تحسين أمن الاتصالات والإدارة المثلى لبروتوكول Fieldbus في أنظمة التحكم الإشرافي باستخدام DNP3-OPC

د.م مسعود الأتاسي. استاذ مساعد في قسم هندسة الميكاترونك. جامعة حمص.

الملخص

تعتبر برتوكولات Fieldbus بأنواعها المختلفة أساساً لإدارة الشبكات الصناعية حيث تضمن نقل بيانات الشبكة الصناعية بشكل موثوق بين عقد الشبكة المتقاربة أو المتباعدة جغرافياً. ويرتبط أداء الشبكات الصناعيّة بمجموعة من البارامترات مثل زمن تأخير الإطار، استخدامية الشبكة، إنتاجية الوصلات، معدل ارسال الأطر في الثانية وغيرها، حيث تتأثر هذه البارامترات بعدة عوامل نذكر منها عدد العقد، حجم الإطار، طوبولوجيا الشبكة، نوعية خطوط النقل، نوعية الأجهزة البينية التي تربط بين عقد الشبكة وغيرها، ويعكس الأداء العالي للشبكة الصناعيّة قدرتها على تلبية مُتطلبات الزمن الحقيقي وجودة الخدمة التي تُلبي الاحتياجات المطلوبة.

وطريقة دمج أنظمة التحكم الإشرافي SCADA (Supervisory Control And Data Acquisition) باستخدام بروتوكول اتصال المنصة المفتوحة OPC (Open Platform Communication) يسمح بتأمين إدارة مثلى للشبكة، حيث تربط الوحدات الفرعية RTUs لنظام السكادا مع الوحدة الأساسية Master عبر روابط الاتصالات الموزعة بعيدة المدى DNP3 (Distributed Network Protocol) ومن ميزاته أنه موثوق ضد البيئات الصاخبة وتداخل الإشارات. وهو بروتوكول اتصال يستخدم على نطاق واسع في محطات الطاقة الكهربائية والمياه والغاز، وخاصة في المراقبة والتحكم عن بعد في المعدات والأجهزة. ومن سيئاته انه معرض لعدد من الهجمات مثل العبث بالأجهزة أو هجوم الرجل في المنتصف، لذلك اقترحنا أول تحسين لأمن المعلومات DNP3 باستخدام خوارزمية Diffie-Hellman. تم محاكاة هذه الخوارزمية باستخدام لغة بايثون، ولاحظنا أن المستخدمين حصلوا على نفس قيمة المفتاح على الرغم من وجود متنصت

على الخط، وعلى الرغم من حصولها على قيم p، g، A، B، إلا أنها لم تستطع الحصول على المفتاح السري K، لأنها لم تعرف القيم السرية المختارة a(160، 212) وb(114، 601) من قبل المرسل والمستقبل. تم تحقيق التحسين الثاني باستخدام التشفير غير المتماثل من خلال تطبيقه على شبكة Modbus لتوقيع الشهادات الرقمية ومفاتيح التبادل باستخدام أداة OpenSSL. يوفر هذا النوع من التشفير وظائف آمنة في تبادل البيانات، مما يحل مشكلة القنوات غير الآمنة ويحمي من الاختراق.

وتم أيضاً بناء نموذج شبكة صناعية تستخدم بروتوكول Modbus ذو الناقل التسلسلي وهو أحد أنواع برتوكولات Fieldbus الصناعية وباستخدام محاكي الشبكات OPNET، بإجراء عملية تحليلية للنتائج وبهدف تحديد القيم الأفضل للعوامل المؤثرة في الأداء العام للشبكة الصناعيّة الحقلية عندما يتغير حجم البيانات وعدد الأطر للوصول للإدارة المثلى لبروتوكولModbus .

وتوصلنا إلى أن زيادة استخدامية الناقل تكبر بزيادة عدد العقد في الشبكة وحجم الإطار المرسلة، ولكن بالمقابل يزداد زمن التأخير، لذلك لتحقيق متطلبات الزمن الحقيقي للقيمة الحدية 0.5 ثانية للشبكة الصناعيّة Modbus من أجل حجم البيانات المرسلة 256Byte، يجب عدم تجاوز عدد العقد لقيمة (1000 عقدة). أما أهمية البحث فتكمن أولاً في تحقيق أمن معلومات وحماية الشبكة وإزالة مخاطر الهجمات وثانياً في معرفة عدد العقد الأعظمي لأخذ مؤشر عن زيادة الاستخدامية للشبكة مما يُسبب زيادة في الأداء العام للشبكة.

الكلمات المفتاحية: SCADA، بروتوكولDNP3 ، أمن الشبكات الصناعية، خوارزمية ديفي–هيلمان، بروتوكولModbus ، استخدامية الشبكة، التشفير غير المتناظر،Openssl .

Improved communications security and optimal management of the Fieldbus protocol in SCADA systems using DNP3-OPC

Dr. Massoud ATASSI. Associate Professor at Mecatronics Engineering Department – Homs University

ABSTRACT

Fieldbus protocols of various types form the basis for industrial network management, ensuring reliable transmission of industrial network data between nearby or geographically distant network nodes. The performance of industrial networks relate with a set of parameters such as frame latency, network utilization, link throughput, frame rate per second, etc. Several factors affect these parameters, including the number of nodes, frame size, network topology, transmission line quality, and the type of interface devices that connect the network nodes. The high performance of an industrial network reflects its ability to meet real-time requirements and the quality of service that meets the required needs.

The integration of SCADA (Supervisory Control and Data Acquisition) systems using the Open Platform Communication (OPC) protocol allows for optimal network management, as SCADA sub-units (RTUs) connect to the master unit via DNP3 (Distributed Network Protocol) communication links. Its advantages include reliability in noisy environments and signal interference. It is a communication protocol widely used in power, hydraulic, and gas plants, particularly in the remote monitoring and control of equipment and devices. One of its disadvantages is that it is vulnerable to several attacks, such as hardware tampering or man-in-the-middle attacks. Therefore, we proposed the first improvement of DNP3 information security using the Diffie-Hellman algorithm. This algorithm was simulated using the Python language, and we noticed that users obtained the same key value despite the presence of an eavesdropper on the line, and although it obtained the values of p, g, A, B, it could not

obtain the secret key K, because it did not know the secret values chosen a(160, 212) and b(114, 601) by the sender and the receiver. The second improvement was achieved by using asymmetric cryptography by applying it on the Modbus network to sign digital certificates and exchange keys using the OpenSSL tool. This type of encryption provides a secure feature in data exchange, which solves the problem of insecure channels and protects against hacking.

An industrial network model is realized using the Modbus serial bus protocol. Using the OPNET network simulator, the results were analyzed to determine the optimal values of the factors that affect the overall performance of the industrial field network when the data volume and the number of frames change, thus achieving optimal management of the Modbus protocol. We found that bus utilization increases with the number of nodes in the network and the size of the transmitted frame. However, the delay time also increases. Therefore, to achieve the real-time threshold of 0.5 seconds for an industrial Modbus network with a transmitted data size of 256 bytes, the number of nodes must not exceed 1,000 nodes. The importance of the research lies, firstly, in achieving information security and protecting the network to eliminate the risk of attacks. Secondly, it defines the maximum number of nodes to provide an indication of increased network utilization, which leads to an increase in overall network performance.

Keywords: SCADA, DNP3 Security, Diffie-Hellman Algorithm, Modbus, Modbus Protocol, OPNET, Network Uutilization. Asymmetric Cryptography, Openssl.

مقدمة

يعتبر برتوكول الشبكة الموزعةDNP3 أحد حلول أنظمة الاتصال بين الأجهزة التي تستخدم برتوكولات Fieldbus بأنواعها المختلفة وهذه الطريقة أساسية لإدارة الشبكات الصناعية في نظام SCADA، لأننا نضمن نقل بيانات الشبكة الصناعية بشكل موثوق بين عقد الشبكة المختلفة المتقاربة أو المتباعدة جغرافياً وخلال البيئات الصاخبة والإشارات المتداخلة. لكن هذه

الطريقة سيئتها أنها غير محمية ومعرضة للهجمات والتنصت على المعلومات، لذلك بروتوكول الاتصال الموزع DNP3يتطلب تحسيناً في أمن نقل معلوماتها.

في البدايات صمم DNP3 خصيصاً لتطبيقات الاتصالات في نظام الـ SCADAوتم استبداله لاحقاً ببروتوكول IEC61850 المحسن لاستخدامه في أوروبا. في بحثنا استخدمنا خوارزمية Diffie-Hellman والتشفير الغير متناظر asymmetric cryptography لتحقيق أمن المعلومات وحماية الشبكة من القرصنة وإزالة مخاطر الهجمات. وقمنا أيضاً باستخدام محاكي الشبكات OPNET لإجراء عملية تحليلية لنتائج شبكة صناعيّةModbus لمعرفة عدد العقد الأعظمي اللازم لتحقيق متطلبات الزمن الحقيقي ومعرفة أفضل استخدامية للشبكة من أجل زيادة أداء العام.

