IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

IMPLEMENTAION OF BI-DIRECTIONAL IoT GATEWAYS FOR INTEROPERABILITY OF HETEROGENOUS DEVICES USING MQTT PROTOCOL

A S Kirubha PG – M Tech Student, Kumaraguru College of Technology, Coimbatore.

M V Umesh Associate Professor, Department of Electronics and Instrumentation Engineering, Kumaraguru College of Technology, Coimbatore.

ABSTRACT

The manufacturing industry has been revolutionized by Industry 4.0, vastly improving the manufacturing process, increasing production quality and capacity. Machine-to-Machine (M2M) communication protocols were developed to strengthen and bind this ecosystem by allowing machines to communicate with each other. This greatly helps in remote/real-time monitoring, data collection which in turn reduces defective products and improves customer satisfaction.

This paper emphasizes on the design and development of a new Bi-Directional IoT Gateways, which makes the communication among the heterogeneous appliances incorporated with various wireless protocols and wired protocol such as (Wi-Fi, ZigBee, MQTT, Bluetooth, GSM and Ethernet). It makes the interlinking and interoperability among various wired and wireless protocols, by restoring the obtained sensor data got from discrete wireless nodes, for regulating and monitoring a machine by the instructions specified by remote users. This Bi-Directional gateway gives crucial advantages over the existing: (i) makes the connectivity among ZigBee, Wi-Fi, Bluetooth, GSM and Ethernet (ii) data is transformed into needed protocol formats. It converts heterogenous protocols data into homogeneous protocol data and homogenous protocol data into heterogenous protocols data. (iii) utilizes a light weighted protocol for sending the information to cloud and getting information from the remote place through computer or through a smart phone.(iv) Gives local storage space in the gateway and send into cloud for evaluating and future use of the received and sent data (v) The sensors information can be seen and monitored over a smart phone, tablet or a personal computer.

KEYWORDS: Machine-to-Machine communication, Data collection, Communication protocol, MQTT, IOT, GSM.

INTRODUCTION

Machine to Machine communications, often termed M2M/IoT is going to be the next generation of Internet revolution connecting more and more devices on Internet. M2M communications refer to automated applications which involve machines or devices communicating through a network without human intervention. Sensors and communication modules are embedded within M2M devices, enabling data to be transmitted from one device to another device through wired and wireless communications networks. The Internet of Things (IoT) is a hype topic for nearly a decade now. Broadly growing, millions of devices get direct access to the Internet provides plenty of applications such as smart homes or mobile health management. This trend can also be found in the industry where IoT components hardened for these environments are introduced, called Industrial IoT (IIoT) devices which can be either sensors or actuators, as well as mobile equipment such as smartphones, tablets, and smart glasses. Consequently, mobile communication becomes universal in smart factories. IIoT devices provide massive data on temperature, pressure, machine states, etc. But still, most of the SME level industries in the Asian region are new to these technological advancements. They still operate their facilities with conventional setups without absorbing the new opportunities which are presented by IoT.

EXISTING SYSTEM

LPWANs

Low Power Wide Area Networks (LPWANs) are the new phenomenon in IoT. Nevertheless, LPWANs can only send small blocks of data at a low rate, and therefore are better suited for use cases that don't require high bandwidth and are not time-sensitive.

Drawbacks:

- LPWAN supports low data rate, hence LPWAN cannot be used for high data rate applications.
- It offers high latency between end to end nodes. Hence LPWAN is not ideal for low latency applications.

Cellular (3G/4G/5G)

Well-established in the consumer mobile market, cellular networks offer reliable broadband communication supporting various voice calls and video streaming applications. They fit well in specific use cases such as connected cars or fleet management in transportation and logistics. For example, in-car infotainment, traffic routing, advanced driver assistance systems (ADAS) alongside fleet telematics and tracking services can all rely on the ubiquitous and high bandwidth cellular connectivity. Cellular next-gen 5G with high-speed mobility support and ultra-low latency is positioned to be the future of autonomous vehicles and augmented reality. 5G is also expected to enable real-time video surveillance for public safety, real-time mobile delivery of medical data sets for connected health, and several time-sensitive industrial automation applications in the future.

Drawbacks:

- They impose very high operational costs and power requirements.
- Cellular networks are not viable for the majority of IoT applications powered by battery-operated sensor networks

