Unit 4. IOT Systems and Networks

What this unit is about

What this unit is about

This unit is giving information about IOT Sensors and Wireless Networks

What you should be able to do

After completing this unit, you should be able to:

- Understand IoT Sensors
- IoT Network Devices

How you will check your progress

- Checkpoint

References

- Radio Frequency Energy Harvesting and Management for Wireless Sensor Networks - Adamu Murtala Zungeru, Li-Minn Ang, SRS. Prabaharan, Kah Phooi Seng
- A Wireless Sensing Platform Utilizing Ambient RF Energy - Aaron N. Parks, Alanson P. Sample, Yi Zhao, Joshua R. Smith

Unit objectives

IBM ICE (Innovation Centre for Education)

After completing this unit, You should be able to

- Understand IoT Sensors
- IoT Network Devices

Figure 4-1. Unit objectives

IOT011.0

Notes:

IBM

IBM ICE (Innovation Centre for Education)

Topics

- Study of RF Wireless Sensors
  - What is a sensor
  - Different type of sensors
- Wireless Networks
  - Wireless Sensor Networks
  - Different Types of Wireless networks Technology
    - Zigbee
    - Wi-Fi
    - Satellite Communications
  - Energy Harvesting RF Networks
- Computer Connected to Internet
- Network devices
  - Hubs
  - Switches
  - Routers
  - Gateways
  - Firewalls
- Device Configuration and Management
- Exchange Information in real time without human intervention

Figure 4-2. Topics

IOT011.0

Notes:

Study of RF Wireless Sensors (1 of 23)

IBM ICE (Innovation Centre for Education)

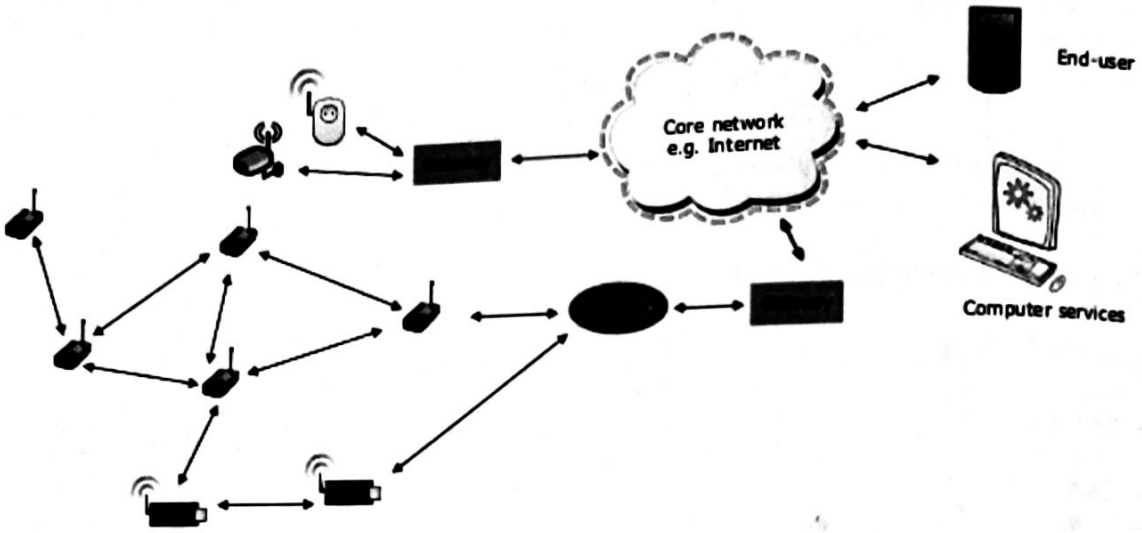


Figure 4-3. Study of RF Wireless Sensors (1 of 23) IOT011.0

Notes:

Device that detects (senses) the changes in ambient conditions or in the state of another device or a system, and conveys or records this information in a certain manner. The specific input could be light, heat, motion, moisture, pressure, or any one of the great number of other environmental phenomena. The output is generally a signal that is converted to the human-readable display at the sensor location or can also be transmitted electronically over a network for reading or further processing.

