Survey Paper For 'CS 695 - 002 Wireless and Mobile Computing'. Fall 2016.

THE INTERNET OF THINGS: A SURVEY OF IoT PROTOCOLS AND RELATED TECHNOLOGIES

Rishi Mehta- MS in Information Systems
George Mason University
Fairfax, Virginia

ABSTRACT

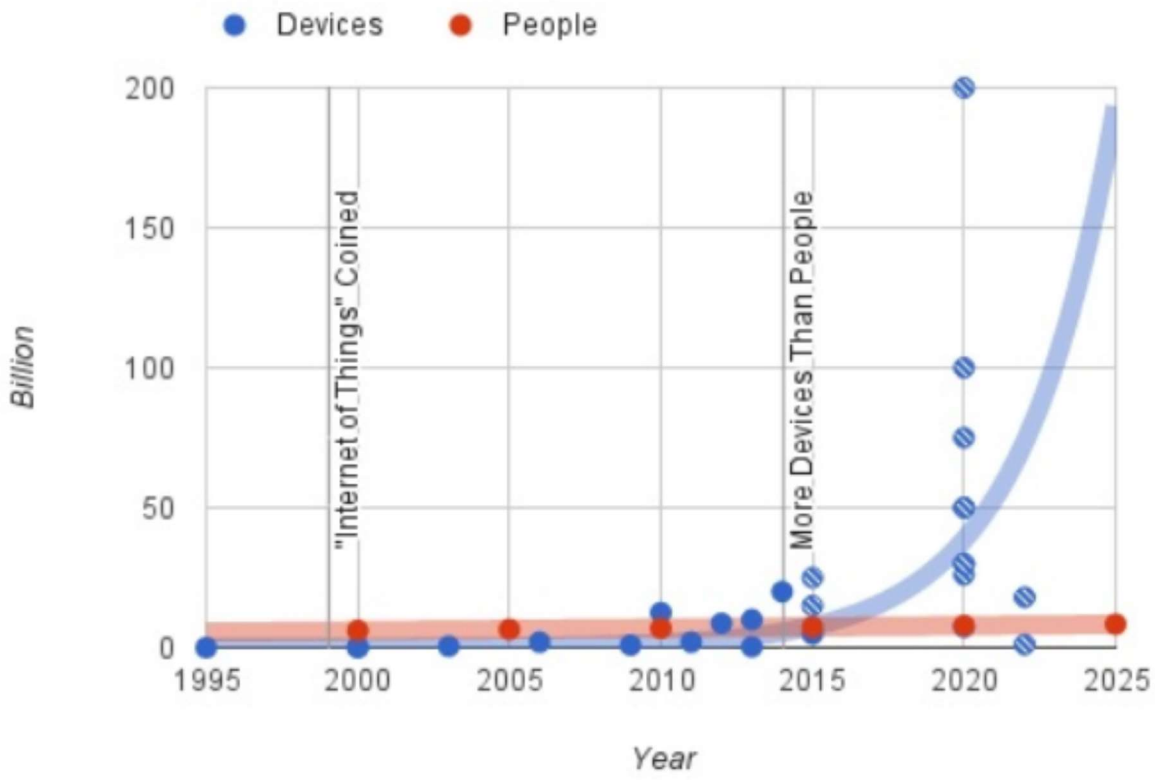
This is a survey paper that I have written for my course "Wireless and Mobile computing" as a part of the final project. The paper starts with an introduction to the Internet of Things (IoT) and various technologies involved as well the impact of IoT on the current technological scenario. Next I have presented a detailed explanation of the IoT architecture and different wireless communication standards. Then I shed some light upon different IoT protocols in existence. I then compare these protocols in order to try and draw a clear picture of IoT infrastructure and applications. Next I have discussed about the interoperability issue and the importance it holds in the development of IoT infrastructure in the upcoming years. This is followed by introduction to IoT Gateways. Later comes a segment about different IoT application use-cases. This section includes information about various fascinating use-cases that already exists and use IoT as a medium to optimize and improve their respective domains. Finally I conclude the paper with closing statements which includes what we learnt from this survey paper. This is followed by the references segments.

1. INTRODUCTION

This paper surveys important trends, key technologies and emerging technological solutions for the internet of things. These things are our day-to-day objects, but integrated with special software to "communicate" amongst each other as well as other devices that analyze the data sent by these "objects". These "objects" are what we call as the "smart things" because of their ability to interact and sense other "things".

The number of smart things is growing exponentially. By 2020, tens of billions of things will be deployed worldwide, collecting a wealth of diverse data. Computers collect in-field data and transmit it to a central data center where analytics are applied to it, but this is no longer a sustainable model. There are instabilities and growing issues related to collection of this type of data and preserving it [2]. Applications related to IoT can be found in several and different domains: energy, health, transportation, environment, etc. Thousands of applications can be identified in each domain and new ones appear every day, requiring a strong interconnection among things [25]. This brings us to the next major issue in the internet of things, which is interoperability. As these "smart things" grow in number, it becomes of utmost importance to connect them to each other on a naturally stable and accepted platform.

According to this analysis from Evans in 2011 [7], there is a great number of connected devices already existing. As a matter of fact the analysis points out that this number had already exceeded the total human population in 2010.



