ISSUE - 2

2021-22

ICA-TECH

Instrumentation, Control & Automation TECHNICAL MAGZINE

Department of
Electronics & Instrumentation Engineering

Instrumentation, Control & Automation Technical Magazine ICA-TECH

Department of Electronics & Instrumentation Engineering

Editorial Board	ISSUE-II	Academic Year
Dr G N Swamy, Dr S Srinivasulu Raju	JAN- JUNE	2021-22

TABLE OF CONTENTS

Smart Parking Using RFID Technology

T Siva Sree, III- EIE

Car parking is done in many countries using conventional methods. Check-ins and check-outs involve a wide range of processes. A lot of time gets wasted waiting in queues. The scenario is fast changing with the introduction of smart parking method making use of radio frequency Identification (RFID) technology. As you are aware, RFID is one of the most fundamental technologies that enable wireless data transmission.

Introduction to RFID

RFID is an area of automatic identification that has quietly been gaining momentum in recent years and is now being seen as a radical means of enhancing data handling processes, complementary in many ways to other data capture technologies such as bar coding. Developments in RFID technology continue to yield larger memory capacities, wider reading ranges, and faster processing.

The objective of any RFID system is to carry data in suitable transponders, generally known as tags, and to retrieve data, by machine-readable means, at a suitable time and place, to satisfy particular application needs. Data within a tag may provide identification for an item in manufacture, goods in transit, a location, a vehicle, an animal or an individual.

This system requires, in addition to tags, a means of reading or interrogating the tags and some means of communicating the data to a host computer or information management system. A system will also include a facility for entering, or programming, data into the tags, if this is not undertaken at source by the manufacturer. Quite often an antenna is considered as a separate part of an RFID system.

Both readers and tags have antenna which are essential for communication between the two. An RFID system has the following components: RFID device, that contains data about an item, antenna, used to transmit the RF signals between the reader and the RFID device, RF transceiver that generates the RF signals and the reader, that receives RF transmissions from the RFID device. The read data is passed to a host system for processing.

General structure and design of the system In a study and test setup, parking-lot check-ins and checkouts were configured using a central database system. Hardware components were used for the central management of the parking lot, while software components were used to control the hardware.

Hardware consisted of RFID readers, labels, USB cables, toy cars, barriers with USB port connection and laptop computers. A database management system was used as software to store and manage the vehicle tracking data. Identification data that was read by the RFID reader consisted of 40 bits. The RFID readers utilized were considerably small with circular shape and thus they could easily be attached to the vehicles.

The computers used in this application were connected to the internet. In the database, a main table "Vehicle information" and a sub table "Vehicle Circulation lnfo" were created. The general information about a vehicle was stored in the main table and its circulation information was kept in the sub table.

Vehicle information table consisted of fields such as vehicle ID, plate number, type and model. “Vehicle Circulation lnfo” table was used to monitor a vehicle’s check-in and check-out attempts, the date, the time, the parking-lot information and total parking fee. These two tables were prepared by a database management system and administered through software. RFID reader was connected to a computer’s USB port by USB cable for communication between the developed software and RFID reader. For each of the parking lots, one barrier and one RFID reader were utilized.

A USB connection was established for the barrier as well. All the information about a vehicle possessing an RFID label was easily accessible from the Vehicle lnformation system. When a vehicle arrived at any parking-lot to check-in, the system checks whether it is already registered with it or not. If it is registered, and it does not have any check-in or check-out records available, the check-in information is stored in the database and the barrier lifts off for the vehicle to drive in.

A checking-out vehicle’s identification information is searched in the database first. If it is a registered vehicle and it did not have any unauthorized access, the system would allow its check-out. During the check-out, the system finds its check-in date and time and updates check-out date and time. If a vehicle doesn’t have any previous entry corresponding to it in the database, the initial entry level information of a vehicle is stored in the database. If a vehicle has a previous record stored in the system, there won’t be any secondary information entry, thus avoiding duplication.

If a checked-in vehicle does not get checkedout in the records maintained in the data base, it won’t be able to check-in to any of the parking lots in the city. Only the administrator of the central database could bring a solution to this problem. If two vehicles enter a parking-lot side by side, being within the range of the RFID reader, the system will not read their identification information and process it. To avoid such problems, parking-lot entrances should be designed to enable passage for only one vehicle at a time. Spotlights directly connected to the RFID reader that notify drivers about the availability of parking space in the lot will provide great convenience if located at the entrances of parking-lots.

Failure in internet connection during any process will shut down the connection to the central database. In such cases, a local database will get enabled. When Internet connection is restored, the system will switch back to the remote database.

The system can keep account of payments also, so that vehicle owners need not have to make payments upon every check-out. SPICE (Simulation Program for Integrated Circuits Emphasis) is a powerful general-purpose analog and mixed-mode circuit simulator that offers a total solution for code design tasks. It is used to verify circuit designs and to predict the circuit behaviour.

Brain computer interface and neuroprosthetics

A S Aiswarya Vallika, IV- EIE

A brain–computer interface (BCI), sometimes called a direct neural interface or a brain–machine interface, is a direct communication pathway between brain and an external device. BCIs were aimed at assisting, augmenting or repairing human cognitive or sensory-motor functions. Research on BCIs began in the 1970s at the University of California Los Angeles (UCLA) under a grant from the National Science Foundation followed by a contract from DARPA.

The field has since blossomed spectacularly, mostly toward neuroprosthetics applications that aim at restoring damaged hearing, sight and movement. Thanks to the remarkable cortical plasticity of the brain, signals from implanted prostheses can, after adaptation, be handled by the brain like natural sensor or effector channels. Following years of animal experimentation, the first neuroprosthetic devices implanted in humans appeared in the mid-nineties. Neuro prosthetics Neuroprosthetics (also called neural prosthetics) is a discipline related to neuroscience and biomedical engineering concerned with developing neural prostheses.

Neural prostheses are a series of devices that can substitute a motor, sensory or cognitive modality that might have been damaged as a result of an injury or a disease. An example of such devices is Cochlear implants. The development of such devices has a profound impact on the quality of human life, and research in this field intends to resolve disabilities. The first cochlear implant dates back to 1957. In order to achieve these devices there are many challenges.

Any implanted device has to be very small in order to be to minimally invasive, especially in the brain, eye, cochlea. Also this implant would have to communicate with the outside world wirelessly. Having wires sticking out of the head, eye, etc is not an option. Besides the discomfort and restrictions it would impose on the subject this could lead to infection in the tissue. This bidirectional wireless communication requires a high bandwidth for real-time data transmission; this is a great challenge considering that this data link has to operate through the skin. The minimal size of the implant means no battery can be embedded in the implant, the implant works on wireless power transmission through the skin which is equally challenging as the data transmission.

The tissue surrounding the implant is usually very sensitive to temperature rise so the implant must have very low power consumption in order to assure it won't harm the tissue. Another very important issue is the bio compatibility of the material that the implants are coated with. The more biocompatible these materials are, lesser the tissue reaction that they will cause, thus resulting in less implant risk and longer implant period. Gradually, as these devices become safer and our understanding of how the brain works is enhanced, the use of these devices will become more and more common and help people with severe disabilities live a normal life. The most widely used neuroprosthetic device is the cochlear implant.

There are approximately 100,000 implanted devices in worldwide as of 2020. Today, the use of cochlear implants and pacemakers has become an indispensable fact of life. The future holds an exciting prospect for the everyday use of a variety of neural prostheses.

Opportunities of Blockchain Technology in Healthcare Industry

Yerravarapu Prasanth, IV- EIE

Abstract:

The significance of an agile and widespread healthcare system was evident from the recent pandemic, Covid-19. Healthcare encompasses different stakeholders and many domains that include pharmaceutical supply chain management (SCM), electronic medical records, patient histories, clinical trial results, imaging and scans, insurance claim records, and doctors' information as well. Currently, there are many domains in healthcare with challenges and issues where improvements are due. Blockchain is the single most imperative technology that could be integrated with healthcare to enhance the capabilities in every aspect of the trivial system. In this paper, the benefits of integrating blockchain with healthcare shall be discussed. A discussion of the challenges and possible solutions in healthcare using blockchain shall also be given.

Introduction:

Blockchain is a fast-growing technology that is fundamentally based on a distributed ledger in which the data is stored using blocks. Blockchain technology, which is non-editable, distributed, completely anonymous, and secure, finds applications in many areas other than cryptocurrencies like insurance, SCM and healthcare, etc. A blockchain network has no single owner or organizing entity. It is a distributed network with nodes present in a peer-to-peer topology that are the main executors of all the necessary transactions in a blockchain. Consensus algorithms are used in a blockchain network to make sure the consistency of the blockchain ledger. The general architecture of blockchain consists of various transaction blocks as shown in Fig. 1, connected/linked using hashes, most commonly used SHA256.

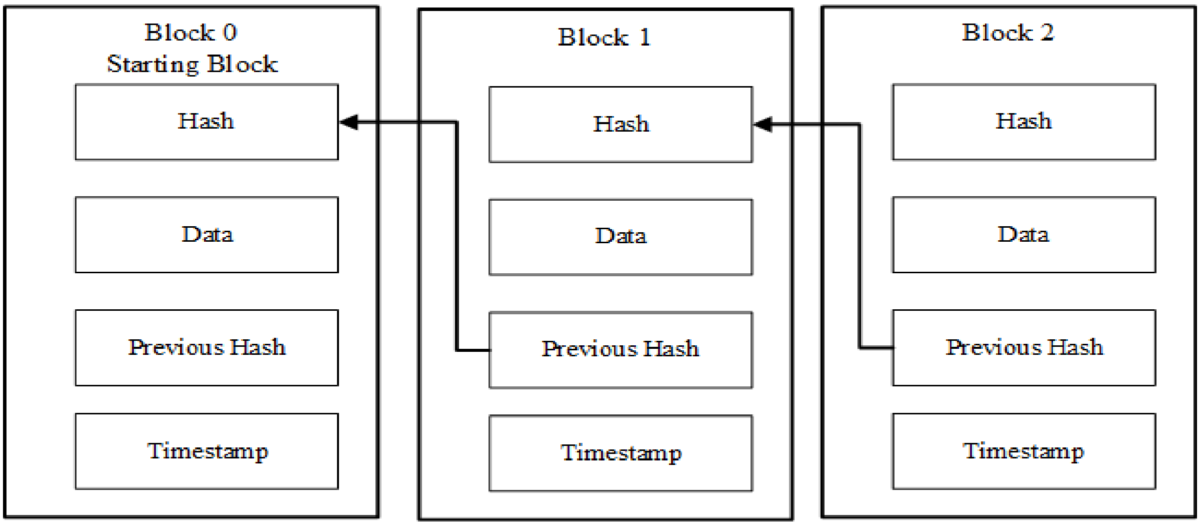


Fig.1: **Blockchain Architecture**

Each block in a blockchain consists of many pieces of information; a timestamp, hash, the necessary transaction data, and the hash of the previous node. AS far as the starting/first block of a blockchain s concerned, it has no previous hash and is essentially known as the genesis block. Healthcare is one area that is characterized by trivial industry practices yet. There are many issues associated with healthcare including privacy, information exchange security, etc., that need to be addressed using sophisticated technologies like Blockchain. This technology not only promises to improve the quality of healthcare support but could also increase the total value (42 million by 2023) generated by the healthcare industry as was reported by Market Research Future. Since blockchain technology inherently provides better security and privacy feature with immutable characteristics, it could easily help in making improved healthcare support by reducing costs and security & privacy issues and enhancing the quality of healthcare. A peer-to-peer topology in a blockchain network and a real-time updating of transactions/records help in the reduction in associated costs. The immutable characteristic of blockchain makes it a very feasible option for all the entities in a healthcare system to access any record at any time without any overhead costs. The probability of losing a record is virtually negligible in a blockchain-based healthcare system.

Why blockchain in healthcare?

There is still a big gap in understanding the complete potential of Blockchain technology as was recently shown in a report by. Nonetheless, this technology is ready to make profound changes in the healthcare system. In a healthcare system, the data, particularly patient data, needs to be exchanged among multiple users securely without compromising privacy. The distributed and immutable nature of blockchain and the storage of records in blocks linked together using cryptographic hashes helps achieve the goal of information exchange in the healthcare system. A patient record can never be modified because any change in a data block would mean changing all the subsequent blocks in the chain which is impossible without the consensus of the network. In any healthcare system, there could be external entities that collaborate with the system, this should not in any way jeopardize the security, information leak, or increased costs. Blockchain provides a transparent and enhanced security system of information exchange with negligible risk to security leaks or modifications. In the blockchain, there are multiple copies of information shared among multiple nodes on a blockchain network. The integrity, security, and consistency of such distributed systems are ensured by many nodes with special roles on the network. If and when a block is created and added to a blockchain, it cannot be eliminated or changed. There are self -executing programs used in blockchain technology known as smart contracts. These are used to execute code that may be complex without any human intervention, thus reducing the costs of observing and contracting. The smart contracts of blockchain can help make completely autonomous applications that could dramatically reduce intermediate costs in a setting like a healthcare system. The Healthcare industry is in dire need of solving the issues related to secure information exchange, cost reductions, and privacy issues. The distributed nature, permission-less and immutable blockchain network may finally address all the challenges and issues in the healthcare industry. The new and cutting-edge technologies in healthcare systems like wearables and remote patient monitoring could reach a profoundly higher beneficial level using blockchain technology. In any healthcare system, data need not be changed or altered. The data should be securely stored that encompasses patients as well as data from any ongoing research or clinical trials. There should also be a real-time observation of patients. All of these features could be achieved using blockchain technology and in particular smart contracts could easily take up the challenge of real-time monitoring of patients.

Benefits of blockchain

The Healthcare system provides healthcare support to individuals using the best possible services available traditionally. There are many challenges and issues with the current environment for providing medical care support and the integration of Blockchain with Healthcare could prove profoundly beneficial. Fig. 2, provides the main areas that would benefit from Blockchain technology.

