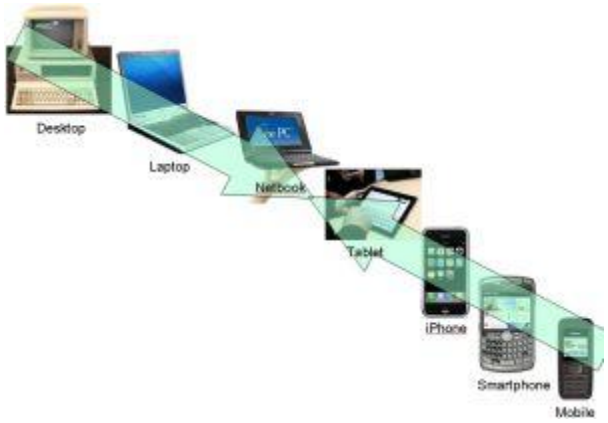
History of mobile computing

The Idea of mobile computing has only been around since the 1990s. Since then, Mobile computing has evolved from two-way radios that use large antennas to communicate simple messages to three inch personal computers that can do almost everything a regular computer does. People can't go to their local Starbucks and not see a laptop linked up to a hotspot Static network. This actually used to mean radio transmitters that operated on a stable base, usually with the help of large antennas. 2 way radios used by police officers were also considered mobile technology but now, it means people can connect wirelessly to the internet or to a private network almost anywhere. As long as a person has one of the devices capable of wirelessly accessing the internet, they are participating in mobile computing. Chances are, you have done it with a laptop computer or a personal digital assistant or PDA.So they decide to came up with an idea of portable devices These days, Pocket PCs are another way to conveniently access the internet on the earth devices that have been developed for mobile computing have taken over the wireless industry. This new type of communication is a very powerful tool for both businesses and personal use. The portable computer has change computing world confiered to hundred years' back. from huge machines that could not do much more than word processing to tiny hand held device. It offers the opportunity to bring people together and give everyone access to a greater wealth of information and knowledge, and to share their knowledge with others.



WHY MOBILE COMPUTING

Mobile computing is all about portable and small computers, which includes PDAs (Personal Digital Assistants) like mobile phones, palmtops, laptops etc. In this growing technological world, people are much bound to work on computers and Internet. People are attracted towards mobile devices because of their major features such as-

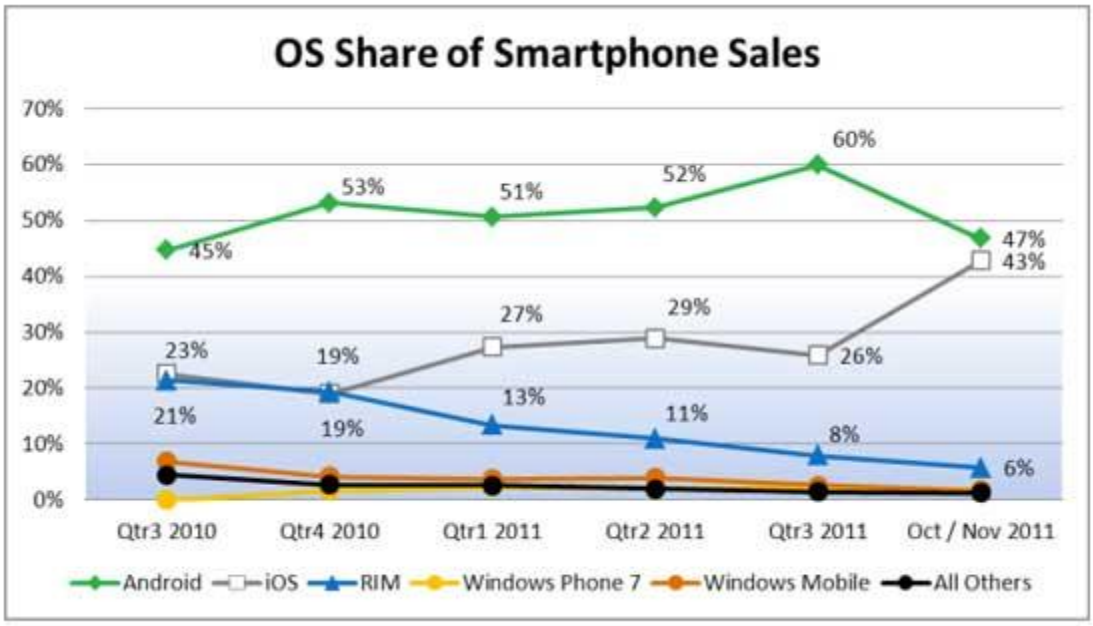
Mobile computing can be defined as the ability to use technology that is not physically connected to any static network. Nowadays, most laptops and personal digital assistants(PDA) all have wireless cards or Bluetooth interfaces built into them for very Good mobile internet access. Mobile computing is "taking a computer and all necessary files and software to the next Level.

They are wireless devices.
Mobile devices are portable that enables easy to carry and work with while you are on the move.
Has attractive user interface.
Provide many features like wireless LAN to access Internet from any part of the world.
Enables voice and typical data transmission
Enables one to one contact to have conversations
Though the mobile computing devices have drawbacks such as low bandwidth, lack of security, loss of connectivity and battery backup issue, people still prefer mobile computing devices to desktops.
They are wireless devices.
Mobile devices are portable that enables easy to carry and work with while you are on the move.
Has attractive user interface.
Provide many features like wireless LAN to access Internet from any part of the world.
Enables voice and typical data transmission
Enables one to one contact to have conversations
Though the mobile computing devices have drawbacks such as low bandwidth, lack of security, loss of connectivity and battery backup issue, people still prefer mobile computing devices to desktops.

In today's computing world, different technologies have emerged. These have grown to support the existing computer networks all over the world. With mobile computing, we find that the need to be confined within one physical location has been eradicated. We hear of terms such as telecommuting, which is being able to work from home or the field but at the same time accessing resources as if one is in the office

The advent of portable computers and laptops, Personal Digital Assistants (PDA), PC tablets and smartphones, has in turn made mobile computing very convenient. The portability of these devices ensure and enable the users to access all services as if they were in the internal network of their company. For example, the use of Tablet PC and iPads. This new technology enables the users to update documents, surf the internet, send and receive e-mail, stream live video files, take photographs and also support video and voice conferencing.

The constant and ever increasing demand for superior and robust smart devices has been a catalyst for market share. Each manufacturer is trying to carve a niche for himself in the market. These devices are invented and innovated to provide state-of-the-art applications and services. For instance, different manufacturers of cellular phones have come up with unique smartphones that are capable of performing the same task as computers and at the same processing speed. The market share for different competitors is constantly being fought for. For example, the manufacturers of Apple's iPhone OS, Google's Android' Microsoft Windows Mobile, Research In Motion's Blackberry OS, are constantly competing to offer better products with each release.



Source: The NPD Group, Consumer Tracking Service, Mobile Phone Track

The need for better, portable, affordable, and robust technology has made these vendors to constantly be innovative. Market figure and statistics show an ever growing need to purchase and use such devices for either professional or personal use. It is in this light that services to suit long-term implementation are developed or innovated. It has also pushed other industry vendors to adopt services that will provide better services. For example, cellular service providers are forced to improve and be innovative to capture more subscribers. This can be in terms of superior services such as high speed internet and data access, voice and video service etc. Hence the adoption of different generations of networks like of 2G, 2.5G, 3G, 4G network services.

The essence of mobile computing is to be able to work from any location. The use of iPads, tablets, smartphones, and notebooks, have pushed the demand for these devices. Modern day workers have such devices that enable them to carry out their work from the confines of their own location. These devices are configured to access and store large amounts of vital data. Executive and top management can take decisions based on ready information without going to the office. For example, sales reports and market forecasts can be accessed through these devices or a meeting can take place via video or audio conferencing through these devices. With such features being high in demand, manufacturers are constantly coming up with applications geared to support different services in terms of mobile computing.

Mobile Computing Security Issue:

Mobile computing has its fair share of security concerns as any other technology. Due to its nomadic nature, it's not easy to monitor the proper usage. Users might have different intentions on how to utilize this privilege. Improper and unethical practices such as hacking, industrial espionage, pirating, online fraud and malicious destruction are some but few of the problems experienced by mobile computing.

Another big problem plaguing mobile computing is credential verification. As other users share username and passwords, it poses as a major threat to security. This being a very sensitive issue, most companies are very reluctant to implement mobile computing to the dangers of misrepresentation.

The problem of identity theft is very difficult to contain or eradicate. Issues with unauthorized access to data and information by hackers, is also an enormous problem. Outsiders gain access to steal vital data from companies, which is a major hindrance in rolling out mobile computing services.

No company wants to lay open their secrets to hackers and other intruders, who will in turn sell the valuable information to their competitors. It's also important to take the necessary precautions to minimize these threats from taking place. Some of those measures include −

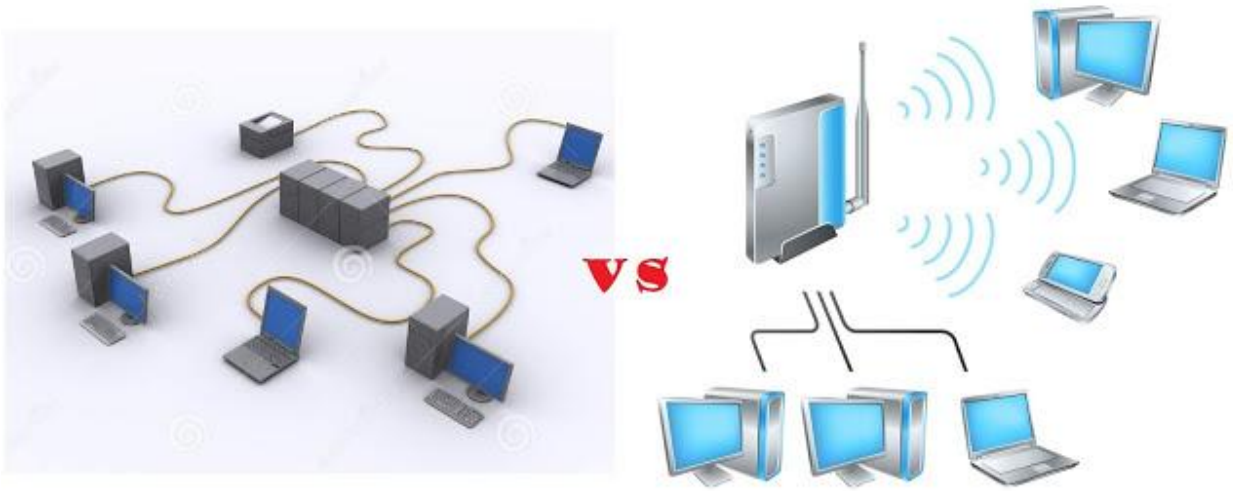
- Hiring qualified personnel.
- Installing security hardware and software
- Educating the users on proper mobile computing ethics
- Auditing and developing sound, effective policies to govern mobile computing
- Enforcing proper access rights and permissions
- These are just but a few ways to help deter possible threats to any company planning to offer mobile computing. Since information is vital, all possible measures should be evaluated and implemented for safeguard purposes.
- In the absence of such measures, it's possible for exploits and other unknown threats to infiltrate and cause irrefutable harm. These may be in terms of reputation or financial penalties. In such cases, it's very easy to be misused in different unethical practices.
- If these factors aren’t properly worked on, it might be an avenue for constant threat. Various threats still exist in implementing this kind of technology.

- **A General Security Issue Confidentiality:** Preventing unauthorized users from gaining access to critical information of any particular user.
- **Integrity:** Ensures unauthorized modification, destruction or creation of information cannot take place.
- **Availability:** Ensuring authorized users getting the access they require.
- **Legitimate:** Ensuring that only authorized users have access to services.
- **E. Accountability:** Ensuring that the users are held responsible for their security related activities by arranging the user and his/her activities are linked if and when necessary.
- **B Wireless Security Issues**
- The security issues that related of wireless networks are happened by intercepted of their radio signals by hacker, and by non-management of its network entirely by user because most of wireless networks are dependent on other private networks which managed by others, so the user has less control of security procedures. There are some of the main security issues of mobile computing, which introduced by using of wireless networks are:
- **Denial of Service (DOS) attacks:** It's one of common attacks of all kinds of networks and specially in wireless network, which mean the prevent of users from using network services by sending large amounts of unneeded data or connection requests to the communication server by an attacker which cause slow network and therefore the users cannot benefit from the use of its service.
- **Traffic Analysis:** It's identifying and monitoring the communicating between users through listening to traffic flowing in the wireless channel, in order to access to private information of users that can be badly used by attacker.
- **Eavesdropping:** The attacker can be log on to the wireless network and get access to sensitive data, this happens if the wireless a network was not enough secure and also the information was not encrypted. Session Interception and Messages Modification: Its interception the session and modify transmitted data in this session by the attacker through scenario which called: man in the middle which inserts the attacker's host between sender and receiver host.
- **Spoofing:** The attacker is impersonating an authorized account of another user to access sensitive data and unauthorized services.
- **Captured and Re transmitted Messages:** Its can get some of network services to attacker by get unauthorized access through capture a total message and replay it with some modifications to the same destination or another
- **C Device Security Issues** Mobile devices are vulnerable to new types of security attacks and vulnerable to theft not because of the get these devices itself, but because of get to sensitive data That exists within its devices. Mobile computing, like any computer software may damage by malware such as Virus, Spyware and Trojan. A virus is a real part of malicious software and Spyware is gathering information about the user without his knowledge. Some of main new mobile computing security issues introduced by using mobile devices include:

- **Pull Attacks:** In pull Attack, the attacker controls the device as a source of data by an attacker which obtained data by device itself.
- **Push Attacks:** It's creation a malicious code at mobile device by attacker and he may spread it to affect on other elements of the network.
- **Forced De-authentication:** The attacker convinces the mobile end-point to drop its connection and re-connection to get new signal, then he inserts his device between a mobile device and the network. Multi-protocol Communication: It is the ability of many mobile devices to operate using multiple protocols, e.g. a cellular provider's network protocol, most of the protocols have a security holes, which help the attacker to exploit this weakness and access to the device.
- **Mobility:** The mobility of users and their data that would introduce security threats determined in the location of a user, so it must be replicate of user profiles at different locations to allow roaming via different places without any concern regarding access to personal and sensitive data in any place and at any time. But the repetition of sensitive data on different sites that increase of security threats.
- **Disconnections:** When the mobile devices cross different places it occurs a frequent disconnections caused by external party resulting hand off.