Wireless sensor network refers to the group of spatially dispersed and dedicated sensor for monitoring and also recording the physical conditions of environment and organizing the collected data at a central location. Wireless Sensor Networks measures environmental conditions like temperature, sound, pollution levels, humidity, wind speed and direction, pressure, etc. Wireless Sensors Networks were initially designed to facilitate military operations but its application has been extended to the health, traffic, and many other consumer and the industrial areas. A WSN consists anywhere from a few hundreds to the thousands of the sensor nodes. The sensor nodes equipment includes a radio transceiver along with the antenna, also a micro controller, an interfacing electronic circuit, and an energy source like battery. A non-rechargeable battery (e.g., alkaline) is also suitable for the micro sensor with very low power consumption (e.g., 50 µW). Alternatively, a rechargeable battery (e.g., lithium ion) is been used widely in sensor nodes with energy harvesting technology.

Study of RF Wireless Sensors (2 of 23)

IBM

IBM ICE (Innovation Centre for Education)

- Available "On Demand"
- Works in perpetually dark locations
- Works in hazardous locations
- Provides mobility
- Provides tracking capability
- Can take advantage of electricity tariffs
- Can charge a secondary battery
- Scalable to many nodes without a change to source
- Can be embedded between walls
- Sealable within an enclosure

IOT011.0

Figure 4-4. Study of RF Wireless Sensors (2 of 23)

need of a battery limits the app space and increases the initial and recurring costs

Notes:

In practical wireless sensor usage, the need of a battery limits the application space and increases the initial and recurring costs, making the traditional wired sensors more appealing in some cases. RF (Radio Frequency) energy harvesting offers a unique solution to this practical problem and that facilitates the implementation of a battery and the super capacitor-free wireless sensing node with 24-hour operation. Most commonly used wireless sensor nodes to consume few µW in sleep mode and hundreds µW in active mode.

The main advantage of RF harvesting is that it is available all hours of the day and night. A solar harvesting node which needed to be operated during the night, it must include a large charge storage device, such as a battery or super capacitor, to deal with the blackout period in which its energy source is not yet available. The RF harvesting node typically need not deal with such blackout period, and therefore does not need to store as much energy. When requirement for the on-board energy storage decreases, and a smaller (longer-lived, more efficient, and less expensive) storage device may be used. A modern RFID tag, which also consists of an RF-powered communication IC and a low-cost printed antenna, has been demonstrated as a good potential form factor for the RF energy harvesting sensor node which doesn't require significant charge storage.

Study of RF Wireless Sensors (3 of 23)

IBM

IBM ICE (Innovation Centre for Education)

