

Resource Material (E- Content)
for
Diploma in Electronics & Telecommunication
Semester- Sixth
As per syllabus of
Chhattisgarh Swami Vivekanand University,
Bilal (C.G.)

Prepared By Abhiranyu Kumar Singh
Lecturer,ET&T
Government Polytechnic Jashpur(C.G.)

Unit -1 Introduction to mobile communication

History of wireless technology

Marconi, an Italian inventor, transmitted Morse code signals using radio waves wirelessly to a distance of 3.2 KMs in 1895. It was the first wireless transmission in the history of science. Since then, engineers and scientists were working on an efficient way to communicate using RF waves.

Telephone became popular during the mid of 19th century. Due to wired connection and restricted mobility, engineers started developing a device which doesn't requires wired connection and transmit voice using radio waves.

Martin Cooper, an engineer at Motorola during 1970s working on a handheld device capable of two way communication wirelessly, invented the first generation mobile phone. It was initially developed to use in a car, the first prototype was tested in 1974.

This invention is considered as a turning point in wireless communication which led to an evolution of many technologies and standards in future.

another popular technology CDMA2000 was also introduced to support higher data rate for CDMA networks. This technology has the ability to provide up to 384 kbps data rate (maximum).

Evolution of wireless technologies 1G to 5G in mobile communication

Mobile wireless communication system has gone through several evolution stages in the past few decades after the introduction of the first generation mobile network in early 1980s. Due to huge demand for more connections worldwide, mobile communication standards advanced rapidly to support more users. Let's take a look on the evolution stages of wireless technologies for mobile communication.



(I) 1G – First generation mobile communication system

The first generation of mobile network was deployed in Japan by Nippon Telephone and Telegraph Company (NTT) in Tokyo during 1979. In the beginning of 1980s, it gained popularity in the US, Finland, UK and Europe. This system used analogue signals and it had many disadvantages due to technology limitations.

Most popular 1G system during 1980s

- Advanced Mobile Phone System (AMPS)
- Nordic Mobile Phone System (NMTS)
- Total Access Communication System (TACS)
- European Total Access Communication System (ETACS)

Key features of 1G system

- Frequency 800 MHz and 900 MHz
- Bandwidth: 10 MHz (666 duplex channels with bandwidth of 30 KHz)
- Technology: Analogue switching
- Modulation: Frequency Modulation (FM)
- Mode of service: voice only
- Access technique: Frequency Division Multiple Access (FDMA)

Disadvantages of 1G system

- Poor voice quality due to interference
- Poor battery life
- Large sized mobile phones (not convenient to carry)
- Less security (calls could be decoded using an FM demodulator)
- Limited number of users and cell coverage
- Roaming was not possible between similar systems

(II) 2G – Second generation communication system GSM

Second generation of mobile communication system introduced a new digital technology for wireless transmission also known as Global System for Mobile communication (GSM). GSM technology became the base standard for further development in wireless standards later. This standard was capable of supporting up to 14.4 to 64kbps (maximum) data rate which is sufficient for SMS and email services. Code Division Multiple Access (CDMA) system developed by Qualcomm also introduced and implemented in the mid 1990s. CDMA has more features than GSM in terms of spectral efficiency, number of users and data rate.

Key features of 2G system

- Digital system (switching)
- SMS services is possible
- Roaming is possible
- Enhanced security
- Encrypted voice transmission
- First internet at lower data rate
- Disadvantages of 2G system
- Low data rate
- Limited mobility
- Less features on mobile devices

- Limited number of users and hardware capability

2.5G and 2.75G system

In order to support higher data rate, General Packet Radio Service (GPRS) was introduced and successfully deployed. GPRS was capable of data rate up to 171kbps (maximum).

EDGE – Enhanced Data GSM Evolution also developed to improve data rate for GSM networks. EDGE was capable to support up to 473.6kbps (maximum).

another popular technology CDMA2000 was also introduced to support higher data rate for CDMA networks. This technology has the ability to provide up to 384 kbps data rate (maximum).

(III) 3G – Third generation communication system

Third generation mobile communication started with the introduction of UMTS – Universal Mobile Terrestrial / Telecommunication Systems. UMTS has the data rate of 384kbps and it support video calling for the first time on mobile devices.

After the introduction of 3G mobile communication system, smart phones became popular across the globe. Specific applications were developed for smart phones which handle multimedia chat, email, video calling, games, social media and healthcare.

Key features of 3G system

- Higher data rate
- Video calling
- Enhanced security, more number of users and coverage
- Mobile app support
- Multimedia message support
- Location tracking and maps
- Better web browsing
- TV streaming
- High quality 3D games

3.5G to 3.75 Systems

In order to enhance data rate in existing 3G networks, another two technology improvements are introduced to network. HSDPA – High Speed Downlink Packet access and HSUPA – High Speed Uplink Packet Access, developed and deployed to the 3G networks. 3.5G network can support up to 2mbps data rate.

3.75 system is an improved version of 3G network with HSPA+ High Speed Packet Access plus. Later this system will evolve into more powerful 3.9G system known as LTE (Long Term Evolution).

