Al-Rafidain Engineering Journal (AREJ) Vol.30, No.1, March 2025, pp. 104-111

Enhancing Industrial Internet of Things Availability and Reliability Using Dual-Communication Links Mechanism Based on the OPC UA Protocol

Mohammed B. Mahmood*
mohammed.basil@ntu.edu.iq

Jassim M. Abdul-Jabbar**
drjssm@almaaqal.edu.iq

*Medical Instrumentation Techniques Eng., Technical Engineering College, Northern Technical University, Mosul, Iraq.
**Control and Computer Engineering Department, College of Engineering, Almaaqal University, Basra, Iraq.

Received: May 16th, 2024 Received in revised form: July 16th, 2024 Accepted: July 31th, 2024

ABSTRACT

In this paper, we designed a practical Industrial Internet of Things (IIoT) system for the regions of the world that suffer from low-quality Internet Service Providers. The developed system depends on the duplication and sending of the same stream of data simultaneously through dual communication links between the OPC UA (Open Platform Communications United Architecture) server and a remote OPC UA client. This method can improve the designed system's availability and reliability. Six analog tags are monitored and controlled simultaneously through the remote OPC UA client with a scan rate of 100 ms at both the server and the client sides. A secure and reliable data transfer has been done, using 256-bit AES to encrypt the analog tags. The results show a significant improvement in the availability and reliability of the designed system when using dual communication links to send the same data simultaneously.

Keywords:

OPC UA, Industrial Internet of Things, Information Technology, Operation Technology, Computer Network.

https://rengj.mosuljournals.com
Email: alrafidain_engjournal3@uomosul.edu.iq

==========

1. INTRODUCTION

Enabling sensors and local processing to communicate globally for information sharing is referred to as the Internet of Things (IoT). This technology allows users to remotely make decisions using the information received via the Internet. The IoT encompasses familiar applications like smart homes, connected toys, and mobile fitness [1], [2]. The term IoT finds diverse applications globally. Nevertheless, when the applications pertain to manufacturing segments, industrial processes, smart agriculture, smart cities, and smart grids, it is referred as the Industrial Internet of Things (IIoT). The communication protocols utilized by the Industrial Internet of Things (IIoT) include OPC UA, Hypertext Transfer Protocol (HTTP), Message Queuing Telemetry Transport (MQTT), Java Message Service (JMS), Constrained Application Protocol (CoAP), Data Distribution Service (DDS), and Windows Communication Foundation (WCF) [3]- [7].

The Industrial Internet of Things (IIoT) is often referred to as The Fourth Industrial Revolution or Industry 4.0 [8]. Industrial communication for data transfer between devices and equipment involves specific communication protocols tailored for each industrial layer, including Real-Time Ethernet (RTE) [9], Fieldbuses [10], and wireless networks [11]- [13].

Securing the Industrial Internet of Things (IIoT) has become increasingly challenging for three primary reasons. Firstly, there exists a robust interconnection between IIoT and Information Technology (IT). Secondly, the escalating power of hackers, viruses, and worms is attributed to advancements in software and microprocessor technologies. Lastly, the conventional security approaches employed in IT systems cannot be directly applied to safeguarding IIoT information [14]– [16].

Communication cables such as Ethernet, Profibus, and Profinet are extensively employed in industrial applications due to their high reliability in data transmission. Nevertheless, wireless communication technologies like ZigBee, Wi-Fi, NFC, Bluetooth, Z-Wave, and others can also be utilized [17], [18].

In this paper, the designed system allows a global client to access the industry from anywhere without extra network configuration (i.e., plug-and-play). In addition, the developed system can work efficiently for the region suffering from low-quality internet service providers.

2. THEORETICAL BACKGROUND OF IIOT

2.1. OPC Unified Architecture

The success of the Industrial Internet of Things (IIoT) relies on adopting a standardized open communication platform that fulfills the following specifications [19]:

- Scalability, enabling seamless expansion of the industrial system network from individual sensors and actuators to ERP and MES applications.
- Independence across industry sectors, manufacturers, programming languages, and operating systems.
- Representation of any communication contents used to model virtual objects as representatives of authentic products with their production sequences.

