International Journal of Engineering Research and Technology. ISSN 0974-3154, Volume 12, Number 5 (2019), pp. 647-657
© International Research Publication House. http://www.irphouse.com

# Review of Various IoT Standards and Communication Protocols

**Deepti Rani[1] and Nasib Singh Gill[2]**

*[1]Research Scholar, Department of Computer Science & Applications, Maharshi Dayanand University, Rohtak, Haryana, India.*
*[2]Professor, Department of Computer Science & Applications, Maharshi Dayanand University, Rohtak, Haryana, India.*
*ORCIDs: 000-0003-1565-224X(Deepti), 0000-0002-8594-4320(Nasib)*

**Abstract:**

With tremendous growth in IoT devices in last few years, research has also geared up in finding solutions to make cloud related services more scalable. The present paper is focusing on study and survey of object-to-object communication protocols enabling Internet of Things (IoT) environment. The paper also covers range of various existing networking communication protocols, routing protocols, data transfer protocols and security protocols. These protocols are adopted in IoT based environment, with layer based taxonomy. Security is one of the main concerns of IoT based environment. So many security and lightweight protocols also have been detailed out. Few of the protocols proposed by researchers have been adopted very successfully in IoT enabled environment. Various IoT enabling standards and technologies have also been reviewed in this paper. Further this paper also highlights the properties, characteristics and specialties of these protocols. Last but not least, the comparative analysis of various messaging protocols has also has been presented on the basis of their performance.

**Keywords:** Internet of Things; IoT Application Domains; IoT Enabling Standards and Protocols; Analysis and Performance of Messaging Protocols.

## 1. INTRODUCTION

IoT has made human life more easy and efficient by enabling many non-living things to behave intellectually and smartly. Today's modern society has led to significant growth in IoT by virtually integrating things and people [1]. Number of objects and devices are being connected to smart environment at highly increasing rate [2]. Network that used to include only computers, mobile phones and some selected nodes only; now have included home appliances, vehicles and many more objects also. IoT network on small scale uses Wireless Personal Area Network (WPAN) that relies on technologies like Bluetooth, Zigbee [3], 6LowPAN and etc. and slightly on larger scale uses Wireless Local Area Network (WLAN) that includes Wi-Fi that has been used in different mobile communication technologies such as 2G, 3G, 4G, LTE and etc [3]. Forming a desirable and globally acceptable IoT system based on these technologies is a crucial challenge. Furthermore, data confidentiality as well as network security raises some issues [4]. These challenges are required to be addressed according to adopted networking technologies. This paper represents an overview of various applications, technologies, services, standards and protocols of Internet of Things. Using these technologies, one machine can communicate to other machine [5]. IoT protocols operate on different layers of networking stack which include MAC layer, session layer and network layer [6]. Most commonly used IoT Protocol standards are Zigbee and Bluetooth but IEEE 802.11ah [7] is easiest to be used in wireless applications. The main aspects of IoT protocols on all the layers are security and security mechanism. The authors in [6] concentrate on interconnection layers of IoT ecosystem containing applications, security, management, routing and sensing protocols. Data Transfer Protocol's suite can be classified into two parts, which are File Transfer Protocols and Messaging Protocols [8]. Protocols are used for transferring data packets from one node to another node. These nodes are devices which are characterized by unique ID, an address and probably a tag.

Evolution of IoT has been drawn from the convergence of Internet using electromechanical systems, wireless technology and Internet. Kevin Ashton, co-founder and executive director of MIT Auto-ID Center, mentioned IoT in a presentation; he made for P&G [9].

## 2. IoT APPLICATION DOMAINS

Now a day, Smart home market [10] [11] has become more dynamic. According to a survey done by Deloitte for smart home market review, only one million smart home customers already could be in Germany in 2018. The main concern of smart home households is in the safety and comfort followed by cost saving and less power consumption. But some barriers on the way of customers are data protection, data security and costs of efficient IoT objects.

Smart transport system is also one of the application domains that cover a wide area of IoT environment. The implementation of Controlled Area Network (CAN) [12] is used for system of Automation Control with 5G [13] communication technology, new protocols and Narrow Band-IoT (NB-IoT) [14], that is developed by 3GPP. NB-IoT is a radio technology standard that is used in many IoT application domains such as smart transportation for information exchange.

Patient's health monitoring is also an important application area of IoT that is operated using many mobile devices, technologies and protocols. According to a survey [15], Arduino was used in smart system of health monitoring.

Smart energy system [16] is also an application domain where IoT is being deployed. Some relevant applications of this area are: predictive maintenance, performance management of digital data, energy optimization, and throughput optimization, quality management of digital objects, automation level maintenance and quality control of sensors [11]. Some Protocols which have been considered in smart home domain are EnOcean, Z-Wave, Zigbee [17], KNX-RF [18] and Thread. Each protocol provides one or more security services like encryption, authentication and integrity.

## 3. IoT ENABLING STANDARDS AND PROTOCOLS

This section provides an overview of standards, technologies and different protocols which make things and environment IoT enabled. IEEE.15 and IEEE.11 [19] based standards are very common and widely used IoT protocols standards.

### *A. Standardizations/ Standards*

Most of the devices used in IoT have been standardized by one or more standardizations but most widely IEEE and Internet Engineering Task Force (IETF) [20] standardizations have been adopted. IEEE 802.15.4 is a radio frequency standard developed for constrained devices with low power and also defined operations in low rate wireless personal area network (LR-WPAN) [21]. Mainly this standard enables companies for IoT environment. In [22] Ahmed et al. addressed various IoT enabling standardizations, protocols, technologies and security issues in IoT enabled environment. First IEEE 802.15.4 [23] standard was announced in 2011 and later IEEE 802.15.4e [24] in 2012 was released. Later standard was accomplished with new MAC specifications having time slots channel capabilities. IETF developed standardizations by creating 6LOWPAN [24] for resource constrained devices in 2007. Then in 2008, IETF organization established “Routing Over Low Power Lossy Networks (ROLL)”, which was a routing protocol. Other achievements of IETF were, in 2010 “Constrained RESTful Environments (CORE)”, in 2013 “DTLS In Constrained Environment (DICE)” and in 2014 “Authentication and Authorization in Constrained Environment (ACE)” [22] [25].

### IEEE 802.15.4

IEEE supports huge range of working groups for wireless and wired communications. Industries are adopting 802.15.4e standardization on wide level where 802.15.4f is adopted for active Radio Frequency Identification (RFID) [26] and smart utility networks (SUNs) are adopting 802.15.4g to monitor smart grids. The versions discussed above use similar base of protocols and radio technology i.e. 802.15.4a/b. 802.15.4 and defines star and peer-to-peer topologies for communications between nodes and communicated data; that must pass through coordinator node or centre. This standard specifies media access control (MAC) layer and physical layer (PHY), lower layers of OSI network model that is used worldwide and maintained by IEEE 802.15 group [22]. Fig. 1 shows stack of 802.15 standards. Here, IEEE 802.2 is used as logical link control that communicates with convergence sub-layers. LLC is upper portion of DLL in OSI model. IEEE 802.15.4 is a well known technical standard for LR-WPAN.