Disadvantages of 3G systems

- Expensive spectrum licenses
- Costly infrastructure, equipment and implementation
- Higher bandwidth requirements to support higher data rate
- Costly mobile devices
- Compatibility with older generation 2G system and frequency bands

(IV) 4G – Fourth generation communication system

4G systems are enhanced version of 3G networks developed by IEEE, offers higher data rate and capable to handle more advanced multimedia services. LTE and LTE advanced wireless technology used in 4th generation systems. Furthermore, it has compatibility with previous version thus easier deployment and upgrade of LTE and LTE advanced networks are possible.

Simultaneous transmission of voice and data is possible with LTE system which significantly improve data rate. All services including voice services can be transmitted over IP packets. Complex modulation schemes and carrier aggregation is used to multiply uplink / downlink capacity.

Wireless transmission technologies like WiMax are introduced in 4G system to enhance data rate and network performance.

Key features of 4G system

- Much higher data rate up to 1Gbps
- Enhanced security and mobility
- Reduced latency for mission critical applications
- High definition video streaming and gaming
- Voice over LTE network VoLTE (use IP packets for voice)

Disadvantages of 4G system

- Expensive hardware and infrastructure
- Costly spectrum (most countries, frequency bands are too expensive)
- High end mobile devices compatible with 4G technology required, which is costly
- Wide deployment and upgrade is time consuming

(V) 5G – Fifth generation communication system

5G network is using advanced technologies to deliver ultra fast internet and multimedia experience for customers. Existing LTE advanced networks will transform into supercharged 5G networks in future.

In earlier deployments, 5G network will function in non standalone mode and standalone mode. In non standalone mode both LTE spectrum and 5G-NR spectrums will be used together. Control signaling will be connected to LTE core network in non standalone mode.

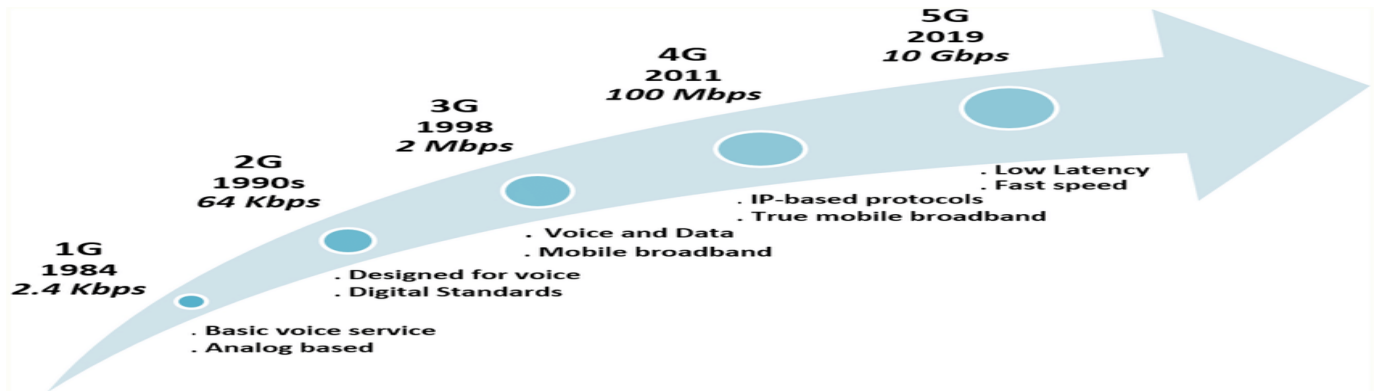
There will be a dedicated 5G core network higher bandwidth 5G – NR spectrum for standalone mode. Sub 6-GHz spectrum of FR1 ranges are used in the initial deployments of 5G networks.

In order to achieve higher data rate, 5G technology will use millimeter waves and unlicensed spectrum for data transmission. Complex modulation technique has been developed to support massive data rate for Internet of Things (IoT).

Key features of 5G technology

- Ultra fast mobile internet up to 10Gbps
- Low latency in milliseconds (significant for mission critical applications)
- Total cost deduction for data
- Higher security and reliable network
- Uses technologies like small cells, beam forming to improve efficiency
- Forward compatibility network offers further enhancements in future

- Cloud based infrastructure offers power efficiency, easy maintenance and upgrade of hardware



Comparison of 1 G to 5G technology

Generation	Speed	Technology	Key Features
1G (1970–1980s)	14.4 Kbps	AMPS, NMT, TACS	Voice only services
2G (1990 to 2000)	9.6/ 14.4 Kbps	TDMA, CDMA	Voice and Data services
2.5G to 2.75G (2001-2004)	171.2 Kbps 20-40 Kbps	GPRS	Voice, Data and web mobile internet, low speed streaming services and email services.
3G (2004-2005)	3.1 Mbps 500- 700 Kbps	CDMA2000 (1xRTT, EVDO) UMTS and EDGE	Voice, Data, Multimedia, support for smart phone applications, faster web browsing, video calling and TV streaming.
3.5G (2006-2010)	14.4 Mbps 1-3 Mbps	HSPA	All the services from 3G network with enhanced speed and more mobility.
4G (2010 onwards)	100-300 Mbps 3-5 Mbps 100 Mbps (Wi-Fi)	WiMax, LTE and Wi-Fi	High speed, high quality voice over IP, HD multimedia streaming, 3D gaming, HD video conferencing and worldwide roaming.
5G (Expecting at the end of 2019)	1 to 10 Gbps	LTE advanced schemes, OMA and NOMA	Super fast mobile internet, low latency network for mission critical applications, Internet of Things, security and surveillance, HD multimedia streaming, autonomous driving, smart healthcare applications.