(Figure 1: Trend of devices vs people [15])

The above figure shows that by 2020, it is predicted that about 50 billion devices will be connected under the Internet of Things. This is a whooping number and we also see that in the last few years since 2011, the number of connected devices has already grown exponentially [3]. Since the last decade, we are assisting in a progressive jump from a non-ubiquitous Internet, where humans access Internet using a computer at their work or at home, to the current ubiquitous Internet where we access the Internet using smartphones, tabs, or TVs, anytime, anywhere. In the same way, now is the time of the Internet of Things (IoT) when not only humans but also "*things",* are present in the Internet [26] [4]. Accessibility is now a major point of discussion as we move towards this age of virtually connecting everything to one another. To keep up with the rising demand of technology and to match the trend, newer architectures and protocols are to be established every now and then. This also ensures that as the number grows, so does the accessibility and interoperability amongst devices and the so called "things".

A question may arise as to what is considered into the bracket of "smart things" and if a device is not connected to the Internet while communicating with other devices, is it still considered to be a part of the IoT. This is very well explained by my professor Parth H. Pathak[6] in one of his lectures. H explains that the "Internet of Things" is an umbrella term which consists of a lot of devices and "things" connected to each other and not necessarily connected to the Internet at all points of time. What comprises into to the term "Internet of Things" and what not, is a little ambiguous right now as we figure out the various application of this relatively new technology. He then goes on to mention that it also depends on which protocol stack we prefer to implement in order to connect these "things" that determines if the device requires to have its own IP or not. Determining the correct protocol stack to implement for our application

is another one of major issues we talk about and explore in this paper ahead as we compare different IoT protocols and try to put a perspective into the general direction of implementing these protocols in the Internet of Things.

The IoT transforms these objects from being traditional to being smart by exploiting the technologies. These underlying technologies take the form of the day to day objects and these get transformed into smart objects. This leads us to the development of the "smart homes". These smart homes will consist a number of "smart" objects that are all heterogeneously interconnected to one another and have a solid and stable communication system equipped that connects the whole house. The smart-homes will enable their residents to automatically open their garage upon reaching home, prepare their coffee on demand, control climate control systems, televisions and other home equipment and devices with a "smart remote". In order to realize this potential growth, emerging technologies and innovations, and service applications need to grow proportionally to match market demands and customer needs. Utilizing a large addressing space (e.g., IPv6) becomes necessary to meet customer demands for smart objects in order to catch up with the rising demand of these devices and their interconnectivity. Security and privacy are other important requirements for the IoT due to the inherent heterogeneity of the Internet connected objects and the ability to monitor and control physical objects [5]. Security of the residents of these "smart homes" and other IoT users in general is at a huge risk as they are constantly tracked and data is continuously being transmitted to the could sources. This leaves us vulnerable to data theft, eavesdropping, malicious intent towards the collected data and also being exposed to loss of control over devices to outside party. Next we talk about privacy, as we have come to figure in the past decade or so, privacy and security now go hand-in-hand and are a part of a large trade-off that we slowly are coming to terms with. The privacy of the IoT users is always at stake as these connected devices constantly track important details, from the temperature of the environment to the heartbeat-rate of the users and also sensitive information such as the user's location. These devices also track the user's whereabouts including where they have been and how often. This is the part where it gets scary. All things considered, user's privacy and security may account to a great amount of negligence to this technology and might cause hindrance to the development of these "smart" devices as some users may be reluctant to give so much control and power in the hands of a machine.

Currently, Internet acts as the base infrastructure for the exchange of information. However, access to it has several constraints such as the need for unique identifier, the change of communication technology, and the adoption of the Internet Protocols. These constraints have cause to divide all protocols to IP-based and Non IP-based. This has created a virtual "IP wall" which needs to be deconstructed in order to achieve full benefits of the IoT infrastructure on every platform. Nowadays, this "IP wall" is usually jumped through an IoT gateway.
Although IP connectivity is not necessarily required to ensure inter-*thing* communication, many standards include IP as part of their specification to ease the process of connecting "things". IP connectivity has gradually become a big concern in the IoT world and implementation of different gateways has because absolutely necessary to overcome this IP connectivity problem. Nevertheless, this is not enough to ensure interoperability at required IoT application level. As *things* are resource-challenged communication nodes, efficient data transmission mechanisms are needed at IP level;
Wireless communication protocols are mandatory if "*things"* need to be mobile and ubiquitous. Depending on the different applications, different standards are commonly used to provide connectivity:
ZigBee, RFID, Bluetooth, 6lowPAN, WIFI, 3G, and so forth are some of the standards commonly used for the Internet of Things connectivity [4].

2. IoT ARCHITECTURE

To connect millions of "things" together, there needs to be set up and implemented a robust architecture that follows IoT designated protocol stacks to develop integrated systems for communications. Various models have been suggested to implement this sort of architecture over time. These models are layered

The platform designed for the IoT applications must handle the needs of all kinds of users. These include administrators, developers and most importantly the end users. These are the general public at large who consume the IoT applications. Different types of services need to be provisioned on this common platform. These services include device management, data storage and retrieval, data management and analytics as well as end-user management. These IoT platforms need to be integrated to other services to improve their performance. Integration with Infrastructure-as-a-service (IAAS) clouds enables them to be highly scalable. The platform must also support virtually any kind of sensor.

Since there are no commonly accepted layer architectures for IoT, there is a difficulty in specifying a common set of services and an environment for service design and composition [1].

