ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

A Survey on Routing Protocols of Internet of Things

Gauri S. Rapate[1], Dr. N C Naveen[2]

Assistant Professor, Department of Information Science & Engineering, Vemana Institute of Technology, VTU, Bangalore, India[1]

Professor, Department of Information Science & Engineering, JSS Academy of Technical Education, VTU, Bangalore, India[2]

ABSTRACT: Internet of things (IoT) has become a potential future for all technologies related to human life. In IoT, communication between social environment and user contexts is done through smart interfaces. IoT has to connect to various heterogeneous devices in a Wireless Sensor Network.Hence energy efficient routing optimization is a key factor for network performance in IoT. With reference to this context, in this paper we have explained extensively used routing protocols in IoT. We have focused on 6LoWPAN, RPL and CoAP protocol in detail which is mainly used in energy efficient routing optimization.

KEYWORDS*:* Internet of Things; IoT Protocols CoAP; RPL; 6LoWPAN.

I. Introduction

The IoT (Internet of Technology) also known as WoT (Web of Technology) is a concept where day to day devices like home appliances, sensors, monitoring devices can be accessed through the internet using well known technologies such as URLs and HTTP requests. It is a wireless networking system of living or nonliving objects with the ability to communicate with each other using unique identifiers with minimal human or computer interaction. By gathering the information from the connected devices, action can be taken based on analysis of data. IoT is able to provide advance level of services in many fields like business/manufacturing, retail, healthcare, security, etc.One of the dominant applications of IoT ruling all over is a Smart City through which major problems faced by the citizens like pollution, traffic congestion and shortage of energy supplies etc. will be solved.

IoT is built as a synchronous operation of trillions of sensors, billions of smart systems, and millions of applications. Experts have estimatedof about 30 billion IoT objects by 2020. Huge numbers of applications offered by IoT will generate enormous data and then it becomes a tedious task to route this data to a desired destination for further processing. Also security is of prime importance while processing this data. Considering that this processing has less power and lossy links and mesh topologies with multiple hops, the power consumption in sensor nodes drain out due to hop to hop mobility and mobile network topologies.

IoT has six elements which are used to deliver the functionality of IoT [6]. They are Identification which provides each device a clear identity between the networks, Sensing which gathers data from devices, Communication to connect heterogeneous devices together, Computation to perform required computation on gathered data, and Semantics to extract the knowledge

A. SCHEMA OF INTERNET OF THINGS

Internet of Things architecture consist of four stages where first stage is responsible for sensing and gathering data. The gathered data will go through gateway for processing and forwarded to EdgeIT and finally to cloud for in depth analytics and processing.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

FOUR STAGE ARCHITECTURE OF IoT

Stage 1: Sensors Actuators and connected devices

Stage 1 has the responsibility to gather data and process the data, and take the required action. Here, the former responsibility is handled by sensors and later by actuators.

A sensor's responsibility is to sense changes in the surroundings or another device's state or a system, and forwards or processes this information in a particular way [5]. Sensors perform some input functions by sensing or feeling the physical changes in characteristics of a system in response to a stimulus. For example heat is converted to electrical signals in a temperature sensor. An actuator is a machine component or system that moves or controls the mechanism or the system. A control signal and a source of energy are required for an actuator.