OPC UA serves as an industrial communication standard facilitating interoperability with both vertical and horizontal information integration across the industrial hierarchy from the foundational industrial floor (sensors and actuators) to the upper layer, ERP (Enterprise Resource Planning). Figure 1 illustrates the functionality of the OPC UA protocol and its integration throughout the entire industrial pyramid.

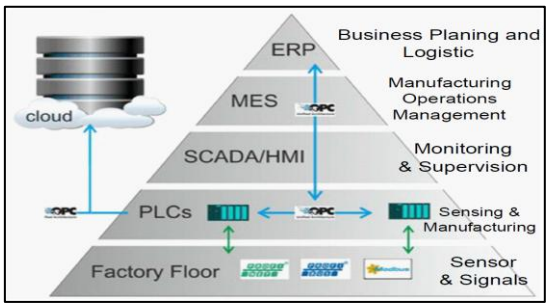

Fig. 1. Horizontal and vertical automation integration in a factory with OPC Unified Architecture [20], [21].

OPC UA's main benefit is that it can work with different operating systems and suppliers on its own. As a result, it has developed into a practical method for guaranteeing compatibility across several industries and sectors. Data interfaces and data structures are used by OPC UA to specify machines and manufacturers [20].

OPC UA is a framework for sharing and representing object-oriented information and data. The transport mechanisms determine data exchange, and information models regulate information exchange. Object-oriented techniques are used for OPC UA information modeling, defining a set of base types extended by objects and references. Data types are specified by vendors, organizations, or standardization committees [22].

2.2. OPC Unified Architecture

The significant increase in the number of computers connected through the Internet and the significant increase in data transmission over the Internet makes the overall systems vulnerable to various forms of active or passive attacks. Therefore, a new security solution has emerged in recent years. The digital certificates are used to ensure the identity of communicating parties by using a pair of encryption keys that guarantee the identity of the communication parties and they cannot deny their identity or the messages that they transmitted (non-repudiation) [23], [24].

Digital certificates come in different types, such as X.509v3 certificates, Pretty Good Privacy (PGP) certificates, Simple Public Key Infrastructure (SPKI) certificates, and Attribute certificates. OPC UA systems are generally use X.509v3 digital certificates [22].

The X.509 digital certificate is a public key certificate that depends on linking the value of a public key with the server or user identity specified in the certificate. The concept behind X.509 involves the use of a pair of public and private keys, which are employed to encrypt and decrypt data [25], [26].

3. METHODOLOGY

3.1. Designed IIoT System Configuration

The OPC UA server autonomously manages connections to Remote OPC UA clients via the Internet. The maximum number of OPC UA clients authorized by the server at any given time determines the simultaneous connections allowed. On the plant (factory), the server auto-configures local industrial devices, such as PLCs,

HMI, and local OPC UA clients. The server should have full information about the local industrial devices, including their IPs and variables. Conversely, the Remote OPC UA client requires complete access information for the server, including the server's Public IP Address, authentication username, authentication password, server certificate, and variable tag numbers. Once the Remote OPC UA client completes the configuration with the OPC UA server, the server establishes a link channel between both ends through the Internet.

In this paper, the designed system addresses different types of IIoT security, such as; data integrity, confidentiality, and access control. The integrity of the data is accomplished by using dual communication links, which provide redundancy and allow for error checking between the two streams of data, reducing the likelihood of data corruption. In addition, the system employs a 256-bit AES encryption method to encrypt the analog tags and make them unreadable to unauthorized parties. OPC UA protocol is used to build a more secure system by using digital certificates (X.509v3) to authenticate the identities of communicating parties. This ensures that only authenticated parties are allowed to communicate with the system, therefore maintaining access control and preventing unauthorized users from entering the system.

The designed system applies to remote industrial automation applications, especially for controlling and operating critical components in any industrial plant. In general, the designed system can serve in two different scenarios. In the first scenario, when giving an ignition command to a plant to start or stop working (or for any critical devices), the command should come through two different ISPs within a specified time interval (depending on the network time delay). If an order is received only from one link and the same command is not received from the other link within the specified time interval, the system will initiate an alarm to inform the operator that one way is failing to take action. In the second scenario for the alarm signal, when it is received at least from one link, it will initiate an alarm indication to inform the operator that this alarm has come from a single link or two links. This method of organization provides robustness, availability, reliability, and security for our designed system. The two scenarios are based on the digital voting principle.