يتم استخدام DNP3-OPC Server في أنظمة الأتمتة واسعة النطاق والتحكم الصناعي، بمثل تلك الموجودة في محطات الطاقة، ومرافق معالجة المياه، وعمليات النفط والغاز. ويمكن استخدامها أيضًا في التطبيقات الأخرى التي تتطلب الوصول إلى البيانات ومراقبتها. ويعد DNP3-OPC Serverمن الحلول البرمجية التي توفر الاتصال بين الأجهزة من مختلف الشركات الصناعية باستخدام بروتوكول DNP3 وخوادم OPC .حيث يقوم خادم DNP3-OPC بتحويل البيانات من بروتوكول DNP3 إلى بروتوكول OPC وبالعكس. بدون هذه الحلول، لن تتمكن الأجهزة التي تستخدم بروتوكول DNP3 من الاتصال بالأنظمة والتطبيقات التي تستخدم بروتوكولات OPC. هذه الحلول المتكاملة السلسة بين الأجهزة والأنظمة المختلفة تعزز الكفاءة والوظائف الشاملة للنظام[2] .

1. هدف البحث

- تحسين أداء المنظومة الإشرافية والإدارة المثلى وذلك من خلال بناء نموذج لشبكة صناعية Modbusالصناعية باستخدام محاكي الشبكات OPNET، ثم القيام بتحليل النتائج بهدف تحديد القيم الأفضل والقيم الحرجة التي تُخرج الشبكة الصناعيّة عن تلبيتها لمتطلبات الزمن الحقيقي الأعظمي والذي يساوي 0.5 ثانية لبروتوكول Modbus[21].

- تحسين الأمان في أنظمة SCADA والتي تعتمد على بروتوكول الاتصالات الموزعة DNP3 وذلك من أجل التحكم في الزمن الحقيقي ومراقبة نظام واسع النطاق الموزع بواسطة بناء معمارية آمنة لبروتوكول DNP3 باستخدام خوارزمية ديفي هيلمان وذلك أثناء تراسل البيانات بين محطات Modbusومن ثم استخدام شهادات رقمية موقعة ومشفرة باستخدام المفاتيح غير المتناظرة والتحقق باستخدام الأداة OpenSSL، وهذا يحل مشكلة القناة الغير آمنة والقرصنة. ونلخص أهم النقاط الواجب حلها في هذا البحث هي:

–حماية المعلومات في بروتوكول DNP3بين المرسل والمستقبل من مخاطر الهجمات وهجوم الرجل في المنتصف وأيضاً مصادقة الشهادات الرقمية وتوقيعها وتشفيرها باستخدام المفاتيح غير المتناظرة بين الوحدات الطرفية clients والمحطات الرئيسية servers داخل شبكةModbus

– معرفة عدد العقد الأعظمي لتحقيق متطلبات الزمن الحقيقي للشبكة الصناعيّة Modbus ذو الناقل التسلسلي مما ينعكس إيجابياً على الأداء العام للشبكة.

2. مواد وطرق البحث

1.2 أدوات البحث

تمّ استخدام أداة محاكاة الشبكات OPNET، ولغة البرمجة Python والأداة OpenSSL من أجل إنجاز هذا البحث:

1) محاكي الشبكات OPNET: هي أداة محاكاة للشبكات واختصار لـ Optimized Network Engineering Tools، أي أداة هندسية الشبكات المحسنة .ساعدت هذه الأداة في بناء نماذج شبكات صناعيّة واقعية وأخرى افتراضية من أجل تحديد العوامل المؤثرة في الأداء بهدف تحسينه. [3]
2) لغة Pythonلبرمجة خوارزمية Diffie Hellman (DH) كطريقة لشرح تبادل مفاتيح التشفير بشكل آمن عبر قناة الاتصالات لبروتوكول DNP3 والمخصص لتطبيقات أنظمة SCADA.[4, 5, 6]

3) OpenSSL هو تطبيق مفتوح المصدر يحتوي على أدوات التشفير ويستعمل بروتوكولات طبقة النقل الامن .مكتبته الأساسية مكتوبة بلغة البرمجة C لإجراء اختبارات بين خادمClient وعميل SSL/TLS-Server، إصداراته متاحة لمعظم أنظمة التشغيل، وفعال لتوقيع وتشفير الرسائل[27] .

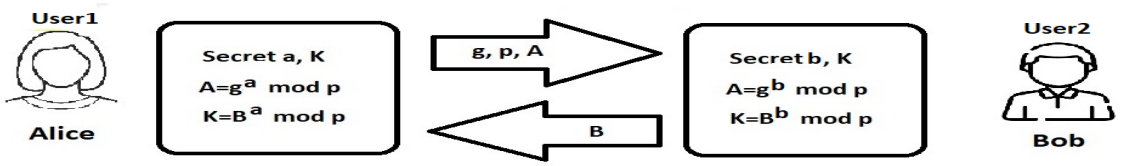
2.2محاكي الشبكات OPNet:

هو أحد أشهر المحاكيات الشبكية وأكثرها شعبية بسبب استخدامه الكبير والواسع في مجالي الصناعة والأبحاث الشبكية، وهو نظام هندسي قادر على محاكاة شبكات الاتصال الضخمة مع نمذجة تفصيلية للبرتوكولات، والتطبيقات، والأجهزة وتحليل الأداء. ميزته أنه يمتلك واجهات رسومية قوية جداً للنموذج، ومحاكاة ديناميكية، ونواة محاكاة معتمّدة على جدولة للأحداث، وأدوات تحليل متكاملة مضمنة داخله، وهرمية للبيانات، ببساطة هو أداة محاكاة للشبكات تتيح تعريف طوبولوجيا الشبكة، العقد، التوصيلات، التطبيقات وغيرها. كما يمكن للمستخدم أن يُعرّف العمليات التي يمكن أن تحدث في عقدة جزئية وخصائص توصيلات الإرسال، وبعد ذلك تنفذ المحاكاة وتحلل النتائج لأي عنصر في شبكة المحاكاة. كما أنّ OPNET هو بيئة محاكاة غرضيّة التوجّه يحقّق كل المتطلبات ويعدّ محاكي الشبكة الأكثر فعالية للأغراض العامة، ويشمل أيضاً على أدوات التحليل المخصصة لتفسير وتركيب الخرج ويعتمّد محاكاة الأحداث المتقطعة. علاوةً على ذلك فإنّه يتضمن دعم للغة الـ C مزوداً بالقدرة على تحقيق أي مهمة أو برتوكول اتصال ولمجال واسع من أنظمة الاتصال بدءاً من شبكات LAN البسيطة حتى شبكات الأقمار الصناعيّة مدعومة من قبل OPNET [7, 8].

3.2 خوارزمية تبادل المفاتيح ديفي-هيلمان(D-H) Diffie-Hellman key exchange

بروتوكول ديفي–هيلمان هو بروتوكول لتبادل المفاتيح في علوم الكمبيوتر يسمح لطرفين بمشاركة مفتاح سري بشكل آمن عبر قناة غير آمنة دون الكشف عن المفتاح نفسه. يتضمن استخدام خوارزمية تبادل المفاتيح ديفي–هيلمان D–H الأعداد الصحيحة الأولية والعشوائية الكبيرة والحسابات المعيارية لإنشاء مفتاح سري مشترك بين الطرفين.

مثال خطوات خوارزمية ديفي-هيلمان[9]: هناك شخصان معروفان (user1)Alice و (user2)Bobوعدد أولي **p** وجذر بدائي**g**. نفرض أنBob و Alice يريدان تبادل مفتاح حسب الشكل (2.1):



الشكل (2.1):Diffie-Hellman key exchange Protocol

- يختار أليس وبوب معًا، على سبيل المثال،**g=7 p=11** .
- تختار أليس(**A**) **a= 3** لحساب g^a:

$$A= g^3 \text{mode } p$$

$$A = 7^3 \text{ mod } 11$$

$$A=343 \text{ mod } 11$$

$$A=2$$

- يختار بوب(**B**) **b= 5** لحساب g^b:

$$B=g^5 \text{ mode } p$$

$$B = g^y= 7^5= 16807 \equiv 15 \text{ mod } 11$$

$$B=10$$

- تبادل القيم **A=2** و **B=10** لحساب قيمة المفتاح السري **K**

$$K=B^a \text{ mod } p=10^3 \text{ mod } 11=10 \quad : \text{Alice}$$

$$K=A^b \text{ mod } p=2^5 \text{ mod } 11=10 \quad : \text{Bob}$$

نلاحظ أن المستخدمين حصلوا علة نفس قيمة المفتاح رغم وجود المتصنت على الخط ورغم أنه حصل على قيم **p, g, A, B** لكنه لن يستطع الحصول على المفتاح **K** الصحيح لأنه لا يعرف قيم المختارة a, bمن قبل اليس وبوب ولو حسابياً. لذلك طريقة ديفي-هيلمان D-Hتحترم السرية التامة المستقبلية (PFS: Perfect Forward Secrecy)، وهي إحدى

ميزات بروتوكولات اتفاقية المفاتيح المحددة التي تقدم ضمانات بأن مفاتيح الجلسة لن يتم المساس بها حتى في حالة المساس بالأسرار طويلة الأمد المستخدمة في تبادل مفاتيح الجلسة، مما يحد من الضرر. ولأن طريقة D-H تقوم بتوليد القيم السرية a ,b بكل جلسة جديدة وهذا ما يسمى DHE والذي يشير إلى " ديفي-هيلمان المؤقتEphemeral " وهذا يعني أن المفتاح المستخدم في تبادل المفاتيح يتم استخدامه مرة واحدة فقط ثم يتم حذفه.