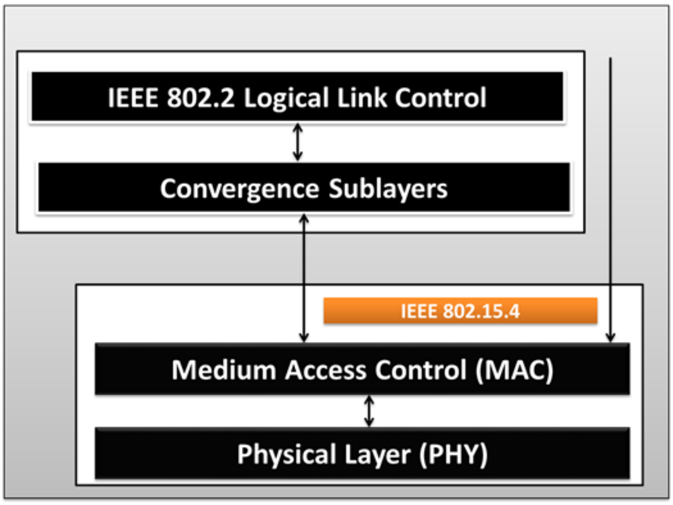


**Figure 1:** IEEE 802.15 Standard’s Stack

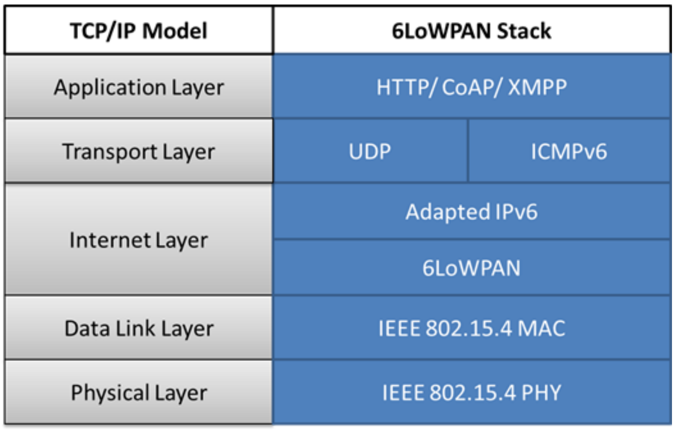
Some well known protocols based on IEEE 802.15.4 are Zigbee, WirelessHART [27] and ISA100.11a, Microchip Wireless Network (MiWi (mainly used in smart homes)) [28] [29], Thread [30], SNAP and 6LoWPAN. To offer lower network layers of WPAN targeting low cost, low speed and low bandwidth is an objective of IEEE 802.15.4 [19]. For more bandwidth it can be contrasted with Wi-Fi. The main feature of IEEE standard 802.15.4 is to achieve very low cost (manufacturing and operation) as well as technical simplicity without sacrificing generality and flexibility. This standard is highly suitable for real time applications and also to operate in TDMA and CSMA/CD access modes.

### Zigbee

Zigbee [3] [17] [19] is the most widely used due to its simplicity and it is deployment of 802.15.4 standard. Zigbee is a popular device used for low power and low bit rate and it is based on wireless mesh network standard and is motivated by WPAN [16]. Zigbee protocols are developed, supported and maintained by Zigbee Alliance group [30]. It uses mesh topology. Enhanced features of this standard include data encryption, authentication, data routing and forwarding. So the protocols inspired by Zigbee standard provide more security. The advance standard uses layer 3 and layer 4 for additional communication. Most popularly, it is used in wireless sensor networks. Using mesh topology any node can communicate with other node but within defined range. Versions of Zigbee can support energy harvesting in condition of unavailability of battery and AC mains. Applications inspired Zigbee include features such as Remote controlling, smart energy monitoring, building automation, smart health care, smart lighting, peripherals and devices (keyboard, mouse, touch pads, etc.) and many smart network services. It is reliable device and it is used globally. According to study done by many researchers, power consumption is an issue and it needs an improvement till satisfaction of users [3]. 5G communication technology is deployed in smart devices and terminals having potential to join ZigBee network to improve the performance of data transmission.

### 6LoWPAN

IPv6 over Low Power Personal Area Networks (6LoWPANs) was also created by IETF. Due to continuous increase in IoT smart devices; much stable, scalable and secure IP addresses are required for these devices. IPv6 is very efficient and enabling technology in such conditions where huge number of IP addresses is needed. 6LoWPAN is a protocol transports IPv6 packets through the links of IEEE 802.15.4 and enables IP connectivity in resource constrained network systems [22] [25]. 6LoWPAN working group works on optimization of protocols of IPv6 over the network, by using 802.15.4. 6LoWPAN also helps in applying IPv6 to MAC and Network layers of 802.15.4. Different features of 6LoWPAN are 64 bit or 16 bit address supporting, IPv6 and UDP header compression, targeting low power network using Bluetooth Low Energy (BLE), unicasting, broadcasting and multicasting support, and fragmentation [31]. Therefore, 6LoWPAN is very suitable protocol for Internet of Things. 6LoWPAN is an open protocol of IoT network. Using this protocol, home automation cost and architecture complexity can be decreased [32].



| TCP/IP Model | 6LoWPAN Stack | |
|---|---|---|
| Application Layer | HTTP/ CoAP/ XMPP | |
| Transport Layer | UDP | ICMPv6 |
| Internet Layer | Adapted IPv6 | |
| | 6LoWPAN | |
| Data Link Layer | IEEE 802.15.4 MAC | |
| Physical Layer | IEEE 802.15.4 PHY | |

**Figure 2:** 6LoWPAN protocol stack corresponding to TCP/IP Model

This technology can replace costly Wi-Fi also. Here, Fig. 2 shows 6LoWPAN protocol stack corresponding to TCP/IP model. Adaptation Layer used between Network and Data Link Layer fragments and reassemble IPv6 packets. 6LoWPAN is also useful for routing decision; so it is also called 6LoWPAN Border Router (6LBR) [33].

### LoRAWAN

Low Power Wide Area Network (LPWAN) [3] [34] technology was designed to integrate large number of devices in IoT. This technology is reverse to short range cellular networks having devices with range of large communication and less cost with long battery life. Long Range Wide Area Network (LoRAWAN) was designed by optimization of LPWAN to have low cost, lower energy consumption, large range and capacity. LoRAWAN is developed and maintained by LoRAWAN Alliance that is non-profit open association. LoRAWAN networks use the star topology, in which end devices transfer messages to gateways and gateways relay messages to server.

