İSTANBUL UNIVERSITY
CERRAHPAŞA

ORIGINAL ARTICLE
Electrica 2023; 23(1): 70-78

A Novel Approach to Noise Reduction in IIoT Environment Using MCU

Sadeq Othman Al-Hamouz

Department of Computer Science, The World Islamic Sciences and Education University, Amman, Jordan

Cite this article as: S. O. Al-Hamouz, "A novel approach to noise reduction in IIoT environment using MCU," *Electrica*, 23(1), 70-78, 2023.

ABSTRACT

Everything in our modern life is connected through some kind of connectivity, and the term "internet" of everything is becoming widely applicable to almost every aspect of the modern lifestyle. Industries are very capable, and even in need, to get this connectivity all over their elements. This was the main push to launch the industry 4.0 that adapts the Internet of things (IoT) in industrial facilities.

The industrial IoT (denoted by IIoT) was a big breakthrough in modern industrial facilities that accelerated the production process and reduced accidents and the probability of human errors. Yet, there are some challenges that industrial facilities face in adopting IoT, one of which is the noise originating from the heavy motors and machines working around the factory.

This research introduces an easy to plug-and-play solution to the noise that affects data transmission between IIoT nodes, by programming a frequency-choosing and -hopping algorithm on a programmable chip that can be embedded within a microcontroller unit in IIoT nodes.

Index Terms—Internet of Things (IoT), Industrial Internet of Things (IIoT), Micro-controlling unit (MCU), frequency, programmable chip, Radio Frequency (RF)

I. INTRODUCTION

Internet of Things (IoT) is a term that denotes the connectivity of "things" in a certain environment through the "internet." This term is becoming familiar to almost everyone who has some knowledge of technology and communications. The environments where IoT is applied range over a wide spectrum, from simple house light controls to complex industrial facilities and large factories.

This term has expanded to include connectivity of everything (Internet of Everything) [1]. This connectivity has been classified into three main categories based on what is connected and where the data flows from/to as follows: people-to-people, people-to-machine, and machine-to-machine (M2M). The latter acts as the basis for understanding the manufacturing process [2, 3], which leads to efficient and sustainable production in industrial facilities [4]. Fig. 1 shows the interaction between the Internet of Everything main contributors.

In this research we shall focus on the M2M communication, since most IoT for industry uses them the most. Industrial IoT (IIoT) implies using intelligent advanced data analytics for transformation business outcomes.

Adding to the benefits of IoT, IIoT has additional advantages to the industries by lowering the risks of human-generated errors and increasing the precision of production, which would have a massive positive impact on the industrial processes [5]. Market revenues over the past years provide conclusive evidence of the positive impact of IIoT and experts [6] expect these revenues to reach about $110 billion by the year 2025, jumping from 82.7 in 2020. The chart in Fig. 2 shows this growth in revenues.

But same as everything in life, nothing comes without challenges. The IIoT has a set of challenges that might have a negative impact on adaptation and evolution in modern industries. These challenges include: standardization in some industrial facilities, especially when it comes to the infrastructure of the sensors and other entities' distribution and communications. Data integrity also has some negative impacts on the adoption of IoT technologies in the industry, along with some internal systems barriers and the liability of old and sometimes-obsolete technologies

Corresponding author:
Sadeq Othman Al-Hamouz

E-mail: sadeq.alhmouz@wise.edu.jo

Received: December 5, 2021

Revised: March 14, 2022

Accepted: March 21, 2022

Publication Date: May 30, 2022

DOI: 10.54614/electrica.2022.21167

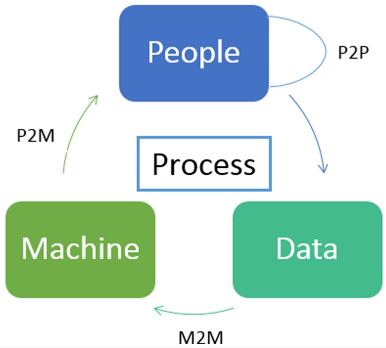

Fig. 1. Internet of Everything contributors (adapted from CISCO, accessed online from: (https://iotworm.com/cisco-internet-every thing-ioe-overview).

[8]. The Morgan Stanley/Automation World survey [9], conducted in 2016, whose respondents were workers in cybersecurity and industries, listed the top concerns and challenges to adopting IIoT. Fig. 3 shows the percentage of some of those challenges according to their impact on the adoption of IIoT.

As mentioned above, one of these challenges relies on the lack of standardization along with internal system barriers. Industrial facilities tend to have very big and very loud machines and moving parts. These are controlled through microcontroller units (MCUs) that communicate through wireless fidelity (WIFI), Bluetooth, or other radio frequencies (RF) frequencies, so some parts have an antenna and an interface device to facilitate the connections [10].

