International Journal of Latest Engineering and Management Research (IJLEMR)
ISSN: 2455-4847
www.ijlemr.com || Volume 02 - Issue 04 || April 2017 || PP. 25-37

Wireless Routing Protocols for Internet-of-Things (IoT)-A Survey

Vidya Rao[1], Vallabh Mahale[1], G G Sivasankari[1], Venugopal K R[2]
[1](*Department Computer Science & Engineering, AMC Engineering College, India)*
[2](*Department Computer Science & Engineering, University Visvesvaraya College of Engineering, India)*

Abstract: The innovative growth in the field of wireless technology makes the entire globe to be connected with Internet-of-Things (IoT) i.e. Internet-of-Everything. The outcomes of research in wireless technology support different protocols and strategies. There is a need for standard architectural design in such network to meet the global standards and requirements. The most important objective in Internet-of- Things is to design intercommunication protocol for different devices and dynamically support the scalability issues. This survey describes the various research directions, IoT applications, layered architecture, fusion of IoT in the field of sensor networks, with routing requirements and challenges faced in Internet-of-Things.
Keywords: Internet-of-Things (IoT), Layered Architecture, Wireless Routing Protocols.

1. Introduction

The unpredictable growth of wireless technology leads to huge network of devices from different vendors of various countries. One of the most important task of Internet of things is to provide reliable services on a scalable network. In the coming era of wireless technologies, we can expect billions and trillions of devices across the worldwide to form a huge undeterminable network. Devices from many vendors across hundreds of countries will appear on the IoT completely unimaginable and is unpredictable. The greatest research challenges are providing secure and scalable network services along with energy efficient communication in the heterogeneous environment.

At the advent of wireless technologies, the first internet-connected smart device was initiated at Carnegie Mellon University in the year 1982 by maintaining a coke machine which sells coke bottle around the campus. Later in 1994, Reza Ragi [1] proposed that IoT includes moving of small packets of data to a large set of nodes and this integration and automation of everything from home appliances to industry is possible. In 1998 Ragi presented a document on real-time web-based IoT, which enable to remotely controlling and monitoring home devices by interfacing camera and special web pages.

Similarly series of solutions are proposed by various companies like Microsoft, NEST etc. to solve the issue related with connecting every object around us. In 1999, Bill Joy [2], developed "Six Web Framework" which includes "the Near Web, the Here Web, the Far Web, the Wired Web, the Business-to-Business (B2B) and lastly The Device-to-Device (D2D)" [3]. Among these networks, D2D was adaptable to the existing internet infrastructure and provided maximum network throughput. Joy described D2D as a collection of self organizing sensors connected over a mesh network and communicated through Internet. This network enabled the administrator to manage, monitor and control the network remotely. But Joy failed to justify his arrangement for a multiple device communication.

Later, in early 2000s a British Entrepreneur, Kevin Ashton introduced Radio Frequency Identification (RFID) based IoT at his MIT Auto ID Labs [4]. Ashton observed that RFIDs information can be linked to Internet through sensors and actuators. He visualized IoT as RFID and sensor technology enabled computers to handle data transmission and reception without human interference. The due course of research, Ashton failed to address the issue pertaining to cost effective adaptability of these large number of devices over the existing internet infrastructure. To address the above issue, IoT sprouted by integrating and processing heterogeneous information like sound, light, electricity, mechanics, heat, chemical, location, etc.

Since the concept of IoT was introduced in 2005, the evolution of sensor era, saw the development of smart network enabled objects with device integration, Artificial Intelligence supported systems and other capabilities of devices started communicating each other for the numerous applications such as agriculture, defense, smart buildings, weather forecasting, mechatronics and robotics, transportation, healthcare and Social networking etc.

Internet of Things (IoT) otherwise called as Internet of Everything is an electronic network of physical objects embedded with sensors and software to enable the objects to communicate with the manufacturers, operators and other connected devices based on the infrastructure of Internet.

IoT has various sensing devices such as RFID, sensors, gas indicators, laser scanner, Global Positioning System (GPS) and infrared sensors, etc. These devices are used over has wide range of application

ranging from hospital management, agricultural field monitoring, developing smart cities and connecting every object under the sky as given in Figure 1.shows the arrangement of devices for multiple applications support.

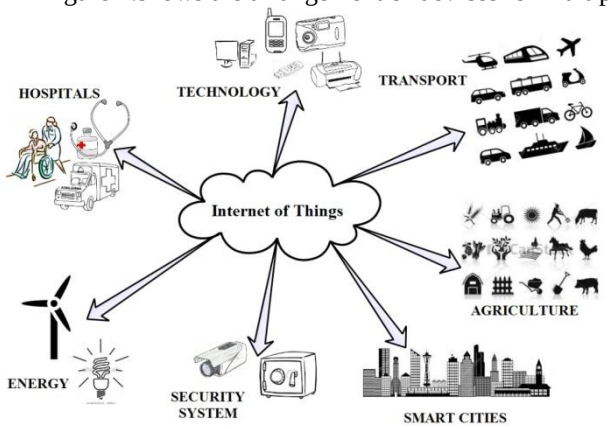

Fig 1. IoT Environment Connecting Various Applications

In an IoT environment every sensor device is provided with Unique Identification Number (UIN) which helps in communication among the end users. As per US National Intelligence Council in 2025 IoT can connect everything in our life. Some of the features of IoT are;

- Connect both inanimate and living things
- Use sensors for data collection or gathering
- Converts the raw data into meaningful information and are communicated
  Activities of every object can be analyzed.