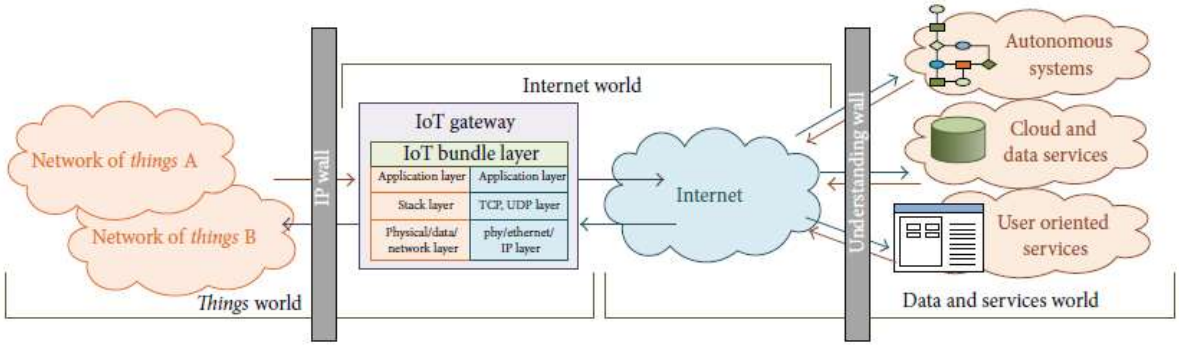


Figure 2: IoT Architecture [4]

2.1 WIRELESS COMMUNICATION

This segment throws light upon different wireless communication standards and technologies. These technologies have huge role to play in connecting various devices and "smart things" into the overall IoT infrastructure. These standards include WiMAX, IEEE 802.16, Zigbee, 6LowPAN, RFID, Bluetooth, WIFI, and 3G amongst others. Wireless Communication standards such as ZigBee or 6LoWPAN are much more used in IoT applications but involve hardware restrictions and lack of interoperability among them.

2.1.1 ZigBee

The main reason for the introduction of the ZigBee standard was short-ranged communication of wireless networks. This has developed to be one of the most important criteria in recent history for wireless communication. The range of ZigBee's wireless communication can be as short as a few meters (10 to 100). The Zigbee standard stack includes a security model. ZigBee works on the network layer and the layers above it. ZigBee is optimized for low power applications and supports different application profiles (e.g., ZigBee Home Automation, ZigBee Health Care, ZigBee Building Automation, etc.), with each profile engineered according to the requirements of a particular application domain [2]. Important Zigbee applications include monitor and control.
ZigBee not only defines vertical profiles (home automation, energy metering, healthcare, etc.), but also horizontal functional domains to specify how devices must exchange application data [11]. Every ZigBee compliant temperature sensor must implement "measurement & sensing functional domain" and any other

device in the network would be able to get temperature information as defined in the specification. ZigBee allows instantiation of intelligence in the network by defining how to coordinate devices to produce scenes and create virtual bindings among devices [12], for example, to program a switch to turn on two lights and open a motorized door [2].

2.1.2 6LowPAN

6LowPAN stands for IPv6 over Low-Power Wireless Personal Area Networks. It is designed for low-cost implementation of IPv6. 6LowPAN is known for its very low power consumption in the Wireless Personal Area Networks, hence the name. According to a research done by Chawathaworncharoen et al. [10], "the power consumption of 6LoWPAN over BLE is one-tenth lower than that of IP over Wi-Fi". Because of these characteristics, 6LowPAN develops a huge market demand when it comes to wireless communication. The 6LowPAN is implemented on the Network Layer and has applications in Automation and Factory Environment. 6LowPAN is also used to accelerate the integration between Bluetooth Low Energy (BLE) and the Internet of Things, among other applications. 6LowPAN is IP based protocol standard, meaning it relies on the IP address for the transmission of data. The 6LoWPAN also supports routing in mesh networks assisting the mobility of the nodes in these networks.

2.1.3 WiMAX and IEEE 802.16

Worldwide Interoperability for Microwave Access (WiMAX) certifies and promotes the compatibility and interoperability of broadband wireless products based on the IEEE Standard 802.16. It is designed as wireless broadband access technology. WiMAX can support up to 1 Gigabytes per second of speed. This makes WiMAX one of the most commonly used Wireless Communication technologies across the world for long-range communication. These technologies are implied on the PHY and Medium Access Control (MAC) layers. WiMAX now supports machine-to machine (M2M) applications, which further strengthens its stature as a common wireless communication technology. It introduces enhancements to Medium Access Control (MAC) which, enables lower power consumption at the communication device. Typical application areas for IEEE 802.16p are applications for observation and control purposes. [2]

2.1.4 Bluetooth

Bluetooth is a very common modern-day wireless communication standard. Bluetooth technology interface can be integrated into mobile phones, car hands-free sets, navigation systems, etc. for short-distance wireless data transmission. Bluetooth devices emit signals with a unique Media Access Identification (MAC-ID) number that can be read by Bluetooth sensors within a given area. This range of Bluetooth signal transmission varies for different versions. Bluetooth is also famous for its near-perfect interoperability which includes the ability to define profiles and device objects, just like ZigBee technology. Bluetooth can be used in a sensor-receiver pairing for a number of in-door applications. The receivers at random locations are used to identify the movement of the devices with sensors on them.
The different versions of Bluetooth over time include classic Bluetooth, Bluetooth 4.0, Bluetooth 4.1, Bluetooth 4.2 and iBeacon which is a product of Apple and is based on the Bluetooth Low Energy (BLE) standard.