4.2 دراسة مرجعية

– الدراسة المرجعيّة [11] تمّ فيها تحليل أداء برتوكول الاتصال Modbus/TCP الصناعي وركّز البحث على تقييم الأداء من خلال زمن الاستجابة T مُرتبطاً بعدد العقد والطوبولوجيا، وأظهرت النتائج أنّ الطوبولوجيا النجميّة ذات زمن استجابة ثابت تقريباً مع زيادة عدد العقد وبتالي مُناسبة لنظم الزمن الحقيقي. هذا البحث لم يحدد عدد العقد الأعظمي بحيث زمن التأخير لا يتجاوز الزمن الحقيقي 0.5 ثانية في بروتوكول Modbus ذو النقل التسلسلي[21] من أجل حجم البيانات المرسلة 256Byte، وهذا ما تم دراسته وتحليله في بحثنا.

– الدراسة المرجعيّة [12] قدمت تحليل لأداء شبكات ايثرنت الصناعيّة باستخدام برنامج المحاكاة OPNET، ففي البداية تمّ التأكد من قابلية برنامج OPNET في نمذجة الشبكات الصناعيّة من خلال مقارنة نتائج تجارب شبكة عملية مع نتائج المحاكاة ومن ثمّ تمّ دراسة تأثير عدد من العوامل على الأداء مثل طول الحزمة وعدد العقد ومعدل إنتاجية العقد ، وقدمت هذه الدراسة فائدة كبيرة حيث أثبتت قابلية برنامج OPNET في محاكاة الشبكات الصناعيّة من خلال مقارنة نتائج المحاكاة مع قيم تجريبية إلا أنّها عانت أيضاً من العموميّة فلم تعرض آلية نمذجة العقد المُستخدمة في الشبكة المدروسة و خصائص كل منها وحجم البيانات وعدد الأطر وهذا تم في بحثنا من خلال بناء نموذج شبكة صناعية تستخدم بروتوكول Modbus وباستخدام محاكي الشبكات OPNET بهدف تحسينها ومعرفة خصائصها وزيادة استخدامية الناقل بشكل كبير بزيادة عدد العقد في الشبكة لعدد محدد تم معرفته بفضل الاختبارات.

– هدفت الدراسة [13] إلى التحقق من القيود والعيوب التي تعيب بروتوكول الاتصالات DNP3المستخدم بشكل شائع في SCADA، والتحقيق في الهجمات الإلكترونية التي تستغل نقاط الضعف في هذا البروتوكول، وتقديم توصية لحماية شبكات SCADA ومنع العواقب المدمرة.

– أما الدراسة المرجعية [14] قدمت اختبار لمعالجة تحليل الثغرات الأمنية واختبار الاختراق الذي يشمل على هجوم رجل في المنتصف وتحليل مختلف التهديدات ونقاط الضعف في بروتوكول DNP3 الذي يعمل في تطبيق SCADA. النتائج التي حصل عليها الباحث تبين أنه يمكن اكتشاف هذه الهجمات بنجاح باستخدام بنية تستند إلى خوارزمية (DCA: Dendritic Cell Algorithm) المعتمدة على نظام المناعة الاصطناعي (AIS: Artificial Immune System)، وأن اهم نقاط الضعف في DNP3 هي: هجوم رجل في الوسط، تعديل حزمة DNP3 وتعطيل الرسائل.

–في الدراسة المرجعيّة [22] قام الباحث بإجراء اختبار الاختراق باستخدام سيناريوهات الهجوم المختلفة في بيئة افتراضية من خلال محاكاة تتضمن بروتوكول DNP3. تم معالجة تحليل الثغرات الأمنية واختبار الاختراق الذي يشمل على هجوم رجل في المنتصف (MITM). تضمنت تقنيات الفحص الذي استخدمها الباحث إجراء فحص صحي للشبكة، ثم إجراء تقييم نقاط الضعف في DNP3 والهجمات الأمنية والاكتشافات والوقاية والتدابير المضادة. قام الباحث بتحليل مختلف التهديدات ونقاط الضعف في بروتوكول DNP3 الذي يعمل في تطبيق SCADA كجزء من الشبكة الذكية باستخدام النماذج الأولية والبيئات الافتراضية، كما تم إجراء اختبار كفاية الأمان باستخدام أربعة سيناريوهات للهجوم الأساسي بما في ذلك نوع هجمات رفض الخدمة (MITM). لاحظ الباحث أن استخدام النماذج النظرية لهجمات الشبكة الذكية باستخدام نظرية اللعبة أدت إلى تحسين استراتيجيات الكشف وذلك من خلال الحد من التهديدات الالكترونية في بيئة DNP3.

–أما الدراسة المرجعية [23] ناقش الباحث الهجمات التي تستهدف الشبكات الذكية التي تستخدم بروتوكول DNP3، وكيف يمكن اكتشاف هذه الهجمات باستخدام الإصدارات الحتمية لخوارزمية الخلايا الجذعية (DCA) والتي تعد خوارزمية قائمة على نظام المناعة الصناعي (AIS) لتقييم فعالية DCA. عمد الباحث إلى إنشاء مجموعة بيانات اختبار من خلال تنفيذ هجمات متنوعة ثم تنفيذها في بيئة الشبكة الذكية DNP3.

في الدراسة المرجعيّة [28]تقدم نهجًا توضيحيًا لدمج تقنية توزيع المفاتيح الكمومية (QKD) في مكتبة .Openssl ومعرّفًا التشفير غير المتماثل كأحد تقنيات التشفير الرئيسية المستخدمة في الاتصالات والأنظمة. على الرغم من فوائد هذه الطريقة وفعاليتها، إلا أن لها بعض المشكلات

المعقدة المتعلقة بتوزيع المفاتيح الكمومية، لذلك في التشفير الغير متناظر لا يتم نقل المفتاح السري عبر الشبكة وحتى إذا سُرق المفتاح الخاص، لا يمكن فك تشفير الجلسات السابقة وهو سهل التطبيق وحماية مناسبة

بعض الأبحاث السابقة أكدت أنه من الأفضل دمج عدة استراتيجيات للأمان بدلاً من استخدام استراتيجية واحدة أو استخدام طرق مثل DCA، MITM وAIS مما يعطي أمان أكثر للنظام ولكن على حساب تعقيد الخوارزميات. أما خوارزمية ديفي هيلمان فهي طريقة معيارية أثبتت فعاليتها في العديد من بروتوكولات الانترنت. مثل (Internet Protocol Security)، (Secure Shell) و Transport Layer Security (TLS). ويعتبره البعض الحل الأكثر كفاءة وسهل التنفيذ. لكن لا يزال البعض الآخر يفضل خوارزميات أخرى نظراً لكونها أوسع استخداما منه، مثل RSA التي تستخدم إلى جانب تبادل المفاتيح البصمات الإلكترونية.

في هذا البحث عملنا على تحسين أمن الاتصالات لبروتوكول DNP3 باستخدام خوارزمية سهلة وفعالة وهي ديفي هيلمان لمنع هجوم رجل في الوسط، وتم تحسين أمن شبكةModbus بمصادقة الشهادات الرقمية وتوقيعها وتشفيرها باستخدام المفاتيح غير المتناظرة بين Clients وServers. وتم تحديد أيضا القيم الأفضل للعوامل المؤثرة في الأداء العام للشبكة الصناعيّة الحقلية عندما يتغير حجم البيانات Byte256 بالإطار ومن أجل 1000 عقدة محققاً متطلبات الزمن الحقيقي (0.5) ثانية، من خلال بناء نموذج شبكة صناعية تستخدم بروتوكول Modbus وباستخدام محاكي الشبكات OPNET بهدف تحسينها ومعرفة خصائصها.