2. Future Trends and Research Directions for Internet of Things

Business forecast experts has proposed that more than 220 exabytes of data is going to be processed over internet by 2020. Henceforth the wide spread IoT has predicted four major trends [5]. Primarily, "Data Swamp", huge amount of data is collected and exchanged between various devices. As the existing network are incompatible for this exponential traffic growth, it is essential for all the users to rethink over network architecture and storage models. Secondly, the energy consumed by all IoT device is reduced through replacing in-exhaustible energy resource with self charging batteries. Next comes the minimizing the size of these devices to increase the ease of placing them in various regions.

Lastly, most important task is to more towards automatic resource management. To manage the growing complex system, devices should poses self management, self-healing and self configuring properties. Some of the major research challenges are discussed below:

2.1 Architectural Dependencies

IoT comprises of trillions of various technologies involving smart device with sensors like cameras, biometric devices, physical and chemical sensors. It is essential to design a scalable and efficient architecture to provide a reliable and dynamic communications among these inter connected devices. As IoT integrates data over different environments, it becomes difficult to have standard reference architecture. Having a single reference architecture cannot suffices all possible solution for such an enormous amount of data from various sources. Hence it is advisable to have heterogeneous reference architectures which do not restrict users to use fixed end-to-end solution. Therefore it is essential to design an architecture that is flexible to all technologies like RFIDs, Intelligent devices and smart objects.

2.2 User Privacy & Data Security Challenges

Massive amount of important data are communicated over internet; IoT holds two types of sensitive data they are, personal data (consumer driven) and big data (enterprise-driven). Hence it is essential to provide privacy for consumer data and security for enterprise-driven data. The privacy of individual's information leads to major research issue under IoT. To secure the personal data of individual, set of privacy policies are framed for each domain. Similarly, the security issue is exacerbated because the existing security architecture is designed from perspective of human communication. It leads to easy tampering of devices and data by various attacks. To meet realistic security requirement, IoT application must be able to continue to operate satisfactorily in presence of attacks. To overcome such attacks, new solution like downloading new codes that detect the attacks, diagnose the attack and exhibits countermeasures to repair themselves. But most of today security

protocols includes heavy weighted computations and requires large memory space and thus security solutions for IoT are major research challenges.

2.3 Openness

Conventionally, the sensor based application systems are closed system. Examples are car, aircraft, ship and smart cities have networked with sensor operates within the predefined area. As the application domain grows, cars can talk to each other and will be able to control collision; aircrafts can able to communicate with control systems from any part of world and people can exchange their data automatically even before they meet up. But these applications are spreads on wide dimensional area; it needs for an openness of the network. However, supporting openness creates many new challenges like complexity of different objects, feedback control system and robust performance. The other important challenge of openness is constantly changing infrastructure which leads to difficulty in scaling and analyzing the interactions within the network that creates a need for decentralized control system.

2.4 Robustness

The main objective of IoT is to efficiently connect every object around us which can sense, process and communicate among each other i.e. objects can talk among themselves. To establish such an environment each object in the network must possess knowledge with respect to their (i) location, (ii)neighbors information, (iii)obtain pair wise security keys parameter, (iv)synchronize the clocks, (v)power levels. These parameters are deteriorated with time, for example problem with synchronous clock, movement of nodes, energy drains, physical wear & tear. To achieve the coherent services, IoT combines with many other methodologies to produce robust system operation. This includes dynamic fault tolerance, reliable code implementations, in-situ debugging technique, on field monitoring and general health analysis services. These problems are aggravated due to unattended operations of system and thus it becomes a major task to include robustness to provide lower noise and fault tolerance in the network.

2.5 Big Data

In IoT paradigm Data is termed as *Gold* since it is a vital component. There are two types of challenges they are multimedia data and log files from sensor nodes. By the evolution of the Internet of Things towards connecting many devices together leads to many challenges and requirements. As per the Big Data are concern The major challenges are collecting, analysis and retrieval of data in these devices includes:

- High scalable environment for the data storage
- Enormous storage capacity
- Good computing power
- Data preservation and transformation
- Searching and retrieval of data
- Higher real-time guarantee for data processing
- Support of cloud computing environment for Big Data
- Transparency, Availability and Privacy of Big Data

Data collected from the sensors are in analog form and it has to reach the users in human readable format. Hence data mining techniques are expected to provide the creation of knowledge from all the data. Uncertainty in data interpretation cause user to lose trust over the network and thus data analysis over big data is important. Another major challenge of IoT data set is availability of knowledge.

2.6 Data Context

Designing context data has become a critical role as it is essential to provide meaning for the sensed data. Hence it is required for IoT infrastructure to consider functionality process for various data context aware services. As these wireless devices store huge amount of assorted data [3], the major challenge is to convert raw data into useful information as:

- Ontology-based models for complex data
- Semantics of context data
- Event-Driven Architecture
- Web-service –based context aware systems
- Context-aware services

In course of time researchers have implemented various prototypes, systems and solutions using

context-aware computing techniques. Finding universal solution for IoT is difficult as it is not feasible to process all the data collected by those sensors. Therefore, context-awareness plays a major role in deciding which data need to be processed.

2.7 Manufacturing and Interoperability

The manufacturing industries are getting more excited about the future possibilities of sensor, equipments, machines, softwares, public and personal devices. But these manufactures have major hurdles regarding interoperability of these devices among internet enterprises. The biggest challenge for manufacturers is to compete with the growth of data.