2.1.4.1 Bluetooth Low Energy (BLE)

The Bluetooth Low Energy (marketed as ‘Bluetooth Smart’) is a low-cost, low-power wireless communication standard introduced in Bluetooth version 4.0. Just like ZigBee, BLE provides low-cost data communication to various devices. As mentioned in Litepoint [13], this new low energy technology of

Bluetooth supports short data-packages with the speed of 1Mbps. In addition, it supports fast transactions as short as 3ms. Communication between BLE devices is based on GATT (Generic Attribute Profile) and ATT (Attribute Protocol). [3] Advanced versions of Bluetooth have improved security and provide a better speed of data transmission. Also in the later BLE versions, they have tried to resolve problems arising due to interference and better integration with other technologies.

	Zigbee	6LowPAN	WiMAX	BLE
OSI Layer	Network	Network	PHY/MAC	Network
Power Consumption	Low	Low	High	Low
Cost	Low	Low	Medium	Low
Range	~(10-100)m	~20m	~30km	~100m
Applications	Home Automation, Health Care	Automation and factory Environment	Industrial Automation	Retail, Social Networks

(Table 1: Comparing Different Wireless Communication Standards.)

There are a number of other network protocols such as RF4CE, WirelessHART, and 6LoWPAN that use common low layers defined by the 802.15.4 specification. Also a number of proprietary wireless protocols are gaining recognition in the wireless market, such as Z-Wave in applications for home automation and ANT in sports-related products. The market for wireless solutions is still very much divided since there isn't a standard solution that tick all the boxes of market requirement [14].

2.2 LAYERED ARCHITECTURE

While deciding upon the right protocol stack and wireless technology for your IoT implementation is a very important step, system designers also have to make another vital decision regarding the architecture of their IoT structure. The architecture needs to flexible, to accommodate and interconnect the absolutely gigantic number of "smart things" across the internet in a heterogeneous manner. This calls for a layered architecture and more importantly, a common one to be implemented all across the IoT universe. While we are yet to fixate on a single model I have listed down a few of the proposed models for the IoT architecture.

The pool of current proposed models include [5], the relatively common three-layered architecture, the middleware-based architecture, the SOA-based architecture and the five-layered architecture. Apart from these, [16] proposes a Mixed Integer Linear Programming (MILP) model which is an energy efficient four-layered model of IoT architecture. Next I take a look at the different layers and their roles in a typical IoT layered model.

2.2.1 Perception Layer

Typically the lower-most layer is the 'Perception Layer' and it comprises of the physical objects like sensors, used to sense/collect data. Information gathered included the likes of temperature, location and sometimes speed. This layer is also known as the 'Object' layer or 'Device' layer.

2.2.2 Network Layer

The next layer is the 'Network layer' or the 'Abstraction layer'. This layer takes care of the secure transmission of the data gathered by the Perception layer. This layer usually contains of Bluetooth, Wifi,

3G, Zigbee, etc. This is the layer where the IoT gateways are applied to ensure interoperability and smooth interaction with other technology platforms.

2.2.3 Service Layer

The Network layer is followed by the 'Service' layer or as it is also known, 'Service Management Layer' or 'Middleware Layer'. This layer takes care of processing all the data it receives from the previous layer and stores the data. It also connects the gateway service with the Application layer and passes over the processed data. To make up for the lacking flexibility in the previous players, the service layer implements protocols such as 6LowPAN which act as a bridge to many services operating in the IPv6. Here is what [17] has to say about the contribution of this layer "6LoWPAN standard was proposed as a possible method to bring IPv6 to WSNs which made sensor nodes to be natively addressable and connectable through the IP protocol. 6LoWPAN is an important protocol or technology which allows merging of newer and older Web services, and support the IoT interaction paradigm, while still running everything over the Internet infrastructure." Thus the Service layer helps integrate different services to provide further flexibility in the IoT paradigm.

2.2.4 Application Layer

The next layer is the 'Application layer'. The application layer consists of smart user applications and takes care of the management and implementation of these applications in the IoT architecture. Once the data is processed and passed to the applications, this layer deals makes the data available to the end-user. The application layer manages customer interests, for example it provides the temperature readings to the customer or indicates the user location in form of various statistical analysis.

2.2.5 Business Layer

The final layer is the uppermost 'Business' layer. This layer takes care of building business models for the IoT architecture and also design business strategy for further use. It manages the data received from the previous layers and uses it for building the business model [16]. Apart from the business model, the 'Business layer' also monitors and evaluates the data it receives to enhance the services provided by the IoT architecture.

3. IoT PROTOCOLS

Keeping in mind the importance privacy and security hold in the world of IoT, I have segregated the major aspects for IoT into these: Connectivity, Security, Privacy, Interoperability and Standardization. The IoT protocols can be classified or differentiated based on several criterions. Resource-rich and resource-constrained, IP-based and Non IP-based, broker-based, message queue oriented and web service based. There are many existing IoT protocols like CoAP, SOAP, REST, AMQP, MQTT, XMPP, JMS, etc. currently used for different application. In this section I introduce as well as compare a few of them.