In case both communication links fail simultaneously, the output can be deactivated or continue working in local mode, depending on the programming of the ladder diagram in the PLC.

3.2. OPC UA Client-Server Reconfiguration Time

The Wireshark software is employed, in this paper, for monitoring and testing of real-time data exchanged between the OPC UA server and the Remote OPC UA client. Two scenarios were examined to demonstrate the time required for reconfiguring the communication link between the server and the Remote client. In these scenarios, two analog tags are transferred between them using the OPC UA protocol with a 256-bit AES encryption method.

Scenario 1. The communication link between the Remote OPC UA client and the OPC UA server is manually interrupted by disconnecting the internet at the client side and then immediately reconnecting it. The time of reconfiguration is shown in Figure 2. The two peaks shown in the figure are preceded by a region when there is no data flow and the time required to reconfigure the client to the server is about 10 seconds which is indicated in the regions inside the red circles. Furthermore, the number of packets reaching the peak value during the reconfiguring time is approximately 30 packets/second.

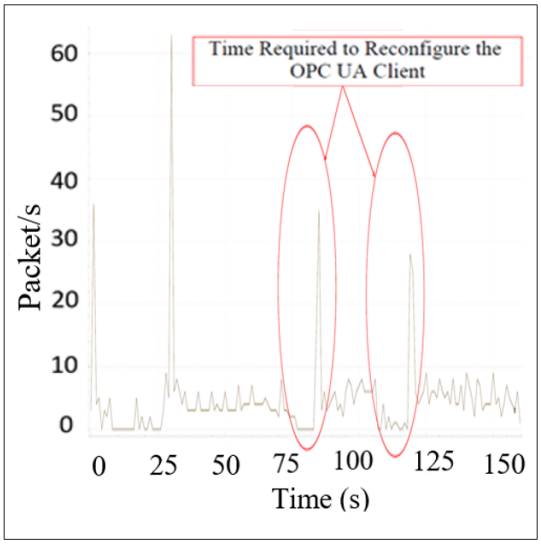

Fig. 2. Time Required to Reconfigure OPC UA Client When the Internet is Disconnect at the Client Side.

Scenario 2. The communication link between the Remote OPC UA client and the OPC UA server is manually interrupted by disconnecting the internet at the server side and then immediately reconnecting it. The time of reconfiguration is shown in Figure 3. The three peaks shown in the figure are preceded by a region where there is no data flow and the time required to reconfigure the client to the server is

about 15 seconds which is indicated in the regions inside the red circles. Furthermore, the number of packets reaching the peak value during the reconfiguration time is approximately 40 packets/second.

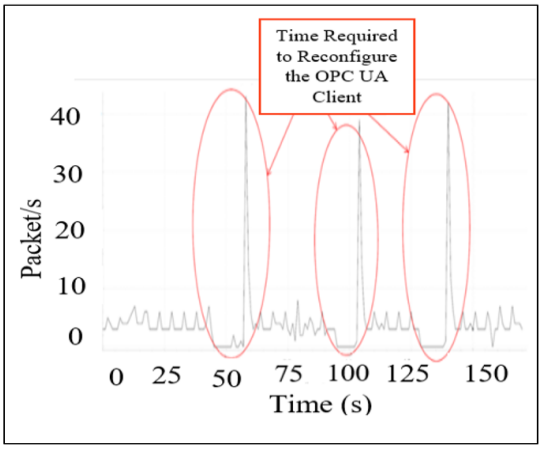

Fig. 3. Time Required to Reconfigure OPC UA Client When the Internet is Disconnect at the Server Side.