As we know each object over IoT have been provided with unique identification tag, it is primary requirement that these tags must be portable to any protocol and platform to operate at different frequencies and architecture. According to Stanford University, the internet is generating around 1,200 exhabytes of data per year. Wherein future it is expected to generate data at the rate of 40\% higher every year. Hence developing infrastructure for handling this huge data becomes a challenge for these manufacturers.

2.8 Lack of Universal Governance

Another important issue is widespread adoption of the Internet of Things is not under any government bodies. It is difficult to have impartial governing authority that can initiate IoT in all states, companies, trade and common people. Many companies are implementing wearable devices that help parents to track their infants, doctors can remotely monitor patience health and farmers can control various activities at their farm. But industries are restricted in their practice as there is no global governance to approve the implementation of IoT. According to industries, by 2020 approximately 3 trillion objects can be connected over internet that in turn produces double the data generation. But these productions may be fewer benefits for industries as adoption of IoT at government level becomes difficult.

2.9 Battery Lifetime

In any sensor enabled network posses an important challenge of maximizing their network lifetime. As each IoT devices are imbibed with number of sensors, these sensors consume energy for various tasks like reception, transmission and processing of data. As these devices are battery powered devices, the IoT can become a true reality only if sensor battery life becomes long enough. If batteries are drained off implementation of IoT become waste and thus it becomes difficult task to replace batteries across wide area. It is a major task for researchers to embedded efficient and compact energy storage components like fuel cells, polymer battery, solar cells, piezoelectric elements and thermoelectric elements to convert heat energy, light and vibrations into electricity.

2.10 Standardization of IoT

As IoT works with many sensor devices over a large ad-hoc environment interoperability and integrity issues need to be designed with new standards to support all kinds of infrastructures. The major existing standards such as Electronic Product Code (EPC), ISO/ IEC 18000 and IEEE 802.15.4 (Zigbee) can be used to design new avenues in IoT standardization. The design paradigm requirements and challenges are given below:

(i) ***Research Perspectives***

a. Electromagnetic spectrum frequency band selection
b. Individual coding standards for encoding calibrations
c. Universal protocol design
d. Security, availability, integration and reliability standards support.

(ii) ***Data Content Perspective***

a. Data format standards
b. Standards for public services
c. Productivity and manufacturing standards
d. Middleware support/ Third party vendor support standards
e. Data transmission standards.

(iii) ***Technology Enhancement Perspective***

a. Device Integrity
b. Data Integrity
c. Conceptual to reality based model and infrastructure standards.

3. Applications of Internet of Things

The term *Things* in IoT can be referred as blend of various embedded devices such as automobile built-in sensor, home automation, health monitoring, biochip animal tracker, filed operation devices to assist the fire-fighter in search and rescue operations.

3.1 Health Care Assistance

IoT enables the doctor to monitoring patient health by keeping track of patient's body temperature, heartbeat, blood pressure, etc., through sensors and other integrated gadgets [6]. These data are automatically collected and transferred to doctor using wireless networks and therefore computational time is reduced, error free data is collected and frequent auditing of patient.

3.2 Traffic Monitoring

One of the major problems in big city is traffic management [7]. Traffic congestions and accidents are the causes of traffic jam that leads to huge waste of time, property damages and environmental pollution. Omar et al., [8] has presented a solution for these traffic problems. He has proposed an architecture that combines IoT objects with agent technologies into a single platform. These agent technologies communicate with numerous heterogeneous highly distributed and decentralized devices in the IoT. In this architecture all the objects are tagged and queried using existing networks like RFIDs, object-ad hoc networking, wireless sensor and internet based information system.

3.4 Home and Personal Tracking Gadgets

In home automation, IoT takes an important share by remotely connecting and controlling various gadgets like air-conditions, refrigerator, washing machines, ovens, etc that helps in energy management. Through smart home design it is possible to monitor age old people's activities and health conditions. Sean Dieter et al., [9] has proposed an IoT based monitoring system for controlling domestic appliances by means of low cost ubiquitous sensing system. They designed an architecture using ZigBee technology to track and control the domestic objects of IoT.

3.4 Business Enterprise

Evolution of smart environment like cities, workplace, retail shops, transport, water management, so on, has lead to smart business. Hence sensors have become an integral part of the factory setup to monitor inventory, security implementation, analysis of climate, object detection. All these objects in such an environment is connected using IoT. Hence, IoT has its wide application in social and economical growth of a country.

3.5 Food and Agricultural Environment

Food and agricultural industries are spread on a wide area with complex operational process that needs to be monitored on a regular note. Integrating IoT into food and agricultural environment improve the operational efficiency, quality of products and avoids public food safety.

4. The Element of IOT in Sensor Networks

The prologue development of sensor networks is the most fundamental part of the IoT. A sensor network system embodies one or more sensor hubs, which communicate between themselves utilizing wired and remote innovations. In sensor systems, sensors can be like and alternately alike. Different sensor systems can be associated together through distinctive advancements and conventions. One such way is through the internet.

The parts and the layered structure of a normal sensor system are as per the following. Not with standing, there are different advancements that can supplement the detecting and correspondence foundation in IoT standard, for example, customary specially appointed systems such as Ad- Hoc systems. These are obviously an alternate innovation from sensor systems and have numerous shortcomings.