RF powered sensor node architecture

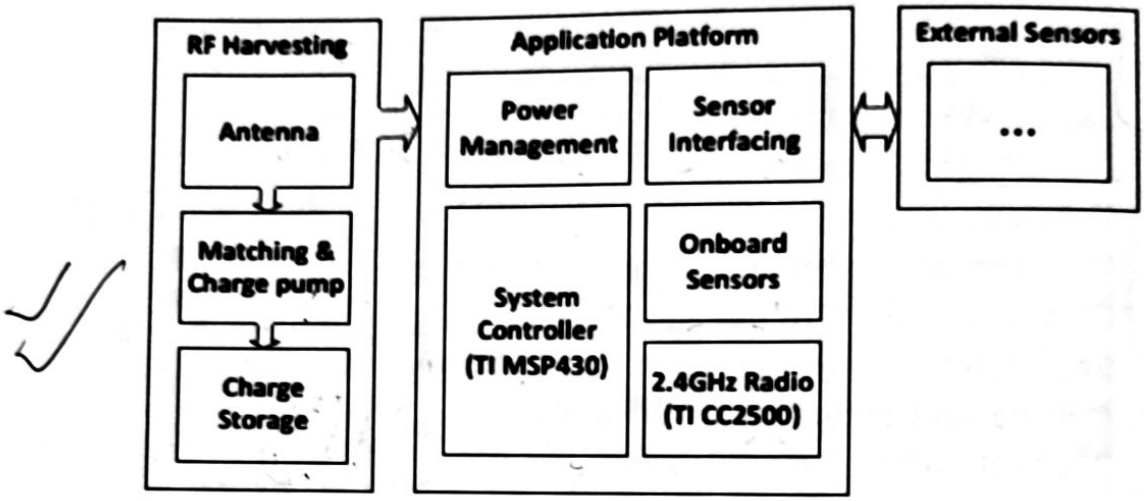


Figure 4-5. Study of RF Wireless Sensors (3 of 23)

IOT011.0

Notes:

Wi-Fi transceivers, cellular base stations, AM/FM radio transmitters, and a TV broadcast transmitters are all the ambient RF energy sources, by varying ubiquity and power output. Radio wave, are the part of an electromagnetic spectrum consists of magnetic and electrical component. The radio waves carry information by varying the combination of the amplitude, frequency and phase of the wave within a frequency band. On contact with the conductor such as an antenna, the Electromagnetic (EM) radiation induces an electrical current on the conductor's surface, which is known as the skin effect. The communication devices also uses antenna for the transmission and/or reception of data by utilizing the different frequencies of spectrum from 10Kz to 30Kz. The maximum theoretical power is also available for the RF energy harvesting is 7.0μW and 1.0μW for 2.4GHz and 900MHz frequency is respectively been used to free space distance of 40 meters. Figure above shows the architecture of sensor node. The first section includes an antenna, harvesting circuit, and the charge storage. The second is an application platform which also does useful work for sensing and transmitting data, and which also includes power management functionality and the simple physical sensors. External sensors may also be interfaced with the systems. The system is a duty-cycled which reduces the average power requirements. The majority of the time is spent in a charging state, waiting for a specified charge to accumulate on the storage capacitor. When this charge is been collected, the system switches to an active state and then performs the one is Sense ? Process ? Transmit operation. The cycling period is therefore been determined by the amount of power available.

Study of RF Wireless Sensors (4 of 23)

IBM

IBM ICE (Innovation Centre for Education)

