UGC Approved Journal

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified

Vol. 4, Issue 7, July 2017

Internet of Things – A Big Challenge in getting the Right Protocol

Ch. V. Raghavendran[1], G. Naga Satish[2], P. Suresh Varma[3]

Professor, Holy Mary Institute of Technology & Science, Bogaram, Telangana, India[1]

Associate Professor, BVRIT Hyderabad College of Engineering for Women, Hyderabad, India[2]

Professor, College of Engineering, Adikavi Nannaya University, Rajamahendravaram, India[3]

Abstract: Internet of Things (IOT) is an ambitious paradigm which significantly increases the scale of connected devices from personal electronics to industrial machines and sensors which are wirelessly connected to the Internet. In order to manage the complexity of such a scale, interworking solutions that can reuse pre-existing technologies seamlessly with newer and more efficient technologies is a requirement. Covering a wide variety of use cases, in various environments and serving diverse requirements, no single wireless standard can adequately exist. A number of different standardization bodies and groups are actively working on creating more inter-operable protocol stacks and open standards for the Internet of Things. With numerous standards deployed in the market, spreading over multiple frequency bands and using different communication protocols, choosing the right wireless connectivity technology for an IoT application can be relatively challenging. Ongoing standardization efforts towards harmonizing internet protocols for wireless sensor networks-based internet of things have raised hopes of global interoperable solutions at the transport layer and below. In this paper we review the predominant wireless connectivity technologies in the market, discuss their key technical concepts present guidelines for selection of the right wireless technology for different applications.

Keywords: Internet of Things, IoT, Smart devices, Protocols, Communication.

I. INTRODUCTION

The Internet of Things (IoT) paradigm has gained popularity in recent years. At a conceptual level, IoT refers to the inter connectivity among our everyday devices, along with device autonomy, sensing capability, and contextual awareness. IoT devices include personal computers, laptops, tablets, smart phones, PDAs, and other hand-held embedded devices. Devices now communicate smartly to each other or to us. Connected devices equipped with sensors and/or actuators recognize their surroundings, understand what is going on and act accordingly [1] [2]. This technology takes advantage of advancements in computing power, electronics miniaturization, and network interconnections to offer new capabilities not previously possible. A large number of conferences, reports, and news articles discuss and debate the potential impact of the "IoT revolution"—from new market opportunities and business models to concerns about security, privacy, and technical interoperability.

The Internet of Things is an emerging topic of technical, social, and economic significance. Consumer products, durable goods, cars and trucks, industrial and utility components, sensors, and other everyday objects are being combined with Internet connectivity and powerful data analytic capabilities that promise to transform the way we work, live, and play. Projections for the impact of IoT on the Internet and economy are impressive, with some anticipating as many as 100 billion connected IoT devices and a global economic impact of more than $11 trillion by 2025.

IoT has been defined from various different perspectives and hence numerous definitions for IoT exist in the literature. The Internet Architecture Board (IAB) [3] defined IoT in "Architectural Considerations in Smart Object Networking" as – The term "Internet of Things" (IoT) denotes a trend where a large number of embedded devices employ communication services offered by the Internet protocols. Many of these devices, often called "smart objects," are not directly operated by humans, but exist as components in buildings or vehicles, or are spread out in the environment". The RFID group defines Internet of Things as – "The worldwide network of inter-connected objects uniquely addressable based on standard communication protocols". According to Wikipedia – "The Internet of Things, also called The Internet of Objects, refers to a wireless network between objects; usually the network will be wireless and self-configuring, such as household appliances".

All of the definitions describe scenarios in which network connectivity and computing capability extends to a group of objects, devices, sensors, and everyday items that are not ordinarily considered to be "computers"; this allows the devices to generate, exchange, and consume data, often with minimal human intervention. The various definitions of IoT do not necessarily disagree – rather they emphasize different aspects of the IoT phenomenon from different focal points and use cases.

UGC Approved Journal

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified

Vol. 4, Issue 7, July 2017

In 2012, an estimated 8.7 billion "things" were connected worldwide, and projections show that this could grow to 50 billion devices around the world will be connected to the Internet by the year 2020 – generating global revenues of $8.9 trillion in the process. A third of them will be computers, smart phones, tablets and TVs… The remaining two-thirds will be other kinds of things: sensors, actuators, and newly invented intelligent devices that monitor, control, analyze, and optimize our world [4]. According to a new International Data Corporation (IDC) Spending Guide, worldwide spending on the Internet of Things (IoT) will grow at a 17.0% Compound Annual Growth Rate (CAGR) from $698.6 billion in 2015 to nearly $1.3 trillion in 2019 [5].

The Internet of Things (IoT) forms a dynamic global network infrastructure with self configuring capabilities, based on standard and interoperable communication protocols [6]. It represents the interconnection of numerous things—smart devices and services. IoT is an integrated part of future Internet including existing and evolving Internet and network developments and could be conceptually defined as a dynamic global network infrastructure with self configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes, and virtual personalities, use intelligent interfaces, and are seamlessly integrated into the information network.

II. INTERNET OF THINGS: PROPERTIES, CLASSES AND VISION

A. IoT Properties

In contrast to traditional IT systems such as enterprise applications, cloud computing, and big data, a combination of a number of properties makes the IoT unique in terms of the challenges that need to be deal with. By analyzing related IoT research [7]–[17] four distinguishing properties can be identified. These properties are: the uncontrolled environment, the heterogeneity, the need for scalability, as well as the constrained resources utilized in the IoT.

1) Uncontrolled environment: Many things will be part of a highly uncontrolled environment; things travel to untrustworthy surroundings, possibly without supervision. Properties of the uncontrolled environment are: mobility, physical accessibility, and the lack of trust.

- Mobility: Stable network connectivity and constant presence cannot be expected.
- Physical accessibility: Sensors can be publicly accessible, e.g., traffic control cameras, and environmental sensors.
- Trust: A priori trusted relationships are unlikely for the large amount of devices interacting with each other and users [16].

2) Heterogeneity: IoT is expected to be a highly heterogeneous ecosystem as it will have to integrate a multitude of things from various manufacturers. Therefore, version compatibility, and interoperability have to be considered.

3) Scalability: The vast amount of interconnected things in the IoT demands highly scalable protocols.

4) Constrained resources: Things in the IoT will have constraints that need to be considered for security mechanisms. This includes energy limitations, e.g., battery powered devices, as well as low computation power, e.g., micro sensors. Thus, heavy computational cryptographic algorithms cannot be applied to all things.

