A Comprehensive Survey on- Data Exchange Protocols in IoT

Mrs.Shifana Begum[1], Mukesh K[2], Suzanne Britto[3], Supriya K[4], Santosh Kumar [5]

[1]Assistant Professor, [2]UG Student, [3]UG Student, [4]UG Student, [5]UG Student
Department of CSE,
SUIET, Mukka Mangalore, India.

***Abstract*: Lot of information is found on google related to the word IoT, what does it actually mean, does it really exist or it is virtual. Our future depends on IoT, it is the base of all artificial intelligence proficiencies. IoT aims to control everything around us, command and control the system. IoT is basically that two or more than two devices can talk (communicate) to each other.**

This is what IoT is all about where two or more objects connected to the internet can share information so that things become easier to human. The rapid growth in technology and internet connected devices has enabled Internet of Things (IoT) to be one of the important fields in computing. Standards, technologies and platforms targeting IoT ecosystem are being developed at a very fast pace. This paper surveys several standards by IEEE, IETF and ITU that enable technologies enabling the rapid growth of IoT. These standards include communications, routing, network and session layer protocols that are being developed to meet IoT requirements.

***Keywords*: Internet of Things (IoT), standards, Data link, IoT protocols, IoT network layer protocols, IoT transport layer protocols, MQTT (Message Queuing Telemetry Transport), CoAP (Constrained Application Protocol).**

I. INTRODUCTION

Internet of Things describes itself as the wireless network of interconnected objects that can be anything like doors, fans, cooler, washing machine etc. Which can communicate with each other with our intervention. This basically requires few artificial intelligences or when our environment will be embedded with sensor and technologies such as RFID (Radio Frequency Identification), WSN (Wireless Sensor Network), software, actuators etc.

Internet is a medium or a way to connect the people that are far apart, in the same way internet of things is interconnection via internet of computing device embedded in day to day objects, enabling all of them to connect together for sending and receiving the data. This includes the object like cell phone, washing machine, air conditioner and doors etc.

The term IOT was first proposed by Kevin Ashton in a presentation to proctor and gamble in the year 1999. At first, he proposed the phrase that internet for things which was later turned to the Internet of Things. It was earlier discussed in 1982 as a concept of network of smart devices as a modification of coke machine where newly loaded cokes were cold.

IoT plays a significant role in different types of applications including healthcare, transportation, automation, agriculture, vehicles and emergency response to disasters. In addition, it is expected to play additional roles to improve the quality of life, business applications, and smart homes. An example of currently available IoT ecosystem is smart homes, which are composed of sensors for controlling temperature, heat, and air conditioning in our homes remotely. Future extensions of such system can be preparing our coffee, controlling TV, tracking our health statistics and driving our vehicles. These applications would impose further challenges and need for standards to handle the diversity of application requirements.

IoT protocols are a crucial part of the IoT technology stack — without them, hardware would be rendered useless as the IoT protocols enable it to exchange data in a structured and meaningful way. Out of these transferred pieces of data, useful information can be extracted for the end user and thanks to it, the whole deployment becomes economically profitable, especially in terms of IoT device management.

The paper is divided into 4 Sections. Section 2 describes the framework and architecture of IOT. Section 3 represent data access protocols in detail, which is employed in IOT. Section 4 concludes about the paper.

II. IOT FRAMEWORK AND ARCHITECTURE

Iot Framework-The equation below will depict the action and communication of data in successive level in IOT. It manages IOT services using the data from the internetwork of the device and object, internet cloud services and helps to represent the data from the IOT device for managing the IoT cloud server.

Equation: Gather + Consolidate + Connect + Collect + Assemble + Manage and Analyze = Internet of Things with connectivity to cloud services.

This equation represents a complex conceptual framework for IOT using cloud-platform-based processes and services. The specific steps are as follows:

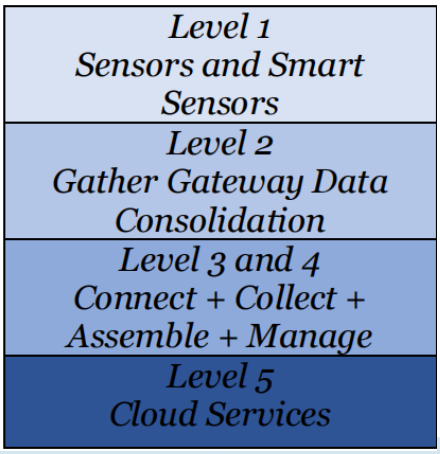


Figure 1: IoT Framework

• Level 1 and 2 consist of a sensor network to gather and consolidate the data. First level gathers the data of the things (devices) using sensors circuits. The sensor connects to a gateway. Data is then consolidates at the second stage, for example, transformation at the gateway at level 2.
• The gateway at level 2 communicates the data streams between levels 2 and 3. The scheme uses a communication management subsystem at level 3.
• An information service consists of connecting, collect, assemble and manage subsystems at level 3 and 4. The services render from level 4.
• Real time series analysis, data analytics and intelligent subsystem are also at level 4 and 5. A cloud infrastructure, a data store or database acquires the data at level 5.