Definition of Basic term used in mobile communication

Mobile Station (MS) – The Mobile Station (MS) communicates the information with the user and modifies it to the transmission protocols of the air interface to communicate with the BSS. The user information communicates with the MS through a microphone and speaker for the speech, keyboard and display for short messaging and the cable connection for other data terminals. The mobile station has two elements Mobile Equipment (ME) and Subscriber Identity Module (SIM).

Mobile Equipment (ME) – ME is a piece of hardware that the customer purchases from the equipment manufacturer. The hardware piece contains all the components needed for the implementation of the protocols to interface with the user and the air-interface to the base stations.



Subscriber Identity Module (SIM) – SIM is a smart card issued at the subscription to identify the specifications of a user such as address and type of service. The calls in the GSM are directed to the SIM rather than the terminal.

SMS are also stored in the SIM card. It carries every user's personal information which enables a number of useful applications.

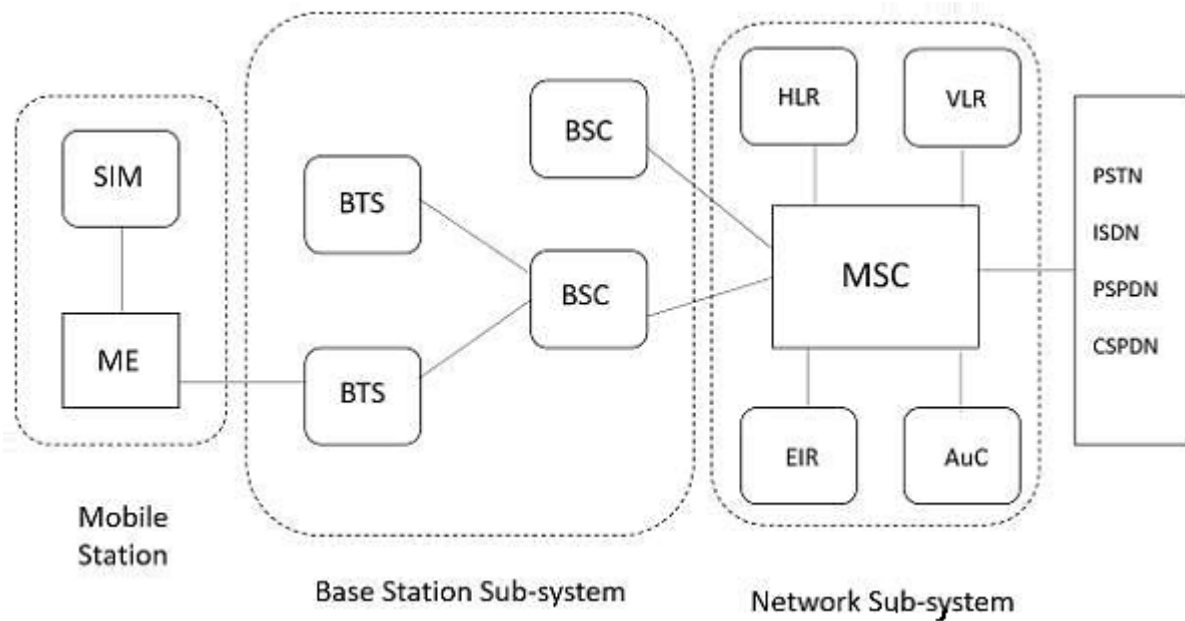


Base Station (BS) – A base station transmits and receives user data. When a mobile is only responsible for its user's data transmission and reception, a base station is capable to handle the calls of several subscribers simultaneously.

Base Transceiver Station (BTS) – The user data transmission takes place between the mobile phone and the base station (BS) through the base transceiver station. A transceiver is a circuit which transmits and receives.

Mobile Switching Center (MSC) – MSC is the hardware part of the wireless switch that can communicate with PSTN switches using the Signaling System 7 (SS7) protocol as well as other MSCs in the coverage area of a service provider. The MSC also provides for communication with other wired and wireless networks as well as support for registration and maintenance of the connection with the mobile stations.

The following image illustrates the parts of different sub-systems. HLR, VLR, EIR and AuC are the sub-systems of Network sub-system.



Channels – It is a range of frequency allotted to particular service or systems.

Control Channel – Radio channel used for transmission of call setup, call request, call initiation and other beacon or control purposes.

Forward Control Channel (FCC) – Radio channel used for transmission of information from the base station to the mobile.

Reverse Channel (RC) – Radio channel used for transmission of information from the mobile to base station.

Voice Channel (VC) – Radio channel used for voice or data transmission.

Handoff – It is defined as the transferring a call from the channel or base station to another base station.

Roamer – A mobile station which operates in a service area other than that from which service has been subscribed.