### Z-Wave

Z-Wave is also a wireless communication networks that uses low power [11]. It was designed by Sigma Design Inc. Z-Wave is widely used in remote control application in smart home and commercial environments on small scale [6]. Z-Wave is mainly designed to connect smart devices to central hub in smart homes and it allows devices to communicate with each other for data exchange. Z-Wave covers layers from physical to application. At physical layer it operates in scientific, organizational and medical related radio frequency band. Low-frequency data communication frequency bands are used in such applications. It can be used as alternate of ZigBee. It is simple to use and installs Z-Wave and it is an active technology too.

### Bluetooth Low Energy (BLE)

Bluetooth Low Energy (BLE) was introduced by Special Interest Group (SIG) of Bluetooth [6] [35]. It was specified in version 4.0 of specifications for Bluetooth Protocol. As compared to classic Bluetooth it is very much efficient for reducing the device cost and energy consumption. BLE structure includes Physical layer (PHY), Data link layer, Logical link control and Adaptation Protocol (L2CAP). Upper layer and attribute protocols are multiplexed. In discovering way, transporting attributes and Generic attribute profiles (GATT) are defined. Protocol stack is divided in two parts: Controller and Host. Both components can communicate with each other with standardized host controller interface [36].

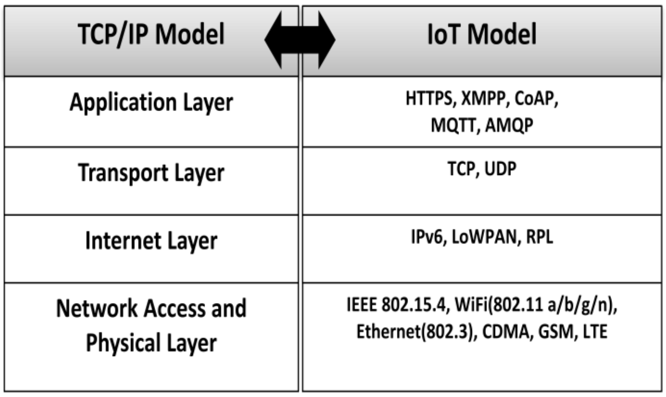
### IPSec

IPSec [36] [37] is also network protocol suite that establishes secure channels over various unreliable networks. Components and features of IPSec have been defined in RFC 4301. Availability of IPSec is defined in all IPv6 and it is also compatible to IPv4. IPsec provides confidentiality, integrity and authentication at TCP/IP protocol stack at Internet layer. As compared to the upper layer, security protocol (TLS) in stack, IPSec has more ability to protect and secure IP header and Transport layer header (including IP address and Port number). But data security with IPSec is more expensive as compared to some other layers. IPsec channel consists of two phases: First phase performs peer authentication that also negotiates security parameters and ends successfully after data exchange. Second phase uses secure channels for secret exchange and parameter exchange. But validity of parameter is limited. Protocols of IPsec can operate on transport mode as well as tunnel mode.

### *B. Wireless Network Protocols*

First, Wireless Sensor Network connections increase productivity of various smart domains (smart home, smart city and etc.) and some risks are also introduced. Wireless physical networks give opportunity to attackers to attack on communicating data as well as Internet of Things (IoT) to reveal useful information. Stefan et al. [11] addressed some security challenges of various protocols used in Smart home domain. According to authors the security analysis need to be performed in all existing technologies to discover the root cause and to verify the security system to reach the secure IoT environment. Authors in [11], described some IoT protocols used for smart home applications specifically in perspective of security. The standard architecture of OSI model defines a standard architecture with all layers used in network communication. While TCP/IP model is a simplified view of OSI network model containing four layers which are used for Internet communication.

Before the study of IoT protocols, it is very much necessary to study the relation between traditional OSI or TCP/IP model and IoT protocol stack for better understanding of implementation of protocols in smart environment. Fig. 3 shows the layout of IoT protocol stack corresponding to layers of TCP/IP model.



| TCP/IP Model | IoT Model |
|---|---|
| Application Layer | HTTPS, XMPP, CoAP, MQTT, AMQP |
| Transport Layer | TCP, UDP |
| Internet Layer | IPv6, LoWPAN, RPL |
| Network Access and Physical Layer | IEEE 802.15.4, WiFi(802.11 a/b/g/n), Ethernet(802.3), CDMA, GSM, LTE |

**Figure 3:** IoT Protocol Stack Model

Some other standards offered by Institute of Electrical and Electronics (IEEE) and International Telecommunication Union (ITU) for IoT were proposed in [6**]**. Network protocols, schemes and mechanisms for IoT with their features, trends of networking mechanisms and open challenges were discussed in detail in [1]. In smart production system, wireless sensor networks (WSN) play very important role for increasing the flexibility. Wireless Sensor Network (WSN) is one of the critical parts of Internet of Things (IoT) architecture while designing a framework for IoT installations. Paper [1] also deals with low energy consuming networking protocols for wireless sensor networks and IoT networks.

### *C. Key Exchange and Data Authentication Protocols*

The Sensory information provided by IoT devices need to be communicated securely. Main constraints of IoT devices are power, energy, speed and computational limits [38]. Information is exchanged through gateway. The gateway connection needs to be secure and trustworthy. IoT devices must be authenticated by this gateway. Authors in [38] provided the discussion about lightweight authentication and key exchange protocols. These protocols depend on pair of devices having pair of unique keys (one master key and one session key) which are provided at the time of configuration. Session key changes constantly during session and it is used for exchange of frames securely. These lightweight protocols use only symmetric key cryptography and HMAC based key derivation function to provide confidentiality, integrity, key exchange and authentication in wireless as well as physical medium of communication. Devices in IoT environment communicate and exchange key with rest of the environment using gateway or sink so the communication needs to be secure and authenticated. Key exchange and authentication between two nodes without trusted third party (TTP) requires a prior establishment for sharing secret between two nodes. There can be more than one secret key which serve different purposes. Protocols provide Perfect Forward Secrecy; means if key is known at some point in a session, all past session communicated information must be secure. The contribution of paper [38] is complete analysis of various network communication technologies for IoT; regardless of network topology, application domain and communication range and an overview of IoT architecture, technology usage and application usage in a better way [1].

### *D. IoT Messaging Protocols*

IoT messaging protocols are also known as Instant Messaging Protocols (IM) and mainly used for chat communication on Internet. HTTP, MQTT, CoAP, XMPP and AMQP are protocols which are mainly designed for IoT applications. The properties of these protocols are message management, lightweight message overhead and small messaging.