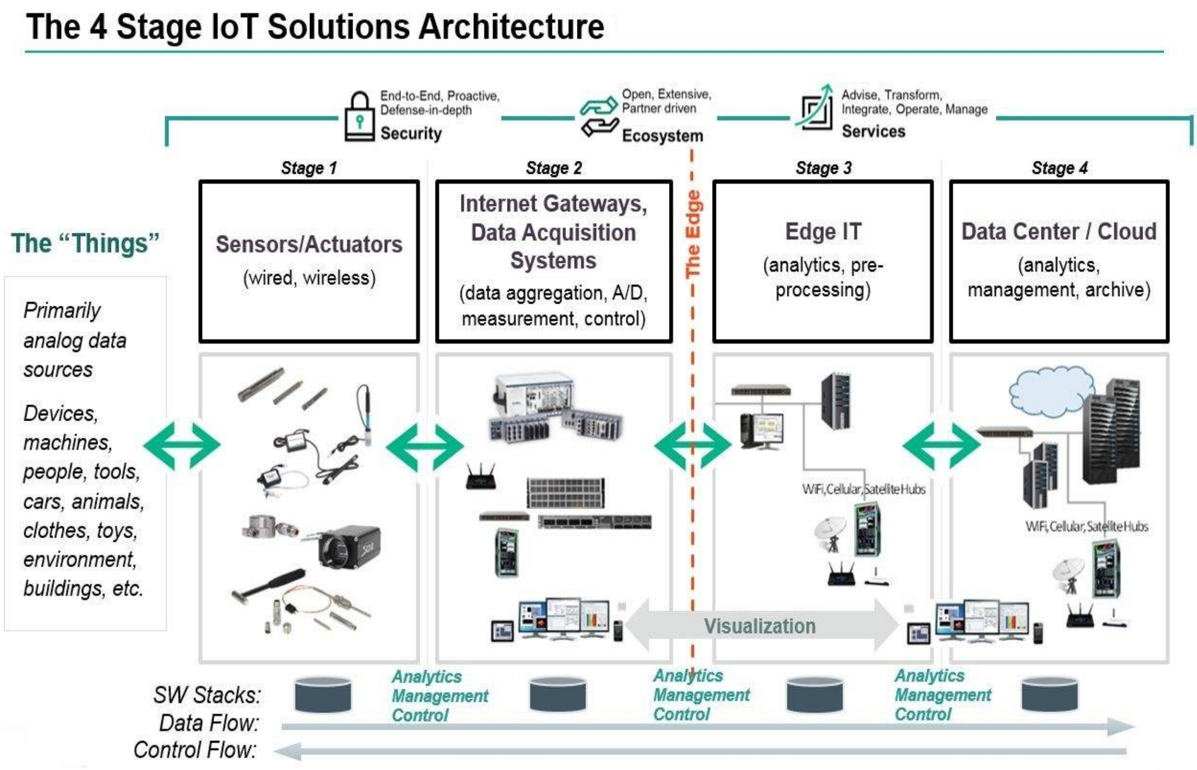


Fig 1:Four Stage Architecture of Internet of Things

Stage 2:Gateway

The information gathered from the sensors should be aggregated and converted which can be done using DAS (Data Acquisition system). The main functionality of DAS is to retrievedigital data from analog data. Then it is fed to gateway to process data and forward it to stage 3

Stage 3:EdgeIT

Since the volume of the acquired data may be huge, there should be some system at the edge to perform analytics work so as to reduce the storage issues and delay in processing. This can be overcome using EdgeIT.

Stage 4:Device Cloud Architecture

The data can be stored securely in cloud for more powerful data analysis and in-depth processing.

B. **ROUTING IN IoT**

In the earlier section, we have seen stages of IoT, where information is carried among devices across network. Transferring data from one node to another node through some intermediate node across inter – network is called as routing. Basically it is selection of path from source to destination. Routing occurs at Network layer i.e. layer3. Routing

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

is classified in two types, they are Static Routing and dynamic routing. In **Static routing** admin configures a routing table manually. In **Dynamic routing**using the routing information routers add network locations automatically.
In IoT data can be transferred from machine to machine(m2m) or machine to human or viceversa. Transferring of data among heterogeneous nodes is routing in IoT.IoT provides vital solution to many real world problems. Data sensed is sent in a continuous way which requires communication which is energy efficient in between nodes. In the whole process a large amount of power consumption is done due to more objects placed in an IoT network.

Implementation of appropriate Routing techniques in IoT based networks can be very challenging because of the below reasons:

1. M2M machine can be of various types(sensors, phone, etc)
2. Even if the machine is same, brands may vary. Depending on the brand, there may be variations in the implementation of network stacks
3. It is difficult to get a seamless M2M connectivity because of vast heterogeneity.
4. Due to mobility of machines the topology keeps changing
5. There can be multiple hops in end to end connectivity
6. Every device should have unique address for m2m connectivity
7. And the most important part is the energy efficiency. Network intensive mobile devices may drain the battery very quickly.

