A COMPARATIVE STUDY TO EXPLORE COMMUNICATION PROTOCOLS FOR IOT AND IIOT DEVICES

Pravin M. Sontakke, Amrut S. Lanje

Department of Electronics, Kamla Nehru Mahavidyalaya, Nagpur (M. S.) India

Department of Electronics, Dr. Ambedkar College, Chandrapur (M. S.) India

ABSTRACT

This paper presents a comparative study of various wireless communication protocols used in the Internet of Things (IoT) and Industrial Internet of Things (IIoT). It analyses protocols like Wi-Fi, Bluetooth, Zigbee, Z-Wave, LoRaWAN, NB-IoT, Sigfox, Thread, and 6LoWPAN, focusing on their unique use cases and trade-offs. The study aims to guide decision-making and help engineers, developers, and stakeholders make informed decisions in designing and deploying IoT and IIoT solutions. As the landscape of communication protocols evolves rapidly, this comparative study seeks to unravel the complexities of connectivity, providing insights into the strengths and limitations of each protocol. This paper also covers the wired connectivity options for the stand-alone embedded systems and an overview on minimum hardware and software requirement for the implementation of typical protocol in an IoT and IIoT system. Through a meticulous analysis, this research endeavours to contribute to the advancement of resilient and scalable communication frameworks, fostering innovation and efficiency in the ever-expanding domains of IoT and IIoT.

Keywords: Communication protocols, IoT (Internet of Things), IIoT (Industrial Internet of Things), Wireless communication, Connectivity, Power consumption, Topology, Security Wi-Fi, Bluetooth, Zigbee, Z-Wave, LoRaWAN, NB-IoT (Narrowband IoT), Sigfox, Thread, 6LoWPAN

INTRODUCTION:

The continuous use of smart technology to change conventional manufacturing and industrial processes is known as the Fourth Industrial Revolution, or Industry 4.0[1]. It is marked by the Internet of Things (IoT), automation, and the incorporation of digital technology into many industrial domains[2]. Within this framework, Industry 4.0 improvements are mostly driven by the Internet of things (IoT) and Industrial Internet of Things (IIoT). The IoT and IIoT revolutionize communication by enabling seamless data exchange between devices. In a society with increasing use of internet, devices like industrial sensors, smart homes, and automated machinery are connected through the use of wireless communication protocols. So it is essential to understand and optimize the wireless communication protocols to cater the growing number of IoT and IIoT devices. These protocols act as the hidden threads that connect a wide range of IIoT and IoT devices, allowing them to exchange data, connect, and work together to create the connected intelligence systems. The key requirements of the IoT and IIoT protocols are reliability, low latency, and ability to communicate with minimum power consumption[3,4]. Thus on this background the study of wireless communication protocols becomes very important to provide precise overview which can comprehend, optimize and innovate the networking of devices.

This study explores the complex field of wireless communication protocols designed for Internet of Things and Internet of Things-related applications. It looks at the special qualities, advantages, and disadvantages of various protocols in an effort to understand their complexities. We want to clarify the important factors that engineers, developers, and stakeholders need to take into account when choosing the best protocol for a particular IoT or IIoT implementation

This study explores various wireless communication technologies like Bluetooth Low Energy, Wi-Fi, LoRa, Zigbee, and NB-IoT, highlighting their unique qualities for designing scalable, resilient IoT and IIoT ecosystems and opens the gateway to unprecedented opportunities for innovation, efficiency, and a more connected future with the better ability to make correct choice of a communication protocol. Some key aspects highlighting the significance of such study are:

1. Optimized System Design
2. Efficient Resource Utilization
3. Scalability and Interoperability
4. Security Implementation
5. Energy Efficiency
6. Application-Specific Suitability
7. Cost-Effectiveness
8. Adaptability to Environmental Conditions
9. Future-Proofing
10. Informed Decision-Making.

With this consideration comparative study of wireless communication protocols for IoT devices ensures technical robustness and alignment with specific application needs and constraints.