Wired network

1. The wired networks require that the cables are connected to each and every one of the computers in the network.
2. The cost of a wired network is lower compared to the wireless network since Ethernet, cables, and switches are not expensive.
3. Wired LAN offers better performance compared to wireless networks. The wired network can offer a bandwidth of 100 Mbps with Fast Ethernet technology.
4. Ethernet cables, the switches that are used in wired networks are reliable.
5. The security considerations for a wired network connected to the internet are firewalls. Firewall software can be installed ...



COMPARISON BETWEEN WIRED AND WIRELESS NETWORKS

Below table mention comparison between wired network and wireless network:-

Sr. No	Parameters	Wired Network	Wireless Network
1	Installation	Difficult (Because more no's of compound are used during installation and required no's of cables for connecting each and every computers)	Easy installation
2	Speed and Bandwidth	High (up to 100mbps)	Low (up to 54mbps)
3	Reliability	High(Due to existence of wired technology and as manufactured cable have higher performance)	Reasonably high(because if the major section like router break down the whole network will be affected)
4	Cables	Ethernet, copper and optical fibers	Works on radio waves and microwaves
5	Mobility	Limited, as it operates in the area covered by connected systems with the wired network	Not limited, as it operates in the entire wireless network coverage
6	Security	Good	Weak
7	Interference	Less (Networks are invisible to other wired networks.	Higher (the potential for radio interference due to

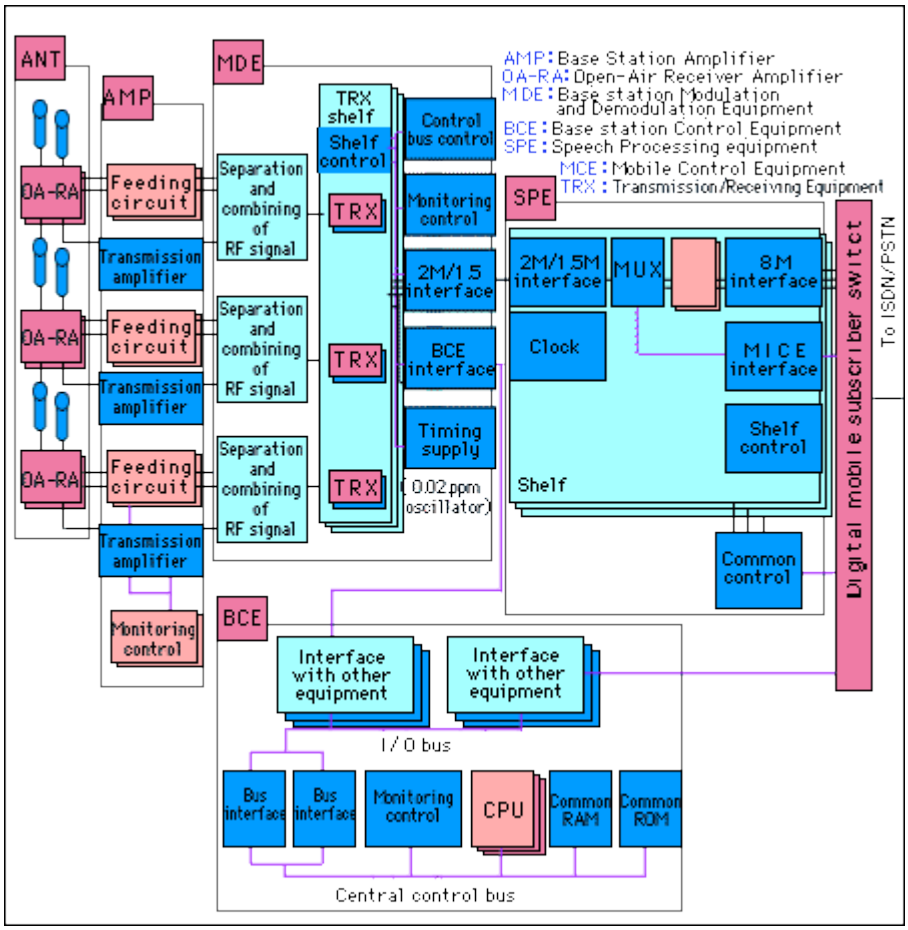
Sr. No	Parameters	Wired Network	Wireless Network
		The presence of one wired network has no effect on the performance of another wired network)	weather, other wireless devices, or obstructions like walls)
8	Quality of Service	Better	Poor
9	Connection setup time	Less	More
10	Devices used	Hubs and Switches	Routers
11	Cost	Less as cables are not expensive	More as wireless subscriber stations, wireless routers, wireless access points and adapters are expensive
12	Applications	LAN (Ethernet), MAN	WLAN, WPAN(Zigbee, bluetooth), Infrared, Cellular(GSM,CDMA, LTE)
13	Standards	IEEE802.3	IEEE802.11a, IEEE 802.11b , IEEE802.11g

base station

A base station is a fixed point of communication for customer cellular phones on a carrier network.

The base station is connected to an antenna (or multiple antennae) that receives and transmits the signals in the cellular network to customer phones and cellular devices. That equipment is connected to a mobile switching station that connects cellular calls to the public switched telephone network (PSTN).

A single base station may extend the service providers network by blocks or by miles. Base stations are company-specific. However, a single site may host multiple base stations from competing telecommunication companies.



Size matters

Small cells are a growing trend in base station technology. They provide the provider with the ability to cover smaller ranges as needed, using less power in each station. This is particularly useful in urban areas, where there's a high demand on the network that a larger macrocell wouldn't be able to handle on its own without cutting out. Most operators use a combination of sizes to prevent this from happening. A user walking through a city may connect to a larger base station atop a hillside in more remote or open areas, then to a smaller base station that's attached to the nearest traffic light when walking through more pedestrian-dense areas. This will depend on the city's infrastructure as well as the networking needs.

A more efficient option

Along with reliability, efficiency is another big concern for network providers, who want to create base stations that use the least amount of power while providing the most seamless service. Some, like Nokia Networks, are looking at renewable power sources like solar or wind energy to power their mobile towers. Others are using lithium-ion batteries. The size of the base station, as well as its location, have an impact on its power needs, so alternative forms of energy are a trend along with the use of small cells.

The bottom line

The future of base stations and cellular service depends on a variety of factors. Efficiency, performance, and user needs all factor into this developing technology. When users are on the go, radio signals can drop off without an efficient network of base stations in place. Service can also drop if too many users are trying to access the same station at the same time. For this reason, technology keeps improving to fill these gaps in the network and ensure that users get the clearest, most reliable, and most efficient service possible.

Wireless Network Applications

Wireless networks support many applications that benefit from user mobility and higher reliability because of less error-prone cabling. Furthermore, many wireless network applications realize significant cost savings because of increases in efficiencies and less downtime as compared to a wired network. Most wireless network technologies are license free, making them simple and cost effective to deploy.

Basic Configurations

In most cases, the wireless network is merely an extension of an existing wired network. In this case, a user is able to perform a particular task at an optimum location instead of somewhere that is less than ideal. A clerk unloading a truck, for example, can use a wireless handheld unit to scan items that the clerk removes from the truck. This is much more effective than writing down the item numbers and later entering them at a desktop terminal located somewhere inside the facility and far away from the loading dock.

Other situations involve dedicated wireless networks, which completely eliminate the need for wiring. For example, an emergency team responding to an airplane crash scene can quickly establish a temporary wireless network within the immediate area of the crash. All computer devices communicate directly with each other. This makes it possible for team members to have centralized access to important data concerning the crash.

Applications of wireless networks also fall within private or public scenarios. A company or homeowner that purchases and installs a wireless network for its own use is enabling a private application. Usually, private applications are made only available for company employees or home occupants. Access to the applications is not made available to the general public. In fact, companies generally implement security safeguards to ensure that only authorized people can connect to the network and access services.

Public applications, on the other hand, provide open access to anyone. A business traveler, for example, can use a public wireless LAN at an airport to access the Internet while waiting for a flight. These public hotspots are becoming widely available in airports and other areas, such as hotels, convention centers, and coffee shops where there are large concentrations of people toting computer devices.

Internet Access

One of the most compelling reasons to install a wireless network is to enable the sharing of a single high-speed Internet connection. With this type of configuration, every member of a family or small business can easily share a single high-speed connection that a cable or DSL modem

offers. This is convenient and saves money because everybody can simultaneously have access to the Internet and roam anywhere in the house or office.

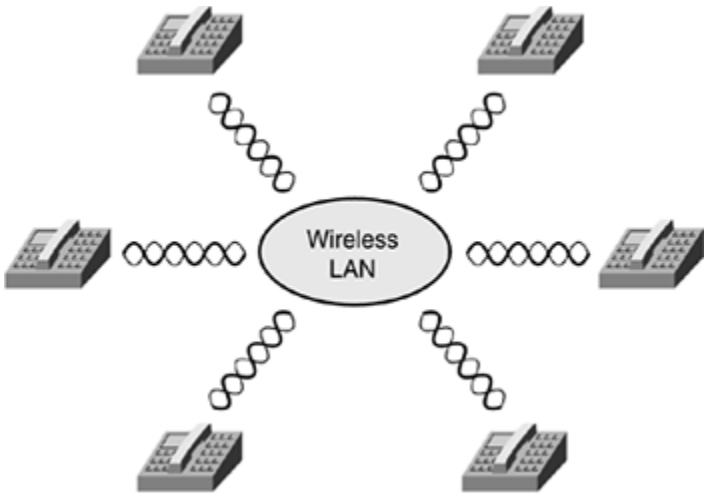
The wireless network in this scenario also increases the flexibility of the network because it's easy to add new workstations at any time without having to run cable. The relocation of wireless PCs, along with any printers and servers, is also painless.

A company can implement a wireless network to allow visiting employees and guests with wireless computer devices to quickly connect to the network with little configuration. The ability to use the Internet while away from the home location can greatly enhance productivity. The visitor can just turn on their laptop and have instant access to e-mail and applications.

Voice over Wireless

The use of wireless networks to support the transmission of voice conversations is a beneficial solution when people need to constantly stay in contact with each other. In fact, a wireless LAN designed to support voice communications can completely replace a traditional wire-based telephone system within a particular facility. (See Figure 1-5.) The combination of voice and data over the same wireless network provides total mobility and lower operating costs.

Figure 1-5. Wireless LAN Provides the Infrastructure for a Telephone System Within a Building



For example, employees within a retail store can locate certain clothes for a customer or check inventory by using special wireless LAN phones. The wireless LAN in the retail store can also support the transmission of bar codes when performing inventory or pricing using a wireless, handheld bar code scanner. Cost savings result because the company needs only to install and support a single communications system that carries both voice and data.

Likewise, a business can deploy their entire telephone system over a wireless LAN. This enables employees to carry their phone with them at all times, similar to a standard cell phone. Employees can accept calls within the facility at any time using a single phone.

Inventory Control

Many businesses profit from using wireless LANs when managing their manufacturing processes. This lowers operating costs. Because the connections between the manufacturing equipment and main control systems are wireless, the company can reconfigure the assembly process at any time from anywhere, saving time and money.

Through the use of a wireless LAN, a company can track and update inventory in real time, enabling efficiency and accuracy to increase dramatically. In a retail environment, as soon as a clerk purchases or stocks a product, a wireless management solution can update the inventory. In a manufacturing setting, the company can keep the raw materials and finished product statistics up-to-date. Employees equipped with wireless-enabled bar code scanners can check or change product prices or check the number in stock.

The improved accuracy provided by using a wireless LAN to manage inventory creates a chain reaction of benefits. Because the clerks enter the information directly into the main computer through handheld scanners, there is no paperwork to deal with. This significantly reduces human error when entering data, which leads to accurate financial records. This is important to manufacturing companies because accurate financial records ensure correct taxes are paid and fines (and possible law suits) are kept to a minimum.

Health Care

More and more hospitals are deploying wireless networks to improve operational efficiency and convenience. In most cases, hospitals deploy wireless LANs in high patient-traffic areas including emergency rooms, critical care wards, nursing stations, as well as in doctor's offices and patient waiting areas. Hospital staff can use mobile computer devices to increase efficiency and accuracy when caring for patients.

Health-care centers must maintain accurate records to ensure quality patient care. A simple mistake can cost someone's life. As a result, doctors and nurses must carefully record test results, physical data, pharmaceutical orders, and surgical procedures. This paperwork often overwhelms health-care staff, taking 50-70 percent of their time. The use of a mobile data collection device that wirelessly transmits the data to a centralized database significantly increases accuracy and raises the visibility of the data to those who need the information.

Doctors and nurses are also extremely mobile, going from room to room caring for patients. The use of electronic patient records, with the ability to input, view, and update patient data from anywhere in the hospital, increases the accuracy and speed of health care. This improvement is possible by providing each nurse and doctor with a wireless pen-based computer, such as a tablet or PDA, coupled with a wireless network to databases that store critical medical information about the patients.