B. Classes of IoT devices

IoT devices can be classified based on the type of data handled. It is useful to view the requirements for IoT devices in this way as a way of determining the device requirements from a power, connectivity and security perspective. We can classify the devices as follows:

- Machine to machine data
- Audio
- Audio/video

Table 1 shows the requirements of the IoT devices and is for illustrative purposes and specific IoT device, requirements may vary.

C. Vision

The Internet of Things could allow people and things to be connected Anytime, Anyplace, with Anything and Anyone, ideally using Any path/network and Any service. This is stated as well in the ITU vision of the IoT, according to which: "From anytime, anyplace connectivity for anyone, we will now have connectivity for anything" [18]. The vision of what exactly the Internet of Things will be, and what will be its final architecture, are still diverging.

The vision of Future Internet based on standard communication protocols considers the merging of computer networks, Internet of Things (IoT), Internet of People (IoP), Internet of Energy (IoE), Internet of Media (IoM), and Internet of Services (IoS), into a common global IT platform of seamless networks and networked "smart things/objects". A vision of an IoT built by smart objects, able to sense, interprets, and react to external events is proposed in [19]. Within this

UGC Approved Journal

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified

Vol. 4, Issue 7, July 2017

vision, by capturing and interpreting user actions, smart items will be able to recognize and initiate their environment, to analyze their observations and to communicate with other objects and the Internet. This new Internet will co-exist and be closely bound up with the Internet of information and services [20].

In the vision of the IoT European Research Cluster (IERC), Ubiquitous/pervasive computing, The Internet Protocol, Communication technologies, Embedded devices and Applications are part of Internet of Things and are enablers of implementing the concept of Internet of Things in different applications. The IERC strategic research agenda is addressing these challenges, considering and integrating the different point of views and differentiating between the Internet of Things from the other concepts and trying to identify the research needs for the implementation and deployment of IoT applications. The interface between the real and digital worlds requires the capacity for the digital world to sense the real world and act on it. This implies the convergence of at least three domains: Technologies (nano-electronics, sensors, actuators, embedded systems, cloud computing etc.), Communication and Intelligence [21].

Table 1. IoT device classification

	IoT (M2M data)	IoT (Audio)	IoT (Video and imaging)
Device example	Personal health Sensor hubs Smart home Energy management	Wireless audio	Chromecast Connected camera Video analytics Ray tracing enabled imaging
CPU type/ performance	M51xx/50 MIPS	M51xx/300 – 500 MIPS I6400/500 – 800 MIPS	MIPS I6400/P5600 2000 – 5000 MIPS; GPU
OS requirement	RTOS or No OS	Linux/Android or RTOS	Linux/Android
Power requirements	30 days on 700 mA-hr battery	1 day at 1000 mA-hr	Line powered by USB or line
Connectivity	BTLE and low power Wi-Fi 802.11n/BT/BTLE Later – 802.11ah	Low power 802.11n/BT/ BTLE	802.11ac
Semicon process	40 nm	40 nm/28 nm	28 nm/16 ff
Differentiators	Data security Low power Integrated connectivity Cloud ready	Data security Secure update Digital Rights Management Integrated connectivity Cloud ready	Data security Secure update Digital Rights Management Integrated connectivity Cloud ready

III. MOTIVATION OR BACKGROUND OR RELATED WORK

A Protocol Stack

Communication systems operate on a set of rules and standards to format data and control data exchange. Open Systems Interconnection (OSI) is a reference model for how applications can communicate over a network. A reference model is a conceptual framework for understanding relationships. The purpose of the OSI reference model is to guide vendors and developers so that the digital communication products and software programs they create will interoperate, and to facilitate clear comparisons among communications tools. OSI was officially adopted as an international standard by the International Organization of Standards (ISO).

The concept of OSI is that the process of communication between two endpoints in a tele-communication network can be divided into seven distinct groups of related functions, or layers. In a given message between users, there will be a flow of data down through the layers in the source computer, across the network and then up through the layers in the receiving computer. The seven layers of function are provided by a combination of applications, operating systems, network card, device drivers and networking hardware that enable a system to put a signal on a network cable or out over Wi-Fi or other wireless protocol. The TCP/IP reference model is the network model used in the current Internet architecture [22]. The reference model was named after two of its main protocols, TCP (Transmission Control Protocol) [23] and IP (Internet Protocol). Its simplicity and power has led to its becoming the single network protocol of choice in the world today. TCP/IP is a set of protocols developed to allow cooperating computers to share resources across the network. A 4-layer simplified version of the OSI model for TCP/IP protocol is shown in Fig 1.

UGC Approved Journal

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified

Vol. 4, Issue 7, July 2017

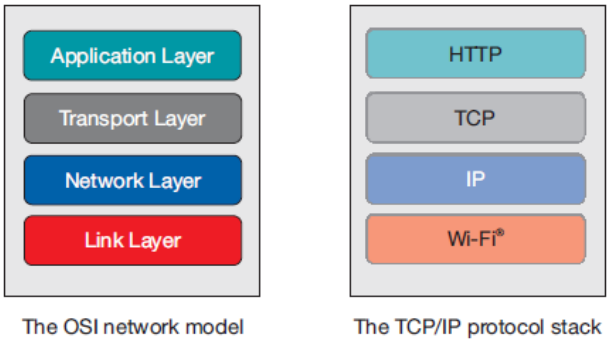

Fig 1. Simplified OSI model and TCP/IP protocol stack

Software developers face a wide range of protocol choices in creating applications for the Internet of Things (IoT). These applications need to be able to consume information from a large number of devices. The choice of protocol depends on the use case and where the application will be staged in the software environment.

The IoT is all about connecting things to the Internet. Devices that are (directly) connected to the Internet must use the IP suite to be able to exchange data with devices and servers over the Internet. Nevertheless, devices in a local network can use non-IP protocols to communicate within the local network. Connectivity to the Internet of non-IP devices can be achieved via an Internet gateway. The gateway communicates with local devices using a non-IP method on one side, and with other devices on the Internet using IP on the other side. The gateway in this case is an application layer gateway because it needs to strip down the data coming in from the local network and restructure it with a TCP/IP stack to enable communication with an Internet service.

The number of application protocol implementations created for TCP/IP over the last 20 years is vast. Reusing existing proven protocol implementations can significantly cut down development time. One of the disadvantages of the TCP/IP stack is that it is complex and large, and therefore requires a fair amount of processing power and sizeable memory, implying more development time and more expensive devices. The complexity also results in larger data packets, hence consuming more power to send and receive. For these reasons many simple networks choose to implement simpler and often times proprietary protocols.