Frequency bands used in India:

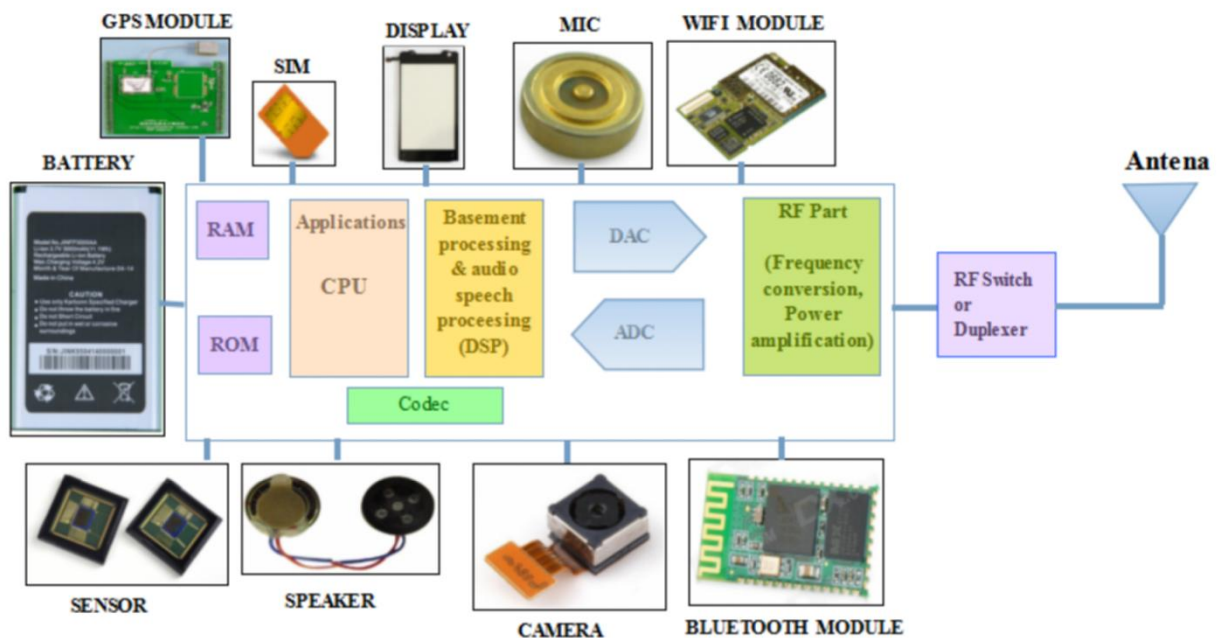
Here is a table for the different frequency bands in India for mobile technology 2G, 3G, and 4G.

Sr. No.	Mobile Technology in India	Frequency used
1	GSM (2G)	900 MHz , 1800 MHz
2	CDMA	850 MHz
3	WCDMA (3G)	900 MHz, 2100 MHz
4	Wi-MAX	2300 MHz

5	4G (LTE)	850 MHz (Jio), 1800 MHz & 2300 MHz (AirTel, Idea, Vodafone, Jio) 2500 MHz (BSNL, Idea & Vodafone)
---	----------	--

Block Diagram of Mobile phone Handset:-

Typically Mobile phone will have display (LCD, touch screen), keypad, microphone, speaker, SIM card, battery, USB port, antenna, memory unit(RAM,ROM), camera, CODEC, RF part, DAC/ADC, baseband part (L1/Layer1/physical layer) running on DSP, Application/protocol layers running on CPU, ON/OFF switch and Bluetooth/GPS features. All these features are based on specific standard specifications designed, like it may be based on GSM, WCDMA or LTE etc.



RF Part:

As shown in figure above, every phone will have RF part which consists of RF frequency up converter and RF frequency down converter, analog filters, digital attenuator (whose attenuation is controlled digitally), driver amplifiers etc. For system, up converter converts modulated baseband signal (I and Q) either at zero IF (Intermediate frequency) or some IF to RF frequency. RF down converter converts RF signal to baseband signal (I and Q). The basic component used for frequency conversion is RF mixer. Analog filters pass only desired band of signals. Amplifiers boost the signal to the required transmit power level.

Baseband Part:

Baseband part in a mobile is comprised of a digital signal processor (DSP) to process forward voice/data signals for transmission and to process reverse voice/data signals received. This is the core processing part which changes for various air interface standards like GSM, HSPA, LTE and more. It is often named as physical layer or Layer 1 or L1. For Speech/audio, **codec** is used to compress and decompress the signal to

match the data rate to the frame it has to fit in. The baseband or physical layer will add redundant bits to enable error detection as well as error correction. Error detection is obtained with CRC and error correction with forward error correction techniques. Other than this interleaving is done for the data of one burst which helps in spreading the error over the time hence helps receiver de-interleave and decode the frame correctly.

ADC and DAC:

ADC (Analog to Digital Converter) and DAC (Digital to Analog Converter) is used to convert analog speech signal to digital signal and vice versa in the mobile handset.

RF Switch / Duplexer:

RF switch is used for TDD configuration, which switches the RF path between transmit chain and receive chain and on the other side, Duplexer is used for FDD configuration which passes the transmitted signal and received signal at the same time through it. Like GSM 900MHz in India is FDD, so Duplexer is used there and LTE Band 40 is TDD in India, RF switch is used there.