Global importance: Wireless communication protocols for IoT devices significantly impact businesses and daily life worldwide, facilitating smooth connectivity, data sharing, and automation. Recent advancements in these protocols have global significance in following areas of applications:

1. **Global Interconnectedness:**
   Wireless communication protocols enable global IoT ecosystems, connecting devices and systems across borders, crucial for industries like logistics, supply chain management, and smart cities, requiring international collaboration.
2. **Industrial IoT (IIoT) Advancements:**
   Wireless protocols in the industrial sector enable advanced monitoring, control, and optimization of processes, with recent innovations focusing on reliability, low-latency communication, and integration with edge computing[5].
3. **Smart Cities and Infrastructure:**
   Wireless communication protocols are crucial for smart cities, enabling IoT devices to monitor and manage infrastructure, support efficient traffic, waste, energy optimization, and public safety applications globally[6–8].
4. **Agricultural IoT (AgriTech):**
   IoT devices, particularly precision agriculture protocols, are revolutionizing international agricultural practices by enabling farmers to optimize crop yield, conserve resources, and make data-driven decisions[6].
5. **Healthcare IoT:**
   Wireless protocols are crucial for healthcare IoT applications, enabling remote patient monitoring, asset tracking, and efficient equipment management, with recent innovations focusing on security and privacy measures[5].
6. **Global Supply Chain Optimization:**
   Wireless communication protocols enhance global supply chain optimization by providing real-time visibility, improving tracking accuracy, reducing latency, and enhancing overall efficiency[9,10].

7. **Emerging LPWAN Technologies:**

   LPWAN technologies like LoRaWAN and NB-IoT offer long-range communication with minimal power consumption, with innovations focusing on extending range, improving data rates, and enhancing coverage.

8. **5G Integration:**

   IoT integration with 5G networks improves connectivity, data speeds, and reliability, supporting mission-critical IoT applications globally and leveraging 5G's ultra-low latency capabilities.

9. **Edge Computing Integration and Blockchain Integration for Security:**

   Edge computing and wireless communication protocols are enhancing IoT data processing efficiency and security, while blockchain technology enhances data integrity, authentication, and secure transactions in global IoT applications[11].As international collaboration continues, standardization efforts and the development of open protocols are crucial for ensuring seamless communication across diverse IoT ecosystems globally. Innovations in wireless communication protocols contribute to creating a more interconnected and efficient world.

WIRED AND WIRELESS CONNECTIVITY OPTIONS FOR MICROCONTROLLER BASED SYSTEMS:

Microcontroller-based standalone control systems offer wired and wireless connectivity options for PC interface, based on factors like data transfer rate, range, power consumption, and application requirements as shown in table 1:

Wired and wireless connectivity options			
Type of connectivity	**Name of the connectivity option**	**Description**	**Application**
Wired connectivity	Serial Communication (UART, RS-232, RS-485)	Serial communication protocols like UART, RS-232, and RS-485 provide simple, low-to-medium data rate communication	Programming microcontrollers, data logging, debugging
	Ethernet	Ethernet enables high-speed data transfer over local networks.	Industrial automation, remote monitoring, high-speed data exchange.
	USB (Universal Serial Bus)	USB is a widely used wired connectivity option that allows high-speed data transfer	Programming microcontrollers, data

		between a microcontroller and a PC.	logging, debugging.
Wireless Connectivity	Wi-Fi	Wi-Fi enables wireless communication over local area networks (LANs). It allows for high-speed data transfer and is suitable for applications requiring wireless connectivity within a limited range.	Home automation, IoT applications, remote monitoring
	Bluetooth/BLE (Bluetooth Low Energy)	Bluetooth and BLE provide short-range wireless communication. BLE is particularly suitable for low-power applications	Wireless sensors, wearable devices, short-range communication
	Zigbee	Zigbee is a wireless communication standard designed for low-power, low-data-rate applications. It operates in the 2.4 GHz frequency band	Home automation, industrial control systems, wireless sensor networks.
	RF (Radio Frequency)	RF modules enable wireless communication over radio frequencies. They can be used for simple wireless data exchange between a microcontroller and a PC.	Remote control systems, low-cost wireless communication
	NRF24L01 (2.4 GHz Wireless Transceiver Module)	The NRF24L01 is a popular wireless transceiver module operating in the 2.4 GHz frequency range. It is commonly used for low-cost wireless communication between microcontrollers	Wireless sensor networks, hobbyist projects.
	LoRa (Long Range):	LoRa is designed for long-range communication with low power consumption. It is suitable for applications that require communication over extended distances.	Long-range sensor networks, IoT applications in rural areas.
	NB-IoT (Narrowband IoT)	NB-IoT is a cellular communication standard designed for IoT applications. It provides wide-area coverage with low power consumption.	IoT devices in remote locations, smart city applications
	Z-Wave	Z-Wave is a wireless communication protocol operates in the sub-1GHz frequency range and is known for its low power consumption and reliability	Home automation
	Sigfox	Sigfox is a proprietary, low-power, wide-area networking technology designed for long-range communication with a focus on low-cost, low-power devices.	Asset tracking and environmental monitoring
	Thread	Thread is a wireless networking protocol built on IPv6 and is designed to provide secure and reliable communication between IoT devices	Home automation
	6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks)	6LoWPAN is an open standard that enables the transmission of IPv6 packets over low-power, low-data-rate wireless networks.	sensor networks and IoT applications