As the technology advances, processing power and memory become more available and affordable. With wireless network processors and microcontrollers (MCUs) available today, TCP/IP communication becomes more attractive than ever, even for small and simple networks. With integration of a full TCP/IP stack into products, we expect more and more applications to move from proprietary protocols to IP-based protocols, enabling flexible Internet connectivity and faster development cycles. As shown in Fig 2, a network's range is typically categorized into four classes: Personal Area Network (PAN), Local Area Network (LAN), Neighborhood Area Network (NAN) and Wide Area Network (WAN).

Fig 2. Different ranges and applications for personal, local, neighborhood and wide area networks

B. Standards and Interoperability

One of the biggest challenges in communication systems is interoperability – the ability of devices from different vendors to exchange data. Addressing this challenge is the main goal of many standards organizations that define specifications and testing procedures designed to assure interoperability between devices. Recalling the OSI network model from Fig. 1 – some standards define one or several network layers, while others define the entire end-to-end network specifications.

UGC Approved Journal

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified

Vol. 4, Issue 7, July 2017

The Institute of Electrical and Electronics Engineers (IEEE) has a considerable focus on communication and radio engineering, and one of its familiar contributions to the networking technology is the IEEE 802.x family of standards. To name a few members of the 802.x family – 802.3 defines the Ethernet specification, which governs most wired computer networks today. 802.11 defines the WLAN specification, which is the baseline of the Wi-Fi standard, 802.15.4 defines the wireless PAN standard. It is important to point out that the 802.x standards define only the link layer of the network.

The Internet Engineering Task Force (IETF) is an open standard organization is responsible for development of Internet standards, particularly the TCP/IP suite. IETF specifications are established through the publication of draft specifications under the title "Request For Comments" (RFCs). There are thousands of Internet standards defined by RFCs. A few examples are RFC 791, which describes the IPv4 protocol; RFC 793, which describes the TCP protocol, and RFC 2616, which defines the HTTP/1.1 protocol.

The IETF, like the IEEE, does not run certification programs. That is, vendors cannot get recognition from either one of these organizations that their products comply with any of the standards. Three well-known organizations that manage certification programs today to assure interoperability between wirelessly connected devices are the Wi-Fi Alliance, the Bluetooth Special Interest Group (SIG) and the ZigBee Alliance. All three organizations provide member companies the option to take products through an interoperability test plan, which grants rights to wear the Wi-Fi, Bluetooth or ZigBee logo.

IV. PROTOCOLS FOR INTERNET OF THINGS

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. As the things in IoT use the Internet, it must also adhere to the Internet Engineering Task Force's (IETF) Internet Protocol Suite. The Internet protocols have been considered too heavy to apply for applications in the emerging IoT due to these protocols are designed for resource-rich devices with lots of power, memory and connection options. There are other aspects of the IoT which also drive modifications to IETF's work. In particular, networks of IoT end nodes will be lossy, and the devices attached to them will be very low power, loaded with constrained resources, and expected to live for years. The requirements for both the network and its end devices might look like the table 2. This new model needs new, lighter weight protocols that don't require the large amount of resources.

Table 2: Requirements for low-cost, power-constrained devices and associated networks

IoT End Network Requirements	Networking Style Impact
Self-Healing / Scalable	Mesh capable
Secure	Scalable to no, low, medium and high security without over burdening clients
End-node Addressability	Device specific addressing scalable to thousands of nodes
Device Requirements	**Messaging Protocol Impact**
Low Power / Battery-Operated	Lightweight connection, preamble, packet
Limited Memory	Small client footprint, persistent state in case of overflow
Low cost	Ties to memory footprint

Internet of Things (IoT) intelligently connects all the objects with self-configuring capabilities based on standard and interoperable protocols and formats [24]. There are hundreds of protocols supported by IoT. Of the many protocols, wireless protocols play an important role in IoT development. Understanding IoT protocol and their usage when implementing a specific application could be a complex and discouraging task. There are many wireless protocols (like IEEE 802.11 Series, 802.15 Series, Zigbee, etc) for communication between devices. However, considering a lot of small devices are unable to communicate efficiently with constrained resources. The Fig 3 presents the simplified OSI model for TCP/IP stack and IP Smart objects protocol stack [25].

Ongoing standardization efforts towards harmonizing Internet protocols for wireless sensor networks-based IoT have raised hopes of global interoperable solutions at the transport layer and below. As we move from the HTTP, TCP, IP stack to the IOT specific protocol stack we are suddenly confront with an acronym soup of protocols- from the wireless protocols like ZigBee, RFID, Bluetooth and BACnet to next generation protocol standards such as 802.15.4e, 6LoWPAN, RPL, CoAP etc. which attempt to unify the wireless sensor networks.

UGC Approved Journal

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified

Vol. 4, Issue 7, July 2017

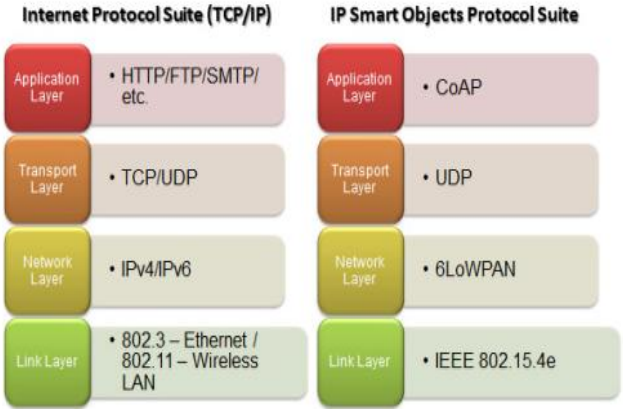

Fig 3. Simplified OSI model for TCP/IP stack and IP Smart objects protocol stack

A. IETF protocols

The Internet Engineering Task Force (IETF) is an open standard organization formed in 1986 that is responsible for development of Internet standards, particularly the TCP/IP suite. IETF publishes draft specifications under the title "request for comments" (RFCs). There are thousands of Internet standards defined by RFCs. A few examples are RFC 791, which describes the IPv4 protocol; RFC 793, which describes the TCP protocol, and RFC 2616, which defines the HTTP/1.1 protocol.

1. 6LoWPAN Working Group:

6LoWPAN is an acronym for IPv6 over Low power Wireless Personal Area Networks. The guarantee of 6LoWPAN is to apply IP to the smallest, lowest-power and most limited processing power device. 6LoWPAN is really the first wireless connectivity standard that was created for the IoT. The standard was created by the 6LoWPAN working group of the IETF and formalized under RFC 6282 "Compression format for IPv6 datagram's over IEEE 802.15.4-based networks", in [26]. As indicated by the RFC title, the 6LoWPAN standard only defines an efficient adaptation layer between the 802.15.4 link layer and a TCP/IP stack. The term 6LoWPAN is loosely used in the industry to refer to the entire protocol stack that includes the 802.15.4 link layer, the IETF IP header compression layer and a TCP/IP stack.