Application layer

It consists of protocols that focus on process-to-process communication across an IP network and provides a firm communication interface and end-user services. It also runs on CPU. It includes audio, video and image/graphics applications. The application layer provides many services, including: Simple Mail Transfer, Protocol File transfer, graphics etc.

Camera

Now-a-days with almost all the mobile phone camera feature is available for clicking pictures at various occasions. It is the major specifications which increases cost of mobile phone. There are various mega pixel cameras for mobile phones are available such as 5 mega pixel, 13 mega pixel and even 41 mega pixel available in smart phones. This has become evident because of advancement in sensor technology.

Display

There are lot of display types used in mobile phones. They can be either color or monochrome. The color displays usually are CSTN (Super twisted nematic display), TFT (Thin film transistor), TFD (Thin film Diode) or OLED (organic light emitting Diode) with a predominant use of TFT displays in current mobile lineups. There are also two types of touch screen displays – capacitive and resistive, which are both based on TFT technology.

CAPACITIVE touch screens work by sensing the electrical properties of the human body, while RESISTIVE touch screens operate by sensing direct pressure applied by the user.

Microphone

Microphone or mic converts air pressure variations (result of our speech) to electrical signal to couple on the PCB for further processing. Usually in mobile phone condenser, dynamic, carbon or ribbon types of microphones are used.

Speaker

It converts electrical signal to audible signal (pressure vibrations) for human being to hear. This is often coupled with audio amplifier to get required amplification of audio signal. It also tied with volume control circuit to change (increase or decrease) the amplitude of the audio signal.

Antenna

An antenna converts electromagnetic radiation into electric signal and vice versa. In mobile phone, antenna is embedded inside, which is not visible to us. A metal strip pattern is served as an antenna.

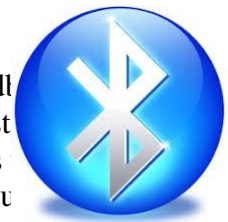


Connectivity (Wi-Fi, Bluetooth, GPS, Sensors)

To make data transfer fast enough between mobile phone and other computing devices or between mobile there are various technologies are evolved which include Wi-Fi, Bluetooth, and Sensors. GPS (global positioning system) is used for location assistance and will enable Google map to work efficiently.

Bluetooth

The development of the Bluetooth technology was initiated in 1989 by Nils Rydell, CTO at Ericsson Mobile in Lund, Sweden. Bluetooth is a wireless technology standard used for exchanging data between fixed and mobile devices over short distances using short-wavelength UHF radio waves of 2.400 to 2.485 GHz which is used in industrial, scientific and medical applications.



Wi-Fi

Wi-Fi (Wireless Fidelity) is a popular wireless networking technology. It is commonly called as "Wireless LAN" (local area network). Wi-Fi allows local area networks to operate without cable and wiring. It is making popular choice for home and business networks.



RFID

RFID means Radio Frequency Identification. RFID is a technology which works on radio frequency or radio waves. This technology is used for tracking objects automatically. The objects could be anything. It could be books in the library, or it could be any item purchasing from shopping mall or inventory in the warehouse or it could be a car. Not only the objects but it can be also used for tracking animals or birds.



GPS

The Global Positioning System (GPS) was developed by the U.S. Department of Defence. The only system of its kind in the world, GPS uses the transmission of microwave signals from a network of 30 satellites orbiting 12,000 miles above Earth to pinpoint a receiver's location, as well as its speed and direction of travel.

A **GPS** is a device that is capable of receiving information from GNSS satellites and then to calculate the device's

geographical position. Using suitable software, the device may display the position on a map, and it may offer routing directions. The Global Positioning System (GPS) is one of a handful of global navigation



satellite systems (GNSS) made up of a network of a minimum of 24, but currently 30, satellites placed into orbit by the U.S. Department of Defence.

Sensors

A sensor is a transducer whose purpose is to sense some characteristic of its environs. It detects events or changes in quantities and provides a corresponding output, generally as an electrical or optical signal. In mobile phone, there are various kind of sensors are used like accelerometer, magnetometer, proximity sensor, light sensor, barometer, pedometer, thermometer etc.

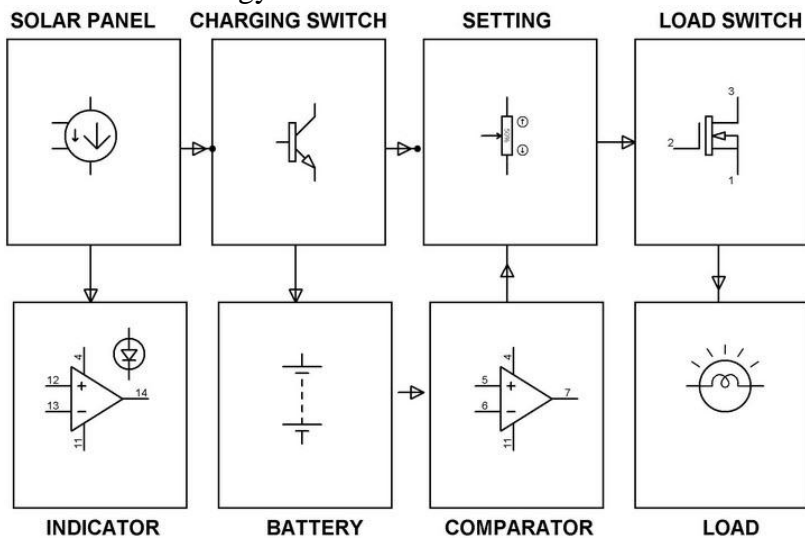
The charging voltage, depending on the NiCd cell, can be determined with the specifications provided by the manufacturer. The charging voltage is set at 7.35V for four 1.5V cells. Currently, 700 mA cells, which can be charged at 70 mA for ten hours, are available in the market. The voltage of the open circuit is about 1.3V.