A doctor caring for someone in the hospital, for example, can place an order for a blood test by keying the request into a handheld computer. The laboratory receives the order electronically and dispatches a lab technician to draw blood from the patient. The laboratory runs the tests requested by the doctor and enter the results into the patient's electronic medical record. The doctor can then check the results via the handheld appliance from anywhere in the hospital.

Another hospital application is tracking of pharmaceuticals. The use of mobile handheld bar code printing and scanning devices dramatically increases the efficiency and accuracy of all drug

transactions, such as receiving, picking, dispensing, inventory, and expiration dates. Most importantly, however, it ensures that hospital staff can administer the right drug to the right person in a timely fashion.

Education

Many colleges and elementary schools are finding beneficial reasons to install wireless LANs, mostly to provide mobile network applications to their students. In fact, schools have begun using the existence of wireless LAN access as a competitive advantage. These schools are targeting the growing number of students with laptops and expectations of accessing the Internet and school resources from anywhere on campus, such as classrooms, libraries, quads, and dormitories. Students are able to readily check e-mail, surf the Web, access specialized school applications, check grades, and view transcripts. As a result, students make better use of their time.

It's expensive to establish and maintain computer labs for students to utilize for accessing the Internet and completing assignments. Students must often wait in line for using a computer in a lab, which cuts into other activities. A wireless LAN, however, gives students access to needed resources using their own laptop from anywhere on campus at any time, even after the traditional computer lab closes. This more evenly distributes network access to all students, enhancing student efficiency. Of course, the school can also save the costs of running the computer lab.

Real Estate

Real estate salespeople perform a great deal of their work away from the office, usually talking with customers at the property being sold or rented. Before leaving the office, salespeople normally identify a few sites to show a customer, print the Multiple Listing Service (MLS) information that describes the property, and then drive to each location with the potential buyer. If the customer is unhappy with that round of sites, the real estate agent must drive back to the office and run more listings. Even if the customer decides to purchase the property, they must both go back to the real estate office to finish paperwork that completes the sale.

Wireless networking makes the sale of real estate much more efficient. The real estate agent can use a computer away from the office to access a wireless MLS record. An agent can also use a portable computer and printer to produce contracts and loan applications for signing at the point of sale.

Utilities

Utility companies operate and maintain a highly distributed system that delivers power and natural gas to industries and residences. Utility companies must continually monitor the operation of the electrical distribution system, gas lines, and water consumption, and must check usage meters at least monthly to calculate bills. Traditionally, this means a person must travel from location to location, visit residences and company facilities, record information, and then enter the data at a service or computing center.

Today, utility companies employ wireless WANs to support the automation of meter reading and system monitoring. Instead of a meter reader recording the data on a sheet of paper to later enter in a computer for processing, the meter can periodically transmit the data through the wireless WAN to the utility company. This saves time and reduces overhead costs by eliminating the need for human meter readers.

Field Service

Field service personnel spend most of their time on the road installing and maintaining systems or inspecting facilities under construction. To complete their jobs, these individuals need access to product documentation and procedures. Traditionally, field service employees have had to carry several binders of documentation with them to sites that often lacked a phone and even electricity.

In some cases, the field person might not be able to take all the documents to a job site, causing delay while obtaining the proper information. On long trips, this information might also become outdated. Updates require delivery that might take days to reach the person in the field. Wireless WAN access to documentation can definitely enhance field service. A field service employee, for example, can carry a portable computer that connects to the office LAN that contains accurate documentation of all applicable information.

Field Sales

Sales professionals are always on the move and meeting with customers. While on site with a customer, a salesperson needs access to vast information that describes products and services. Salespeople must also place orders, provide status?such as meeting schedules?to the home office, and maintain inventories.

With wireless access to the main office network, a salesperson can view centralized contact information, retrieve product information, produce proposals, create contracts, and stay in touch with office staff and other salespeople. This contact permits salespeople to complete the entire sale directly from the customer site, which increases the potential for a successful sale and shortens the sales cycle.

Vending

Beverage and snack companies place vending machines in hotels, airports, and office buildings to enhance the sales of their products. Vending machines eliminate the need for a human salesclerk. These companies, however, must send employees around to stock the machines periodically. In some cases, machines might become empty before the restocking occurs because the company has no way of knowing when the machine runs out of a particular product.

A wireless WAN can support the monitoring of stock levels by transporting applicable data from each of the vending machines to a central database that can be easily viewed by company personnel from a single location. Such monitoring allows companies to be proactive in stocking their machines, because they always know the stock levels at each machine. This enables the vending company to schedule appropriate stops for people who refill the machines.

Public Networks

Because of the significant proliferation of laptops, PDAs, and cell phones, a growing need exists for mobile interfaces to the Internet and corporate applications. Users want and expect seamless, constant mobile connectivity to all information sources with high levels of performance and availability. Wireless networks provide the infrastructure to support these needs in public areas that are away from the home or office.

A public wireless network offers a means for people on the go to connect with the Internet. In general, the places that have large groups of people that need or want network connections have wireless LAN access. Wireless MANs and WANs, on the other hand, provide coverage over larger areas having sparsely distributed populations.

Public wireless LANs are in common places such as hotels and restaurants, but all kinds of places are installing wireless LANs for public access. For example, approximately 90 percent of all boaters use the Internet regularly while at home or in the office. Many still want access to the Internet while relaxing on their boats, especially when parked overnight at a marina. As a result, marinas around the globe are installing wireless LANs to enable boaters to have access to Internet applications.

note

Refer to the following website for an extensive list of public wireless LANs: http://www.wi-fihotspotlist.com/.

To use a public wireless LAN, users must have a computer device, such as a laptop, with a wireless LAN NIC. IEEE 802.11b (Wi-Fi) is the most common type of wireless LAN today that public wireless network providers install. The computer device's NIC automatically senses the presence of the wireless LAN and associates with the network. Before accessing the Internet, the user must subscribe to the service, generally through a website accessible from the wireless LAN. Some public wireless LANs are free, but most providers charge a nominal price for using the service.

Another form of public wireless network uses wireless MAN technologies to provide wireless communications links between subscribers (homes and offices) and the Internet. The provider mounts a small antenna dish on the home or small office and points it to a centralized hub. This point-to-multipoint system provides the last-mile connection necessary to supply Internet access to locations where DSL and cable modem connections are not available or feasible.

Location-Based Services

With wireless networks, you can make the location of a particular person or item available to a central location. The ability to track the position of moving objects brings about some interesting applications. The coordinates of users can feed into a server-based application that implements a location-based service.

For example, a public wireless LAN provider can use this concept to display pertinent information to travelers as they walk through an airport or train station. Information might include their location on a moving map, in a way that the passenger can use to find the way to the next departure gate or the nearest restaurant. The value of this location-based service could entice passengers to use the particular venue.

A hospital might use location-based services to track the positions of doctors and nurses. This enables hospital administrators to dispatch the right person to an emergency. Patients end up receiving more rapid and effective care.

The usage of location-aware systems over wireless LANs is also moving to the consumer market. For example, the ability to track children is extremely valuable. Imagine being in a theme park and a toddler wandering off without the knowledge of the parent. With a location system, the parent can easily find the toddler among a large crowd. With a concealed wireless tracking tag located on the child, this type of system can aid tremendously if someone kidnaps a child.

A shopping mall might deploy a location system and send electronic flyers and advertisements to customers carrying PDAs. The system takes into consideration the physical location of shoppers within the facility and customizes actual content appropriately. Shoppers then make better use of their time, and stores make more money.

Users in this example might receive an electronic directory and advertisement flyer on their wireless PDA after entering the mall. The directory includes a map of the facility that identifies the person's exact position. As the shopper clicks on a store, restroom, or ATM in the directory, the map indicates directions that take them to the desired selection. If a spouse or shopping friend is carrying a wireless device, everyone can keep track of each other's location as well.

As global markets continue to develop at an amazing pace, it is becoming increasing important to ensure that all communication is accurately conveyed. Whether you are hosting an international convention or leading a group tour around your manufacturing plant, wireless audio receivers and headphones allow for fluid reception of everything said. However, several crucial factors come into play when selecting the best equipment for your attendees.

Infrared vs radio frequency

Listed below are some of the advantages and disadvantages of infrared (IR) wireless transmission.

Infrared Wireless Systems

Utilizing the same technology as most inexpensive TV remote control units, infrared wireless transmitters deliver the audio feed to your audience using invisible pulses of light. Some key points about Infrared systems:

- IR headphones require a clear line-of-sight to the signal, so there are limitations to where and how the transmitter(s) is setup.
- IR systems are immune to radio interference eliminating the need to search for the frequency.
- IR transmitters and receivers are sensitive to interference from waves of light (i.e., bright or flashing), so infrared technology is not suitable for applications outdoors or around flashing lights.
- IR signals are not easily intercepted making infrared transmission ideal when higher levels of security and privacy are required.
- IR wireless listening devices are confined within opaque walls and are not a good choice when people are moving between rooms or even large open spaces.

Although infrared transmissions offer better fidelity and security much of the time, you cannot ignore the physical variables that can cause serious limitations.

Radio Frequency Wireless Systems

RF or radio frequency communication uses electromagnetic waves for transmission, with frequencies below those of visible light. Some key points about RF transmissions include:

- RF signals can penetrate walls, and most other obstacles, making them a good choice for multiple room events.
- RF transmission offers excellent portability for events where attendees are on the move; and systems are easy to setup and use.
- RF receivers and portable transmitters are light and are ideal for guided tours or other on-the-go applications.
- RF systems are immune to interference from light, so transmission and reception are perfect for both indoor and outdoor uses.
- RF receivers have multi-channel configuration to support the transmission of multiple languages at the same time.

In general, RF systems are less expensive, easier to setup and do not require a lot of additional equipment for events with larger coverage areas.

To host a successful event, it is important to make everyone feel included and hearing what's going on is a crucial component. Wireless portable listening devices are the answer to deliver clear, crisp communication as your guest and staff move from place to place. But the physical restrictions of your coverage areas as well as your specific needs for security are two of the basic considerations when choosing between Infrared or Radio Frequency.

For additional information or professional advice in selecting the best equipment options for your meeting, conference, convention, training sessions or group tour, contact ProLingo. Our experienced staff is ready to help with whatever level of assistance you need. With a well-established network of strong business partners, we can deliver our quality standards anywhere in the world.

RF, also known as “radio frequency,” and IR, which stands for “Infrared,” are two kinds of energy used in remote controls to communicate commands. RF uses radio waves and IR is a kind of light that can’t be seen with the naked eye.

A good many consumers, when holding a remote control, may not know which kind is in his or her hand. As long as it works, few people care. But if you’re curious, the easiest way to tell is if you need to point the remote directly at the device you’re trying to control. Your TV remote is IR. Your garage door is RF.

Both technologies have advantages and disadvantages. IR is quick, efficient, and offers an ability to communicate a wide variety of commands. Its downside is that you always need line-of-sight for it to work properly. If something is in the way, you’re sunk. It also works over relatively short distances. Across a room is about as much as you can expect.

RF, on the other hand, can work over much longer distances. You can be down your street and still open your garage. Some high-end remote-controlled vehicles can be miles from their RF controls. RF can pass through solid walls too – as long as they’re not metal. However, RF

doesn’t transmit as complex patterns as IR, so commands must be simpler. Open, close; up, down; on, off – we’re talking really basic commands.

Because the data payload is quite small with RF, the components end up being less expensive to manufacture. You find them in common appliances like ceiling fans and garage doors: the commands don’t need to be complex and RF keeps the overall costs down while increasing range.

Now, as to “why should I care?” – YOU might not. But for those of us trying to create Smart Home products that bring everything together, having two very different technologies in almost every home creates quite a challenge.

We designed the Bond to work with both IR and RF in order to maximize the number of products we can help you to control. Ceiling fans can be either IR or RF. Garage doors, RF. AC units, IR. With the Bond, everything will work. It won’t matter whether you understand the difference between RF and IR – even though you do now.

WiMAX

is a wireless broadband solution that offers a rich set of features with a lot of flexibility in terms of deployment options and potential service offerings. Some of the more salient features that deserve highlighting are as follows −

Two Type of Services

WiMAX can provide two forms of wireless service −

- **Non-line-of-sight** − service is a WiFi sort of service. Here a small antenna on your computer connects to the WiMAX tower. In this mode, WiMAX uses a lower frequency range -- 2 GHz to 11 GHz (similar to WiFi).
- **Line-of-sight** − service, where a fixed dish antenna points straight at the WiMAX tower from a rooftop or pole. The line-of-sight connection is stronger and more stable, so it's able to send a lot of data with fewer errors. Line-of-sight transmissions use higher frequencies, with ranges reaching a possible 66 GHz.

OFDM-based Physical Layer

The WiMAX physical layer (PHY) is based on orthogonal frequency division multiplexing, a scheme that offers good resistance to multipath, and allows WiMAX to operate in NLOS conditions.

Very High Peak Data Rates

WiMAX is capable of supporting very high peak data rates. In fact, the peak PHY data rate can be as high as 74Mbps when operating using a 20MHz wide spectrum.

More typically, using a 10MHz spectrum operating using TDD scheme with a 3:1 downlink-to-uplink ratio, the peak PHY data rate is about 25Mbps and 6.7Mbps for the downlink and the uplink, respectively.

Scalable Bandwidth and Data Rate Support

WiMAX has a scalable physical-layer architecture that allows for the data rate to scale easily with available channel bandwidth.

For example, a WiMAX system may use 128, 512, or 1,048-bit FFTs (fast fourier transforms) based on whether the channel bandwidth is 1.25MHz, 5MHz, or 10MHz, respectively. This scaling may be done dynamically to support user roaming across different networks that may have different bandwidth allocations.