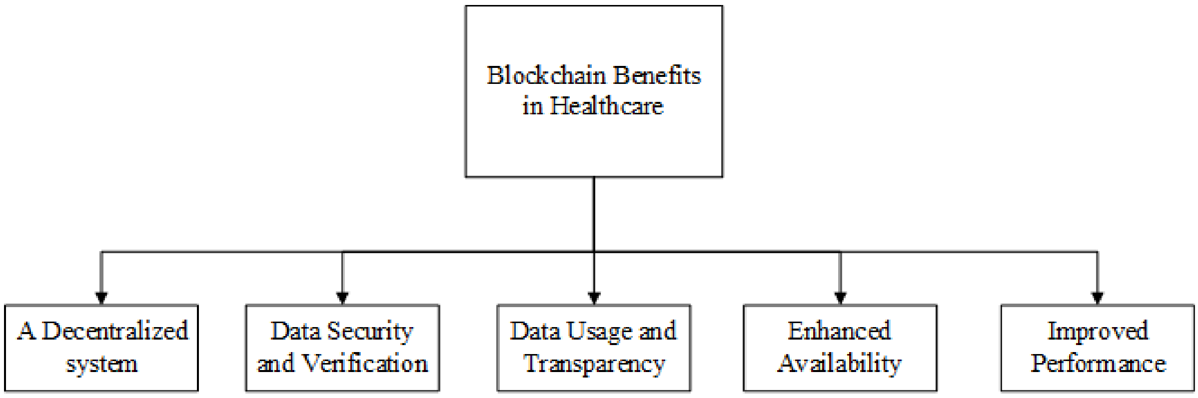


Fig. 2:Benefits of using Blockchain

Decentralized Management System

A healthcare system inherently comprises many entities/stakeholders that are distributed and hence asks for a distributed management system. A distributed and controlled access to all the health data related to patients or any other significant data for any stakeholder of the system can be achieved using a blockchain-based distributed management system.

Enhanced Data Security

All the data in a healthcare system could be saved on a blockchain using cryptographic hashes. The non-editable nature of the blockchain makes this data secure and incorruptible. The health records on the blocks in a blockchain have guaranteed security using encryption. In the modern world of cyber information, there have been tremendous efforts to breach data all around the world. Medical data is one sensitive piece of information that needs to be stored securely and with utmost care. The medical data does not comprise just plain patient data but may include insurance data, medical histories, SCM data, clinical trials, and imaging, etc. Health and Human services have reported many medical data breaches in which 114 million people may have been affected. Blockchain with its distributed ledger characteristic can make hacking very difficult. A hacker does not just have to breach a single point and would be given access to everything on the blockchain. Even if a hacker gets access to a patient's medical record, he would not be able to read the record because of the encryption done on the patient medical records which could only be decrypted using the patient's private key.

Easy Data Verification

Every record stored on a blockchain can be verified quite easily. It would help expedite the processes of insurance claims and the verification of records in pharmaceutical SCM.

Data Association and Usage

A patient's data belongs to a patient and it is in the interest of a patient to decide where his/her data would be used or how it would be used. A patient should have complete control over his/her data without misuse of his/her data by any stakeholders. Blockchain provides strong security protocols using encryption and smart contracts to deal with such issues.

Enhanced Transparency

Blockchain is a transparent technology with a trust-based framework making healthcare applications easily adaptable. As already discussed, any addition to a blockchain would easily be visible to all the participants (in healthcare scenarios, patients) in the blockchain instantly. An effort to rectify a record in the blockchain could easily be detected. The immutable nature of blockchain also makes it suitable for application in healthcare supply chain management systems. For example, detection of a fake drug, tracking of raw materials, and improving standards could be enforced using this technology. Supply chain management of pharmaceuticals currently comprises many loopholes where anyone can fake documents, modify or remove evidence of any fishy business. Turning this SCM into a blockchain-based shared and fundamentally trustworthy framework could prove profound. From acquiring the raw materials to making the drugs to the supply of drugs, a blockchain-based solution could bring the change in healthcare SCM which people have always dreamed of. Any medical worker doing any piece of work anywhere in a healthcare system could be added to their skillset in the blockchain which could eventually help trace and verify a person's skill set required for a particular job in a specific medical setting. Transparency of blockchain technology could also help in the real-time processing of insurance as already discussed earlier. The insurance companies could be given access to the blockchain network where they can verify the patient details regarding any medical care in real-time and process the claims instantly. While trying to provide the best medical care to a patient possible, doctors sometimes need to share the medical histories of patients with other colleagues or collaborators, which in the current setting is a very hectic and time-consuming job. Blockchain networks can give access to the medical histories of patients to the collaborators with no hindrance whatsoever.

Enhanced Availability

The health data on the blockchain is stored in multiple places which provides enhanced availability of data (100% availability). Also, since the technology is immutable and incorruptible, it becomes more robust and resilient to data losses. Due to the distributed nature of blockchain where data is digitally stored at multiple locations, a single point of weakness does not exist. Consequently, this reduces the chance of a medical record being not available. Also, the patients are at liberty to share their data with any third party they desire. In addition to this, the data is provided to the healthcare service providers in real-time, also guaranteeing fault-tolerant access to this data 24x7 which ensures suitable response in emergency medical situations. This real-time data could also prove beneficial to researchers to recognize and work on any parameter that might inhibit the proper response to any medical emergency (for example epidemics) in the future.

Improved Performance

The performance bottlenecks in a trivial healthcare system make timely processing of almost all the important operations while providing healthcare support an impossible job. The decentralized nature, the real-time information dissipation, and the robust and fault-tolerant availability of medical records in the blockchain eliminate all the bottlenecks and helps improve the performance of healthcare support profoundly.

Challenges and Possible Solutions

The challenges in different aspects of healthcare is shown in Fig. 3. The discussion of many potential solutions is given below.

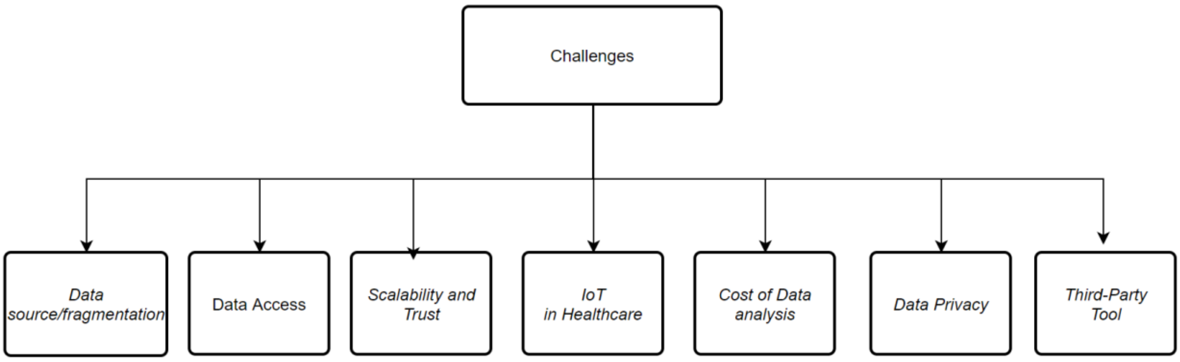


Fig. 3: Challenges in Healthcare

Data source/fragmentation

Data comes from a plethora of sources like patients, doctors, clinics, and many more in a fragmented form. A distributed network like a blockchain can cope with all the data produced separately by different stakeholders of the healthcare system.

Data Access

The data shared among multiple stakeholders of a healthcare system in addition to the intermediaries for policy management etc., drastically inhibit the timely and concurrent access to the data. Concurrent and timely access to the data on a distributed network of blockchain is easily achieved without the fear of jeopardizing the integrity and consistency of the data.

Scalability and Trust

A healthcare system is a collaboration of many stakeholders where trust issues could hinder the smooth timely function of the system. Storage of images in the form of MRIs or scans which could take TBs of memory for direct storage in a blockchain is one of the biggest challenges. The scalability would be an issue with the increase in demand for participation nodes due to the need for more ever-increasing storage space. The researchers in provide a solution, an off-chain solution in which heavy data is stored in a repository away from the blockchain. The security of this data would still not be compromised because the access to this data will again be through the blockchain. The patient would be at liberty to decide what and who can use his data hence enforcing privacy policies as well. A robust verification and validation process for all participating nodes and the use of the consensus algorithms in a blockchain network makes it less risky.

IoT in Healthcare

IoT integration in healthcare is a new but already implemented technology in which thousands of IoT sensors collect data from patients, doctors and clinics, etc., and there is no proper way to keep track of it or handle it. A blockchain-based IoT can save the overhead of keeping track of IoT devices for tampering by making the information exchange among the devices secure using cryptographic measures.

Cost of Data analysis

Healthcare systems currently lack the internal provisions for the analysis of data and hire third-party personnel/tools for the analysis of data which in turn increases the cost. Blockchain-based distributed and non-intermediary processing and analysis can easily reduce analytical costs.

Data Privacy

In the current setting of a healthcare system, there are no provisions for the privacy of patient’s data. Anyone can virtually access any data. Blockchain makes data secure and enhances data privacy using cryptographic measures and data integrity and consistency using consensus algorithms and smart contracts. The users may still not be quite familiar with the usage of cryptographic measures to secure their data. Authorizing access to their medical data requires encryption/decryption key pair which could be a little too much to handle for the users. A GUI-based application for handling such situations may suffice. There may also be emergencies where the medical data of a patient may be required by the healthcare personnel without the proper authentication available. Hence, a wallet may be maintained to hold certificates as was proposed by.

Third-Party Tools

The mediators and third-party collaborators manipulate the data in their interest to benefit from it as much as possible. In a healthcare system, many hospitals may work in collaboration to promote interoperability programs and access a patient’s records. But the challenge arises when third-party collaborators access these records and there is no way of knowing who and when these records are being accessed. Data breaches could also leak by giving access to third-party tools. Blockchain eliminates all intermediaries to provide a boundary-less distribution of data in a very secure manner.

Conclusion

Blockchain is a futuristic technology with seemingly a plethora of applications in almost every area. In healthcare, blockchain provides a tremendous potential for improvement in the current setting of the healthcare environment; from storing and accessing medical records to treatments and drug supply chain management. It was observed that we are still in the infancy of integrating blockchain with healthcare. Many benefits of blockchain in healthcare were discussed with a focus on security and privacy concerns. The fundamental challenges in healthcare and the solutions using blockchain were also discussed. Many technical challenges and limitations still exist in blockchain and hence inhibit the complete implementation of such a profound technology, but this is the single most technology that promises to cater to all our healthcare problems. In the future, the challenges of throughput, size, bandwidth, and security, etc., in blockchain have to be properly addressed before a complete transformation of healthcare using blockchain could be possible.

REFERENCES

[1] Correia, M.: From Byzantine Consensus to Blockchain Consensus. In: Essentials of Blockchain Technology, pp. 41–80, Nov. 2019.
[2] Wang, L., Shen, X., Li, J., Shao, J., Yang, Y.: Cryptographic primitives in blockchains. In: Journal of Network and Computer Applications,
vol. 127, pp. 43–58, Feb. 2019.
[3] Ben Ayed, A.: A Conceptual Secure Blockchain Based Electronic Voting System. In: International Journal of Network Security & Its
Applications, vol. 9, no. 3, pp. 01–09, May 2017.
[4] Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H.: An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In:
IEEE International Congress on Big Data (BigData Congress), Jun. 2017.

Design and Implementation of Fuzzy PID Controller for Controlling the Speed of Robotic Vehicle System

P Venkata Sushma, IV-EIE

Abstract:

In recent years, researchers have been developed robotic vehicles for different applications especially in agriculture system. This system consists of a Robotic Vehicle which directs through the area in the required path doing digging as it goes through the path. This paper includes the design and simulation results of conventional and fuzzy PID controller for tracking the speed of the robotic vehicle. The proposed controller has been implemented to track the desired speed and tracks the direction of the robot vehicle. Ziegler Nicholas and Auto tune based PID algorithm have been used by some authors to find the tuning parameters of P, PI and PID Controllers for achieving the desired set point. The Conventional PID and fuzzy PID algorithms are modelled and simulated in the MATLAB environment using programming code and Simulink. Finally, the performance analysis is compared with conventional controller PID and fuzzy PID. Fuzzy PID controller will be able to track the desired speed of robotic vehicle with accuracy in performance indices as compared to conventional PID controller, specified by the designer.

Introduction

The Robot Vehicle is fundamentally intended to work the field to the predefined area and the vehicle movement towards the specified path, in any route be it forward or opposite, have to be in a straight line. Otherwise, the vehicle might move indiscriminately, not cultivation the bottom in an exceedingly line. If this operation is distributed manually, the output is painfully low. If the whole agricultural operation is administered using Robotic vehicle, like the proposed one, which is unmanned, then care has got to be taken to make sure that the movement of the vehicle is within the desired direction always. The automated feedback system is used to track of the direction of wheels and speed of the robotic vehicle and contrasts it with the desired direction and takes measurement to reduce the error, i.e deviation among the desired speed and direction. There are many methods described to accomplish the control of direction and control of speed of the wheels of programmed automated vehicles utilizing PID controller. A. Harsha Vardhan et.al. implemented and demonstrated the fuzzy PID controller for tracking the position of a DC motor. Fuzzy Logic, PID and Fuzzy PID controllers are used for tracking the position of DC motor and the performance analysis of an open loop system was carried out to conclude that fuzzy PID provides better tracking as compare to PID and Fuzzy Logic controllers. MPC and adaptive PID controller were used to demonstrate level control of nonlinear conical tank system by, T.Pushpaveni et,al,. the authors used relay feedback method to tune the PID parameters, and MPC algorithm designed and simulated in MATLAB for multi set point tracking of level control. Authors concluded that, MPC tracks the servo and regulatory response without overshoot and within less time. Vinothkumar. C, et.al., used the tuning methods - Ziegler Nicholas and Cohen coon for tuning the controller parameters of P, PI, and PID for level control of nonlinear systems used in pharmaceutical industry. The open loop performance analysis was carried out to conclude that the PID controller was able to track the level with in specified limits of nonlinear system. Srinivasulu et, al., designed and implemented the DMC control algorithm for concentration control of CSTR process in MATLAB Simulation environment. The control algorithms PID and DMC are analysed and found Dynamic matrix control provided better response for tracking the concentration of CSTR System. Fuzzy PID controller was used to track the temperature set point of a continuous stirred tank reactor process by T.K.S. Ravi Kiran et,al,. A relay feedback technique is used to find the PID parameters using ultimate gain and period. Fuzzy PID was implemented for the process using data process technique by authors and concluded that advanced controller like Fuzzy PID enhances the performance of temperature control in CSTR Process.

The aim of this work is demonstrating the speed control of robotic vehicle using conventional and fuzzy PID control algorithms. Mostly the process behaves nonlinear with nature and offers an inspiring task for industries to reach the level at preferred set point. The most popular basic and widespread control algorithm is PID (integral proportional derivative control algorithm) used as feedback controller for industry process. Due to its remarkable performance, PID controller is widely used to control strategy for most industrial automation process for improving the efficiency. In this paper, fuzzy PID control algorithm are derived and implemented the P, PI, PID and fuzzy PID in the MATLAB environment using Simulink.

