبكة الصناعية الاختبارية:

1. (Packet Network Delay): وهو من النوع (Global Statistics) ويُمثل 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 ويُقاس هذا التأخير الزمني بالثانية ويتناسب عكساً مع أداء الشبكة فبنقصانه يزداد الأداء.
2. (Traffic Received): وهو من النوع (Node Statistics) ويُمثل عدد الرزم المستلمة من قبل العقدة بواحدة الزمن ويقدر [Packets/Sec] ويتناسب طرداً مع أداء الشبكة فبزيادته يزداد الأداء.

تم تشغيل المحاكاة لمدة (100) ثانية وحصلنا على الشكلين 16 و17.



الشكل (16) عدد الرزم المستلمة في العقدة الرئيسية في واحدة الزمن.



الشكل (17) التأخير الزمني للإطار المرسل.

النتائج الخاصة بنموذج التحقق:

من خلال مقارنة النتائج التي حصلنا عليها في المحاكاة باستخدام برنامج OPNET ونتائج الدارة العملية نلاحظ تطابق كبير بنسبة خطأ لا تتجاوز (% 0.25) مما يؤكد صحة النموذج المُصمّم وقابلية برنامج OPNET في محاكاة الشبكات الصناعية و هو ما يعكس تحقيق نتائج البحث، مما يسهل علينا فيما بعد بناء شبكات ذات عقد أكثر و بأشكال مختلفة وتغيير عوامل تؤثر على بارامترات الأداء ودراسة أثر هذه التغيرات على الأداء و هو ما ينعكس على أليات تطوير نماذج مشابهه تمكننا من نمذجة الشبكات الصناعية بشكل عام، وبالتالي تحسين جودة الخدمة للشبكة الصناعية المدروسة من كافة النواحي و إيجاد أليات جديده للتطوير بما يتناسب مع أنظمة التشغيل المستحدثة و البروتوكولات الجديدة في عالم الشبكات الصناعية.

التوصيات والآفاق المستقبلية:

تنفيذ دارات عملية للمقارنة بين بارامترات أداء برتوكولات صناعية أخرى.

دراسة عوامل أخرى مؤثرة في بارامترات الأداء من خلال النمذجة.

استخدام برنامج OPNET في نمذجة شبكات واقعية ودراسة وتحليل أداءها.

التمويل: هذا البحث ممول من جامعة دمشق وفق رقم التمويل (501100020595).

References:

1. Ferrari P., Flammini A., Marioli D., Taroni A. and F. Venturini,2007- New Simulation Models to Evaluate Performance of PROFINET IO Class 1 Systems. IEEE, University of Brescia, Dept. of Electronics for Automation,Brescia, Italy,p 237-242.

2. 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.

3. Lu Yang,H 2012. Unloking The Power of OPNET Modeler. CAMBRIDGE, UK, 253p.

4. Mangkalajan. S, Koodtalang.W, Sangsuwan.T and Pudchuen.N,2019 - Virtual Process Using LabVIEW in Combination with Modbus TCP for Fieldbus Control System. IEEE International Conference on Control System, Computing and Engineering ,Penang, Malaysia.p 21-24.

5. Modbus Application Protocol Specification ,V1.1b3, April 26, 2012. Available at https://modbus.org/docs/Modbus_Application_Protocol_V1_1b3.pdf

6. MODBUS over serial line specification and implementation guide V1.02. 2016 Available at https://modbus.org/docs/Modbus_over_serial_line_V1_02.pdf

7. Shukla.P , Singh.S , Joshi.T, Kumar.S, Kelkar.S , Das.M, 2017- Design and Development of a MODBUS Automation System for Industrial Applications, IEEE, Bengaluru, India,p 515-520