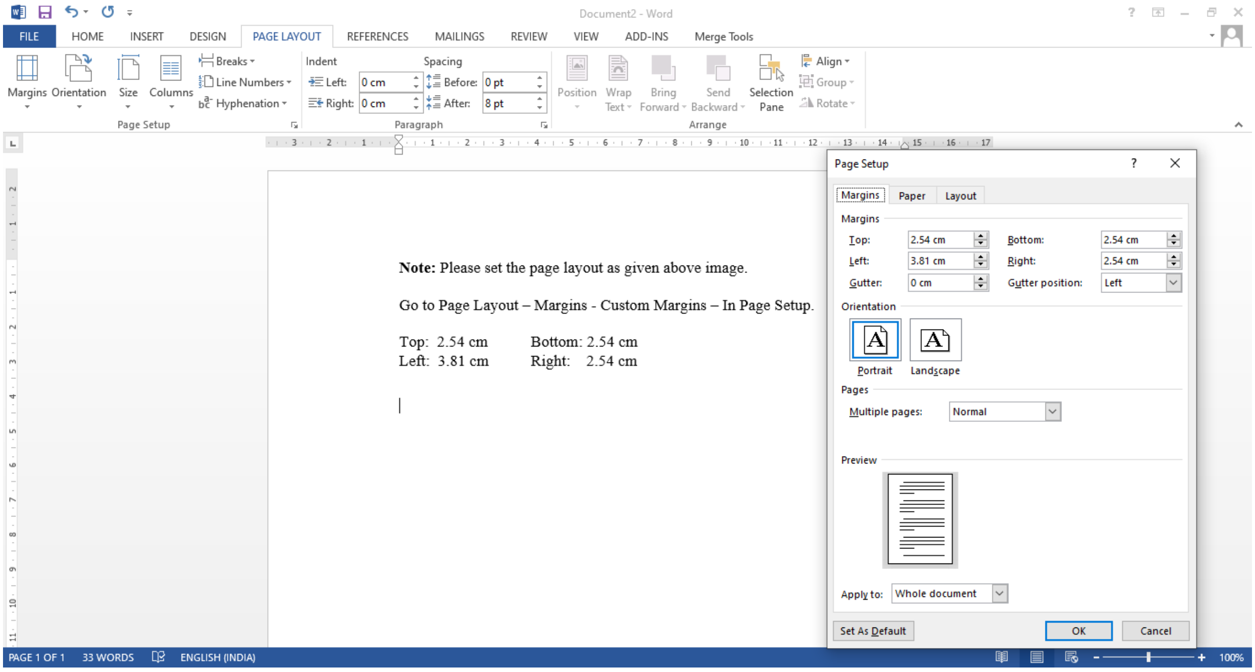

Left: 0 cm
Right: 0 cm
Before: 0 pt
After: 8 pt

**Note:** Please set the page layout as given above image.

Go to Page Layout – Margins - Custom Margins – In Page Setup.

Top: 2.54 cm Bottom: 2.54 cm
Left: 3.81 cm Right: 2.54 cm

Top: 2.54 cm
Bottom: 2.54 cm
Left: 3.81 cm
Right: 2.54 cm
Gutter: 0 cm
Gutter position: Left
Multiple pages: Normal
Apply to: Whole document

**Note:** Please set the page layout as given above image.

Go to Page Layout – Margins - Custom Margins – In Page Setup.

