Experimental Investigation of Integrated Id Method to Mitigate Message Loss in Iot Control Devices

Ankit Khare

University of Petroleum and Energy Studies (UPES), India

Abstract

Number of devices connected to the internet are rapidly growing and control devices are connected to the sensor to monitor certain conditions. An increase in the number of devices in the server causes high message loss for various messaging techniques. This requires effective method to minimize the message loss in the various devices. The aim of this research is to develop the model of integrate Identity (ID) technique to minimize message loss and test it in Internet of Things (IoT) environment. Integrated ID developed on the push message service of Message Queuing Telemetry Transport Protocol (MQTT). Integrated ID is the method of combining the hexadecimal number in the actual message and the ID is used to retrieve the data in the edge devices if the message is lost. The message consists the temperature data of the subject and order of ID is added in the message in hexadecimal value. The message ID in hexadecimal value is added in the prefix of the data, the device ID is represented in 2 bit, which is added after the temperature data. The control device checks the order of the message and found the missing data, then requested for the lost data. This condition requires very less memory to store the message order and supports a number of devices in the network. Experimental results show that proposed method transfer the first message within 0.86 s and have satisfactory latency.

Intern of things (IoT) integrates the physical world with a computer system that helps to operate the device smoothly even from the remote area. The sensors are placed across the environment for monitoring purpose and the suitable action is taken after analysing the data. Presently, a number of devices equipped with sensors and processing devices, that helps in monitoring and controlling the various devices. IoT is more useful in Healthcare application and involves in monitoring the patients remotely with considerable scalability, flexibility, and interoperability. This device uses a cloud system to store and manage data that involves in the enhancement of resource utility of the devices. In order to improve the function of the IoT, existing research and industries provide many frameworks, tools, and software. Some of the techniques have compatibility issues between the devices and complex implementation of comprehensive consumer applications. A new communication method is needed to easily control different kind of smart devices by the same user. The message passing between several devices requires one or more communication protocols between them. IoT devices having limited resources, so the protocols are designed to operate in low bandwidth, communication instability and high latency networks. With the help of this protocol, the smart devices can smoothly communicate with other smart devices. The different communication protocols are MQTT, Constrained Application Protocol (CoAP), HyperText Transfer Protocol (HTTP), Representational State Transfer (REST) used to interface sublayer that allows the devices to engage and interact. The communication endpoints are often special devices like sensor and actuators, which exchange the data to coordinate their operations. The communication between these smart devices defines the process of IoT, two most popular communication protocols are Message Queuing Telemetry Transport Protocol (MQTT) and Hypertext Transfer Protocol (HTTP). MQTT protocol is one of the common technique used to transmit the message between the servers and to control the devices.

Note: This work is partly presented at 34th International Conference on Nanotechnology & Expo at November 15-16, 2019 | Madrid, Spain