The advantage is that 6LoWPAN devices running on different networks can communicate with each other over the Internet, provided that they use the same Internet application protocol. A 6LoWPAN device can communicate with any other IP-based server or device on the Internet, including Wi-Fi and Ethernet devices. IPv6 was chosen as the only supported IP in 6LoWPAN (excluding IPv4) because it supports a larger addressing space, hence much larger networks, and also because it has built-in support for network auto configuration. 6LoWPAN networks require an Ethernet or Wi-Fi gateway to access the Internet. Building on the 802.15.4 advantages – mesh network topology, large network size, reliable communication and low power consumption – and on the benefits of IP communication, 6LoWPAN is well positioned to fuel the exploding market of Internet-connected sensors and other low data throughput and battery-operated applications.

2. ROLL (Routing Over Low-power Lossy Networks) Working Group:

Routing issues are very challenging for 6LoWPAN, given the low-power and lossy radio-links, the battery supplied nodes, the multi-hop mesh topologies, and the frequent topology changes due to mobility. An effective solution is being developed by the IETF "Routing Over Low power and Lossy (ROLL) networks" working group. The group has proposed the leading IPv6 Routing Protocol for Low power and Lossy Networks (LLNs), RPL, based on a gradient based approach [27] - [30].

Low power and Lossy Networks (LLNs) are made up of many embedded devices with limited power, memory, and processing resources. They are interconnected by a variety of links, such as IEEE 802.15.4, Bluetooth, Low Power WiFi, wired or other low power PLC (Power Line Communication) links. LLNs are transitioning to an end-to-end IP-based solution to avoid the problem of non-interoperable networks interconnected by protocol translation gateways and proxies. There is a wide scope of application areas for LLNs, including industrial monitoring, building automation (HVAC, lighting, access control, fire), connected homes, health care, environmental monitoring, urban sensor networks (e.g. Smart Grid), asset tracking. The Working Group focuses on routing solutions for a subset of these.

The group has proposed IPv6 Routing Protocol for LLNs (RPL) in [27] to meet the requirements mentioned in [31-34]. In order to be useful in a wide range of LLN application domains, RPL separates packet processing and forwarding from the routing optimization objectives including minimizing energy, minimizing latency, or satisfying constraints. A RPL implementation, in support of a particular LLN application, will include the necessary Objective Function(s) as required by the application. RPL operations require bidirectional links. RPL provides a mechanism to disseminate

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified

Vol. 4, Issue 7, July 2017

information over the dynamically formed network topology. This dissemination enables minimal configuration in the nodes, allowing nodes to operate mostly autonomously. RPL routes are optimized for traffic to or from one or more roots that act as sinks for the topology. As a result, RPL organizes a topology as a Directed Acyclic Graph (DAG) that is partitioned into one or more Destination Oriented DAGs (DODAGs), one DODAG per sink.

3. Constrained RESTful Environments (CoRE) Working Group (REST for IoT, CoAP, Resources directory etc…):
The use of web services (web APIs) on the Internet has become ubiquitous in most applications and depends on the fundamental REpresentational State Transfer (REST) architecture of the Web. The work on Constrained RESTful Environments (CoRE) aims at realizing the REST architecture in a suitable form for the most constrained nodes and networks (e.g., 6LoWPAN). Constrained networks such as 6LoWPAN support the fragmentation of IPv6 packets into small link-layer frames; however, this causes significant reduction in packet delivery probability.
Constrained Application Protocol (CoAP) has been designed to keep message overhead small, thus limiting the need for fragmentation [35]. CoAP is an application layer protocol that is intended for use in resource-constrained internet devices, such as WSN nodes. One of the main goals of CoAP is to design a generic web protocol for the special requirements of this constrained environment, especially considering energy, building automation, and other Machine-to-Machine (M2M) applications. CoAP is designed to easily translate to HTTP for simplified integration with the web, while also meeting specialized for M2M such as built-in discovery, very low overhead, simplicity, multicast support, and asynchronous message exchanges. CoAP would become the standard protocol to enable interaction between devices and to support IoT applications [36]. CoAP needs to consider optimizing length of datagram and satisfying REST protocol to support URI (Uniform Resource Identifier). It also needs to provide dependable communication based on UDP protocol. Some of the important features of CoAP are

- Simple proxy and caching capabilities
- URI and Content-type support
- Security binding to Datagram Transport Layer Security (DTLS)
- Asynchronous message exchanges
- UDP binding with optional reliability supporting unicast and multicast requests
- Low header overhead and parsing complexity

4. Transport Layer Security (TLS) Working Group (Datagram Transport Layer Security: DTLS):
The TLS (Transport Layer Security) working group was established in 1996 to standardize a "transport layer" security protocol. The TLS working group has completed a series of specifications that describe the TLS protocol v1.0 [RFC2246], v1.1 [RFC4346], and v1.2 [RFC5346]. The Transport Layer Security (TLS) protocol [37] is a widely deployed security solution for reliable transport protocols. Although it has been developed for any transport protocol which is reliable and maintains the order of the messages, these requirements are only met without limitations by the Transmission Control Protocol (TCP). Securing the unreliable User Datagram Protocol (UDP) as well as the Stream Control Transmission Protocol (SCTP) [38] is not possible or only very limited. As a result Datagram Transport Layer Security (DTLS) protocol version 1.0, a modification of the Transmission Control Protocol (TCP) for unreliable transport protocols is described in RFC 4347 [39].
The DTLS protocol provides communications privacy for datagram protocols. This allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery. The DTLS protocol is based on the Transport Layer Security (TLS) protocol and provides equivalent security guarantees. An updated version 1.2 of the Datagram Transport Layer Security (DTLS) protocol is proposed in RFC 6347 [40].
The primary additional security consideration raised by DTLS is that of Denial of Service (DoS). DTLS includes a cookie exchange designed to protect against denial of service. However, implementations that do not use this cookie exchange are still vulnerable to DoS. In particular, DTLS servers that do not use the cookie exchange may be used as attack amplifiers even if they themselves are not experiencing DoS. Therefore, DTLS servers should use the cookie exchange unless there is good reason to believe that amplification is not a threat in their environment. Clients must be prepared to do a cookie exchange with every handshake. DTLS uses all of the same handshake messages and flows as TLS, with three principal changes [40]:

- A stateless cookie exchange has been added to prevent denial-of-service attacks.
- Modifications to the handshake header to handle message loss, reordering, and DTLS message fragmentation to avoid IP fragmentation.
- Retransmission timers to handle message loss.

