International Journal of Trendy Research in Engineering and Technology
Volume 4 Issue 4 August 2020
IJTRET
ISSN NO 2582-0958

COMPARATIVE STUDY BETWEEN VARIOUS PROTOCOLS USED IN INTERNET OF THINGS

C.Lakshmi, K.Elangovan, A.Rajiv, S.Vinothkumar,
Assistant Professors, Dept.of Electronics & Communication Engineering,
Sriram Engineering College, Chennai – 602024,Tamilnadu, India
lakshmic.ece@sriramec.edu.in

ABSTRACT

Internet Of Things(IoT) is emerging technology in future world.The term IoT comprises of Cloud computing, Data mining, Big data analytics, hardware board. The Security and Interoperability is a main factor that influences the IoT Enegy consumption is also main fator for IoT application designing.The various protocols such as MQTT,AMQP,XMPP are used in IoT.This paper analysis the various protocols used in Internet of Things.

Keywords-Internet of Things, MQTT,AMQP, XMPP, Security, Interoperability

I.INTRODUCTION

Internet of things (IoT) is a future tech trend that huge number of objects connected to the Internet worldwide. IoT is a system, combination of Embedded controllers, Sensors, Software and Network. In rapidly growing IoT application from personal electronics to Industrial Machines and Sensors are getting wirelessly connected to the Internet. Each device is assigned with a valid IP address IoT doesn't have standard architecture, because it varies from application to application

IoT can be used in internet or Intranet environment. Intranet environment the devices are connected with gateways by using Wi-Fi, Zigbee or Bluetooth. For remote access the devices are connected with gateway by using Internet.The data acuquired by the sensors are stored in the cloud for future reference. The application field of IoT includes Agriculture, Healthcare, Home automation, Industrial automation etc.,

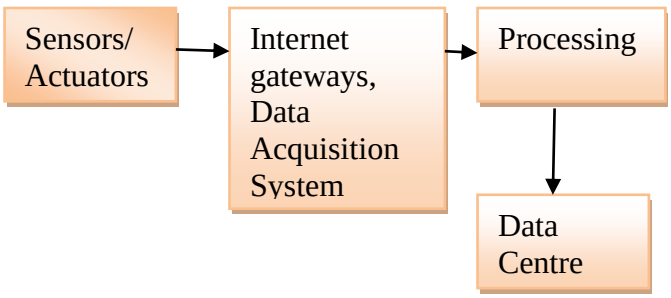

Figure 1:Basic Elements of Internet of Things

II.STAGES OF IoT ARCHITECTURE

There are four main stages in IoT

A. Sensors

Sensors collect data from the environment or object under measurement and turn it into useful data. Think of the specialized structures in your cell phone that detect the directional pull of gravity—and the phone's relative position to the "thing" we call the earth—and convert it into data that your phone can use to orient the device. Actuators can also intervene to change the physical conditions that generate the data. An actuator might, for example, shut off a power supply, adjust an air flow valve, or move a robotic gripper in an assembly process.

B. *Internet Gateway*

The data from the sensors starts in analog form. That data needs to be aggregated and converted into digital streams for further processing downstream. Data acquisition systems (DAS) perform these data aggregation and conversion functions. The DAS connects to the sensor network, aggregates outputs, and performs the analog-to-digital conversion. The Internet gateway receives the aggregated and digitized data and routes it over Wi-Fi, wired LANs, or the Internet systems for further processing.

C.Edge IT

Once IoT data has been digitized and aggregated, it's ready to cross into the realm of IT. However, the data

may require further processing before it enters the data center. This is where edge IT systems, which perform more analysis, come into play. Edge IT processing systems may be located in remote offices or other edge locations, but generally these sit in the facility or location where the sensors reside closer to the sensors, such as in a wiring closet.

D. Data Center

Data that needs more in-depth processing, and where feedback doesn't have to be immediate, gets forwarded to physical data center or cloud-based systems, where more powerful IT systems can analyze, manage, and securely store the data. It takes longer to get results when you wait until data reaches ,the data from sensor should be combined with data from other sources for deeper insights. In this stage processing may take place on-premises, in the cloud, or in a hybrid cloud system, but the type of processing executed in this stage remains the same, regardless of the platform.

III.OVERVIEW OF CONSTRAINT APPLICATION PROTOCOL

Internet of things (IoT) is an important part of a new generation of technology that every object no matter things or human could be connected to Internet. However, considering a lot of small devices are unable to communicate efficiently with constrained resources, Constrained Application Protocol (CoAP) is developed.

Figure 2:Typical COAP and HTTP protocol

In CoAP the UDP is used instead of TCP. The publisher Publish the data in terms of token and receiver read the data. CoAP is now becoming the standard protocol for IoT applications. Security is important to protect the communication between devices.