3.3. Overall System Test and Data Analysis During Normal Operation

The system has been tested many times through world wide web with real communication between the OPC UA client and the OPC UA server. The server is connected via a Fiber to the Home-Internet Service Provider (FTTH-ISP). Meanwhile, the client device is connected through two different ISPs, which are the 3G mobile network and FTTH ISPs. A dedicated public IP is used on the server side while a private IP is assigned for the client device. Since the 3G mobile network is less reliable than the FTTH therefore more attention is given to the 3G mobile network. The OPC UA server and the client device started working together to control and monitor six analog tags. By using the built-in random number generator of the Siemens S7 1200 PLC, the analog tag values were generated. The analog tags are level measurement, flow measurement, temperature measurement, pressure measurement, filling control valve, and discharge control value. The six tags are deployed to measure the analog parameters required to monitor and control most types of tanks as shown in Figure 4. When using a 3G mobile network on the client side, the whole data required for this session is 21.14 MB, with a scan rate of 100 ms at each entity (server and client).

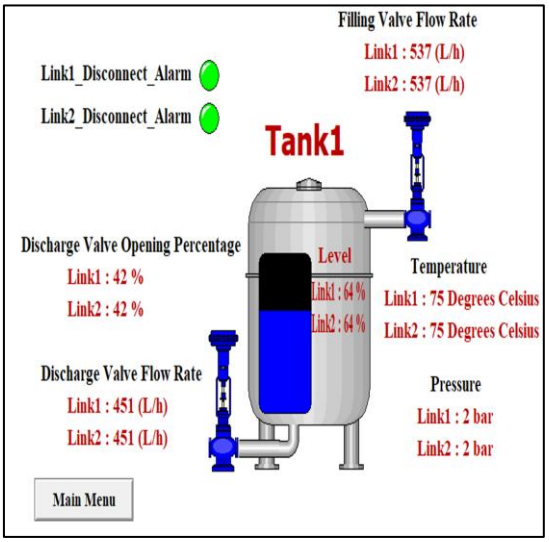

Fig. 4. Visualization of Analog and Redundant Tags for Tank Monitoring and Control

4. RESULTS AND DISCUSSIONS

As shown in Tables 1 and 2, the total number of the TCP packets (concerning our OPC UA payload) is 43418 packets on the server side and 42912 on the client side. A 506 difference in the packet numbers is that some packets are missed during the transmission process and then these packets are retransmitted again. Table 1 shows that 99.85% of packets have small lengths (40-319). The small packet sizes indicate fragmentation happened to the packets because these packets are less than 1/3 of the maximum packet size allowable in the IP Network (1500 Bytes). The Ethernet MTU [27] standard capacity is 1,500 bytes, not including the 18 or 20-byte Ethernet header. Any higher-level networks' MTU must be compatible with this number.

Table 1. Packet lengths Distribution for all TCP traffic in the manufacturing cell network at the Server Side using 3G Mobile Data.

Packet Lengths (bytes)	Transmitted Packets count	Lost Packets count	Percentage of the packet loss
0-19	0	0	0.00%
20-39	0	0	0.00%
40-79	16245	203	1.25%
80-159	12308	104	0.84%
160-319	14804	74	0.50%
320-639	58	57	98.28%
640-1279	3	1	33.33%
1280-2559	0	0	0.00%
2560-5119	0	0	0.00%
>= 5120	0	0	0.00%
0- 5120	43418	439	1.01%

Table 2. Packet lengths Distribution for all TCP traffic in the manufacturing cell network at the Client Side using 3G Mobile Data.

Packet Lengths (bytes)	Transmitted Packets count	Lost Packets count	Percentage of the packet loss
0-19	0	0	0.00%
20-39	0	0	0.00%
40-79	15549	151	0.97%
80-159	12421	105	0.85%
160-319	14903	47	0.32%
320-639	37	34	91.9%
640-1279	2	0	0.00%
1280-2559	0	0	0.00%
2560-5119	0	0	0.00%
>= 5120	0	0	0.00%
0- 5120	42912	337	0.79%

A comparison between Tables 1 and 2 reveals that the highest percentage of packet loss occurs in long-length packets. Specifically, for packet lengths of (320 – 1279) bytes.

In Figure 5, the OPC UA traffic is displayed for server-client data transmission sessions. The client is connected via 3G mobile data, while the server is connected through FTTH. A short disconnection occurred at 1347 seconds, lasting for 30 seconds until reconnection at 1377 seconds. Such interruptions could halt production or jeopardize worker safety. Therefore, the implementation of dual communication links becomes crucial to ensure continuous communication by maintaining at least one active link between the client and the server during any connection failure.