B. Message Queue Telemetry Transport (MQTT)
The MQTT protocol is a publish-subscribe messaging model in an extremely lightweight way. IBM invented this protocol for satellite communications with oil field equipment. It had reliability and low power at its core and so made good sense to be applied to IoT networks. MQTT uses a "publish/subscribe" model, and requires a central MQTT

UGC Approved Journal

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified

Vol. 4, Issue 7, July 2017

broker to manage and route messages among an MQTT network's nodes. Eclipse describes MQTT as "a many-to-many communication protocol for passing messages between multiple clients through a central broker."
Similar to CoAP, it was built with resource-constrained devices in mind. MQTT has a lightweight packet structure designed to conserve both memory usage and power. A connected device subscribes to a topic hosted on an MQTT broker. Every time another device or service publishes data to a topic, all of the devices subscribed to it will automatically get the updated information. It is useful for connections with remote locations where a small code footprint is required and/or network bandwidth is at a premium. Strengths of the protocol includes

- MQTT's "pub/sub" model scales well and can be power efficient.
- Pub/Sub model has specific benefits like – Space decoupling, Time decoupling and Synchronization decoupling.
- MQTT uses unencrypted TCP and is not "out-of-the-box" secured.
- In MQTT, "QoS" levels 0, 1 and 2 describe increasing levels of guaranteed message delivery.
- MQTT provides a "last will and testament (LWT)" message that can be stored in the MQTT broker in case a node is unexpectedly disconnected from the network.

C. Zigbee IP

ZigBee offers the only open, global wireless standard enabling everyday simple and smart objects to work together and help you control your world. ZigBee is the leading standard for monitoring and control used in consumer, commercial and industrial markets around the world. The Alliance is an open, non-profit ecosystem of approximately 400 organizations developing and promoting standards defining the Internet of Things for use in homes and businesses. The ZigBee protocol is traditionally used in industrial settings and was designed for the special requirements of device-to-device communication. ZigBee PRO and ZigBee Remote Control (RF4CE) are based on the IEEE802.15.x protocol, an industry-standard wireless networking technology operating at 2.4GHz. ZigBee is suitable for applications that require infrequent data exchanges at low data-rates, usually operating within a 100m range, such as in a home or building. ZigBee RF4CE's advantages include low-power operation, high security, robustness, high scalability, and high node counts. ZigBee is well placed to take advantage of wireless control and sensor networks in M2M and IoT applications. The ZigBee Alliance, a global ecosystem of organizations creating wireless solutions for use in energy management, commercial and consumer applications, today announced it has completed testing and development of 920IP, an update to ZigBee IP, the first open, global standard for an IPv6 based full wireless mesh networking solution to control low power, low cost devices [41].
ZigBee IP is the first open standard for an IPv6-based full wireless mesh networking solution and provides seamless Internet connections to control low-power, low-cost devices. It connects dozens of the different devices into a single control network. ZigBee IP was designed to support ZigBee 2030.5. It has been updated to include 920IP, which provides specific support for ECHONET Lite and the requirements of Japanese Home Energy Management systems. 920IP is the only standard referenced by the Telecommunications Technology Committee (TTC) which supports multi-hop mesh networking.

The ZigBee IP specification enriches the IEEE 802.15.4 standard by adding network and security layers and an application framework. ZigBee IP offers a scalable architecture with end-to-end IPv6 networking, laying the foundation for an Internet of Things without the need for intermediate gateways. It offers cost-effective and energy-efficient wireless mesh network based on standard Internet protocols, such as 6LoWPAN, IPv6, PANA, RPL, TCP, TLS and UDP. ZigBee IP enables low-power devices to participate natively with other IPv6-enabled Ethernet, Wi-Fi and, HomePlug devices. One of the key advantages of ZigBee IP over other offerings using 802.15.4 is that it provides a scalable architecture with end-to-end IPv6 networking. In this way it provides an ideal basis for many applications that are considered as part of the Internet of Things. Characteristics of ZigBee IP include [42]:

- Global operation in the 2.4GHz frequency band according to IEEE 802.15.4
- Regional operation in the 915Mhz (Americas), 868Mhz (Europe) and 920 MHz (Japan)
- Incorporates power saving mechanisms for all device classes
- Supports development of discovery mechanisms with full application confirmation
- Supports development of pairing mechanisms with full application confirmation
- Multiple star topology and inter-personal area network (PAN) communication
- Unicast and multi-cast transmission options
- Security key update mechanism
- Utilizes the industry standard AES-128-CCM security scheme
- Supports Alliance standards or manufacturer specific innovations

D. Open Mobile Alliance (OMA)

OMA is the Leading Industry Forum for Developing Market Driven – Interoperable Mobile Service Enablers. This was formed in June 2002 by the world's leading mobile operators, device and network suppliers, information technology

UGC Approved Journal

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified

Vol. 4, Issue 7, July 2017

companies and content and service providers. OMA is a non-profit organization that delivers open specifications for creating interoperable services that work across all geographical boundaries, on any bearer network. OMA's specifications support the billions of new and existing fixed and mobile terminals across a variety of mobile networks, including traditional cellular operator networks and emerging networks supporting M2M device communication.

1. Lightweight M2M Enabler Standard (CoAP/DTLS based):
The industry has been looking for a simple, low-cost remote management and service enablement mechanism, which embraces modern architectural principles (in line with Internet standards), also works over wireless connections and is fit for purpose due to being lightweight. This new standard is thus called OMA Lightweight Machine to Machine (LWM2M).

OMA LWM2M is a protocol from the Open Mobile Alliance for M2M or IoT device management. Lightweight M2M enabler defines the application layer communication protocol between a LWM2M Server and a LWM2M Client, which is located in a LWM2M Device. The OMA Lightweight M2M enabler includes Device Management (DM) and Service Enablement (SE) for LWM2M Devices. The target LWM2M devices for this enabler are mainly resource constrained devices. Therefore, this enabler makes use of a light and compact protocol as well as an efficient resource data model. It provides a choice for the M2M Service Provider to deploy a M2M system to provide service to the M2M User. The LWM2M protocol, to be used for remote management of M2M devices and related service enablement, has at least four outstanding characteristics:

1) it features a modern architectural design based on REST appealing to software developers,
2) it defines a resource and data model that is extensible,
3) it has been designed with performance and the constraints of M2M devices in mind, and
4) it reuses and builds on an efficient secure data transfer standard called the Constrained Application Protocol (CoAP) that has been standardized by the Internet Engineering Taskforce (IETF)

Lightweight M2M 1.0 enabler introduces the following features.