Controllers in factories usually communicate through RF, where sensors installed in mechanical parts send (and receive) data (and

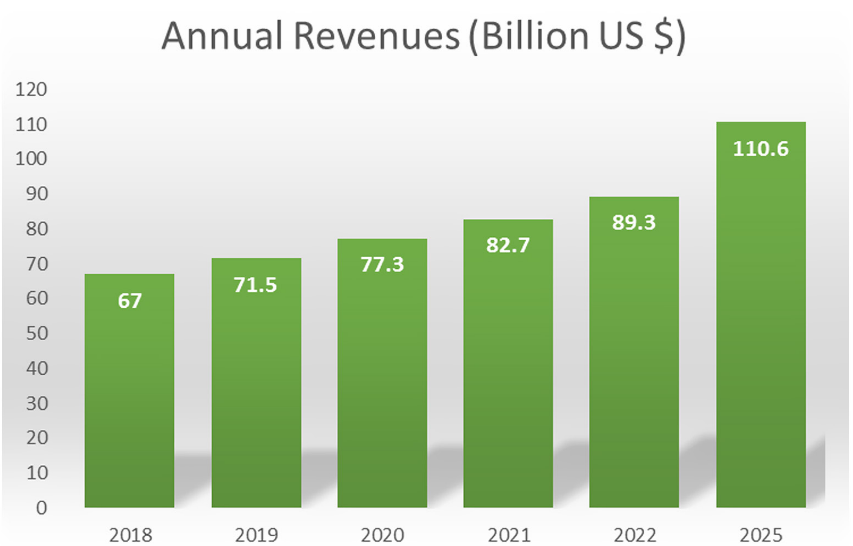

Fig. 2. Growth of IIoT revenues over the years (Source: Statista, 2021 [7]). IIoT, Industrial Internet of Things.

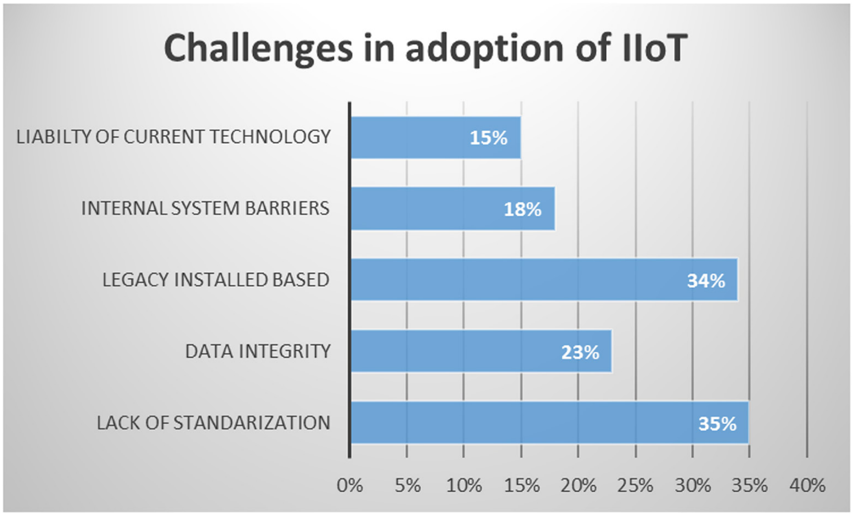

Fig. 3. Percentage of some challenges in adoption of IIoT (Source: Morgan Stanley Research, 2016 [9]). IIoT, Industrial Internet of Things.

commands). Interference with this RF has been a critical issue in most wireless communication, among which are factories and industrial facilities.

Research and inventions have focused on finding low-energy consumption and low-cost solutions to the RF signal interference issue. Some found that having a centralized co-ordination mechanism for wireless devices is a feasible solution [11], in which dedicated algorithms are operated through a shared service-level platform, which would serve as a flexible RF range devices manager. Yet, such a solution requires all IoT devices to be connected over the same platform and to be geographically co-located, which is not always the case in modern industrial facilities.

On the other hand, having distributed intelligent devices would be more efficient [12], especially in terms of power consumption for wide areas. These intelligent devices could have some machine learning techniques to help them self-organize by adapting communication parameters [13].

Other solutions to the RF interference issue were to have a symbiosis between cellular networks that provide IoT devices with needed communication signals infrastructure and a dedicated IoT network for connected devices by maximizing the sum rate of all IoT devices, to decide on the best cellular user RF to connect through [14], and this is done through deep reinforcement learning algorithm, which would consume time in the learning process.

In huge industrial facilities, most of the RF interference comes from the loud noise machines and robots produce. Limiting the effect of this noise would certainly improve signal transmission between connected devices in an IoT environment [15].

Machine learning was the main solution to resolving the noise reduction issue (or at least its effect on communication). Shao et. al. [16] adopted feature learning ML and deep auto-encoder's algorithms to reduce the effect of background noise in machines. The continuous hidden Markov model (CHMM) was also used in noise detection and removal in large industries [17]. Noise detection was done in the time and frequency domain, and the CHMM was used to characterize electromagnetic noise in detected signals.

Programmable chips provide a feasible solution to noise reduction issues in large industrial facilities. Some used programmable RF amplifiers [18] or some MCU [19], or dedicated circuits [20].

