A Review Paper of Internet of Thing: Communication Protocol

[1]Ghanshyam Dhomse

[1]Assitant Professor,
[1]Computer Engg Department,
[1]SNJB's Late Sau K.B. Jain College of Engineering, Chandwad India

Abstract : IoT is very famous and interesting field now days for many researcher, every day device become most intelligent and smarter to make communication informative. But IoT field has required solving variety of question while doing research at different aspects of communication between the large numbers of heterogeneous smart devices to serve meaning purpose. Due to lack of overall communication protocol knowledge. In this review paper mainly focused on comparative study of various communication protocol and challenges involved in IoT.

***Index Terms* – IoT, NFC,WSN, Zigbee, RFID**

I. INTRODUCTION

The term IoT means "Internet of Thing" there is no unique definition available for IoT that is acceptable by the world community of users. In fact, there are many different groups of researchers, developer and innovator people that have defined the term "anytime, anywhere and any media, resulting into sustained ration between radio and man around 1:1" by Srivastva [1]. In IoT all devices and appliances connected to network and internet so storage and processing data is most important edge of network, while communication happened between the devices. The data can gather from various types of sensor and actuator or other kind of device that send it remote server via cloud platform or other available technology.

IoT devices has limitation in size, power , energy and computational capability as a result main challenge ensure the right communication protocol usage while data gather from devices to get more accurate. Most of communication between IoT devices mainly wireless collecting the data from different location of countries so reliability and distortion of data again new challenges. Due to heterogeneous types of device is difficult to identify the right communication protocol match with architectural layer.
IoT work at different architecture layer like perception, network and application layer.

There are several networking protocol are used at various layer. Like Radio frequency Identification (RFID), local area network (LAN), Near Field Communication(NFC), Wireless Sensor Network(WSN), Bluetooth, Zigbee, and WiFi. To enhance interoperability of service between the middleware and Application many services level networking protocol is required. The middleware services comes with many open source service [2] and commercial services like OpenIOT [3], MiddleWhere [4], Hydra[5], FiWare[6].

In IoT devices most of communication technologies comes with low power and very short range like RFID and NFC so again new challenges come while gather the data between different geographical location. also for Zigbee, Wifi and Bluetooth comes under medium range. So new networking mechanism protocol come in picture while providing the middleware services to application.

Apart from this some leading protocol like LoraWAN, SigFox , 6LoWAN and IEEE 802.15.4 are introduced to for low power consumption and wireless purpose[7]

In 2025 the number of devices connected in IOT there will be more than 50 billion so how these devices communicate each other with wireless freedom option, what kind of network, power and communication option is available for these billion of devices is major aspects for many researcher. Some protocol like MQTT (***Message Queue Telemetry Transport***) [8] are used to monitor the sensor data remotely. This protocol mainly used nowadays to save Power and storage memory. It is also designed for low cost device. It is work on Publish-Subscribe kind of pattern make the communication between various devices. It works in 3G and Wifi Network. In compare with HTTPS protocol the sendind and receive the message take less time with low battery consumption.

CoAP (***Constrained Application Protocol***)[12] this is another internet application protocol used to connect the devices over internet. This mainly work on Application layer the purpose of this protocol is group communication and send the notification to each device. So this also infrastructure dependent type of protocol connected to wired and wireless. This protocol alternative to HTTPS used in most of IoT application. It uses XML/HTML data format.

6LoWPAN is also very popular standard for Wireless communication it work on Adaption Layer to compress the header of packet, make the fragmentation with maximum transmission unit , support the mesh routing at data link layer.

Bluetooth Low Energy is used for small File or Chunk of data transfer. It is mainly used in wearable devices for connecting the IoT devices with smart watches. Most of smart phones are Bluetooth enable.it is used for small operation Quickly transfer the small packet of date. But when we transfer the stream of data the BLE does not support. Energy efficient wise better option.

Zigbee[13] is used to transfer the large size of data with cheaper in communication. It also support the different topologies mainly star, mesh and tree.Zigbee uses the routing Schema depends on routing protocol. It has two different types FFD (Fully Functional Device) and RFD (Reduced Functional Device). It make the communication secure and used over large distributed application.