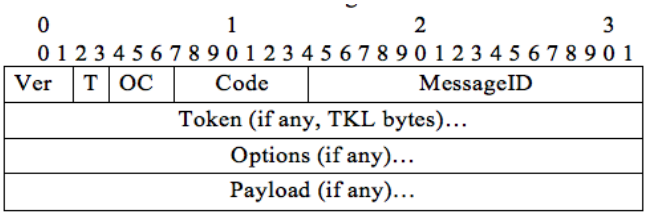

Figure 3: Message Format of CoAP

CoAP messages are 4 bytes header followed by options (Typically, 10-20 bytes header) and four message types Con_rmable [CON], Non-con_rmable [NON], Acknowledgments [ACK] , and Reset [RST] are used.

Four CoAP methods are used like HTTP.They are GET,POST, PUT and DELETE

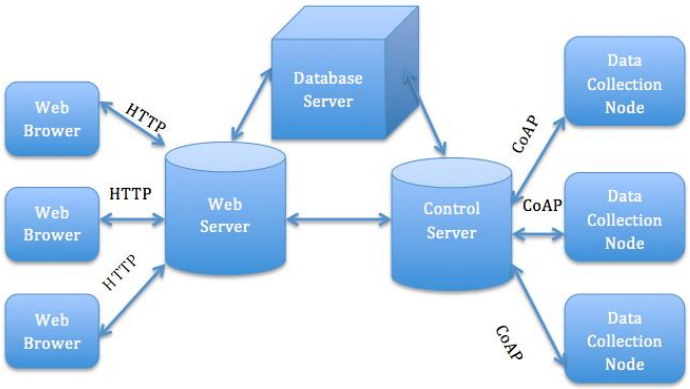

Figure 4:Energy Control System in CoAP

Typically, the 6LoWPAN network consists of one border router on multiple low-powered nodes. The nodes are connected to a cloud service for feeding in the sensor or control data. A border router is the coordinator of the 6LoWPAN network. It handles the translations between the 6LoWPAN and IPv6 networks.

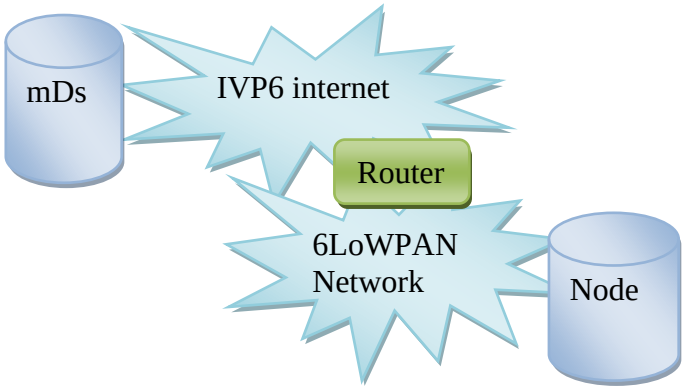

Figure 5: 6LoWPAN Network

IV.OVERVIEW OF VARIOUS PROTOCOL USED IN IoT

AMQP and MQTT are two protocols used in Internet of Things. In AMQP comprises an efficient wire protocol that separates the network transport from broker architectures and management. AMQP version 1.0 supports various broker architectures that may be use to receive, queue, route, and deliver messages or be used peer-to-peer.

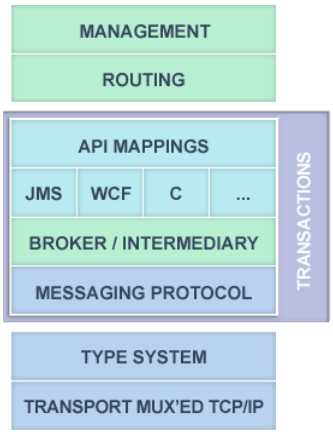

Figure 6:Architecture of AMQP protocol

AMQP and MQTT are open source protocols used for asynchronous message queuing protocol. MQTT is a machine-to-machine (M2M) or Internet of Things connectivity protocol for use on top of the TCP/IP protocol stack which was designed as an extremely lightweight broker based publish/subscribe messaging protocol for small code footprints, low bandwidth and power, high-cost connections and latency, variable availability, and negotiated delivery guarantees. In the hub and spoke model of Message Oriented Middleware messaging server forwards messages from sensor devices to monitor devices. In such architecture, a sensor device whose main task is to continuously produce and send data to server is defined as publisher. Central server, an MQTT broker, collects messages from publishers and examines to whom the message needs to be send.