Different Type of Sensors

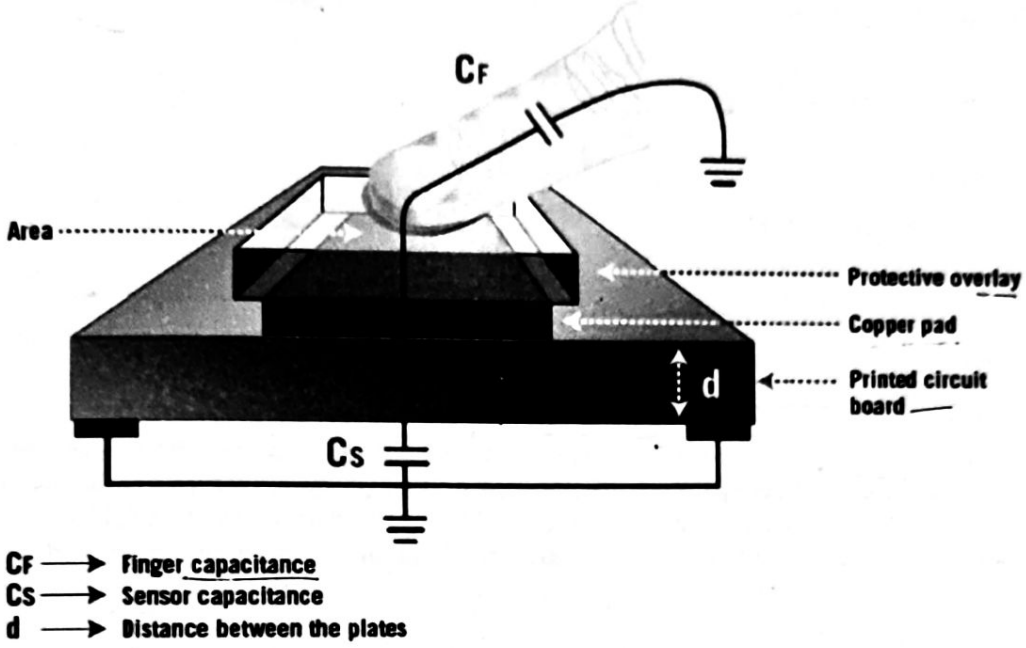


Figure 4-6. Study of RF Wireless Sensors (4 of 23)

IOT011.0

Notes:

There are number of sensors are available and some of them are mentioned below;

- Capacitive sensors
- Current sensors
- Gas and Chemical sensors
- Hall effect sensors
- Humidity sensors
- Inductive sensors
- Optical sensors
- Pressure based sensors
- Temperature sensors
- Ultrasonic based sensors
- Below are the details of each sensor.

Capacitive sensors:

The sensor in a capacitive sensing system is a type of conductor allowing for the low cost and highly flexible system design and capacitive sensing with ground capacitors is a high resolution, low cost, the contact less sensing technique that can be applied to a number of and variety of applications.

As discussed earlier the sensor in a capacitive sensing system is of any metal or conductor, this capacitive sensing is differs from capacitive touch in that it provides a higher resolutions to allow for the further sensing distance and higher-performance in sensing applications, including gesture, liquid level, proximity and material properties.

Following are the applications of the capacitive sensors:

- proximity sensor
- Gesture recognition
- Automotive door and kick sensors
- Automotive rain sensors
- Remote and direct liquid level sensors
- Material size detection

The example for the capacitive sensing system is FDC1004.

The FDC1004 is a 4-channel capacitance-to-digital converter is designed for capacitive sensing applications. Its features are more compared to 16-bit those are effective noise-free resolution and provides compensation up to 100 pF offset capacitance to accommodate the use of the remote sensors. The FDC1004 also includes the two strong drivers for the sensor shields to allow focusing on sensing direction and to reduce EMI interference.

Study of RF Wireless Sensors (5 of 23)

IBM

IBM ICE (Innovation Centre for Education)

Capacitive Sensors

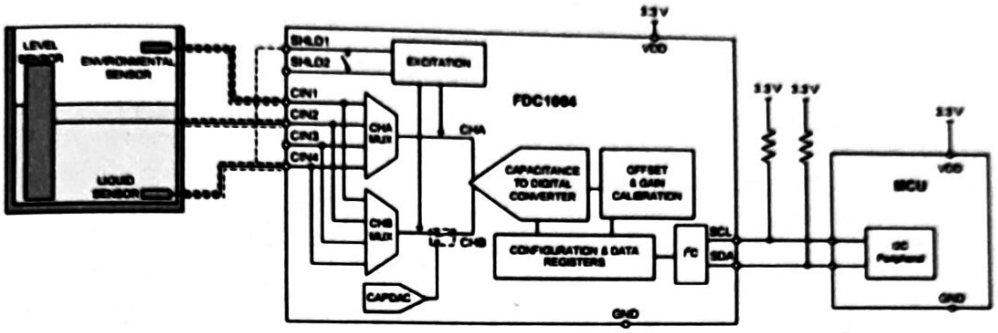


Figure 4-7. Study of RF Wireless Sensors (5 of 23)

IOT011.0

Notes:

Here one of the capacitive sensing application liquid level sensors is explained.