II. Comparative Study

Standard	**Bluetooth 4.2**	**Zigbee**	**Z-Wave**	**NFC**	**WiFi**
IEEE Spec	IEEE 802.15.1	IEEE 802.15.4	ITU-T G.9959	ISO/IEC 18000-3	802.11n
Frequency	2.4 GHz ISM	2.4 GHz	900 GHz	13.56MHz (ISM)	2.4GHz and 5GHz bands
Range	50-150m	10-100m	30m	10cm	50m
Data Rate	1 mbps	250kbps	9.6/40/100kbit/s	100-420kbps	600 Mbps maximum, but 150-200Mbps is more typical, depending on channel frequency used and number of antennas (latest 802.11-ac standard should offer 500Mbps to 1Gbps)
Network Type	WPAN	WPAN	WPAN	P2P	WPAN/P2P
Power Consumption	~12.5mA	~40mA	~2.5mA	~50mA	~116mA
Applications usages	Smart watch, Smart Phones, PDA, BLE enable PC or Laptop Wireless Mouse Wireless Keyboard Printers etc.	Automation system, Wireless sensor networks, Industrial control Medical data collection Smoke alarms	Smart Locks, Automatic Heat Control, Automatic Light Control, Smoke Sensors Flood Sensors Smart Locks	Car Keys to Compatible Scanner ie for Identification, QR Code Downloading ,Scanning etc, Ticketing Purpose in Public Transport etc.	Remote Control Smart Phones Smart printers File Sharing Push Notification Wireless transfer of Photos, Movie other formats of data.

Table 1: Comparison between Various Protocol [8][9]

Standard	**6LowPAN**	**Sigfox**	**LoRaWAN**	**Neul**	**Thread**
IEEE Spec	RFC6282	Sigfox	LoRaWAN	Neul	IEEE802.15.4 and 6LowPAN
Frequency	(adapted and used over a variety of other networking media including Bluetooth Smart (2.4GHz) or ZigBee or low-power RF (sub-1GHz)	900 MHz	865-867 MHz for India	900MHz (ISM), 458MHz (UK), 470-790MHz (White Space)	2.4GHz (ISM)
Range	less than 500 kHz	30-50km (rural environments), 3-10km (urban environments)	2-5km (urban environment), 15km (suburban environment)	10km	Not Available
Data Rate	64 Byte	10-1000bps	0.3-50 kbps	Few bps up to 100kbps	Not Available
Network Type	WPAN	WPAN	WAN	WPAN	WPAN
Power Consumption	Not Available	Depend on Chip.	2.5 mA	20 to 30mA	Not Available
Applications	Smart Homes Smart Meter Thermostats Smart Lighting, In Low power radio Communication for IP Networking.	Smart meter, Healthcare, Transportation Remote monitoring Retail industry, Security.	Air Quality, Pollution monitoring, Smart Light, Fire detection system, Waste Management System Infrastructure Management system.	Health care, Smart Cities, Oil and Gas management, Transport, Sensor Network.	Authentication and Encryption of near about 250 nodes in mesh network operated by thread radio transceiver.

Table 2: Comparison between Various Protocols [8][9]

Table 3: Comparison between Various Message Protocols [10][11]