#### Hyper Text Transfer Protocol (HTTP)

HTTP is being used as a very famous communication protocol for many years. It is widely used with its APIs in many programming languages. This is one of the oldest protocols used for IoT. Author in [39] compared this protocol with many other modern protocols used in IoT environment. It has many footprints. Due to running over TCP and using 3-way handshake process, it needs more resources. It is not much suitable to run over embedded processes with low power. It can be achieved by only optimization of TCP. This protocol follows client-server model. The communication takes place using request/ response format of messaging. HTTP is associated with REST. It is based on IETF standard. GET, POST, PUT and DELETE methods are used for update, create, read and delete operations respectively [40] [41].

#### Message Queue Telemetry Protocols (MQTT):

MQTT is one of the top lightweight protocols that works on publish-subscribe archetype. In IBM, Andy Stanford Clark introduced MQTT in 1999. It was standardized by OASIS later in 2013 [6]. This paradigm makes the protocol suitable for resource constrained devices and network connections with non ideal conditions like high latency and low bandwidth [40]. This is a simple structured protocol with higher reliabiliy. As compared with other reliable messaging protocols it has lighter header and requires less power. Due to its simplicity and having a small message header it is often recommended as compared to other message protocols for communication in IoT. IBM recently released MQTT v3.1, a new version of MQTT [41] adopted by IoT by OASIS. MQTT in [42] was proposed for drawing reality in the industry 4.0. This protocol is not like request-response type protocol. This lies on top of tranport protocols.

Fig. 4 shows an MQTT Model of message Exchange in IoT environment. MQTT protocol uses publish/subscribe pattern for flexibility in transition and implementation. It is an ideal lightweight messaging protocol. MQTT is message centric protocol mainly designed for Mobile-to-mobile (M2M) communication and remote telemetry applications [8].

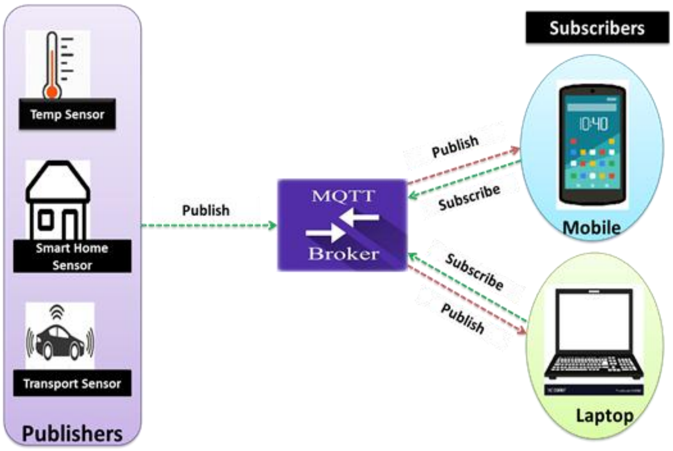


**Figure 4:** MQTT Model of message Exchange in IoT

MQTT includes four major components [43]: (1) Broker- This is the foremost component. Broker works like a server and is used for data monitoring between remote devices and sensors. Broker enables devices to connect automatically with other devices using three major Quality of Services (QoSs), (2) Another component of MQTT is Topic that enables sensors and devices to produce information based on some Topics. Two more components are: (3) Publisher and (4) Subscriber [42]. Usually clients are the devices which are capable of publish messages; Subscribers can receive messages or play the roles of both [40]. Clients know about the brokers to that it connects and when it plays the role of subscriber, it must know about subscribing subject or topic. In order to receive a corresponding message, a client can subscribe to a specific topic. Other clients can also subscribe the same topic for getting updates from the brokers with every arrival of message. Broker is the centre component that accepts published messages with the help of topic and subscribed client send filtered message. In other words, Publish means to send data to the broker and subscribe means to get data from broker [42]. Publishers are actually lightweight sensors that send data to broker and go to sleep mode back whereas subscribers are applicable, which are interested in the sensory data or topics and connect to the certain brokers. Brokers must classify this sensory data into topics and send to those subscribers who are interested in corresponding topics. MQTT is designed to establish embedded connection between middleware and applications as well as communications and networks [6].

### Secure MQTT (SMQTT)

SMQTT [6] is secure extension of MQTT protocol. SMQTT uses lightweight encryption attributes. It was introduced to enhance security feature of MQTT. The most important feature of this protocol is broadcast encryption. Using this one message is encrypted can be sent to multiple other devices. Four main stages of this algorithm are: First is setup phase where publishers and subscribers register themselves with the broker and also get a secret master key according to the key generation algorithm chosen by developer. Second phase is encryption that is followed after data is published to encrypt the data, decryption, Using publish phase data is published and is sent to subscriber and final phase is decryption to decrypt the data using secret master key. There is no standardized algorithm for key generation and encryption.

### Advanced Message Queuing Protocol (AMQP)

AMQP is a session layer messaging protocol. It was designed for industrial and business management in order to offer non-proprietary solutions to exchange large amount of messages. Main possibilities for message delivery offered by AMQP are: point-to-point and store-and forward. Advanced Message Queuing Protocol is an open standard protocol that was standardized by OASIS [44]. So many features of AMQP are similar to MQTT. MQTT and AMQP use same technique for message delivery [45]. It also runs over TCP platform and follows publisher/ subscriber architecture.

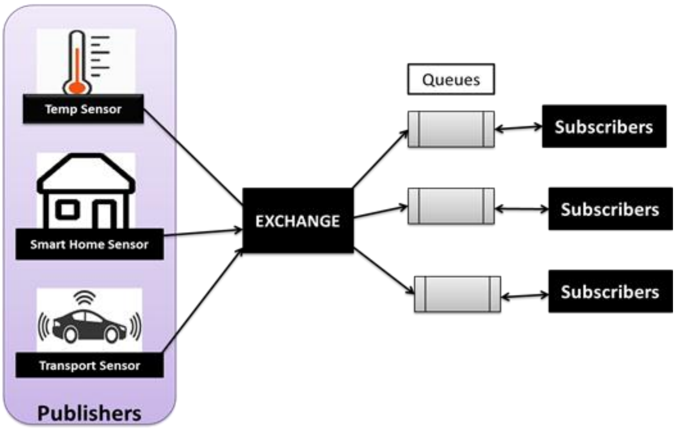


**Figure 5:** AMQP Model of message Exchange in IoT

Fig. 5 shows AMQP based Model of message Exchange in IoT environment. It was designed to enable interoperability between wide range of domain applications and systems. The interoperability feature of AMQP is significant as it allows different platforms and implemented in different languages to exchange messages. So it can be useful for heterogeneous systems [40]. AMQP works like email or instant messaging system and it comprises of network protocols specifying the entities producer/consumer and broker to interoperate with protocols model.