Controller Design for Robotic Vehicle

The typical goal of control hypothesis is to figure answers for the best possible restorative activity from the controller that outcomes in framework dependability, that is, the framework will hold the setpoint and not sway around it. The fundamentally utilized regular controllers are conventional controllers. They are P, PI, and PID Controllers. PID controller has proportional, integral as well as derivative so these control actions are as follows. PID is an additive combination of Proportional, Integral, and Derivative actions and is shown in figure 1. The PID tuning parameters are obtained using Ziegler Nicholas Method and employed in the MATLAB Simulation to analyze the performance of open loop and closed loop system.

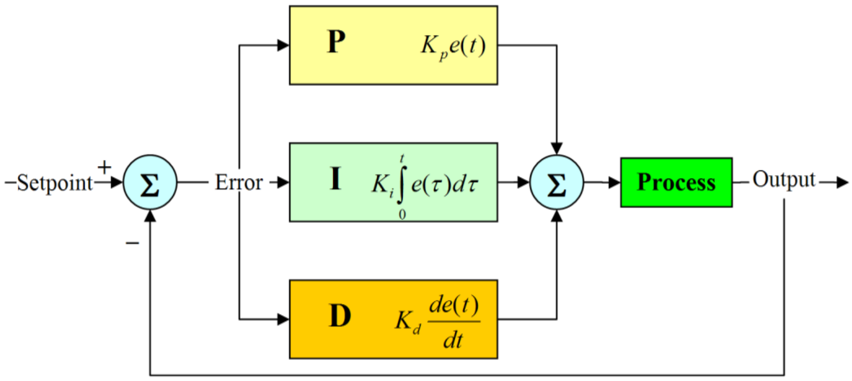


Fig 1. Block diagram of PID Controller

Fuzzy Logic Controller:

Design and implementation of intelligent control systems became an interest area in the field of robotics. Artificial intelligence plays a vital role and provides the effective methodology in designing the control systems for robotic vehicle. Fuzzy logic controller mostly used when the analytical model of the system is not accurate, to track the desired response mostly for control problems in manufacturing and product-based industries. A simple rule based " IF X AND Y THEN Z" method is used to frame the rules based on the membership functions for solving the control engineering problems instead of striving to analytical model of a system. Fuzzy logic mostly used in analysis and design the control system for engineering problems, which are very complex in nature, difficult to attain the model of a system. The expert knowledge and his experience about the process will be required to frame the rule base, which effectively used for setpoint tracking of the robot vehicle system. The basic architecture of fuzzy logic is shown in figure 2. From the figure 2, the four principal techniques are involved in the fuzzy logic are knowledge base block, decision making block, fuzzification and defuzzification units. Membership functions are used to frame the rules using knowledge base and inference engine implies fuzzy operations on rules, finally the fuzzified control output transforms to numeric value to process into the system.

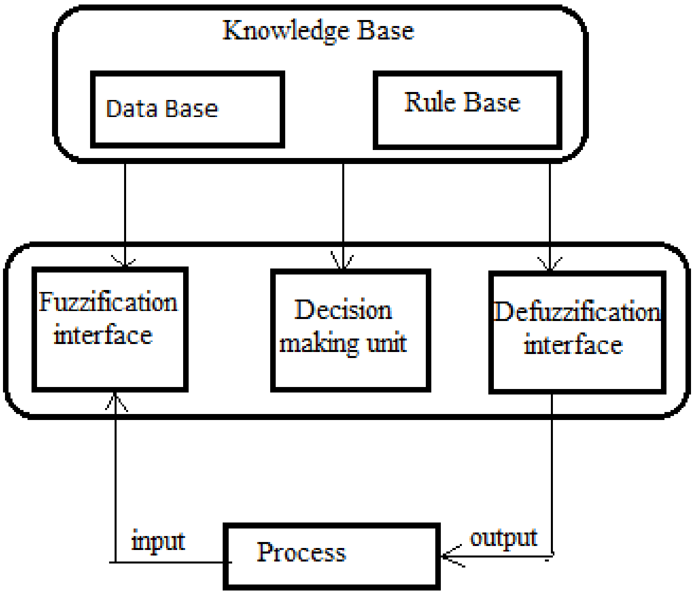


Fig.2: General structure of fuzzy Inference System

Fuzzification:

The error input in fuzzy set consists 7 triangular memberships as shown in figure 4. Figure-5 illuminates the fuzzy set relates to change in error input contains 7 triangular memberships. Figure-6 shows the fuzzy set of the output contains 7 triangular memberships.

Control Base Rules:

The fuzzy rules are framed using the knowledge base by considering the input and output relationship of system. The rules are defined and presented in table 1, based on the expert knowledge about the system.

Defuzzification:

Centroid method is used a defuzzification technique, which converts the fuzzified value into the crisp value, and the fuzzy controller has been implemented in MATLAB Simulink.

Fuzzy PID Control Algorithm

The formation of fuzzy PID algorithm is shown in fig:3, comprises of two parts; one is the conventional PID controller and the second one is fuzzy controller. The proposed work consists of three output and two input fuzzy PID controller for tracking the speed of the robot vehicle. Error and change in error are considered as input to fuzzy PID, and the output of controller is to find the tuning parameters of the PID controller such as proportional gain, integral gain, and derivative gain. The tuning parameters of PID controller are adapted in online to meet the desires specified by the designer to achieve the good stability.

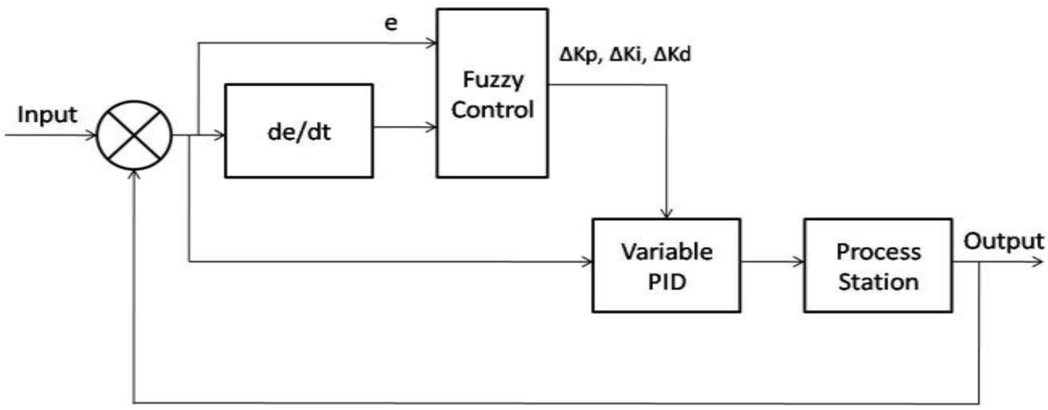


Fig.3 Structure of Fuzzy Adaptive PID

Model of Fuzzy PID controller:

Fuzzy controller creates the input precise magnitude to fuzzy quantity. The knowledge base contains the experienced expertise of the flow process base. Fuzzy Data comprises the membership function of each linguistic variable. The controlling rules are from the fuzzy data base. The fuzzy quantity converts to non-fuzzy quantity using defuzzification method, in which the centroid method is mostly used to convert into precise quantity.

Membership Function:

Triangular and gaussian membership function is used by fuzzy controller to frame the linguistic variables. The input varies from -7 to +7 and the fuzzy subset are Negative Big, Negative middle, Negative small, Zero, Positive small, Positive middle and Positive Big correspondingly labeled as NB,NM, NS, ZO, PS, PM, PB. The scaling and quantization factor perform an crucial role in the execution of the fuzzy controller.

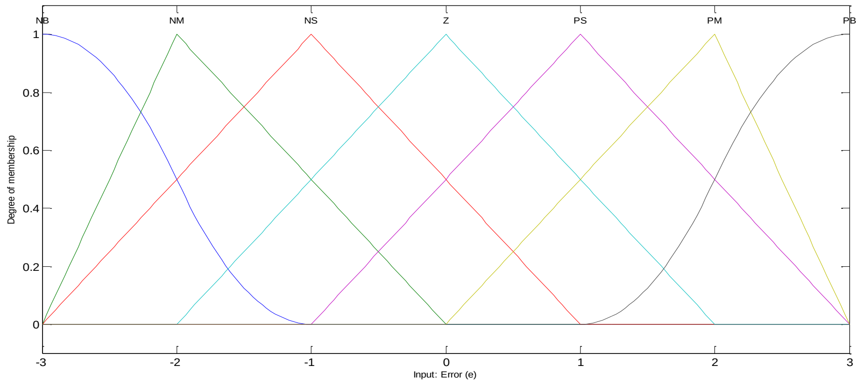


Fig.4 Membership Functions of Error Input in Fuzzy Set

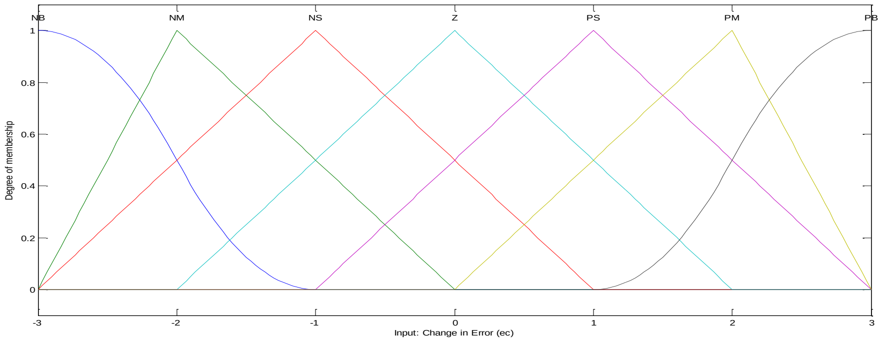


Fig.5 Membership Functions of change in Error Input in Fuzzy Set

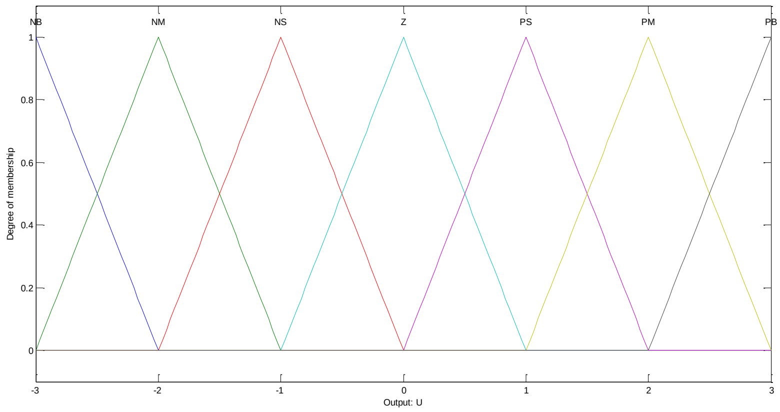


Fig.6 Membership Functions of output in Fuzzy Set

Control Rules of the Fuzzy Controller:

The control rules are framed to attain the best implementation of the fuzzy controller to tune the PID parameters for satisfactory and good stability response of the system.

Table 1: Rule base implemented in fuzzy PID

E / CE	NB	NM	NS	ZE	PS	PM	PB
NB	NM	NS	Z	NS	NB	NB	NM
NM	NS	Z	PS	NS	NB	NM	NM
NS	NS	PS	PS	Z	NM	NM	NS
ZE	Z	PS	PM	PS	NM	NS	NS
PS	PS	PM	PM	PS	NS	NS	Z
PM	PS	PM	PB	PM	NS	Z	PS
PB	PM	PB	PB	PM	Z	PS	PS

The rules are used to create the flow.fis in MTLAB environment using programming. The fuzzy sets along with the membership functions and the rule base forms as the fuzzy controller, the output of the fuzzy PID tunes the PID controller parameters for desirable speed tracking of the system. The inference engine used here is the Mamdani Inference engine.

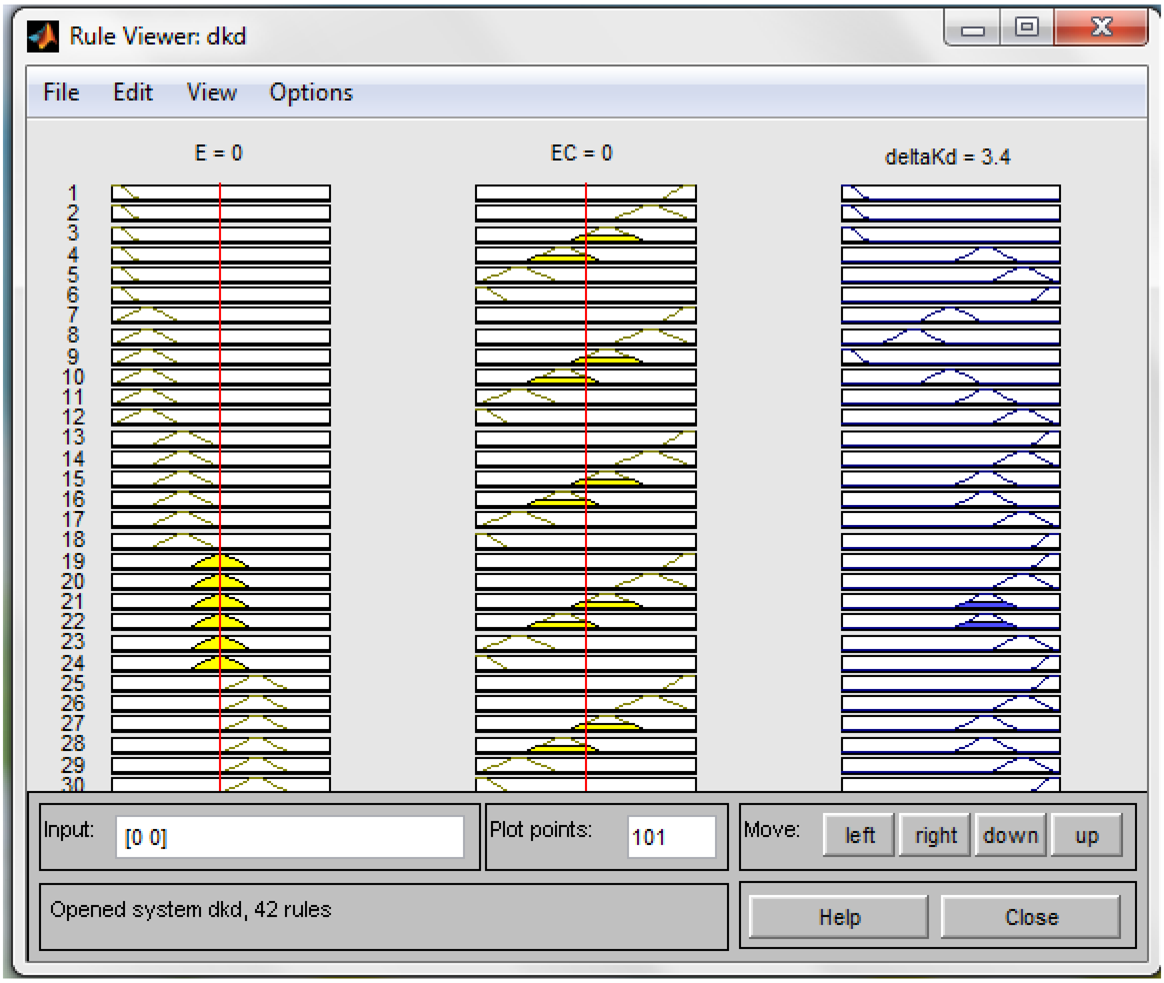


Fig.7 Fuzzy PID rule viewer

Performance analysis and simulation results

The Open and closed-loop studies have been done for the speed control of robotic vehicle system to achieve desired level setpoint. MATLAB software (R2020a) is used to obtain the analytical results and analysed the performance criterion. The tuning parameters of PID controller are designed using Zeigler Nichols closed loop method and used to analyse the closed loop performance of the system with controller. The open-loop studies are analysed in MATLAB (R2020a) and figure 8 shows the respective results. The response of first principal model is validated with open loop response and shown in figure 8.