PROPOSED SYSTEM

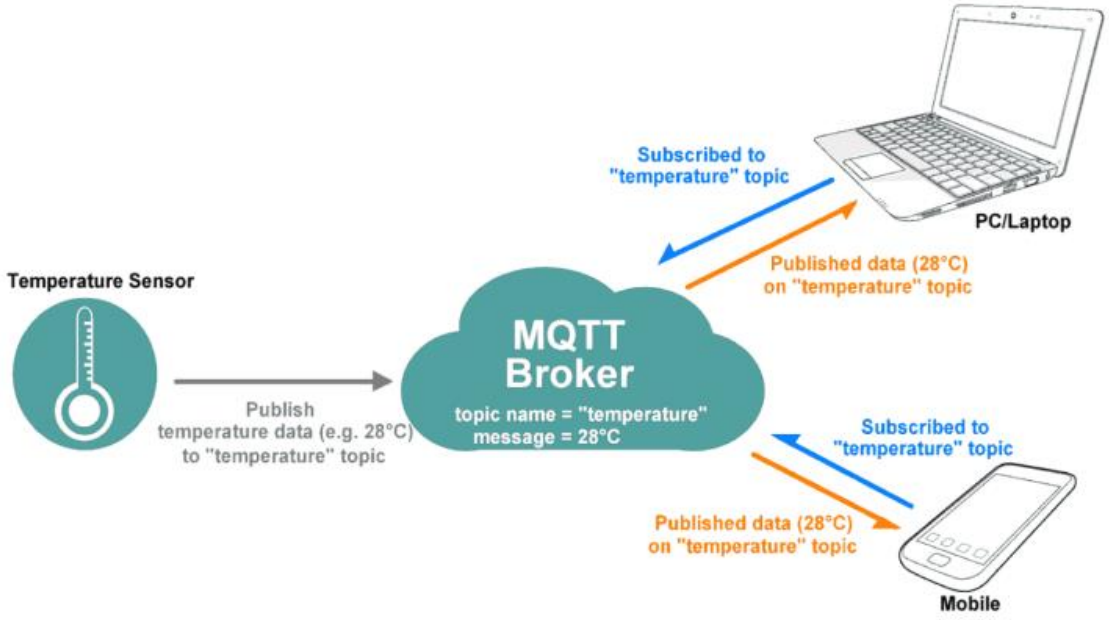
MQTT is an OASIS standard messaging protocol for the Internet of Things (IoT). It is designed as an extremely lightweight publish/subscribe messaging transport that is ideal for connecting remote devices with a small code footprint and minimal network bandwidth. MQTT today is used in a wide variety of industries, such as automotive, manufacturing, telecommunications, oil and gas, etc. MQTT is lightweight publish-subscribe based messaging protocol.

- It is quicker (faster) than other request-response based APIs like HTTP.
- It is developed on the base of TCP/IP protocol.
- It allows remote location devices to connect, subscribe, publish etc. to a specific topic on the server with the help of message broker.
- MQTT Broker/Message broker is a module in between the sender and the receiver. It is an element for message validation, transformation and routing.
- The broker is responsible for distributing messages to the interested clients (subscribed clients) of their interested topic.

WORKING

The MQTT protocol enables resource constraint IoT devices to publish or send information about some topics to a server that functions as an MQTT message broker. The function of the broker is to push that piece of information to only those clients that are previously subscribed to that topic. In simple words, we can explain this basic idea as the publisher is responsible for generating and transmission of information to subscribers through a broker. The main function of a broker is to ensure security by checking the authorization of subscribers and publishers. To explain the working of MQTT protocol we will divide the MQTT session into 4 stages such as connection, authentication, communication, and termination.

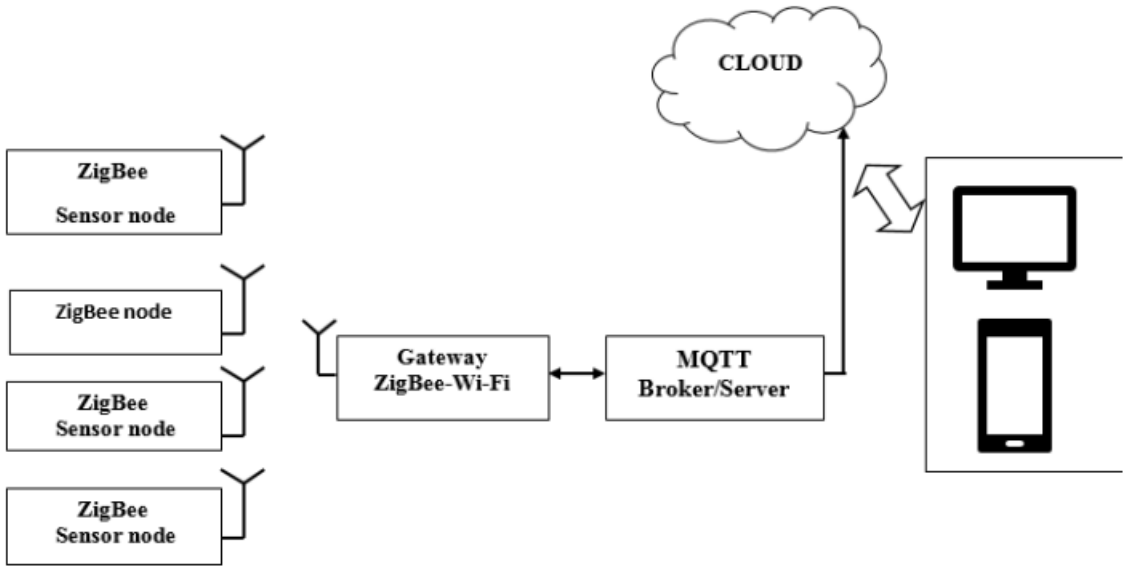
- First of all, a TCP / IP connection is initiated from client to broker by using a standard or custom port which is defined by a broker's operation.
- While establishing a connection, it's important to recognize that whether the server has continued an old session or a new session.
- The old session continued if reused client identity is provided to the broker. With development of smart devices, to collect data, gateways play a significant role in interlinking with different sensor nodes. The gateway can transform data into distinctive formats for further reference utilizing various wireless protocols and standards with sensor nodes. These distinctive formats send transformed data into clouds that accept the instructions from peripheral users in the remote location from a personal computer or a smartphone.



