

# Analysis of Dynamic Topology Wireless Sensor Networks for the Internet of Things (IOT)

R.Praveen Kumar

*Department of Electronics and Communication Engineering  
Easwari Engineering College, Chennai, Tamilnadu, India*

Dr.S.Smays

*Department of Electronics and Communication Engineering  
RVS Technical Campus, Coimbatore, Tamilnadu, India*

**Abstract - This paper provides an overview of the Internet of Things (IoT) with emphasis on enabling Architecture, protocols, and application issues. The IoT is enabled by the latest developments in RFID, smart sensors, communication technologies, and Internet protocols. The basic premise is to have smart sensors collaborate directly without human involvement to deliver a new class of applications. The current revolution in Internet, mobile, and machine-to-machine (M2M) technologies can be seen as the first phase of the IoT. In the coming years, the IoT is expected to bridge diverse technologies to enable new applications by connecting physical objects together in support of intelligent decision making. This paper starts by providing a horizontal overview of the IoT. Then, we give an overview of some technical details that pertain to the IoT enabling protocols, and applications.**

**Keywords: Internet of Things (IoT), MQTT, CoAP, XMPP, IoT Gateway**

## I. INTRODUCTION

Though quickly advancing technologies, society is stirring toward an always connected model. Wired and wireless networks are ubiquitous; open standards are defined and allowed for particularly addressing procedure. Concepts associated with the Future Internet are being researched [1], developed and continuously adapted to daily life. One new concept associated with the "Future Internet" is called "Internet of Things" (IoT). The IoT turns into a vision where real-world objects are part of the internet: every object is exclusively identified and accessible to the network, its position, and status is known, where numerous services and intelligence are added to expand the Internet effectively, seamlessly combining between the digital and physical world, ultimately affecting on personal and social environment. This paper presents an overview of the Internet of Things, general architecture, and protocols, applications, future trends. It is positioned as an introductory paper beneficial to a wide audience ranging such as networks researchers, consultants, and pronouncement makers in the business firm and so on.

## II. EVOLUTION OF INTERNET OF THINGS

The Internet of Things (IoT) is generally thought of as networking things to the Internet and using that connection to provide some kind of useful remote monitoring or control of those things. This definition of IoT is limited and references only part of the IoT evolution. It is basically a reshaping of the existing Machine to Machine (M2M) market of today.

In the 1990s, Internet connectivity began to boom in enterprise and consumer markets but was still limited in its use because of the low performance of the network interconnect. In the 2000s, Internet connectivity became the norm for many applications and today is expected as part of many enterprises, industrial and consumer products to provide access to information. However, these devices are still primarily things on the Internet that require more human interaction and monitoring through apps and interfaces. The true promise of the IoT is just starting to be realized – when imperceptible technology operates behind the scenes dynamically responding to how we want “things” to act. To date, the world has deployed about 5 billion “smart” connected things. Predictions say there will be 50 billion connected devices by 2020 and in our lifetime, we will experience life with a trillion-node network. Those are really big numbers. How things are fundamentally deployed today is a barrier to realizing those numbers. The industry will only achieve the reality of 50 billion connected devices by simplifying how things connect and communicate today.



Figure 1: Evolution of IoT

The Internet of Things (IoT) completely transforms connectivity from "any-time, any-where" for "any-one" into "any-time, any-where" for "any-thing". The IoT is able to connect real world elements and entrenches the intellectual in a communication system for smart process its specific information and autonomous decision. Hence, IoT is a key enabling the different types of beneficial applications and services which can sustain our economies, transportation, environment and health that we never expected before.