- Simple Object based resource model
- Resource operations of creation/ retrieval/ update/deletion/configuration of attribute
- Resource observation/notification
- UDP and SMS transport layer support
- Queue mode for NAT/Firewall environment
- Multiple LWM2M Server support
- Basic M2M functionalities: LWM2M Server, Access Control, Device, Connectivity, Firmware Update, Connectivity Statistics [43]

2. Device Management 2.0 Enabler Standard (HTTP/TLS based):
The Device Management (DM) Working Group (WG) specifies protocols and mechanisms to achieve the management of mobile devices, services access and software on connected devices. The OMA Device Management (OMA DM) Enabler is a set of specifications designed for the management of mobile devices such as mobile phones, PDAs, tablet computers and, more recently, M2M devices. The OMA DM Enabler is intended to support multiple uses including Provisioning, Device Configuration, Software Upgrades and Fault Management [44]. OMA DM is a specification suite of OMA Enablers. It consists of core protocols and application data models.
OMA DM Version 1.2 Enabler defines interfaces between a DM Client and a DM Server. The protocol is designed as a representation of SyncML, which is robust over band-constrained, packet-lossy wireless networks. OMA DM Version 1.3 introduces new notifications, transport protocols and a new DM Server to DM Server interface for delegation. OMA DM Version 2.0 introduces new Client-Server DM protocol and new user interaction method on Device Management using Web Browser Component.

For authentication, OMA DM provides its own (application-level) mechanism as well as transport-layer authentication. For confidentiality and integrity, it depends on transport layer mechanisms, e.g. SSL/TLS in HTTP binding. OMA DM does include security requirements including:

- Credentials
- Initial Provisioning of Credentials
- Authentication
- Integrity
- Confidentiality
- Notification of initiated session
- Bootstrap

UGC Approved Journal

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified

Vol. 4, Issue 7, July 2017

The reasons for adopting OMA DM by other organizations are:

- It is a widely deployed standard across many devices
- It is managed by Mobile Operators through Device Management Servers
- It has proven interoperability among different servers and devices vendors
- It has been adopted by other SDOs such as 3GPP, oneM2M, Wi-Fi Alliance and so on.

E. ETSI/OneM2M

OneM2M was launched in 2012 as a global initiative to ensure the most efficient deployment of Machine-to-Machine (M2M) communications systems and the Internet of Things (IoT). OneM2M comprises fourteen partners including European Tele-communications Standards Institute (ETSI) and seven other leading Information and Communications Technologies (ICT) Standards Development Organizations (SDOs) and also representatives of different industry sectors. The purpose and goal of OneM2M is to develop technical specifications which address the need for a common M2M Service Layer that can be readily embedded within various hardware and software, and relied upon to connect the numerous devices in the field with M2M application servers worldwide. A critical objective of OneM2M is to attract and actively involve organizations from M2M-related business domains such as: intelligent transportation, healthcare, utilities, industrial automation, smart homes, etc.

F. eXtensible Messaging and Presence Protocol (XMPP)

The XMPP community has since 2013 been working to enable the federated XMPP network to support Internet of Things (IoT). The XMPP-IoT initiative is an Internet of Things solution from the XMPP standards foundation XSF. It consists of several extensions to the common known XMPP instant messaging standard. One of the core values of the technology is that XMPP already has a large federated server to server infrastructure for messaging. Using this will create an open interoperable middleware for IoT [45]. Where any device in a domain freely can choose to interact with anybody else through the federation and friendship mechanisms, just as the chat network is used today. Using standard XML creates good interoperability possibilities and during 2014 the XMPP network also upgraded to demand participants in the network to enforce encryption both server to server and client to server to increase security.

This protocol is a TCP communications protocol based on XML that enables near-real-time exchange of structured data between two or more connected entities. The advantage is XMPP is decentralized nature [46]. XMPP offers an easy way to address a device. This is especially handy if that data is going between distant, mostly unrelated points, just like the person-to-person case. It's not designed to be fast. A protocol called BOSH (Bidirectional streams over Synchronous HTTP) lets severs push messages. But "real time" to XMPP is on human scales, measured in seconds [47].

XMPP works similar to email, operating across a distributed network of transfer agents rather than relying on a single, central server or broker (as CoAP and MQTT do). As with email, it's easy for anyone to run their own XMPP server, allowing device manufacturers and API operators to create and manage their own network of devices. And because anyone can run their own server, if security is required, that server could be isolated on a company intranet behind secure authentication protocols using built-in TLS encryption. One of the disadvantages is the lack of end-to-end encryption. While there are many use cases in which encryption may not yet be necessary, most IoT devices will ultimately need it. The lack of end-to-end encryption is a major downside for IoT manufacturers. Another disadvantage is the lack of Quality of Service (QoS).

G. Data Distribution Service

"Machine-to-Machine" (M2M) intelligent systems, like navy combat ships or 500-turbine wind power arrays, face challenges not addressed by most enterprise networking software. Of the thousands of messaging protocol standards, two are becoming most important in this market: the Data Distribution Service (DDS), an international standard by the Object Management Group (OMG), and the Advanced Message Queuing Protocol (AMQP), managed by the Organization for the Advancement of Structured Information Standards (OASIS).

The DDS is an M2M standard that aims to enable scalable, real-time, dependable, high-performance and interoperable data exchanges between publishers and subscribers. DDS addresses the needs of applications like financial trading, air-traffic control, smart grid management, and other big data applications. The standard is used in applications such as smartphone operating systems [48], transportation systems and vehicles [49], software-defined radio, and by healthcare providers. DDS may also be used in certain implementations of the Internet of Things [50].

DDS is a standard technology for ubiquitous, interoperable, secure, platform independent, time and space efficient data sharing across network connected devices. DDS provides a Global Data Space abstraction that allows applications to autonomously, anonymously securely and efficiently share data. Highlights of DDS includes

- Elegant and High Level Data Sharing Abstraction
- Polyglot and platform independent
- Peer-to-Peer by nature, Brokered when useful

UGC Approved Journal

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified

Vol. 4, Issue 7, July 2017

- Time and Space efficient
- Run efficiently over small bandwidth links and is provides minimal latency
- Content and Temporal Filtering (both sender and receiver filtering supported)
- 20+ QoS to control existential, temporal, and spatial properties of data
- High Performance and Scalable

H. Thread protocol

Thread is an IPv6-based[51] royalty-free [52] protocol for "smart" household devices to communicate on a network [53]. In July 2014 Google Inc's Nest Labs announced a working group with the companies Samsung, ARM Holdings, Freescale, Silicon Labs, Big Ass Fans and the lock company Yale. They proposed an open and standard set of protocols for home automation called Thread. This is an IP based wireless networking protocol designed for low-power connected products in home automation space. They made an attempt to make the Thread become an industry standard by providing Thread certification for products [54]. Other protocols in use include ZigBee and Bluetooth Smart [55].