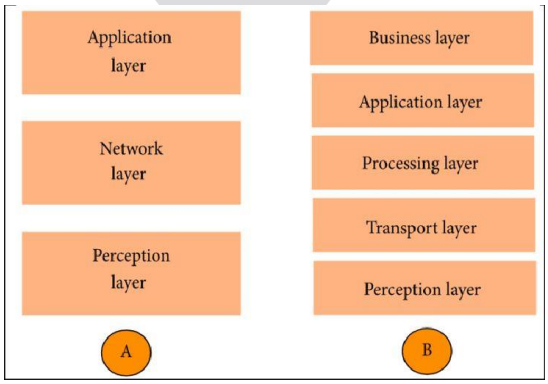
Iot Architecture (A: three layers, B: five layers) -
There are three and five layer achitecture.As shown in **Fig 2**.A and B.
The most basic architecture is a three-layer architecture. It was inaugurated in the early stages of researchers in this area. It takes in three layers, namely, the perception, network and application layers.

- *Perception layer*: it is a physical layer, which has a sensor for sensing and gathering information about the environment. It senses some physical parameters or identifies other smart objects in the surroundings.
- *Network layer*: it is responsible for connecting to other smart things, network devices, and servers. Its features are likewise used for transmitting and processing sensor data.
- *Application layer*: It is responsible for delivering application specific services to the user. It defines various applications in which the internet of things can be deployed.

Ace is the five-layer architecture, which additionally includes the processing and business layer. The role of perceptual experience and the application layer is same as the architecture with the three layers. The schema for the other layer is:

- *Processing layer*: it is also known as the middleware layer. It stores, analyses, and process huge amount of data that comes from the transport layer. It can manage and provide a diverse set of service to the lower stratum.
- *Transport layer:* it transfers the sensor data from the perception layer to the processing layer and processing layer to perception layer through the networks such as wireless, 3G, LAN, RFID, Bluetooth and NFC.
- *Business layer*: it manages the whole IOT system, including applications, business and profit models, and users' privacy stages of researchers in this area. It takes in three layers, namely, the perception, network and application layers.

Figure 2: A) Three-layer Architecture and B) Five-layer Architecture



III. DATA PROTOCOLS USED IN IOT

It is intended for efficiently supporting the big data transfer of host monitoring and control applications, including loading/dumping and remote debugging. It provides packet-based application like remote loading and debugging with an efficient, trusted data transport service. The primary objective of RDP is to remain effective in environments where there could be a non-sequential message-segment delivery or prolonged transmission delays and loss.

Key goals of data protocols are:
• To represent a full-duplex communications channel between the two hops of every transport connection.
• To precisely transport every user message and to report a message delivery, abortion to the user in case the message transfer abort.
• To discover and abolish any defective or duplicate segments. In order to fulfil this task, RDP employs a checksum and sequence number in every segment header.
• To optionally offer sequenced segment delivery. Sequenced segment delivery should be described at the time a connection is gained.
• To acknowledge the segments acquired from a sequence, as they get in. This consequences in the freeing up of resources on the sending side.

There are various different data protocols to opt for when it comes to connecting various devices to the internet of things. Few are new while few are older and legacy protocols. Depending on various implementations and sensors, use of protocols differs. Each one experiences, their own strength and weakness. It is important to stick to open standards for maximum interoperability between devices and applications.

***A. MQTT (Message Queuing Telemetry Transport*):** It is An ISO standard (ISO/IEC PRE 20922) Publisher-subscriber (It is a messaging pattern where senders of messages, called the publisher, do not program the message to be posted directly to specific receivers called subscriber, but instead categorize published messages into classes without knowledge of which subscribers, if any, there may be) based messaging protocol. Andy Stanford Clark of IBM and Arlen Nipper of Cirrus Link Authored the first edition of the protocol in 1999. In 2013, IBM presented MQTT V3.1 to the OASIS specification body with a charter the ensured only minor alterations to the specification could be accepted.