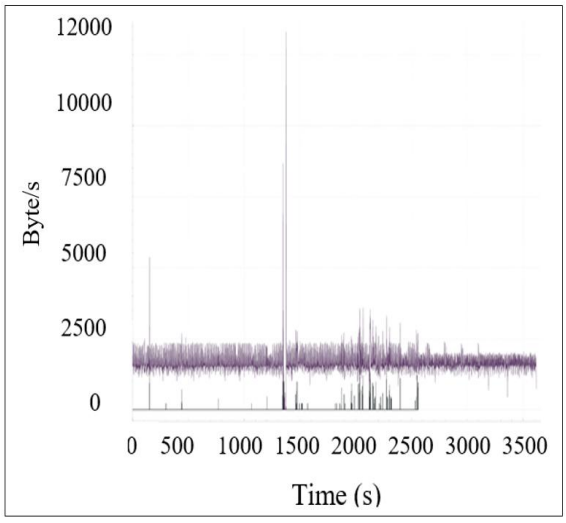

Fig. 5. OPC UA Bytes per second for the Server-Client communication when the Client is connected to 3G mobile data.

Simultaneously, the same data has been transmitted through the other communication link, utilizing FTTH on the client side. In Table 3, the total number of TCP packets related to our OPC UA payload is outlined, totaling 41,840 packets on the client side. Notably, Table 3 indicates that all 100% of the packets have small lengths (40-319) because no auto-configuration occurs between the client and the server, and there are no disconnections during the test period.

Table 3. Packet lengths Distribution for all TCP traffic in the manufacturing cell network at the Server Side using FTTH Data.

Packet Lengths (bytes)	Transmitted Packets count	Lost Packets count	Percentage of the packet loss
0-19	0	0	0.00%
20-39	0	0	0.00%
40-79	15632	0	0.00%
80-159	14483	0	0.00%
160-319	11725	0	0.00%
320-639	0	0	0.00%
640-1279	0	0	0.00%
1280-2559	0	0	0.00%
2560-5119	0	0	0.00%
> = 5120	0	0	0.00%
0- 5120	41840	0	0.00%

Fig. 6 shows the overall OPC UA traffic when the OPC UA client connects through the FTTH ISP.

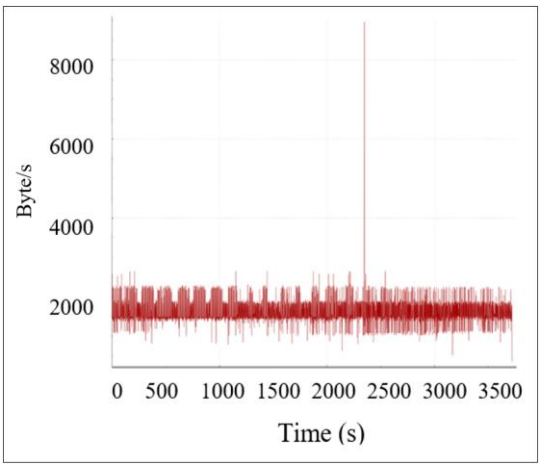

Fig. 6. OPC UA Bytes per second for the Server-Client communication when the Client is connected to FTTH.

Figure 6, representing the FTTH link, demonstrates that in the event of a disconnection in one of the links between the client and the server, the data flow continues seamlessly

through the other link. Notably, the PLC is programmed to effectively manage data from both connections simultaneously, ensuring a continuous and uninterrupted flow of information even during disruptions in one of the communication links.

From Figure 6, the Uptime is 3600s, and the Downtime is the 30s. The following formula is used to calculate the availability of one communication link connected to the Internet provided by 3G mobile on the client side [28]:

$$Availability=[Uptime / (Uptime + Downtime)]x\ 100\% \quad \ldots(1)$$

$$= [3600/ (3600+30)]x100\%$$

$$=99.174\%$$

The value of 99.174 % is for one communication link availability during regular operation. Because our designed system has another communication link that works in parallel, the system has a high level of availability. This value is calculated by ignoring the overall network system (ISP) failure.