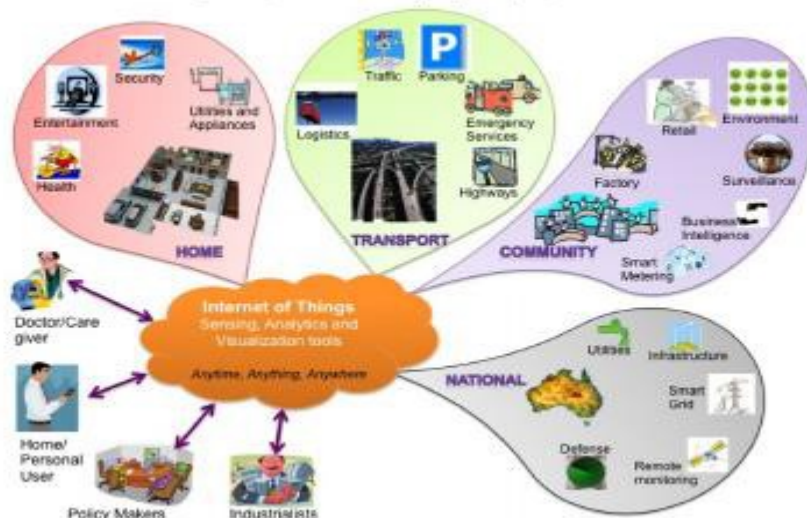


Figure 2: Overview of IoT

### III. IoT ARCHITECTURE

The TCP/IP protocol stack plays a key role in digital communication which was defined long time ago. Nevertheless, the IoT may connect a vast number of objects which will create an immense traffic, and a tremendous amount of data capacity is needed. Moreover, IoT will face numerous challenges especially privacy and security issues [2]. Therefore, the new standard architecture and protocols for IoT desire to address many crucial factors (i.e., reliability, Quality of Service, confidentiality, integrity, etc.). Due to the IoT procedures are mainly to connect with everything and everyone to exchange information with each other that not only exponentially increasing the network traffic but also storage capacity as well. Thus, IoT improvement relies on the developments in technology and applies to different types of useful applications.

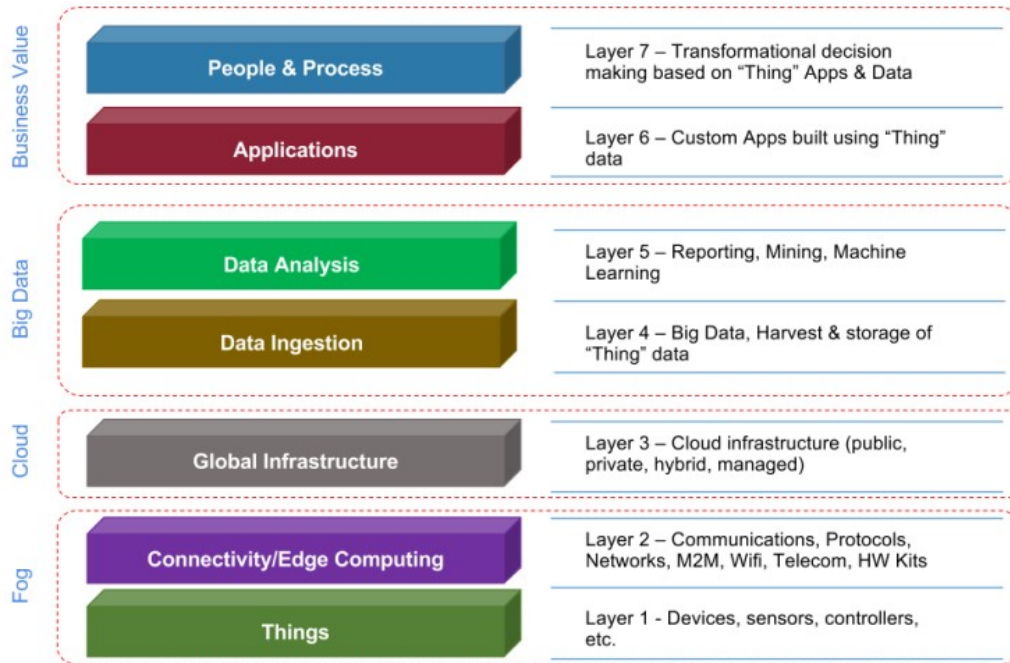


Figure 3: IoT Reference layer Architecture

*Perception Layer (Layer 1) :*

The perception layer is similar to a physical layer in OST model which consists of the different types of sensor (i.e. RFTD, Zigbee, QR code, Infrared, etc.) devices and environmental elements. This layer generally manages with the overall device management viz; identification and collection of specific information by each type of sensor devices. The gathered information can be location, wind speed, vibration, pH level, humidity, the amount of dust in the air, etc. This gathered information transmits through the Network layer for its secure communication toward central information processing system.