Thread would allow all the devices in your home to communicate with one another without any hassle. Thread is designed for all home automation products including appliances, access control, climate control, energy management, lighting and safety. Thread uses 6LoWPAN, which in turn uses the IEEE 802.15.4 wireless protocol with mesh communication, as does ZigBee and other systems. Thread however is IP-addressable, with cloud access and AES encryption. It supports over 250 devices on a network [56]. Thread tries to solve the existing issues in home automation by leveraging the following features [57]:

- Open standard protocol
- Simple for consumers to use
- Secure
- Power-efficient
- No single point of failure
- Designed to support a wide variety of products for the home

V. PROTOCOL SELECTION PROBLEM

Higher-level protocols for the Internet of Things (IoT) offer various features that make them suitable for a broad range of applications. For example, SNMP has been used for many years to manage network devices and configure networks and DDNS has been used to provide browser access to web devices. Either protocol can also be used for managing and configuring a variety of home devices. In comparison, CoAP is more suited to very small sensor deployments with tiny hardware and completely different security. A deeper understanding of these protocols and the applications requirements is necessary to properly select which protocol is most suitable for the application at hand.

Once the correct protocol or set of a few protocols is known to have the right characteristics for the application deployment, management and application support, the best implementation of each protocol should be understood. From this understanding, the designer can select the optimal implementation of each protocol for the system and then from these, select the best protocol implementation for the system. The protocol selection problem is closely tied to the implementation of the protocol and the components that support the protocol are often essential in the final design. All aspects of deployment, operation, management, and security must be considered as part of the protocol selection including the implementation environment.

In addition, there are not any converged standards for particular applications, and these standards are generally selected by the market. This is a problem and an opportunity because the protocol selected for an application today may become obsolete in the future and may need to be replaced, or could become the standard if done correctly. As a developer, using specific features of the environment, to satisfy system requirements that, in turn, rely on the details of the protocol can make change in the future very difficult.

Most of these protocols were developed by specific vendors, and these vendors typically promote their own protocol choices, don't clearly define their assumptions, and ignore the other alternatives. For this reason, relying on vendor information to select IoT protocols is problematic and most comparisons that have been produced are insufficient to understand tradeoffs. The key assumptions behind the use of the protocol are not clearly stated which makes comparison difficult. The fundamental assumptions associated with IoT applications are:

- Various wireless connections will be used
- Data will be stored in the cloud and may be processed in the cloud
- Connections back to the cloud storage are required
- Routing of information through wireless and wire line connections to the cloud storage is required
- Devices will range from tiny MCUs to high-performance systems with the emphasis on small MCUs
- Security is a core requirement

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified

Vol. 4, Issue 7, July 2017

Other assumptions made by the protocol developers require deeper investigation and will strongly influence their choices. By looking at the key features of these protocols and looking at the key implementation requirements, designers can develop a clearer understanding of exactly what is required in both the protocol area and in the supporting features area to improve their designs.

VI. CONCLUSION

Today, IoT is a strong term that every manufacturer wants to take advantage of the enormous IoT media coverage. The Internet Protocol (IP) is a carrier; it can encapsulate just as many protocols for the IoT as it does today for the Web. A lot of industry people are calling for protocol standardization. People choose the protocols that meet their requirements. The only difference is that the IoT protocols are still fairly young, and have yet to demonstrate their reliability. When the Internet became a reality, IP version 4 was what made it possible. We are now deploying IP version 6, and IoT is the killer application that telecommunication carriers have been waiting for to justify the investment required. All these protocols are positioned as real-time publish-subscribe IoT protocols, with support for millions of devices. Depending on how you define "real time" (seconds, milliseconds or microseconds) and "things" (WSN node, multimedia device, personal wearable device, medical scanner, engine control, etc.), the protocol selection for your product is critical. Fundamentally, these protocols are all very different.

REFERENCES

[1] Q. Zhou and J. Zhang, "Research prospect of Internet of Things geography," in Proceedings of the 19th International Conference on Geoinformatics, IEEE, pp. 1–5, 2011.
[2] Y. Yu, J. Wang, and G. Zhou, "The exploration in the education of professionals in applied Internet of Things engineering," in Proceedings of the 4th International Conference on Distance Learning and Education (ICDLE), IEEE, pp. 74–77, 2010.
[3] RFC 7452, "Architectural Considerations in Smart Object Networking", https://tools.ietf.org/html /rfc7452, March 2015.
[4] Burkitt Frank, "A Strategist's Guide to the Internet of Things", Strategy + Business, Nov. 2014.
[5] http://www.idc.com/getdoc.jsp?containerId=prUS40782915.
[6] Andrea Zanella, Nicola Bui, Angelo P Castellani, Lorenzo Vangelista, and Michele Zorzi. Internet of things for smart cities, IEEE Internet of Things Journal, 2014.
[7] Ahmad W Atamli and Andrew Martin. Threat-Based Security Analysis for the Internet of Things. In Secure Internet of Things (SIoT), pages 35–43. IEEE, 2014.
[8] Luigi Atzori, Antonio Iera, and Giacomo Morabito. The Internet of Things: A survey, Computer Networks, 54(15):2787–2805, Oct-2010.
[9] Sachin Babar, Parikshit Mahalle, Antonietta Stango, Neeli Prasad, and Ramjee Prasad. Proposed security model and threat taxonomy for the Internet of Things (IoT). In International Conference on Network Security & Applications (CNSA), volume 89, pages 420–429. Springer Berlin Heidelberg, 2010.
[10] G A N Gang, L U Zeyong, and Jiang Jun. Internet of Things Security Analysis. In Internet Technology and Applications (iTAP), pages 1–4. IEEE, 2011.
[11] Vangelis Gazis, Carlos Garcia Cordero, Emmanouil Vasilomanolakis, Panayotis Kikiras, and Alex Wiesmaier. Security Perspectives for Collaborative Data Acquisition in the Internet of Things. In International Conference on Safety and Security in Internet of Things. Springer, 2014.
[12] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7):1645–1660, September 2013.
[13] Anth´ea Mayzaud, R´emi Badonnel, and Isabelle Chrisment. Monitoring and Security for the Internet of Things. In International Conference on Autonomous Infrastructure, Management, and Security, pages 37–40. Springer, 2013.
[14] Daniele Miorandi, Sabrina Sicari, Francesco De Pellegrini, and Imrich Chlamtac. Internet of things: Vision, applications and research challenges. Ad Hoc Networks, 10(7):1497–1516, September 2012.
[15] Huansheng Ning, Hong Liu, and Laurence T Yang. Cyberentity Security in the Internet of Things. Computer, 46(4):46–53, 2013.
[16] R Roman, P Najera, and J Lopez. Securing the internet of things. Computer, 44(9):51–58, 2011.
[17] Rolf H. Weber. Internet of Things – New security and privacy challenges. Computer Law & Security Review, 26(1):23–30, January 2010.
[18] ITU Internet Reports, The Internet of Things, November 2005.
[19] G. Kortuem, F. Kawsar, V. Sundramoorthy, and D. Fitton, "Smart objects as building blocks for the internet of things," IEEE Internet Computing pp. 30–37, January/February 2010.
[20] Future internet 2020, Visions of an Industry Expert Group, May 2009.
[21] White Paper: Smart Networked Objects & Internet of Things, Les Instituts Carnot, V1.1, January 2011.
[22] Tanenbaum A S, Computer Networks, 3rd Edition, Prentice Hall, 1996.
[23] Postel J, RFC793 Transmission Control Protocol, Defense Advanced Research Projects Agency, 1981.
[24] St.Petersburg, "Internet of Things, Smart Spaces, and Next Generation Networking", Russia, August 27-29, 2012 http://link.springer.com /book/ 10.1007%2 F978-3-642-32686-8.
[25] R. Sutaria & R. Govindachari, "Making Sense of Interoperability. Protocols and Standardization Initiatives in IOT". 2nd International Workshop on Computing and Networking for Internet of Things (CoMNet-IoT) held in conjunction with 14th International Conference on Distributed Computing and Networking (ICDCN 2013), 2013. Online: http://bit.ly/1tipZyH.
[26] J. Hui and P. Thubert, Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks, RFC 6282, Internet Engineering Task Force RFC 6282, September 2011.
[27] T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J. P. Vasseur, and R. Alexander, RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks, RFC 6550, Internet Engineering Task Force RFC 6550, March 2012.
[28] J. W. Hui and D. E. Culler, "IPv6 in Low-Power Wireless Networks," Proc. IEEE, vol. 98, no. 11, pp. 1865 – 1878, November 2010.
[29] K. Jeonggil, A. Terzis, S. Dawson-Haggerty, D. E. Culler, J. W. Hui, and P. Levis, "Connecting Low-power and Lossy Networks to the Internet," IEEE Communications Magazine, vol. 49, no. 4, pp. 96 – 101, April 2011.