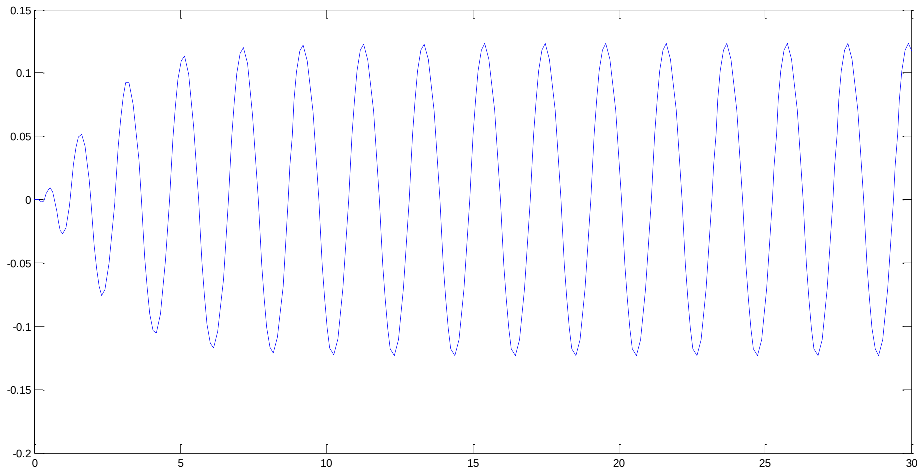


Fig 8: Closed loop response of speed control of vehicle system

The closed loop response for speed desired level tracking is shown in figure 9. From the figure, we can conclude that the PID controller able to track the setpoint, which relates speed of the vehicle within acceptable range of oscillations with specified rise time. The performance criteria of ISE, ITAE, IAE and ISTE are found for the closed loop system and given in table 2.

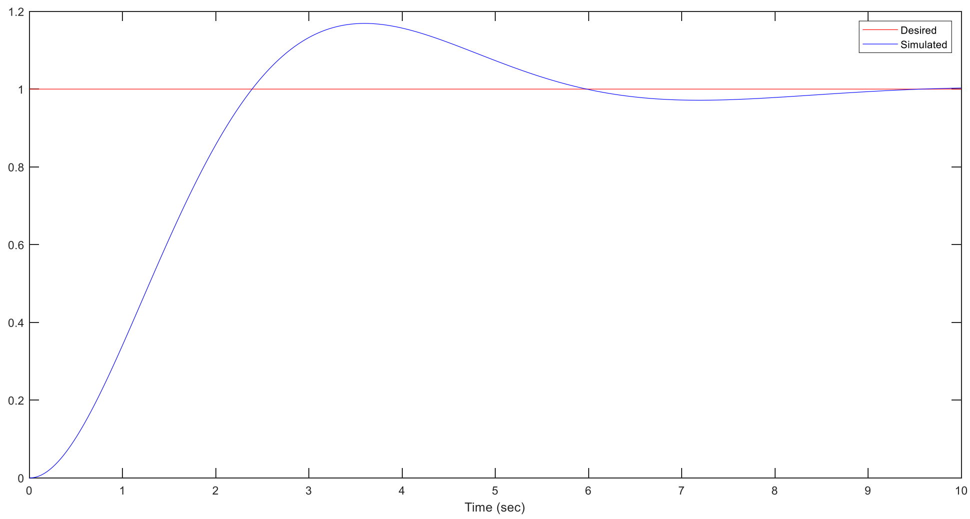


Fig 9: conventional PID response of speed tracking system

Table 2: Tuned parameters of PID controller

Performance parameters	**Tuned values**
Rise time	6.214 seconds
Settling time	9.03 seconds
Overshoot	52.27 %

Gain margin	Inf dB @ Inf rad/s
Phase margin	83.2 deg @7.98 rad/s
Peak	10.07
Closed loop stability	Stable
IAE	7.254
ITAE	59.243
ISE	4.987
ITSE	44.354

PID controller provides overshoot for depth tracking; these drawbacks are overcome by using a fuzzy PID controller, to tune the parameters of PID adaptively with respect to change in the plant dynamics. Fuzzy logic is used to tune the controller parameters with constraints in a discrete domain to track the set point. The fuzzy algorithm for desired level of speed is designed and simulated in MATLAB software. Initially, the system will be sampled into a discrete domain, then the system passed to the controller block to change the process variable with respect to the controller output. The MATLAB Simulink diagram is shown in figure 10. The response of the fuzzy PID controller is given in figure 11. The performance tuning parameters are given in table 2. From the results, we can conclude that the fuzzy PID controller stabilizes the process, speed of the vehicle reaches the setpoint. Hence, we can conclude that fuzzy PID controller able to track the speed setpoint of vehicle system without any overshoot, with less settling time and zero rise time and the system will stabilize even in the case of perturbations.

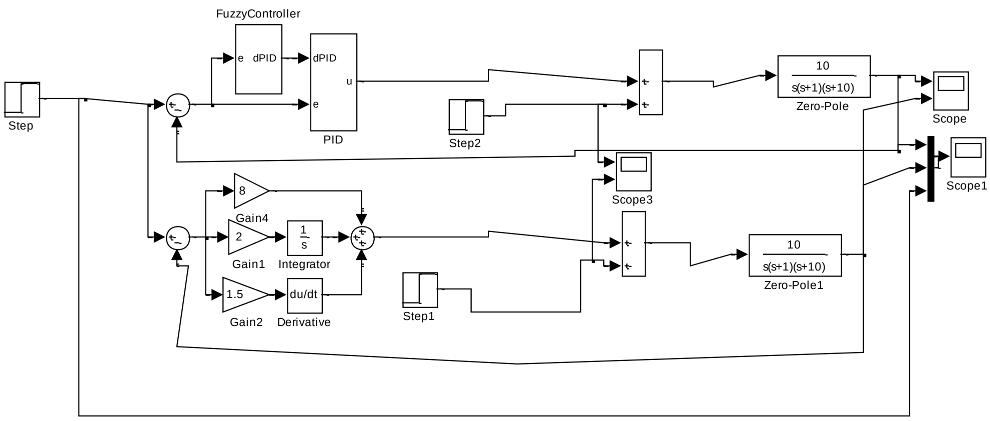


Fig 10: Implementation of fuzzy PID controller for desired response of the system.

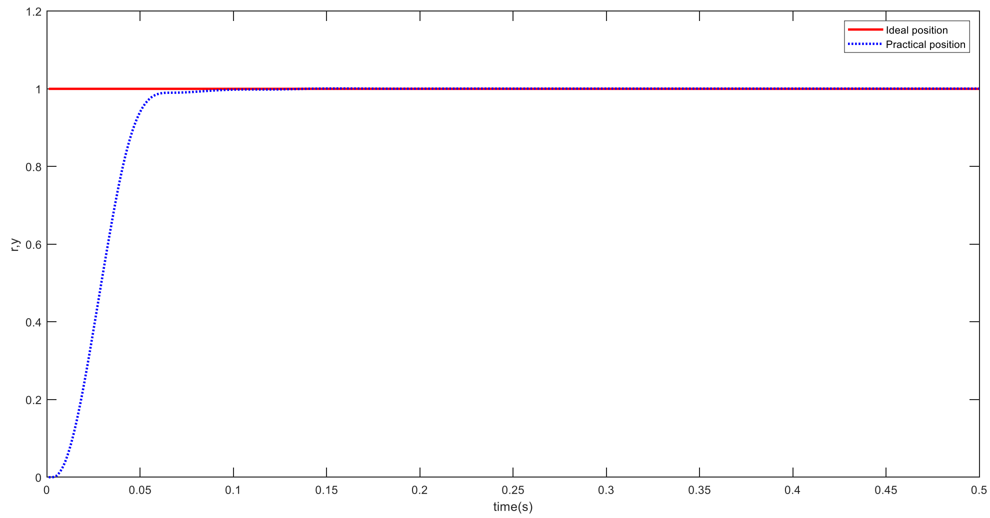


Fig 11. The response of Fuzzy PID controller for speed tracking of robotic vehicle

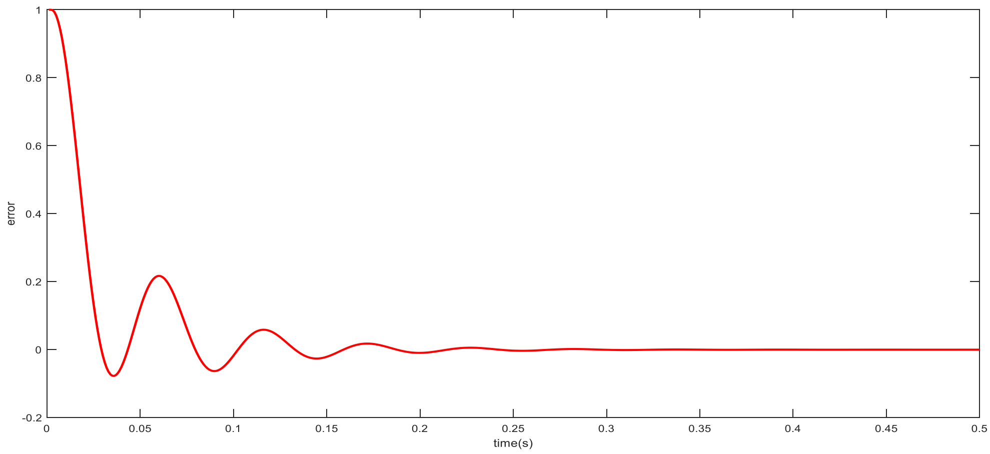


Fig 12. The controller response for speed tracking of the system

Table 2: Performance results of fuzzy PID controller for speed tracking system

Performance parameters	**Tuning values**
Reference time (T_{ref})	6 sec
Settling time (T_s)	0.06 sec

Table 3: Qualitative similarity of PID and fuzzy PID controller

Performance	PI-Controller	Fuzzy Controller
ISE	2.915	2.857
IAE	4.46	4.116
ITAE	20.61	20.45

Conclusion

In this work, the authors considered the speed control of robotic vehicle system at agriculture is concerned with direction and speed of vehicle. Conventional controller PID and fuzzy PID are used to track the speed setpoint and rejects the perturbations at output level. Zeigler Nichols is used to determine the PID parameters using ultimate gain and period. The tuning parameters are imposed in MATLAB environment for tracking of speed of vehicle system. From the response of the PID, we can conclude that the PID controller provides satisfactory response for level tracking with oscillations and overshoot. The performance analysis IAE, ISE, ITAE, ISAE are carried out for a closed loop system. Fuzzy logic is used to track the speed by tuning PID parameters adaptively for robotic vehicle system. The performance indices for fuzzy PID controller also carried out and conclude that, fuzzy PID rejects the disturbance and tracks the level without oscillations, less setting time. Hence, fuzzy PID provides best performance as compared to conventional PID controller considered in this work.

References

[1] Ravi.V.R and Thangavelu Thyagarajan, “Adaptive Decentralized PI controller for two conical tank interacting level system”, Arabian Journal for science and Engineering, Vol.39, No12, 2014, pp.8433-8451.

[2] A. Harsha Vardhan, A. Sai Bharadwaj, S. Srinivasulu Raju , N.Archana [2013] Implementation of Fuzzy Pid Controller And Performance Comparision With Pid For Position Control Of Dc Motor, International Journal of Engineering Research and Development, Volume 7, Issue 9 (July 2013), PP. 78-84.

[3] T.Pushpaveni, N.Archana, M.Chandana [2013] Modelling and Controlling of Conical tank system using adaptive controllers and performance comparison with conventional PID, International Journal of Scientific & Engineering Research, Volume 4, Issue 5, May-2013.

[4] Vinothkumar. C, Esakkiappan. C [2019] Level Control of Nonlinear Hopper Tank Process in Pharmaceutical Industry using Ziegler Nicholas and Cohen Coon Tuning Techniques, International Journal of Innovative Technology and Exploring Engineering (IJITEE), Volume-8 Issue-10, 2019.