Liquid level sensor:

The FDC1004 can be used to measure the liquid level in a non-conductive containers. Capacitive sensors can be attached to the outside of the container or to be located remotely from the container, allowing for a contact less measurements. The working principle is based on a ratio metric measurement. Figure above shows a possible system implementation which uses three electrodes. The Leveled electrode provides a capacitance value that is proportional to the liquid level. And the Reference Environmental electrode and the Reference of Liquid electrode are used as the references. The Reference Liquid electrode accounts for liquid dielectric constant and its variations while the Reference Environmental electrode is also used to compensate for any other environmental variations are not due to liquid itself. Note that a Reference Environmental electrode and Reference Liquid electrode are of same physical size. For this application, single-ended measurements which are on the appropriate channels are appropriate, as tank is grounded. Use the following formulas to determine the liquid level from measured capacitances:

Where,

- C_{RE} is the capacitance of the Reference Environmental electrode.
- C_{RL} is the capacitance of the Reference Liquid electrode.
- C_{Lev} is the current value of the capacitance is measured at the Level electrode sensor.

- $C_{Lev(0)}$ is the capacitance of the Level electrode when the container is empty.
- h_{REF} is the height in the desired units of a Container or Liquid Reference electrodes.

The ratio between capacitance of the level and reference electrodes allows a simple calculation of the liquid level inside a container itself. Very high sensitivity values (that is, many LSB/mm) that can be obtained due to high resolution of the FDC1004, and even when the sensors are located remotely from the container.

Design requirements of the liquid level monitor is given below.

The liquid level measurement must be independent of liquid, which can be achieved using the 3-electrode design is described above. Moreover, the sensor should be immune to the environmental interferers such as a human body, other objects, or EMI. This can also be achieved by shielding side of the sensor which does not face the container.

Procedure for design:

In capacitive sensing systems, the design of sensor plays an important role for determining the system performance and capabilities. In most of the cases sensor is simply the metal plate that can be designed on the PCB. The sensor used in this example is also implemented with the two-layer PCB. On the top layer, which faces the tank, there are 3 electrodes of (Reference Environmental, Reference Liquid, and Level) with the ground plane surrounding the electrodes. The bottom layer is been covered with a shield plane in order to isolate electrodes from any of the external interference sources. Depending on the shape of a container, the FDC1004 can be located on a sensor PCB to minimize the length of traces between the input channels and the sensors which increase the immunity from EMI sources. In case the shape of the container or the other mechanical constraints which do not allow having the sensors and the FDC1004 on the same PCB, traces which connect the channels to the sensor and are need to be shielded with the appropriate shield. In this design the example all of the channels are shielded with SHLD1. For this type of configuration, the FDC1004 measures a capacitance of the 3 channels versus ground; so the SHLD1 and SHLD2 pins are been internally shorted in the FDC1004.

Study of RF Wireless Sensors (6 of 23)