Adaptive Modulation and Coding (AMC)

WiMAX supports a number of modulation and forward error correction (FEC) coding schemes and allows the scheme to be changed as per user and per frame basis, based on channel conditions.

AMC is an effective mechanism to maximize throughput in a time-varying channel.

Link-layer Retransmissions

WiMAX supports automatic retransmission requests (ARQ) at the link layer for connections that require enhanced reliability. ARQ-enabled connections require each transmitted packet to be acknowledged by the receiver; unacknowledged packets are assumed to be lost and are retransmitted.

Support for TDD and FDD

IEEE 802.16-2004 and IEEE 802.16e-2005 supports both time division duplexing and frequency division duplexing, as well as a half-duplex FDD, which allows for a low-cost system implementation.

WiMAX Uses OFDM

Mobile WiMAX uses Orthogonal frequency division multiple access (OFDM) as a multiple-access technique, whereby different users can be allocated different subsets of the OFDM tones.

Flexible and Dynamic per User Resource Allocation

Both uplink and downlink resource allocation are controlled by a scheduler in the base station. Capacity is shared among multiple users on a demand basis, using a burst TDM scheme.

Support for Advanced Antenna Techniques

The WiMAX solution has a number of hooks built into the physical-layer design, which allows for the use of multiple-antenna techniques, such as beamforming, space-time coding, and spatial multiplexing.

Quality-of-service Support

The WiMAX MAC layer has a connection-oriented architecture that is designed to support a variety of applications, including voice and multimedia services.

WiMAX system offers support for constant bit rate, variable bit rate, real-time, and non-real-time traffic flows, in addition to best-effort data traffic.

WiMAX MAC is designed to support a large number of users, with multiple connections per terminal, each with its own QoS requirement.

Robust Security

WiMAX supports strong encryption, using Advanced Encryption Standard (AES), and has a robust privacy and key-management protocol.

The system also offers a very flexible authentication architecture based on **Extensible Authentication Protocol (EAP)**, which allows for a variety of user credentials, including username/password, digital certificates, and smart cards.

Support for Mobility

The mobile WiMAX variant of the system has mechanisms to support secure seamless handovers for delay-tolerant full-mobility applications, such as VoIP.

IP-based Architecture

The WiMAX Forum has defined a reference network architecture that is based on an all-IP platform. All end-to-end services are delivered over an IP architecture relying on IP-based protocols for end-to-end transport, QoS, session management, security, and mobility.

1.What is WiMAX

WiMAX is an IP based, wireless broadband access technology that provides performance similar to 802.11/Wi-Fi networks with the coverage and QOS (quality of service) of cellular networks. WiMAX is also an acronym meaning "Worldwide Interoperability for Microwave Access" (WiMAX).

WiMAX is a wireless digital communications system, also known as IEEE 802.16 that is intended for wireless "metropolitan area networks". WiMAX can provide broadband wireless access (BWA) up to 30 miles (50 km) for fixed stations, and 3 - 10 miles (5 - 15 km) for mobile stations. In contrast, the WiFi/802.11 wireless local area network standard is limited in most cases to only 100 - 300 feet (30 - 100m).

The most recent versions of both WiMAX standards in 802.16 cover spectrum ranges from at least the 2 GHz range through the 66 GHz range.

a. WiMAX Features

WiMAX is a wireless broadband solution that offers a rich set of features with a lot of flexibility in terms of deployment options and potential service offerings. Some of the more salient features that deserve highlighting are as follows:

1. Two Types of Services: WiMAX can provide two forms of wireless service:
    i. Non-line-of-sight: service is a Wi-Fi sort of service. Here a small antenna on your computer connects to the WiMAX tower. In this mode, WiMAX uses a lower frequency range- 2 GHz to 11 GHz (similar to Wi-Fi).
    ii. Line-of-sight: service, where a fixed dish antenna points straight at the WiMAX tower from a rooftop or pole. The line-of-sight connection is stronger and more stable, so it's able to send a lot of data with fewer errors. Line-of-sight transmissions use higher frequencies, with ranges reaching a possible 66 GHz.
2. OFDM-based physical layer: The WiMAX physical layer (PHY) is based on orthogonal frequency division multiplexing, a scheme that offers good resistance to multipath, and allows WiMAX to operate in NLOS conditions.
3. Very high peak data rates: WiMAX is capable of supporting very high peak data rates. In fact, the peak PHY data rate can be as high as 74Mbps when operating using a 20MHz wide spectrum. More typically, using a 10MHz spectrum operating using TDD scheme with a 3:1 downlink-to-uplink ratio, the peak PHY data rate is about 25Mbps and 6.7Mbps for the downlink and the uplink, respectively.
4. Scalable bandwidth and data rate support: WiMAX has a scalable physical-layer architecture that allows for the data rate to scale easily with available channel bandwidth. For example, a WiMAX system may use 128, 512, or 1,048-bit FFTs (fast Fourier transforms) based on whether the channel bandwidth is 1.25MHz, 5MHz, or 10MHz, respectively. This scaling may be done dynamically to support user roaming across different networks that may have different bandwidth allocations.

Despite an increasingly globalize economy, spectrum resources for wireless broadband worldwide are still quite disparate in its allocations. Mobile WiMAX technology therefore, is designed to be able to scale to work in different canalizations from 1.25 to 20 MHz to comply with varied worldwide requirements.

Wireless Broadband Technologies: Wimax Features

5. Adaptive modulation and coding (AMC): WiMAX supports a number of modulation and forward error correction (FEC) coding schemes and allows the scheme to be changed on a per user and per frame basis, based on channel conditions. AMC is an effective mechanism to maximize throughput in a time-varying channel.

6. Link-layer retransmissions: WiMAX supports automatic retransmission requests (ARQ) at the link layer for connections that require enhanced reliability. ARQ-enabled connections require each transmitted packet to be acknowledged by the receiver; unacknowledged packets are assumed to be lost and are retransmitted.

7. Support for TDD and FDD: IEEE 802.16-2004 and IEEE 802.16e-2005 supports time division duplexing and frequency division duplexing, as well as a half-duplex FDD, which allows for a low-cost system implementation.

8. WiMAX uses OFDM: Mobile WiMAX uses orthogonal frequency division multiple access (OFDM) as a multiple-access technique, whereby different users can be allocated different subsets of the OFDM tones. Flexible and dynamic per user resource allocation: Both uplink and downlink resource allocation are controlled by a scheduler in the base station. Capacity is shared among multiple users on a demand basis, using a burst TDM scheme.

9. Support for advanced antenna techniques: The WiMAX solution has a number of hooks built into the physical-layer design, which allows for the use of multiple-antenna techniques, such as beam forming, space-time coding, and spatial multiplexing.

10. Quality-of-service support: The WiMAX MAC layer has a connection-oriented architecture that is designed to support a variety of applications, including voice and multimedia services.

11. WiMAX system offers support for constant bit rate, variable bit rate, real-time, and non-real-time traffic flows, in addition to best-effort data traffic.

12. WiMAX MAC is designed to support a large number of users, with multiple connections per terminal, each with its own QoS requirement.

13. Robust security: WiMAX supports strong encryption, using Advanced Encryption Standard (AES), and has a robust privacy and key-management protocol. The system also offers a very flexible authentication architecture based on Extensible Authentication Protocol (EAP), which allows for a variety of user credentials, including username/password, digital certificates, and smart cards.

14. Support for mobility: The mobile WiMAX variant of the system has mechanisms to support secure seamless handovers for delay-tolerant full-mobility applications, such as VoIP.

15. IP-based architecture: The WiMAX Forum has defined a reference network architecture that is based on an all-IP platform. All end-to-end services are delivered over an IP architecture relying on IP-based protocols for end-to-end transport, QoS, session management, security, and mobility.

Difference between WiFi and WiMax:

WIFI	WIMAX

WIFI	WIMAX
Wifi is defined under IEEE 802.11x standards where x stands for various WiFi versions.	WiMax is defined under IEEE 802.16y standards where y stands for various WiMax versions.
WiFi is for LAN (Local Area Network) applications.	WiMax is for MAN (Metropolitan Area Network) applications.
WiFi does not guarantee any Quality of Service (Qos).	WiMax guarantee Quality of Service (Qos).
WiFi network range is around 100 meters.	WiMax network can reach about 50-90 km.
WiFi MAC layer uses CSMA/CA protocol which is not connection oriented.	WiMax is connection oriented in nature.
WiFi is short range technology.	WiMax is long range technology.
WiFi connection can	**WiMax connection can**

WIFI	WIMAX
transmit upto 54 mbps.	transmit upto 70 mbps.

Introduction to GSM

Global system for mobile communication (GSM) is wide area wireless communications system that uses digital radio transmission to provide voice, data, and multimedia communication services. A GSM system coordinates the communication between a mobile telephones (mobile stations), base stations (cell sites), and switching systems. Each GSM radio channel is 200 kHz wide channels that are further divided into frames that hold 8 time slots. GSM was originally named Groupe Special Mobile. The GSM system includes mobile telephones (mobile stations), radio towers (base stations), and interconnecting switching systems. The GSM system allows up to 8 to 16 voice users to share each radio channel and there may be several radio channels per radio transmission site (cell site).

Figure 1.1 shows an overview of a GSM radio system. This diagram shows that the GSM system includes mobile communication devices that communicate through base stations (BS) and a mobile switching center (MSC) to connect to other mobile telephones, public telephones, or to the Internet. This diagram shows that the MSC connects to databases of customers. This example shows that the GSM system mobile devices can include mobile telephones or data communication devices such as laptop computers.

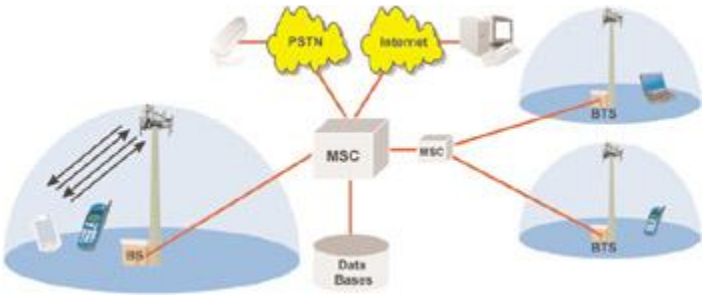


Figure 1.1: Global System for Mobile Communications (GSM)

The GSM specification was initially created to provide a single industry standard for European cellular systems. In 1982, the development of the GSM specification began and the first commercial GSM system began operation in 1991. In 2004, there were more than 1.046 billion GSM subscribers in 205 countries

1. 1. GSM – GLOBAL SYSTEM FOR MOBILE COMMUNICATION Private & Confidential property of Shilpin Pvt. Ltd. 1
2. 2. Why we chose GSM o Drivers influencing change in Telco industry o o o o Deregulation Competition Customers Technological Advances Private & Confidential property of Shilpin Pvt. Ltd. 2
3. 3. TOPICS • GSM Overview • System Architecture • GSM Call Flow • GSM Services Private & Confidential property of Shilpin Pvt. Ltd. 3
4. 4. GSM OVERVIEW • GSM (Global System for Mobile communications: originally from Groupe Special Mobile) is the most popular standard for mobile phones in the

world. • GSM is used by over 3 billion people across more than 212 countries and territories. Its ubiquity makes international roaming very common between mobile phone operators, enabling subscribers to use their phones in many parts of the world. Private & Confidential property of Shilpin Pvt. Ltd. 4

5. 5. System Architecture 5 Private & Confidential property of Shilpin Pvt. Ltd.
6. 6. System Architecture • Mobile Station (MS) • Base Station Subsystem (BSS) • Network Switching Subsystem (NSS) Private & Confidential property of Shilpin Pvt. Ltd. 6
7. 7. System Architecture Mobile Station (MS) The Mobile Station is made up of two entities: 1. Mobile Equipment (ME) 2. Subscriber Identity Module (SIM) Private & Confidential property of Shilpin Pvt. Ltd. 7
8. 8. System Architecture Mobile Station (MS) contd. Mobile Equipment • • • Produced by many different manufacturers Peripheral device of the Mobile Station and offers services to the user Uniquely identified by an IMEI (International Mobile Equipment Identity) Private & Confidential property of Shilpin Pvt. Ltd. 8
9. 9. System Architecture Mobile Station (MS) contd. Subscriber Identity Module (SIM) • • • • • • Smart card containing the International Mobile Subscriber Identity (IMSI) Allows user to send and receive calls and receive other subscribed services Encoded network identification details Protected by a password or PIN Can be moved from phone to phone – contains key information to activate the phone Private & Confidential property of Shilpin Pvt. Ltd. 9
10. 10. System Architecture Mobile Station (MS) contd. International Mobile Subscriber Identity (IMSI) • • • • • An IMSI is usually a 15 digits long number The first 3 digits : Mobile Country Code (MCC), Followed by Mobile Network Code (MNC), either 2 digits (European std) or 3 digits (North American std). Mobile station identification number (MSIN) within the network's customer base. Example : IMSI: 310150123456789 MCC 310 USA MNC 150 AT&T MSIN 123456789 Private & Confidential property of Shilpin Pvt. Ltd. 10
11. 11. System Architecture Base Station Subsystem (BSS) Base Station Subsystem is composed of two parts that communicate across the standardized Abis interface allowing operation between components made by different suppliers 1. Base Transceiver Station (BTS) 2. Base Station Controller (BSC) Private & Confidential property of Shilpin Pvt. Ltd. 11
12. 12. System Architecture Base Station Subsystem (BSS) contd. Base Transceiver Station (BTS) • • • • Houses the radio transceivers that define a cell Handles radio-link protocols with the Mobile Station Speech and data transmissions from the MS are recoded Requirements for BTS: ruggedness reliability portability minimum costs Private & Confidential property of Shilpin Pvt. Ltd. 12
13. 13. System Architecture Base Station Subsystem (BSS) contd. Base Station Controller (BSC) • • • • Manages Resources for BTS Handles call set up Location update Handover for each MS Private & Confidential property of Shilpin Pvt. Ltd. 13
14. 14. System Architecture Network Switching Subsystem • Central component of GSM system. • Carries out switching functions. • Manages communications between mobile phones and PSTN. • Architecture closely resembles a telephone exchange, but also supports mobility management. • NSS usually refers to Circuit Switched core network. GPRS core network is a separate component (technically not a part of NSS). Private & Confidential property of Shilpin Pvt. Ltd. 14