There are three primary architectures in sensor systems based on number of levels, level building design in which information exchanges from static sensor hubs to the sink hub utilizing a multi-hop form, two-layer design which has more number static sensor and portable sink hubs that being are connected to gather information from sensor hubs and three-layer building design, numerous sensor systems are associated together over the internet. Along these lines, IoT takes after a three- layer building design. The greater part of the sensors connected today are remote.

There are a few noteworthy remote innovations used to fabricate remote sensor systems, wireless personal area network for example bluetooth, wireless local area network for example WiFi, wireless metropolitan area network for example WiMax, wireless wide area network for example 2G and 3G,

furthermore, satellite system, for example, GPS. Sensor systems likewise utilize two sorts of protocols for communication, non-IP based, for example, Zigbee and sensor-net and IP-based conventions for example nano-stack, phynet and IPv6.

The sensor system is not an idea that developed with the IoT. The idea of a sensor system and related examination existed quite a while before the IoT is presented. In any case, sensor systems are utilized as a part of constrained areas to accomplish particular purposes, for example, environment observing, farming, medical consideration, event identification, structural health observing and so forth. Further, there are three classes of sensor systems that include the IoT, body sensor network systems, object sensor network systems and environment sensor network systems.

A common structure of a sensor arrangement embodies the most well- known parts in a sensor system. Information is produced by the low end sensor hubs and top of the line sensor hubs. At that point, information is gathered by portable and static sink hubs. The sink hubs send the information to low end computational gadgets. These gadgets perform a certain measure of handling on the sensor information. At that point, the information is sent to top of the line computational gadgets to be handled further. At last, information achieves the cloud where it will be shared, put away and handled fundamentally. Taking into account the capacities of the gadgets included in a sensor system, as recognized six layers. Data can be prepared in any layer. Capacity implies the preparing, memory, correspondence, and vitality limit. Abilities to increment from layer one to layer six. Taking into account our recognizable proof of layers, it is obvious that a perfect framework ought to comprehend the capacity contrasts and perform information administration as needs be. Well it is all about effectiveness and viability.

For instance, performance handling in the initial few layers could diminish information correspondence. In any case, gadgets in the initial few layers don't have an adequate measure of vitality and handling energy to do extensive information preparing. Sensor Network and the IoT. In prior segments we presented both IoT and sensor system ideas. In this segment we clarify the relationship between the two ideas. Already, we contended that sensor systems are the most fundamental segments of the IoT cause it includes sensors and actuators. The information is gathered utilizing sensors. At that point, it is handled and choices are made. At long last, actuators perform the chose activities.

The comparison between sensor networks and the IoT is to a great extent unexplored and obscured. We can expand a percentage of the attributes of both sensor networks and IoT to distinguish the distinctions. Sensor network contains the equipment, sensors and actuators, firmware and a slim layer of programming. The IoT contains everything that sensor network includes and further it embodies a thick layer of programming, for example, middleware frameworks, structures, APIs and numerous more programming segments. The programming layer is introduced crosswise over computational gadgets and the cloud. From their source, sensor networks were planned, created and utilized for particular application purposes, for instance, recognizing shrub fire. In the good old days, sensor systems were to a great extent utilized for checking purposes and not for incitation.

In contrast, IoT is not centered on particular applications. The IoT can be clarified as a universally useful sensor network system. Consequently, the IoT ought to backing numerous sorts of applications. Amid the phase of conveying sensors, the IoT would not be focused to gather particular sorts of sensor information, rather it would convey sensors where they can be utilized for different application areas. Case in point, organization might convey sensors, for example, weight sensors, on a recently assembled scaffold to track its basic wellbeing. On the other hand, these sensors may be reused and associate with numerous different sensors in request to track movement at a later stage. In this way, middleware arrangements, systems, and APIs are intended to give nonexclusive administrations and functionality that are needed to perform correspondence in the middle of sensors and actuators viably. Sensor systems can exist without the IoT. Notwithstanding, the IoT can't exist without sensor networks, in light of the fact that sensor network gives the dominant part of equipment.

5. Architectural Design for Internet-of-Things

Designing an adaptable architecture for all platform of IoT is a major challenge. For Connecting every object under IoT raised major issues pertaining to reliability, scalability, security and semantic representation of data in the heterogeneous objects. To overcome these issues, researchers proposed a dynamic global infrastructure that provides self organizing capability among the objects. But to setup an IoT environment there are three phases: (i) installation phase of sensors in the field, (ii) RFID transmission and reception phase and (iii) storage phase. Researchers have proposed few layered architecture to increase the flexibility and to bind all data models, interfaces and protocols together.

5.1 The 5-Layer Architecture of IoTs

The 5-layer architecture of IoT is built on the existing TCP/IP architecture and it consist of five layers namely, (i) Perception Layer, (ii) Network Layer, (iii) Transport Layer, (iv) Data Processing layer and (v) Application Layer as given in Figure 2. The 5-layer architecture helps in binding all data model, interfaces and protocols to support heterogeneous system [10], [11] and [12].

5.1.1 The Perception Layer

The functionality of perception layer is to collect information from physical objects are situated in various networks like RFID, GPS and sensor networks etc. Perception layer consist of three types of nodes they are: sensing nodes, actuator nodes and coordinator nodes. The interactions between these nodes are as followed,

- Physical objects collects the data periodically.
- Coordinator node transmits the raw data through network.
- Control instructions are framed and sent to actuators over the network.
- At actuator node, the control instructions are executed and respective actions are performed.