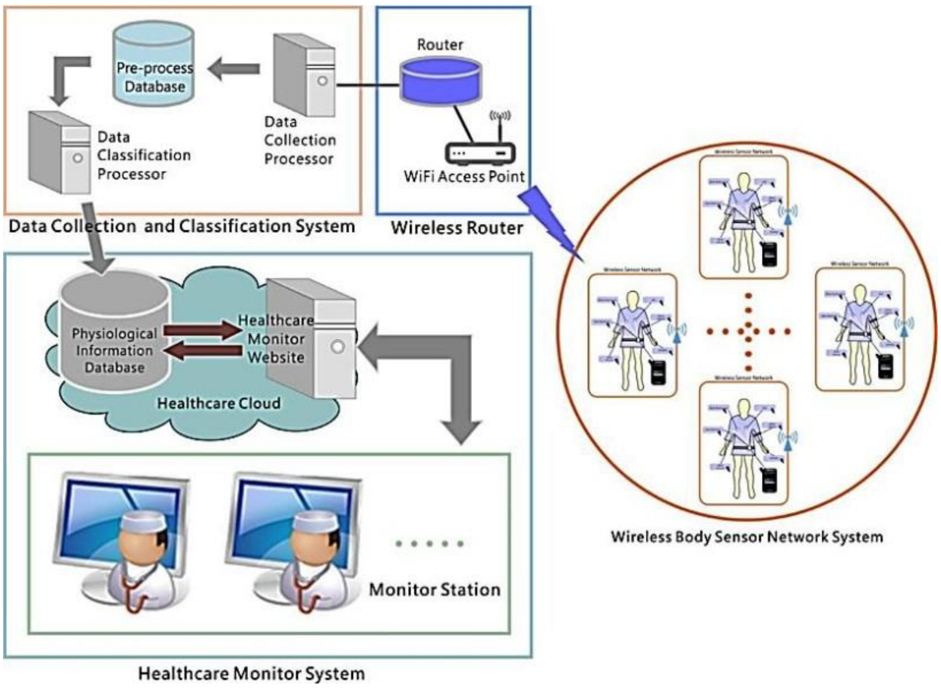
Wireless Body Sensor Networks for Remote Health monitoring

P Akhil Sai, III- EIE

Wireless Body Sensor Networks have been popularly employed to measure people's physiological parameters, particularly for disease monitoring, prevention, and treatment. In this study, we propose a smartphone-based WBSN, named Mobile Physiological Sensor System (MoPSS), which collects users' physiological data with body sensors embedded in a smart shirt. A patient's vital signs are continuously gathered and sent to a smart phone in a real-time manner. The data are then delivered to a remote healthcare cloud via WiFi. After performing necessary classification and analysis, the health information of individual patients is also stored in the cloud, from which authorized medical staffs can retrieve required data to monitor patients' health conditions so that when necessary, caregivers are able to reach the patients as soon as possible and provide required assistance.

A. Mobile Physiological Sensor System (MoPSS)

The MoPSS has three functions, including sensing, communication, and management. The first function, i.e., sensing, is to employ a



set of physiological sensors embedded in the mentioned wearable smart shirt to measure user's physiological signals.

Wearing this shirt, the patient is able to move freely and comfortably. The second function, i.e., communication, is referred to the processes of delivering physiological data and controlling instructions to a backend server through wireless networks. The transmission protocols include Bluetooth, WLAN (i.e., WiFi) and 3G/4G in the future, when 5G is online, it will be employed. The last function, i.e., management, represents that server-side is responsible for collecting, classifying and monitoring the physiological data, and furthermore, being able to issue warning messages to medical professionals or caregivers whenever the physiological data are abnormal. The architecture of MoPSS platform as shown in comprises three main systems, the wireless body sensor network system (WBSNS), the data collection and classification system (DCCS), and the healthcare monitor system.

One of the many applications of Wireless Body Area Network is in medial environment where conditions of patients are continuously monitored in real time. In order to deploy a complete wireless senor network in healthcare systems, wireless monitoring of physiological data from a large number of patients is one of the current needs. A wireless network containing small interdependent sensor nodes is called WSN (wireless sensor network). Such a wireless sensor network system is very suitable to be used in hospital environments to reduce human errors, to reduce health care cost, to provide more time to health professionals to deal with other important issues. Physiological data are to be measured and monitored with the help of this proposed system. The data that is measured by these sensor nodes is sent to a base station using RF (radio frequency) communication. The communication between the nodes and the base station can be a single hop communication or it can be a multi hop communication depending on the remoteness of the sensor node. The base station also controls the whole network. On each sensor node there are various hardware components. Some of those are Microcontroller, Sensor or Transducer, Radio Frequency Transceiver, Battery or some other power source. Several other components are used for signal processing purpose to bring the sensor output signal in proper form and for proper power supply required for main components. The components required for this purpose are voltage regulators, Amplifiers, resistors and capacitors. The main purpose of this system is to achieve the communication between different sensor nodes and a single receiver simultaneously. The receiver that is base station should be able to display the information received from the sensor nodes. Three similar nRF24L01+ nodes were designed and tested to monitor patient's data. An ATmega328 microcontroller is used to design both the sensor nodes and at the base station. These microcontrollers are programmed in C with Arduino 1.0.5-r2. The signal received from the sensors is converted from analog to digital by the microcontroller and delivered it to nRF24L01 where it is sent by the radio. The communication between base station and PC is established by a USB connection. PC is used as a display device.

Heart rate is the number of heartbeats per unit of time and is usually expressed in beats per minute (bpm). In adults, a normal heart beats about 60 to 100 times a minute during resting condition. The resting heart rate is directly related to the health and fitness of a person and hence is important to know. This system has incorporated a microcontroller-based heart rate and body temperature measurement system that uses optical sensors to measure the alteration in blood volume at fingertip with each heartbeat and LM35 sensor for body temperature. The heartbeat sensor consists of an infrared light-emitting-diode (IR LED) and a photodiode. The IR diode transmits an infrared light into the fingertip (placed over the sensor unit), and the photodiode senses the portion of the light that is reflected back. The intensity of reflected light depends upon the blood volume inside the fingertip. So, each heartbeat slightly alters the amount of reflected infrared light that can be detected by the photodiode. The changing blood volume with heartbeat results in a train of pulses at the output of the photodiode, the magnitude of which is too small to be detected directly by a microcontroller.

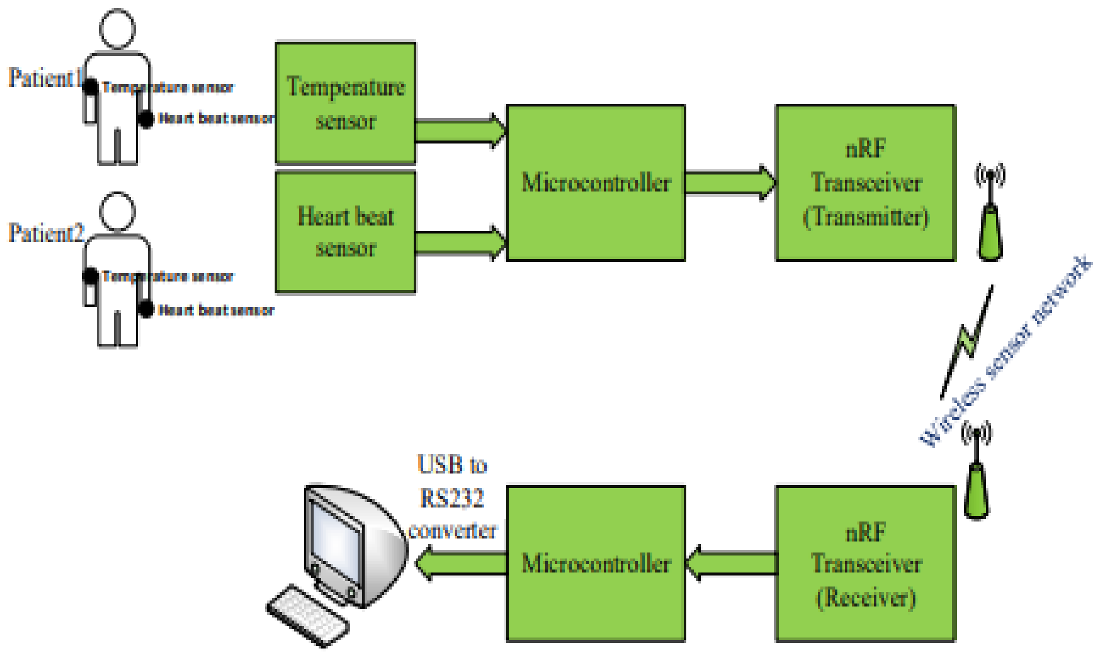


Fig:1 Block diagram of patient health monitoring via wireless body area network

Therefore, a two-stage high gain, active low pass filter is designed using two Operational Amplifiers (Op-Amps) to filter and amplify the signal to appropriate voltage level so that the number of pulses within a certain interval (say 15 sec) can be counted by a microcontroller and easily determined the heart rate in bpm. Fig 1 is given below indicate block diagram of patient health monitoring via wireless body area network. This might be the wireless monitoring system caretaker of a medical doctor to multi-patients.

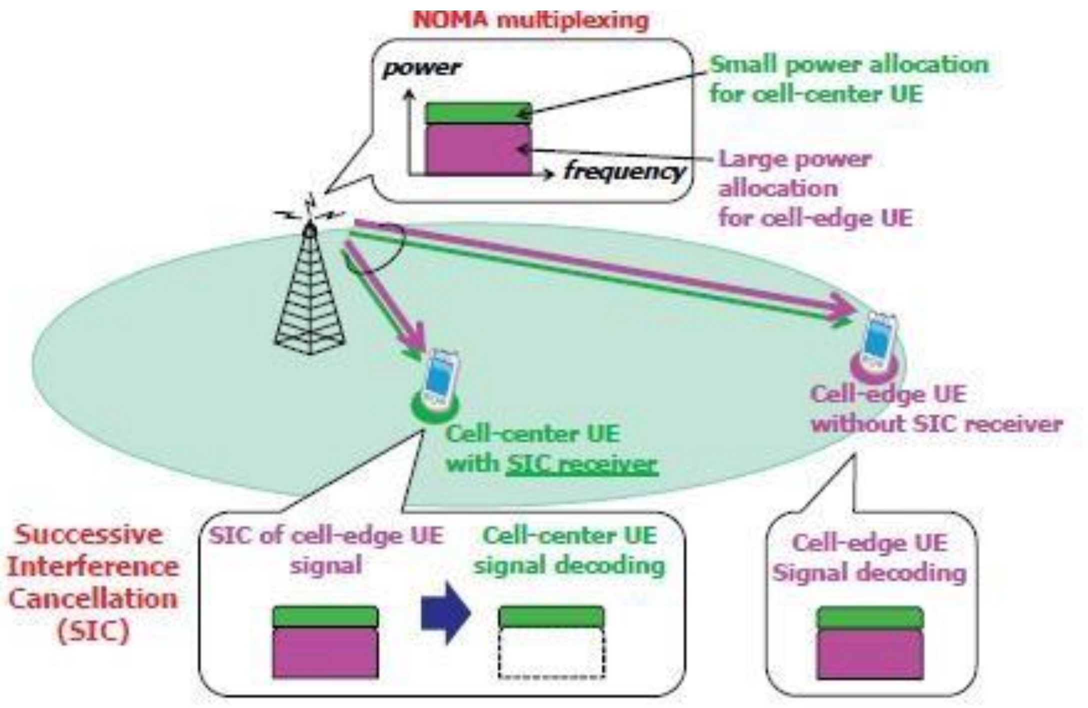
Non Orthogonal Multiple Access (NOMA)

A Snehaja, IV-EIE

The expanding interest of mobile traffic and the Internet of Things postures testing necessities for 5G wireless communications, such as more spectral efficiency and massive connectivity of users. Non-orthogonal multiple access (NOMA) is a fundamental empowering innovation for the fifth-generation (5G) wireless networks to meet the requirements on less latency, maximum reliability, massive connectivity, improved fairness and high throughput. The basic idea behind NOMA is to serve multiple users in the same resource block, such as a frequency and time slot, subcarrier or spreading code. The NOMA Concept can be viewed as special cases and proposed as a 5G multiple access schemes. In this multiuser assigning strategy is different from Traditional orthogonal multiple access technologies. It can provide much more device connections by assigning non orthogonal resource allocation. NOMA is supporting many users by assigning non-orthogonal resource and hence introduces a controllable and measurable amount of inter-user interference that can be mitigated with the aid of sophisticated multi-user detectors at the cost of increased receiver complexity.

Various novel approach of NOMA schemes recently has been investigated for Fifth Generation, such NOMA in power-domain and NOMA in code-domain, including multiple access strategies relying on low- density spreading, sparse code multiple access, lattice partition multiple access, multi-user shared access, as well as pattern division multiple access. Moreover, standardization work on NOMA has been started in the Third Generation Partnership project (3GPP) named multi-user.

superposition transmission (MUST). In Power-domain NOMA superposition coding is utilized in the transmitter section and successive interference cancellation is used at the receiver end. The superposition coding principle is to combine many users in the same time slot and frequency band. NOMA can expand the number of network connections by introducing measurable amount of symbol collisions.



Superposition coding at the transmitter and successive interference cancellation (SIC) at the receiver makes it possible to utilize the same spectrum for all users. At the transmitter site, all the individual information signals are superimposed into a single waveform, while at the receiver, SIC decodes the signals one by one until it finds the desired signal. Figure 2 illustrates the concept. In the illustration, the three information signals indicated with different colors are superimposed at the transmitter. The received signal at the SIC receiver includes all these three signals. The first signal that SIC decodes is the strongest one while others as interference. The first decoded signal is then subtracted from the received signal and if the decoding is perfect, the waveform with the rest of the signals is accurately obtained. SIC iterates the process until it finds the desired signal.

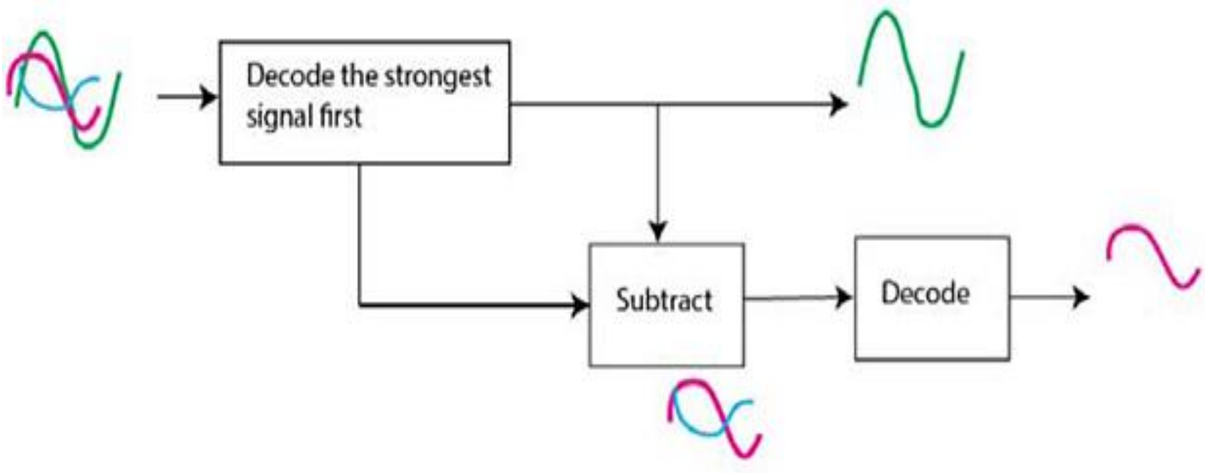


Fig:2. Successive interference cancellation.

