IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 17, Issue 2, Ser. I (Mar. – Apr. 2022), PP 43-52
www.iosrjournals.org

Comparative Analysis of CoAP and RPL routing protocol

Tanmay Joshi[1], Saloni Hegishte[2], Rutuja Jadhav[3], Ankita Bhagat[4], Prof. Jyoti Gurav[5]

[1]*(Electronics And Telecommunication, Atharva College of Engineering/ Mumbai University, India)*
[2]*(Electronics And Telecommunication, Atharva College of Engineering/ Mumbai University, India)*
[3]*(Electronics And Telecommunication, Atharva College of Engineering/ Mumbai University, India)*
[4]*(Electronics And Telecommunication, Atharva College of Engineering/ Mumbai University, India)*
[5]*(Electronics And Telecommunication, Atharva College of Engineering/ Mumbai University, India)*

Abstract: *In this paper, a comparison of Internet of Things protocols used for data transfer in Internet of Things constrained networks is presented. Setting up such a network with a large number of physical interconnected IoT devices can be a challenge. In the IoT world, one of the key challenges is to efficiently support M2M communication in constrained networks. This can be achieved using CoAP (Constrained Application Protocol) protocols and RPL (Routing Protocol for Low-Power and Lossy Networks). Choosing the appropriate protocol can be difficult while developing IoT application. There are several conditions that need to be considered while determining which protocol should be used. In this paper, we will evaluate performance and compare these protocols through different scenarios.*

Key Word: *IoT, CoAP, RPL*

Date of Submission: 05-04-2022 Date of Acceptance: 21-04-2022

I. Introduction

Everyday growing number of objects connected to the internet Worldwide has promoted the Internet of Things technologies and protocols as one of the most commonly used in the modern systems. IoT refers to the networked interconnection of everyday objects which are often equipped with electronic circuits and sensors. In the IoT sense these objects can refer to a vide variety of small objects that are integrated into a larger system. The amount of systems based on Internet of Things (IoT) has grown at an unprecedented rate over the last years and such an expansion tends to continue. As a consequence, billions of devices are expected to be deployed on diverse industries (e.g., healthcare, automotive) during the next decade. From this, the question of which protocol to use for the Internet of Things becomes a topic of high interest. Due to the remote nature and need for wireless networking of smart objects, IoT systems must be able to cope with potentially unreliable, intermittent, and low bandwidth connections for its access network. and, thus, distinct communication protocols have been proposed for these systems.

The routing protocols discussed in this literature are primarily focused on increasing the network performance in terms of load balancing, congestion, and energy consumption. These protocols employ various routing metrics and scenarios to improve the network performance through the routing protocol.

This paper is mainly focused on a comparative analysis on the bacis of the Internet of Things' architecture. This analysis will help us to develop communication among two protocols, RPL, and CoAP. In addition, it will also find out the best communication path between the IoT nodes. A large amount of the data that are consumed by IoT will be kept in the cloud. The real issue is to develop the ability of the people to understand the variations and their inferences more clearly, and to take solid actions accordingly. Different simulators have been used by a number of researchers, such as NS-3, Tossim, and OPNET for different platforms like TinyOS, POSIX, lwIP, etc. However, cooja was selected to simulate contiki nodes on a large scale. This simulator is specially designed to simulate sensors that consume very low power and proven to be very accurate. This paper is concentrated on finding out the best protocol for communication between IOT nodes, and therefore, the study can be useful in personal and home application, health care, utilities and services, enterprise application, and industrial automation

II. IoT Protocol Stack

There are several protocols for M2M/IoT communications with a focus on constrained environments. Most frequently adopted protocols are CoAP (Constrained Application Protocol) and RPL (Routing Protocol for Low Power Networks). We shall further discuss and compare them.

A. CoAP: -

CoAP is a stateless protocol developed by the IETF to replace HTTP in resource-constrained devices. Being a UDP based RESTful protocol, it uses a request/reply structure and has low overhead and a low degree of optional QoS. In order to receive telemetry, a client must constantly request the server to send the information. CoAP primarily supports a peer-to-peer style of communication but can be expanded to support one-to-many functions via the use of IP multicast. Since HTTP and CoAP share the REST model, they can easily be connected using application-agnostic cross-protocol proxies. A Web client may not even notice that it just accessed a sensor resource. CoAP can carry different types of payloads, and can identify which payload type is being used. It can integrate with any data format of your choice. The Internet of Things will need billions of nodes, many of which will need to be inexpensive. CoAP has been designed to work on microcontrollers with as low as 10 KiB of RAM and 100 KiB of code space. CoAP is designed to use minimal resources, both on the device and on the network. Instead of a complex transport stack, it gets by with UDP on IP. A 4-byte fixed header and a compact encoding of options enables small messages that cause no or little fragmentation on the link layer. Many servers can operate in a completely stateless fashion. The CoAP resource directory provides a way to discover the properties of the nodes on your network. The protocol has been designed to last for decades. Difficult issues such as congestion control have not been swept under the rug, but have been addressed using the state of the art technology. The Internet of Things cannot spread as long as it can be exploited by hackers. CoAP does not just pay lip service to security, it actually provides strong security. CoAP's default choice of DTLS parameters is equivalent to 3072-bit RSA keys, yet still runs fine on the smallest nodes. Following are the features of CoAP Protocol:

- It is very efficient RESTful protocol.
- Easy to proxy to/from HTTP.
- It is open IETF standard
- It is Embedded web transfer protocol (coap://)
- It uses asynchronous transaction model.
- UDP is binding with reliability and multicast support.
- GET, POST, PUT and DELETE methods are used.
- URI is supported.
- It uses small and simple 4 byte header.
- Supports binding to UDP, SMS and TCP.
- DTLS based PSK, RPK and certificate security is used.
- uses subset of MIME types and HTTP response codes.
- Uses built in discovery mechanism.