The shut-off voltage point is determined by charging the four cells fully (at 70 mA for fourteen hours) and adding the diode drop (up to 0.65V) after measuring the voltage and bias LM317 accordingly.

In addition to the above simple circuit, the real-time implementation of this circuit based on the solar power projects are discussed below.

Solar Power Charge Controller

The main objective of this solar power charge controller project is to charge a battery by using solar panels. This project deals with a mechanism of the charge controlling that will also do overcharge, deep discharge, and under-voltage protection of the battery. In this system, by using photovoltaic cells, solar energy is converted into electrical energy.



Solar Power Charge Controller

This project comprises hardware components like a solar panel, Op-amps, MOSFET, diodes, LEDs, potentiometer, and battery. Solar panels are used to convert sunlight energy into electrical energy. This energy is stored in a battery during day time and makes use of it during night time. A set of OP-AMPS are used as comparators for monitoring of panel voltage and lead current continuously.

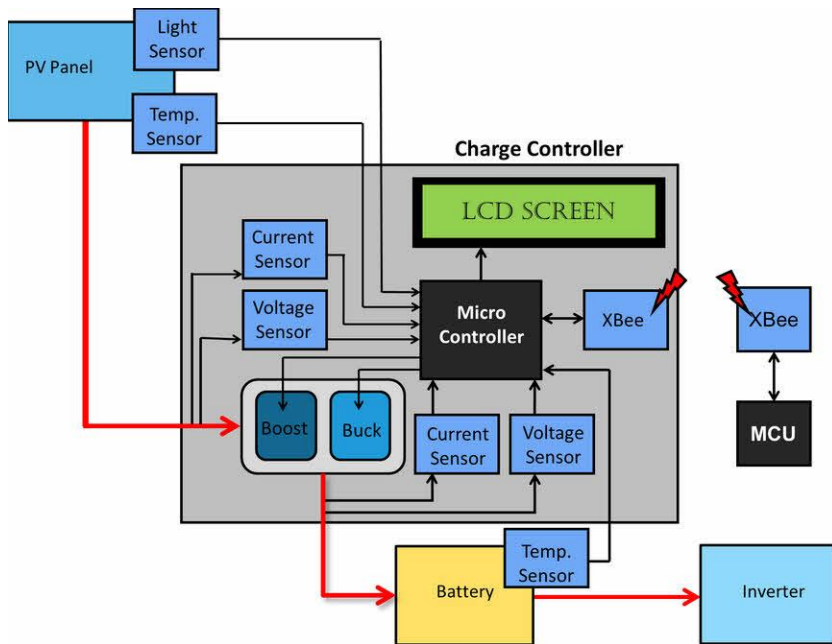
LEDs are used as indicators and by glowing green, indicates the battery as fully charged. Similarly, if the battery is undercharged or overloaded, they glow red LED. The Charge controller makes use of MOSFET – a power semiconductor switch to cut off the load when the battery is low or in an overload condition. A transistor is used to bypass the solar energy into a dummy load when the battery is fully charged and it protects the battery from getting overcharged.

Auto-Turn off Battery Charger

This project aims to automatically disconnect a battery from the mains when the battery gets fully charged. This system can be used to charge partially discharged cells as well. The circuit is simple and consists of AC-DC converter, relay drivers, and charge stations.

Microcontroller Based Photovoltaic MPPT Charge Controller

This project aims to design a charge controller with a maximum power point tracking based on a microcontroller.



Photovoltaic MPPT Charge Controller

The major components used in this project are solar panel, battery, inverter, wireless transceiver, LCD, current sensor, and temperature sensor. The power from the solar panels is fed to the charge controller which is then given as output into the battery and is allowed for energy storage. The output of the battery is connected to an inverter that provides outlets for the user to access the stored energy.

The solar panel, battery, and inverter are bought as the off-shell parts while the MPPT charge controller is designed and built by solar knights. An LCD screen is provided for displaying storage power and other alert messages. The output voltage is varied by pulse width modulation from the microcontroller to MOSFET drivers. The way to track a maximum power point by using MPPT algorithm implementation in the controller ensures that the battery is charged at maximum power from the solar panel.