3. الناقل الحقلي(Fieldbus):

هو عبارة عن ناقل اتصال رقمي ثنائي الاتجاه بين الأجهزة الحقليّة الذكية، وتُعد بمثابة شبكة محلية مُخصّصة للأتمتة الصناعيّة، حيث تُستبدل شبكات التحكّم المركزية بشبكات التحكّم الموزّعة والتي تربط الأجهزة الحقليّة. هناك العديد من أنواع البرتوكولات الحقليّة المُستخدمة اليوم، ويعتمّد النوع الذي سيتمّ استخدامه على نوع المصنع، ونذكر منها (Foundation Fieldbus وPROFIBUS وDeviceNet وControlNet وInterbus وHART وAS-i وMODBUS وCAN Bus وEthernet وLon Works وWorldSIM). إنّ تطبيق برتوكول الناقل الحقلي في أتمّتة العمليات الصناعيّة له ميزات عديدة، فهو يؤدي لتحكم أفضل في

العملية إلى جانب زيادة إنتاجية المنتج[10]. وأهم الخصائص التي تميّز شبكات (Foundation Fieldbus) الصناعيّة هي:

- برتوكول أتمتة وتحكم بالعمليات الرقمية ثنائي الاتجاه.
- تمتلك المنظومة ثلاث طبقات: (طبقة فيزيائية – طبقة اتصال بيانات – طبقة التطبيقات) كما تمتلك طبقة إضافية ثامنة تدعى طبقة المستخدم (USER LAYER).
- لديها بنية ثنائية المستوى مكوّنة من مستوى منخفض (H1) ومستوى أعلى (H2)، ويعمل المستوى (H1) بسرعة ([Kbps] 31.25) بينما (H2) يعمل بسرعة (12.5 [Mbps]).
- يدعم الاتصالات المجدولة وغير المجدولة.
- تدعم التوافقية ويمكن للأجهزة المختلفة الموجودة من قبل مصنعين مختلفين أن تتصل بسلاسة مع بعضها.

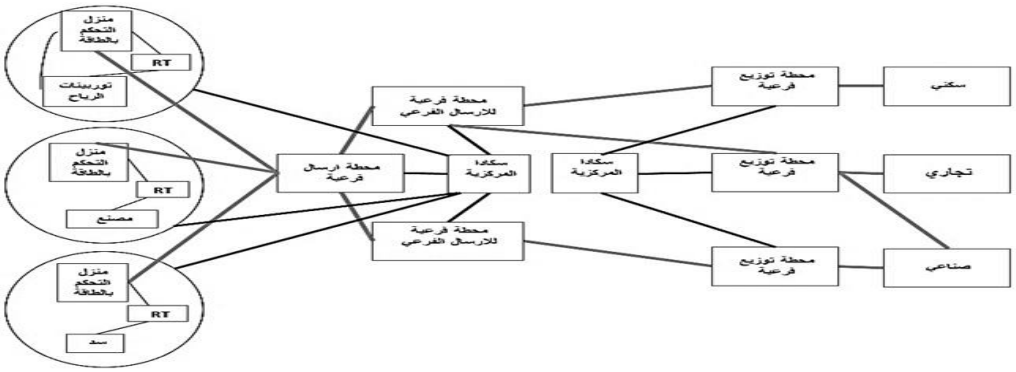
تعتمد شبكات Foundation Fieldbus على نموذج OSI (Open Systems Interconnection) المرجعي، ويتكون نموذج Fieldbus من ثلاث طبقات:(PHL ، DLL، APL)، فبالنسبة للطبقة السابعة APL (Application Layer) تُقسم إلى طبقتين فرعيتين هما: طبقة مواصفات رسائل FMS (Fieldbus Message Specification) وطبقة الوصول الفرعي FAS (Fieldbus Access Sub-layer)، وهناك طبقة فوق الطبقة السابعة تسمى طبقة تطبيق المستخدم، وهذه هي الطبقة الثامنة من نموذج Foundation Fieldbus، ولا يتمّ استخدام الطبقات من 3 إلى 6 الموجودة في OSI. تستقبل الطبقة الفيزيائية PDU (Physical Data Unit) البيانات من طبقة اتصال البيانات حيث يتمّ تحويلها إلى إشارة فيزيائية ونقلها على ناقل Fieldbusبوسيلة كهربائية أو ضوئية. [15]

4. لمحة عن بروتوكول DNP3 المستخدم في البحث:

DNP3 أو بروتوكول الشبكة الموزعة النسخة الثالثة هو معيار اتصال يعرف الاتصالات بين المحطة الرئيسة ووحدات القياس البعيدة RTUs وغيرها من الأجهزة الالكترونية الذكية IEDs. تم تطويره لتحقيق التوافقية بين الأنظمة في المجالات الصناعية، فجاء مخصصاً

لتطبيقات أنظمةSCADA، هذا يتضمن تحصيل المعلومات وإرسال تعليمات التحكم بين حاسوبين منفصلين فيزيائياً، وصمم لإرسال رزم صغيرة نسبياً من البيانات ولكن بطريقة موثوقة من خلال رسائل تصل بتسلسل قطعي، وهذا الاختلاف الأساسي عن بروتوكولات الأغراض العامة كـ FTP، والذي هو جزء من بروتوكول TCP/IP الذي يستطيع إرسال ملفات كبيرة الحجم ولكن بطريقة ليست متوافقة مع نظم سكادا. أهم مميزات بروتوكول DNP3 هي المعايير المفتوحة التي تمكن من عمل توافق بين تجهيزات من مصنعين مختلفين، هذا يعني أن المستخدم يستطيع شراء محطة رئيسة من مصنع ما ويستطيع جلب وحدات RTUs من مصنع أخر، وبدورها تمتلك هذه الوحدات مرحلات تحكم متصلة بها هي أجهزة إلكترونية ذكية تستعمل برتوكول DNP3، وكل هذه التجهيزات يمكن أن تأتي من شركات ومصنعين مختلفين من بداية التصميم أو حتى عند القيام بالتحديثات.[16]

تكون أفضل تطبيقات أنظمة سكادا في العمليات الموزعة على مساحات ومناطق جغرافية واسعة، وتكون سهلة المراقبة والتحكم وتتطلب تدخلاً متكرراً أو منتظماً أو عادياً. سوف يتم تطبيق أنظمة السكادا في بحثنا على أنظمة نقل القدرة الكهربائية التي تغطي عادة آلاف الكيلومترات المربعة، ويتم التحكم بها عن طريق فتح قواطع وإغلاقها، ويجب أن تكون سريعة الاستجابة لتغيرات الأحمال على الخطوط الكهربائية .



الشكل (4.1): نظام قدرة[17].

5. النتائج ومناقشتها

❖ **إجراء اختبار لتحديد القيمة العظمى للبيانات المُرسلةMTU**

نستطيع القول أنّ OPNET محاكٍ قوي وشائع الاستخدام في المصانع والأبحاث وذلك بسبب خصائصه والمجموعة الكبيرة من الخيارات المضمنة داخله والتي تساعد في نمذجة ومحاكاة الشبكات الكبيرة. الشكل (5.1) يبين خطوات انشاء أي مشروع باستخدام المحاكي OPNET.

الشكل(5.1): خطوات انشاء شبكة باستخدام المحاكي OPNET

- لدينا العلاقة الرياضية التي تعطي زمن الارسال اللازم $\mathbf{T_{transmission}}$.[18]

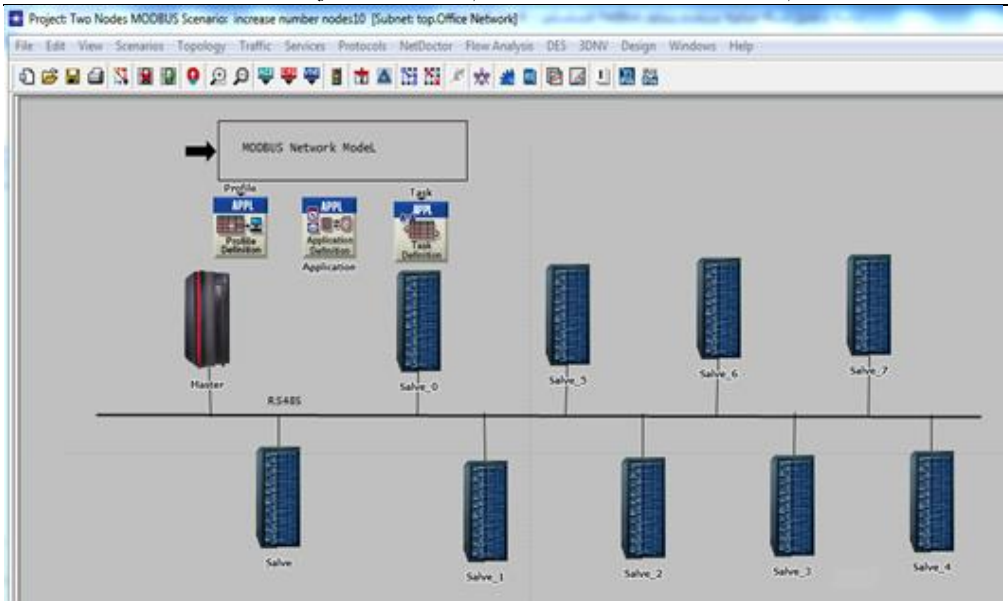
$$\mathbf{T_{transmission}} = \frac{\mathbf{D\ (H+MTU)}}{\mathbf{MTU*R}}$$

حيث أنّ:

- MTU (Maximum Transmission Unit) حجم الأقصى لوحدة البيانات.
- (D): حجم البيانات الكلي (Data).
- (H): حجم الإطار للبرتوكول المستخدم.
- (R): معدّل الارسال.