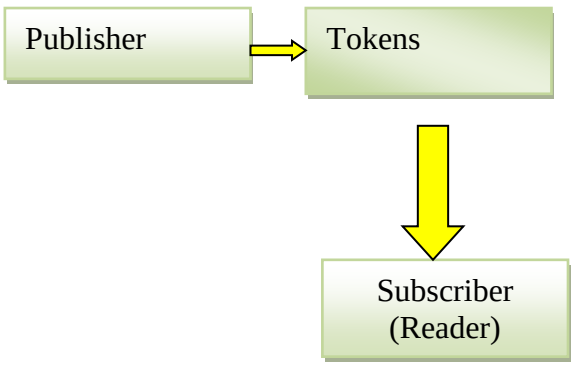

Figure 7: Architecture of MQTT Protocol

MQTT broker is central device that is responsible for communication between MQTT client and server. The various sensors that are connected to the gateway, accuracy is a major factor. In agriculture the soil moisture , Temperature, Humidity sensors are used

V. SECURITY CHALLENGES AND REQUIREMENTS IN IOT APPLICATIONS

Security issues in IoT is discussed following

Denial-of-Service: Apart from conventional denial-of service (DoS) attacks like exhausting resources and bandwidth, IoT can be susceptible to attacks on communication infrastructure like channel jamming. Adversaries who are privileged insiders can gain control of the relevant infrastructure to cause more chaos in the network.

Controlling: Active attackers can gain partial or full control of IoT entities and the extent of damage that can be caused is based on the following:

- Services being provided by the entity.
- Relevance of the data being managed by that entity

Eavesdropping: This is a passive attack through which information can be gathered from channel communication. A malicious insider attacker can also gain more advantage by capturing infrastructure or entities.

Physical damage: The easy accessibility of IoT entities and applications can be exploited by attackers to cause physical harm hindering services by attacking an entity or the hardware of the module creating it virtually. Attackers lacking technical knowledge and wanting to cause considerable damage can utilize this.

Node capture: Easy accessibility can also be a vulnerability for information extraction through capturing entities and trying to extract stored data. This is a major threat against data processing and storage entities.

V.CONCLUSION

Implementing IoT testbed comprising heterogeneous legacy and possible new types of devices Support IoT experiments to benefit academic and research community in improving the knowledge of IoT hardware and software infrastructure Semantic technologies. While designing of IOT the designer concentrate on energy efficient and Interoperability of the system. Because the existing node should detect the new node. So the designer should select the proper protocol among various protocols based on the application concern.

VI.FUTURE ENHANCEMENT

The IoT is still a emerging field. The smart cities uses more number sensors. The system should be constructed to enhance the performance of existing system. The IoT application to be selected for the benefit of the society

REFERENCES

[1]. K. Grgić, I. Špeh and I. Heđi, "A web-based IoT solution for monitoring data using MQTT protocol," *2016 International Conference on Smart Systems and Technologies (SST)*, Osijek, 2016, pp. 249-253.

[2]. V. L. Shivraj, M. A. Rajan, M. Singh and P. Balamuralidhar, "One time password authentication scheme based on elliptic curves for Internet of Things (IoT)," *2015 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW)*, Riyadh, 2015, pp. 1-6.

[3] Langmann R., Meyer L., "Architecture of a Weboriented Automation System", IEEE 18th Conference on Emerging Technologies for Factory Automation (ETFA), pp. 1–8, 2013.

[4]. D. Evans, "The internet of things – how the next evolution of the internet is changing everything," white paper, April 2011

[5].CoAP Reference: http://www.cse.wustl.edu

[6].HiveMQ Enterprise MQTT Broker : http://www.hivemq.com/.

[7] V. Karagiannis, P. Chatzimisios, F. Vazquez-Gallego, and J. Alonso-Zarate, "A survey on application layer protocols for the internet of things," Transaction on IoT and Cloud Computing, vol 1., January 2015.

[8] K. Tang et al., "Design and implementation of push notification system based on the MQTT protocol," in International Conference on Information Science and Computer Applications, September 2013.

[9] S.K. Shriramoju, J. Madiraju, and A.R. Babu, "An approach towards publish/subscribe system for wireless networks," International Journal of Computer and Electronics Research, vol. 2., pp. 505-508, August 2013.

[10] E.G. Davis, A. Calaveras, and I. Demirkol, "Improving packet delivery performance of publish/subscribe protocols in wireless sensor networks," Sensors, 2013.

[11]. S. Patinge, Y. Suryawanshi and S. Kakde, "Design of ARM based data acquisition & control using GSM & TCP/IP network," Computational Intelligence and Computing Research (ICCIC), 2013 IEEE International Conference on, Enathi, 2013, pp. 1-4.

[8]. AMQP Reference:https://www.amqp.org

[9]. 6LoWPAN Reference :https://docs.mbed.com

[10]. S. Challa; M. Wazid; A. K. Das; N. Kumar; A. Goutham Reddy; E. J. Yoon; K. Y. Yoo, "Secure Signature-Based Authenticated Key Establishment Scheme for Future IoT Applications," in *IEEE Access* , vol.PP, no.99, pp.1-1