5.1.2 Network layer

The second layer of IoT architecture is network layer. This layer establishes connection among all the network devices and assign them a individual IP address. The network layer uses Internet Protocol Security [IPSec] to provide integrity, confidentiality and authentication of data. It also uses Internet Protocol version 6 (IPv6) that provides functionalities like

- Data addressing
- Routing data to correct destination
- Translating logical address into physical address.

5.1.3 Transport Layer

The next upper layer is Transport layer. Its objective is to ensure the reliable communication. As we know that in sensor networks energy consumed during transmission and reception is more when compared with energy consumed during data processing, thereby it is essential for these sensor object to exhibit sleep and awake phases during transmission of data packets to the gateway. Transport layer uses TCP and UDP protocols for performing reliable communication. It also enables header compression, packet fragmentation, reassembling and edge routing. The major task of transport layer is to:

- *Addressing:* each object in IoT is mapped to only one address in the digital world.
- *Network Integration:* multiple heterogeneous terminals are integrated over a large scale.
- *Resource Management:* efficient resource utilization is achieved by designing good network topology.

5.1.4 Data Processing layer

Data processing layer concentrates on data formatting and schematic understanding of gathered data. Functions of processing layer is storing, analyzing, querying and mining the data. This layer uses ubiquitous computing, cloud database storage and intelligent processing to handle large volume of data.

5.1.5 Application Layer

Application layer aims to converge between the IoT social needs and industrial technology. It is located at the top of layered architecture, providing a variety of IoT applications such as monitoring the status of things, Operational control, public enquiries and other value added services to use, interconnection and collaboration service between things and things. Once the sensed data is analyzed and processed, application layer use these data to provide to the users. Application layer is to define different business strategies of IoT application like charges and management. It also renders services based on information obtained through analytics, security protocols, processing models and management devices.

5.2 The Cross Layer Reference Architecture Model

In the layered approach, each layer provides services only for their neighboring layers [13]. From Figure 3, physical layer consists of physical objects/devices from various networks like sensor network, GPS, RFIDs, etc. To setup a IoT network, all devices must communicate directly or indirectly with the Internet. For instance to have direct internet communication, Intel Galileo, Arduino, Raspberry Pi uses Ethernet or Wi-Fi. For indirect communication with internet, ZigBee, Bluetooth etc, uses ZigBee Gateway or Mobile phones.

Physical layer communicates to transportation layer through Gateway. At the transportation layer a communication path is established using TCP/IP or UDP protocols. At the application layer client system can

communicate with the server using HTTP/HTTPS (and RESTful protocol), MQTT 3.1/3.1.1 and Constrained Application Protocol (CoAP). These protocols service the request sent from client via web portal or APIs.

Device manager layer can provide cross functional services to all the layer. It has two major components: server side system and device side services. At the server side system communicates with the devices via various protocols and provides both individual and bulk control of devices. At the device side, various software and application are managed. It locks and removes the devices if necessary for various security constraints.

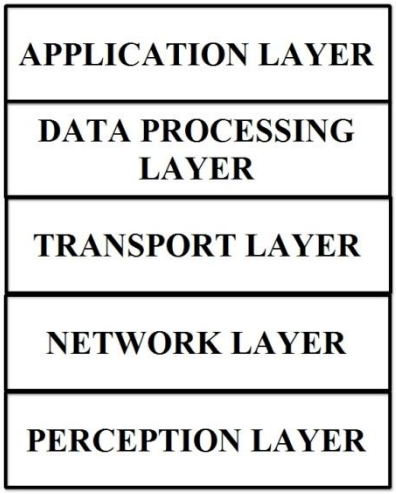

Fig 2. The 5-Layered architecture

The Device Manager works in conjunction with the device management agent. There are multiple different agents for different platforms and device types. The Device Manager also needs to maintain the list of device identities and map these into owners at the physical layer. It must coherently work with the User Identification (UID) Management layer to manage access control over device's privileges for example, who all can manage the device apart from the owner, how much control the owner has against the administrator, etc.

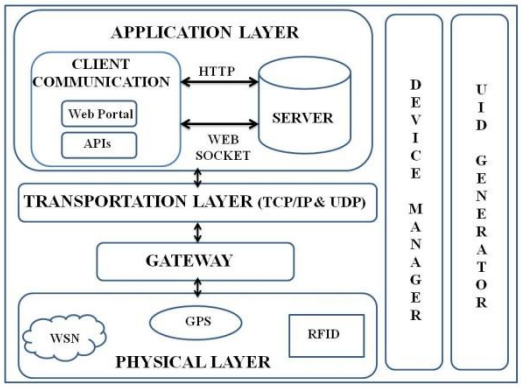

Fig 3. IoT Cross Layer Reference Architecture

6. Fusion of IOT Into Wireless Sensor Network

Wireless Sensor Network consists of tiny heterogeneous inexpensive autonomous devices equipped with sensors that can process and communicate the sensed data among each other [5] [10]. The purpose of connecting WSN with IoT is establish interaction between environment around us at the multiple levels like social, cultural, business and educational. These environments are connected to IoT using smart phones, laptops, tablets, internet TV, routers, desktops through a unique identification number for each device.

Sensor networks are normally centralized networks where there is a central node called sink and it is in-charge of gathering the sensed information from the sensors. The sensors collects information from physical environment like temperature, humidity and proximity that are converted and stored. However, there have been important advances in electronic, micromechanical and chemistry manufacturing processes that make possible to find more sophisticated sensor nodes.