In this research, a single chip that is designed for very low power and very low voltage wireless applications is programmed to transmit or receive signals in an IIoT environment of a factory with large machines. An MCU tunes transmitted signals in order to get maximum gain at desired frequency and eliminate the noise originating from the machines.

II. RADIO SIGNAL INTERFERENCE

As IIoT is used in industrial sites, noise from surrounding machines is expected, especially with big air conditioning (AC) motors [21]. This noise affects the micro-controllers of small devices in three different ways: (1) big machines throw harmonics to the grid, which can be picked by the MCU, especially if they share the same power line, (2) direct electromagnetic interference (EMI) which can affect the controlling chip itself, and (3) EMI on the RF which decays data, corrupts it, weakens the signal, slows it down, and sometimes even cuts the signal. The harmonics issue can be solved with a good electric isolator and MCU can be protected from EMI by replacing it with something more resistible such as a programmable logic controller or by adding an isolation metal sheet around the controller to filter out the amount of EMI that it gets. However, there is no well-working solution to stop interference over RF simply because the signals are mixed in the air and there is nothing we can do about it. In this paper, we will propose a unique algorithm, which will not only solve the whole problem but will also be easy to implement and fully automated.

The proposed solution to this issue is to programing a dedicated chip [22] to transmit or receive any frequency between 300 and 1000 MHz. After transmitting the signal, an amplifier is used on the signal output, which consists of a multistage LC circuit (a tuned circuit), which mainly consists of an inductor (the L) and a capacitor (the C). The C value can be tuned digitally from the microcontroller to match the required frequency. In other words, the MCU can tune both the amplifier and the RF output in order to get the maximum gain of the desired frequency.

The CC1000 chip is a true single chip, ultra-high frequency transceiver designed for very low power and very low-voltage wireless applications, and it is based on Chipcon's SmartRF® technology in 0.35 μm CMOS with Cascaded noise figure 433/868 MHz of 12/13 dB [22].

Microcontrolled unit used in this research is ESP32, which has a built-in 2.4GHz antenna for WIFI and Bluetooth connectivity, in addition to two cores, which we will use in this research. This unit has embedded memory as a 448 KB Internal Read-only memory, a 520 KB Internal Static random-access memory, an 8 KB RTC FAST Memory, and an 8 KB RTC SLOW Memory [23]. Fig. 4 shows the structure of this unit.

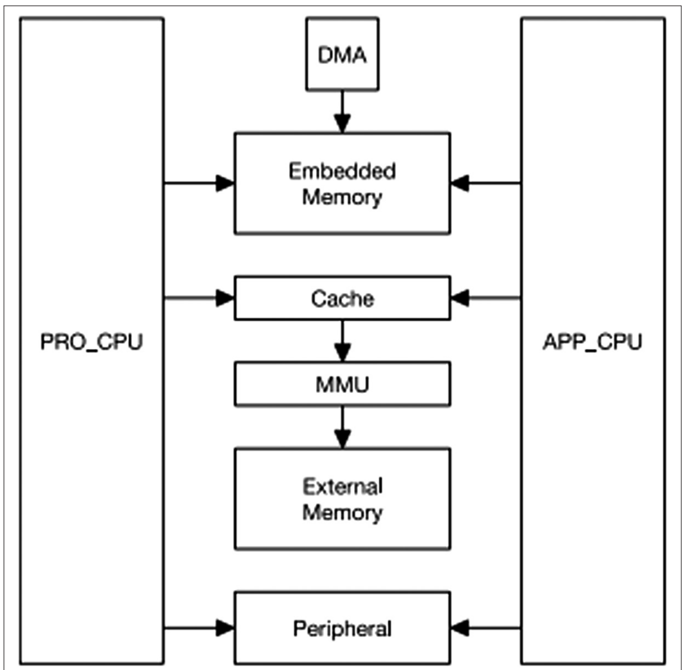

Fig. 4. ESP32 MCU system structure (adapted from EXP Technical Reference Manual). MCU, microcontroller unit.

In this research, Core1 in the MCU manages the frequency-filtering algorithm, the built-in 2.4GHz communication antenna, as well as tune frequency on the RF antenna and amplifier. In the meanwhile, core 0 is responsible for user application and does the actual data transmission on the RF antenna. This ensures achieving a plug-and-play transmission without complexities as no modifications are required to be made on the user's application. The system was tested in the packaging section of a plant, where noise induced from lifts and mechanical robots has effects on the sending and receiving test nodes.

III. SETTING THRESHOLDS

To choose on best frequency to send and receive data through, an acceptable threshold for RF as well as a threshold of noise (in order to divide it from actual data being transferred) need to be set ahead of running the algorithm. A threshold can be defined by user input, where a higher threshold means it is easier and faster to find a suitable frequency, but it also means slower data transfer rate and shorter distances as dropped packages number will increase and vice versa.