Message processing in AMQP are self contained and data contained by these messages are opaque. AMQP can support any size of message [45]. AMQP is middleware protocol and it is used for exchange messages in distributed area of applications. It also provides abstraction and simplification in communication programs. It provides reliable performance in different application entities. But in context of mobile networks the implementation has not been well tested.

In [45] AMQP was proposed to identify the limits of middleware applicability, capacity of message loss and latency during interrupted and disconnected condition of wireless devices. Jorge et al. [45] also compared the capabilities of AMQP and MQTT through suitable measurements under wireless network and the also presented evaluation results. Nitin Naik in [46] shows the dilemma of messaging protocol in IoT industry and compared various protocols. He also presented the evaluation of four established messaging protocols, which are: MQTT, CoAP, AMQP and HTTP for IoT.

RabbitMQ, a very popular implementation of message broker, is used as a message bus. It is very popular implementation of Advanced Message Queuing Protocol (AMQP). Using this implementation, messages are stored in queues on a centre node server i.e. RabbitMQ, before sending to the client [47]. In essence, RabbitMQ is an open-source implementation of AMQP. It is a standard protocol with scrutinized design. It enjoys a higher level of interoperability and can work very easily with other AMQP-compliance implementations [48].

### Constrained Application Protocol (CoAP)

CoAP is a request/ response synchronous application layer protocol. It was formularized by Internet Engineering Task Force (IETF) and Constrained RESTful Environment (CORE) for providing a lightweight RESTful interface [6]. CoAP is deployed in various application domains from smart energy system to environment monitoring. CoAP is used in tiny size devices with low power, less computation and communication capabilities to enable them to utilize the RESTful interaction.

Fig. 6 shows CoAP based Model of message Exchange in IoT environment. It is a web transfer protocol similar to HTTP that is able to extend the architecture from Representational State Transfer (REST) to LoWPANs [8]. REST is actually a standard interface between client and server and it was developed to enable sensors with low power. Instead of TCP that is used in HTTP, CoAP is build over UDP platform and it is a binary protocol. The major reason for developing over UDP is to remove the TCP overhead to reduce the requirement of bandwidth [49]. But reliability reduces too.

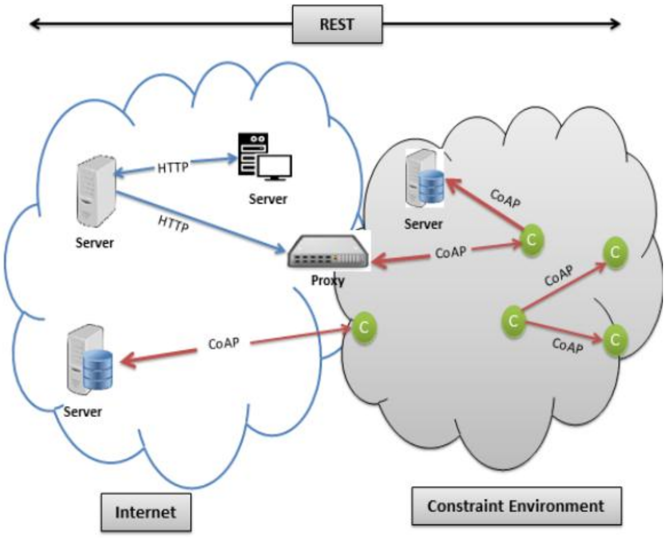


**Figure 6:** CoAP Model of message Exchange in IoT

Then IETF created the document for CoAP with possibility of running over TCP [50]. When a single or multiple requests are sent from client to server then the response is always sent over new connection. It has a light reliability mechanism. Architecture of CoAP has mainly two sub-layers: (1) messaging and (2) request/response. Messages are communicated through these sub-layers. Messaging sub-layer provides redundant detection and reliable delivery of message that is based on stop and waits messaging transmission. Request/response sub-layer is responsible for communication. This sub-layer can utilize both synchronous and asynchronous Responses. CoAP has four transmission modes: (1) Confirmable, (2) Non-confirmable, (3) Piggyback and (4) Separate. Confirmable and non-confirmable modes permit reliable and non-reliable transmission. Piggyback is used to provide direct communication to client-server direct communication and acknowledged. In HTTP, CoAP uses GET, PUT, PUSH and DELETE request methods to retrieve, create, update and delete the messages respectively in the network to manage URI identifier [41].

### Extensible Messaging and Presence Protocol (XMPP)

XMPP is an open standard technology of messaging protocol designed by IETF [51]. Initially, it was designed for instant message exchange between applications to achieve basic security features including end-to-end encryption, authentication and compatibility [52]. This protocol is a text based protocol based on XML that can implement both publish-subscribe and client-server interaction. Though XMPP supports client-server model for interaction but there are new extensions also; which can enable public-subscribe generic model. XMPP can create topics and publish information by these generic extensions. The client-server communication in XMPP is done through XML streams. Data is exchanged in form of XML structured stanzas or tags. Three types of tags are defined, which are: <presence/>, <message/> tag that defines title and body, and <iq/> i.e. info/query that pairs message senders and receivers. Each iq tag must have an identity. XMPP specification follows TLS and DTLS reliable encryption that ensure data integrity and confidentiality [40].

XMPP is also known as instant messaging (IM) standard given by IETF. Some useful application of XMPP are video calling, teleconferencing, and chatting. It is a secure protocol and more suitable for IoT compared to CoAP request/ response. This is one of top protocols on IoT platform. Its functons are similar to HTTP GET and POST methods while getting information from server and applying settings to server.

## 4. PERFORMANCE BASED RELATIVE ANALYSIS AND COMPARATIVE STUDY OF VARIOUS MESSAGING PROTOCOLS OF IOT SYSTEMS

On the basis of the study and survey of literatures in the related area; the performance analysis of various messaging protocols has been carried out based on different scales including message size, overhead, power consumption, resourse requirement, latency, bandwidth, interoperability, reliability and most important security level. Below table 1 shows the performance analysis of some widely used messaging protocols (MQTT, CoAP, AMQP and HTTP) in IoT enabled smart environment. These messaging protocols have been studied and comparison analysis has been carried out. The mssaging protocols proposed and implemented in different application areas and researches [42] [44] [45] [46] [48] [50] [51] have been analysed. It has been analyzed that HTTP is good on many scales but it is less reliable while MQTT is highly reliable protocol. Further MQTT is less secure. Table 2 presents comparison analysis of these protocols in the context of their , header and message size, architecture, quality of service, reliability, security, standards, licencing and encoding scheme.