Top: 2.54 cm Bottom: 2.54 cm
Left: 3.81 cm Right: 2.54 cm

- Font text is Times New Roman
- Font Size Remark in blue color

REVA UNIVERSITY
Bengaluru, India

# CLOCK SYNCHRONIZATION AND LOCALIZATION OF NODES IN WIRELESS SENSOR NETWORK (16)

*(A Thesis submitted in partial fulfilment of the requirements for the award of the degree of Doctor of Philosophy in Mechanical Engineering)* (12)

Submitted by

**ABCD**

(SRN - R21PEE09)

Under the Supervision of

**Dr. XYZ**
Director
School of Electrical & Electronics Engineering
REVA University, Bengaluru

**&**

**Dr. PQR**
Professor
School of Electrical & Electronics Engineering
REVA University, Bengaluru

**SCHOOL OF ELECTRICAL & ELECTRONICS ENGINEERING (14)**

**REVA UNIVERSITY (14)**

Rukmini Knowledge Park, Kattigenahalli, Yelahanka, Bengaluru – 560 064

**2021**

REVA UNIVERSITY
Bengaluru, India

## SCHOOL OF ELECTRICAL & ELECTRONICS ENGINEERING (14)

## DECLARATION

I ABCD declare that the thesis entitled **“Clock synchronization and localization of nodes in wireless sensor network”** submitted by me in partial fulfillment of the requirements for the award of the degree of Doctor of Philosophy in Mechanical Engineering, REVA University is based on the results of the research work carried out and reported by me under the guidance of Dr. XYZ, Director, School of Electrical & Electronics Engineering, REVA University and Dr. PQR, Professor, School of Electrical & Electronics Engineering, REVA University.

I also declare that this thesis or any part of it has not been submitted for award of any other degree / diploma of this or any other University / Institute.

I further declare that this thesis has undergone plagiarism verification and it is found to be within the permissible limit.

Bengaluru

Date: **ABCD**

It is certified that, Mr/Mrs ABCD has carried out the research and has prepared the thesis submitted in partial fulfillment of the requirements for the award of the degree on the above mentioned topic under my guidance and supervision. This thesis has undergone plagiarism check and it is found to be within the permissible limit. Further, this thesis or any part thereof has not been submitted for any purpose to any other University or Institute.

**Dr. XYZ**
**Supervisor**
**School of ………**

**Dr. PQR**
**Co- Supervisor**
**School of ………**

**Director Name**
**Director**
**School of Electrical & Electronics Engineering**

Date:

# CLOCK SYNCHRONIZATION AND LOCALIZATION OF NODES IN WIRELESS SENSOR NETWORK (16)

*(A Thesis submitted in partial fulfilment of the requirements for the award of the degree of Doctor of Philosophy in Mechanical Engineering)* (12)

Submitted by

**ABCD**

(SRN - R21PEE09)

Under the Supervision of

**Dr. XYZ**
Director
School of Electrical & Electronics Engineering
REVA University, Bengaluru

**SCHOOL OF ELECTRICAL & ELECTRONICS ENGINEERING (14)**

**REVA UNIVERSITY (14)**

Rukmini Knowledge Park, Kattigenahalli, Yelahanka, Bengaluru – 560 064

**2021**

REVA UNIVERSITY
Bengaluru, India

## SCHOOL OF ELECTRICAL & ELECTRONICS ENGINEERING (14)

## DECLARATION

I ABCD declare that the thesis entitled **“Clock synchronization and localization of nodes in wireless sensor network”** submitted by me in partial fulfillment of the requirements for the award of the degree of Doctor of Philosophy in Mechanical Engineering, REVA University is based on the results of the research work carried out and reported by me under the guidance of Dr. XYZ, Director, School of Electrical & Electronics Engineering, REVA University.

I also declare that this thesis or any part of it has not been submitted for award of any other degree / diploma of this or any other University / Institute.

I further declare that this thesis has undergone plagiarism verification and it is found to be within the permissible limit.

Bengaluru

Date: **ABCD**

It is certified that, Mr/Mrs ABCD has carried out the research and has prepared the thesis submitted in partial fulfillment of the requirements for the award of the degree on the above mentioned topic under my guidance and supervision. This thesis has undergone plagiarism check and it is found to be within the permissible limit. Further, this thesis or any part thereof has not been submitted for any purpose to any other University or Institute.