SIM Card:



The data stored in the SIM card includes a unique serial number called ICCID, International Mobile Subscriber Identity or IMSI, Security Authentication information, temporary information about the network, a Personal Identification Number or PIN and a Personal Unblocking code or PUK for unlocking. SIM card contains its internal memory in which stores the data, personal and financial information, identity for GSM/CDMA. Modern SIM cards allow the storage of application data that communicate with the handset or server using the SIM application tool kit. The SIM card stores network-specific information to authenticate the identity of the subscriber in the network. Out of the many keys, the most important keys are ICCID, IMSI, Authentication key or Ki, Local Area Identification or LAI, and an operator-specific emergency

number. Micro sim has been invented for the latest mobile phones. The SIM also contains other data like Short Message Service Centre number or SMSC, Service Provider Name or SPN, Service Dialing Number or SDN, Value Added Service or VAS, etc. The SIM comes in various data capacities ranging from 32KB to 128K and can store 250 contacts.

Keys of SIM Card:

1. Integrated Circuit Card Identifier or ICCID – It is the Primary account number that has 19 digits long. The number has sections like Issuer Identification Number or IIN, Individual Account Identification, Check digit, etc.

2. International Mobile Subscriber Identity or IMSI – It is used to identify the individual operator's network. Normally it has 109 digits. Its first 3 digits represent Mobile Country Code or MCC, the next 2 to 3 digits represent the Mobile Network Code or MNC, The next digits represent the Mobile Subscriber Identification Number or MSIN.

ogy is one of the most popular technologies which is used in Mobile phones to activate the connection and to communicate and for making links with the server system and also used in various [electrical and electronic projects](#). It is the Subscriber Identity Module that contains the integrated circuit to store the International Mobile Subscriber Identity or IMSI and the keys to identify and authenticate the subscribers on the communication system. The SIM is embedded in a [smart card](#) that can be removed and transferred to different mobile phones. SIM card provides [security system](#) to users. The first SIM card was made in 1991 by Giesecke and Deviant of Sagem communications in France.

3. Authentication Key or Ki – It is a 128 bit used to authentication of the SIM card on the Mobile Network. Each SIM has a unique Authentication key assigned by the operator during personalization. The Authentication Key is also stored in the database of the carrier's network. When the mobile phone first activates using the SIM card, it gets the International Mobile Subscriber Identity or IMSI from the SIM card and transfers it to the mobile operator for authentication. The database in the operating system then searches for incoming IMSI and the associated Authentication key. The operator database then generates a Random Number or RAND and signs it with the IMSI and gives another number called Signed Response 1(SRES_ 1). The RAND will be sent to the mobile phone and the SIM then signs it with the Authentication Key and produces the SRES_ 2 which then passes into the operator network. The operator network then compares the SRES_1 it produced and the SRES_2 from the mobile phone. If both match, the SIM is authenticated.

4. Location Area Identity or LAI– This the information stored in the SIM about the local network available. The operator network is divided into different small areas each having an LAI.

5. SMS messages – SIM card can store many SMS

6. Contacts – SIM can store around 250 contacts.

Functions of SIM card:

The SIM card performs the following functions:

1) It identifies the subscriber: The IMSI programmed on the SIM card, is the identity of a subscriber. Each IMSI is mapped to a mobile number and provisioned on the HLR to allow a subscriber to be identified.

2) Authenticate the subscriber: This is a process, where, using the authentication algorithm on the SIM card, a unique response is provided by each subscriber based on IMSI (stored on SIM) and RAND (provided by network). By matching this response with values computed on the network a legal subscriber is logged on to the network and he or she can now make use of the services of the mobile service provider. SIM card is becoming a feature of mobile work.

3) Storage: To store phone numbers and SMS.

4) Applications: The SIM Tool Kit or GSM 11.14 standard allows creating

Applications on the SIM to provide basic information on demand and other

Applications for m-commerce, chatting, cell broadcast, phonebook backup,

Location-based services etc.

Microprocessor-based SIM cards:

The most important part of the SIM card is its Microcontroller. It is a paper sized chip which is a typical ROM with a size between 64 KB to 512 KB. The RAM size ranges between 1KB to 8KB while the EEPROM size is in between 16KB to 512 KB. The ROM contains the OS or operating system for the card, while the EEPROM contains data called personalization that includes security keys, phone book, SMS settings, etc. The operating voltage of SIM maybe, 1.8V, 3V or 5V but the operating voltages of most of the modern SIM support 5V, 3V, and 1.8V.

There are two types of microprocessor cards. These cards take the form of either contact cards, which require a card reader, or contactless cards, which use radio frequency signals to operate.



Types of SIM Card:

There are two types of SIM cards that are GSM and CDMA:

GSM:

GSM technology stands for Global System for Mobiles and its foundation can be credited to Bell Laboratories in 1970. It uses a circuit-switched system and divides each 200 kHz signal into 8 25 kHz time slots and operates in 900 MHz, 800 MHz, and 1.8GHz bands. It uses a narrow band transmission technique- basically Time Division Access Multiplexing. The data transfer rates vary from 64kbps to 120kbps.

CDMA:

CDMA means code division multiple access which explains about communication channel principle that employs spread-spectrum technology and a special coding scheme which are time-division multiplexing scheme and frequency division multiplexing scheme.