*Network Layer (Layer 2 & 3):*

The Networks layer plays an important role in secure transfers and keeps the sensitive information confidential from sensor devices to the central information processing system through 3G,4G, UMTS, WiFi, WiMAX, RFTD, Infrared, Satellite, etc. dependent upon the type of sensors devices. Hence, this layer is mainly responsible for transfer the information from Perception layer to upper layer.

*Middleware Layer (Layer 4 & 5):*

The devices in the IoT system may generate various type of services when they are connected and communicated with others. Middleware layer has two essential functions, including service management and stores the lower layer information into the database. Moreover, this layer has the capability to retrieve, process, compute information, and then automatically decide based on the computational results.

*Application Layer (Layer 6):*

The application layer is responsible for inclusive applications management based on the processed information in the Middleware layer. The IoT applications can be smart postal, smart car, smart glasses, smart home, smart independent living, smart transportation, etc.

*Business Layer (Layer 7):*

The layer 7 functions cover the whole IoT applications and services management. It can create practically graphs, business models, flow chart, executive report, etc. based on the amount of precise data received from lower layer and actual data analysis process. Based on the proper analysis results, it will help the functional managers or executives to make more accurate decisions about the business strategies.

#### IV. IOT PROTOCOLS

The protocol is the special set of rules and regulations that end point in a telecommunication connection use when they need to communicate to another end point which connected to the same/different network. In this subsection will briefly describe the most frequently used protocols for Machine-to-Machine (M2M) communication.

##### 1.1 Application Protocols:

MQTT (Message Queue Telemetry Transport): MQTT is a Client Server publishes or contributes messaging transport protocol. It is simple and designed so as to be easy to implement. The protocol runs over TCP/IP or over other network protocol that provided ordered, lossless, bi-directional connections. The MQTT [15] features include: use of the publish/subscribe message pattern which provides one-to-many message distribution, a messaging transport that is doubting to the content of the payload, and this protocol also has three qualities of service for message delivery viz; "At most once", where messages are delivered according to the best efforts of operating environment. The message loss can occur, and this level could be used, secondly, "At least once", where message are assured to arrive but duplicate messages can occur. Finally, "Exactly once", where message are assured to arrive exactly once. This level could be used [5]. This that cause to drastically reduce network traffic. Furthermore, the MQTT protocol is not only minimized transport overhead and protocol exchange to reduce network traffic but also has an extraordinary mechanism to alert interested parties when an abnormal disconnection occurs as well.