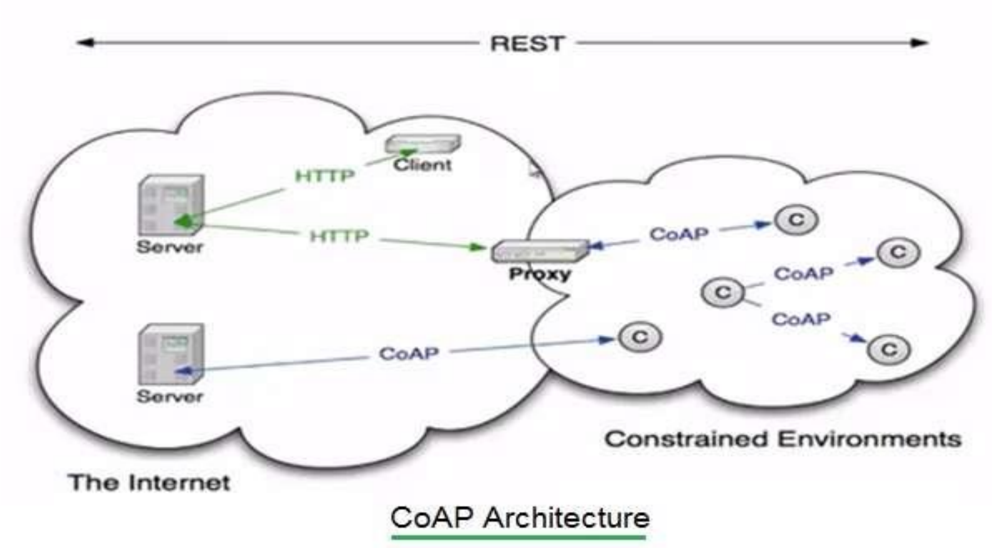

Fig-1

Shown above is the CoAP architecture. As shown it extends normal HTTP clients to clients having resource constraints. These clients are known as CoAP clients. Proxy device bridges gap between constrained environment and typical internet environment based on HTTP protocols. Same server takes care of both HTTP and CoAP protocol messages.

B. RPL: -

RPL (Routing Protocol for Low-Power and Lossy Networks) is a routing protocol for wireless networks with low power consumption and generally susceptible to packet loss. It is a proactive protocol based on distance vectors, optimized for multi-hop and many-to-one communication, but also supports one-to-one messages. RPL can support a wide variety of link layers, including those with limitations, with potential losses or that are used in devices with limited resources. This protocol can quickly create network routes, share routing knowledge and adapt the topology in an efficient way. The Routing Protocol (RPL) for Low power and Lossy Networks (LLN) assist the Objective Function (OF) to design a Destination Oriented Directed Acyclic Graph (DODAG) established on a group of rules and limitations. The RPL designed graph is a rational routing topology designed for a physical network to get multiple routing with a various bunch of requirements as Energy, Distance, Link Stability, and Bandwidth Availability. The diverse applications of LLNs include scenarios ranging from basic temperature measurements to high-volume multimedia services that require efficient communication support. Following are the features of RPL Protocol:

- Loop avoidance and detection
- Self configuration
- Communication paradigms
- Target networks
- Identifiers
- Security mode
- Mode of operation

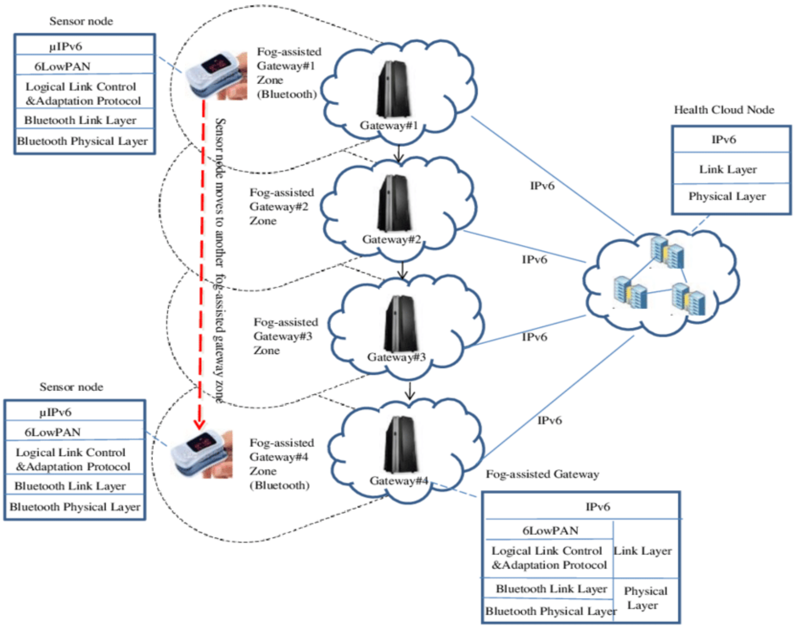

Fig-2

RPL is strictly compliant with layered IPv6 architecture. Further, RPL is designed with consideration to the practical support and implementation of IPv6 architecture on devices which may operate under severe resource constraints, including but not limited to memory, processing power, energy, and communication. The RPL design does not presume high quality reliable links, and operates over lossy links (usually low bandwidth with low packet delivery success rate).