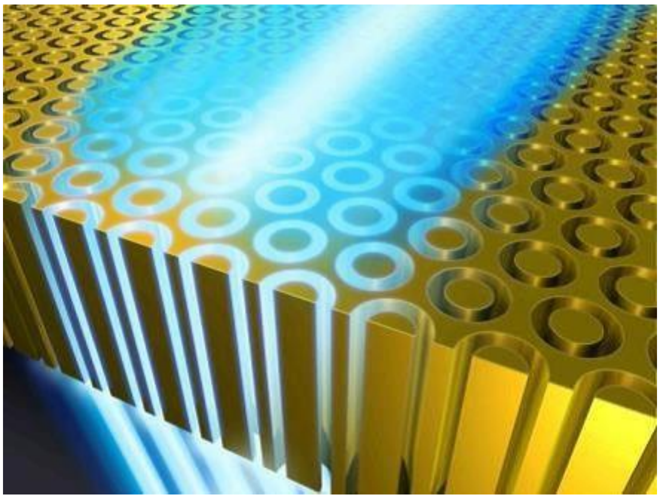
The success of SIC depends on the perfect cancellation of the signals in the iteration steps. The transmitter should accurately split the power between the user information waveforms and superimpose them. The methodology for power split differs for uplink and downlink channels.

Photonic Metamaterials

N Aleshwari, II- EIE

The word “Meta” is taken from Greek whose meaning is “beyond”. “Metamaterials” has the exotic properties beyond the natural occurring materials.

These are the materials that extract their properties from their structure rather than the material of which they are composed of Electromagnetic field is determined by the properties of the materials involved. These properties define the macroscopic parameters permittivity ε and permeability μ of materials. Electromagnetic metamaterials (EM) are the materials which have a new sub section within electromagnetism and physics. EM is used for optical and microwave applications like, band-pass filters, lenses, microwave couplers, beam steerers, and antenna randoms. A metamaterial affects lesser on electromagnetic waves as compared to wavelength of electromagnetic radiation. The Photonic metamaterials are the type of electromagnetic metamaterials that designed to interact with optical frequencies is known as Optical metamaterials. Photonic metamaterials radiate the source at optical wavelengths. Furthermore, the sub wavelength period differentiates the photonic metamaterials from photonic band gap structure. This is because the optical properties do not arise from photonic band gaps, rather from a sub wavelength interaction with the light spectrum. The metamaterials with the capability of zero index of refraction (ZIMs) and negative values for index of refraction (NIMs) is the active area of research in optical materials.



Photonic metamaterials are artificially engineered optical materials containing nanostructures which give them truly remarkable optical properties. These structures are made from at least two different materials (often involving both metals and dielectrics). They are normally periodic, with the period being small compared to the optical wavelength. Therefore, the special optical properties do not arise from photonic bandgaps as for certain photonic crystals, but rather from an interaction which is more similar to that of atoms or ion in a normal solid medium. In contrast to photonic bandgap materials, photonic metamaterials can be described as homogeneous optical materials, much like natural materials, although with partly rather unusual material parameters. For example, some metamaterials have a negative relative permittivity ε and/or a negative relative permeability μ. Others have a near-zero ε value. Such properties lead to very peculiar wave propagation phenomena, such as negative refraction, propagation with very small phase delays, and an extremely large nonlinear index.

There is a more general class of electromagnetic metamaterials, operating in different frequency regimes. Many of such metamaterials have been realized for microwaves, where the wavelengths are much longer than in the optical domain, and thus it is easier to fabricate sub-wavelength structures. Photonic metamaterials are generally more difficult to realize, but substantial progress in the area of nanotechnology has been achieved particularly since the year 2000.

Structures Containing Nano-Resonators

Photonic metamaterials typically contain some kind of metallic nanoscopic electromagnetic resonators, even though it is not always obvious from looking at the shapes of the structures that these acts as resonators. An early approach, which has been taken over from previous work in the microwave domain, is based on split-ring resonators (Figure 1). These can be considered as simplified LC circuits, where the inductance has been replaced with a not fully closed metallic ring and the capacitor is formed by the opening in that ring. Such resonators can also have approximately rectangular forms or (if the opening is made larger) like horseshoes. The resonances of such a resonator can be in the mid-infrared domain (with wavelengths of a few microns) when its width is reduced to the order of a few hundred nanometers. Note that multiple resonances with different frequencies may occur, but the lowest-frequency resonance is often most relevant for the application.

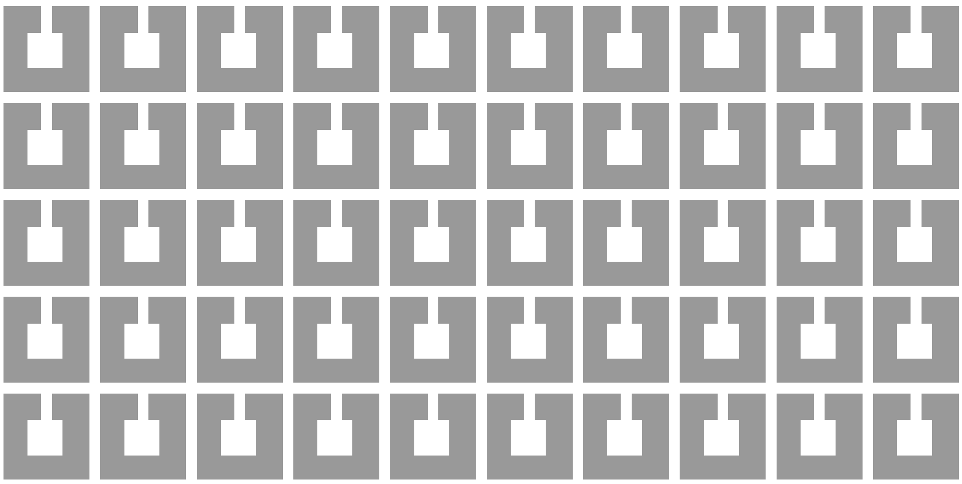


Figure 1: One layer of a photonic metamaterial, containing metallic nano-resonators on a non-conducting (dielectric) substrate. Light impinging such a structure in a direction perpendicular to the shown plane can excite resonances and experience unusual propagation effects.

Such metal–dielectric composites can be fabricated, e.g., with lithographic methods. A frequently used metal is gold. Silver is better suited for high frequencies, but is more difficult to process due to its tendency to be oxidized.

Certain experiments are made only with single layers (monolayers) as described above; these are also called photonic metasurfaces, and many interesting optical functions can already be implemented with those. Three-dimensional structures (3D metamaterials) can be made by stacking such arrays in the vertical direction with a period which is again well below the optical wavelength.

When light impinges such nano-resonators, it can excite electromagnetic oscillations. These are particularly strong for frequencies near the resonance frequency, but the most interesting optical effects may occur somewhat above or below the resonance. As the period of the structure is well below half the optical wavelength, there are no photonic bandgap effects, and the effect on light propagation can be described with a (frequency-dependent) effective relative permittivity ε and relative permeability μ of the metamaterial. (The latter can strongly deviate from 1 even if no (ferro)magnetic materials are used.) In addition, one may need a bi-anisotropy parameter ξ, which describes the coupling of electric field strength E and magnetic field density B, or magnetic field strength H and electric displacement field D. Such couplings can occur, e.g., because in a split-ring resonator and electric field can induce a ring current, generating a magnetic field, and a magnetic field can induce a current which leads to the build-up of an electric field. However, ξ can be zero for reasons of symmetry if structures are combined in a suitable way. Still more simplified forms of resonators may consist only of a periodic arrangement of short wires, or of metallic pieces with other shapes. Such forms can be used at shorter wavelengths, now reaching the red end of the visible optical spectrum. There are also metamaterial structures where the whole metallic structure is electrically connected, in contrast to the isolated nano-resonators as described above. Furthermore, there are structures with genuinely three-dimensional building blocks, such as short helically wound wires (helical antennas), which are sensitive to the direction of circular polarization. Such three-dimensional structures can be fabricated, e.g., with direct laser writing in polymer materials, combined with subsequent processing steps for introducing metallic parts.

Special Optical Properties of Metamaterials

As explained above, the optical properties of metamaterials can be described with the permittivity ε and the permeability μ, and in some cases in addition the bi-anisotropy parameter ξ. Whereas for ordinary optical materials, μ is very close to 1, μ can have totally different values in metamaterials, even though these usually do not contain ferromagnetic materials.

All three parameters are generally frequency-dependent and often also dependent on the propagation direction and polarization state of the light. Also, these parameters are not necessarily real (apart from ξ, which is zero at all frequencies for certain structures). The non-negligible optical losses of typical metamaterials (particularly when operating at high frequencies) lead to substantial imaginary parts of ε and μ.

The magnitude of the refractive index is determined by the following equation:

$$n^2 = \varepsilon\mu - \xi^2$$

For purely real ε and μ, and assuming $\xi = 0$, the refractive index n is real but can be positive or negative. The sign of the refractive index is chosen such that Snell's law correctly describes the direction of the refracted beam at an optical interface.

The electromagnetic *impedance* of a material is given by

$$Z = \sqrt{\frac{\mu\mu_0}{\varepsilon\varepsilon_0}}$$

As the impedance depends on μ / ε, whereas the refractive index depends on $\mu \cdot \varepsilon$, two media with the same refractive index do not need to have the same impedance, if μ can vary. (For ordinary optical media, the refractive index determines the impedance and vice versa, as μ is very close to 1.) Similarly, two media can have the same impedance while differing in the refractive index. This is relevant, e.g., for the magnitude of reflections from optical interfaces, which depends on the different impedances. For example, there would be no reflection at the interface between vacuum and a medium with $\mu = \varepsilon = -1$, although the refractive index changes from +1 to −1: the impedance is the same on both sides of the interface.

Another interesting point is that the impedance can be extremely large for a material with very low ε but a normal value of μ. In that case, the reflectivity of an interface to another (ordinary) optical material can exhibit very strong reflection; it becomes difficult to get any light into such a low-ε material. That can be a reason to search for materials where μ also gets small, avoiding a huge impedance. The following subsections discuss photonic metamaterials with optical properties which are of particular interest.

Near-zero Epsilon Materials

Materials with very small ε also exhibit a very low refractive index (assuming that μ is not very large). That can have very peculiar consequences:

- The optical wavelength in such material (for a given optical frequency) becomes much longer than in an ordinary material. The oscillation at different positions in the material can occur with nearly the same optical phase.

- Refraction of light coming from such a medium into an ordinary optical medium works such that the propagation direction in the latter is nearly independent of the incidence angle.

- Radiative properties can be substantially modified: spontaneous emission can be suppressed, while laser gain can be high. That could be used for thresholdless lasers.

- The nonlinear index can become very large, because it is proportional to the χ(3) coefficient divided by the refractive index and its real part.

Negative-index Media

If both ε and μ are negative (→ double-negative metamaterial) and ξ is zero, one can show that the phenomenon of negative refraction occurs at interfaces between vacuum and the metamaterial. (For a bi-anisotropic material with $\xi \neq 0$, negative refraction can also occur [16].) As illustrated in Figure 2, the refracted beam is not on the usual side. This can be described with a negative refractive index, changing the sign of the angle in Snell's law.

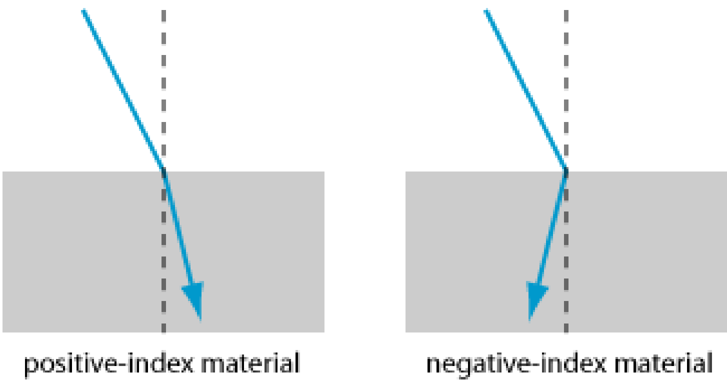


Figure 2: When a beam coming from vacuum hits a negative-index material (right side), the refractive beam inside the medium is on the same side of the surface normal as the incident beam. This is in striking contrast to the situation for “ordinary” positive-index materials (left side). The reflected beams have been omitted in the drawing.

Negative refraction has a number of consequences, leading to additional very unusual optical properties. In particular, the wavefronts of the refracted beam travel toward the interface, i.e., in a direction opposite that of the energy flow (as indicated by the Poynting vector). The direction of the Poynting vector is still given by $E \times H$, but as B is now in the direction opposite to H, the Poynting vector is opposite to the direction of $E \times B$. For that reason, such media are also called left-handed metamaterials (LHM): a left-hand rule instead of the usual right-hand rule delivers the direction of the Poynting vector from E and B. The term “left-handed” is somewhat unfortunate as it may suggest a (non-existing) relation to the phenomenon of chirality, as discussed below.

A convex lens made of a negative-index material could be defocusing rather than focusing, and a concave lens could be focusing. Even a simple plate (with planar and parallel end faces) of a negative-index medium could act as a lens. If the refractive index is -1, this could even lead to a superlens (perfect lens), creating images of objects with a resolution not limited by diffraction. It has been shown, however, that this property would be achieved only if the refractive index is extremely close to -1 [5] – so close in fact that such an application appears utterly unrealistic. Still, superlenses based on a modified scheme are possible [3, 6], where however the distance from the object to the lens must be extremely small, and the effect is thus less intriguing. Note also that there are superlenses based on effects other than negative refraction.

Very peculiar effects would occur if some object could be embedded in a negative-index metamaterial. Depending on its depth in the medium, it may appear strongly magnified and distorted for an observer outside the material. It should even be possible to make cloaking devices (invisibility cloaks), which can hide objects within them against viewing with light from outside, although probably only in a very limited frequency range.

Chiral Media

As mentioned above, there are also metamaterials containing metallic helical nanowires. These have a certain handedness, which can lead to substantially different optical effects for light with different directions of the circular polarization. It is possible to obtain metamaterials which are highly absorbing for one circular polarization direction and have a high transmittance for the other polarization direction. The resulting device can be called a circular polarizer. A negative refractive index is not required for that phenomenon.