Current Sensors

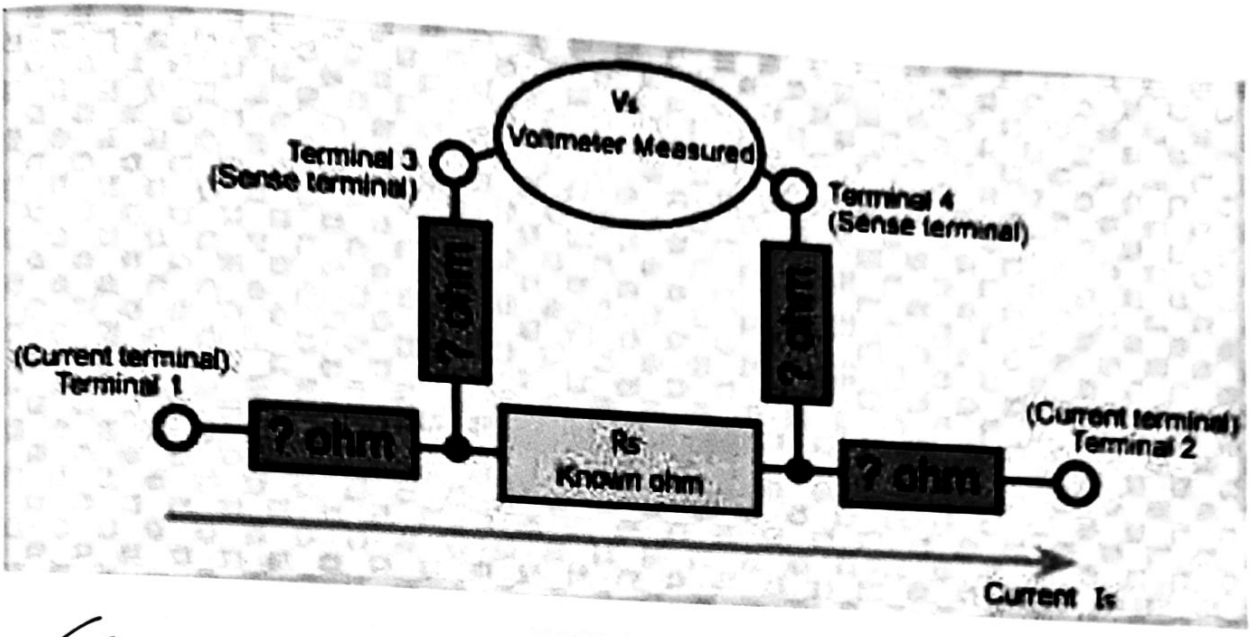


Figure 4-8. Study of RF Wireless Sensors (6 of 23)

Notes:

Current sensors offer a unique input stage topology which allows the common mode voltage to exceed the supply voltage. The Integrated precision gain resistors enable the very accurate measurements. Current shunt monitors, or the current sense amplifiers, are designed to monitor current flow in a load by measuring the voltage drop across a resistor.

Current shunt amplifiers enabled the lower cost method of current measurement than indirect methods of sensing. Current sense amplifiers enable a wide range of applications including power supply monitoring, motor/valve control, and a battery management. They are recommended for currents under 100A and voltages under 100V.

Different ICs are available in the current sensor examples are IN282, INA226 and INA300.

A **current sensor** is a device that detects the electric current (AC or DC) in a wire, and generates a signal proportional to it. The generated signal can also be analog voltage or current or even digital output. It can be then utilized to display the measured current in an ammeter or even it can be stored for further analysis in a data acquisition system or can be utilized for the control purpose.

The sensed current and the output signal can be:

Alternating current input,

- analog output, which duplicates the wave shape of a sensed current

- bipolar output, which duplicates the wave shape of a sensed current
- unipolar output, which is also proportional to the average or RMS value of the sensed current

Direct current input,

- unipolar, with an unipolar output, which also duplicates the wave shape of the sensed current
- digital output, which switches when the sensed current exceeds a certain threshold

Study of RF Wireless Sensors (7 of 23)

IBM

IBM ICE (Innovation Centre for Education)