3.1 REST

Representational State Transfer (REST) is a service oriented architectural protocol. The REST protocol is based on various "resources". Resources uniquely identified through Uniform Resource Identifiers (URIs).

These resources provide access to data via GET and accept inputs via PUT. RESTful services, as they are known are Web Services that are preferred for tactical scenarios and ad-hoc integration in contrast to other web services [1]. RESTful services are widely regarded as user-friendly protocol compared to other Web Services. REST protocol uses much lighter Web implementations to ensure that IoT application development is as effortless as possible. RESTful Web Services have many advantages over other Web Services such as statelessness, lesser parsing complexity, less overhead, and tighter integration with HTTP. But, in terms of security and QoS (Quality of Service) requirements other web services offer a much better competition [2].

In a typical REST request, the client discovers a service by browsing or crawling its HTML representation. The client then sends an HTTP call to this service with a given verb (GET, POST, PUT, etc.), a number of options, and a payload in the negotiated format [19]. Since they are web based services, RESTful applications and Web Services protocols are often compared to each other. REST is considered better in terms of accessibility and ease of use, but can be overlooked when security is a clinical concern. Yazar et al. [20] compare the performances of Web Services architecture and RESTful applications by deploying them each on wireless sensor nodes with limited resources and reach a conclusion that REST comes out on top among the two.

3.2 CoAP

CoAP stands for Constraint Application protocol. In many ways, CoAP model is similar to HTTP's client-server model. There are a few differences though. CoAP is designed to use the RESTful features of HTTP protocol but in a way that suits constraint environments. Also CoAP runs on the unreliable UDP unlike HTTP and REST, which usually run on the very reliable TCP protocol. Since CoAP operates on UDP, it does not store any state information about the connection during communication. One of the main advantages of CoAP over HTTP and REST, and why it fits the IoT requirements perfectly is its ability to work with lossy and noisy links. Also low power consumption makes it very easy to choose over other protocols.

CoAP is basically divided into two separate layers in structure. A messaging layer used to deal with UDP and the asynchronous nature of the interactions, and a request/response layer for communication using Method and Response Codes [18]. The messaging layer of CoAP operates over the UDP protocol where messages are transmitted between endpoints. The messages are of four types in CoAP, namely: Confirmable message (CON), Non-confirmable message (NON), Reset Message (RST) and Acknowledgement Message (ACK). The Confirmable messages (CON) are to provide extra reliability in CoAP. The Acknowledgement Messages (ACK) are tracked by the Message Identifier which is unique for every message sent or received. When the extra reliability is not required, the Non-Confirmable Messages are used, which still have the Message Identifier to avoid duplicates [18].

3.3 SOAP

Simple Object Access Protocol (SOAP) is an important payload container protocol. SOAP is used to exchange structured data over the internet. SOAP messages are in Extensible Markup Language (XML) format and it relies on HTTP and SMTP for message transmission. While one can draw similarities between the CoAP and SOAP protocols, there are features that differentiate these two completely. One major difference between CoAP and SOAP is that SOAP does not operate in real-time, while CoAP is almost

real-time protocol. Also that unlike CoAP, SOAP relies on TCP transport layer rather than UDP for data transmission. This means SOAP can have reliable and store the state of the connection.

Although most of the interactions on the cloud right now are SOAP-based interactions, the RESTful based web services are more preferable to management of lightweight wireless sensor devices, hence the SOAP-REST transformation can be achieved using additional adapters. These adapters can receive the REST service invocation request, and transform it into a SOAP request [21] [22].

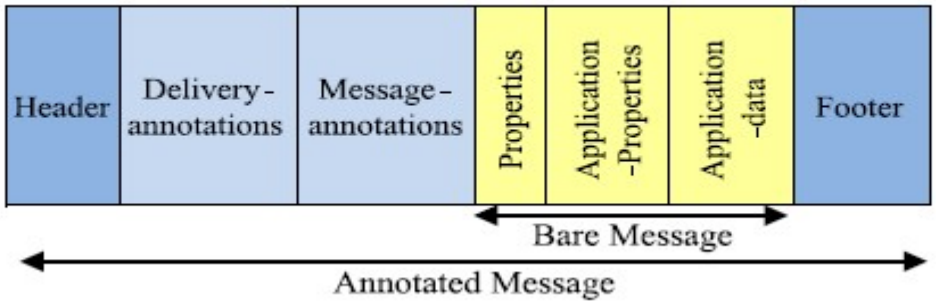
3.4 MQTT and MQTT-SN

Message Queue Telemetry Transport (MQTT) is an open and lightweight publish-subscribe protocol. MQTT transfers telemetry-style data and is designed for mobile and machine-to-machine (M2M) applications. It is a highly optimized protocol, designed to handle intermittent network connections. MQTT is also designed as a low-power and low-bandwidth option. MQTT enables data transfer to small message brokers or servers in constraint environments [23]. MQTT requires an underlying network, such as TCP/IP to operate upon.

MQTT-SN is a revised version of MQTT which is designed keeping in mind the suitability of a wireless communication environment. MQTT-SN has wireless-friendly features such as low bandwidth, high link failures, short message length, etc. It is also optimized for implementation on low-cost, battery-operated devices with limited processing and storage resources. MQTT-SN is designed in a way that it remains unaware of the underlying networking services. Any network which provides a data transfer service between nodes or gateways should be able to support MQTT-SN [24].