III. Experimental setup

For our comparative intent and purposes, we are going to create and simulate networks and find out their physical and network parameters and compare them to find out which protocol in more suited to our needs. For this simulation we going to Cooja software in Contiki OS. We will be running them on a virtual machine in VMware workstation using Ubuntu.

A. Contiki OS: -

Contiki is an operating system for IoT that specifically targets small IoT devices with limited memory, power, bandwidth, and processing power. It uses a minimalist design while still packing the common tools of modern operating systems. It provides functionality for management of programs, processes, resources, memory, and communication. It owes its popularity to being very lightweight (by modern standards), mature, and flexible. Many academics, organization researchers, and professionals consider it a go-to OS. Contiki only requires a few kilobytes to run, and within a space of under 30KB, it fits its entire operating system − a web browser, web server, calculator, shell, telnet client and daemon, email client, vnc viewer, and ftp. It borrows from operating systems and development strategies from decades ago, which easily exploited equally small space. It has been extensively used in the industry. This OS is used in numerous commercial and non-commercial applications: street light network, electrical power meter network, energy meter, many monitoring applications: industrial, radiation, remote etc. Contiki supports standard protocols and recent enabling protocols for IoT −

uIP (for IPv4) − This TCP/IP implementation supports 8-bit and 16-bit microcontrollers.
uIPv6 (for IPv6) − This is a fully compliant IPv6 extension to uIP.
Rime − This alternative stack provides a solution when IPv4 or IPv6 prove prohibitive. It offers a set of primitives for low-power systems.
6LoWPAN − This stands for IPv6 over low-power wireless personal area networks. It provides compression technology to support the low data rate wireless needed by devices with limited resources.
RPL − This distance vector IPv6 protocol for LLNs (low-power and lossy networks) allows the best possible path to be found in a complex network of devices with varied capability.
CoAP − This protocol supports communication for simple devices, typically devices requiring heavy remote supervision.

B. Cooja Network Simulator: -

Cooja is a cross-layer java-based wireless sensor network simulator distributed with Contiki. It allows the simulation of different levels from physical to application layer, and also allows the emulation of the hardware of a set of sensor nodes.

IV. Results and Discussion

After the simulation is completed for both the networks, we have the following physical and network parameters to compare: -

A. Latency

Latency is the time it takes for data to pass from one point on a network to another. Most often, latency is measured between a user's device (the "client" device) and a data center. This measurement helps developers understand how quickly a webpage or application will load for users. Although data on the Internet travels at the speed of light, the effects of distance and delays caused by Internet infrastructure equipment mean that latency can never be eliminated completely. It can and should, however, be minimized. A high amount of latency results in poor website performance, negatively affects SEO, and can induce users to leave the site or application altogether.

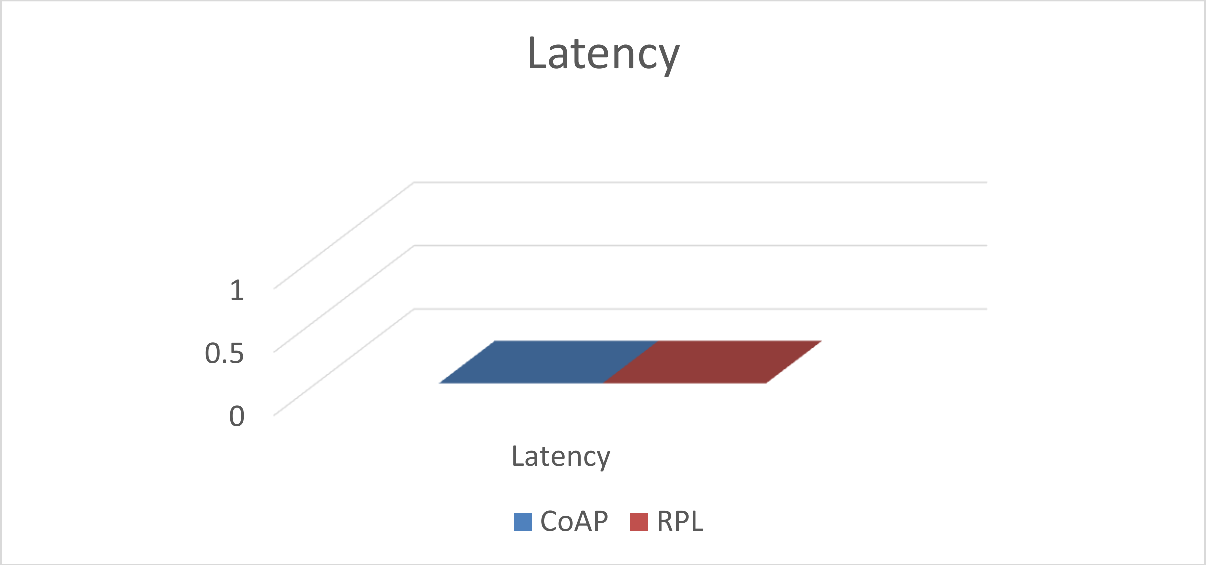

Fig-3

As we can see from the above graph, the latency for both CoAP and RPL protocols is zero, which means that there is no delay in the transference of data.

B. Packet loss

Packets are bits of data, tiny fragments of a larger whole, that move across a network. The things you see and send on the internet are all made of packets! Every time you receive an email, or download a video or picture, you're dealing with packet transfers. Packets are the busy little bees that keep the internet alive and moving, and they make up just about everything that you can send and receive online. Packet loss occurs when these packets don't reach their final destination – some of them can get lost in congested networks, diverted by an interrupted signal, or snatched away by cybercriminals. In addition to being an indication of a network's ailing health, packet loss can lead to plenty of frustrations and costly consequences – ranging from slow load times and buffering videos to expensive investments in lag prevention.