لا بد من إجراء اختبار لتحديد القيمة العظمى للبيانات المُرسلةMTU لتحقّيق أفضل أداء للشبكة بالاعتمّاد على البارامترات المضبوطة في الشبكة الصناعيّة الأساسية، تمّ رصد تأثير العاملين (عدد العقد وحجم الإطارH وحجم البيانات المُرسلة MTU) على الأداء العام للشبكة الصناعيّة والتي تستخدم أحد أنواع برتوكولات Fieldbus الصناعيّة وهو برتوكول MODBUS ذو الناقل التسلسلي.[19]

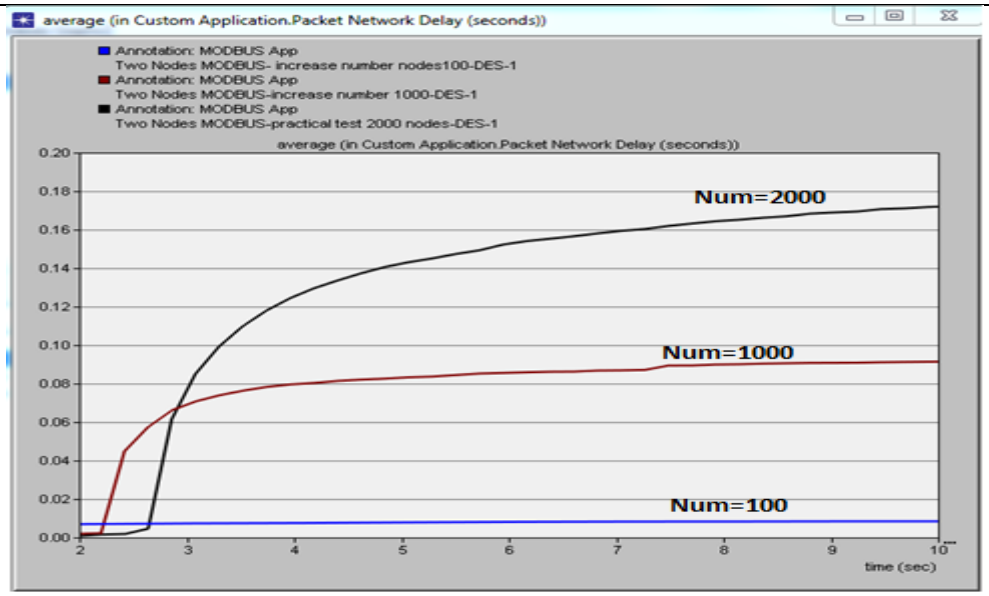
يُظهر الشكل(7.2) نموذج لشبكة صناعيّة Modbusمؤلفة من 10 عقد (9 Master /Slaves،



الشكل(5.2): شبكة صناعيّة مؤلفة من ماستر و9 توابع.

دراسة وتحليل النتائج:

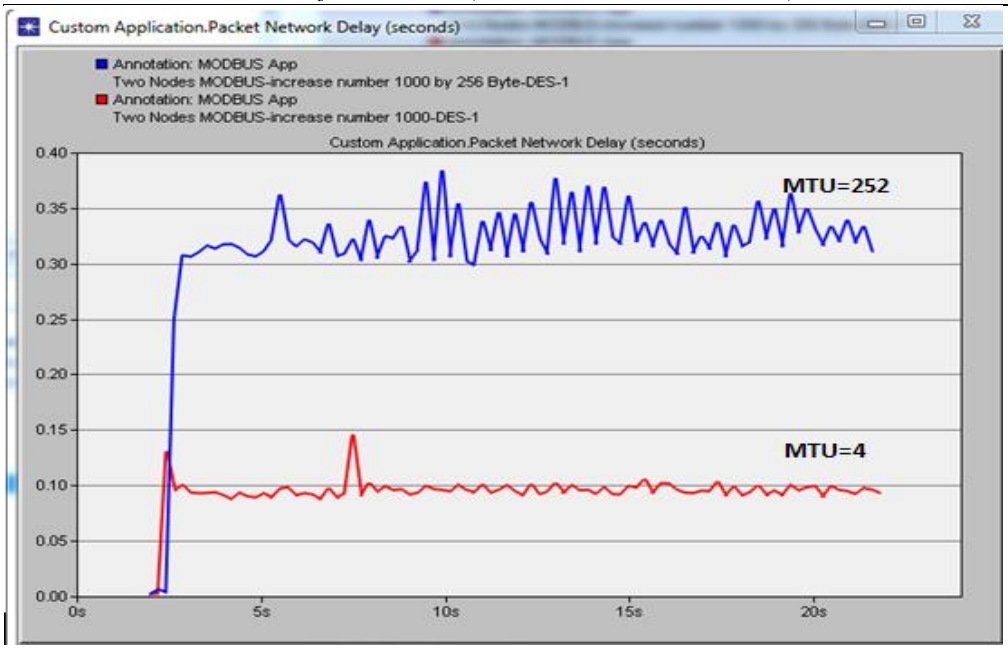
في الحالة الأولى: تمّ زيادة عدد العقد التابعة في الشبكة الصناعيّة بشكل تصاعدي وفق التسلسل الآتي (100–1000–2000) مع تثبيت حجم الإطار على قيمة 8Byte وتمّ رصد تغيّر زمن تأخير إطار الشبكة حيث تمّ تشغيل المحاكاة لمدة 10 ثانية.



الشكل(5.3): تغيّر زمن تأخير الإطار للشبكة الصناعيّة عند زيادة كبيرة لعدد العقد.

يُوضح الشكل(5.3) أن زمن التأخير سجل ارتفاع بشكل كبير من القيمة 0.1s عند عدد العقد (1000) وصولاً للقيمة 0.2s عند العدد (2000).

في الحالة الثانية: تمّ تغيير حجم البيانات المرسلة من القيمة 8Byte إلى القيمة 256Byte لشبكة صناعيّة مؤلفة من (1000) عقدة وتمّ رصد تأثير هذا التغيّر على زمن تأخير الإطار حيث تمّ تشغيل المحاكاة لمدة 20 ثانية.



الشكل(5.4): أثر العامل MTU على زمن تأخير الإطار لشبكة مؤلفة من 1000 عقدة.

نلاحظ من الشكل(5.4) تسجيل قيمة تأخير 0.4s عند الحجم 256Byte على الرغم من تلبية الشبكة لمتطلبات الزمن الحقيقي إلا أنه يجب عدم تجاوز عدد العقد الشبكة ذات الناقل التسلسلي لقيمة (1000) عقدة نتيجة الاقتراب الكبير من القيم الحدية 0.5s التي تخل بمتطلبات الزمن الحقيقي.

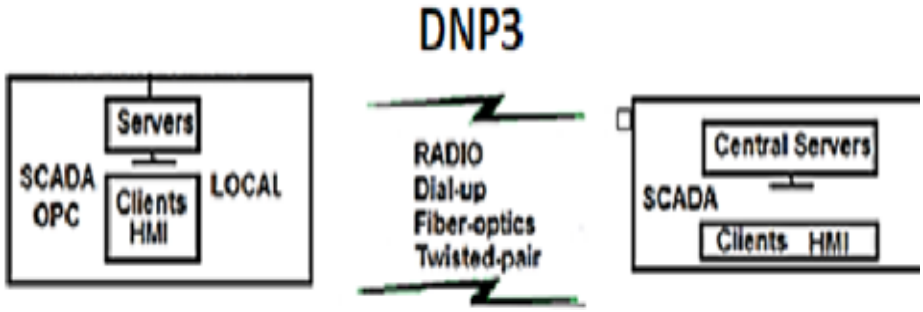
نتائج شبكة صناعيّة تستخدم برتوكول MODBUS ذو الناقل التسلسلي:

1) زيادة استخدامية الناقل بشكل كبير بزيادة عدد العقد في الشبكة.
2) زيادة تأخير الشبكة بزيادة عدد العقد وزيادة حجم الإطار المرسل.
3) يجب عدم تجاوز عدد العقد لقيمة (1000) والإطار عند الحجم الأعظمي256Byte حرصاً على تحقيق متطلبات الزمن الحقيقي والقيمة المعيارية (0.5) ثانية. حيث0.5 ثانية هي القيمة الحدية لزمن استجابة الإطار في بروتوكول Modbus ذو النقل التسلسلي.Page5 [21]

❖ **إجراء اختبار وتحسين امن بروتوكول DNP3 باستخدام خوارزمية ديفي هيلمان**

يتم ربط بروتوكول الاتصالات DNP3 ببرمجة خوارزمية تبادل مفتاح ديفي–هيلمان ضمن حاسوب HMI/Client عند المرسل والمستقبل. تتم عملية تطبيق المصادقة بين الطرفية client والمحطة الرئيسية severو فق الخطوات التالية:

1–تبادل المفاتيح وفق خوارزمية ديفي هيلمان.2–بعدها يصبح لدى الطرفين نفس المفتاح السري ندعوه مفتاح الجلسة. 3–تقوم الطرفية بإنشاء شهادة رقمية وتشفيرها بالمفتاح العام وارسالها للمحطة الرئيسية لفك تشفير الشهادة بالمفتاح الخاص والتأكد منها.4–بعد نجاح التأكد يحصل اتصال بين الطرفين.