Calculating the system availability when the two-communication links are working depends on the probability of occurrence. Since the disconnection of link1 is independent of the disconnection of link2, the likelihood of disconnecting the two connections is calculates using the formula:

$$P(A\&B) = P(A)*P(B) \quad \ldots (2)$$

Where;
P(A&B): The probability of Link1 and Link2 is unavailable.
P(A): Probability of Link1 not available.
P(B): Probability of Link2 not available.

Since we assumed the link availably is 99.174%, then

$$(A) = (1- 99.174/100) = 0.00826= 0.\ 826\%$$
$$P(B) = (1- 99.174/100) = 0.00826= 0.\ 826\%$$
$$P(A\&B) = 0.00826* 0.00826= 0.0000682276= 0.00682276\%$$

Then to calculate the availability of the system for the dual links:

$$Dual\text{-}link\ System\ Availability = [1- P(A\&B)]$$
$$Dual\text{-}link\ System\ Availability = [1- 0.0000682276]$$
$$= 0.999932$$
$$= 99.9932\%$$

The calculation shows that the system availability when using dual communication links is 99.9932%, which is much better than the system availability when using a single communication link, which is 99.174%. The initial costs of the dual communication links are higher than the single links, which include extra hardware devices such as; routers, switches, and cables. In addition, there are extra software costs such as; licenses, and labor for installation and setup. Finally, the operational costs add recurring ISP fees, regular maintenance, and higher energy consumption due to additional equipment. However, the designed system significantly improves system availability, resulting in enhanced reliability, which can help avoid substantial financial losses due to halted operations, missed deadlines, potential penalties, and the cost of restarting production processes, which can have considerable economic impacts.

5. CONCLUSIONS

For the communication session between the OPC UA Server and the OPC UA client, about 21.1MB of data is transferred between the two entities when the Client-Server scan rate is 100 ms, 3G mobile data is used at the client side and reliable FTTH is used at the server side.

The large packets are appearing only when a disconnection in the communication link happens during the normal operation. The results showed that most of the transmitted TCP packets between the OPC UA client and the OPC UA Server are small packet lengths (40-319). The small packet sizes indicate that fragmentation happened to the packets because these packets are less than 1/3 of the maximum packet size allowable in the IP Network (1500 Bytes).

For the packet lengths of (640 – 1279) one of three packets is lost which means 33.33% of the packets are lost. For the packet lengths (320 – 639), 21 packets are lost which means 36.2% of the packets are lost, and for the packet lengths (40 – 319) 303 packets are lost which means 0.7% of the packets are lost.

The time required to reconfigure the OPC UA Client to the OPC UA Server When the Internet Disconnect happens at the Client Side is 50% less than the time required to reconfigure the OPC UA Client to the OPC UA Server When the Internet disconnect happens at the Server Side.

The calculations showed a significant improvement in the system availability when depending on dual communication links to send the same data simultaneously at each communication link.

REFERENCES

[1] D. Singh, G. Tripathi, A. Jara, "A survey of Internet-of-Things: Future vision, architecture, challenges and services". IEEE World Forum on Internet of Things (WF-IoT), pp. 287-292, 2014, doi: 10.1109/WF-IoT.2014.6803174.

[2] K. Juma, et al, " IoT Based Gas Leakage Detection and Alarming System using Blynk platforms", Iraqi Journal for Electrical and Electronic Engineering, vol. 18, no. 1, pp. 64-70, 2022, doi:10.37917/ijeee.18.1.8.

[3] I. González, A. Calderón, J. Figueiredo, J. Sousa, "A Literature Survey on Open Platform Communications (OPC) Applied to Advanced Industrial Environments", Electronics, vol. 8, no. 5, 2019, doi: 10.3390/electronics8050510.

[4] M. Salhaoui, A. Guerrero-González, M. Arioua, Ortiz, A. El Oualkadi, C. Torregrosa, "Smart Industrial IoT Monitoring and Control System Based on UAV and Cloud Computing Applied to a Concrete Plant", Sensors, vol. 19, no. 15, 3316, 2019, doi: 10.3390/s19153316.

[5] OPC Foundation. OPC UA Part 1 - Overview and Concepts, https://reference.opcfoundation.org, last accessed 2023/1/2.