3.5 AMQP

AMQP stands for Advanced Message Queuing Protocol. AMQP is another publish-subscribe messaging protocol like MQTT. AMQP is open, and provides flow-controlled communication with guaranteed message delivery [2]. Similar to MQTT and MQTT-SN, AMQP requires an underlying transport layer protocol like TCP to operate on and provide reliable service. There are two main communication components in AMQP, 'message queues' and 'exchanges'. Exchanges route the messages to appropriate queues, pertaining to some pre-defined rules and conditions. The messages are stored in message queues and then be sent to receivers [5].
There is a messaging layer explicitly designed to handle AMQP's messaging capabilities. All information regarding the message delivery is contained in the message header.



(Figure 3: AMQP message format [5])

The AMQP message, as shown in the figure above, contains a header, delivery annotations, message annotations, space for bare message and a footer. The bare messages are supplied by the sender and contain application properties and application data.

3.6 XMPP, JMS and DDS

XMPP stands for Extensible Messaging and Presence Protocol. Like AMQP and MQTT, it is a messaging protocol that operates on TCP transport layer. XMPP is XML-based, open and works in near real-time. XMPP is famous for being extensible and being easily able to interact with other objects that are using XMPP. XMPP implements a 'store and push' mechanism that allows the protocol to store data if the other object is unavailable (i.e. in sleep mode) [2]. XMPP waits for the other object to come back online to start communicating again.

Java Messaging Service (JMS) is an international messaging standard developed through the Java Community Process (JCP). JMS is a part of the Java Enterprise Edition (Java EE) and is very widely used as an affective publish-subscribe messaging protocol. In JMS, the communication between different components can be loosely coupled, reliable (because of TCP), and asynchronous. JMS supports both point-to point and publish-and-subscribe style routing. One major drawback of JMS is that it does not define a wired protocol, meaning interoperability with other operators is usually lacking [23].

Data Distribution Service (DDS) is a real-time, scalable and interoperable publish-subscribe messaging standard. DDS, unlike other messaging protocols mentioned here is specifically designed for mission and business-critical purposes. One of the major positives of DDS is that it is language and operating system independent. Meaning major issues arising due to lack of interoperability are not found in this protocol. DDS also has the "Automatic Discovery" feature which enables participating entities to declare their communication information in order to get easily discovered by other participating entities. This information contains details of what they are looking for or what they can provide to other entities trying to interconnect with them. DDS automatically connects appropriate entities then, based on their declared information. . This process significantly reduces the efforts to connect and configure systems with multiple entities trying to communicate with each other [23].

4. INTEROPERABILITY

Beyond the standards and protocols that define the internet of things, we need to take care of other aspects like security and interoperability. Interoperability is a massive challenge in the Internet of Things because of the need to handle a humungous number of heterogeneous devices. These heterogeneous devices often belong to completely different platforms and need to be interconnected. Establishment of interoperability and interaction mechanism between machines and devices mean there needs to be proper communication and understanding among them, across the internet.
IoT interoperability is achieved, to an extent, by the implementation of IoT Gateways. These gateways act as 'bridges' to connect protocols and other services with varied platforms. Achieving interoperability is not a simple task as it requires the gateway to have a lot of power consumption in order to handle the requests and responses. Along with this, the gateways also require to have a very flexible architecture to take the load of all these requests [4].

To deal with diverse nature of devices into existence and tackle the task of interoperability, we take a look at the IEEE 1905.1 standard. The IEEE 1905.1 standard is designed for convergent digital home networks and heterogeneous technologies [25]. The standard includes an abstraction layer which does the job of hiding away the diverse MAC topologies, while not enforcing any significant change in the underlying layers of the architecture. This protocol provides an interface to common home network technologies so that a combination of data link and physical layer protocols can coexist [5].
Interoperability between two devices need to be tested to avoid ambiguities. This can be done through various testing projects. PROBE-IT [5] is one such research project. According to its official website, "PROBE-IT is a two years European project that aims at supporting exploitation of European research advances in IoT deployments. It ensures interoperability and acceptance of validated IoT solutions in a global context" [26].

5. IoT GATEWAYS

IoT Gateways are devices that connect sensor networks to communication networks. They essentially act as a bridge between these networks. As shown in figure 2, the IoT Gateways are included in the 'things world' and connect the network of things to the internet. The structure of a typical IoT Gateway usually includes an IoT bundle layer. It is designed as a layered middleware architecture to provide flexibility. This bundle consists of different layers such as the application layer and TCP/UDP layers. These layers act as the network bridge, provide effective communication, manage the networks and discover devices, handle network unavailability, and link different services or provide offline service [4]. Together, the bundle layer's task is to translate and process the incoming messages to the required format and platform before passing it over to the next step in architecture.

IoT Gateways' main objective is protocol conversion. They take charge of the interoperability issue and help IoT systems to integrate different protocols that belong to different platforms. Another IoT Gateway objective is device management, where the gateway devices control the flow of data from one network to another and manage the parameters of exchange. IoT gateways are devices on the edge of IoT environments, they have processing power and thus are able to process immediately the incoming data. This helps to reduce the bandwidth required to send data to the control center. Being on the very edge of the IoT environment also helps to speed up a response that needs to be sent to a detected event [2]. Processors present in these IoT gateways themselves manage all the communication and control all the applications, without needing external help. IoT Gateways make sure that constraints such as the requirement of a unique identifier to communicate with other devices is eliminated. This is very useful to integrate resource-constraint devices into the internet of things. It makes the scope of IoT a whole lot larger. IoT acts as a protocol aggregator to connect devices using a particular wireless communication standard such as WIFI, to devices using a completely different standard like Bluetooth. The IoT gateways translate messages for different protocols like CoAP or deliver them directly to receiving sensors (Example: ZigBee based sensors).