15. 15. System Architecture Network Switching Subsystem 15 Private & Confidential property of Shilpin Pvt. Ltd.
16. 16. System Architecture Network Switching Subsystem Components of NSS • • • • • Mobile Switching Centre (MSC) Home Location Register (HLR) Visitor Location Register (VLR) Authentication Centre (AUC) Equipment Identity Register (EIR) Private & Confidential property of Shilpin Pvt. Ltd. 16
17. 17. System Architecture Network Switching Subsystem Mobile Switching Center (MSC) • Primary service delivery node for GSM • Sets up and releases end-to-end connections • Handles voice calls, SMS and supplementary services (e.g. conference calls, call hold etc.) • Delivers messages from subscribers to SMSC and viceversa • Handles mobility management • Handles hand-over requirements during the call (BSC to BSC as well as this MSC to other MSC) • Handles generation of information used for billing • For pre-paid, handles real time account monitoring (with help of IN) Private & Confidential property of Shilpin Pvt. Ltd. 17
18. 18. System Architecture Network Switching Subsystem Different names for Mobile Switching Centers (MSCs) • G-MSC (Gateway MSC) MSC that determines which Visited MSC (V-MSC) the subscriber being called is currently located. Interfaces with the PSTN. All incoming calls to mobile are routed through G-MSC. Other external networks • V-MSC (Visited MSC) MSC where a customer is currently located. The VLR associated with V-MSC will have the subscriber's data • Anchor MSC MSC from which a handover has been initated. • Target MSC MSC towards which a handover should take place. 18 Private & Confidential property of Shilpin Pvt. Ltd.
19. 19. System Architecture Network Switching Subsystem Home Location Register (HLR) • Central database for every PLMN containing details of each subscriber. • Stores data for each subscriber as long as the subscriber remains with the PLMN (mobile phone operator). • MSISDN (subscriber number) is the primary key for HLR records. • Stores SIM number (IMSI). • Stores GSM services that the subscriber can use. • Stores GPRS settings for the subscriber. • Stores current location of subscriber (VLR and SGSN). • Stores call divert settings, if any, for each MSISDN. • Stores SMSC address (for routing SMS's) Private & Confidential property of Shilpin Pvt. Ltd. 19
20. 20. System Architecture Network Switching Subsystem Functions of HLR • Manages the mobility of subscribers by means of updating their 'location areas' (area covered by a set of base stations). • Sends the subscriber data to a VLR or SGSN when a subscriber first roams there. • Brokers between the G-MSC or SMSC and the subscriber's current VLR in order to allow call/SMS to be delivered. • Removes subscriber data from the previous VLR when a subscriber has roamed away from it. Private & Confidential property of Shilpin Pvt. Ltd. 20
21. 21. System Architecture Network Switching Subsystem Visitor Location Register (VLR) • Serves a specific geographical area. • Temporary database of the subscribers who have roamed into its served area. • Each base station is served by exactly 1 VLR. • In other words, a subscriber can not be present in more than 1 VLR at any point of time. • Stores SIM number (IMSI). • Stores authentication data. • Stores MSISDN (subscriber number). • Stores GSM services that are allowed for the subscriber. • Subscribed access point (APN) for GPRS use. • HLR address of the subscriber. Private & Confidential property of Shilpin Pvt. Ltd. 21

22. 22. System Architecture Network Switching Subsystem Functions of VLR • Informs HLR that his subscriber has arrived. • Tracks where the subscriber is still within the VLR area (location area) when no call is ongoing. • Allows or disallows which services the subscriber may use. • Allocates roaming numbers (MSRN) during the processing of incoming calls. • Purges the subscriber record if a subscriber becomes inactive for some fixed time whilst in the area of a VLR (e.g. switched off or moved to no-network area. Informs HLR accordingly. • Alternatively, deletes the subscriber record when a subscriber explicitly moves to another, as instructed by the HLR. 22 Private & Confidential property of Shilpin Pvt. Ltd.
23. 23. System Architecture Network Switching Subsystem Authentication Centre (AUC) • The authentication centre (AUC) is a function to authenticate each SIM card that attempts to connect to the GSM core network. • Typically used when the phone is powered on. • Generates an encryption key that is subsequently use to encrypt all wireless communication (voice, SMS etc.) • A key element in an operator's strategy to avoid SIM cloning. • Security of the process depends upon a shared secret between the AUC and the SIM called Ki. Private & Confidential property of Shilpin Pvt. Ltd. 23
24. 24. System Architecture Network Switching Subsystem Equipment Identity Register (EIR) • Database of mobile phones which are to be banned from network or monitored. • Used to allow tracking of stolen mobile phones. • Often integrated with the HLR. • Some EIRs have the capacity to log handset attempts and store it in a log file. • In theory, all data about all stolen mobile phones should be distributed to all EIRs in the world through a central EIR (CEIR). • In practice this is not the case however. There are some countries for which EIR is not even in operation. Private & Confidential property of Shilpin Pvt. Ltd. 24
25. 25. GSM Call Flow • Components – Subscription – Mobile phone – SIM • Terms – – – – – Home Location Register (HLR) Coverage – Base Transceiver Station Visitation Visitor Location register (paging) Authentication Center Private & Confidential property of Shilpin Pvt. Ltd. 25
26. 26. GSM Call Flow contd… • Outgoing Voice Call Flow – Dials a number – Mobile sends call setup request to BTS – Request handled by MSC • Checks subscriber's record in VLR • Routes the call via HLR – http://www.eventhelix.com/realtimemantra/Telecom/GSM_Origin ating_Call_Flow.pdf • Incoming Voice Call Flow – Routed to Gateway MSC • Determines the called phone location via HLR Private & Confidential property of Shilpin Pvt. Ltd. 26
27. 27. GSM Call Flow contd… • Call Routing – HLR determines call divert or direct call – Call divert – CFU/ CFNRc number – Roaming – HLR requests MSRN from VLR which is routed to MSC via Gateway MSC • Ringing – MSRN used to determine the phone – MSC pages the BTS – If subscriber answers, speech path created Private & Confidential property of Shilpin Pvt. Ltd. 27
28. 28. GSM Call Flow contd… – Ringing of Phone • • • • • • MSRN Paging Speech path CFB CFNRy Voice mail Private & Confidential property of Shilpin Pvt. Ltd. 28
29. 29. GSM Services o The GSM services can be grouped under 3 categories: o Teleservices o Bearer Services o Supplementary Services Private & Confidential property of Shilpin Pvt. Ltd. 29
30. 30. Services Contd… • Teleservices • Regular telephony • emergency calls • voice messaging • Bearer Services • Data Services • SMS – Messages upto 160 characters •

Cell Broadcast – Messages upto 93 characters Private & Confidential property of Shilpin Pvt. Ltd. 30

31. 31. Services Contd… • Supplementary Services • • • • • • • Barring Outgoing Calls Barring of International Calls Barring of Roaming Calls Call Forward, Call Hold, Call Wait, Call Transfer Completion of calls to busy subscribers Calling number identification presentation/restriction

GPRS (General Packet Radio Services)

General Packet Radio Services (GPRS) is a packet-based wireless communication service that promises data rates from 56 up to 114 Kbps and continuous connection to the Internet for mobile phone and computer users. The higher data rates allow users to take part in video conferences and interact with multimedia Web sites and similar applications using mobile handheld devices as well as notebook computers. GPRS is based on Global System for Mobile (GSM) communication and complements existing services such circuit-switched cellular phone connections and the Short Message Service (SMS).

In theory, GPRS packet-based services cost users less than circuit-switched services since communication channels are being used on a shared-use, as-packets-are-needed basis rather than dedicated to only one user at a time. It is also easier to make applications available to mobile users because the faster data rate means that middleware currently needed to adapt applications to the slower speed of wireless systems are no longer be needed. As GPRS has become more widely available, along with other 2.5G and 3G services, mobile users of virtual private networks (VPNs) have been able to access the private network continuously over wireless rather than through a rooted dial-up connection.

GPRS also complements Bluetooth, a standard for replacing wired connections between devices with wireless radio connections. In addition to the Internet Protocol (IP), GPRS supports X.25, a packet-based protocol that is used mainly in Europe. GPRS is an evolutionary step toward Enhanced Data GSM Environment (EDGE) and Universal Mobile Telephone Service (UMTS).

General Packet Radio Service (**GPRS**) is a packet oriented mobile data standard on the 2G and 3G cellular communication network's global system for mobile communications (GSM). GPRS was established by European Telecommunications Standards Institute (ETSI) in response to the earlier CDPD and i-mode packet-switched cellular technologies. It is now maintained by the 3rd Generation Partnership Project (3GPP).[1][2]

GPRS is typically sold according to the total volume of data transferred during the billing cycle, in contrast with circuit switched data, which is usually billed per minute of connection time, or sometimes by one-third minute increments. Usage above the GPRS bundled data cap may be charged per MB of data, speed limited, or disallowed.

GPRS is a best-effort service, implying variable throughput and latency that depend on the number of other users sharing the service concurrently, as opposed to circuit switching, where a certain quality of service (QoS) is guaranteed during the connection. In 2G systems, GPRS provides data rates of 56–114 kbit/sec.[3] 2G cellular technology combined with GPRS is sometimes described as *2.5G*, that is, a technology between the second (2G) and third (3G) generations of mobile telephony.[4] It provides moderate-speed data transfer, by using unused time division multiple access (TDMA) channels in, for example, the GSM system. GPRS is integrated into GSM Release 97 and newer release

GSM (Global System for Mobile communication)

GSM (Global System for Mobile communication) is a digital mobile network that is widely used by mobile phone users in Europe and other parts of the world. GSM uses a variation of time division multiple access (TDMA) and is the most widely used of the three digital wireless telephony technologies: TDMA, GSM and code-division multiple access (CDMA). GSM digitizes and compresses data, then sends it down a channel with two other streams of user data, each in its own time slot. It operates at either the 900 megahertz (MHz) or 1,800 MHz frequency band.

GSM, together with other technologies, is part of the evolution of wireless mobile telecommunications that includes High-Speed Circuit-Switched Data (HSCSD), General Packet Radio Service (GPRS), Enhanced Data GSM Environment (EDGE) and Universal Mobile Telecommunications Service (UMTS).

History

Predecessors to GSM, including Advanced Mobile Phone System (AMPS) in the United States and Total Access Communication System (TACS) in the United Kingdom, were built with analog technology. However, these telecommunications systems were unable to scale with the adoption of more users. The shortcomings of these systems pointed to a need for a more efficient cellular technology that could also be used internationally.

To achieve that goal, the European Conference of Postal and Telecommunications Administrations (CEPT) set up a committee to develop a European standard for digital

telecommunications in 1983. CEPT decided on several criteria that the new system must meet: international roaming support, high speech quality, support for handheld devices, low service cost, support for new services and Integrated Services Digital Network (ISDN) capability.

In 1987, representatives from 13 European countries signed a contract to deploy a telecommunications standard. The European Union (EU) then passed laws to require GSM as a standard in Europe. In 1989, the responsibility of the GSM project was transferred from CEPT to the European Telecommunications Standards Institute (ETSI).

Mobile services based on GSM were first launched in Finland in 1991. That same year, the GSM standard frequency band was expanded from 900 MHz to 1,800 MHz. In 2010, GSM represented 80% of the global mobile market. However, several telecommunications carriers have decommissioned their GSM networks, including Telstra in Australia. In 2017, Singapore retired its 2G GSM network.

Composition of the network

The GSM network has four separate parts that work together to function as a whole: the mobile device itself, the base station subsystem (BSS), the network switching subsystem (NSS) and the operation and support subsystem (OSS).

The mobile device connects to the network via hardware. The subscriber identity module (SIM) card provides the network with identifying information about the mobile user.