[6] M. Mahmood, and J. Abdul-Jabbar, "Securing Industrial Internet of Things (Industrial IoT)- A Reviewof Challenges and Solutions", Al-Rafidain Engineering Journal, vol. 28 no. 1, pp. 312-320, 2023, doi: 10.33899/rengj.2022.135292.1196.

[7] R. AlSheikh, R.M. Hagem, O. Salim, "A Survey on Smart Monitoring System of Environment Based on IoT", Al-Rafidain Engineering Journal, vol. 26, no. 1, pp. 146-158, 2021, doi: 10.33899/rengj.2021.128944.1072.

[8] Z. Bakhshi, A. Balador, J. Mustafa, "Industrial IoT security threats and concerns by considering Cisco and Microsoft IoT reference models", IEEE Wireless Communications and Networking Conference Workshops (WCNCW), pp. 173-178 2018, doi:10.1109/WCNCW.2018.8368997.

[9] J. Decotignie, "Ethernet-Based Real-Time and Industrial Communications", In: Proceedings of the IEEE, vol. 93, no. 6, pp. 1102-1117, 2005, doi: 10.1109/JPROC.2005.849721.

[10] D. Dzung, M. Naedele, T. Hoff, M. Crevatin, "Security for Industrial Communication Systems", In: Proceedings of the IEEE, vol. 93, no. 6, pp. 1152-1177, 2005, doi: 10.1109/JPROC.2005.849714.

[11] S. Vitturi, C. Zunino, T. Sauter, "Industrial Communication Systems and Their Future Challenges, Next-Generation Ethernet, IIoT, and 5G", In: Proceedings of the IEEE, vol. 107, no. 6, pp. 944-961, 2019, doi: 10.1016/j.procs.2023.03.014.

[12] A.: Willig, "Recent and Emerging Topics in Wireless Industrial Communications" A Selection. In: IEEE Transactions on Industrial Informatics, vol. 4, no. 2, pp.102-124, 2008, doi: 10.1109/TII.2008.923194

[13] S. Alabady, and A. Hameed, "Design, Simulation, and Performance Evaluation of Reactive and Proactive Ad-Hoc Routing Protocols", Iraqi Journal for Electrical and Electronic Engineering, vol. 20, no. 1, pp. 1-15, 2023, doi: 10.37917/ijeee.20.1.1.

[14] P. Jie, and L. Li, "Industrial Control System Security", Third International Conference on Intelligent Human-Machine Systems and Cybernetics, pp. 156-158, 2011, doi: 10.3390/sym12101583

[15] A. Salauyou, M. Ehunou, "Technology of modulation by synthesized digital method of carrier in analogue signal transmission systems", Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO), Minsk, Belarus, pp. 1-3, 2018.

[16] S. Qaddoori, and Q. Ali, "An Efficient Security Model for Industrial Internet of Things (IIoT) System Based on Machine Learning Principles", Al-Rafidain Engineering Journal (AREJ), vol. 28, no.1, pp. 329-340, 2023, doi: 10.33899/rengj.2022.134932.1191.

[17] A. Gavlas, J. Zwierzyna, J. Koziorek, "Possibilities of transfer process data from PLC to Cloud platforms based on IoT", IFAC-PapersOnLine, vol. 51, no. 6, pp. 156-161, 2018, doi: 10.1016/j.ifacol.2018.07.146.

[18] M. Rashid, "Design and Implementation of Smart Electrical Power Meter System. Iraqi Journal for Electrical and Electronic Engineering", vol. 10, no. 1, pp. 1-14, 2014, doi: 10.37917/ijeee.10.1.1.

[19] F. Pauker, I. Ayatollahi, B. Kittl, "OPC UA for machine tending industrial robots", In: Proceedings of the 2nd International Conference on Advances in Robotics Engineering, pp. 79–8, 2014, doi: 10.15224/978-1-63248-031-6-155.

[20] P. Drahoš, E. Kučera, O. Haffner, I. Klimo, "Trends in industrial communication and OPC UA" Cybernetics & Informatics (K&I), pp. 1-5, 2018, doi: 10.1109/CYBERI.2018.8337560.