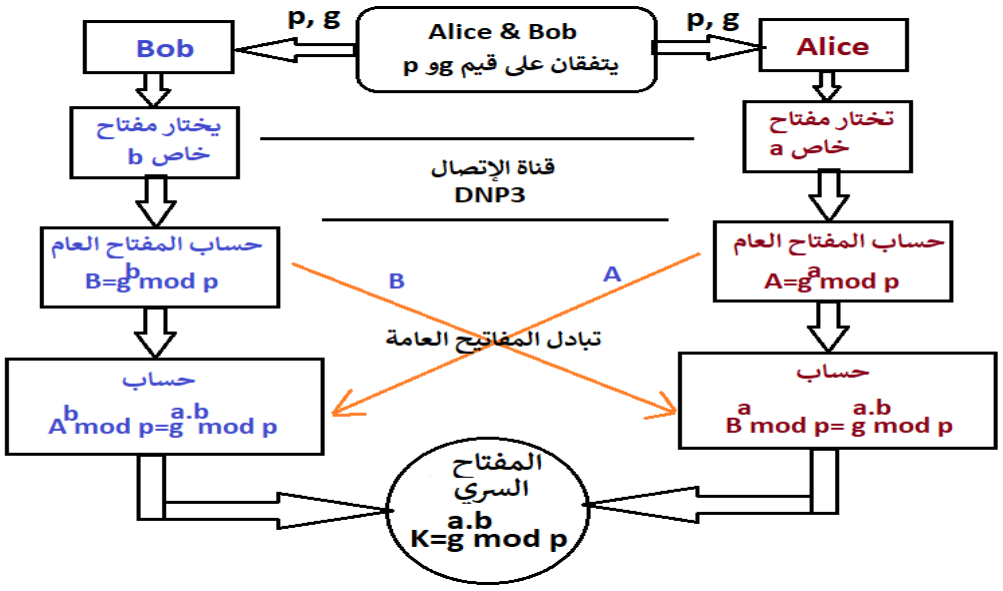


الشكل(5.5): بروتوكول الشبكة الموزعة DNP3 للاتصالات بين المحطة الرئيسة والطرفية

تُعتبر خوارزمية D–H الأول من نوعها في موضوع تبديل المفاتيح، حيث تسمح لشخصين بتبادل بيانات حساسة دون أن يفهمها الطرف الثالث (المتصنت) حتى ولو حصل على نسخة منها. تعتمد الخوارزمية في عملها على إنشاء مفتاح سري مشترك يمكن استخدامه فيما بعد لتشفير المحادثات باستخدام خوارزمية تشفير مفتاح متماثل Symmetric–key.وهو بروتوكول موثوق به للغاية ضد التداخلات الكهرومغناطيسية EMI، لكنه غير آمنًا من هجمات المتسللين.

في وقتنا الحالي، تبادل مفتاح ديفي–هيلمان هو الخوارزمية المعيارية في العديد من بروتوكولات الانترنت للأمان والحماية. مع تطور الشبكات الصناعية عبر روابط الاتصالات الموزعة DNP3، الشكل(5.5) ، جعل مسالة الأمان والحماية من الاختراقات ضرورة قصوى.

إن بروتوكول DNP3 معرض لعدد من الهجمات مثل العبث بالأجهزة أو هجوم الرجل في المنتصف، اقترحنا في بحثنا التحسين الأول في زيادة امن بروتوكول DNP3 باستخدام خوارزمية الشكل الآتي (5.6).



الشكل(5.6): خوارزمية ديفي هيلمان D–H [20]

وتمت المحاكاة لخوارزمية ديفي هيلمان بواسطة لغة Python وفق الآتي:

```
# Generate prime number and generator
    import random
    def generate_prime_number():
    """
    Generate a random prime number between 100 and 1000.
    """
    prime = random.randint(100, 1000)
    while not is_prime(prime):
    prime = random.randint(100, 1000)
    return prime
    def is_prime(n):
    """
    Check if a number is prime.
    """
    if n <= 1:
    return False
    for i in range(2, int(n**0.5) + 1):
    if n % i == 0:
    return False
    return True
    def calculate_public_key(prime, generator, private_key):
    """
    Calculate the public key using the Diffie-Hellman algorithm.
    """
    return (generator ** private_key) % prime

    def calculate_shared_secret(prime, public_key, private_key):
    """
     Calculate the shared secret using the Diffie-Hellman
     algorithm.
    """
    return (public_key ** private_key) % prime



prime = generate_prime_number()
generator = random.randint(2, prime - 1)
```

```
# Generate private keys for Alice and Bob
alice_private_key = random.randint(2, prime - 1)
bob_private_key = random.randint(2, prime - 1)

# Calculate public keys for Alice and Bob
alice_public_key = calculate_public_key(prime, generator, alice_private_key)
bob_public_key = calculate_public_key(prime, generator, bob_private_key)
# Calculate shared secrets for Alice and Bob
alice_shared_secret = calculate_shared_secret(prime, bob_public_key, alice_private_key)
bob_shared_secret = calculate_shared_secret(prime, alice_public_key, bob_private_key)


# Print the results
print("Prime number:", prime)
print("Generator:", generator)
print("Alice's private key:", alice_private_key)
print("Bob's private key:", bob_private_key)
print("Alice's public key:", alice_public_key)
print("Bob's public key:", bob_public_key)
print("Alice's shared secret:", alice_shared_secret)
print("Bob's shared secret:", bob_shared_secret)
```

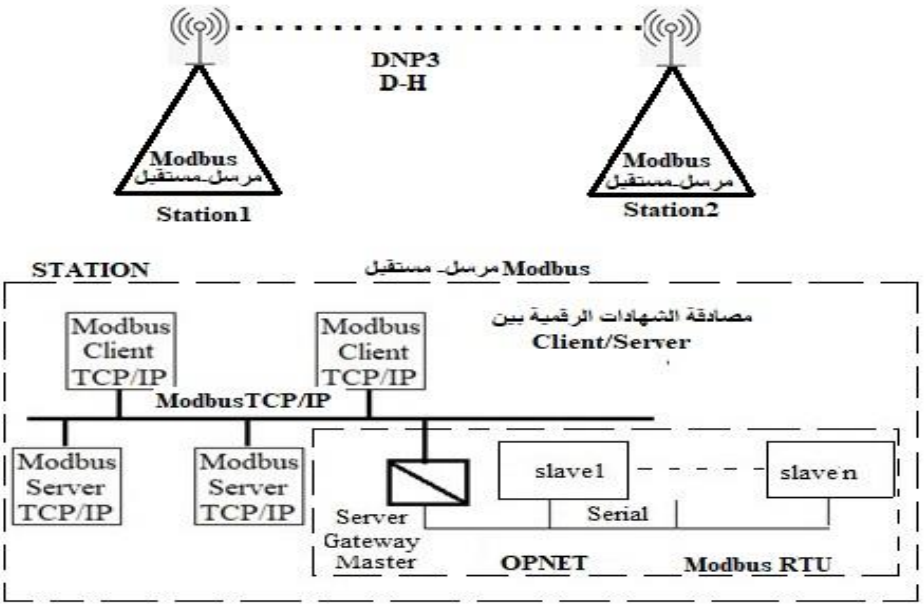
Prime number: 193
Generator: 137
Alice's private key: 160
Bob's private key: 114
Alice's public key: 108
Bob's public key: 27
Alice's shared secret: 1
Bob's shared secret: 1

Prime number: 877
Generator: 545
Alice's private key: 212
Bob's private key: 601
Alice's public key: 553
Bob's public key: 694
Alice's shared secret: 647
Bob's shared secret: 647

نلاحظ من النتائج أن المستخدمين (Master-Clients) حصلوا على نفس قيمة المفتاح **(1, K 647,….)** عند وجود هجمات مثل العبث بالأجهزة أو رجل دخل على الخط، رغم أنه حصل

على القيم **p(139, 877,…), g(137, 575,...), A(108, 553,...), B(27, 694,...)** لكنه لم يستطيع الحصول على المفتاح **K** الصحيح لأنه لا يعرف قيم المختارة السرية **a(160, 212, ….), b(114, 601,…)** من قبل Master(Bob)/Slave(Alice).