MQTT	CoAP	HTTP	AMQP
Message Queue Telemetry Transport	Constrained Application Protocol	it is Transport , Authentication and security protocol.	It is message format protocol for Communication
It is Open Standard protocol	It is also Open Standard protocol	It allows the Communication between Component	It allows the Communication between Component
it is work like client server model every sensors of client can connect to server.	It is also Client Server model.	Traceable	Traceable
Well Documented	Well Documented	Well Documented	Well Documented
Asynchronous	Asynchronous	Synchronous.	Asynchronous
It is Publish Subscribe Model	It is designed for Constraint devices.	Easy to debug	It is difficult to debug because you need the connection with library queue and scripting for same etc.
Designed for light weight machine to machine communication initially developed by IBM.	Constraint devices means without consume the extra RAM, packet easily generate and parsed.	Well mapped with interface Support to Every Programming language.	It Support to few programming Language like JAVA, .net, Ruby, Python, PHP etc.
It has broker over TCP	It is run over UDP	It require some kind of Service Discovery	It needs to know the broker to reach the queue to read/write.
Every Message is chunk of data. Every message to publish the address called Topic. So many client can subscribe for many topics. YouTube is best example of this model.	It is smaller in Packet size over TCP and HTTP. Due to work over UDP guaranteed delivery of packet or message.	Most of people aware with this protocol so it is familiar with many developer use in Application development so cost of training is reduced no extra effort will require to learn the things using HTTP. but	It require Extra training for to learn the Concept While debug and Application Development Using AMQP
It require username and password for Authentication purpose.	It is SMS and Packet based communication.	This Protocol not supported in internet so HTTP API Mostly used.	This Protocol Support to internet.
It work over TCP so Strong security is provided over communication.	It Work over UDP so less security provided over Communication.	not guaranty of message delivery due to Synchronous type of Communication	Guaranteed message delivery due to Asynchronous Type of Communication
TCP connection may be encrypted with SSL/TLS.	It support TLS, AES and RSA.	Not easy to maintain and Scale due to different Host region.	Easy to maintain and Scale by deliver/receive message by AMQP broker.
Some environment Packet loss is possible for various resources	Packet loss is less compare the MQTT.	It works for different IP Region.	To know the IP of Cluster can easily by deliver/receive message by AMQP broker.
Most recent Persistent message is stored so MQTT brokers do not allow send the persisted messages to back up inside the server in network.	It require back up inside the server response in network. Client can get post and delete the resources available in network. Message can fired or forget ie acknowledge by user using ack packet.	It require send the message to every component due to different host/IP region depend on Cluster.	It uses the FANOUT Concept one message is sufficient to send to different component while it is not mandatory to send the message separately to each and Every Component. It reduce the communication.
It is many to many Communication protocol.	It is One to One Communication protocol	Less faster compare to AMQP	Reliable and faster.
It not support the labeling of message or type of metadata. All client make communication only for known message format.	It supports the labeling of message or type of metadata. It provide the bulletin support for message transmission So it not necessary the client know the message format to allow the communication ove the network. Reduce the content and allow the discovery of ways to exchange the data.		

III CHALLENGES IN COMMUNICATION

In Internet of thing connect the various physical devices and gather the data via cloud to deliver the quick Access of data for business insight.

To make IoT Devices work smoother there are various technological challenges concern like security ,connectivity, compatibility, standards and Analytics of data or information.

Out of these we mainly highlight the Connectivity and Standards like Networking Protocol is the biggest challenge in IoT field. Some question comes to in mind IoT researcher as per following.

1. What types of Architecture framework choose for connecting the million of heterogeneous devices like client/server, peer to peer, centralized ?
2. How to Authenticate, Authorize, Accountability of individual using various Encryption method?
3. What different types of low power communication protocol used for short range distance?
4. What different types of low power communication protocol used for medium range distance?
5. What different types of low power communication protocol used for long range distance?
6. What different types of open source services choose according to required imposed by IoT?
7. How to handle data most efficiently as per type, size and formation parameter in concern?
8. How to store and process data efficiently as per Bigger in Size, real time and rapid speed parameter in concern?
9. What types of software component choose for optimization at protocol level?
10. What types of hardware component choose for optimization at protocol level?
11. What types of software services choose to handle the identification, addressing and administration?
12. What type of Infrastructure, storage and process technologies choose to Handel real time data?
13. How to integrate the different resources at product level?
14. How to integrate distributed application, smart grids over IoT architectural network?
15. How to improve life style of ruler management using IoT field?
16. How to handle individual privacy issue using IoT field?
17. What SOA architecture choose handle millions of devices?
18. How to handle non relevant data?
19. How to provide the security against hacking of device?
20. Which tools are choose to Analyze Big data?

In this way reliable, trusty, interoperable, effective and powerful mechanism is required for IoT is top priority at this moment.

This section trying to cover general challenges for new researcher.

IV CONCLUSION

In this review paper mainly focused on the different types of communication protocol used in IoT field. In upcoming years lots of IoT Application and communication technologies are coming soon that definitely impact on human life in next generation. IoT is growing very faster day by days add the million of device in every year. As per definition of IoT is concern communication between the smart devices are practically possible now days.

To this end it is observe that various types of Protocol are developed to make the communication between various machine but still factor are till limited because the types of machine or devices may be similar or different. The machine or device usage the different architecture framework in IoT so to bridge the gap between the from front end the end user include the various challenges due to same or different types of information or message or object.