**Table1:** Performance Based Relative Analysis of Various Application Layer Messaging Protocols of IoT Systems: MQTT, COAP, AMQP and HTTP on the basis of their Performance

| Criteria | MQTT | CoAP | AMQP | HTTP |
|---|---|---|---|---|
| **Message size** | Medium (Higher than CoAP) | Low | Medium (>MQTT and <HTTP) | High |
| **Message Overhead** | Medium (Higher than CoAP) | Low | Medium (>MQTT and <HTTP) | High |
| **Power Consumption** | Medium (Higher than CoAP) | Low | Medium (> MQTT and <HTTP) | High |
| **Resource Requirement** | Medium (Higher than CoAP) | Low | Medium (> MQTT and <HTTP) | High |
| **Latency** | Medium (Higher than CoAP) | Low | Medium (> MQTT and <HTTP) | High |
| **Bandwidth** | Medium (Higher than CoAP) | Low | Medium (> MQTT and <HTTP) | High |
| **Interoperability** | Low | Medium (Higher than AMQP and Lower than HTTP) | Medium (> MQTT and <HTTP) | High |
| **Reliability** | High | Medium (Higher than HTTP and Lower than AMQP) | Medium (>CoAP and <MQTT) | Low |
| **QoS** | High | Medium (Higher than HTTP and Lower than AMQP) | Medium (>CoAP and <MQTT) | Low |
| **Security** | Low | Medium (Higher than MQTT and Lower than HTTP | High | Medium (Lower than AMQP but Higher than CoAP) |
| **Provisioning** | Low | Medium (Higher than MQTT and Lower than HTTP | High | Lower than AMQP but Higher than CoAP) |
| **Standardization** | Low | Medium (Higher to AMQP but Lower to HTTP) | Medium (Higher to MQTT but Lower to CoAP) | High |
| **IoT Usage** | High | Medium (Higher to HTTP but Lower to AMQP | Medium (Higher to CoAP but Lower to MQTT) | Low |

**Table 2:** Comparative Study of Messaging Protocols for IoT Environment: MQTT, CoAP, AMQP and HTTP

| Criteria | MQTT | CoAP | AMQP | HTTP | DDS | XMPP |
|---|---|---|---|---|---|---|
| **Year** | 1999 | 2010 | 2003 | 1997 | 2001 | 1999 |
| **Architecture** | Client/Broker | Client/Server or Client/Broker | Client/Broker or Client Server | Client/Server | Broker-less architecture | Client/Server |
| **Abstraction** | Publish/Subscribe | Request/Response or Publish/Subscribe | Request/Response or Publish/Subscribe | Request/Response | Real Time Data Centric Publish/Subscribe | Request/Response or Publish/Subscribe |
| **Header Size** | 2 Bytes | 4 Bytes | 8 Bytes | Undefined | Undefined | Undefined |
| **Message Size** | Small and Undefined (upto 256MB maximum size) | Small and undefined (Small to fit in single IP datagram) | Negotiable and Undefined | Large and Undefined (depends on the web server or the programming technology) | Undefined | Undefined |
| **Semantics/ Methods** | Connected, Disconnected, Publish, Subscribe, Unsubscribe, Close | Get, Post, Put, Delete | Consume, Deliver, Publish, Get, Select, Ack, Delete, Nack, Recover, Reject, Open, Close | Get, Post, Head, Put,<br>Patch, Options, Connect, Delete | Connected, Disconnected, Publish, Subscribe without Broker | HTTP GET and POST methods, Defined Tags <presence/>, <message/> and <iq/> |
| **Cache and Proxy Support** | Partial | Yes | Yes | Yes | Yes | Yes |
| **Quality of Service(QoS)/ Reliability** | Qos 0- At most once (Fire and Forget),<br>QoS 1- At least once,<br>QoS 2- Exactly once | Confirmable Message(similar to At most once) or Non-confirmable Message (similar to At least once) | Settle Format (Similar to At most once) or Unsettle Format (Similar to At least once) | Limited (via Transport Protocol - TCP) | 23 excellent quality of service levels, High reliability | No Quality of Service |
| **Standards** | OASIS, Eclipse Foundation | IETF, Eclipse Foundation | OASIS, Eclipse Foundation | IETF and W3C | Open | IETF |
| **Transport Protocol** | TCP (MQTT-SN can use UDP) | UDF, SCTP | TCP, SCTP | TCP | TCP/UDP | TCP/IP |
| **Security** | TLS/SSL | DTLS, IPSec | TLS/SSL, IPSec, SASL | TLS/SSL | No Security | SASL and TLS |
| **Default Port** | 188/ 8883 (TLS/SSL) | 5683(UDP Port)/ 5684 (DTLS) | 5671 (TLS/SSL), 5672 | 80/ 443 (TLS/SSL) | 7400/7410/7411 | 5222 |
| **Encoding Format** | Binary | Binary | Binary | Text | Text | XML |
| **Licensing Model** | Open Source | Open Source | Open Source | Free | Open Source | Open Source |
| **Applications/ Supporting Organizations** | IBM, Facebook, Eurotech, Cisco, Software AG, Red Hat, Tibco, Amazon Web Services, M2Mi, InduSoft, Fiorano | LargeWeb Community Support, Cisco, Contiki, Erika, Iotivity | Microsoft, Bank of America, Barclays, JP Morgan, Goldman Sachs, Credit Suisse | Global Web Protocol Standard | Military Applications | Skype, O'Reilly |

## 5. CONCLUSION

In this paper we reviewed literature related to IoT messaging protocols, network protocols, key exchange and security protocols for IoT enabled smart environment. Some of these papers relate to existing protocols and standards while some others relate to proposed and accepted protocols for IoT environment. In recent years, various lightweight protocols and security protocols have been proposed. We also compared some messaging protocols on the basis of their performance and reviewed various standards, algorithms, technologies and techniques used for designing a protocol for IoT environment.

As this paper presents advantages, disadvantages and performance of various message protocols, it will help in designing new protocols and improving existing protocols in future.

## REFERENCES

[1] Anna Triantafillou, Panayiotis Sarigiannidis, and Thomas D. Lagkas, "Network Protocols, Schemes, and Mechanisms for Internet of Things (IoT): Features, Open Challenges, and Trends", Wireless Communications and Mobile Computing 2018, Article ID 5349894, Sep 2018, 24 pages. https://doi.org/10.1155/2018/5349894

[2] Snehal Deshmukh and S. S. Sonavane, "Security protocols for Internet of Things: A survey", 2017 International Conference on Nextgen Electronic Technologies: Silicon to Software (ICNETS2), 16 October 2017, pp. 71-74. IEEE. https://doi.org/10.1109/ICNETS2.2017.8067900

[3] Jiasong Mu and Liang Han, "Performance analysis of the ZigBee networks in 5G environment and the nearest access routing for improvement", Ad Hoc Networks, Vol. 56, March 2017, pp. 1-12.