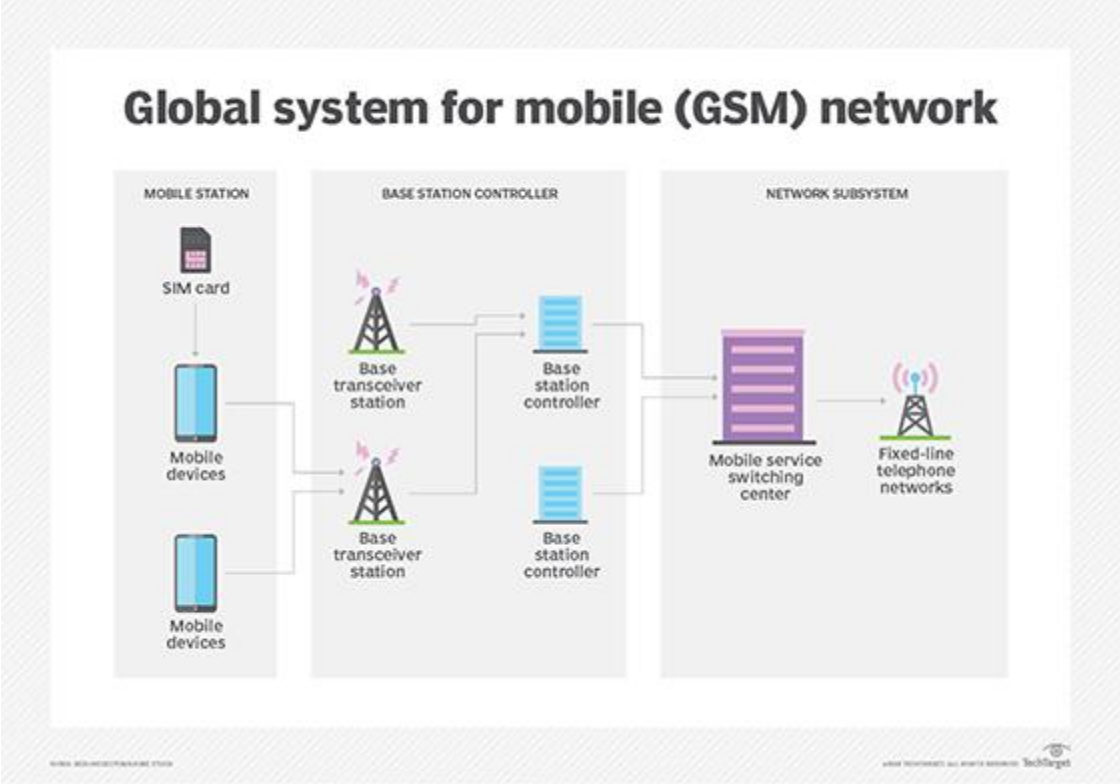


Diagram of the GSM network organization

The BSS handles traffic between the cell phone and the NSS. It consists of two main components: the base transceiver station (BTS) and the base station controller (BSC). The BTS contains the equipment that communicates with the mobile phones, largely the radio transmitter receivers and antennas, while the BSC, is the intelligence behind it. The BSC communicates with and controls a group of base transceiver stations.

The NSS portion of the GSM network architecture, often called the core network, tracks the location of callers to enable the delivery of cellular services. Mobile carriers own the NSS. The NSS has a variety of parts, including mobile switching center (MSC) and home location register (HLN). These components perform different functions, such as routing calls and Short Message Service (SMS) and authenticating and storing caller account information via SIM cards.

Discover the differences between CDMA and GSM.

Since many GSM network operators have roaming agreements with foreign operators, users can often continue to use their phones when they travel to other countries. SIM cards that hold home network access configurations may be switched to those with metered local access, significantly reducing roaming costs, while experiencing no reductions in service.

Security details

Although GSM was designed as a secure wireless system, it can still experience attacks. It uses authentication measures, such as challenge-response authentication, which prompts a user to provide a valid answer to a question, and a preshared key that can come in the form of a password or passphrase.

GSM Architecture

A GSM network consists of the following components:

- **A Mobile Station:** It is the mobile phone which consists of the transceiver, the display and the processor and is controlled by a SIM card operating over the network.
- **Base Station Subsystem:** It acts as an interface between the mobile station and the network subsystem. It consists of the Base Transceiver Station which contains the radio transceivers and handles the protocols for communication with mobiles. It also consists of the Base Station Controller which controls the Base Transceiver station and acts as a interface between the mobile station and mobile switching centre.
- **Network Subsystem:** It provides the basic network connection to the mobile stations. The basic part of the Network Subsystem is the Mobile Service Switching Centre which provides access to different networks like ISDN, PSTN etc. It also consists of the Home Location Register and the Visitor Location Register which provides the call routing and roaming capabilities of GSM. It also contains the Equipment Identity Register which maintains an account of all the mobile equipments wherein each mobile is identified by its own IMEI number. IMEI stands for International Mobile Equipment Identity.

Features of GSM Module:

- Improved spectrum efficiency
- International roaming
- Compatibility with integrated services digital network (ISDN)
- Support for new services.
- SIM phonebook management
- Fixed dialing number (FDN)
- Real time clock with alarm management
- High-quality speech
- Uses encryption to make phone calls more secure
- Short message service (SMS)

The security strategies standardized for the GSM system make it the most secure telecommunications standard currently accessible. Although the confidentiality of a call and secrecy of the GSM subscriber is just ensured on the radio channel, this is a major step in achieving end-to- end security.

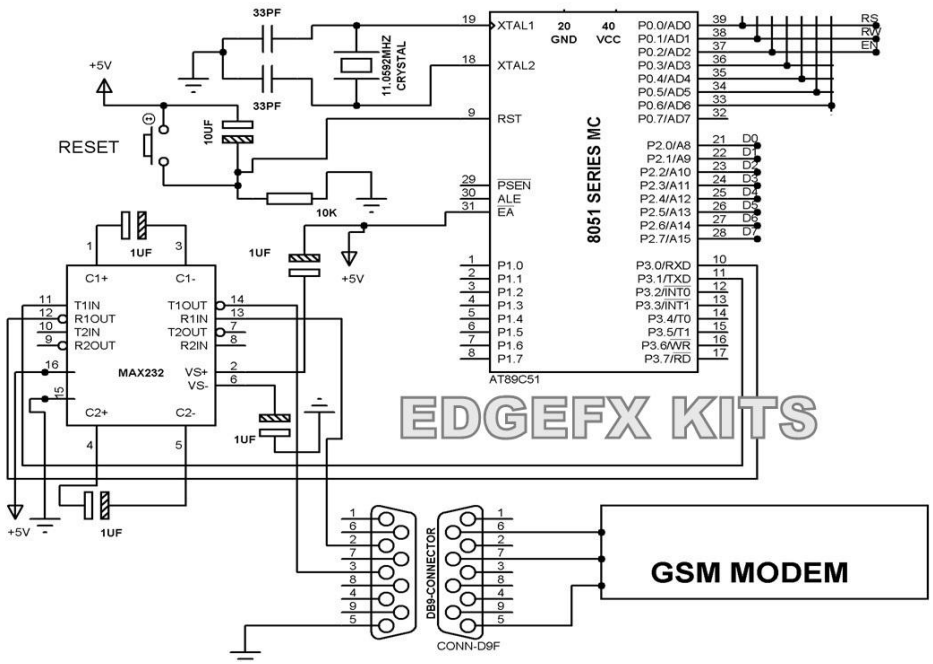
GSM Modem

A GSM modem is a device which can be either a mobile phone or a modem device which can be used to make a computer or any other processor communicate over a network. A GSM modem requires a SIM card to be operated and operates over a network range subscribed by the network operator. It can be connected to a computer through serial, USB or Bluetooth connection.

A GSM modem can also be a standard GSM mobile phone with the appropriate cable and software driver to connect to a serial port or USB port on your computer. GSM modem is usually preferable to a GSM mobile phone. The GSM modem has wide range of applications in transaction terminals, supply chain management, security applications, weather stations and GPRS mode remote data logging.

Working of GSM Module:

From the below circuit, a GSM modem duly interfaced to the MC through the level shifter IC Max232. The SIM card mounted GSM modem upon receiving digit command by SMS from any cell phone send that data to the MC through serial communication. While the program is executed, the GSM modem receives command ‘STOP’ to develop an output at the MC, the contact point of which are used to disable the ignition switch. The command so sent by the user is based on an intimation received by him through the GSM modem ‘ALERT’ a programmed message only if the input is driven low. The complete operation is displayed over 16×2 LCD display.



GMS Modem Circuit

Intelligent GSM Device for Automation and Security

In these days, the GSM mobile terminal has become one of the items that are constantly with us. Just like our wallet/purse, keys or watch, the GSM mobile terminal provides us a communication channel that enables us to communicate with the world. The requirement for a person to be reachable or to call anyone at any time is very appealing.

In this project, as the name says project is based on GSM network technology for transmission of SMS from sender to receiver. SMS sending and receiving is used for ubiquitous access of appliances and allowing breach control at home. The system proposes two sub-systems. Appliance control subsystem enables the user to control home appliances remotely and the security alert subsystem gives the automatic security monitoring.

The system is capable enough to instruct user via SMS from a specific cell number to change the condition of the home appliance according to the user's needs and requirements. The second aspect is that of security alert which is achieved in a way that on the detection of intrusion, the system allows automatic generation of SMS thus alerting the user against security risk.

Android

Introduction:

Android is a Linux based operating system it is designed primarily for touch screen mobile devices such as smart phones and tablet computers. The operating system have developed a lot in last 15 years starting from black and white phones to recent smart phones or mini computers. One of the most widely used mobile OS these days is android. The android is software that was founded in Palo Alto of California in 2003.

The android is a powerful operating system and it supports large number of applications in Smartphones. These applications are more comfortable and advanced for the users. The hardware that supports android software is based on ARM architecture platform. The android is an open source operating system means that it's free and any one can use it. The android has got millions of apps available that can help you managing your life one or other way and it is available low cost in market at that reasons android is very popular.

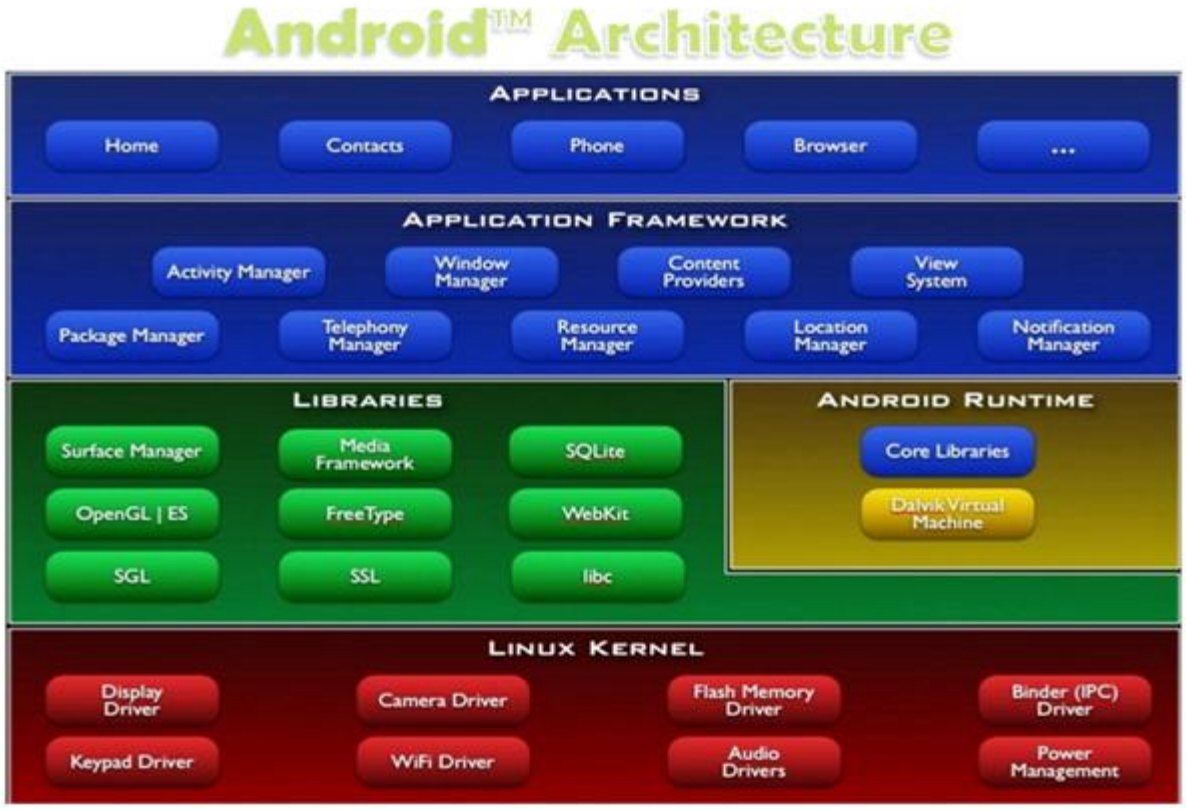
The android development supports with the full java programming language. Even other packages that are API and JSE are not supported. The first version 1.0 of android development kit (SDK) was released in 2008 and latest updated version is jelly bean.

Android Architecture:

The android is a operating system and is a stack of software components which is divided into five sections and four main layers that is

- Linux kernel
- Libraries
- Android runtime

Application frame work:



Linux kernel:

The android uses the powerful Linux kernel and it supports wide range of hardware drivers. The kernel is the heart of the operating system that manages input and output requests from software. This provides basic system functionalities like process management, memory management, device management like camera, keypad, display etc the kernel handles all the things. The Linux is really good at networking and it is not necessary to interface it to the peripheral hardware. The kernel itself does not interact directly with the user but rather interacts with the shell and other programs as well as with the hard ware devices on the system.

Libraries:

The on top of a Linux kennel there is a set of libraries including open source web browser such as webkit, library libc. These libraries are used to play and record audio and video. The SQLite is a data base which is useful for storage and sharing of application data. The SSL libraries are responsible for internet security etc.

Android Runtime:

The android runtime provides a key component called Dalvik Virtual Machine which is a kind of java virtual machine. It is specially designed and optimized for android. The Dalvik VM is the process virtual machine in the android operating system. It is a software that runs apps on android devices.

The Dalvik VM makes use of Linux core features like memory management and multithreading which is in a java language. The Dalvik VM enables every android application to run it own process. The Dalvik VM executes the files in the .dex format.

Application frame work:

The application frame work layer provides many higher level services to applications such as windows manager, view system, package manager, resource manager etc. The application developers are allowed to make use of these services in their application.