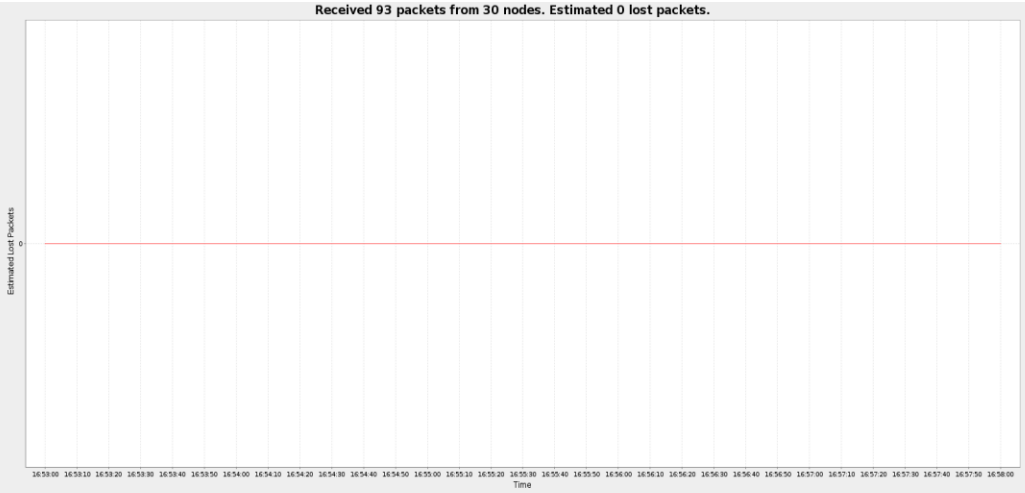

Fig-4. CoAP packet loss

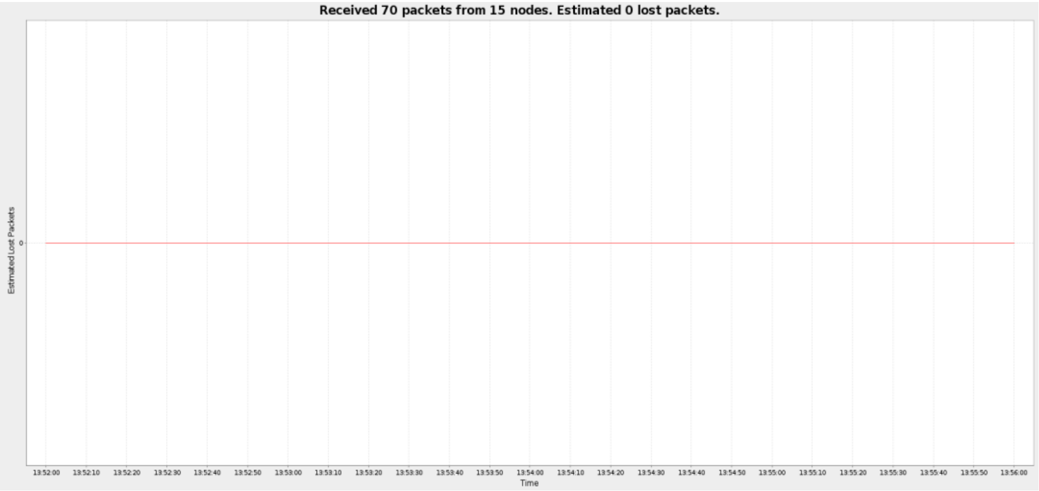

Fig-5. RPL packet loss

From these results we can see that there is no packet loss in these two networks. We can also observe that the number of packets received in CoAP are more than the number of packets received in Rpl even though the network conditions of 15 nodes and the runtime was the same.

C. Average sensor Temperature: -

Temperature sensors measure the amount of heat generated from an area or an object. They detect a temperature change and convert the findings to data. Temperature sensors are used in various industries, including manufacturing, healthcare, and agriculture. Some examples are thermistors, thermocouples, and resistor temperature detectors (RTD). In our research we are going to measure the temperature of each mode in the network for each protocol. As we can see from Fig-4. The average temperature of each node in the network is the same for both the protocols.