[4] Harpreet S. Dhillon, Howard Huang, and Harish Vishwanathan, "Wide area wireless communication challenges for the Internet of Things", IEEE Communications Magazine, Vol. 55, Issue 2, 03 February 2017, pp. 168-174. https://doi.org/10.1109/MCOM.2017.1500269CM

[5] Vangelis Gazis, "A survey of standards for machine-to-machine and the Internet of Things", IEEE communications Surveys and Tutorals, Vol. 19, No. 1, 2017, pp. 482-511. https://doi.org/10.1109/COMST.2016.2592948

[6] Tara Salman and Raj Jain, "Networking Protocols and Standards for Internet of Things", Chapter 13, John Wiley & Sons, Inc, 2017. https://doi.org/10.1002/9781119173601.ch13

[7] Freddy K. Santoso and Nicholas CH Vun.,"Securing IoT for smart home system", IEEE International Symposium on Consumer Electronics (ISCE), June 2015, pp. 1–2. IEEE. https://doi.org/10.1109/ISCE.2015.7177843

[8] Tanya Mohan Tukade and R M Banakar, "Data Transfer Protocols in IoT-An overview", International Journal of Pure and Applied Mathematics, Vol. 118, No. 16, January 2018, pp. 121-138. url: http://www.ijpam.eu

[9] Stephan Haller, Stamatis Karnouskos, and Christoph Schroth, "The internet of things in an enterprise context", Future Internet Symposium- FIS 2008, Springer, 2009, pp. 14-28.

[10] Deloitte, "Switch on to the connected home | The Deloitte Consumer Review", July 2016, pp.1-23.

[11] Stefan Marksteiner, V. J. Exposito Jimenez, H. Vallant, and H. Zeiner, "An Overview of Wireless IoT Protocol Security in the Smart Home Domain", Joint 13th CTTE and 10th CMI Conference on Internet of Things Business Models, Users, and Networks, Copenhagen. 18 Jan, 2018, pp. 1-8, IEEE. https://doi.org/10.1109/CTTE.2017.8260940

[12] M. Goossens, F. Mittelbach, and A. Samarin, "CAN System Engineering: From Theory to Practical Applications" New York City: Springer International Publishing A G, 2013.

[13] A. Gupta and R. K. Jha, "A survey of 5g network: Architecture and emerging technologies," IEEE Access, Vol. 3, 28 July 2015, pp. 1206–1232. https://doi.org/10.1109/ACCESS.2015.2461602

[14] Yihenew Dange Beyene, Riku Jantti, Kalle Ruttik, and Sassan Iraji, "On the performance of narrow-band internet of things (nb-iot)," IEEE Wireless Communications and Networking Conference (WCNC) 11 May 2017, pp. 1–6. https:/doi.org/10.1109/WCNC.2017.7925809

[15] B. N. Karthik, L. Durga Parameswari, R. Harshini and A. Akshaya, "Survey on IOT & Arduino Based Patient Health Monitoring System", International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 2018 IJSRCSEIT, Vol. 3, Issue 1, ISSN : 2456-3307, pp.1414-1417, 2018.

[16] S. Wang, J. Wan, D. Li, and C. Zhang, "Implementing smart factory of industrie 4.0: an outlook," International Journal of Distributed Sensor Networks, Vol. 12, No. 1, 19 Jan 2016. https://doi.org/10.1155/2016/3159805

[17] Milu Hanna Mathew and Dr. T. Parithimar Kalaignan, "A Literature Survey On Zigbee", International journal of current engineering and scientific research (IJCESR), Vol. 5, Issue 2, 2018, pp. 57-60. https://doi.org/10.21276/Ijcesr

[18] KNX Association, "KNX Secure," KNX Association, KNX Position Paper. Available at: https://www.knx.org/media/docs/downloads/Marketing/Flyers/ KNX-Secure-Position-Paper/KNX-Secure-Position-Paper en.pdf

[19] Arda Surya Editya, Surya Sumpeno and Istas Pratomo, " Performance IEEE 802.14.5 and ZigBee protocol on realtime monitoring augmented reality based wireless

sensor network system" International Journal of Advances in Intelligent Informatics, ISSN: 2442-6571, Vol. 3, No. 2, July 2017, pp. 90-97. https://doi.org/10.26555/ijain.v3i2.99

[20] Zhengguo Sheng, Shusen Yang, Yifan Yu, Athanasios V. Vasilakos, Julie A. McCann, and Kin K. Leung, "A survey on the IETF Protocol suite for the Internet of Things: Standards, Challenges, and Opportunities," IEEE Wireless Communications Magazine, Vol. 20, No. 6, 6 December 2013 pp. 91–98. https://doi.org/10.1109/MWC.2013.6704479

[21] Hong Min Bae, Chan Min Park, Shinil Suh and Rana Asif Rehman, "Performance Improvement in Beacon-enabled LR-WPAN-based Wireless Sensor Networks" SENSORNETS 2016- 5th International Conference on Sensor Networks, January 2016. https://doi.org/10.5220/0005632400890094

[22] Ahmed Mohammed Ibrahim Alkuhlani and Dr. S.B. Thora, "Internet of Things (IoT) Standards, Protocols and Security Issues", In International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), Vol. 4, Issue 11, pp. 491-495, November 2015. https://doi.org/10.17148/IJARCCE.2015.411109

[23] 802.15.4-2011:IEEE Standard for Local and Metropolitan Area Networks- Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs), Institute of Electrical and Electronics Engineers Std., September 2011.

[24] 802.15.4e-2012: IEEE Standard for Local and Metropolitan Area Net-works - Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 1: MAC Sublayer, Institute of Electrical and Electronics Engineers Std.

[25] C. Lakshmi Devasena, "IPv6 low power wireless personal area network (6LoWPAN) for networking Internet of Things (IoT) - Analyzing its suitability for IoT", Indian Journal of Science and Technology, Vol. 9, No. 30, August 2016, pp. 1-6. https://doi.org/10.17485/ijst/2016/v9i30/98730

[26] Alireza radan, Hoseine samimi, and Ali moeni, "A new lightweight authentication protocol in IoT environment for RFID tags", International Journl of Engineering and Technology, Vol. 7, No. 4.7, 2018, pp. 44-351. https://doi.org/10. 14419/ijet.v7i4.7.23028

[27] Jianping Song, Song Han, Aloysius Mok and Deji Chen "Wirelesshart: Applying Wireless Technology in Real-Time Industrial Process Control" Conference: Real-Time and Embedded Technology and Applications Symposium 2008, Proc. IEEE RTAS, May 2008, pp. 377–86. https://doi.org/10.1109/RTAS.2008.15

[28] Suman Chhajed, Mohammad Sabir and Kiran P. Singh, "Wireless Sensor Network implementation using MiWi wireless protocol stack", 2014 IEEE International Conference Advance Computing Conference (IACC), 21-22 February 2014, pp. 239-244. https://doi.org/10.1109/IAdCC.2014.6779327

[29] Juan Aponte-Luis, Juan Antonio Gómez-Galán, Fernando Gómez-Bravo, Manuel Sánchez-Raya, Javier Alcina-Espigado and Pedro Miguel Teixido-Rovira, "An Efficient Wireless Sensor Network for Industrial Monitoring and Control", Sensors 2018, Vol. 18, No. 1, January 2018, pp.1-15. https://doi.org/10.3390/s18010182, MDPI Journals,.