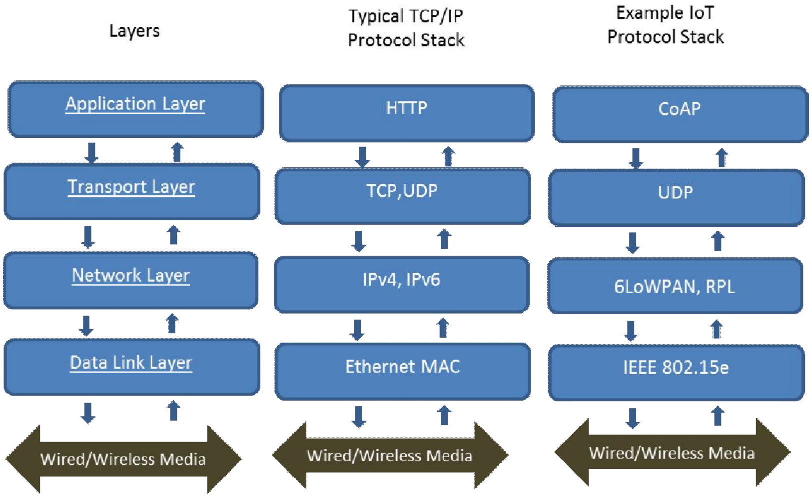
Optimization in routing

To address some of the challenges mentioned above, IoT optimization can be done in few of the different ways mentioned below:

1. Energy efficient routing: Here the source to destination path is optimized by using the way such that the energy of the devices will be saved. Eg: if the node is not having sufficient energy that node will be ignored from the routing path. This can be checked by setting the threshold value for the energy and increase the network lifetime.
2. Data redundancy elimination: Many routing techniques will increase data redundancy. Increase in data redundancy increases energy requirements of nodes and eventually network lifetime. Elimination of data redundancy will result in energy efficient routing

3. Delay reduction: IoT is a network with many devices where delay of nanosecond may also cause problem. Hence the delay should be reduced

Table I: TCP/IP and IoT Protocol Stack with Layers



ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

II. RELATED WORKS

Classification of the IoT protocols are done into four different categories,namely: application protocols, service discovery protocols,infrastructure protocols and other influential protocols.

A. EXISTINGIoT PROTOCOLS

a) Ad-hoc on demand Multipath Distance vector routing protocol for IoT (AOMDV-IoT)

The ad hoc on-demand multipath distance vector (AOMDV) is an extension of AODV protocols [4] that finds many routes during the route discovery phase from source to destination vehicles. AODV gathers many routing paths between source vehicles to destination vehicles in the process of route discovery.

b) Secure Multihop Routing Protocol (SMRP)

In wireless sensor networks for communication node may have to traverse multi-hops especially if it has to communicate with a sink node. In order to achieve this node takes help from neighbors' node to be used as relays which may not be secured. In WSN secure energy-efficient route discovery and forwarding mechanisms is required to ensure privacy and maximize lifetime of the network which is provided by secure multi-hop routing protocol.

c) Energy aware Ant Routing Algorithm (EARA)

EARA Wireless Sensor Networks have specific constraints related to energy, memory and processing power. Although these networks have potential applications in habitat monitoring, military, traffic[2]. Ant based protocol achieves maximization of the network lifetime by minimizing energy consumption and balancing the energy load among all the nodes.

d) PAIR (Pruned Adaptive IoT Routing)

IoT network is the integration of heterogeneous nodes and devices. Spatially correlated entities in the IoT which interact more often may have a communication overhead if all intermediate packets need to be routed. PAIR protocol selectively establishes routes of communication between IoT nodes along with a pricing model which serves the exchange of costs by intermediate nodes for utilizing their resources.

e) REL(Routing protocol based on Energy and Link Quality)

A routing protocol based on Routing by Energy and Link quality (REL) for IoT applications. REL increases its reliability and energy efficiency by selecting routes based on hop count and residual energy of a proposed end to end link. An event-driven mechanism is proposed in REL so that the load balancing can be done and the premature energy depletion of nodes can also be avoided. Its performance was evaluated with simulation and testbed experiments. Eventually the results show that REL increases the network lifetime and services availability, as well as the quality of service of IoT applications. This protocol distributes network resources evenly and also reduces the packet loss. So the performance of this protocol is better than other renowned protocols.

f) 6LoWPAN(IPv6 over Low-Power Wireless Personal Area Networks)

Low power and lossy networks i.e. LLN's where networks is of constrained nodes which are interconnected through low power radio links. This type of network has unstable connectivity, gives poor performance, and has poor speed with low cost.

6LoWPAN is a low power wireless network where every node has its own IPv6 address, allowing it to connect directly to the internet using open standards. It is based on IPv6 and operates in fully asynchronous way. It adopts mesh topology and uses a routing algorithm which does not take care of the sleeping nodes thus requiring approaches such as low power listening for energy saving purpose. Its Personal Operating System is defined by IEEE 802.15.4 which implies a range of 10 meters which can also extend up to 100 meters in some situations. This characteristic of 6LoWPAN makes its application area of short range.