Iot mainly concern with sensor and actuator so different types of sensors like Temperature sensors, Proximity sensor, Pressure sensor, Water quality sensor, Chemical sensor, Gas sensor ,Smoke sensor.IR sensors etc help in interact with different types of physical environment. Every sensor can gather the data in different format so it again challenging develop the architecture and communication protocol that support to device fo storage and processing purpose.

MQTT type of client/server model now days most successful to understood the people thoughts in tern of architecture and transportation. Every communication protocol usage depends on the application environment with some pros and cons. It is again need the deep study for upcoming years with new trends and technology coming soon.

Practically make the communication between the applications used in education, tourism, defense, military etc require more intelligent and smart device. Recent protocol may or may not work properly as per the these application is concern so need new type of Architecture and protocol design require to sustain in era of IoT.

In this review paper firstly introduce the various types of protocol used in communication to send and receive the message or data over network. While using the heterogeneous types of devices an important parameter comes in sense like IEEE Standard, frequency range, data rate, power consumption, networking type and their application usage. IoT filed diverse with set of application like Home Automation, Smart Cities, Healthcare monitoring and fitness, smart locks, smart agriculture and irrigation, smart Tv and Security camera, Automatic Appliances in home like smart meter, smoke detector, gas detector, smart thermostat etc so communication between these application with architecture and End user need additional security and simplicity so communication protocol again play important role over these application.

Second discussion comparative study of various protocol used in communication can clear the idea about the pros and cons of each protocol while used in application.

A main contribution of this review paper compare to other is that focuses on various challenges with related do different application highlight the research opportunities for future IoT researcher.

References

[1] Srivastava L 2006. Pervasive, ambient, ubiquitous, the magic of radio In: Proceeding of European Commission Conference "From RFID to the internet of Things, Bruxelles, Belgium.

[2] S. Bandyopadhyay, M. Sengupta, S. Maiti, and S. Dutta, "Role of middleware for internet of things: a study ," International Journal of Computer Science & Engineering Survey, vol. 2, no. 3, pp. 94–105, 2011.

[3] J. Soldatos, N. Kefalakis, M. Hauswirth et al., "Openiot: open source internet of-things in the cloud," in Interoperability and Open-Source Solutions for the Internet of Things: International Workshop, FP7 OpenIoT Project, Held in Conjunction with SoftCOM 2014, Split, Croatia, September 18, 2014, Invited Papers, vol. 9001 of Lecture Notes in Computer Science, pp. 13–25, Springer, Berlin, Germany, 2015

[4] A. Ranganathan, J. Al-Muhtadi, S. Chetan, R. Campbell, and M. D. Mickunas, "Middlewhere: a middleware for location awareness in ubiquitous computing applications," inACM/IFIP/ USENIX International Conference on Distributed Systems Platforms and Open Distributed Processing Middleware 2004, pp. 397–416, Springer, New York, NY, USA, 2004

[5] M. Eisenhauer, P. Rosengren, and P. Antolin, "A development platform for integrating wireless devices and sensors into ambient intelligence systems," in Proceedings of the 6th IEEE Annual Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks Workshops (SECON Workshops '09), pp. 1–3, IEEE, Rome, Italy, June 2009

[6] T. Zahariadis, A. Papadakis, F. Alvarez et al., "FIWARE lab: managing resources and services in a cloud federation supporting future internet applications," in Proceedings of the 7th IEEE/ ACM International Conference on Utility and Cloud Computing (UCC '14), pp. 792–799, IEEE, London, UK, December 2014

[7] Pallavi Sethi and Smruti Sarangi "Internet of Things: Architecture, Protocol and Application" review article on published on 26 January 2017

[8] https://www.rs-online.com/designspark/eleven-internet-of-things-iot-protocols-you-need-to-know-about

[9] https://www.cse.wustl.edu/~jain/cse570-15/ftp/iot_dlc/index.html

[10] https://dev.to/fedejsoren/amqp-vs-http

[11] https://www.eclipse.org/community/eclipse_newsletter/2014/february/article2.php

[12] http://opensourceforu.com/2017/10/communication-protocols-internet-things-choices/

[13] http://www.cse.iitd.ac.in/~srsarangi/files/papers/iot-survey.pdf