Table 1: Wired and Wireless connectivity options

COMPARISON OF WIRELESS COMMUNICATION PROTOCOLS:

Wireless Protocol	Range	Data rate	Power Consumption	Topology	Security	Deployment Cost
Wi-Fi	100 meters	High	Relatively high power consumption.	Star topology.	Robust security features.	Moderate to high
Bluetooth /BLE	100 meters / <100 meters	Moderate	Low power consumption, especially BLE.	Point-to-point or star topology.	Good security features.	Low to moderate
Zigbee	100 meters	Low to moderate	Low power consumption.	Mesh	Provides security features	Moderate
Z Wave	100 meters	Low.	Low power consumption.	Mesh.	Security for home automation.	Moderate.
Lora WAN	Several kilometres.	Low.	Low power consumption	Star of stars	Provides security mechanisms.	Relatively low
NB-IoT	Long range	Low to moderate	Low power consumption.	Cellular network topology.	Cellular network security features.	Moderate
Sigfox	Tens of kilometres.	Low.	Low power consumption.	Star	Security features in place.	Low
Thread	100 meters	Moderate	Low to moderate power consumption.	Mesh networking.	Security features based on 802.15.4 and IPv6.	Moderate
6LoWPAN	100 meters	Low to moderate.	Low power consumption.	Mesh networking.	Security considerations are present.	Moderate

Table 2: Comparison of wireless protocols based on different parameters

The following table 3 contains the generalized hierarchy based on the parameters. The consideration of typical parameter or stressing on specific requirement the hierarchy may differ for different users.

Significant IoT design parameter	Typical Value	Wireless communication protocol hierarchy
Communication range	Short-Range	• Bluetooth/BLE • Zigbee • Z-Wave • Thread

		• 6LoWPAN
	Medium Range	• Wi-Fi
	Long Range	• LoRaWAN • NB-IoT • Sigfox
Security and Power Efficiency	High Security and Low Power Consumption	• Bluetooth/BLE • Z-Wave • NB-IoT • Thread
	Moderate Security and Power Consumption	• Zigbee • LoRaWAN
	Varied Security and Low Power Consumption	• 6LoWPAN
	Varied Security and varied Power Consumption:	• Wi-Fi
	Low Security and Low Power Consumption	• Sigfox
Application specific	Home Automation	• Zigbee • Z-Wave • Thread
	Industrial application	• Zigbee • LoRaWAN • NB-IoT
	Wide area application	• LoRaWAN • NB-IoT • Sigfox
	High data rate applications	• Wi-Fi • Bluetooth
	Low power low data rate application	• BLE • Zigbee • Z-Wave • LoRaWAN • NB-IoT • Sigfox • Thread • 6LoWPAN

Table 3: Wireless communication protocol hierarchy based on different design considerations and area of application

The hardware and software requirements for implementing communication protocols in IoT devices vary based on the protocol, application, and device complexity, requiring detailed documentation. Table 4 contains the minimum hardware and software requirement for the implementation of different communication protocols.