The advantages of gateway proposed here are; (i) ZigBee and Wi-Fi connectivity enabled with wireless technologies, (ii) converts the data into needed protocol format, (iii) collecting and sending information from and to the sensor node to gateway through cloud MQTT protocol (iv) space for stocking of analysed data and (v) the observation of sensor values, and the devices or machines can be regulated by a smart phone from remote location. Here the proof of theory for regulating the smart home appliances is demonstrated. This chapter outlines a design and an execution of Bi-Directional IoT gateway by ZigBee and Wi-Fi technologies with MQTT protocol.

The proposed gateway architecture enables the interconnection of ZigBee and Wi-Fi technologies. Every sensor node consists of a sensor, micro controller integrated hardware, and a ZigBee module. The sensor and Zigbee modules are connected to the micro controller that reads the sensor values and transmits to the gateway using the ZigBee communication module. The gateway consists of a ZigBee module and Wi-Fi module that captures the information transmitted by the sensor node enabled with Zigbee and converts it into Wi-Fi protocol by unpacking the ZigBee packet. After converting the protocol format data and it is sent to the cloud through MQTT broker. The MQTT broker is configured with a SoC integrated with processor, RAM, ROM and enabled with different communication protocols that are capable of storing the sensor data. Once the data is arrived at the broker, it publishes that data to the cloud using the internet through that user who can observe or monitor the data of the devices that are connected. For controlling the appliances or the devices a smart phone is used by the end user to transfer the commands. The commands will be received by the broker and it sends to the gateway. The gateway processes by unpacking the Wi-Fi packet and identifies the destination sensor node address. After identifying the sensor node address, the commands are packed with ZigBee protocol format and transmitted to the destination. The destination sensor node acts as per the user's

instructions.



CONCLUSION

The designed gateways have enabled the communication between the devices or the things that use diverse communication protocol that avoided the problem of inter- operability A bi-directional Bluetooth- Zigbee gateway is proposed and implemented using the Raspberry Pi. The sensor node and actuators connected to 8051 microcontrollers integrated with Zigbee. The gateway enabled the interconnection and data transfer among Bluetooth and ZigBee machines by re-establishing the data received from nodes and the commands from external or remote users. BLUE-FI gateway developed to permit inter-association among Bluetooth and Wi- Fi protocols. This gateway renders important advantages. It facilitates to send information among Bluetooth and Wi-Fi devices by restoring the protocols causing it easy and extra consistent, which gets data from different sensors and transfers them into a needed format. This was executed by getting an application of Blue-Fi gateway through Smart health monitoring system (SHMS). Here in SHMS various units are used to assist in determination of the health of a patient that can be updated in real time. A gateway is made with ZigBee and Wi-Fi wireless technologies. The gateway changes the data into the protocol format in bi-directional manner and operates in a light weighted MQTT protocol in sending and receiving data. It gives the storage space and analysed data and the sensor values can be seen, and as well the machines or devices or appliances are monitored by a smart phone from remote place. A GSM integrated gateway is designed that receives the information from the entire sensor nodes using the wired and wireless protocols like ZigBee, Bluetooth, Wi-Fi and ethernet that published the data to the subscriber through cloud. Actions are performed at the sensor nodes based on the commands given by the remote user through GSM module. The gateway users publish and subscribe paradigm that are available in low resourced protocol MQTT. The performance of the gateways is evaluated based on the observations of processor utilization and memory consumption which are acceptable.

FUTURE SCOPE

As the future work it is proposed to optimize and increase the latency of the gateway for faster processing. All the high-speed devices can also be used to communicate through the gateway. All the wired and wireless protocols must be integrated with on single boardslike SoC (System on Chip). Auto configurable Smart gateways have to be designed where new devices 36 can connect to the gateway automatically by the options given by the user through graphical interface.

REFERENCES

G. V. Vivek and M. P. Sunil, "Enabling IOT services using WIFI - ZigBee gateway for a home automation system," pp. 77-80, 2015.

Y.-H. Lee and S. Nair, "A Smart Gateway Framework for IOT Services," pp. 107- 114, 2016.

C. Pereira, J. Rodrigues, A. Pinto, P. Rocha, F. Santiago, J. Sousa, et al., "Smartphones as M2M gateways in smart cities IoT applications," pp. 1-7, 2016.

D. C. Yacchirema, M. Esteve, and C. E. Palau, "Design and implementation of a Gateway for Pervasive Smart Environments," pp. 004454-004459, 2016.

Chia-Shin Yeh, Shang-Liang Chen, I-Ching Li , “Implementation of MQTT protocol based network architecture for smart factory”, Journal of Engineering Manufacture, May 2021.