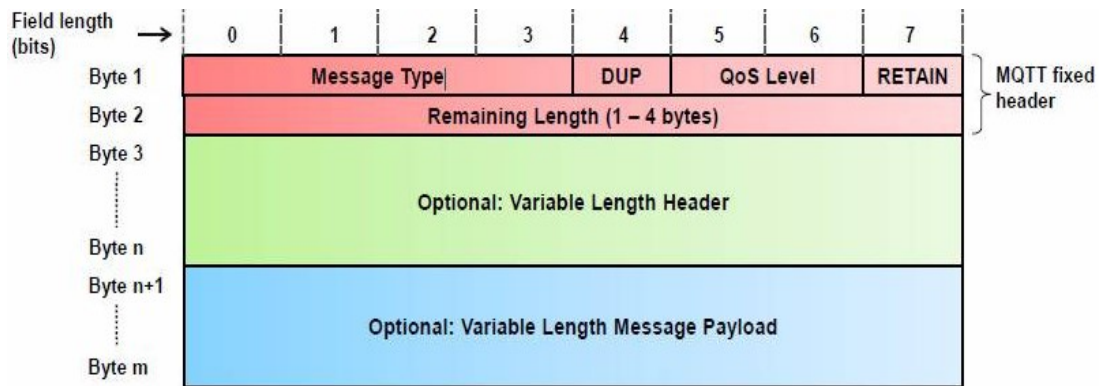


Figure 4: MQTT Message Format

CoAP (Constraint Application Protocol): CoAP is a specialized web transfer protocol for use with constrained nodes and constrained networks (e.g. low-power, lossy). The nodes often have an 8-bit microcontroller with small amounts of ROM and RAM, while constrained network often have a high packet error rate and typical throughput is 10 kbps [6]. This protocol designed for Machine-to-Machine (M2M) [3] application such as smart city and building automation. CoAP provides a demand and reply interaction model between application endpoints, support built-in discovery services and resources, and includes key concepts of the Web such as URIs and Internet media types. CoAP is designed to friendly interface with HTTP for integration with the Web while meeting specialized requirements such as multicast support, very low overhead and simplicity for constrained environments.

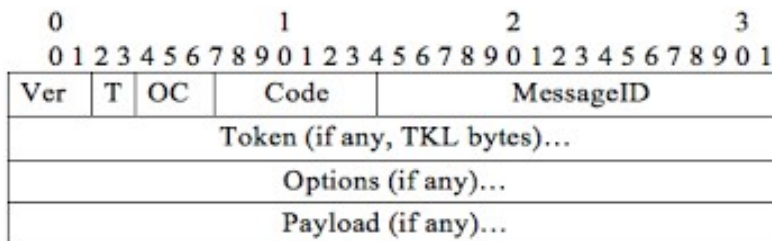


Figure 5: CoAP Message Format

Extensible Messaging and Presence Protocol (XMPP): XMPP is an IETF instant messaging (IM) standard that is used for multi-party chatting, voice and video calling, and telepresence. XMPP was developed by the Jabber open-source community to support an open, secure, spam free and dispersed messaging protocol. XMPP allows users to communicate with each other by sending instant messages on the Internet no matter which operating system they are using.

XMPP allows IM applications to achieve validation, access control, privacy measurement, hop-by-hop and end-to-end encryption, and compatibility with other protocols. Fig.6 shows the overall behavior of XMPP [7] protocol, in which gateways can bridge between foreign messaging networks. Many XMPP features make it an ideal protocol by most IM applications and relevant within the scope of the IoT. It runs on a variety of Internet-based platforms in a distributed fashion. XMPP is secure and allows for the addition of new applications on top of the core protocols. XMPP connects a client to a server using a stream of XML [7] sections. An XML section represents a piece of code that is divided into three components: message, presence, and (info/query). Message sections identify the source (from) and destination (to) addresses, types, and IDs of XMPP entities that utilize a push method to retrieve data. A message stanza fills the subject and body fields with the message title and contents. The presence section shows and notifies customers of status updates as authorized.