Challenges for Operation at Short Wavelengths

A first difficulty with metamaterials for operation at short wavelengths, e.g., in the visible spectral region, is the fabrication of very fine structures such that their period is still well below the optical wavelength (within the medium, not just in vacuum). Some lithographic techniques are just sufficient to fulfill that condition, partly by using shorter wavelengths for the fabrication and partly by achieving a sub-wavelength resolution. Other techniques such as direct laser writing can also be employed. The speed of such fabrication methods may limit the size of the parts made within a reasonable time.

More fundamental limitations arise from the properties of the materials used. In particular, there are no perfect conductors for frequencies of hundreds of terahertz. Therefore, particularly devices for the highest frequencies exhibit relatively high optical losses.

SELECTING THE RIGHT IOT GATEWAY

G Meghana, II- EIE

IoT gateway platforms are an essential component in planning any IoT architecture. Selecting the right one should often be the starting point.

As the trend for the Internet of Things (IoT) accelerates with the number of connected devices surges, the demand for IoT gateways has also increased and is forecast to continue to grow exponentially.

The global IoT gateway market is set to grow at a rate of 30.9% between 2017 and 2023 (according to a research report 'IoT Node and Gateway Market by Hardware, by End-Use, and Geography-Global Forecast to 2023' by Markets and Markets).

The need for IoT gateways is realised because isolated systems are rapidly transforming to the ubiquitous Internet-enabled system (also known as 'connected devices') that can be used to capture and communicate information by leveraging diverse wireless connectivity technologies to IoT gateways for unified edge-analytics.

In other words, IoT gateways play a vital role by providing the fundamental building blocks to develop secure and powerful wireless connectivity between IoT devices and IoT Cloud based applications.

The Internet of Things (IoT) is starting to appear everywhere in many shapes and forms. But security is one of the hurdles that could trip up the growth of the IoT. Following security principles used in enterprise computing can help clear that hurdle.

The selection of an appropriate IoT gateway can be a confusing and daunting task for factory owners and manufacturers. The correct gateway will enable manufacturers to leverage the potential of IoT and other Industry 4.0 applications in their processes.

Consequently, this article reviews ten key steps involved in selecting the right gateway for your industrial needs.

10 key considerations for choosing an Industrial IoT gateway

1. What is the objective of the gateway?

The first phase of IoT gateway implementation involves evaluating the main objective and functionality required from the gateway. This should be the main guide for the selection process.

Let's consider two examples that illustrate this concept.

A factory owner may want to schedule preventative maintenance on machines on the factory floor in order to prevent the breakdown of machinery and costly repairs. To achieve this goal, sensors that measure general performance would have to be installed on the machines. The gateway selected in this case would have to be able to collect this data securely and have built-in alerts that inform the factory owner if a certain machine is overheating or about to go offline.

The gateway would then transfer the performance data to the analytical processing unit in the cloud. The analytical processing unit would evaluate the trends in performance over time of all the machines and be able to see which machines are experiencing performance issues. Consequently, the factory owner could schedule preventative maintenance on the machines experiencing performance issues when needed.

In another scenario, a farmer may want to improve his crop yield and automate irrigation on his farm. In this case, the farmer would have to install multiple sensors on his farm that measure environmental factors such as soil moisture, light, temperature and humidity. The gateway model selected would have to be able to collect data from the sensors, filter the data and send only the needed data to the irrigation system for automation. Additionally, the gateway would have to transfer all the data to the analytical processing unit in the cloud. The analytical processing unit would then evaluate trends and the farmer could see which factors are affecting his crop yield and determine the necessary remedial action.

It is clear from the above examples that the ideal gateway will differ based on the ultimate objective and functionality needed.

2. How much data does the gateway need to collect from the sensors?

Some situations may involve the deployment of hundreds of sensors, whereas in other situations there may be over ten thousand sensors at one location, and each sensor is taking a series of thirty readings per second. Analyzing the data volumes required is the next important step in the gateway selection process.

Additionally, based on the data volume requirements, the manufacturer has the option of installing more than one gateway, so this is another key factor that needs to be taken into account.

3. Does the data being collected from the sensors need to be filtered?

Data from sensors can be collected and then sent directly to the analytical processing unit in the cloud. However, in many IoT projects not all the data from the sensors is needed or the gateway may have to perform some pre-processing operations on the data obtained from the sensors before it is sent to the analytical processing unit.

Therefore, a manufacturer may have to purchase a gateway that can filter the data from the sensors extensively and perform more than one pre-processing operation on the data.

Gateways capable of performing these advanced pre-processing and filtering operations are called edge-analytics-enabled gateways.

4. Where will the gateway be installed?

A gateway may need to be installed in an HVAC unit or at high altitudes and, as a result, the gateway would need to be robust and able to operate in extreme conditions.

Some gateway models are designed to operate in harsh conditions of temperature ranges of -30° C to 70° C, altitude ranges of 15 m to 5000 m, and allow for high shock and vibration situations. The factory owner needs to ensure that they select a gateway that is suitable for the operating environment.

5. Which connectivity options, protocols and interfaces are provided by the gateway?

Many IoT platforms utilize close-range connectivity options such as Bluetooth and Ethernet, with Wi-Fi and Wireless LAN for longer range connectivity needs. Increasingly, manufacturers and factory owners are choosing to monitor operations in their factories or plants remotely, using their smartphones. There are IoT gateway models which do accommodate wider-range connectivity options such as GSM/GPRS-based and LTE-M.

Not all IoT gateways are created equal in this respect and generally, the less expensive the gateway, the fewer connectivity options are provided, which is an important factor to consider.

Standard protocols such as TCP/IP and HTTP should be supported by the gateway, as well as protocols such as Modbus, MQTT and OPC UA. Furthermore, multiple serial interfaces, LAN interfaces and USB ports should be features of a gateway that is utilized in an industrial context.

6. How much data can the gateway store?

Industrial gateways deployed in factories, usually collect multiple sensor readings every second. However, situations such as network failures may arise and as a result the gateway will need to store this data while the network issues are being remedied.

Most gateway models currently available on the market have storage capabilities, but a gateway installed in the typical industrial setting needs to be able to store a significant amount of data and for longer periods of time. It is advisable therefore to invest in a gateway that allows for expansion of storage and additional micro-SD slots so that the gateway can store at least 20 GB of data.

7. Does the gateway have built-in security features and options?

Securing gateways is critical for the security needs of the entire IoT platform. While most modern gateways have built-in security options, it is still worthwhile to check which encryption standards the gateway is using, whether the gateway provides authentication processes as well as whether the gateway can detect tampering.

8. Is the gateway certified?

The gateway model should be FCC/CE/IC certified, in accordance with the standard compliance required for electronic products. There are additional certifications such as Mobile PTCRB/GCF and safety certifications, which are worthwhile to note.

9. Do any existing devices, machinery and legacy equipment need to be integrated into the IoT platform?

Many factories and manufacturers often use legacy equipment and machinery with long life spans. It is often not economically viable or possible to upgrade these devices in order to connect to the cloud directly. In these cases, the gateway chosen should have support for the existing devices and be able to connect to the legacy equipment in order to ensure that all the data from the factory is integrated.

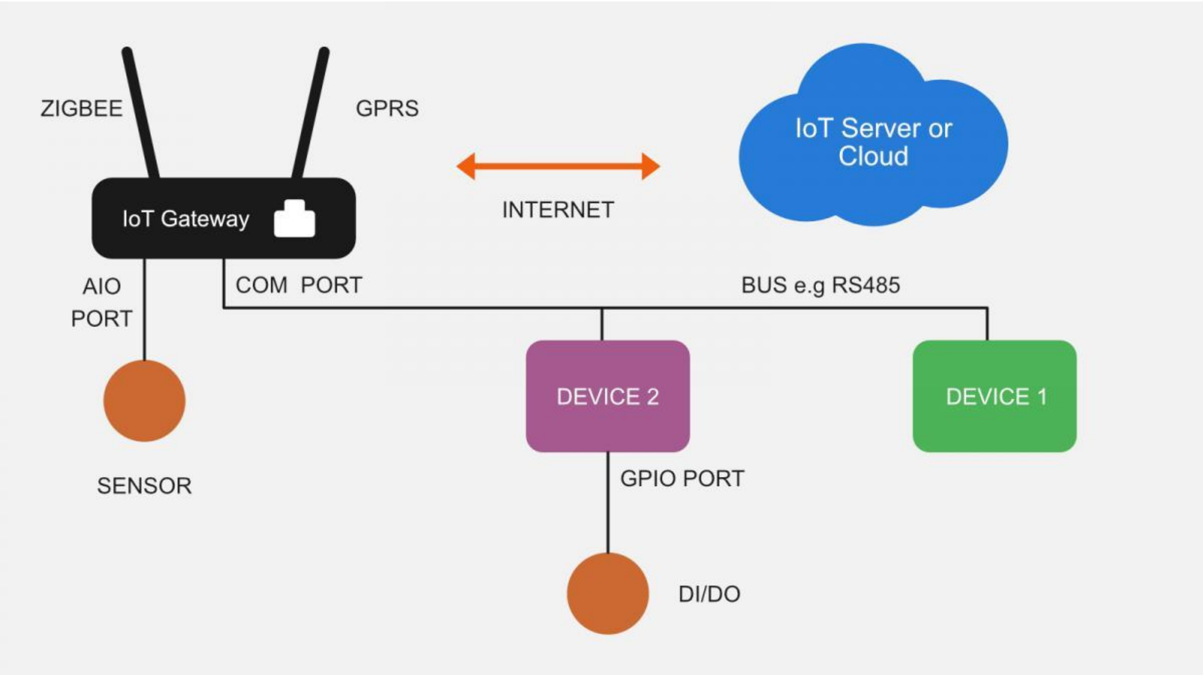
10. Does the factory owner or manufacturer require any additional customization options?

The manufacturer may need additional customization options such as energy-saving options and LTE support. Consequently, it is important to note any additional customizations and configurations and search for a model that can accommodate these customizations.

Conclusion

An IoT gateway has a major impact on the successful deployment of an IoT solution. A significant percentage of IoT projects face implementation and scalability issues due to the incorrect choice of gateway.

Therefore, it is advisable for manufacturers and factory owners to carefully evaluate the selection criteria that will help them choose the right gateway, capable of processing, handling and streaming their industrial data in real-time in order to assist with making critical decisions.



IoT Gateway is the most important part of your IoT infrastructure choosing one wisely is most important for the success of your project.

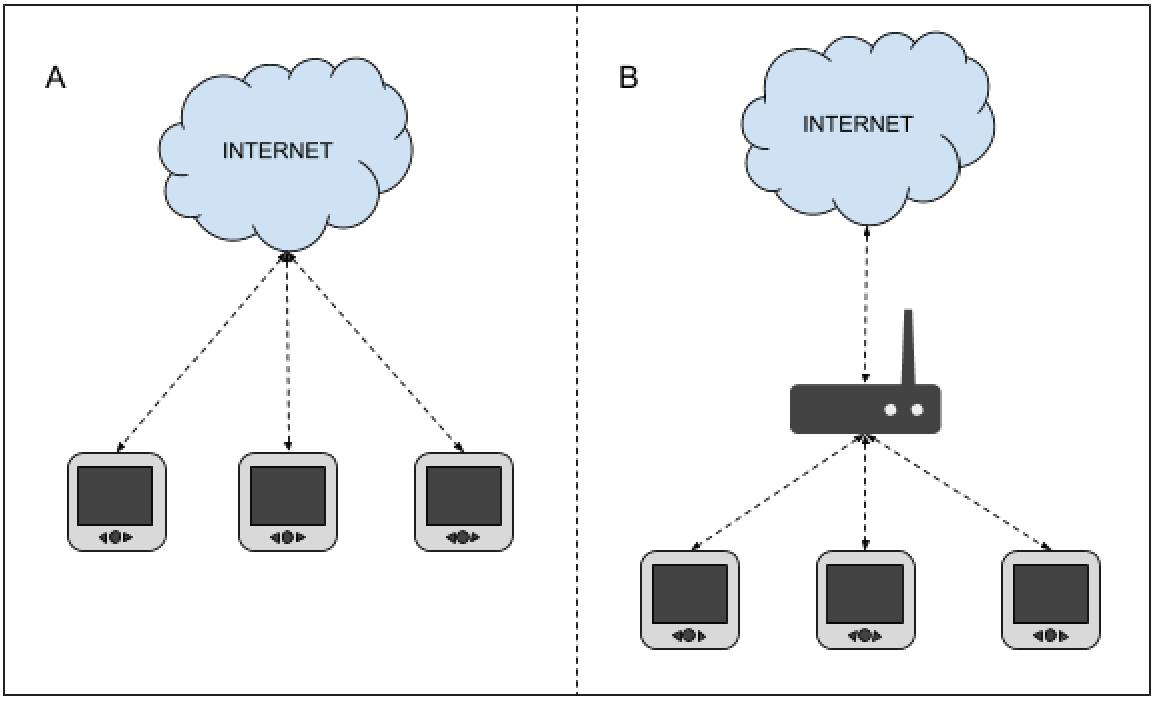
You can choose from the following two IoT architecture:

A. Each end device has inbuilt IoT Gateway functionality - for example, an AMR energy meter.

This approach is useful when the device is self-contained and does not require any external sensors or devices to be connected to it. It requires a custom device to be developed and only makes sense when volumes are high.

B. Each end device connected to a central IoT Gateway - for example, multiple energy meters connecting via an RS485 bus to a central IoT Gateway.

This approach is useful when you need to integrate external sensors and devices. You can leverage off the shelf components, reducing both the time and cost of the project.