Setting a noise threshold should be according to specific frequency. This noise could be continuous, random or on a certain frequency. After monitoring data transmission, most noise was recorded on frequencies ranging between 260 MHz - 300 MHz, and 420 MHz - 470 MHz. a sample transmission that was recorded is shown in Fig. 5, where the amplitude peaks represent noise.

A software-defined radio (SDR) can show these in a much better way, as illustrated in Fig. 6.

Based on this observation, the SDR read frequencies from 330 to 530 MHz, and it is clear that strong noise (according to amplitude) shows on frequencies 334 MHz as it is commonly used, 372 MHz, 384 MHz, 428 MHz, 435 MHz, and 479 MHz. Those frequencies shall be avoided. There is also some noise on frequencies between 445 and 460 MHz, which is most likely from an induction motor nearby, and on frequencies 474–476 MHz

In IIoT systems, communicating nodes usually have a transmitter and a receiver. so noise reduction must be ensured for both sending and receiving nodes to achieve the best communication in the network.

IV. TRANSMITTING AND RECEIVING DATA

Data transmission begins with starting the microcontroller and initializing it. Then the algorithm will start reading the preferred frequencies array from EEPROM (an embedded, non-volatile memory within the MCU) and apply these frequencies one by one. If the array is empty, the algorithm will start with a predefined frequency of 500 MHz.

For each frequency, the amount of noise will be detected, measured, and stored. If the noise value is less than the defined threshold, the frequency is accepted and added to the preferred array.

When at least X number (which can be defined by the user) of noise frequency is detected, the algorithm will transmit data by hopping between these frequencies and waiting for a validation package, and when a validation package is received, the user's application is initialized.

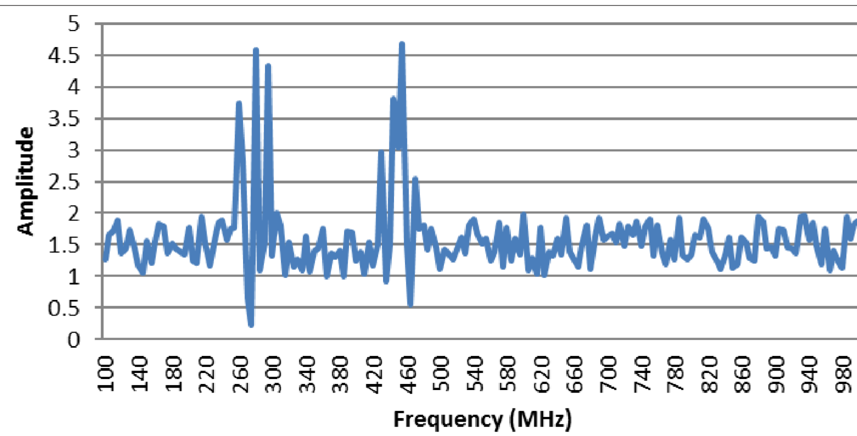

Fig. 5. Sample signal amplitude versus frequency of studied system used to define clear harmonics.

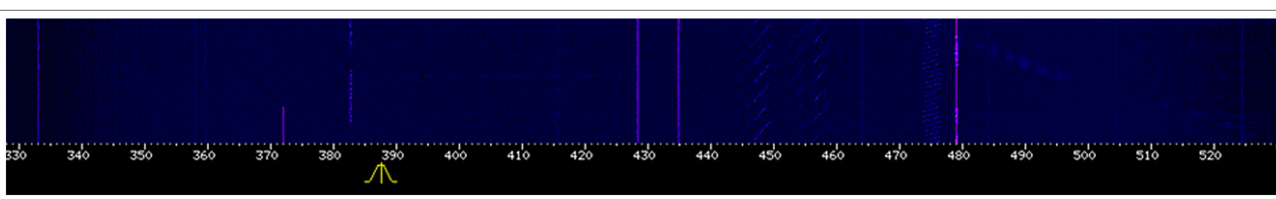

Fig. 6. SDR frequency amplitude. SDR, software-defined radio.

While running the user application, if noise on the stated channel becomes higher than the threshold, the algorithm will pause the user application, start again to search for a different low noise frequency, and then resume the user application.

The algorithm works in a similar manner on both receiver and transmitter nodes in terms of detecting which channels have noise and which do not. However, on the receiving node, nothing is transmitted at the initialization phase. Instead, it waits for the transmitter to send a message, then the receiver will detect that data by hopping and determine if it is a good channel or not according to the noise on it. The system's schematic is shown in Fig. 7, and it is the same for both transmitting and receiving nodes.

V. VALIDATION OF TRANSMISSION

Complexity shows that the receiver node may or may not have the same noise/harmonics depending on its location within the IIoT environment. This means that both receiver and transmitter should agree on a frequency, which urges the need for validation of transmission.

As the transmitter node will send data over multiple frequencies, the receiver node can detect data from frequencies where noise is low on its side and make sure that the transmitter is the source of that data by reading the package and comparing it with what the transmitter should send. If the transmitter offers a good frequency, the receiver will transmit a validation message back on the same channel and then both transmitter and receiver will run the user's application and keep monitoring noise levels at the same time.