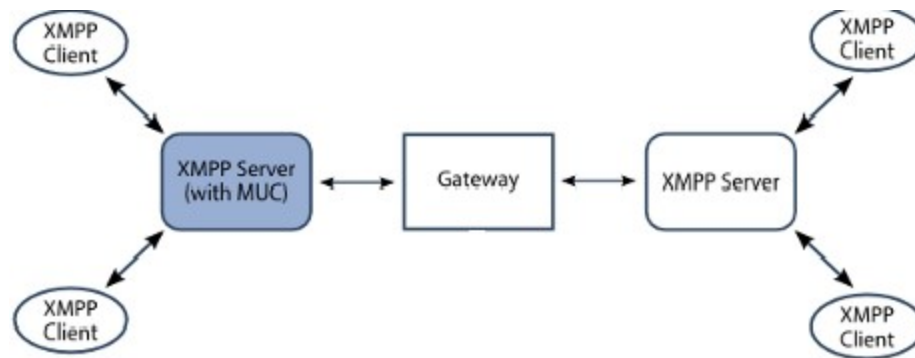


Figure 6: XMPP Operation

### 1.1 Infrastructure Protocols:

- 1) Routing Protocol for Low Power and Lossy Networks (RPL): The IETF routing over low-power and lossy links (ROLL) working group standardized a link-independent routing protocol based on IPv6 for resource-constrained nodes called RPL [16] [17]. RPL was created to support minimal routing requirements through building a robust topology over lossy links. This routing protocol supports simple and complex traffic models like multipoint-to-point, point-to-multipoint and point-to-point.
- 2) 6LoWPAN: Low power Wireless Personal Area Networks (WPANs) which many IoT communications may trust on have some special characteristics different from former link layer technologies like limited packet size (e.g., maximum 127 bytes for IEEE 802.15.4), various address lengths, and low bandwidth. So, there was a need to make an adaptation layer that turns IPv6 packets to the IEEE 802.15.4 specifications. The IETF 6LoWPAN[18] working group developed such a standard in 2007. 6LoWPAN is the specification of mapping services required by the IPv6 over Low power WPANs to maintain an IPv6 network. The standard provides header compression to reduce the transmission overhead, fragmentation to meet the IPv6 Maximum Transmission Unit (MTU) requirement, and forwarding to link-layer to support multi-hop delivery.

6LoWPAN removes a lot of IPv6 overheads in such a way that a small IPv6 datagram can be sent over a single IEEE 802.15.4 hop in the best case. It can also compress IPv6 headers to two bytes.

## V. APPLICATION OF INTERNET OF THINGS

According to a survey done by the IoT-I project in 2010 [8] indicated IoTs situation applications could be grouped in 14 domain viz; Transportation, Smart home, Smart city, Lifestyle, Retail, Agriculture, Smart factory,



Supply chain, Emergency, User Interaction, Healthcare, Culture and tourism, Environment, and Energy. This survey was based on 270 responses from 31 countries demonstrated the most exciting circumstance applications were: smart home, smart city, transportation, and healthcare.

#### 5.1 Mobile ticketing

Electronic posters or billboards providing information in favor to transportation services can be equipped with the NFC tag. The user can get information from the web by either soaring their mobile phone over the NFC tag or pointing the mobile phone to the visual markers [11] [12]. The mobile phone automatically retrieves and combines information from the web related services (stations, the number of passengers, costs, available seats, departure and arrival time, and type of services) and provides the idea about tickets which suitable for each user.

#### 5.2 Assisted driving

Today's different type of transportation such as cars, train and buses along with the road and the rails furnished with sensors, actuators and powerful processors may provide beneficial information to the driver and/or passengers (i.e. accidents, temporary and/or permanent road closures, traffic congestions) to provide better navigation and safety [11]. The numerous profit and non-profit organizations would benefit from gathered road traffic patterns information such as administrative authorities used for construction/planning purpose, freight companies used this information to perform more route optimization which allows energy saving, and so on.

#### 5.3 Thefts

Application informs the user to know if precious objects are moved from a restricted area, which indicates that the object is being stolen [11]. In this case, the event has to be notified quickly to the owner and/or security guards through SMS, call, e-mail, etc.

#### 5.4 Identification and Authentication

Identification and authentication are two relations that described the initial phases of the security process in computer systems which could apply to health care, for instance, patient identification to reduce injurious incidents to the patient, current electronic medical record protection and child identification in hospitals to prevent mismatching. An identification and authentication procedure is most frequently used to manage.

#### 5.4 Sensing

Sensor device enables multifunction focused on both in-patient and out-patients treatment and particularly on diagnosing patient conditions providing real-time information on patient health indicators. Various wireless access-based remote patient monitoring system can be deployed to reach the patient everywhere with multiple wireless technologies integrated to support continuous bio-signal monitoring in presence of patient mobility [11, 12]

## VI. CONCLUSION

The Internet of Things, things which can communicate with each other via Internet, access data on the Internet, store and recover data, and interact with users. This paper describes the evolution and how important of IoT, the general architecture, its most widely used protocols, ample possible applications, future trends and how to implementation IoT by using MQTT Protocol. Based on a lightweight and fast communication protocol designed for IoT, there is trade off with the security and permission policy that should be discussed in protocol development in a future.