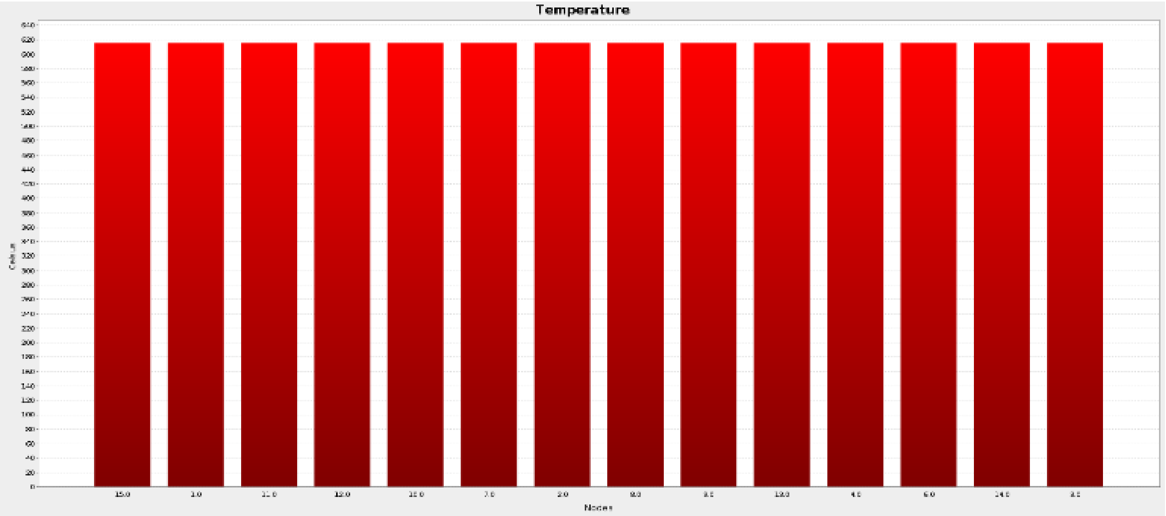

Fig-6. Sensor temperature

D. Power Consumption: -

The Internet of Things with its arrival brought some interesting topics to be addressed. These include issues such as safety, ergonomics, communications technology, but mainly low-power equipment. IoT devices are often powered by a battery because they do not have direct access to a power supply. This is often caused by being located in places where access to the electric network is simply not possible. Finding ways to ensure low consumption of energy certainly did not come with IoT. Long ago we had calculators, remote controls, digital games, and laptops or mobile phones. All of these devices were powered by batteries. However, IoT devices represent a special set of devices where they are expected to be able to operate without user intervention for months or years. And before the battery runs out of power, they will alert you in advance that the battery needs to be replaced. Energetically autonomous devices are the fundamentals of IoT.

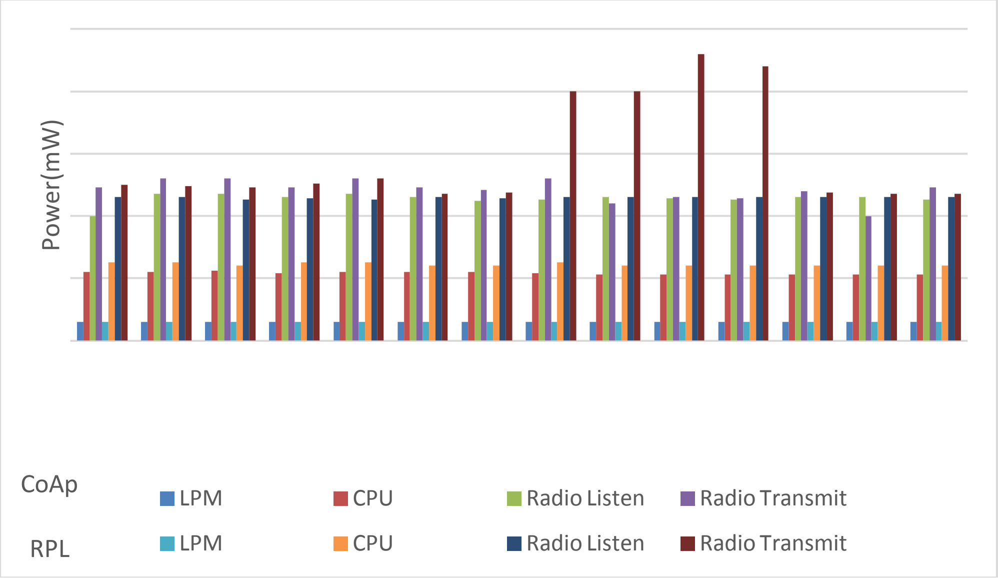

Fig-7

As we can see from the above figure the power consumption in both the protocol networks is very similar excluding radio transmit. When it comes to radio transmission, the RPL network consumes a lot more power than a CoAP network.

E. Beacon Interval: -

A. Beacon interval

Beacon Broadcast interval is the time lag between each of the beacons sent by your router or access points. By definition, the lower the value, the smaller the time lag which means that the beacon is sent more frequently. The higher the value, the bigger the time lag which means that the beacon is sent broadcasted less frequently. The beacon is needed for your devices or clients to receive information about the particular router. In this case the beacon includes some main information such as SSID, Timestamp, and various parameters. Most of the routers out of the box has the default Beacon Interval function value set at 100 ms. In most cases it is a decent number that is compatible with most of the situations. However, it is not the optimal ideal value since it all really depends on how you are setting up your network.

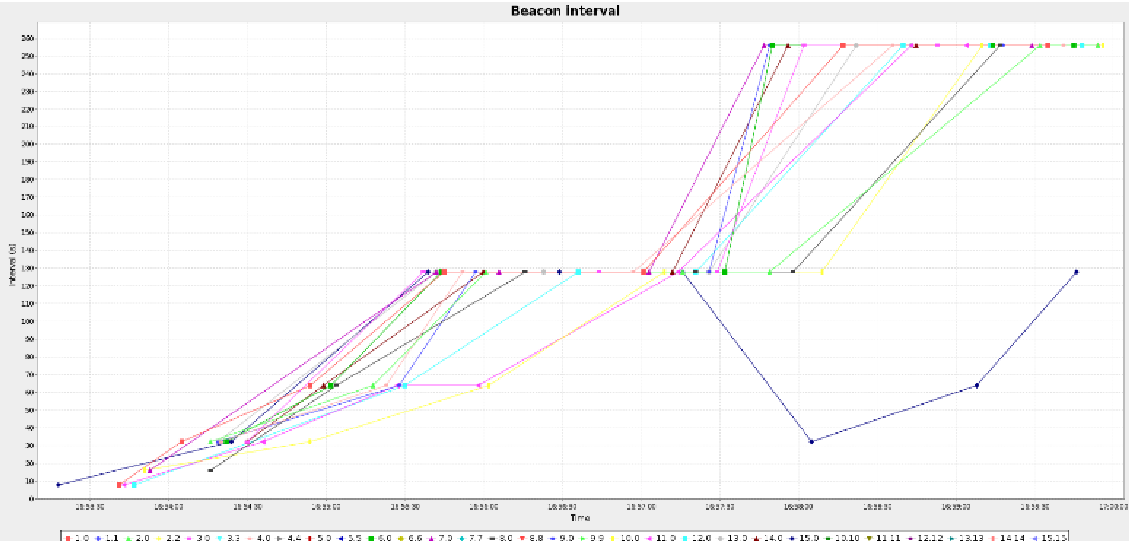

Fig-8. CoAP Beacon Interval

Low Beacon Interval:

Lower beacon interval allows faster discovery of the routers because it sends beacons much more frequently. It can help with weak signal with poor reception environments since the devices have better chances of "catching" the beacons when they are sent more frequently. It can also assist with multiple access points with roaming setup, since your devices can make better decisions about which AP to connect to.