ZigBee defines ZigBeeGateway Public Application Profiles to help ZigBee standard interoperate with other protocol standards. The ConnectPort X2 [27] is an example of such an application profile. ConnectPort X2 is a ZigBee smart energy certified gateway. The gateway incorporates the ZigBee Smart Energy wireless standard, making it interoperable with non-Digi devices. The ZigBee Smart Energy standard also allows the ConnectPort X2 to define and control what information the device sends over the network [27]. An IoT

Gateway is not just a bridge between two networks but also an intelligent protocol aggregator that distributes various services.

Since IoT is characterized by a large number of connected devices, management of these devices and assurance of interoperability becomes of utmost importance. IoT Gateways make sure there is optimal protocol conversion and processing of request, so that the rest of the IoT environment has faultless interconnectivity and application.

6. IoT APPLICATIONS

With the exponential rise in the number of 'smart' devices and the ever-increasing rate of IoT development, multiple wireless communication standards are fast gaining importance in various applications. These applications are spread in many areas and industrial fields such as healthcare, travel, retail, marketing, social networks, location monitoring and many more. This section takes a look at a few of these applications in detail. To be useful in application environments, these "smart" devices need to be deployed keeping in mind the real-time nature of their applications.

Multiple features need to be considered when the sensor devices are implemented such as the resource management, network environment, usability and also scalability of the application to a larger scenario. These sensor devices are usually tiny, containing trackers and attenuators and sensors. But these are just technical considerations. Deployment of 'smart things' also largely depends on the authorizing government. The government plays a huge role in determining the regulation in regard with the deployment of these systems. This is mainly related to the privacy factor involved with this technology. Although the development of IoT is still in its early stages, there isn't a significant acceptance among its customers, largely because of the privacy and security concerns. Here is very the regulatory authorities issue plans to deal with customer's privacy protection, public security and welfare [22]. These plans and regulations differ from country to country.

The growth of these 'smart things' have led to the development of 'smart grids', 'smart transport', 'smart homes' and even 'smart cities'. While the 'smart homes' have systems installed to monitor the temperatures of individual rooms, 'smart transport' using advanced navigation assistance to achieve safe travel, route optimization to manage long routes and monitoring the delivery with the help of tracking system. 'Smart cities' are pre-planned cities that are highly conceptualized. Many developing nations like America, China, India and Russia have already implemented this concept, and Europe is rapidly showing interest in this booming new concept of smarter and more sustainable cities [22].

Specific standards are developed keeping in mind very specific application domains. Like the ZigBee Cluster Library (ZCL) is specifically developed keeping in mind the application domains like home automation and healthcare [4]. [28] Provides a survey of the IoT for specialized clinical wireless devices using 6LoWPAN/IEEE 802.15.4, Bluetooth and NFC for mHealth and eHealth applications [5]. Healthcare is a very important domain in the IoT application environment, and has several standards like 6LoWPAN dedicate special researches for the domain. Healthcare benefits from the ability to monitor machines and constantly communicate with cloud, giving a whole new perspective to medical research and studying patient behavior.

IoT applications are mainly aimed at improving people's quality of life while saving operational costs for companies. New applications appear every day in every domain of IoT, and so the protocols and standards have to evolve constantly to catch up with the innovation pace of IoT application use-cases.

7. CONCLUSION

In this paper, I have put forward the structure and status of Internet of Things in current environment and the technologies leading to it. I have discussed various IoT protocols in detail. I have addressed the main functionality of these protocols so as to clear the fundamentals of these protocols. I have discussed the need to collaborate all such technologies in order to reach a middle ground where there is a single architecture to be implemented and accepted. More stability in the acceptance of the IoT protocols and the evolution of IoT gateways would be key to make this possible. There is a strong need to implement a horizontal platform architecture in order to achieve multiple domain interoperability. The protocols mentioned in this paper have their share of shortcomings, and they need to be evaluated on a thorough basis before one can try and implement them to build an IoT system. The choice and the combination of the technologies should be based on a good understanding of the architecture and requirements of each system. Next I introduced IoT Gateways to tackle the very important inter-operability problem. Finally, IoT applications are presented to illustrate typical protocol integration scenarios.

Going by the trend and numbers, it is certain that IoT will emerge as a dominating market in the foreseeable future. IoT is perceived as a major source of services and application, but still needs to work on features like security, privacy and interoperability to achieve complete success and acceptance. This paper emphasizes on the need to develop an established architecture and maintain an integrative approach when it comes to selection of protocols and architecture. Optimization of the existing protocols is something that requires further development and research. Along with optimization, security and privacy are the main areas where future work needs to be focused on.