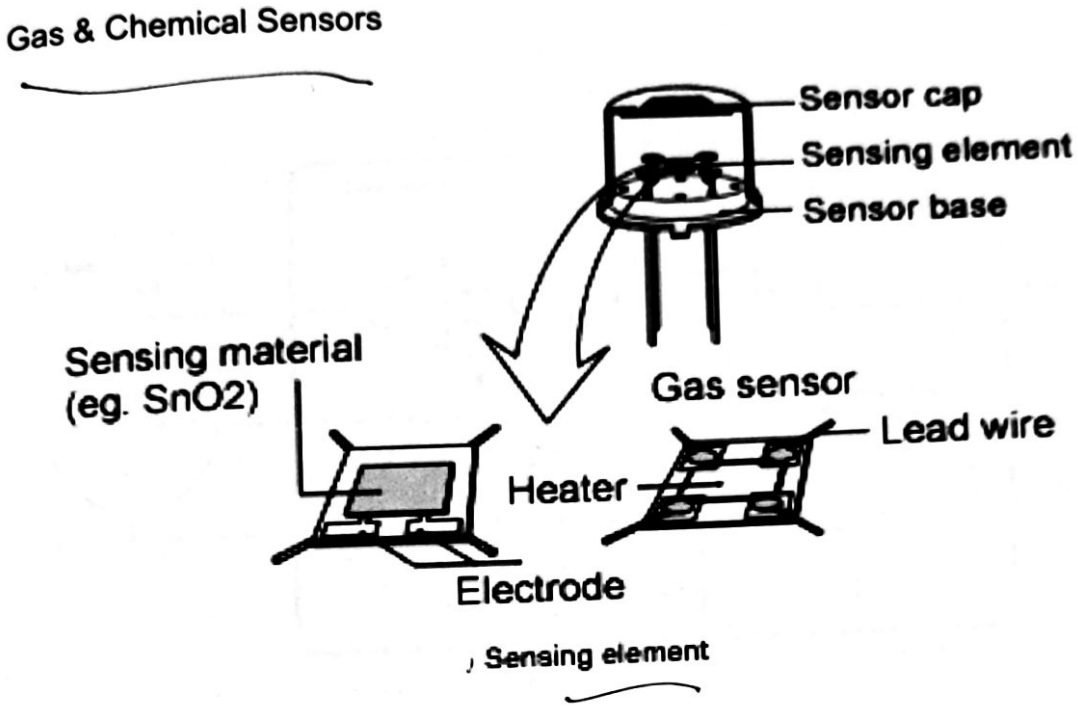


Figure 4-9. Study of RF Wireless Sensors (7 of 23)

Notes:

Gas sensor is a subclass of chemical sensor and it measures the concentration of gas in its vicinity. It interacts with gas to measure its concentration. Each gas has its own breakdown voltage that is the electric field at which it ionized. Sensor identifies gases by measuring these voltages. By measuring the current discharge in the device the concentration of the gas can be determined.

- Applications of GAS Sensors:
- Boiler Control
- Environmental Monitoring
- Fire Detection
- Alcohol Breath Tests
- Process Control Industries
- Home Safety
- Grading of agro-products like coffee and spices
- Harmful gases detection in mines.

Two common technologies to detect gas are electrochemical cells and NDIR sensors. Electrochemical sensors create the potential and measure the current across a cell that responds to the specific gas type. Non

dispersive infrared sensors use infrared light to determine the amount of a specific gas in a container.PH sensing is used to monitor the water quality by measuring the concentration of hydrogen ions in a solution.

Examples of gas sensors: LMP91000, LMP91050, DLP4500NIR etc..,

Study of RF Wireless Sensors (8 of 23)