Applications and Features:

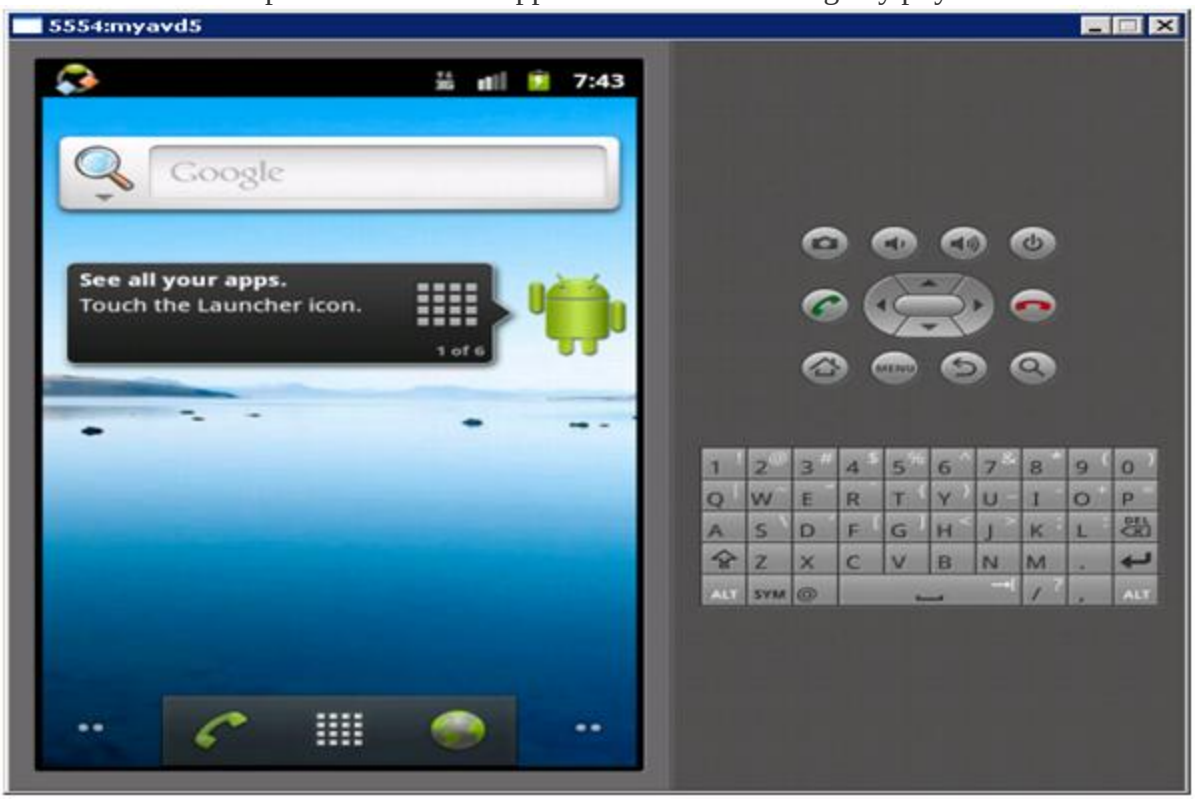
You will find all the android applications at the top layer and you will write your application and install on this layer. Example of such applications are contacts, books, browsers, services etc. Each application perform a different role in the over all applications.

Features:

- Head set layout
- Storage
- Connectivity: GSM/EDGE, IDEN, CDMA, Bluetooth, WI-FI, EDGE,3G,NFC, LTE,GPS.
- Messaging: SMS, MMS, C2DM (could to device messaging), GCM (Google could messaging)
- Multilanguage support
- Multi touch
- Video calling
- Screen capture
- External storage
- Streaming media support
- Optimized graphics

Android Emulator:

The Emulator is a new application in android operating system. The emulator is a new prototype that is used to develop and test android applications without using any physical device.



The android emulator has all of the hardware and software features like mobile device except phone calls. It provides a variety of navigation and control keys. It also provides a screen to display your application. The emulators utilize the android virtual device configurations. Once

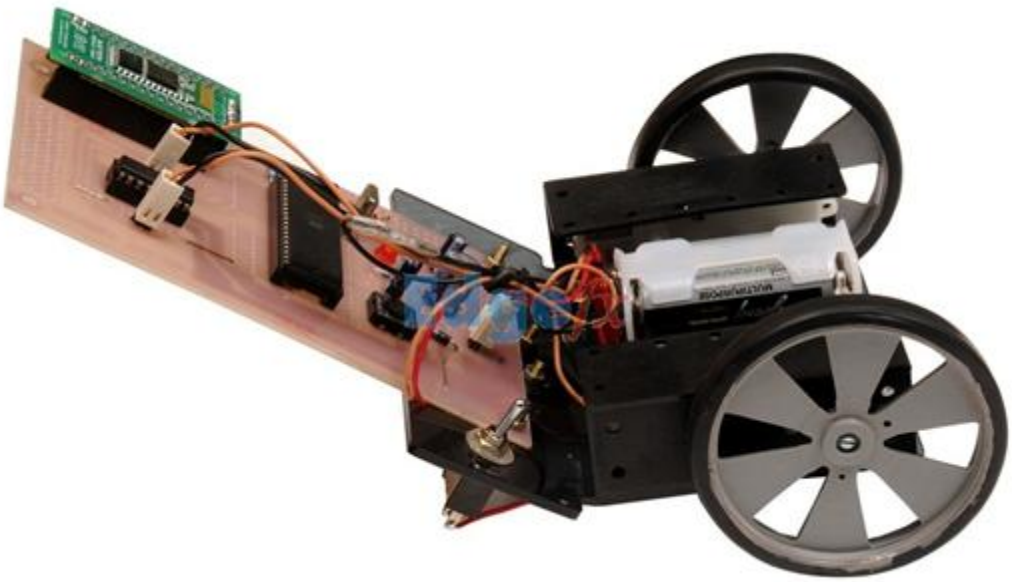
your application is running on it, it can use services of the android platform to help other applications, access the network, play audio, video, store and retrieve the data.

Application of Android- Android Application Controlled Remote Robot

Operation:

It controls the robotic vehicle using an android application. The Bluetooth device is interfaced to control unit on the robot for sensing the signals transmitted by the android application. The remote operation is achieved by any smart-phone or table etc with android OS based on touch screen operation. The transmitting end uses an android application device remote through which commands are transmitted and at the receiver side , these commands are used for controlling the robot in all directions such as forward ,backward and left or right etc.

The receiver end movement is achieved by two motors that are interfaced to the microcontroller. The serial communication data sent from the android application is received by a Bluetooth receiver that is interfaced to the microcontroller.



Advantages:

- Android is Linux based open source operating system , it can be developed by any one
- Easy access to the android apps
- You can replace the battery and mass storage, disk drive and UDB option
- Its supports all Google services
- The operating system is able to inform you of a new SMS and Emails or latest updates.

- It supports Multitasking
- Android phone can also function as a router to share internet
- Its free to customize
- Can install a modified ROM
- Its supports 2D and 3D graphics

On top of Linux kernel there is a set of libraries including open-source Web browser engine WebKit, well known library libc, SQLite database which is a useful repository for storage and sharing of application data, libraries to play and record audio and video, SSL libraries responsible for Internet security etc.

Android Libraries

This category encompasses those Java-based libraries that are specific to Android development. Examples of libraries in this category include the application framework libraries in addition to those that facilitate user interface building, graphics drawing and database access. A summary of some key core Android libraries available to the Android developer is as follows −

- **android.app** − Provides access to the application model and is the cornerstone of all Android applications.
- **android.content** − Facilitates content access, publishing and messaging between applications and application components.
- **android.database** − Used to access data published by content providers and includes SQLite database management classes.
- **android.opengl** − A Java interface to the OpenGL ES 3D graphics rendering API.
- **android.os** − Provides applications with access to standard operating system services including messages, system services and inter-process communication.
- **android.text** − Used to render and manipulate text on a device display.
- **android.view** − The fundamental building blocks of application user interfaces.
- **android.widget** − A rich collection of pre-built user interface components such as buttons, labels, list views, layout managers, radio buttons etc.
- **android.webkit** − A set of classes intended to allow web-browsing capabilities to be built into applications.

Having covered the Java-based core libraries in the Android runtime, it is now time to turn our attention to the C/C++ based libraries contained in this layer of the Android software stack.

Android Runtime

This is the third section of the architecture and available on the second layer from the bottom. This section provides a key component called **Dalvik Virtual Machine** which is a kind of Java Virtual Machine specially designed and optimized for Android.

The Dalvik VM makes use of Linux core features like memory management and multi-threading, which is intrinsic in the Java language. The Dalvik VM enables every Android application to run in its own process, with its own instance of the Dalvik virtual machine.

The Android runtime also provides a set of core libraries which enable Android application developers to write Android applications using standard Java programming language.

Application Framework

The Application Framework layer provides many higher-level services to applications in the form of Java classes. Application developers are allowed to make use of these services in their applications.

The Android framework includes the following key services −

- **Activity Manager** − Controls all aspects of the application lifecycle and activity stack.
- **Content Providers** − Allows applications to publish and share data with other applications.
- **Resource Manager** − Provides access to non-code embedded resources such as strings, color settings and user interface layouts.
- **Notifications Manager** − Allows applications to display alerts and notifications to the user.
- **View System** − An extensible set of views used to create application user interfaces.

Applications

You will find all the Android application at the top layer. You will write your application to be installed on this layer only. Examples of such applications are Contacts Books, Browser, Games etc.

Get the API key

You must have at least one API key associated with your project.

To get an API key:

1. Go to the Google Cloud Platform Console.
2. Click the project drop-down and select or create the project for which you want to add an API key.
3. Click the menu button  and select **APIs & Services > Credentials**.
4. On the **Credentials** page, click **Create credentials > API key**. The **API key created** dialog displays your newly created API key.

5. Click **Close.**
   The new API key is listed on the **Credentials** page under **API keys**. (Remember to restrict the API key before using it in production.)

Add the API key to your request

You must include an API key with every Maps JavaScript API request. In the following example, replace `YOUR_API_KEY` with your API key.

Restrict the API key

We strongly recommend that you restrict your API key. Restrictions provide added security and help ensure only authorized requests are made with your API key. There are two restrictions. You should set both:

- **Application restriction:** Limits usage of the API key to either websites (HTTP referrers), web servers (IP addresses), or mobile apps (Android apps or iOS apps). You can select only one restriction from this category, based on the platform of the API or SDK (see GMP APIs by Platform).

  Note: If you need to call web, web service, and/or mobile APIs from the same (client-side) app, create and restrict multiple keys.
- **API restriction:** Limits usage of the API key to one or more APIs or SDKs. Requests to an API or SDK associated with the API key will be processed. Requests to an API or SDK not associated with the API key will fail. (The API or SDK must be enabled and must support the application restriction.)

To restrict an API key:

1. Go to the Google Cloud Platform Console.
2. Click the project drop-down and select the project that contains the API key you want to secure.
3. Click the menu button ☰ and select **APIs & Services > Credentials**.
4. On the **Credentials** page, click the name of the API key that you want to secure.
5. On the **Restrict and rename API key** page, set the restrictions:

- Application restrictions
- Select **HTTP referrers (web sites)**.
- Add the referrers.

- API restrictions
- Select **Restrict key**.
- Click **Select APIs** and select **Maps JavaScript API**. (If the Maps JavaScript API is not listed, you need to enable it.)
- If your project uses Places Library, also select **Places API**. Similarly, if your project uses other services in the JavaScript API (Directions Service, Distance Matrix Service, Elevation Service, and/or Geocoding Service), you must also enable and select the corresponding API in this list.
- Click **SAVE**.

Geocoding And Reverse Geocoding

20 Dec 2017

Geocoding (converting a physical address or location into latitude/longitude) and reverse geocoding (converting a lat/long to a physical address or location) are common tasks when working with geo-data.

Python offers a number of packages to make the task incredibly easy. In the tutorial below, I use pygeocoder, a wrapper for Google's geo-API, to both geocode and reverse geocode.

Preliminaries

First we want to load the packages we will want to use in the script. Specifically, I am loading pygeocoder for its geo-functionality, pandas for its dataframe structures, and numpy for its missing value (np.nan) functionality.

```
# Load packages
from pygeocoder import Geocoder
import pandas as pd
import numpy as np
```

Create some simulated geo data

Geo-data comes in a wide variety of forms, in this case we have a Python dictionary of five latitude and longitude strings, with each coordinate in a coordinate pair separated by a comma.

```
# Create a dictionary of raw data
data = {'Site 1': '31.336968, -109.560959',
        'Site 2': '31.347745, -108.229963',
        'Site 3': '32.277621, -107.734724',
        'Site 4': '31.655494, -106.420484',
```

```
    'Site 5': '30.295053, -104.014528'}
```

While technically unnecessary, because I originally come from R, I am a big fan of dataframes, so let us turn the dictionary of simulated data into a dataframe.

```
# Convert the dictionary into a pandas dataframe
df = pd.DataFrame.from_dict(data, orient='index')
# View the dataframe
df
```

	0
Site 1	31.336968, -109.560959
Site 2	31.347745, -108.229963
Site 3	32.277621, -107.734724
Site 4	31.655494, -106.420484
Site 5	30.295053, -104.014528

You can see now that we have a a dataframe with five rows, with each now containing a string of latitude and longitude. Before we can work with the data, we'll need to 1) separate the strings into latitude and longitude and 2) convert them into floats. The function below does just that.

```
# Create two lists for the loop results to be placed
lat = []
lon = []


# For each row in a varible,
```

```
for row in df[0]:
    # Try to,
    try:
        # Split the row by comma, convert to float, and append
        # everything before the comma to lat
        lat.append(float(row.split(',')[0]))
        # Split the row by comma, convert to float, and append
        # everything after the comma to lon
        lon.append(float(row.split(',')[1]))
    # But if you get an error
    except:
        # append a missing value to lat
        lat.append(np.NaN)
        # append a missing value to lon
        lon.append(np.NaN)

# Create two new columns from lat and lon
df['latitude'] = lat
df['longitude'] = lon
```

Let's take a took a what we have now.

```
# View the dataframe
df
```

	0	latitude	longitude
Site 1	31.336968, -109.560959	31.336968	-109.560959
Site 2	31.347745, -108.229963	31.347745	-108.229963

	0	latitude	longitude
Site 3	32.277621, -107.734724	32.277621	-107.734724
Site 4	31.655494, -106.420484	31.655494	-106.420484
Site 5	30.295053, -104.014528	30.295053	-104.014528

Awesome. This is exactly what we want to see, one column of floats for latitude and one column of floats for longitude.