[21] M. Akerman, "Implementing Shop Floor IT for Industry 4.0". Ph.D. thesis, Department of Industrial and Materials Science, Chalmers University of Technology, 2018.

[22] W. Mahnke, S. Leitner, M. Damm, "OPC Unified Architecture", Springer Publishing Company, Incorporated, 2009, doi: 10.1007/978-3-540-68899-0.

[23] S. Sejwani, S. Tanwar, "Implementation of X.509 Certificate for Online Applications", International Journal of Research in Advent Technology, vol. 2, no. 3, pp. 250-254, 2014.

[24] A. Wazan, R. Laborde, F. Barrere, A. Benzekri, "The X.509 certificate quality". Third International Conference on Digital Information

Management, pp. 928-930, 2008, doi: 10.1109/ICDIM.2008.4746813.
[25] V. Hawanna, V. Kulkarni, R. Rane, P. Mestri, S. Panchal, "Risk Rating System of X.509 Certificates", Procedia Computer Science, vol. 89, pp. 152-161, 2016, doi: 10.1016/j.procs.2016.06.027.
[26] A. Alrawais, A. Alhothaily, X. Cheng, "X.509 Check: A Tool to Check the Safety and Security of Digital Certificates", International Conference on Identification, Information, and Knowledge in the Internet of Things (IIKI), pp. 130-133, 2015, doi: 10.1109/IIKI.2015.36.
[27] M. Behnam, R. Marau, P. Pedreiras, "Analysis and optimization of the MTU in real-time communications over Switched Ethernet", ETFA2011, pp. 1-7, 2011, doi: 10.1109/ETFA.2011.6059021.
[28] W. Hardy, QoS "Measurement and Evaluation of Telecommunications Quality of Service", John Wiley & Sons, Ltd, 2001.

تحسين توافر وموثوقية إنترنت الأشياء الصناعية باستخدام آلية الاتصال المزدوجة بالاعتماد على بروتوكول البنية الموحدة لاتصالات المنصات المفتوحة (OPC UA)

محمد باسل شكر*
mohammed.basil@ntu.edu.iq

جاسم محمد عبد الجبار**
drjssm@almaaqal.edu.iq

* قسم هندسة تقنيات الأجهزة الطبية، الكلية التقنية الهندسية، الجامعة التقنية الشمالية، الموصل، العراق
** قسم هندسة السيطرة والحاسبات، كلية الهندسة ،جامعة المعقل، البصرة، العراق

Received: May 16th, 2024 Received in revised form: July 16th, 2024 Accepted: July 31th, 2024

تاريخ الاستلام: 16 مايو 2024 استلم بصيغته المنقحة: 16 يوليو 2024 تاريخ القبول: 31 يوليو 2024

الملخص

في هذا البحث تم تصميم نظام عملي لإنترنت الأشياء الصناعي (IIoT) للمناطق التي تعاني من انخفاض جودة خدمات الإنترنت المقدمة من قبل مزودي خدمة الانترنت. يعتمد النظام المطور على نسخ وإرسال نفس البيانات في وقت واحد من خلال روابط الاتصال المزدوجة بين الخادم الذي يعمل ببروتوكول البنية الموحدة لاتصالات المنصات المفتوح (OPC UA) والعميل البعيد الذي يعمل أيضا ببروتوكول OPC UA. يمكن لهذه الطريقة تحسين توفر النظام المصمم وموثوقيته. تمت مراقبة ستة علامات تمثيلية والتحكم فيها في وقت واحد من خلال عميل OPC UA البعيد بمعدل مسح يبلغ 100 مللي ثانية على جانبي الخادم والعميل. تم إجراءعملية نقل آمنة وموثوقة للبيانات باستخدام خوارزمية AES 256 لتشفير العلامات التمثيلية لنقلها بين الخادم والعميل. أظهرت النتائج والحسابات تحسنا ملحوظا في توافر النظام وموثوقيته عند استخدام روابط الاتصال المزدوجة لإرسال نفس البيانات في وقت واحد.

الكلمات الداله:

البنية الموحدة لاتصالات المنصات المفتوحة ، إنترنت الأشياء الصناعية، تكنولوجيا المعلومات، التكنولوجيا التشغيلية، شبكات الحاسوب.