However, if no good frequency is detected (maybe X number that was set by the user was too low for example), then no action is taken from the receiver for a specific timeout. When the transmitter times out and gets no response, it will find another array of frequencies, tries them out, and keeps doing this until the receiver responds over one of these frequencies.

According to this, the algorithm on the transmitting node can establish a connection with other nodes in extreme conditions, where different noise frequencies are applied on the receiver side as well as on the transmitter side.

VI. THE SYSTEM IN ACTION

As mentioned earlier, the programmable chip was installed on the MCU of an IIoT environment in a factory with heavy-duty machines that produce a lot of noise. The chip (shown in Fig. 8) was equipped with an organic light-emitting diode display for better visibility of the system's status and chosen frequency value.

When initializing the system, it enters the "stable" state with the user's application running. The system selected transmission frequency 387 MHz to begin transmitting.

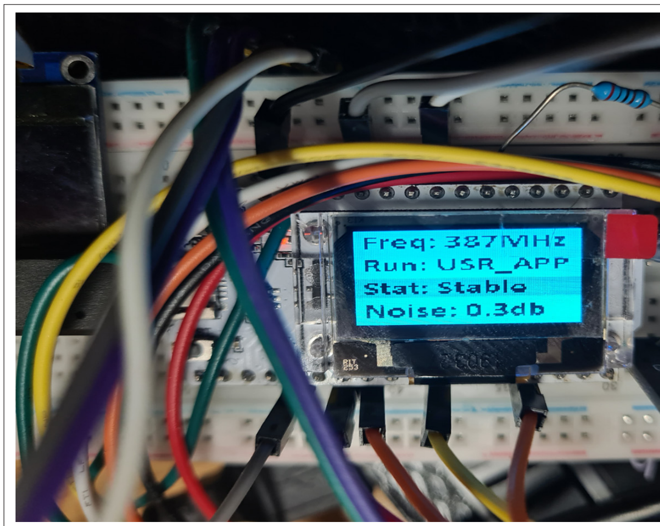

Fig. 8. The system is stable and frequency of 387 MHz is chosen.

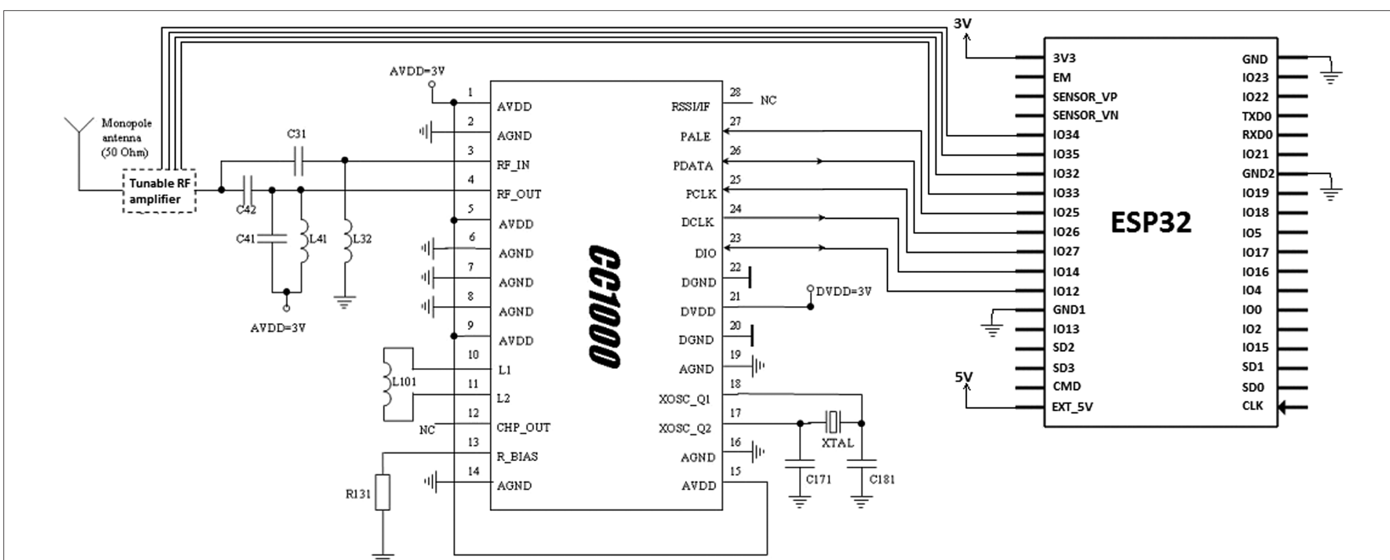

Fig. 7. The system's schematic.