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified

Vol. 4, Issue 7, July 2017

[30] J. Vasseur, N. Agarwal, J. Hui, Z. Shelby, P. Bertrand, and C. Chauvenet, "RPL: The IP routing protocol designed for low power and lossy networks," Internet Protocol for Smart Object (IPSO) Alliance, White Paper, April 2011.
[31] J. Martocci, Ed, P. De Mil, N. Riou, and W. Vermeylen, Building Automation Routing Requirements in Low-Power and Lossy Networks, RFC 5867, Internet Engineering Task Force RFC 5867, June 2010.
[32] A. Brandt, J. Buron and G. Porcu, Home Automation Routing Requirements in Low-Power and Lossy Networks, RFC 5826, Internet Engineering Task Force RFC 5826, April 2010
[33] K. Pister, Ed., P. Thubert, Ed, S. Dwars and T. Phinney, Industrial Routing Requirements in Low-Power and Lossy Networks, RFC 5673, Internet Engineering Task Force RFC 5673, October 2009.
[34] M. Dohler, Ed., T. Watteyne, Ed., T. Winter, Ed. and D. Barthel, Ed., Routing Requirements for Urban Low-Power and Lossy Networks, RFC 5548, Internet Engineering Task Force RFC 5548, May 2009.
[35] Z. Shelby, K. Hartke and C. Bormann, The Constrained Application Protocol (CoAP), RFC 7252, Internet Engineering Task Force (IETF) RFC 7252, June 2014.
[36] S. Keoh, Philips Research, Z. Shelby,Sensinode. Profiling of DTLS for CoAP-based IoT Applications draft-keoh-dice-dtls-profile-iot-00 (2013), http://tools.ietf.org/ html/ draftkeoh-dice-dtls-profile-iot-00
[37] T. Dierks, E. Rescorla, The Transport Layer Security (TLS) Protocol. IETF RFC 5246, August 2008.
[38] R. Stewart, Stream Control Transmission Protocol, IETF RFC 4960, September 2007.
[39] E. Rescorla, N. Modadugu, Datagram Transport Layer Security, IETF RFC 4347, April, 2006.
[40] E. Rescorla, N. Modadugu, Datagram Transport Layer Security Version 1. 2, IETF RFC 6347, January, 2012.
[41] ZIGBEE PRESS RELEASE: 920IP: Low-Power, IPv6 Networking for Home Energy Management by ZigBee Alliance, July, 2014.
[42] http:// www.zigbee.org/ zigbee-for-developers/ network-specifications/ zigbeeip/
[43] http:// technical.openmobilealliance.org/ Technical/ technical-information/ release-program/ current-releases / oma-lightweightm2m-v1-0
[44] http://openmobilealliance.org/oma-dm-qa/
[45] https://archive.fosdem.org/2015/schedule/event/deviot12/
[46] http://www.infoworld.com/article/2972143/internet-of-things/real-time-protocols-for-iot-apps.html
[47] http://electronicdesign.com/iot/understanding-protocols-behind-internet-things
[48] What Can DDS Do For Android, 2012, http://www.omg.org/hot-topics/documents/dds/Android_and_ DDS1.pdf
[49] City of Tokyo Metropolitan Highway Line, 2013, http: //www. Omg .org /hot-topics/ documents/ dds/ Tokyo_Snapshot_1.pdf
[50] Building the Internet of Things with DDS, 2013, http:// www. omg.org/ news /meetings/tc/nj-13/ special-events/iot-pdfs/ corsaro.pdf
[51] "Thread Wireless Networking Protocol Now Available", threadgroup .org, Thread Group, Retrieved 25 October 2015.
[52] "About", threadgroup.org, Thread Group, Retrieved 25 October 2015.
[53] Simon Rockman, "Google Nest, ARM, Samsung pull out Thread to strangle ZigBee", The Register, Retrieved18 July 2014.
[54] Noel Randewich, "Google's Nest launches network technology for connected home", Reuters, Retrieved18 July 2014.
[55] "Samsung, ARM, and Nest launch Thread, a low-power network for the smart home", PC World, Retrieved 18 July 2014.
[56] "Introducing Thread", SI Labs, Retrieved 21 October 2014.
[57] http:// www.infoq.com/ articles/ thread-protocol-for-home-automation