**Dr. XYZ**
**Supervisor**
**School of ………..**

**Director Name**
**Director**
**School of ………….**

**Date :**

# PLAGIARISM CERTIFICATE (16)

(To be inserted after collecting the certificate from R&I Council)

# ACKNOWLEDGEMENT (16)
# (Sample only you may change the contents)

First and foremost I would like to express the deepest appreciation to my supervisor Dr. XYZ, Director, School of Electrical & Electronics Engineering, REVA University, Bengaluru, and Co-Supervisor Dr. PQR, Professor, School of Electrical & Electronics Engineering, REVA University who has continually and convincingly conveyed a spirit of adventure in regard to this research journey. Without his guidance and persistent help this thesis would not have been possible.

I sincerely thank the members of the Doctoral Committee, Research Coordinator, External Examiners and Director name, Director, School of Electrical & Electronics Engineering for providing me the valuable suggestions and guidance throughout my research.

I would like to express my sincere gratitude to Dr. P. Shyama Raju, Honorable Chancellor, Dr. M. Dhanamjaya, Vice Chancellor, Dr. N. Ramesh, Registrar, Dr. Beena G, COE, Dr. B. P. Divakar, Dean R&I Council, Dr. Vishwanath R. Hulipalled, Deputy Director R&I Council, for the support extended during my study at the University.

I thank ………. (12)

**ABCD**

# ABSTRACT (16)

# TABLE OF CONTENTS (16)

# LIST OF FIGURES (16)

# LIST OF TABLES (16)

# LIST OF ABBREVIATIONS

| | |
|---|---|
| AOA | Angle of arrival |
| AOTSP | An on demand time synchronization protocol |
| ATSP | Average time synchronization with pairwise messages |
| BACL | Bilateration and comparison localization |
| BIJLTS | Bi iterative algorithm for joint localization and time synchronization |
| BILSLR | Baysian interference, least square and linear regression |

# LIST OF NOTATIONS (16)

| | |
|---|---|
| $\alpha$ | Clock skew of a node |
| $\beta$ | Clock offset of a node |
| $\gamma$ | Intracluster synchronization factor |
| $\lambda$ | Constant multiple for a node |
| $\mu$ | Inercluster synchronization factor |

# CHAPTER I (16)

## INTRODUCTION (14)

The Internet today is pervasive with all the technological advances, in which connected devices to progress information from anywhere in the world via the Internet - the company's databases, the cluster of servers, mobile phones. This collection of inter-networked devices refers to Internet of Things. ------------ (12)

### 1.1 Overview of the Internet of Things

The major idea of IoT is to endow with the network infrastructure through interoperable communication protocols and the software for a better data collection with a suitable connection, exchange of information through the nodes on several heterogeneous networks. Applications of IoT include, home automation systems of smart lighting, healthcare, pollution monitoring, and smart grid. Inappropriately, many connecting of devices to the Internet presents causes a more possible for cybercrime. Analyst Gartner estimates that in 2025 the IoT devices will be used by 64 billion, except tablets, PCs, and smartphones [1]. Individuals and some companies using IoT devices cross the legal agreement. A smart refrigerator was hacked two years ago wherein it sends indecent spam by building the ice cubes. Baby alarms were used for eavesdrop on and still used to converse to the sleeping children. In the year 2016[1], the ever-largest Distributed Denial of Service (DDoS) attack in opposition to Dyn, a provider of significant Domain Name System (DNS) services to companies like Netflix, Twitter, and CNN was done by hacking thousands of security cameras. And again, in the year 2017[2], Wikileaks divulge that Central Intelligence Agency (CIA) has types of equipment for hacking the IoT devices, such as Samsung Smart TVs, used to vaguely record the conversations in hotels or the discussion rooms.