❖ **إجراء اختبار والتحسين الثاني في أمن شبكة Modbusعن طريق المصادقة Client/Serverبتوقيع وتشفير شهادات رقمية باستخدام الأداة مفتوحة المصدر OpenSSL**

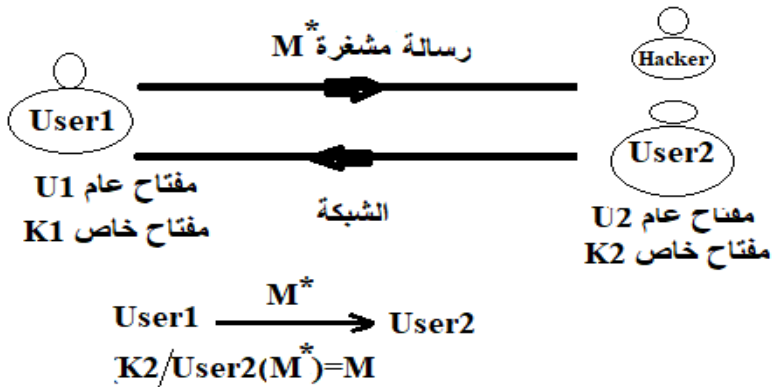


الشكل(5.7): محطة MODBUS

تم الاعتماد على خوارزمية ديفي هيلمان الامنة في نقل البيانات وتبادل المفاتيح بين محطتين عن بعد بواسطة الأنترنت، وسنقوم بتحسين النظام باستخدام OpenSSL للمصادقة باستخدام شهادات رقمية موقعة ومشفرة بشكل امن باستخدام المفاتيح غير المتناظرة وهذا يحل مشكلة القناة الغير آمنة والقرصنة. حيث تقوم الطرفية Clientبإنشاء شهادة رقمية (عبارة عن معرف IDوعنوان الجهاز Addr في الشبكة) وتشفيرها بالمفتاح العام الذي وصلها من خوارزمية D–H وترسل الشهادة للمحطة الرئيسية(Sever/Gateway(Master ، عندئذ تقوم المحطة

الرئيسية بفك تشفير الشهادة بالمفتاح الخاص والتأكد منها وحفظها على انها تابعة للطرفية Client. بعد نجاح المصادقة يحصل اتصال بين المحطة الرئيسية والطرفية.

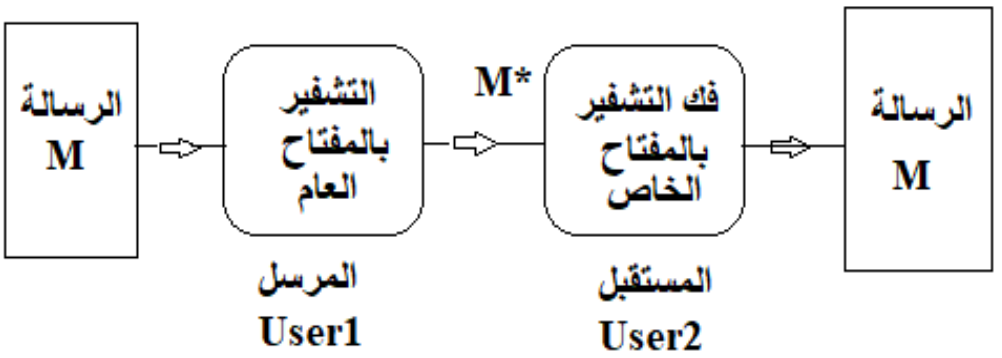
نوع التشفير المستخدم هو التشفير الغير المتماثلAsymmetric encryption ، حيث أن الرسالة المشفرة الرسالة المشفرة بمفتاح عام U لا يمكن قراءتها إلا بواسطة مالك المفتاح الخاصK المقابل .لذا، باستخدام المفتاح الخاص K1 من قبل User1يستطيع أن يوقع معلوماته ويفك رموزها ليعالجها. فمثلاً إذا User1 يرغب في إرسال رسالة M إلى User2، فسوف يستخدم المفتاح العام لـ User2 من أجل تحقيق رسالة مشفرة *M. يستخدم User2 المفتاح الخاص حتى يتمكن من فك الرسالة المشفرة *M ويحصل على الرسالة M. يمكن استئناف العملية وفقًا للشكل الآتي(5.8):



الشكل(5.8): التشفير بالمفتاح العام وفك التشفير بالخاص

إذا اعترض Hacker الرسالة *M، فلن يتمكن من تحديد M من *M بدون المفتاح الخاص K2 لـ User2. لذلك من المستحيل تقريبًا العثور على مفتاح خاص K لعميل User ما من مفتاحه العام U. لكن المشكلة أنه يمكن لخادم "القراصنة" Hacker إ عادة توجيه الموقع للعميل أو الخادم إلى موقع مزيف واسترداد البيانات. والحل هو استخدام الشهادات الرقمية، وهي باختصار وثائق إلكترونية أو شهادات رقمية تستخدم للتحقق من هوية كيان رقمي أو حتى شخصًا يرغب في إنشاء اتصالات آمنة. تُعد الشهادات الرقمية أساسية في التجارة الإلكترونية الحديثة، والشبكات الصناعية، والخدمات المصرفية. إن توقيع وتشفير الشهادات الرقمية يحل مشكلة القناة

الغير آمنة والقرصنة وتتيح هذه الشهادة للموقع إثبات الهوية للعملاء أو للطرفيات Clients كما هو موضح في الشكل الآتي:



الشكل (5.8): توقيع وتشفير الشهادات الإلكترونية

الخطوات الرئيسية في التشفير غير المتناظر باستخدام الأداة OpenSSL

التشفير غير المتناظر (Asymmetric Cryptography) هو نوع من التشفير يستخدم زوجًا من المفاتيح: مفتاح عام (Public Key) ومفتاح خاص (Private Key). يُستخدم المفتاح العام للتشفير، بينما يُستخدم المفتاح الخاص لفك التشفير. هذا النوع من التشفير يوفر ميزة الأمان في تبادل البيانات دون الحاجة إلى مشاركة المفتاح الخاص، مما يجعله مناسبًا للتطبيقات مثل التوقيعات الرقمية وتبادل المفاتيح.

1) يتم أولاً تعزيز أمان شبكة Modbus بإنشاء معلمات نظام (DH) Diffie–Hellman التي تم استقبالها في المحطة

openssl dhparam –out dhparams.pem 2048

```
# إنشاء معلمات DH (عدد أولي كبير وأساس مناسب)
openssl dhparam -out dhparams.pem 2048
```

2) توليد المفاتيح لكل عقدة

- للعميل:

openssl genpkey –paramfile dhparams.pem –out client_dhkey.pem

```
# للعميل:
openssl genpkey -paramfile dhparams.pem -out client_dhkey.pem
```

- للخادم:

openssl genpkey –paramfile dhparams.pem –out server_dhkey.pem

```
# للخادم:
openssl genpkey -paramfile dhparams.pem -out server_dhkey.pem
```

3) عملية تبادل المفاتيح

- العميل يرسل معاملاته العامة للخادم:

openssl pkey –in client_dhkey.pem –pubout –out client_pubkey.pem

- الخادم يرسل معاملاته العامة للعميل:

openssl pkey –in server_dhkey.pem –pubout –out server_pubkey.pem

```
openssl pkey -in server_dhkey.pem -pubout -out server_pubkey.pem
```

```
openssl pkey -in client_dhkey.pem -pubout -out client_pubkey.pem
```

4) توليد المفتاح المشترك:

- على جانب العميل:

openssl pkeyutl –derive –inkey client_dhkey.pem –peerkey server_pubkey.pem –out shared_secret.bin

```
# على جانب العميل:
openssl pkeyutl -derive -inkey client_dhkey.pem -peerkey server_pubkey.pem -out shared_secre
t.bin
```

- على جانب الخادم:

openssl pkeyutl -derive -inkey server_dhkey.pem -peerkey client_pubkey.pem -out shared_secret.bin

```
# على جانب الخادم:
openssl pkeyutl -derive -inkey server_dhkey.pem -peerkey client_pubkey.pem -out shared_secre
t.bin
```

5) استخدام المفتاح المشترك لتشفير الاتصالات

- تحويل المفتاح المشترك إلى صيغة مناسبة للتشفير

openssl enc -aes-256-cbc -kfile shared_secret.bin -in command.txt -out command.enc

```
# تحويل المفتاح المشترك إلى صيغة مناسبة للتشفير
openssl enc -aes-256-cbc -kfile shared_secret.bin -in command.txt -out command.enc
```

- فك التشفير على الطرف الآخر

openssl enc -d -aes-256-cbc -kfile shared_secret.bin -in command.enc -out command_decrypted.txt

```
# فك التشفير على الطرف الآخر
openssl enc -d -aes-256-cbc -kfile shared_secret.bin -in command.enc -out command_decrypted.txt
```

6) تنفيذ التوقيع الرقمي للأوامر:

- العميل: توقيع الأمر قبل الإرسال

openssl dgst -sha256 -sign client.key -out command.sig command.txt

```
# العميل: توقيع الأمر قبل الإرسال
```

- الخادم: التحقق من التوقيع

openssl dgst -sha256 -verify client.pubkey -signature command.sig command.txt

آلية الحماية ضد الهجمات

- حماية ضد التنصت:
  - لا يتم نقل المفتاح السري عبر الشبكة
  - كل جلسة اتصال لها مفتاح مشترك فريد
- حماية ضد هجوم Man-in-the-Middle:
  - دمج آلية المصادقة باستخدام شهادات رقمية

إنشاء شهادة موقعة للخادم (اختياري)

openssl req -x509 -newkey rsa:2048 -keyout server.key -out server.crt -days 365

تحديث المفاتيح الدوري: - تغيير المعلمات الأساسية دورياً - تجديد المفاتيح المشتركة لكل جلسة اتصال

متطلبات التنفيذ

-تعديلات بروتوكول Modbus بإضافة مرحلة مصافحة أولية لتبادل المفاتيح، دعم تشفير AES للبيانات المتبادلة

-إدارة المفاتيح تخزين آمن لمعلمات DH وآلية لتحديث المعلمات الأساسية.