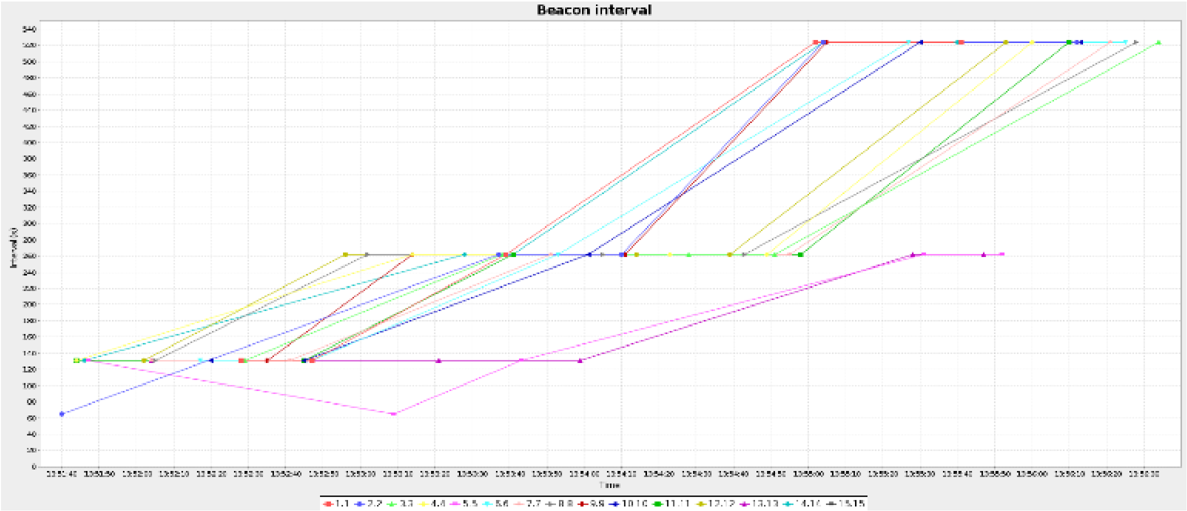

Fig-9. RPL Beacon Interval

High Beacon Interval:

The beacons broadcasted by your router takes up some of the bandwidth that can be used for the actual data transmission. So by having higher numbers, you will be able to achieve better throughput and thus better speed and performance.

F. Routing Metric: -

A routing metric is a unit calculated by a routing algorithm for selecting or rejecting a routing path for transferring data/traffic. A routing metric is calculated by routing algorithms when determining the optimal route for sending network traffic. Metrics are assigned to each different route available in the routing table and are calculated using many different techniques and methods based on the routing algorithms in use. Some of the parameters used for calculating a routing metric are as follows:

1. Hop count
2. Path reliability
3. Path speed
4. Load
5. Bandwidth
6. Latency
7. Maximum transmission unit

Lower metrics are considered better and take precedence over higher once.