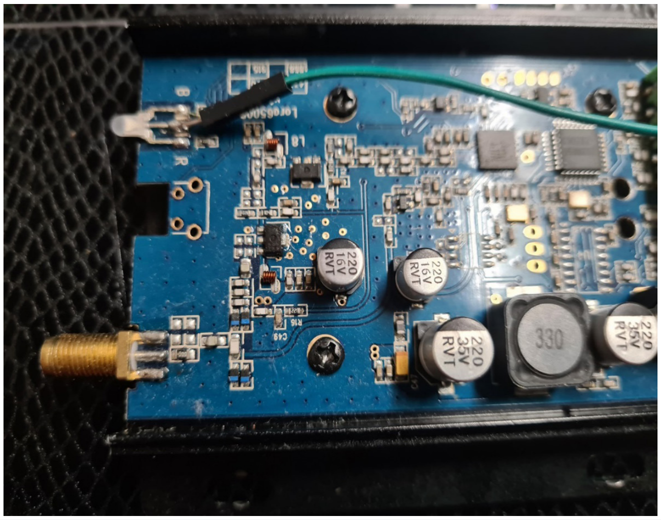

Fig. 9. PCB of programmable chip with amplifier and USB port (red circle). PCB, printed circuit board; USB, Universal Serial Bus.

The system was also equipped with a USD port placed on the printed circuit board with the RF amplifier. This is shown in Fig. 9.

Once the system is run, the frequencies strength is recorded over the chosen fixed frequency of 387 MHz that was selected as the user's application was initialized. This frequency value was chosen as a starting point to compare it with the output of the system as it continues to transmit and receive data. The chart in Fig. 10 shows the recorded signal strength over about 30 hours of the system has run.

These signal strength data and the number of dropped packages in a data transmission were between 0 and 5 as illustrated in Table I.

As the system runs, a strong noise was injected on purpose in the environment discretely (turning it on and off, every time with a different amplitude). This noise targets the exact frequency (387 MHz) to test how the system would react. In the graph in Fig. 11, these noise injections are clearly noticeable, and it shows how increasing the amplitude caused the system to lose the entire connection.

To test the validity of the proposed algorithm, the same exact conditions and signal values were re-applied with the algorithm activated.

TABLE I. SIGNAL STRENGTH RATE AND THE NUMBER OF DROPPED PACKAGES

Signal Strength Rate	Signal Strength	Number of Dropped Packages
5	Excellent	<17%
4	Very good	Between 17% and 34%
3	Good	Between 34% and 50%
2	Bad	Between 50% and 68%
1	Very bad	Between 68% and 90%
0	No connection	>90%

As shown in the plot in Fig. 12, injected noise did affect the signal strength, but this effect was temporary as the system was able to find a new frequency every time this happened. The noise injected had the same amplitude, but it targeted the frequency to which the system's transmission jumped. Connectivity was lost one time, but it was for a very short period as the system immediately jumped to another frequency.

This test shows that the proposed algorithm applied to the system was very effective when dealing with noise targeting transmitted data, as the receiving nodes would only respond if they were able to detect this "noise free" frequency that the transmitter node used.

VII. CONCLUSIONS

Adopting IIoT is becoming inevitable to modern industrial facilities, especially those that seek excellence end efficiency in the production process. Yet, nothing comes challenges-free, as IIoT systems rely on communication between nodes that usually reside within a noisy environment, this communication might suffer from disturbance or loss.

This research paper introduced a novel technique that not only ensures a reliable IIoT communication infrastructure but also can maintain an uninterrupted data transmission at a very low cost and is easy to plug-and-play within standing IIoT systems.

The introduced system uses a programmable chip that connects to an MCU with an amplifier to strengthen the transmitted signal. It

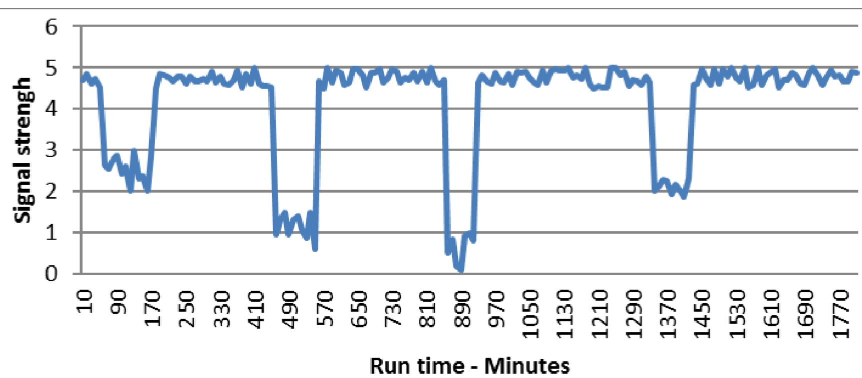

Fig. 10. Signal strength recording over pre-set frequency of 387 MHz for 30 hours.