The IoT Gateway serves two important functions in an IoT application:

1. Provides secure upstream WAN and downstream LAN connectivity
2. Host and run the edge embedded application

1. Provides secure upstream Internet and downstream LAN connectivity

This function of an IoT Gateway is similar to a router:

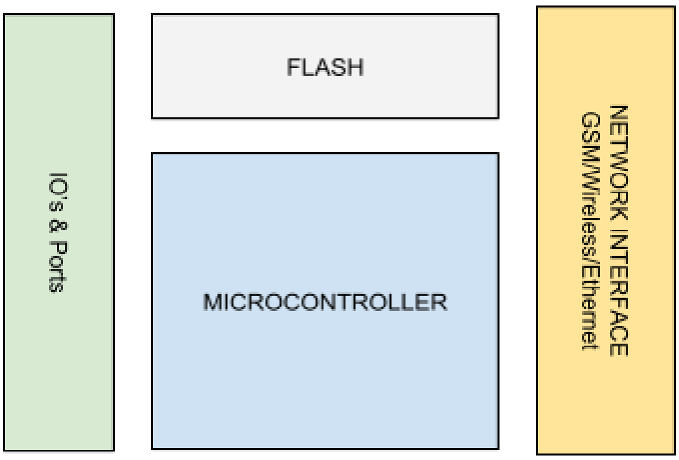
- The IoT Gateway provides single point Internet connectivity and packet routing between the downstream devices and IoT application server by using WiFi, GSM, or some other type of internet connectivity. This layer uses TCP/IP for communication.
- The IoT Gateway creates a LAN (Local Area Network) using that the downstream devices like sensors, actuators, etc. can connect to the IoT Gateway. The LAN could be wired, wireless, mesh, or P2P. The local area network created may or may not be TCP/IP driven.
- Acts as a firewall and provides secure data connectivity between the following two legs of data communication:
  - End devise to IoT Gateway
  - IoT Gateway to IoT application server

2. Host and run the edge embedded application

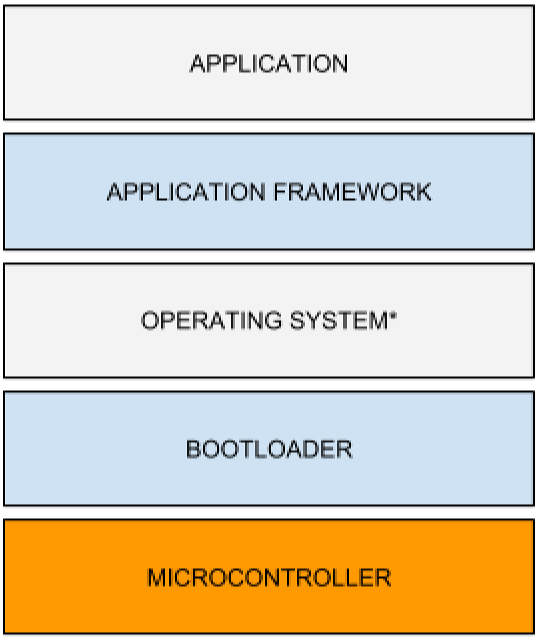
- The IoT Gateway has an inbuilt microcontroller or microprocessor that provides an application environment. The edge application runs within this application environment. Few of the functions the edge application is responsible for are as follows:
- Authentication & Authorization -Provide secure connectivity
- Messaging and communication protocol implementation
- Provisioning of IoT Gateway or end devices on the central IoT application
- Device Management - OTA, Config, Diagnostics, etc.
- Data acquisition and local storage
- Local discrete or scheduled logic control

The architecture of an IoT Gateway Device

Hardware Architecture



Embedded Software Architecture



IoT Gateway Selection

1. The right procedure to select the IoT Gateway is to first list your requirements as follows:
    1. IO & Interface requirements e.g.
        1. 1 x RS232
        2. 1 x RS485
    2. Network requirement e.g.
        1. 1 x GPRS
        2. 1 x Ethernet
        3. 1 x Zigbee
    3. Development environment e.g. C or Python
    4. Memory requirements to run your edge IoT application
    5. Flash required
    6. Power rating
    7. Certifications- CE, RoHS etc
2. Once you have listed the above you can look for IoT Gateways available in the market that meets your requirements.

IoT Gateway Mandatory Features

With our experience for running thousands of IoT Gateways across multiple applications, we have created a mandatory feature list that would help you select an IoT Gateway that would make your solutions robust, secure, and reduce total ownership cost:

1. Memory for Data Logging

IoT relies on the internet as the main communication channel between the IoT devices and the IoT application server. The IoT edge application running on the IoT Gateway would usually be acquiring data from end devices and pushing it to the IoT application server. In the case when the internet on the IoT Gateway is down it should have enough memory to store at least a few days of data and even more in case of difficult to reach sites or sites with poor network connectivity. This will prevent any data loss in absence of the internet to upload it to the server.

2. HW watchdog external to the Microcontroller

This feature will save you many site visits when you’re IoT Gateway, hangs or becomes unresponsive. Most microcontrollers have an internal watchdog but this would only restart the microcontroller in case of edge application hanging. In case the microcontroller itself hangs, e.g. microcontroller becoming unresponsive in cases of external noise on one of the interfaces, the external watchdog will still do the job of restarting the microcontroller.

3. Isolation on all external interfaces i.e. Digital, Power, or Analog

This would prevent external electrical noise from reaching the microcontroller and leading to it becoming unresponsive. It also offers the additional advantage of providing electrical isolation of digital signals, allowing for higher signal levels, reducing component damage, avoiding ground loops, and allowing for safer interfacing to external devices. You can read more about it here

http://www.ti.com/lit/wp/slyy112/slyy112.pdf.

4. LED Indications

LED indications are good for fast troubleshooting on site. E.g. a GSM network LED can help diagnose connectivity issues without the device being connected to a computer for further troubleshooting. A Rx/Tx LED on the RS232 or RS 485 port can help diagnose communication issues. This is usually a very useful feature for your field team for troubleshooting issues in the field.

5. RTC (Real Time Clock)

Most IoT applications rely on data being accurately stamped. Most IoT Gateways that do not have an RTC clock rely on the network time to timestamp the data. This approach has a serious problem in case the device reboots and there is no network to update the current time. In this case, the data would be time-stamped wrongly. An RTC allows accurate time stamping of data even if a reboot occurs in absence of a network time source.

6. Time synchronization via NTP, GSM, or GPS

The RTC clock would slowly drift and would slowly develop a clock error. One needs to synchronize the RTC with an accurate time source via NTP or GPS or GSM network. The IoT Gateway should support RTC synchronization from one of these sources. If you require very accurate timestamps, choose IoT Gateway that has a GPS inbuilt into it.

7. OTA (Over The Air) programming and firmware upgrade

Imagine you had to go to the Microsoft store for every update to your windows software, what a waste of time and money. Similarly, without the OTA feature on your IoT Gateway, you will have to go out to the device site, connect it to your computer, and reprogram it. This would cost you a lot of money and make any IoT project unviable.

8. Remote Reboot

We all would have experienced that at times the only option to resolve an issue with an electronic system is to reboot the system. This feature can help you recover from faults, which have no other solution.

9. Remote Diagnostics

An IoT Gateway that sends diagnostics data to the application server helps you identify issues more effectively. This can reduce a lot of time and money spent on troubleshooting issues. E.g. GSM network strength diagnostic information can help troubleshoot sites with GSM network issues.

10. TLS, SSL, and Client-side X509 Certificate Support

The TCP stack used in the IoT Gateway should support TLS and client-side certificate to secure connection between the IoT Gateway and the IoT application server.

11. **TPM** for certificate storage and identity management

If you have devices that are installed in a location where anyone can physically access them you run a chance of device credentials stored directly on the device (in the application code or a configuration file) being stolen. Devices equipped with TPM store device credentials in a dedicated TPM device. Credentials stored in TPM cannot be read or duplicated even if someone has physical access to the device. However, this is not a mandatory feature on our list but can add an added layer of protection for IoT applications requiring a high-security level.

12. Open Application Environment

The IoT Gateway application framework should be open to developers to develop an application on top of it so that the IoT Gateway does not lock you to a cloud or IoT application vendor. You can anytime replace the application with any other edge application to support the new IoT application service provider.

The global IoT gateway market is set to grow at a rate of 30.9% between 2017 and 2023 (according to a research report 'IoT Node and Gateway Market by Hardware, by End-Use, and Geography-Global Forecast to 2023' by Markets and Markets).

The need for IoT gateways is realised because isolated systems are rapidly transforming to the ubiquitous Internet-enabled system (also known as 'connected devices') that can be used to capture and communicate information by leveraging diverse wireless connectivity technologies to IoT gateways for unified edge-analytics.

In other words, IoT gateways play a vital role by providing the fundamental building blocks to develop secure and powerful wireless connectivity between IoT devices and IoT Cloud based applications.

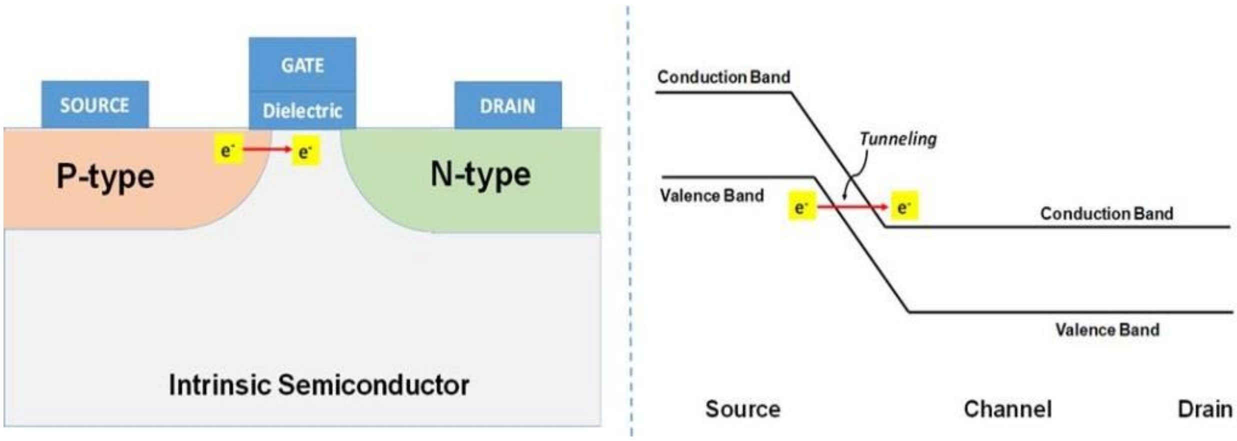
The Internet of Things (IoT) is starting to appear everywhere in many shapes and forms. But security is one of the hurdles that could trip up the growth of the IoT. Following security principles used in enterprise computing can help clear that hurdle.

Tunnel Field Effect Transistors (TFETs)

V Sai Bhargv, II- EIE

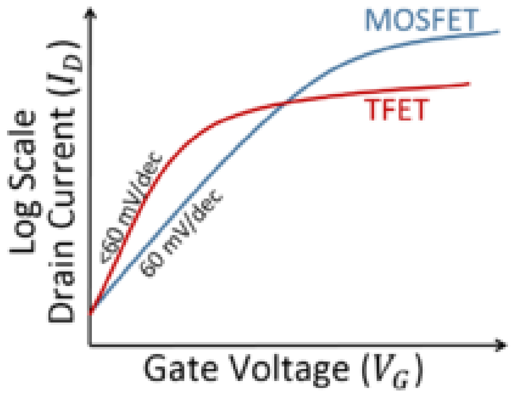
The semiconductor electronics industry owes its tremendous success to the physical down-scaling of its building block - the transistor. An incredibly long journey has been completed from large vacuum tubes to transistors with gate lengths lower than 14 nm. Since 1965, the number of transistors per integrated circuit has doubled every two years in accordance with Moore's law. However, the debate on the future of scaling has gained momentum over the past few years.

Consequently, the search for alternate materials and device systems which can avoid scaling or at least reduce the pace of scaling has attracted significant interest. Major alternatives include: extension of current CMOS technologies (Extended CMOS) and device architectures which are entirely different from existing CMOS technologies (Beyond CMOS). Extended CMOS includes nano-wires, III-V compound semiconductors, carbon nano-materials, etc. Beyond CMOS includes those devices, where conduction mechanism is different from typical CMOS devices, such as tunnel field effect transistors (TFET) and impact ionization (IO) transistors. Amongst Beyond CMOS alternatives, TFETs have attracted significant interest. TFETs have shown that the fundamental limitations of large off-state leakages and poor sub-threshold slope of conventional MOSFETs are largely overcome. This is because the conduction between the source and the drain is not governed by classical thermionic emissions but the quantum phenomenon of tunneling. This tunneling occurs between the valence band of the source and the conduction band of the channel. Another major difference between a TFET and a conventional MOSFET is that the source doping in a TFET is opposite to that of the drain and the channel is generally intrinsic or very lightly doped.



The tunnel field-effect transistor (TFET) is an experimental type of transistor. Even though its structure is very similar to a metal-oxide-semiconductor field-effect transistor (MOSFET), the fundamental switching mechanism differs, making this device a promising candidate for low power electronics. TFETs switch by modulating quantum tunneling through a barrier instead of modulating thermionic emission over a barrier as in traditional MOSFETs. Because of this, TFETs are not limited by the thermal Maxwell–Boltzmann tail of carriers, which limits MOSFET drain current subthreshold swing to about 60 mV/decade of current at room temperature.

TFET studies can be traced back to Stuetzer who in 1952 published first investigations of a transistor containing the basic elements of the TFET, a gated p-n junction. The reported surface conductivity control was, however, not related to tunneling. The first TFET was reported in 1965. Joerg Appenzeller and his colleagues at IBM were the first to demonstrate that current swings below the MOSFET's 60-mV-per-decade limit were possible. In 2004, they reported they had created a tunnel transistor with a carbon nanotube channel and a subthreshold swing of just 40 mV per decade.Theoretical work has indicated that significant power savings can be obtained by using low-voltage TFETs in place of MOSFETs in logic circuits.



Drain current vs. gate voltage for hypothetical TFET and MOSFET devices. The TFET may be able to achieve higher drain current for small voltages.

The device is operated by applying gate bias so that electron accumulation occurs in the intrinsic region for an n-type TFET. At sufficient gate bias, band-to-band tunneling (BTBT) occurs when the conduction band of the intrinsic region aligns with the valence band of the P region. Electrons from the valence band of the p-type region tunnel into the conduction band of the intrinsic region and current can flow across the device. As the gate bias is reduced, the bands becomes misaligned and current can no longer flow.

The basic TFET structure is similar to a MOSFET except that the source and drain terminals of a TFET are doped of opposite types (see figure). A common TFET device structure consists of a P-I-N (p-type, intrinsic, n-type) junction, in which the electrostatic potential of the intrinsic region is controlled by a gate terminal.

TFETs can be realized in many 2-D as well as 3-D architectures such as planar, double gate, dual material gate, heterojunction, gate-all-around etc. The major benefits of TFETs include steeper sub-threshold behavior, lower off-state current, higher on- state current for same gate voltage and better immunity to short channel effects. Going forward some of the reliability issues need to be resolved before devices which use TFETs as the active component can become a major commercial success.

ISSUE - 2

2021-22