Wireless communication protocol	Minimum Hardware requirement	Software requirement
WIFI	• Microcontroller or microprocessor with Wi-Fi module (e.g., ESP8266, ESP32). • Wi-Fi antenna.	• Wi-Fi stack. • TCP/IP stack. • Application-specific software
	• Microcontroller or microprocessor with Bluetooth/BLE module. • Bluetooth/BLE antenna.	• Bluetooth/BLE stack. • Application-specific software
ZigBee	• Microcontroller or microprocessor with Zigbee module (e.g., XBee module). • Zigbee antenna.	• Zigbee stack. • Application-specific software
Z-WAVE	• Z-Wave transceiver module. • Microcontroller or microprocessor.	• Z-Wave protocol stack. • Application-specific software
LoRaWAN	• Microcontroller or microprocessor with LoRa transceiver (e.g., SX127x). • LoRa antenna.	• LoRaWAN stack • Application-specific software
NB-IoT	• NB-IoT modem or module. • Microcontroller or microprocessor.	• NB-IoT stack. • Application-specific software
sigfox	• Sigfox modem or module. • Microcontroller or microprocessor.	• Sigfox stack. • Application-specific software
THREAD	• Microcontroller or microprocessor with Thread module (e.g., Nordic nRF52 series). • Thread-compliant radio.	• Thread stack. • Application-specific software
6LoWPAN	• Microcontroller or microprocessor with 6LoWPAN transceiver.	• 6LoWPAN stack. • Application-specific software

Table 4: Minimum hardware and software requirement of a typical wireless protocol

IoT PROTOCOLS:

The foundation of the Internet of Things ecosystem is made up of networked devices, and IoT protocols are essential to facilitating smooth communication and data sharing between them[12]. MQTT (Message Queuing Telemetry Transport) is a well-known protocol that is renowned for its effective and lightweight communication mechanism. With the help of a central broker, MQTT uses a publish/subscribe architecture to enable device communication. Because it performs well in settings when bandwidth is scarce, smart home automation, industrial applications, and a variety of Internet of things use cases favor it. Constrained Application Protocol, or CoAP, is another important protocol that was created especially for IoT networks' resource-constrained devices. Similar to HTTP, CoAP uses a request/response protocol, although it is designed for low-power and low-bandwidth settings. CoAP is suited for applications because to its RESTful architecture, lightweight design, and use of UDP[13].

HTTP (Hypertext Transfer Protocol) is widely used in traditional online applications, because of which it continues to be a fundamental protocol[14] in the Internet of Things. In web-centric Internet of Things applications, this request/response-based protocol is especially used to enable devices to effectively retrieve data from servers and communicate with them. However, one protocol that stands out as being particularly well-suited for data-centric, real-time communication in distributed systems is DDS (Data Distribution Service). Because DDS supports Quality of Service (QoS) regulations and has a publish/subscribe format, it is widely used in industrial automation and healthcare, where real-time control and monitoring are essential. The selection of a protocol becomes a strategic option as the Internet of Things (IoT) ecosystem grows, taking into account many considerations such device limitations, communication patterns, and application domain needs.

Table 5 gives a quick review on the commonly used IoT protocols: MQTT (Message Queuing Telemetry Transport), CoAP (Constrained Application Protocol), HTTP (Hypertext Transfer Protocol), and DDS (Data Distribution Service)[15].

IoT Protocol	**Feature**	**Communication model**	**Characteristics**	**Applications**
MQTT (Message Queuing Telemetry Transport)	• Lightweight • Efficient • Reliable communication between devices	Publish/subscribe model with a central broker	• Low bandwidth usage. • Asynchronous communication. • QoS levels (Quality of Service) for message delivery reliability. • Widely used in IoT for its simplicity and efficiency.	• **Smart Home Systems** • **Industrial Automation**
CoAP (Constrained Application Protocol)	• Designed for resource-constrained devices and networks, s • suitable for IoT applications	Request/response model, similar to HTTP	• RESTful architecture. • Lightweight header for reduced overhead. • UDP-based for simplicity and efficiency	• **Smart Cities** • **IoT Devices with Low Power Consumption**
HTTP (Hyper Text	• **Text based** • **Simple header**	Request/response model	• Stateful or stateless communication.	• **Web-Based IoT**

Transfer Protocol)	**structure**		• Utilizes TCP for reliable communication.	**Application** • **Data Retrieval s**
DDS(Data Distribution Service)	• Real time and • Data centric communication	Publish/subscribe model with a decentralized architecture	• Support for Quality of Service (QoS) policies. • Optimized for large-scale, real-time systems.	• Industrial automation • Healthcare system

Table 5: Review on different IoT protocols

Merits and Demerits of IoT protocols:

IoT Protocol	Merits	Demerits
MQTT (Message Queuing Telemetry Transport)	• Low Overhead: Lightweight protocol with low network and processing overhead • Publish-Subscribe Model: enabling efficient one-to-many communication. • Quality of Service (QoS) ensuring reliable message delivery. • Asynchronous: real-time communication without the need for continuous connections.	• Designed for Constrained Devices efficient in terms of processing and memory usage. • RESTful Design: simplifying integration with web technologies. • Low Overhead: Compact binary encoding contributing to low overhead. • UDP Transport: useful where low latency is crucial
CoAP (Constrained Application Protocol)	• Designed for Constrained Devices: efficient in terms of processing and memory usage. • RESTful Design: follows a RESTful design similar to HTTP, simplifying integration with web technologies. • Low Overhead: Compact binary encoding reduces message size, contributing to low overhead. • UDP Transport: suitable for scenarios where low latency is crucial.	• Limited Adoption: While gaining traction, CoAP adoption is not as widespread as HTTP or MQTT. • Complicated: be complex for certain use cases due to its RESTful design and reliance on additional protocols for security.
HTTP (Hyper Text Transfer Protocol)	• Simple and Human-Readable: easy to read and debug, simplified development and troubleshooting. • Supports Various Data Formats: handle different data formats, including HTML, XML, JSON, and more. • Statelessness: Each request from the client is independent, promoting scalability and simplicity. • Secured Version (HTTPS): secure connection (HTTPS) ensuring data confidentiality and integrity.	• High Latency: Synchronous nature and request-response model can introduce higher latency compared to other protocols. • Inefficient for Real-Time Communication: Not well-suited for real-time applications due to its connection-based nature and potential delays.
DDS(Data Distribution Service)	• **Real-time Communication:** Optimized for low-latency, real-time communication. • **Decentralized Architecture:** No central broker, which can enhance scalability. • **Quality of Service (QoS):** Supports configurable QoS policies for reliability and latency	• **Complexity: Implementation and configuration can be complex.** • **Resource Usage: May not be suitable for resource-constrained devices due to higher resource usage.**

Table 6: IoT protocols - merits and demerits

RESULTS AND DISCUSSION:

The study investigated and compared various wireless connectivity options and frond that Bluetooth/BLE and Wi-Fi are flexible wireless communication technologies that may be used for a range of Internet of Things applications. Low-power mesh networking options like Z-Wave and Zigbee are perfect for industrial and home automation uses. Low-power, wide-area installations can benefit from NB-IoT, however it does require cellular connectivity and may incur subscription fees. Sigfox delivers secure mesh networking and long-range connection through a subscription model, whereas Thread offers both. The selection of wireless technology is influenced by variables such as infrastructure availability, data rates, power consumption, and range.

The comparative study of various communication protocols for both Internet of Things (IoT) and Industrial Internet of Things (IIoT) devices including MQTT, CoAP, HTTP, and DDS provide insights into the performance, scalability, and suitability of these protocols in different application scenarios.The Internet of Things (IoT) ecosystem relies on networked devices and IoT protocols for smooth communication and data sharing. MQTT, a lightweight protocol, is ideal for smart home automation and industrial applications. Constrained Application Protocol (CoAP), designed for resource-constrained devices, uses a request/response protocol with a RESTful architecture and UDP for low-power and bandwidth settings.HTTP and DDS are key protocols in the Internet of Things, enabling devices to retrieve and communicate data, with their choice based on device limitations and application domain needs. MQTT and CoAP have lower latency compared to HTTP and DDS in both IoT and IIoT environments. These protocols exhibite higher throughput, making them preferable for scenarios demanding efficient data transfer, like sensor networks in industrial settings. thus MQTT and CoAP are more resource-efficient than HTTP and DDS especially for resource-constrained IoT devices with limited processing power and memory. These protocols have better scalability which makes them suitable for large scale deployment of IoT and IIoT devise.

Though each protocol supports encryption and authentication, it is found that MQTT and CoAP have stronger security implementation than other protocols.

CONCLUSION:

Since every protocol has advantages and disadvantages of its own, they can be used for a range of Internet of Things applications. The type of data being sent, the limitations of the device, and the features of the application all influence the protocol that is utilized. As IoT develops, there will probably be additional changes and adjustments made to these protocols to accommodate the expanding requirements of several IoT scenarios. For superior outcomes, the IoT designers should think about adhering to significant benchmarks prior to implementing the communication protocol of their prototype.