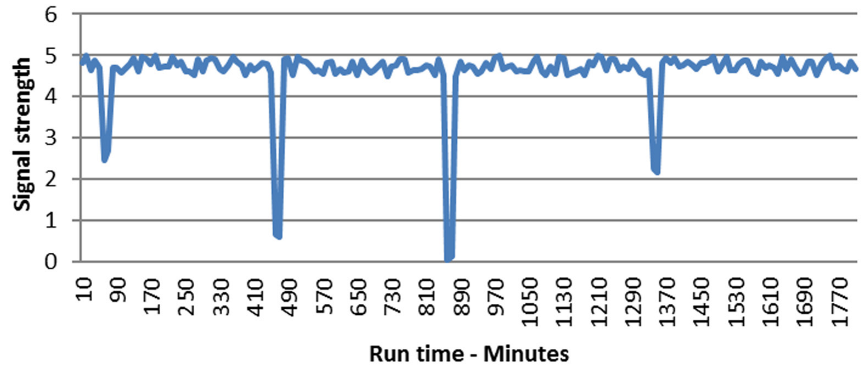

Fig. 11. Signal strength on frequency 387 MHz with injected noise.

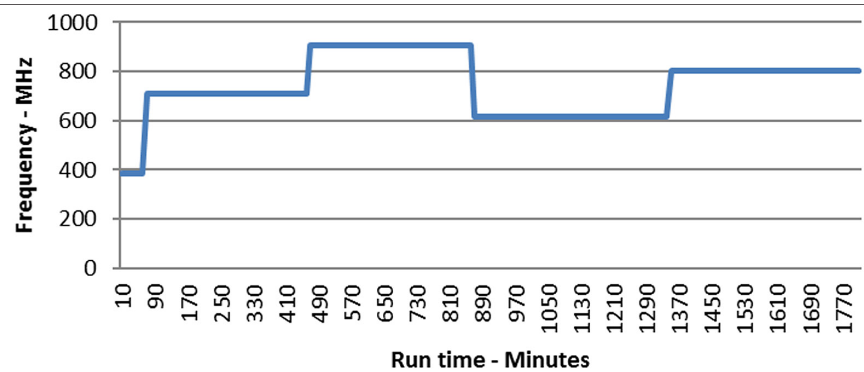

Fig. 12. Frequency selection over time using proposed algorithm.

records available frequencies and uses a pre-defined threshold for usable frequencies along with a threshold for the acceptable noise level. It uses hopping between available, noise-free frequencies that are common between the sender and the receiver nodes.

Testing the system showed great potential to adopt it, with its simple, yet effective, implementation that suits almost any IoT environment and especially those in industrial facilities.

Peer-review: Externally peer-reviewed.

Acknowledgment: I am very much thankful to The World Islamic Sciences and Education University (WISE), the reviewers, and editors.

Declaration of Interests: The author declare that they have no competing interest.

Funding: The author declared that this study has received no financial support.

REFERENCES

1. L. DeNardis, *The Internet in Everything*. New Haven, CT: Yale University Press, 2020.
2. B. DiMartino, K. C. Li, L. T. Yang, and A. Esposito, "Trends and strategic research in internet of everything", in *Internet of Everything*. Singapore: Springer, 2018, pp. 1–12.
3. V. L. Kalyani, and D. Sharma, "IoT: Machine to machine (M2M), device-to-device (D2D) internet of everything (IoE) and human-to-human (H2H): Future of communication," *J. Manag. Eng. Inf. Technol.*, vol. 2, no. 6, pp. 17–23, 2015.
4. E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial internet of things: Challenges, opportunities, and directions," *IEEE Trans. Ind. Inform.*, vol. 14, no. 11, pp. 4724–4734, 2018. [CrossRef]
5. W. Z. Khan, M. H. Rehman, H. M. Zangoti, M. K. Afzal, N. Armi, and K. Salah, "Industrial internet of things: Recent advances, enabling technologies and open challenges," *Comput. Electr. Eng.*, vol. 81, 2020. [CrossRef]
6. IndustryARC Analysis and Expert Insights, *Industrial IoT (IIoT) Market Report - Global Industry Data, Analysis and Growth Forecasts by Type, Application and Region, 2021–2028*", Industry ARC, 2021. Available at: https://www.researchandmarkets.com/reports/5349307/industrial-iot-iiot-market-report-global
7. Statista, "Global business data platform". Available: https://www.statista.com/statistics/611004/global-industrial-internet-of-things-market-size/. [Accessed: October 1st, 2021].
8. A. Chowdhury, andS. A. Raut, "Benefits, challenges, and opportunities in adoption of industrial IoT," *Int. J. Comp. Intell. IoT*, vol. 2, no. 4, 2019.
9. Morgan Stanley Research, "Morgan Stanley Automation world Industrial Automation Survey," 2016. Available: https://www.morganstanley.com/ideas/industrial-internet-of-things-and-automation-robotics. [accessed: October, 2021].
10. K. Mikhaylov, J. Tervonen, J. Heikkilä, and J. Känsäkoski, "Wireless sensor networks in industrial environment: Real-life evaluation results", in 2nd Baltic Congress on Future Internet Communications, Vol. 2012. IEEE Publications, 2012, pp. 1–7. [CrossRef]
11. M. Tesanovic, P. Bucknell, H. Chebbo, and J. Ogunbekun, "Service-domain solutions to radio interference for M2M communications and networking", In *IEEE Globecom Workshops*, Vol. 2012. IEEE Publications, 2012, pp. 1712–1717. [CrossRef]
12. N. Nurelmadina *et al.*, "A systematic review on cognitive radio in low power wide area network for industrial IoT applications," *Sustainability*, vol. 13, no. 1, p. 338, 2021. [CrossRef]
13. A. Azari, and C. Cavdar, "Self-organized low power IOT networks: A distributed learning approach", in IEEE Global Commun. Conference (GLOBECOM), Vol. 2018. IEEE Publications, 2018, pp. 1–7. [CrossRef]