The main characteristic of WSN is the limited resources available in terms of memory and battery power. WSN nodes are fed by batteries so power consumption is an important design factor in WSNs. To solve the battery issues, nodes should transmit their sensed data to the sink node efficiently. Consequently, the majority of routing and MAC protocols for WSNs are focused on reducing the node's power consumption in order to extend the lifetime of the network and to avoid frequent battery replacements.

In general, nodes are static in WSNs, so topological changes are due to bad performances of nodes, i.e. low battery problems or medium accessibility problems. Peer-to-peer (P2P, also known as mesh), Star and Tree topologies are common topologies found in deployed WSNs, see Figure 4. In star topology the nodes are normally located at only one hop distance from the sink so redundant data can be collected from different sensors. The sink is in charge of post-processing such information. In both mesh and tree topologies multi- hops communications take place.

Several algorithms based on graph theory have been proposed to reduce power consumption such as minimum Connected Dominant Set (CDS) or minimum Spanning Tree. As the data is post-processed by sinks, they are normally connected to a higher-level network like Internet in order to monitor the network. With regard to IoT, WSNs can be seen in two different ways: (i) Every node is a different entity or (ii) the whole network is an entity accessible through the sink node which has full information about the network. This point of view is very interesting since a WSN can be integrated into more complex networks.

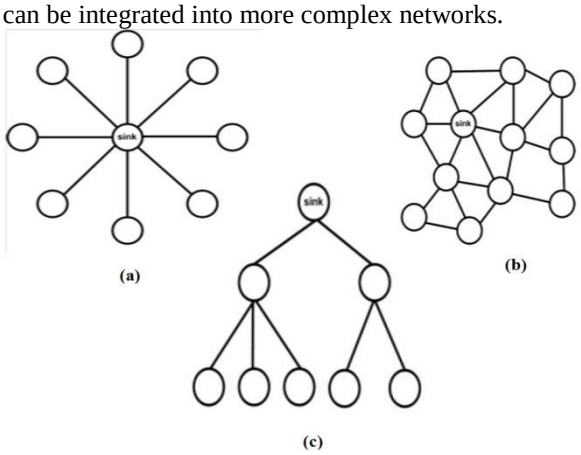

Fig 4. WSN Topologies: (a) Star topology; (b) P2P or mesh topology; (c) Tree topology

A further step in WSNs is the Wireless Body Area Networks (WBAN). These networks rely on the feasibility of attaching or implanting very small bio-sensors inside the human body that are comfortable and that do not impair normal activities. The main application area of WBANs is health care applications. Example, nodes are attached over or inside the human body in order to monitor the health conditions of patient. WBAN makes it possible for the doctors to monitor patient's health in real time, anywhere and at any time.

These sensor nodes are categorized as sensing nodes, actuators and sink. While sensing nodes are capable of sensing the environment, actuators are capable of acting on it and sink nodes gather information from sensor nodes. Wireless Sensing Actuator Networks (WSANs) should not be seen as a mere extension of WSNs since they have their own features. Actuator nodes are more complex and powerful nodes as compared to sensor nodes so a WSAN should not be considered as a homogeneous network with regard to communication flows, there is a significant difference from WSNs. In WSANs multiple sensors may send data to a sink node and multiple sinks may send data to an actuator node. As a consequence, communications can be divided into two types: one-to-many and many-to-one communications. To sum up, the interaction of WSNs with the IoT will enable us to provide more useful services related to real-time data monitoring.

7. Routing in Internet-of-Things

Internet of Things posses various types communication scenarios between Device-to-Device (D2D), Device-to-Distributed Storage System and Device-to-Human and vice versa. It uses either single hop or multi hops communication within the heterogeneous networks [8]. IoT faces various challenges in providing efficient and reliable data delivery among physical objects of the network. In this section we shall concentrate on routing challenges and requirements for an IoT network.

7.1 Routing challenges

Effective transfer of data packet to the destination is referred as routing. To provide such an efficient routing, IoT network encounters various challenges. Few challenges faced during IoT routing is mentioned

below [9].

7.1. 1 Limited Power Resource

Sensor nodes spends their energy for (i) node charging, (ii) storing the data and (iii) converting the data into useful information. Hence conserving the battery becomes a major issue in IoT.

7.1.2 Scalability

As in current era we are able to see more number of devices being added onto the network. It becomes very difficult to have a constant dimension and number of participants connected to internet. Hence scalability of IoT becomes an important task for the manufacturers.

7.1.3 Dynamic Routing Topology

It becomes a difficult task in finding a predefined routing path in IoT as all objects are moving. This dynamic movement of objects shall make or break the communication path resulting in unpredictable routing topology. At the same time objects are scheduled to be idle or working state to reduce the energy consumption which results in routing path selection. Henceforth it is difficult to have a fixed communication path.

Voids and Partitions

Voids and Partitions in the network is another major challenge in the IoT routing. Void is an area that is not connected to the network and the nodes within the void are not connected to any other nodes outside the network. The partition is a disconnected part of network, such that node within the network cannot communicate with nodes outside the network. In such a condition it is hard to construct a routing path. So it is necessary to design the topology such that there is no void and partition been formed.

7.2 Requirements for IoT Routing Protocols

Designing an efficient and reliable routing protocol calls for few basic requirements. In this section we can see some of the requirements that a routing protocol should posses in an IoT environment [9].

7.2.1 Low Packet Delivery Time (PDT)

Delivery time is the time taken for a data packet to travel from its source to its destination; it depends on type of application. For example, a WSN-based forest fire detection application may require that the base station of the WSN receives warnings within a hard time constraint of 3 seconds after the sensed temperature exceeds a certain threshold.