It operates on top of the TCP/IP protocol. It is designed for connections with remote locations where a "small code footprint" is required or the network bandwidth is restricted. It is a protocol that was specifically created for SCADA system (what is SCADA System it is Supervisory Control and Data Acquisition is a control system architecture that uses computers, networked data communication and graphical user interfaces for high level process supervisory management). It uses a publish/subscribe mechanism to minimize the load and overhead with application-specific, custom JSON or binary formats. MQTT is widely undertaken in IT departments worldwide, with many open-source examples available in just about any programming language

***B. CoAP (Constrained Application Protocol*):** It is an application layer protocol that is intended for use in resources-constrained internet devices such as WSN nodes. CoAP is designed to easily translate to HTTP for simplified integration with web, while also meeting specialized integrations such as multicast support, very low overhead and simplicity. The Internet Engineering Task Force (IETF) Constrained RESTful environment Working Group (CoRE) has served the major standardization work for this protocol. In lodge to make the protocol suitable to IoT and M2M application, various new functionalities have been added.

CoAP uses a client/server model where clients send requests to servers and servers respond to Clients. Clients may use GET, PUT, POST and DELETE resources. Messages in CoAP can be “confirmable” or “non-confirmable”.

In CoAP is available content negotiation. To show a preferred representation of a resource clients use Accept option, and servers respond with a Content-Type. This allows the client and the server evolve independently from each other. CoAP Protocol provides its users with the ability to observe a resource. It means that after removing the initial document, a server may keep on replying. You just require to set the observe flag on a CoAP GET request. It allows clients to receive state changes if they happen. Because CoAP is built on top of UDP not TCP, SSL/TLS are not available to provide security. DTLS, Datagram Transport Layer Security provides the same assurances as TLS, but for transfers of data over UDP.

C. AMQP (Advance Message Queuing Protocol): It is an open standard application layer protocol for message-oriented middleware. The determining feature of AMQP is message oriented, queuing, routing (including point to-point and publish-subscribe), reliability and security. AMQP mandates the behaviour of the messaging provider and the client to the extent that implementations from different vendors are interoperable, in the same way as SMTP, HTTP, FTP etc. Have created interoperable systems.

AMQP is a wire-level protocol (a wire level protocol is a description of the format of the data that is shipped across the network as a stream of bytes). AMQP is a binary application layer protocol that was generated to substantiate a huge number of messaging applications and communication designs. It comes-up with flow-controlled, message-oriented communication with built-in options for message delivery guarantees, in addition, authentication and/or encryption based on widely accepted Internet authentication and data security protocols a like Simple Authentication and Security Layer (SASL) and/or Transport Layer Security (TLS).

AMQP is the prime transport layer protocol used by the Azure IoT Hub. AMQP defines a self-describing encoding scheme allowing interoperable representation of a wide scope of commonly used types. It also permits typed data to be annotated with additional meaning.

D. WebSocket: It is a computer communication protocol, unlike http provide full-duplex (bi-directional) communication channel over a single TCP connection. The WebSocket protocol was standardized by the IETF
as RFC 6455 in 2011, and the WebSocket API in Web IDL is being standardized by the W3C. It enables streaming of message on top of TCP. WebSocket was invented by Ian Hickson and Michael Carter. WebSocket was first referenced as TCP Connection in the HTML5 cataloguing, as a procurator for a TCP-based socket
APIs. In June 2008, a series of conversation were led by Michael Carter that resulted in the first version of the protocol known as WebSocket.

WebSocket is currently one of the main players in the Realtime (low-latency) world. WebSockets guarantee, persistent connections with simultaneous bi-directional communication. They come with all the benefits of HTTP since WebSockets initially start off as an HTTP handshake, before getting kicked upstairs to continue the rest of the communication in WebSockets. The very quintessence of WebSockets is a push-based strategy. It supports publisher/subscriber paradigm because it keeps the connection open until deliberately closed by one of the two parties under communication (i.e., Client or a Server).

E. Bluetooth and BLE*:* Bluetooth is a short-range wireless technology that uses short-wavelength, ultrahigh-frequency radio waves. It had most commonly been used for audio streaming, but it has also become a significant enabler of wireless and connected devices. As a result, this low-power, low-range connectivity option is a go-to for both personal area networks and IoT deployments.
Another option is Bluetooth Low Energy, known as either Bluetooth LE or BLE, which is a new version optimized for IoT connections. True to its name, BLE consumes less power than standard Bluetooth, which makes it particularly appealing in many use cases, such as health and fitness trackers and smart home devices on the consumer side and for in-store navigation on the commercial side.