Researchers believe that the integration of IoT with public cloud increases IoT security gaps due to more impending attacks through stealing, and leaking of personal, accessing processing, and networked information. In totting up to that, further moneymaking IoT

attacks were explored, like cryptocurrency mining or the ransomware attacks on medical tools, point-of-sale (POS) machinery, or vehicles. It is important to explore that what makes these devices are so vulnerable in IoT being a runaway train, never going back. Security is not been made very crucial in the progress of these devices creating security on IoT devices with destitute, security absent may be costly, or else slow growth, or sometimes that survive the device performance approaches with term speed and efficiency. The devices that are directly bared to the internet have opened up a backdoor to let the criminals in because of poor network segmentation. Researchers and marketers are engaged in a full range of solutions to protect IoT devices and networks. Instead, there's a long way to go before the standards are established.

## 1.2 IoT Architecture and Protocol Stack

Ongoing research activities propose to provide multi-layered (device, communication, cloud, and lifecycle management layer) security approaches to IoT solution architectures that seamlessly work together to provide complete end-to-end security. The communication layer is defined by IoT Architecture as given in the Figure 1.1 where the Data is received/ transmitted via insecure channels of communication via application layer or Physical networking. The vital technologies concerned in IoT are the Radio Frequency Identification Technology (RFID), the sensing technology, wireless communication, energy-conserving technologies, cloud computing concept, and finally the sophisticated Internet Protocol (IPv6) [2].

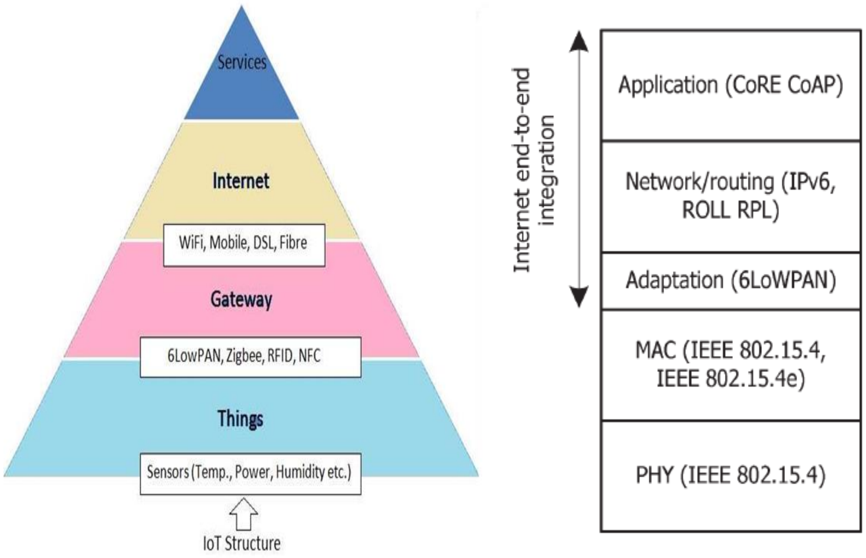
Services
Internet
WiFi, Mobile, DSL, Fibre
Gateway
6LowPAN, Zigbee, RFID, NFC
Things
Sensors (Temp., Power, Humidity etc.)
IoT Structure
Internet end-to-end integration
Application (CoRE CoAP)
Network/routing (IPv6, ROLL RPL)
Adaptation (6LoWPAN)
MAC (IEEE 802.15.4, IEEE 802.15.4e)
PHY (IEEE 802.15.4)

**Figure 1.1:** IoT Architecture & Protocol Stack

The sensor layer is collecting all type of data through physical equipment like RFID readers, sensors, GPS. It uses low battery power and low data rate connectivity. The gateway and the network layer maintain the massive volumes of the IoT data which are produced by the wireless sensor's devices and the smart devices. The network models were designed and intended to support communication Quality of Service (QoS) requirements of latency, scalability, error probability, bandwidth, security while achieving higher levels of energy efficiency. Various applications from the manufacturing and engineering sectors can exploit the use of IoT for overhaul improvement. The applications are mainly categorized based on type of the heterogeneity, network availability, coverage, size, business representations as well as the non-real and real time requirements.