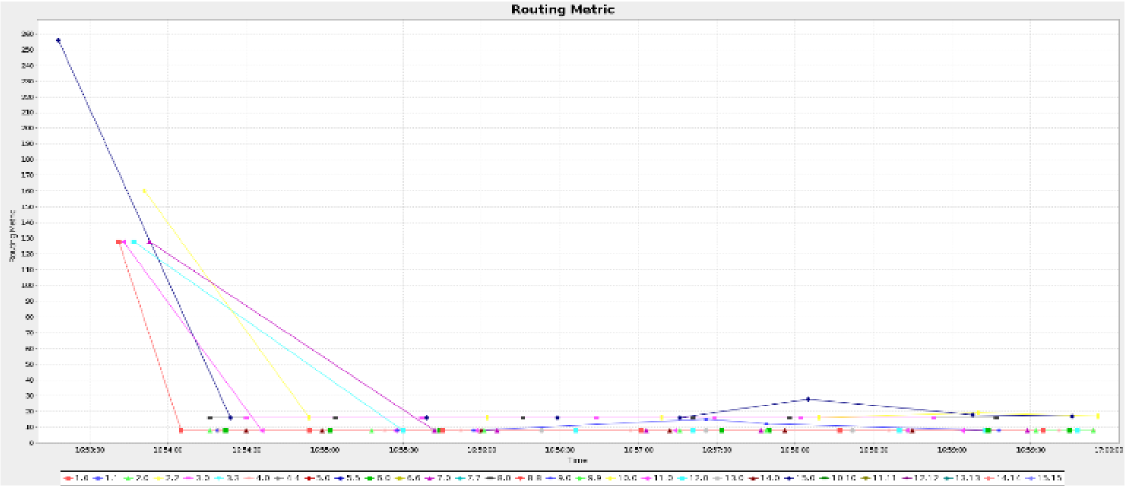

Fig-10. CoAP routing metric

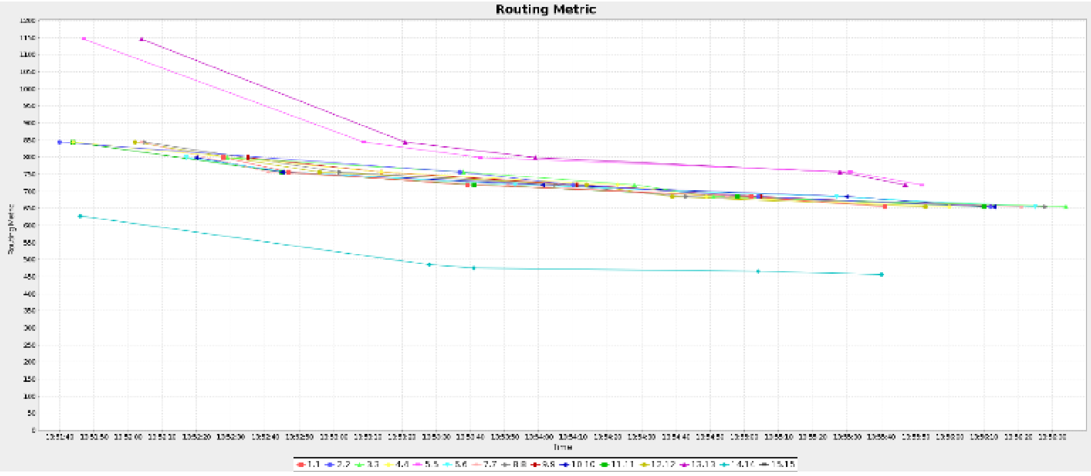

Fig-11. RPL routing metric

G. Network Hops: -

A hop is a computer networking term that refers to the number of routers that a packet (a portion of data) passes through from its source to its destination. Sometimes a hop is counted when a packet passes through other hardware on a network, like switches, access points, and repeaters. This isn't always the case, and it depends on what role those devices are playing on the network and how they're configured.

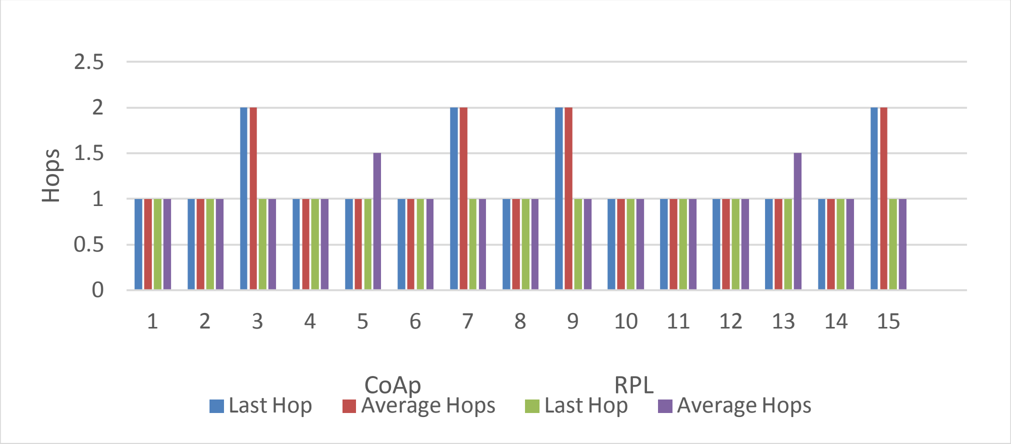

Fig-12. Network hops

H. Radio Duty Cycle: -

Duty cycle typically refers to the ratio of time a transmitter is actually producing full power – and when it is at rest.