Fig 2 shows the working of 6LoWPAN Network through edge routers. Here edge router routes traffic to and fro of the LoWPAN. It also handles IPv4 interconnectivity.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

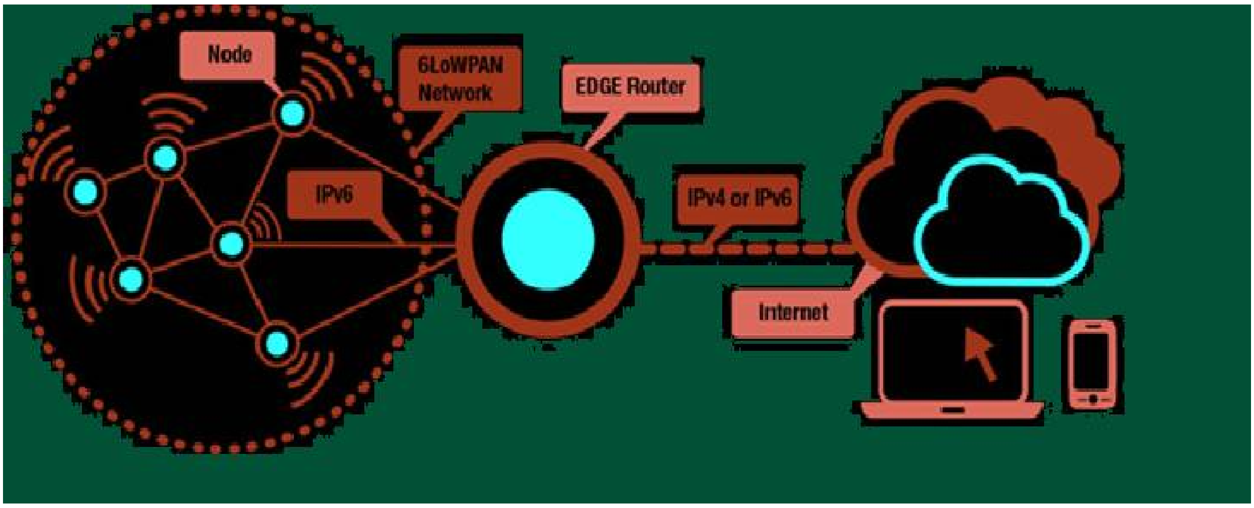


Fig 2: 6LoWPAN Network

Application Areas:
Applications with devices needing wireless internet connectivity at lower data rates are the main target of 6LoWPAN. **So, 6LoWPAN is used mainly in Home Automation systems, Health Care systems, etc.**
Disadvantages: The greatest challenge to 6LoWPAN is the lack of application that utilizes 6LoWPAN because it require extensive training as it is complicated to work with and 6LoWPAN also needs vast knowledge of stack and the feasibility of IPv6.

g) RPL(Routing Protocol for Low Power and Lossy Networks)

RPL is a distance vector IPv6 Routing Protocol designed for Low-Power and Lossy Networks as defined in RFC6550**.** Low Power and Lossy Networks (LLN's) are a class of network in which both the routers and their interconnections are constrained. Routers of LLN generally operate with constraints on energy (battery power), processing power, and memory. LLN's are characterized based on high loss rates and instability. RPL provides a mechanism hereby multipoint to point traffic from devices inside the LLN towards a central control point as well as point to multipoint traffic from the central control point to the devices inside the LLN are supported.

Directed Acyclic Graph (DAG) s a topology which can be partitioned into many Destination Oriented DAG's which are also referred as DODAG's and each sink consist of one DODAG. Multiple roots in DAG are united by a transit link which is considered as a common backbone. Since RPL routes are optimized for traffic to or from one or more roots that act as sinks for the topology, it uses DAG topology.