14. Q. Zhang, Y. C. Liang, and H. V. Poor, "Intelligent user association for symbiotic radio networks using deep reinforcement learning," *IEEE Trans. Wirel. Commun.*, vol. 19, no. 7, pp. 4535–4548, 2020. [CrossRef]
15. T. Rieger, S. Regier, I. Stengel, and N. L. Clarke, *Fast Predictive Maintenance in Industrial Internet of Things (IIoT) with Deep Learning (DL): A Review*. CERC, 2019, pp. 69–80. Available at: http://ceur-ws.org/Vol-2348/paper05.pdf
16. H. Shao, H. Jiang, F. Wang, and H. Zhao, "An enhancement deep feature fusion method for rotating machinery fault diagnosis," *Knowl. Based Syst.*, vol. 119, pp. 200–220, 2017. [CrossRef]
17. Y. Ze, L. Liu, T. Cheng, Z. Kun, and Z. Jianhua, "Measurement based characterization of electromagnetic noise for industrial internet of things at typical frequency bands", In *IEEE Wireless Communications and Networking Conference (WCNC)*, Vol. 2019. IEEE Publications, 2019, pp. 1–6. [CrossRef]
18. H. Xiao-Feng, M. Tai-Shan, M. Cheng-Yan, Y. Tian-Chun, G. Ye-Bing, and Q. Min, "RF programmable amplifier with low noise single-ended differential circuit,"."电子与信息学报," vol. 34, no. 4, pp. 976–980, 2012.
19. A. Villarroel, G. Zurita, and R. Velarde, "Development of a low-cost vibration measurement system for industrial applications," *Machines*, vol. 7, no. 1, p. 12, 2019. [CrossRef]
20. G. M. Dousoky, M. Shoyama, and T. Ninomiya, "FPGA-based spread-spectrum schemes for conducted-noise mitigation in DC–DC power converters: Design, implementation, and experimental investigation," *IEEE Trans. Ind. Electron.*, vol. 58, no. 2, pp. 429–435, 2010. [CrossRef]
21. S. D. Milić, N. M. Miladinović, and A. Rakić, "A wayside hotbox system with fuzzy and fault detection algorithms in IIoT environment," *Control Eng. Pract.*, vol. 104, 2020. [CrossRef]
22. "CC1000 Technical Specifications document, Texas Industries". Available: https://www.ti.com/lit/ds/symlink/cc1000.pdf?HQS=dis-mous-null-mousermode-dsf-pf-null-wwe&ts=1631556210948&ref_url=https%253A%252F%252Feu.mouser.com%252F. [Accessed: Dec. 2021].
23. "ESP32 technical reference manual, Espressif systems 2021". Available: https://www.espressif.com/sites/default/files/documentation/esp32_technical_reference_manual_en.pdf. [Accessed: Dec. 2021].

Dr. Sadeq Al-Hamouz is a professor in artificial intelligence (AI), Vice-dean of the Faculty of Information Technology, and the chair of the Computer Science Department, the World Islamic Sciences and Education University (WISE). He received his first Ph.D. Diplome de Doctuer in Algorithm analysis and design in 1980 from Besancon University/ France. He then joined Yarmouk University/Jordan as an assistant professor (1980-1983). He then acquired a second Ph. D. in Expert Medical Database Systems from the University of Liverpool/England in 1987. He then returned as the chair of the Computer Science Department in Yarmouk University/Jordan (1987-1993). He then worked as the Dean and Center Coordinator of the Technical Industrial College/Sultanate Oman (1993–1999). He then returned and worked as the Department of Computer Information Systems the chair in the Applied Science University/Jordan (1999–2004). He then worked as the chair of the Computing Studies Department in Amman Arab University for Graduate Studies/Jordan (2004–2008). He then joined as a faculty in Um Al-Qura University, KSA (2008–2013). He then returned to Jordan as assistant dean and chair of the Computer Information Systems, Middle East University/Jordan (2013–2016). Prof. Al-Hamouz research interests include Fuzzy Databases, Expert Medical Database Systems, and Health Information systems, Genetic Algorithms, Database Security, Intrusion Detection Systems, Image Steganography, and Human-Robotics Interaction. He has published more than 40 journal papers and conference papers and has published one book entitled Discrete Structures and a dictionary entitled Dictionary of Discrete Structures.