7.2.1 High Packet Delivery Ratio (PDR)

PDR refers to the ratio between the number of the data packets that successfully arrive at their destination and the total number of the data packets that have been sent by their source. The reason that causes unsuccessful delivery is routing loops, which is usually due to a poor routing design. Higher that PDR better is the performance of network.

7.2.3 Low Energy Consumption

As IoT devices usually operate on battery for long time periods (e.g., WSNs to monitor the environment), it is desired that the routing protocol should be aware of the energy status of the network, and acts on that accordingly.

8. Survey on Wireless Routing Protocols for IOT

Routing protocols are broadly classified into Geographical Routing Approaches, Multi-Region Geocast Routing and Stochastic Routing [9]. Some of the wireless routing protocol of IoT is discussed below.

8.1 Depth-First Forwarding (DFF)

Traditional WSN routing protocols find difficulty in balancing requirement of being reactive to topology and channel variation. In the process of topology changes, routing protocols need to re-converge, which may lead to data delivery failure. Hence Jiazi *et al.*, [14] introduced a Depth-First Forwarding (DFF) technique for sensor enabled IoT applications. DFF reacts to the rapid changing of topology and reduces the data delivery failure by providing time stamp. An extension of DFF called DFF++ proposed in order to optimize the performance of DFF with respect to efficient search ordering. The analysis of DFF algorithm is been done by combining DFF with Light-weighted on demand Ad-Hoc Distance Vector Routing protocol next generation (LOADng), Optimized Link State Routing protocol version 2 (OLSRv2) and the IPv6 routing protocol for Low-power and lossy network.

8.2 Multipath RPL protocols (MRPL)

Nien *et al.,* [15] has introduced domestic green house environment monitoring using multipath routing protocol. Through simulation of various versions of multipath RPL (ELB, FLR, ELB-FLR) protocols there is increase rate of packet delivery ratio and decrease in data error received at the base station. But multipath protocol increases the packet delay which leads to failure in better network performance.

8.3 Energy-Efficient Probabilistic Routing (EEPR)

Park *et al.,* [16] presented an Energy Efficient Probabilistic Routing Algorithm (EEPR) to increase the network lifetime. They addressed the issue related to network partitioning and energy consumption by nodes during frequent broadcast of RREQ packets. Hence EEPR algorithm calculates forwarding cost to decrease the packet loss and uses Ad-hoc on Demand Distance Vector (AODV) protocol to reduce congestion in the network. The result is compared between EEPR and AODV protocol which proves that nodes executing EEPR consume lower energy than AODV protocols. Though lifetime of network is increased, EEPR failed to address the issue of delay and packet loss in increased.

8.4 Congestion Avoidance Multipath Routing Protocol (CA-RPL)

Weisheng *et al*., [17] proposed a multipath routing protocol over existing routing protocols of lossy and low power network (RPL) called Congestion Avoidance Multipath Routing Protocol (CA-RPL). The congestion in the network is caused due to poor link quality, large data traffic and packet loss. CA-RPL is able to acquire the knowledge of routing cost that enables it to reduce delay in construction of Directed Acyclic Graph (DAG). There was considerably reduction in packet loss ratio and time delay in CA-RPL than existing RPL. CA-RPL failed to conserve energy in mobile nodes and multi sink nodes.

8.5 Movement-Aided Energy Balance(MAEB)

Haoru Su *et al*., [18] presented a prototype for health case based IoT called Movement-Aided Energy Balance (MAEB) routing protocol. In this protocol each node realizes the trajectory and residual energy of neighboring nodes. After discovering the neighboring nodes information MAEB executes data forwarding algorithm to most suitable neighbor. Using this protocol Haoru Su introduced Wireless Body Area Network (WBAN) architecture for health monitoring application of IoT having ambulatory IoT health Unit and telemedicine system. Ambulatory unit collects vital signals of the user and information if delivered to the Access Gateway (AG) through coordinator nodes. AG transmits the information to the internet from where the telemedicine system can access the information. Experimental results prove that MAEB has high throughput and high packet delivery ratio than Proactive energy Aware OLSR (PAOLSR), Energy Efficient OLSR (EOLSR) and energy metric accuracy protocol (MMPR).

8.6 Least Path Interference Beaconing Protocol (LIBP)

Lutando *et al*., [19], presented a frugal based routing protocol called Least Path Interference Beaconing (LIBP) for dissemination of sensor reading. Based on broadcast of beaconed messages LIBP, a light weighted model, selects path that builds a routing spanning tree rooted at the sink node. This leads to flow balancing as sensor nodes selects path with least interference. Through performance analysis LIBP is able to conserve energy when being compared with collection of tree based protocols and different types of RPL protocols. LIBP took almost 50% less time stamp to recover the network than CTP and other RPL protocols. But LIBP failed to address the issue of routing security and time consumption in tree construction is higher.

8.7 Cognitive Machine-to-Machine RPL Protocol (CoRPL)

Adnan *et al*., [20] designed a cognitive machine-to-machine (M2M) routing protocol [CoRPL] for Internet of things. Proposed protocol combined the functionalities of centralized cognitive medium access control (MAC) protocol, distributive cognitive M2M protocol and special M2M routing protocol. This protocol worked explicitly in the cognitive radio enabled applications. Result shows that, the cognitive based protocol has higher throughput and lower delay.