PROTOCOL SELECTION CRITERIA:

The important characteristics that a designer may consider are low-latency, high through-put, and scalability. Thus the MQTT and CoAP emerge as versatile choicesmaking them suitable for a wide range of IoT and IIoT applications.

TRADE-OFFS AND CONSIDERATIONS:

The existing infrastructure, deployment scale, and device capabilities influences the choice of protocol. For instance, DDS may be more suitable for small-scale deployments with stringent real-time communication requirements while MQTT and CoAP for large-scale deployments.

FUTURE RESEARCH DIRECTIONS:

The study provides a comparative analysis of various communication protocols for IoT and IIoT devices, highlighting their benefits and drawbacks, and suggests that ongoing advancements in these protocols may impact the development of IoT and IIoTenvironment.

REFERENCES:

1. Shahroom AA, Hussin N. Industrial revolution 4.0 and education. *Int J Acad Res Bus Soc Sci*. 2018;8(9):314-319.

2. Lampropoulos G, Siakas K, Anastasiadis T. Internet of things in the context of industry 4.0: An overview. *Int J Entrep Knowl*. Published online 2019:4-19.

3. Madakam S, Uchiya T. Industrial Internet of Things (IIoT): Principles, Processes and Protocols. In: Mahmood Z, ed. *The Internet of Things in the Industrial Sector*. Computer Communications and Networks. Springer International Publishing; 2019:35-53. doi:10.1007/978-3-030-24892-5_2

4. Kuyoro S, Osisanwo F, Akinsowon O. Internet of things (IoT): an overview. In: *Proc. of the 3th International Conference on Advances in Engineering Sciences and Applied Mathematics (ICAESAM)*. ; 2015:23-24. Accessed February 20, 2021. https://www.academia.edu/download/42697929/IoT_overview.pdf

5. Attia TM. Challenges and opportunities in the future applications of IoT technology. Published online 2019. Accessed February 20, 2021. https://www.econstor.eu/handle/10419/201752

6. Tzounis A, Katsoulas N, Bartzanas T, Kittas C. Internet of Things in agriculture, recent advances and future challenges. *Biosyst Eng*. 2017;164:31-48.

7. Survey, comparison and research challenges of IoT application protocols for smart farming - ScienceDirect. Accessed February 20, 2021. https://www.sciencedirect.com/science/article/abs/pii/S1389128619306942

8. Vangala A, Das AK, Chamola V, Korotaev V, Rodrigues JJPC. Security in IoT-enabled smart agriculture: architecture, security solutions and challenges. *Clust Comput*. 2023;26(2):879-902. doi:10.1007/s10586-022-03566-7

9. Shah S, Ververi A. Evaluation of internet of things (IoT) and its impacts on global supply chains. In: *2018 IEEE International Conference on Technology Management, Operations and Decisions (ICTMOD)*. IEEE; 2018:160-165. Accessed February 20, 2021. https://ieeexplore.ieee.org/abstract/document/8691124/

10. Shah S, Bolton M, Menon S. A study of internet of things (IoT) and its impacts on global supply chains. In: *2020 International Conference on Computation, Automation and Knowledge Management (ICCAKM)*. IEEE; 2020:245-250. Accessed February 22, 2021. https://ieeexplore.ieee.org/abstract/document/9051474/

11. Nyamtiga BW, Sicato JCS, Rathore S, Sung Y, Park JH. Blockchain-based secure storage management with edge computing for IoT. *Electronics*. 2019;8(8):828.

12. Salman T, Jain R. A Survey of Protocols and Standards for Internet of Things. Published online February 10, 2019. Accessed February 23, 2021. http://arxiv.org/abs/1903.11549

13. Al-Masri E, Kalyanam KR, Batts J, et al. Investigating messaging protocols for the Internet of Things (IoT). *IEEE Access*. 2020;8:94880-94911.

14. Wukkadada B, Wankhede K, Nambiar R, Nair A. Comparison with HTTP and MQTT in Internet of Things (IoT). In: *2018 International Conference on Inventive Research in Computing Applications (ICIRCA)*. IEEE; 2018:249-253. Accessed February 23, 2021. https://ieeexplore.ieee.org/abstract/document/8597401/

15. Naik N. Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP. In: *2017 IEEE International Systems Engineering Symposium (ISSE)*. IEEE; 2017:1-7. Accessed February 23, 2021. https://ieeexplore.ieee.org/abstract/document/8088251/

.