SIM Number and IMEI number

A Subscriber Identity Module or Subscriber Identification Module (SIM), widely known as a 'SIM Card', is an integrated circuit identification that is intended to securely store the international mobile subscriber identity (IMSI) number and its related key, which are used to identify and authenticate subscribers on mobile telephony devices (such as mobile phones and computers).

SIM number: or Integrated Circuit Card Identifier (ICCID) is 19 or 20 digit number printed on back side of a SIM card. Let us suppose this number is: 8991000900375752261U. Each group of



number has some specific meaning.

89 91 00 090037575226 1 U

89 – First 2 digits are industry code

91 – Next 2 digits for country code

00 – Next 2 digits for issuer number

0900 37575226 – Next 12 digits for customer id

1 – Next one digit for checksum &

U – Stands for Universal

It is also possible to store contact information on many SIM cards. SIM cards are always used on GSM phones; for CDMA phones, they are only needed for newer LTE-capable handsets. SIM cards can also be used in satellite phones, smart watches, computers, or cameras.

The SIM circuit is part of the function of a universal integrated circuit card (UICC) physical smart card, which is usually made of PVC with embedded contacts and semiconductors. SIM cards are transferable between different mobile devices. The first UICC smart cards were the size of credit and bank cards; sizes were reduced several times over the years, usually keeping electrical contacts the same, so that a larger card could be cut down to a smaller size.

A SIM card contains its unique serial number (ICCID), international mobile subscriber identity (IMSI) number, security authentication and ciphering information, temporary information related to the local network, a list of the services the user has access to, and two passwords: a personal identification number (PIN) for ordinary use, and a personal unblocking code (PUC) for PIN unlocking.

IMEI number: International Mobile Equipment Identity number is cell phone's unique identity number. This is the hardware number of a device. Dual SIM cards device has two IMEIs. IMEIs tell information about the device. It is useful for software updates for device and blocking device for accessing telecom network. When a device is stolen its only IMEI which is used to detected the device by roaming network.



It is usually a 15 digit unique number found printed inside the battery compartment of the phone, but can also be displayed on-screen on most phones by entering *#06# on the dial pad, or alongside other system information in the settings menu on smart phone operating systems.

GSM networks use the IMEI number to identify valid devices, and can stop a stolen phone from accessing the network. For example, if a mobile phone is stolen, the owner can have their network provider use the IMEI number to blacklist the phone. This renders the phone useless on that network and sometimes other networks, even if the thief changes the phone's subscriber identity module (SIM).

Devices without a SIM card slot usually don't have the IMEI code. However, the IMEI only identifies the device and has no particular relationship to the subscriber. The phone identifies the subscriber by transmitting the International mobile subscriber identity (IMSI) number i.e. SIM number.

When someone has their mobile equipment stolen or lost, they can ask their service provider to block the phone from their network, and the operator does so if required by law. If the local operator maintains an Equipment Identity Register (EIR), it adds the device IMEI to it. Optionally, it also adds the IMEI to shared registries, such as the Central Equipment Identity Register (CEIR),

which blacklists the device with other operators that use the CEIR. This blacklisting makes the device unusable on any operator that uses the CEIR, which makes mobile equipment theft pointless, except for parts.

Data encryption

Data encryption translates data into another form, or code, so that only people with access to a secret key (formally called a decryption key) or password can read it. Encrypted data is commonly referred to as ciphertext, while unencrypted data is called plaintext. Currently, encryption is one of the most popular and effective data security methods used by organizations. Two main types of data encryption exist - asymmetric encryption, also known as public-key encryption, and symmetric encryption.

Science and encryption are used today to keep our most sensitive and personal data safe and secure from those who we don't wish to access it. Today we have many sophisticated and refined tools that can be put to use in protecting our data. These tools not only keep our data safe, but they also ensure that even if it does fall into the wrong hands, only the intended recipient is available to read it.

Need for data encryption

There are five reasons to encrypt the data. These are-

1. Privacy:

The privacy concern is the big one. Anyone who can lay their hands on an unencrypted file can read its contents. Even with an unknown file type, a lack of encryption would make it possible to find out what it said.

2. Protection by Default:

Having all your mobile storage encrypted is definitely helpful in preventing anyone who steals your phone from stealing your identity. But, what about the stuff you haven't encrypted? A thief can pull those files from your unencrypted phone without even having to power it on and log in.

For this reason, all modern smart phones and all Windows machines since Vista encrypt their hard drives automatically when they are powered off. Until the user turns the device on and enters their password, the files are virtually impossible to decrypt. This means that the average user benefits from strong encryption by default.

3. Virtual Private Networks:

A virtual private network (VPN) is an essential tool for anyone who wants or needs to keep their Wi-Fi communications secure. A VPN creates a secure encrypted communications channel between your device and the internet. A VPN can be used by businesses to keep information encrypted until it reaches its destination. Without the strong encryption offered by a VPN, many businesses would have to reconsider their operations.

4. Trustable Apps:

We all hand over vast amounts of sensitive and personal information to app developers. Whether this is to allow the app to function as intended or not, we would all hope that any data stored about us is kept encrypted. Otherwise, any other app developer could slip in and take a peek at the unencrypted information.