Table 1. Comparison of Protocols

PROTOCOLS	PROPERTIES		
	Average Delivery Ratio	**Average End-to-End Delay**	**Energy Consumption**
DFF [14]	High	Average	-
MRPL [15]	High	Less	Average
EEPR [16]	Average	-	Low
CA-RPL [17]	High	Less	Average
MAEB [18]	High	-	Low
LIBP [19]	High	-	Low
CoRPL [20]	High	Average	Average

9. Conclusion

IoT is an ideal emerging technology for the evolution of machine-to-machine communication. In this paper, various routing protocols such as Depth-First Forwarding (DFF), Multipath Lossy and Low powered network Routing protocols (MRPL), Energy Efficient Probabilistic Routing Algorithm (EEPR), Congestion Avoidance Multipath Routing Protocol (CA-RPL), Movement-Aided Energy Balance (MAEB) and Least Path Interference Beaconing (LIBP) are been compared for the parameters average delivery ratio, average end-to-end delay and energy consumption. We observed that Multipath RPL protocols (MRPL) produced better result than other routing protocols.

References

[1] http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx
[2] Jason Pontin: "ETC: Bill Joy's Six Webs". In: MIT Technology Reviewed 29 September 2005, Retrieved 17 November 2013.
[3] Raji RS, "Smart networks for control", Spectrum, IEEE, Vol:31, Issue: 6, pp 49-55, June 1994.
[4] http://kevinjashton.com/2009/06/22/the-internet-of-things/
[5] Zhibo Pang, "Technologies and Architectures of the Internet-of-Things (IoT) for Health and Well-being", Doctoral Thesis in Electronic and Computer Systems KTH – Royal Institute of Technology, Stockholm, Sweden, January 2013.
[6] Farah Nasri, Neila Moussa And Abdellatif Mtibaa, "Internet of Things: Intelligent system for healthcare Based on WSN and Android", 978-1-4799-3351-8/14/.
[7] Mehaseb Ahmed Mehaseb, Yasser Gadallah, Hadia El-Hennawy, "WSN Application Traffic Characterization for Integration within the Internet of Things", 9th International Conference on Mobile Ad-hoc and Sensor Networks, IEEE, 2013.
[8] Hasan Omar Al-Sakran, "Intelligent Traffic Information System Based on Integration of Internet of Things and Agent Technology", International Journal of Advanced Computer Science and Applications, Vol. 6, No. 2, 2015.
[9] Cuong Duc Truong, "Routing and Sensor Search in the Internet of Things", Ph. D Dissertation Report From the Institute of Computer Engineering of the University of Lubeck, January 2014.
[10] Omar Said, Mehedi Masud, "Towards Internet of Things: Survey and Future Vision", International Journal of Computer Networks (IJCN), Volume (5) : Issue (1) : 2013.
[11] Paul Fremantle, "A Reference Architecture for the Internet of Things", White paper, CA, May 28, 2014, http://wso2.com.
[12] Huasong, C., Leung, V., Chow, C., Chan, H,"Enabling technologies for wireless body area networks: A survey and outlook" IEEE Communications Magazine 47, 84–93 (2009).
[13] WSO2 white paper on "A Reference Architecture for the Internet of Things", http://wso2.com/landing/internet-of-things/
[14] Jiazi Yi, Thomas Clausen, Ulrich Herberg, "Depth-First Forwarding for Unreliable Networks: Extensions and Applications", IEEE INTERNET OF THINGS JOURNAL, VOL. 2, NO. 3, JUNE 2015.
[15] Quynh, Thu Ngo, Nien LeManh, Khoi Nguyen Nguyen, "Multipath RPL protocols for greenhouse environment monitoring system based on Internet of Things", Electrical Engineering/ Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), 2015 12th International Conference on. IEEE, 2015.

[16] Sang-Hyun Park, Seungryong Cho, Jung-Ryun Lee "Energy-Efficient Probabilistic Routing Algorithm for Internet of Things", Hindawi Publishing Corporation, Journal of Applied Mathematics, Volume 2014, Article ID 213106, 7 pages, 2014.

[17] Weisheng Tang, Xiaoyuan Ma, Jun Huang, JianmingWei, "Toward Improved RPL: A Congestion Avoidance Multipath Routing Protocol with Time Factor for Wireless Sensor Networks", Journal of Sensors, Article ID 264982.

[18] Haoru Su, Zhiliang Wang, Sunshin An, "MAEB: Routing Protocol for IoT Healthcare", Advances in Internet of Things, Vol.3, PP. 8-15, Scientific Research, 2013.

[19] Lutando Ngqakaza and Antoine Bagula, "Least Path Interference Beaconing Protocol (LIBP): A Frugal Routing Protocol for The Internet-of-Things", 12th International Conference Proceedings, Wired/Wireless Internet Communications- WWIC 2014 Paris, France,vol: ,PP:148-161, May 26–28, 2014.

[20] Adnan Aijaz and A. Hamid Aghvami, "Cognitive Machine-to-Machine Communications for Internet-of-Things: A Protocol Stack Perspective", IEEE INTERNET OF THINGS JOURNAL, VOL. 2, NO. 2, APRIL 2015.

[21] Kassio Machado, Denis Rosario, Eduardo Cerqueira, Antonio A. F. Loureiro, Augusto Neto and Jose Neuman de Souza, "A Routing Protocol Based on Energy and Link Quality for Internet of Things Applications", Sensors, Vol:13, PP:1942-1964, 2013.