-متطلبات الأجهزة لدعم عمليات حسابية معقدة وذاكرة كافية لتخزين المعلمات

فوائد الحل

-أمان أمامي مثالي: حتى إذا سُرق المفتاح الخاص، لا يمكن فك تشفير الجلسات السابقة.

-مرونة عالية: يمكن تغيير المعلمات الأساسية دون التأثير على النظام.

-تكامل مع أنظمة موجودة: يمكن تطبيقه كطبقة إضافية فوق بروتوكول Modbus الحالي

6. الخاتمة.

- تم في بحثنا التحسين الأول لأمن المعلومات لبروتوكول DNP3 باستخدام خوارزمية ديفي هيلمان أثناء نقل البيانات بين محطتان Modbus، وتمت المحاكاة لهذه الخوارزمية بواسطة لغة Python للحصول على نفس قيمة المفتاح K.
- تم في التحسين الثاني استخدام الأداة OpenSSL في شبكة Modbus للمصادقة باستخدام شهادات رقمية موقعة ومشفرة بشكل امن باستخدام المفاتيح غير المتناظرة بين الوحدات الطرفية clients والمحطات الرئيسية servers وهذا حل مشكلة القناة الغير آمنة والقرصنة.
- تم أيضاً بناء نموذج شبكة صناعية تستخدم بروتوكول Modbus باستخدام محاكي الشبكات OPNET، بإجراء عملية تحليلية للنتائج وبهدف تحديد القيم الأفضل للعوامل المؤثرة في الأداء العام للشبكة الصناعيّة الحقلية عندما يتغير حجم البيانات بالإطار إلى 256 Byte للوصول للإدارة المثلى لبروتوكولModbus .
- توصلنا إلى أن زيادة الاستخدامية بزيادة عدد العقد في الشبكة بحيث لا يتجاوز عددها 1000 عقدة والموافق 0.4 ثانية

أما أهمية البحث فتكمن أولاً في تحقيق أمن معلومات وحماية الشبكة وإزالة مخاطر الهجمات بخوارزميات وأدوات فعالة وسهلة التنفيذ وثانياً في معرفة عدد العقد الأعظمي بشرط عدم تجاوز الزمن 0.5 ثانية وهو زمن استجابة الإطار في بروتوكولModbus .

7. التوصيات والآفاق المستقبلية.

- ✓ نوصي بدراسة تأثير عوامل أخرى تؤثر في بارامترات أداء الشبكة الصناعية مثل هجوم رفض الخدمة الموزع (DDOS) وغيرها من هجمات حرمان الخدمة.
- ✓ نوصي بزيادة موثوقية طريقة D–H باستخدام أعدادًا أولية كبيرة أو منحنيات إهليلجيه (ECDH) واستخدام الذكاء الاصطناعي في الحماية.
- ✓ ننصح باستخدام برنامج التعليمي الإلكتروني Cryptology مفتوحة المصدر والمجاني للتشفير بشكل رسومات بيانيةCryptographic وتشفير تحليليCryptanalytic.
- ✓ نوصي بوضع نماذج لبرتوكولات صناعيّة أخرى مثل (برتوكول PROFINET، برتوكول ASI، برتوكول CAN) وغيرها ودراسة وتحليل أداءها وتأثير الأمان على الأداء.

المراجع العلمية

[1] https://www.opc7.com / **"opc-server-for-Modbus"**. Industrial connectivity solutions and information

[2] https://www.opc7.com/ **"what-technologies-does-opc-use"**/ Industrial connectivity solutions and information.

[3] KUKI. A. 2014 **"Modeling computer networks by the help of OPNET tools** "Proceedings of the 9th International Conference on Applied Informatics, p. 251–258.

[4]. Amoah. R. 2016. **"Securing DNP3 broadcast communications in SCADA systems"**. IEEE Transactions on Industrial Informatics, Camtepe S & Foo, E 12(4), 1474-1485.

[5] AlANAZI. M, ABDUN. M, CHOWDHURY. MJM. 2023 **"SCADA vulnerabilities and attacks"** Computers & security 125: 103028.

[6] PRABHU. A. JENICE. D. RAJESH. H. 2023 **"Authentication of WSN for Secured Medical Data Transmission Using Diffie Hellman Algorithm".** Computer. Syst. Sci. Eng. 45(3): 2363-

[7] SETHI. A .S. HNATISHIN. V .Y. 2013 **"The Practical OPNET User Guide for Computer Network Simulation"**

[8] KRUPANEK.B, BOGACZ.R. 2016. **"OPNET Modeler simulations of performance for multi nodes wireless systems"**, Silesian University of Technology, Poland, 10p.

[9] MITTRA.A. 2017. **" What is the Diffie-Hellman Key Exchange Protocol and how does it work?** "CCNP, CompTIA, Network security.

[10] Larry L. Peterson, Bruce S. Davie. 2012 . **"Network Security"** in Computer Networks (Fifth Edition).

[11] KIM. B, LEE. D, CHOI. T**.** 2015 **"Performance Evaluation for Modbus/TCP Using Network Simulator NS3"**, IEEE, Kyungpook National University, Korea,10p.

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

[13] DARWISH. I, IGOBE. O & SAADAWI. T 2016. **"Vulnerability Assessment and Experimentation of Smart Grid DNP3"**. Journal of Cyber Security and Mobility, 23-54.

[14] IGBE. O, DARWISH. I, SAADAWI. T. 2017**. "Deterministic dendritic cell algorithm application to smart grid cyber-attack**

detection". In 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (pp. 199-204). IEEE.

[15] BERGE. 2004 ."**Fieldbuses for Process Control: Engineering, Operation and Maintenance"** ISA, p. 20, USA.

[16] AXELSON. J 2004. **"Practical modern SCADA protocols dnp3,608705 and Relate Systems"** Serial Port Complete. Lakeview Research communication systems.

[17] ATASSI. M, WAFAI. H 2024 **"Industrial Communication &Networks, Automation"** research seminars and lectures in College of Mechanical and Electrical Engineering at Al-Baath University and Damascus University.

[18] GUO. Y PAN. Y and CAI. L. 2016 **"OPNET-based Analysis of MTU Impact on Application Performance"**IEEE. Communication University. China.pp.197-207.

[19] SETHI.A.S, HnatyshynV.Y. 2013. **"The Practical OPNET User Guide for Computer Network Simulation"**

[20] FAHMY. S 2021 **"Secure voice cryptography based on Diffie-Hellman algorithm"**
IOP Conference Series Materials Science and
Engineering 1076(1):012057

[21] Mahmood,M and Al-Naima,F, **"OPNET Similation of data Transmission Network: A Case Study for Control System in Petroleum Refinery Complex in Iraq"**, IEEE. Nahrain University, Baghdad, Iraq,p12, 2015.

[22] Darwish, I., Igbe, O., & Saadawi, T. (2016). V**ulnerability Assessment and Experimentation of Smart Grid DNP3**. Journal of Cyber Security and Mobility, 5(1), 23.54.

[23] Igbe, O., Darwish, I., & Saadawi, T. (2017, June). **Deterministic dendritic cell algorithm application to smart grid cyber-attack detection**. In 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud) (pp. 199-204). IEEE.

[24] ANSSI, 2013. **"Digital Signature"** The private key, Wikiwix.

[25] Emsisoft, 2014, "**What is a digital certificate?**". Security Blog.

[26] Roche. D **"Securing communications"** Asymmetric encryptions. NSI terminal

[27] Solution ID: INFO141, 2024 "**OpenSSL-Quick-Reference- Guide** knowledge. digicert.com/general-information/
[28] L. Gyongyosi and S. Imre, **"A survey on quantum computing technology"**, Computer Science Review, vol. 31, pp. 51–71, 2019