Constraints of RPL: RPL can be enabled only on the main interface. RPL works better if most of the links have different link local address. In this implementation though probing parameters are not configured in root template, they are required in root template.

h) CoAP (Constrained Application Protocol)

The Constrained Application protocol is a specialized web transfer protocol for use with constrained nodes and constrained networks in the IoT. CoAP is used in applications like smart energy and building automation which are device to device applications. CoAP is a document transfer protocol like HTTP but is designed for the needs of constrained devices. CoAP runs over UDP (User Datagram Protocol). It is an Internet Application Protocol for constrained devices which is defined in RFC 7228. It allows the devices that are constrained to communicate with the extensive Internet using related protocols. Typically, CoAP is designed for devices having the same constrained network among devices and nodes on the internet, as well as devices on the different constrained network connected by an internet. CoAP meets specialized requirements such as multicast support, very low overhead, and simplicity.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

Table II: Parameter Based Comparison of IoT Protocols

Protocol	Context Aware	Secure	Multihop Routing	Supports Dynamic Topology	Incentive Based	Considers Link Quality
AOMDV-IoT	✗	✗	✓		✗	✗
SMRP	✗	✓	✓		✗	✗
EARA	✓	✗	✓		✗	✗
PAIR	✓	✗	✓	✓	✓	✗
REL	✓	✗	✓		✗	✓
CoAP		✓	✓	✓		
6LoWPAN		✓	✓	✓		
RPL	✓	✓	✓	✓	✗	✗

III. PROPOSED SYSTEM

The existing IoT based systems mostly make use of existing protocols for realizing the IoT use based cases. However these protocols have their own limitations as described earlier.

Existing protocols like **6LoWPAN**are intended to extend IPv6 based networks to use cases of IoT. Using this mechanism it is possible to reuse existing IPv6 technologies as infrastructure. But the main problem is that IPv6 is designed for devices which is high on memory resources and processing capability. Hence it is not suitable for IoT network based entities.

Another IPv6 based routing protocol mentioned earlier **is RPL** meant for Low Power and Lossy Network [1]. This protocol is developed for network comprising of devices which consume low power, low computation capability and memory. But here then the problem is that the data transmissions in this type of networks is not very reliable. Data rate is lowhowever rate of loss of data is high.
CoAP - Constrained Application Protocol. The main characteristics of CoAP protocol is that it can be converted to a HTTP message, this immenselyhelps in integrating with web services. It also supports multicast.

To overcome the limitations faced by the above protocols, we have proposed the system which will evolve up with a novel routing technique that supports an efficient communication performance over heterogeneous nodes in Internet-of-Things (IoT). It will also incorporate a cost effective optimization policy to further enhance the operational performance of proposed routing scheme in IoT

IV. CONCLUSION

This paper provides a comprehensive survey of protocols for IoT. IEEE, ITU, IETF and other organizations in past have developed and are currently also developing many protocols. Since, the number of protocols available are many, only a brief discussion of each protocol is provided in this paper. This paper also provides references for further information. The existing routing algorithms in IoT are compared on the basis of different parameters like power consumption, security, context awareness, and so forth. Every routing protocols has its own advantage depending upon

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

the application where it is used. The aim of this paper is to provide an insight to service providers anddevelopers of various layers of protocols in IoT and how to choose between them.

REFERENCES

1. Oana Iova, Fabrice Theoleyre, Thomas Noel, “Using Multiparent Routing in RPL to Increase The Stability and The Lifetime of The Network”, Ad Hoc Networks, Elsevier, pp. 45-62, 2015.
2. Michael Frey, Friedrich Grose, Mesut Gunes, “Energy-aware Ant Routing in Wireless Multi-hop Networks”, IEEE International Conference on Communications (ICC), pp. 190-196, 2014.
3. G. Abowd, A. Dey, P. Brown, N. Davies, M. Smith, and P. Steggles, “Towards a Better Understanding of Context and ContextAwareness,” in Proc. Handheld Ubiquitous Comput.,pp. 304– 307, 1999.
4. Yicong Tian, Rui HOU,“An Improved AOMDV Routing Protocol for Internet of Things”, International Conference on Computational Intelligence and Software Engineering (CiSE), pp. 1-4, 2010
5. Maria Rita Palattella, Nicola Accettura, Xavier Vilajosana, Thomas Watteyne, Alfredo Grieco, Gennaro Boggia, Mischa Dohler, “Standardized Protocol Stack for the Internet of (Important) Things”, IEEE Communications Surveys and Tutorials, IEEE, PP(99):1 –18, ISSN 1553-877X, 2012.
6. Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari, Moussa Ayyash, “Internet of Things: A Survey on Enabling Technologies, Protocols and Applications”, IEEE IEEE Communications Surveys and Tutorials January 2015