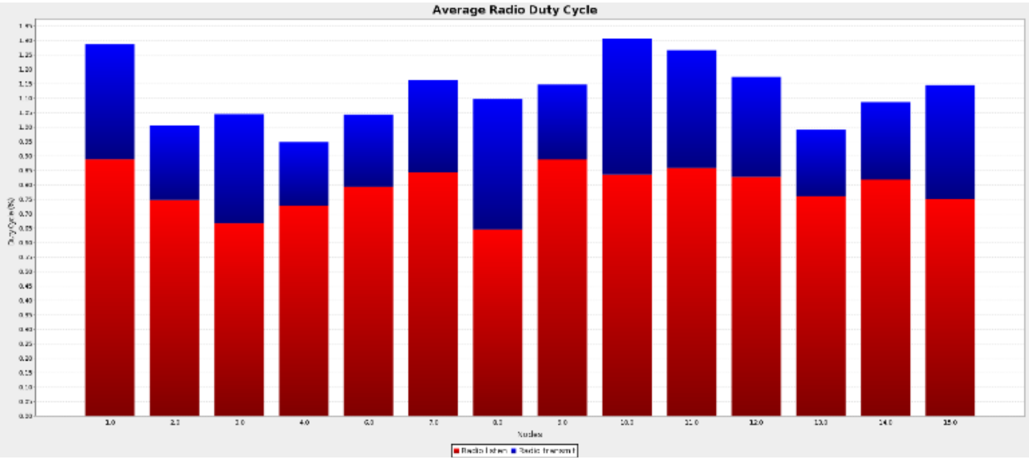

Fig-13. Avg radio duty cycle of CoAP

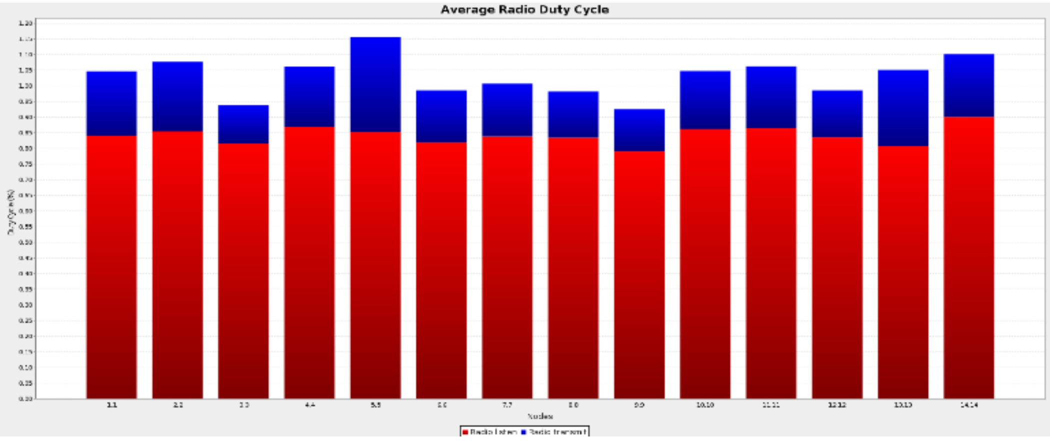

Fig-14. Avg radio duty cycle of RPL

V. Conclusion

We have successfully compared CoAP and RPL Routing Protocols.

References

[1]. Yuang Chen, Thomas Kunz, "Performance Evaluation of IOT Protocols under a Constrained Wireless Access Network," 2016 International Conference on selected topics in Mobiles and Wireless Networking (MoWNeT)

[2]. Monishanker Halder, Mohammad Nowsin Amin Sheikh, Md. Saidur Rahman, Md. Amanur Rahman, "Performance Analysis of CoAP, 6LowPAN and RPL Routing Protocols of IOT using COOJA Simulator," International Journal of Scientific & Engineering Research, Volume 9, Issue 6, June-2018 ISSN 2229-5518

[3]. G. Vennila, Dr. D. Arivazhagan, Dr. R.Jayavadivel, "Experimental Analysis Of RPL Routing Protocol In IOT," INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 8, ISSUE 10, OCTOBER 2019 ISSN 2277-8616"

[4]. Dr.S.Umamaheswari, Dr.Atul Negi, "INTERNET OF THINGS AND RPL ROUTING PROTOCOL: A STUDY AND EVALUATION," 2017 International Conference on Computer Communication and Informatics (ICCCI -2017), Jan. 05 – 07, 2017, Coimbatore, INDIA

[5]. Belghachi Mohamed, Feham Mohamed, "Experimental Evaluation of RPL Protocol," The 11th International Conference for Internet Technology and Secured Transactions (ICITST-2016)

[6]. Md Sayedul Aman, Kumar Yelamarthi, Ahmed Abdelgawad, "A Comparative Analysis of Simulation and Experimental Results on RPL Performance"

[7]. N. Accettura, L. A. Grieco, G. Boggia, P. Camarda, "Performance Analysis of the RPL Routing Protocol," Proceedings of the 2011 IEEE

[8]. Intemational Conference on Mechatronics April 13-15, 2011, Turkey.

[9]. Djana Ugrenovic, Gordana Gardasevic, "CoAP protocol for Web-based monitoring in IOT healthcare applications," 23rd Telecommunications forum TELFOR 2015

[10]. Sharwari Satish Solapure and Harish H.Kenchannavar, "RPL AND COAP PROTOCOLS, EXPERIMENTAL ANALYSIS FOR IOT: A CASE STUDY," International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.10, No.2, April 2019

[11]. Shimaa A. Abdel Hakeem Anar A. Hady and HyungWon Kim, "RPL Routing Protocol Performance in Smart Grid Applications Based Wireless Sensors: Experimental and Simulated Analysis," Published: 5 February 2019

[12]. Burak H. Çorak1 , Feyza Y. Okay1 , Metehan Güzel1 , Şahin Murt2 , Suat Ozdemir1, "Comparative Analysis of IoT Communication Protocols," 978-1-5386-3779-1/18/$31.00 ©2018 IEEE

[13]. Thays Moraes1, Bruno Nogueira2, Victor Lira1 and Eduardo Tavares1, "Performance Comparison of IoT Communication Protocols," 2019 IEEE International Conference on Systems, Man and Cybernetics (SMC) Bari, Italy. October 6-9, 2019

[14]. Meera M. S, Sethuraman N Rao, "Comparative Analysis of IoT protocols for a Marine IoT System," 978-1-5386-5314-2/18/$31.00 ©2018 IEEE

[15]. I. Heđi, I. Špeh, A. Šarabok, "IoT network protocols comparison for the purpose of IoT constrained networks," MIPRO 2017, May 22- 26, 2017, Opatija, Croatia

[16]. Lavinia Năstase, "Security in the Internet of Things: A Survey on Application Layer Protocols," 2017 21st International Conference on Control Systems and Computer Science

[17]. Dae-Hyeok Mun, Minh Le Dinh, Young-Woo Kwon, "An Assessment of Internet of Things Protocols for Resource-Constrained Applications," 2016 IEEE 40th Annual Computer Software and Applications Conference

[18]. 2d Lt Daniel Celebucki, Maj Alan Lin, Dr. Scott Graham, "A Security Evaluation of Popular Internet of Things Protocols for Manufacturers," 2018 IEEE International Conference on Consumer Electronics (ICCE)

[19]. Markel Iglesias-Urkia, Adri ́an Orive, Aitor Urbieta, "Analysis of CoAP Implementations for Industrial Internet of Things: A Survey," Markel Iglesias-Urkia et al. / Procedia Computer Science 109C (2017) 188–195