[30] Stefan Marksteiner, Víctor Juan Exposito Jimenez, Heribert Valiant and Herwig Zei, "An overview of wireless IoT protocol security in the smart home domain", Published in 2017 Internet of Things Business Models, Users, and Networks, January 2018. https://doi.org/ 10.1109/CTTE.2017.8260940

[31] Dr. Lakshmi Devasena C, "IPv6 low power wireless personal area network (6LoWPAN) for networking Internet of Things (IoT) - Analyzing its suitability for IoT", Indian Journal of Science and Technology, Vol. 9, No. 30, August 2016, pp. 1-6. https://doi.org/10.17485/ijst/2016/v9i30/98730

[32] J. Aravindh, V. B. Srevarshan, R. Kishore, R. Amirthavalli "Home Automation in IOT using 6LoWPAN", International Journal of Advanced Computational Engineering and Networking, ISSN: 2320-2106, Vol. 5, Issue 5, July 2017, pp. 26-28.

[33] Snehal Deshmukh-Bhosale and Dr. S. S. Sonavane, "Implementation of 6LoWPAN Border Router (6BR) in Internet of Things", International Journal of Innovations & Advancement in Computer Science (IJIACS), ISSN 2347 – 8616, Vol. 7, Issue 3, March 2018, pp. 269-273. https://doi.org/10.1109/ICNETS2.2017.8067900

[34] A technical overview of LoRa and LoRaWAN Alliance Technical Marketing Workgroup, November 2015.

[35] Julio León, "A proposal for a Bluetooth Low Energy (BLE) autoconfigurable mesh network routing protocol based on proactive source routing", Thesis for: Ph.D., Advisor: Yuzo Iano, October 2016. . https://doi.org/10.13140/RG.2.2.16660.60803

[36] Dan Dragomir, Laura Gheorghe, Sergiu Costea and Alexandru Radovici, "A survey on secure communication protocols for iot systems", 2016 International Workshop on Secure Internet of Things of IEEE, 2016, pp. 47-62. https://doi.org/10.1109/SIoT.2016.8

[37] Minhaj Ahmad Khan and Khaled Salah, "IoT security: Review, blockchain solutions, and open challenges", Future Generation of computer system, Elsevier, 2018, pp.395-411. https://doi.org/10.1016/j.future.2017.11.022

[38] Abdulrahman BIN Rabiah, K. K. Ramakrishna, Elizabeth Liri and Koushik Kar "A Lightweight Authentication and Key Exchange Protocol for IoT", Workshop on Decentralized IoT Security and Standards (DISS), 18, San Diego, CA, USA, ISBN 1-891562-51-7, February 2018, pp.1-6. https://doi.org/10.14722/diss.2018.23004

[39] Makkad Asim, "A Survey on Application Layer Protocols for Internet of Things (IoT)", Vol. 8, No. 3, International Journal of Advanced Research in Computer Science

ISSN No. 0976-5697, March-April 2017 , pp. 996-1000. https://doi.org/10.26483/ijarcs.v8i3.3143

[40] Jasenka Dizdarevic, Francisco Carpio, Admela Jukan and Xavi Masip-Bruin, “A survey of communication protocols for Internet-of-Things and related challenges of fog and cloud computing integration”, ACM computing surveys, Vol.1, No.1, April 2018, pp. 1-27.

[41] Edited by Andrew Banks and Rahul Gupta, “MQTT Version 3.1.1. OASIS standard. Oct 29, 2014.

[42] Nishant M. Sonawala, Bharat Tank and Hardik Patel, “IoT Protocol based environmental data monitoring”, IEEE Proceedings International Conference on Computing Methodologies and Communication, 2017, pp.1041-1045.

[43] MQTT Essentials Part 1 to 9: Detail study on MQTT[Online] Available at: http://www.hivemq.com/blog/mqttessentials-part-6-mqtt-quality-of-service-levels, June 18, 2016

[44] OASIS, 29th October, 2012. Advanced Message Queuing Protocol 2012. Version 1.0 OASIS Standard. http://docs.oasis-open.org/amqp/core/v1.0/os/amqp-core-overview-v1.0-os.html

[45] Jorge E. Luzuriaga, Miguel Perez, Pablo Boronat, Juan Carlos Cano, Carlos Calafate and Pietro Manzoni, “Testing AMQP Protocol on Unstable and Mobile Networks”, International Conference on Internet and Distributed Computing Systems, Springer link, Sept. 2014, pp. 250-260. https://doi.org/10.1007/978-3-319-11692-1_22

[46] Nitin Naik, “Choice of Effective Messaging Protocols for IoT Systems: MQTT, CoAP, AMQP and HTTP”, IEEE International Systems Engineering Symposium (ISSE), 2017, pp.1-7, IEEE.

[47] Sneha Shailesh, Kiran Joshi and Kaustubh Purandare, “Performanc analysis of RabbitMQ as a message bus”, International journal of innovative research in computer and communication engineering (IJIRCCE), Vol. 6, Issue 1, January 2018, pp.242-246.

[48] Dobbelaere, Philippe and Kyumars Sheykh Esmaili. "Kafka versus RabbitMQ: A comparative study of two industry reference publish/subscribe implementations: Industry Paper" Proceedings of the 11th ACM International Conference on Distributed and Eventbased Systems. ACM, 2017. https://doi.org/ 10.1145/3093742.3093908

[49] Sye Loong Keoh, Sandeep S. Kumar, Hannes Tschofenig, “Securing the Internet of Things: A Standardization Perspective, Internet of Things Journal IEEE, Vol. 1, Issue 3, June 2014, pp. 265-275. https://doi.org/10.1109/JIOT.2014.2323395

[50] C.Bormann, S.Lemay, H.Tschofenig, K. Hartke, B.Silverajan, and B.Raymor, “CoAP(Constrained Application Protocol over TCP, TLS and Websockets. RFC8323.” RFC Editor, 2018. https://doi.org/10.17487/RFC8323

[51] P.Saint Andre, “Extensible Messaging and Presence Protocol (XMPP): Core RFC 3920.” RFC Editor, 2004.

[52] J.Ramirez and C.Pedraza, “Performance analysis of communication protocols for Internet of things platforms”, In 2017 IEEE Colombian Conference on Communications and Computing (COLCOM), 2017, pp. 1-7.