F. LoRa and LoRaWAN: LoRa, for long range, is a noncellular wireless technology that, as its name describes, offers long-range communication capabilities. It's low power with secure data transmission for M2M applications and IoT deployments. A proprietary technology, it's now part of Semtech's radio frequency platform. The LoRa Alliance, of which Semtech was a founding member, is now the governing body of LoRa technology. The LoRa Alliance also designed and now maintains LoRaWAN, an open cloud-based protocol that enables IoT devices to communicate LoRa.

G. Wi-Fi: Given its pervasiveness in home, commercial and industrial buildings, Wi-Fi is a frequently used IoT protocol. It offers fast data transfer and is capable of processing large amounts of data. Wi-Fi is particularly well suited within LAN environments, with short- to medium-range distances. Moreover, Wi-Fi's multiple standards -- the most common in homes and some businesses being 802.11n -- give technologists options for deployment. However, many Wi-Fi standards, including the one commonly used in homes, is too power-consuming for some IoT use cases, particularly low-power/battery-powered devices. That limits Wi-Fi as an option for some deployments. Additionally, Wi-Fi's low range and low scalability also limit its feasibility for use in many IoT deployments.

H. Zigbee: Zigbee is a mesh network protocol that was designed for building and home automation applications, and it's one of the most popular mesh protocols in IoT environments. A short-range and low-power protocol, Zigbee can be used to extend communication over multiple devices. It has a longer range than BLE, but it has a lower data rate than BLE. Overseen by the Zigbee Alliance, it offers a flexible, self-organizing mesh, ultralow power and a library of applications.

I. XMPP: Dating back to the early 2000s when the Jabber open source community first designed its Extensible Messaging and Presence Protocol for real-time human-to-human communication, XMPP is now used for M2M communication in lightweight middleware and for routing XML data. XMPP supports the real-time exchange of structured but extensible data between multiple entities on a network, and it's most often used for consumer-oriented IoT deployments, such as smart appliances. It's an open-source protocol supported by the XMPP Standards Foundation.

COMPARISON

Table 1

Features	MQTT	CoAP	AMPQ	XMPP
Transport	TCP/UDP	UDP/IP	TCP/IP	TCP/IP
Communication Model	Publish/ Subscribe	Request/ Response	Request/Response Publish/Subscribe	Publish/ Subscribe
Header Size	2 bytes	4 bytes	8 bytes	-
Power Consumption	Less	Medium	Medium	High
Delivery Level	High	Medium	High	-
QoS Level	High	Moderate	High	Moderate

Table 2

	Bluetooth/BLE	LoRa and LoRaWAN	Wi-Fi	Zigbee
Frequency	2.4 Ghz	subGhz	2.4Ghz, 5Ghz	2.4Ghz
Data Rate	1, 2, 3 Mbps	< 50 kbps	0.1-54 Mbps	250 kbps
Range	~300 ft	1-3 miles	< 300 ft	~300 ft
Power Usage	Low	Low	Medium	Low
Cost	Low	Medium	Low	Medium

IV. CONCLUSION

In this survey paper we have presented a framework, architecture, protocols in IOT mainly focusing on Data Protocols. The technologies in the core infrastructure layer are showing signs of maturity. However, there are a lot more things to be searched in the area of IOT applications and communication technologies. With the constant expansion of the emerging IOT the concept of Internet of Things will soon be unstoppable developing on a very large scale. These fields will surely make an impact on human life and their future aspects. A lot of those protocols have been developed and standardized by IETF, IEEE, ITU, and other organizations while many more are still in development. The discussion was brief due to the large number. Therefore, references for further information have been provided.

REFERENCES

[1] "Internet of Things" Wikipedia official blog it can be accessed at: https://en.wikipedia.org/wiki/Internet_of_things

[2] "Trends and characteristic of Internet of Things" Wikipedia official blog it can be accessed at: https://en.wikipedia.org/wiki/Internet_of_things

[3] A Survey of Protocols and Standards for Internet of Things Tara Salman, Raj Jain Department of Computer Science and Engineering Washington University in St. Louis

[4] Jen Clark in November 17, 2016 "What is Internet of Things" this blog can be accessed at: https://www.ibm.com/blogs/internet-of-things/what-is-the-iot/.

[5] I. Mashal, O. Alsaryrah, T.-Y. Chung, C.-Z. Yang, W.-H. Kuo, and D.P. Agrawal, "Choices for interaction with things on Internet and underlying issues," Ad Hoc Networks, vol. 28, pp. 68– 90,2015.

[6] O. Said and M. Masud, "Towards Internet of Things: survey and future vision," International Journal of Computer Networks, vol. 5, no.1, pp.1–17, 2013.