14. REFERENCES

[1] Software Platforms for Internet of Things and M2M- *Balamuralidhar P., Prateep Misra and Arpan Pal* Journal of the Indian Institute of Science VOL 93:3 Jul.–Sep. 2013 journal.iisc.ernet.in

[2] A Survey of Technologies for the Internet of Things- Vangelis Gazis, Manuel G¨ortz, Marco Huber, Alessandro Leonardi, Kostas Mathioudakis Alexander Wiesmaier, Florian Zeiger, Emmanouil Vasilomanolakis, Conference Paper, August 2015

[3] Bluetooth Low Energy Based CoAP Communication in IoT CoAPNonIP: An Architecture Grants CoAP in Wireless Personal Area Network- NAN CHEN, July/2016.

[4] Protocol and Architecture to Bring Things into Internet of Things Ángel Asensio, Álvaro Marco, Rubén Blasco, and Roberto Casas, Published 13 April 2014

[5] Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications- Ala Al-Fuqaha, *Senior Member, IEEE*, Mohsen Guizani, *Fellow, IEEE*, Mehdi Mohammadi, *Student Member, IEEE*, Mohammed Aledhari, *Student Member, IEEE*, and Moussa Ayyash, *Senior Member, IEEE* IEEE COMMUNICATION SURVEYS & TUTORIALS, VOL. 17, NO. 4, FOURTH QUARTER 2015

[6] Prof. Parth H. Pathak, assistant professor in the Computer Science Dept. at George Mason University. phpathak@gmu.edu December, 2016.

[7] Dave Evans. The internet of things - how the next evolution of the internet. http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf, 2011. Accessed April, 2016.

[10] Varat Chawathaworncharoen, Vasaka Visoottiviseth, and Ryousei Takano. Feasibility evaluation of 6lowpan over bluetooth low energy. arXiv preprint arXiv:1509.06991, 2015.

[11] ZigBee Specification, "ZigBee Cluster Library Specification," (053474r17), 2008.

[12] Y.-F. Lee, H.-S. Liu, M.-S. Wei, and C.-H. Peng, "A flexible binding mechanism for ZigBee sensors," in *Proceedings of the 5th International Conference on Intelligent Sensors, Sensor Networks and Information*

[13] Litepoint. Bluetooth low energy. http://www.litepoint.com/wpcontent/uploads/2014/02/Bluetooth-LowEnergy_WhitePaper.pdf, 2014. Accessed April, 2016.

[14] Bluetooth 4.0: An introduction to Bluetooth Low Energy—Part I. Mikhail Galeev, Z-Focus Consulting, July 2011.

[15] Philip N Howard. Sketching out the internet of things trendline. http://www.brookings.edu/blogs/techtank/posts/2015/06/9-future-of-iot-part-2, 2015. Accessed April, 2016.

[16] Virtualization Framework for Energy Efficient IoT Networks. Zaineb T. Al-Azez, Ahmed Q. Lawey, Taisir E.H. El-Gorashi, Jaafar M.H. Elmirghani School of Electronic & Electrical Engineering University of Leeds Leeds, United Kingdom.

[17] A REFERENCE ARCHITECTURE For IoT. Nupur Tyagi Computer Science, Delhi University, New Delhi, India

[18] The Constrained Application Protocol (CoAP), Internet Engineering Task Force (IETF)- C. Shelby , ARM, K. Hartke, C. Bormann. Universitaet Bremen TZI, June 2014.

[19] D. Guinard, I. Ion, and S. Mayer, "In search of an internet of things service architecture: Rest or ws-*? a developers' perspective," in MobiQuitous, 2011, pp. 326–337.

[20] Dogan Yazar and Adam Dunkels. E_cient application integration in IP-based sensor networks. In Proceedings of the First ACM Workshop on Embedded Sensing Systems for Energy-E_ciency in Buildings, page 4348, Berkeley, CA, USA, November 2009.

[21] X. Hu, T. H. S. Chu, H. C. B. Chan, and V. C. M. Leung, ``Vita: A crowd sensing-oriented mobile cyber-physical system,'' *IEEE Trans. Emerg. Topics Comput.*, vol. 1, no. 1, pp. 148_165, Jun. 2013.

[22] Recent Advances in Industrial Wireless Sensor Networks Toward Efficient Management in IoT ZHENGGUO SHENG1, (Member, IEEE), CHINMAYA MAHAPATRA, (Student Member, IEEE), CHUNSHENG ZHU, (Student Member, IEEE), AND VICTOR C. M. LEUNG, (Fellow, IEEE). June 1, 2015.

[23] A. Foster, "Messaging Technologies for the Industrial Internet and the Internet of Things - A Comparison Between DDS, AMQP, MQTT, JMS, REST, CoAP and XMPP". Version 2.0, 2015.

[24] Stanford-Clark, A.S., and Hong Linh Truong. "MQTT for sensor networks (MQTT-S) protocol specification." (2008). http://mqtt.org/MQTT-S_spec_v1.1.pdf

[25] *IEEE Standard for a Convergent Digital Home Network for Heterogeneous Technologies*, IEEE Std. 1905. 1-2013, pp. 1–93, 2013.

[26] http://www.probe-it.eu/

[27] ConnectPort X2 ZigBee Smart Energy Certified IP Gateway - Datasheet http://www.mouser.com/ds/2/111/digi%20international_ds_connectportx2se-543401.pdf

[28] P. Lopez, D. Fernandez, A. J. Jara, and A. F. Skarmeta, "Survey of Internet of Things technologies for clinical environments," in *Proc. 27th Int. Conf. WAINA*, 2013, pp. 1349–1354.