The main characteristics of the different stack protocols are as follows. (1) The IEEE 802.15.4 protocol supports communication with low power consumption at PHY and MAC level [2]. (2) The IEEE 802.15.4 protocol maintains a maximum of 102 bytes for data transmission to the upper stack layers, which is well below the 1280 byte Maximum Transmission Unit (MTU) required by IPv6. (3) The transmission of IPv6 data packets over IEEE 802.15.4 is performed using 6LoWPAN. The adaptation layer enables packet fragmentation mechanisms and reassembly methods. (4) The Routing Protocol for Low-power and Lossy networks (RPL) supports 6LoWPAN environments. (5) The application level Communication is supported by the Constrained Application Protocol (CoAP)[2].

# REFERENCES (16)

[1] Gupta, KrishnaKanth, and Sapna Shukla. "Internet of Things: Security challenges for next generation networks." Innovation and Challenges in Cyber Security (ICICCS-INBUSH), 2016 International Conference on. IEEE, 2016.

[2] Granjal, Jorge, Edmundo Monteiro, and Jorge Sá Silva. "Security for the internet of things: a survey of existing protocols and open research issues." IEEE Communications Surveys & Tutorials, Vol.17, No.3, 2015, PP. 1294-1312.

[3] Yuchen Yang, Longfei Wu, Guisheng Yin, Lijie Li, and Hongbin Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things", IEEE Internet of Things Journal, Vol: 4, No.5, Oct. 2017, PP.1250 – 1258.

[4] Nawir, Mukrimah ,"Internet of Things (IoT): Taxonomy of security attacks." Electronic Design (ICED), 2016 3rd International Conference on. IEEE, 2016.

[5] Alaba, Fadele Ayotunde, "Internet of Things security: A survey." Journal of Network and Computer Applications, Vol.88, 2017, PP: 10-28.

[6] Rghioui, Anass, Mohammed Bouhorma, and Abderrahim Benslimane. "Analytical study of security aspects in 6LoWPAN networks." Information and Communication Technology for the Muslim World (ICT4M), 2013 5th International Conference on. IEEE, 2013.

[7] Rahman, Reem Abdul, and Babar Shah. "Security analysis of IoT protocols: A focus in CoAP." Big Data and Smart City (ICBDSC), 2016 3rd MEC International Conference on. IEEE, 2016.

[8] Rajandekar, Ajinkya, and Biplab Sikdar. "A survey of MAC layer issues and protocols for machine-to-machine communications." IEEE Internet of Things Journal, Vol.2, No.2, 2015, PP. 175-186.

[9] ShaojieWen, Chuanhe Huang, XiChen, JianhuaMa, NaixueXiong and ZongpengLi, "Energy-efficient and delay-aware distributed routing with cooperative transmission for Internet of Things", Journal of Parallel and Distributed Computing, vol. 118, pp. 46-56, August 2018.

[10] SaptarshiDebroy, PriyankaSamanta, AminaBashir and MainakChatterjee, "SpEED-IoT: Spectrum aware energy efficient routing for device-to-device IoT communication", Future Generation Computer Systems, vol. 93, pp. 833-848, April 2019.

# LIST OF PUBLICATIONS (16)

1. G. Kalyani and Shilpa Chaudhari, the paper Titled “Survey of Security Approaches in Internet of Things Solution Architectures for Communication Layer”, Journal of Advance Research in Dynamical & Control Systems, 2019, volume: 11, Issue: 03, pp: 1889-1907. ISSN 1943-023X

2. G. Kalyani and Shilpa Chaudhari, the paper Titled “Survey on 6LOWPAN Security Protocols in IoT Communication”, Kumar A., Paprzycki M., Gunjan V. (eds) ICDSMLA 2019. Lecture Notes in Electrical Engineering, Volume: 601, pp: 696-702, 2020, Springer, Singapore. https://doi.org/10.1007/978-981-15-1420-3