## REFERENCES

- [1] L. Coetzee, J. Eksteen. The Internet of Things – Promise for the Future? An Introduction. 1ST-Africa 2011 Conference Proceedings (CSIR). 2011.
- [2] N. Tan, N. Wang. Future Internet: The Internet of Things. 3<sup>rd</sup> International Conference on Advanced Computer Theory and Engineering (ICACTE). 2010.
- [3] C. Birmann, A. P. Castellani, Z. Shelby. CoAP: An Application Protocol for Billions of Tiny Internet Nodes. IEEE Internet Computing. 2012.

- [4] K. Bing, L. Fu, Y. Zhao, L. Yanlei. Design of an Internet of Things-based Smart Home System. 2nd International Conference on Intelligent Control and Information Processing. 2011: 921-924.
- [5] P. Saint-Andre, "Extensible messaging and presence protocol (XMPP): Core," Internet Eng. Task Force (IETF), Fremont, CA, USA, Request for Comments: 6120, 2011.
- [6] M.Palattell, N. Accettura, X. Vilajonasa, T.Watteyne, L. Grieco, G.Boggia and M.Dolher. "Standardized Protocol stack for the internet of (important) things. IEEE Communication Surveys & Tutorials. 2013: 1389-1430.
- [7] M. Laine and K. Säilä, "Performance evaluation of XMPP on the Web," Aalto Univ. Tech. Rep., Aalto, Finland, 2012.
- [8] J. A. Stankovic, "Research directions for the Internet of Things," IEEE Internet Things J., vol. 1, no. 1, pp. 3-9, Feb. 2014.
- [9] Luca Mainetti, Luigi Patrono, and Antonio Vilei, "Evolution of Wireless Sensor Networks towards the Internet of Things: a Survey",
- [10] S. M. Riazul Islam, Daehan Kwak, Md. Humaun Kabir, Mahmud Hossain, And Kyung-Sup Kwak, "The Internet of Things for Health Care: A Comprehensive Survey", IEEE Access vol. 3, 2015
- [11] Andrea Zanella, Lorenzo Vangelista, "Internet of Things for Smart Cities", IEEE Internet of Things Journal, Vol. 1, No. 1, February 2014.
- [12] Jorge Granjal, Edmundo Monteiro, and Jorge Sá Silva, " Security for the Internet of Things: A survey of Existing Protocols and Open Research Issues", IEEE Communication Surveys & Tutorials, Vol. 17, No. 3, Third Quarter 2015.
- [13] Alexander Gluhak, Srdjan Krco Michele Nati, Dennis Pfisterer Nathalie Mitton and Tahiry Razafindralambo, "A Survey of Facilities for Experimental Internet of Things Research", IEEE Communication Magazine, Nov 2011
- [14] Chonggang Wang, Kazem Sohraby, Bo Li, Mahmoud Daneshmand and Yueming Hu, "A Survey of Transport Protocols for Wireless Sensor Networks", IEEE Network, May 2006.
- [15] D. Locke, "MQ telemetry transport (MQTT) v3. 1 protocol specification," IBM developerWorks, Markham, ON, Canada, Tech. Lib., 2010. [Online]. Available: <http://www.ibm.com/developerworks/webservices/library/ws-mqtt/index.html>
- [16] Sharief M. A. Oteafy, Fadi M. Al-Turjman and Hossam S. Hassanein, "Pruned Adaptive Routing in the Heterogeneous Internet of Things", Globecom 2012- Ad-hoc and Sensor Networking.
- [17] T. Winter et al., "RPL: IPv6 routing protocol for low power and lossy networks," Internet Eng. Task Force (IETF). Fremont, CA, USA.
- [18] S. Raza, S. Duquenois, J. Höglund, U. Roedig, and T. Voigt, "Secure communication for the Internet of Things—A comparison of link-layer security and IPsec for 6LoWPAN," Security Commun. Netw., vol. 7, no. 12, pp. 2654–2668, Dec. 2012.