Reverse Geocoding

To reverse geocode, we feed a specific latitude and longitude pair, in this case the first row (indexed as '0') into pygeocoder's reverse_geocoder function.

```
# Convert longitude and latitude to a location
results = Geocoder.reverse_geocode(df['latitude'][0], df['longitude'][0])
```

Now we can take can start pulling out the data that we want.

```
# Print the lat/long
results.coordinates
```

(31.3372728, -109.5609559)

```
# Print the city
results.city
```

'Douglas'

```
# Print the country
results.country
```

'United States'

```
# Print the street address (if applicable)
results.street_address
# Print the admin1 level
results.administrative_area_level_1
```

'Arizona'

Geocoding

For geocoding, we need to submit a string containing an address or location (such as a city) into the geocode function. However, not all strings are formatted in a way that Google's geo-API can make sense of them. We can text if an input is valid by using the .geocode().valid_address function.

```
# Verify that an address is valid (i.e. in Google's system)
Geocoder.geocode("4207 N Washington Ave, Douglas, AZ 85607").valid_address
```

True

Because the output was True, we now know that this is a valid address and thus can print the latitude and longitude coordinates.

```
# Print the lat/long
results.coordinates
```

(31.3372728, -109.5609559)

But even more interesting, once the address is processed by the Google geo API, we can parse it and easily separate street numbers, street names, etc.

```
# Find the lat/long of a certain address
result = Geocoder.geocode("7250 South Tucson Boulevard, Tucson, AZ 85756")
# Print the street number
result.street_number
```

'7250'

```
# Print the street name
```

result.route

Reverse geocoding

From Wikipedia, the free encyclopedia

Jump to navigationJump to search

Reverse geocoding is the process of back (reverse) coding of a point location (latitude, longitude) to a readable address or place name. This permits the identification of nearby street addresses, places, and/or areal subdivisions such as neighbourhoods, county, state, or country. Combined with geocoding and routing services, reverse geocoding is a critical component of mobile location-based services and Enhanced 911 to convert a coordinate obtained by GPS to a readable street address which is easier to understand by the end user.

Reverse geocoding can be carried out systematically by services which process a coordinate similarly to the geocoding process. For example, when a GPS coordinate is entered the street address is interpolated from a range assigned to the road segment in a reference dataset that the point is nearest to. If the user provides a coordinate near the midpoint of a segment that starts with address 1 and ends with 100, the returned street address will be somewhere near 50. This approach to reverse geocoding does not return actual addresses, only estimates of what should be there based on the predetermined range. Alternatively, coordinates for reverse geocoding can also be selected on an interactive map, or extracted from static maps by georeferencing them in a GIS with predefined spatial layers to determine the coordinates of a displayed point. Many of the same limitations of geocoding are similar with reverse geocoding.

Public reverse geocoding services are becoming increasingly available through APIs and other web services as well as mobile phone applications.[1] These services require manual input of a coordinate, capture from a localization tool (mostly GPS, but also cell tower signals or WiFi traces[2]), or selection of a point on an interactive map; to look up a street address or neighboring places. Examples of these services include the GeoNames reverse geocoding web service which has tools to identify nearest street address, place names, Wikipedia articles, country, county subdivisions, neighborhoods, and other location data from a coordinate. Google has also published a reverse geocoding API which can be adapted for online reverse geocoding tools, which uses the same street reference layer as Google maps.[3]

Geocoding and reverse geocoding have raised potential privacy concerns, especially regarding the ability to reverse engineer street addresses from published static maps. By digitizing published maps it is possible to georeference them by overlaying with other spatial layers and then extract point locations which can be used to identify individuals or reverse geocoded to obtain a street address of the individual. This has potential implications to determine locations for patients or study participants from maps published in medical literature as well as potentially sensitive information published in other journalistic sources.

In one study a map of Hurricane Katrina mortality locations published in a Baton Rouge, Louisiana, paper was examined. Using GPS locations obtained from houses where fatalities

occurred, the authors were able to determine the relative error between the true house locations and the location determined by georeferencing the published map. The authors found that approximately 45% of the points extracted from the georeferenced map were within 10 meters of a household's GPS obtained point.[4] Another study found similar results in examining hypothetical low and high-resolution patient address maps similar to what might be found published in medical journals. They found approximately 26% of points obtained from a low-resolution map and 79% from a high-resolution map were matched precisely with the true location.[5]

The findings from these studies raise concerns regarding the potential use of georeferencing and reverse geocoding of published maps to elucidate sensitive or private information on mapped individuals. Guidelines for the display and publication of potentially sensitive information are inconsistently applied and no uniform procedure has been identified. The use of blurring algorithms which shift the location of mapped points have been proposed[*by whom?*] as a solution. In addition, where direct reference to the geography of the area mapped is not required, it may be possible to use abstract space on which to display spatial patterns.

SQLite is a opensource SQL database that stores data to a text file on a device. Android comes in with built in SQLite database implementation.

SQLite supports all the relational database features. In order to access this database, you don't need to establish any kind of connections for it like JDBC,ODBC e.t.c

Database - Package

The main package is android.database.sqlite that contains the classes to manage your own databases

Database - Creation

In order to create a database you just need to call this method openOrCreateDatabase with your database name and mode as a parameter. It returns an instance of SQLite database which you have to receive in your own object.Its syntax is given below

SQLiteDatabase mydatabase = openOrCreateDatabase("your database name",MODE_PRIVATE,null);

Apart from this , there are other functions available in the database package , that does this job. They are listed below

Sr.No	Method & Description

1	**openDatabase(String path, SQLiteDatabase.CursorFactory factory, int flags, DatabaseErrorHandler errorHandler)** This method only opens the existing database with the appropriate flag mode. The common flags mode could be OPEN_READWRITE OPEN_READONLY
2	**openDatabase(String path, SQLiteDatabase.CursorFactory factory, int flags)** It is similar to the above method as it also opens the existing database but it does not define any handler to handle the errors of databases
3	**openOrCreateDatabase(String path, SQLiteDatabase.CursorFactory factory)** It not only opens but create the database if it not exists. This method is equivalent to openDatabase method.
4	**openOrCreateDatabase(File file, SQLiteDatabase.CursorFactory factory)** This method is similar to above method but it takes the File object as a path rather then a string. It is equivalent to file.getPath()

Database - Insertion

we can create table or insert data into table using execSQL method defined in SQLiteDatabase class. Its syntax is given below

```
mydatabase.execSQL("CREATE TABLE IF NOT EXISTS TutorialsPoint(Username VARCHAR,Password VARCHAR);");
mydatabase.execSQL("INSERT INTO TutorialsPoint VALUES('admin','admin');");
```

This will insert some values into our table in our database. Another method that also does the same job but take some additional parameter is given below

Sr.No	Method & Description
1	**execSQL(String sql, Object[] bindArgs)** This method not only insert data , but also used to update or modify already existing data in database using bind arguments

Database - Fetching

We can retrieve anything from database using an object of the Cursor class. We will call a method of this class called rawQuery and it will return a resultset with the cursor pointing to the table. We can move the cursor forward and retrieve the data.

```
Cursor resultSet = mydatbase.rawQuery("Select * from TutorialsPoint",null);
resultSet.moveToFirst();
String username = resultSet.getString(0);
String password = resultSet.getString(1);
```

There are other functions available in the Cursor class that allows us to effectively retrieve the data. That includes

Sr.No	Method & Description
1	**getColumnCount()** This method return the total number of columns of the table.
2	**getColumnIndex(String columnName)** This method returns the index number of a column by specifying the name of the column
3	**getColumnName(int columnIndex)** This method returns the name of the column by specifying the index of the column
4	**getColumnNames()** This method returns the array of all the column names of the table.
5	**getCount()** This method returns the total number of rows in the cursor
6	**getPosition()** This method returns the current position of the cursor in the table
7	**isClosed()**

	This method returns true if the cursor is closed and return false otherwise

Database - Helper class

For managing all the operations related to the database , an helper class has been given and is called SQLiteOpenHelper. It automatically manages the creation and update of the database. Its syntax is given below

```
public class DBHelper extends SQLiteOpenHelper {
  public DBHelper(){
    super(context,DATABASE_NAME,null,1);
  }
  public void onCreate(SQLiteDatabase db) {}
  public void onUpgrade(SQLiteDatabase database, int oldVersion, int newVersion) {}
}
```

Example

Here is an example demonstrating the use of SQLite Database. It creates a basic contacts applications that allows insertion, deletion and modification of contacts.

To experiment with this example, you need to run this on an actual device on which camera is supported.

Steps	Description
1	You will use Android studio to create an Android application under a package com.example.sairamkrishna.myapplication.
2	Modify src/MainActivity.java file to get references of all the XML components and populate the contacts on listView.
3	Create new src/DBHelper.java that will manage the database work
4	Create a new Activity as DisplayContact.java that will display the contact on the screen
5	Modify the res/layout/activity_main to add respective XML components

6	Modify the res/layout/activity_display_contact.xml to add respective XML components
7	Modify the res/values/string.xml to add necessary string components
8	Modify the res/menu/display_contact.xml to add necessary menu components
9	Create a new menu as res/menu/mainmenu.xml to add the insert contact option
10	Run the application and choose a running android device and install the application on it and verify the results.

android.database.sqlite

Kotlin | **Java**

Contains the SQLite database management classes that an application would use to manage its own private database.

Applications use these classes to manage private databases. If creating a content provider, you will probably have to use these classes to create and manage your own database to store content. See Content Providers to learn the conventions for implementing a content provider. If you are working with data sent to you by a provider, you do not use these SQLite classes, but instead use the generic android.database classes.

The Android SDK and Android emulators both include the sqlite3 command-line database tool. On your development machine, run the tool from the platform-tools/ folder of your SDK. On the emulator, run the tool with adb shell, for example, adb -e shell sqlite3.

The version of SQLite depends on the version of Android. See the following table:

Android API	SQLite Version
API 27	3.19
API 26	3.18

API 24	3.9
API 21	3.8
API 11	3.7
API 8	3.6
API 3	3.5
API 1	3.4

Some device manufacturers include different versions of SQLite on their devices. There are two ways to programmatically determine the version number.

- If available, use the sqlite3 tool, for example: `adb -e shell sqlite3 --version`.
- Create and query an in-memory database as shown in the following code sample:

```
String query = "select sqlite_version() AS sqlite_version";
SQLiteDatabase db = SQLiteDatabase.openOrCreateDatabase(":memory:", null);
Cursor cursor = db.rawQuery(query, null);
String sqliteVersion = "";
if (cursor.moveToNext()) {
    sqliteVersion = cursor.getString(0);
}
```

Interfaces

SQLiteCursorDriver	A driver for SQLiteCursors that is used to create them and gets notified by the cursors it creates on significant events in their lifetimes.
SQLiteDatabase.CursorFactory	Used to allow returning sub-classes of Cursor when calling query.
SQLiteTransactionListener	A listener for transaction events.

Classes

SQLiteClosable	An object created from a SQLiteDatabase that can be closed.
SQLiteCursor	A Cursor implementation that exposes results from a query on a SQLiteDatabase.
SQLiteDatabase	Exposes methods to manage a SQLite database.
SQLiteDatabase.OpenParams	Wrapper for configuration parameters that are used for opening SQLiteDatabase
SQLiteDatabase.OpenParams.Builder	Builder for OpenParams.
SQLiteOpenHelper	A helper class to manage database creation and version management.
SQLiteProgram	A base class for compiled SQLite programs.
SQLiteQuery	Represents a query that reads the resulting rows into a SQLiteQuery.
SQLiteQueryBuilder	This is a convenience class that helps build SQL queries to be sent to SQLiteDatabase objects.
SQLiteStatement	Represents a statement that can be executed against a database.

Exceptions

SQLiteAbortException	An exception that indicates that the SQLite program was aborted.
SQLiteAccessPermException	This exception class is used when sqlite can't access the database file due to lack of permissions on the file.

SQLiteBindOrColumnIndexOutOfRangeException	Thrown if the the bind or column parameter index is out of range
SQLiteBlobTooBigException	
SQLiteCantOpenDatabaseException	
SQLiteConstraintException	An exception that indicates that an integrity constraint was violated.
SQLiteDatabaseCorruptException	An exception that indicates that the SQLite database file is corrupt.
SQLiteDatabaseLockedException	Thrown if the database engine was unable to acquire the database locks it needs to do its job.
SQLiteDatatypeMismatchException	
SQLiteDiskIOException	An exception that indicates that an IO error occured while accessing the SQLite database file.
SQLiteDoneException	An exception that indicates that the SQLite program is done.
SQLiteException	A SQLite exception that indicates there was an error with SQL parsing or execution.
SQLiteFullException	An exception that indicates that the SQLite database is full.
SQLiteMisuseException	This error can occur if the application creates a SQLiteStatement object and allows multiple threads in the application use it at the same

	time.
SQLiteOutOfMemoryException	
SQLiteReadOnlyDatabaseException	
SQLiteTableLockedException	