Working Principle

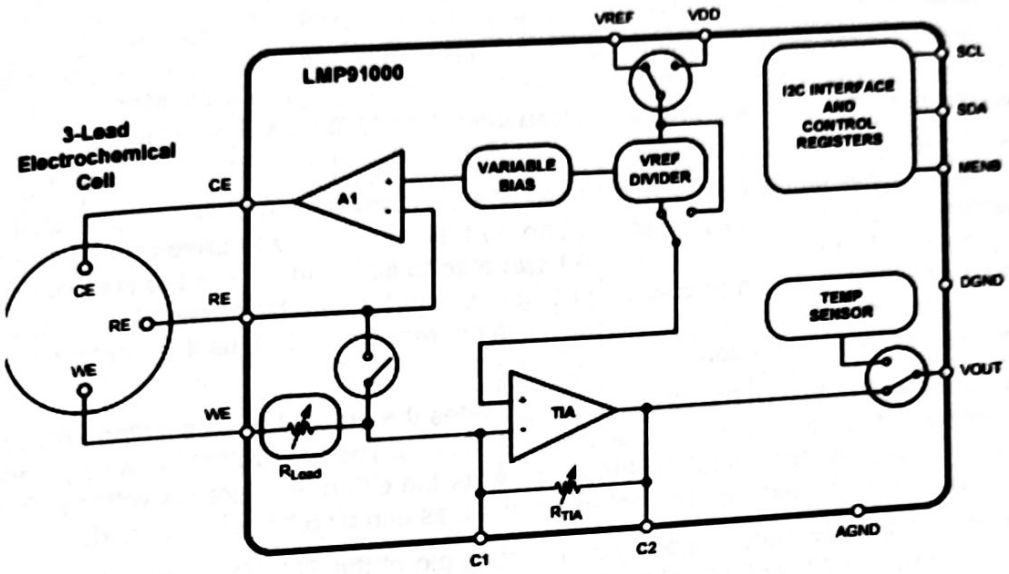


Figure 4-10. Study of RF Wireless Sensors (8 of 23)

Notes:

The LMP91000 is a programmable of analog front-end (AFE) for use in the micro-power electrochemical sensing applications. It provides the complete signal path solution between a sensor and a micro controller that generates an output voltage proportional to a cell current. The LMP91000's programmability enables it to support the multiple electrochemical sensors such as the 3-lead toxic gas sensors and 2-lead galvanic cell sensors with the single design as opposed to the multiple discrete solutions. The LMP91000 also supports gas sensitivities over the range from 0.5nA/ppm to 9500nA/ppm. It also allows for an easy conversion of the current ranges from 5 µA to 750 µA full scale. Transimpedance gain is user programmable through an I2C compatible interface and from 2.75kΩ to 350kΩ making it easy to convert the current ranges from 5 µA to 750 µA full scale. It Optimize for the micro-power applications, the LMP91000 AFE works over the voltage range from 2.7 V to 5.25 V. A temperature sensor is embedded and it also can be power cycled through interface. The output of this temperature sensor can also be read by the user through a VOUT pin. Depending upon the configuration, total current consumption for the device can also be less than 10 µA. And for power savings, the transimpedance amplifier can also be turned off and instead a load impedance is equivalent to the TIA's input impedance is switched in.

Applications of this sensor is

1. Chemical species identification
2. Amperometric Applications
3. Electrochemical Blood Glucose Meter

Functional Blocks:

Potentiostat Circuitry: The core of a LMP91000 is the potentiostat circuit. It consists of a differential input amplifier is used to compare the potential between working and reference electrodes are required to working bias potential (is to be set by the Variable Bias circuitry). The error signal is been amplified and applied to the counter electrode (through a Control Amplifier - A1). Any changes in impedance between the working and reference electrodes which will cause a change in the voltage applied to the counter electrode, in order to maintain a constant voltage between the working and the reference electrodes. A Transimpedance Amplifier is connected to the working electrode, is used to provide an output voltage which is proportional to the cell current. The working electrode is held at a virtual ground (Internal ground) through the transimpedance amplifier. The potentiostat will compare the reference voltage with the desired bias potential and adjusts the voltage at the counter electrode to maintain proper working-to-reference voltage.

Transimpedance Amplifier: The Transimpedance amplifier (TIA) has the 7 programmable internal gain resistors. This accommodates that the full scale ranges is of most existing sensors. Moreover the external gain resistor can be connected to the LMP91000 between the C1 and C2 pins. The gain is been set through the I2C interface.

Control Amplifier: The control amplifier (A1 op amp) has two tasks they are: a) providing the initial charge to the sensor. b) Providing a bias voltage to the sensor. The A1 has a capability to drive up to a 10mA into the sensor in order to provide a fast initial conditioning. A1 can able to sink and source the current according to the connected gas sensor (it is reducing or oxidizing the gas sensor). It can be powered down to reduce the system power consumption. And however power down A1 is not recommended, as it might take long time for the sensor to get recover from this situation.

Variable Bias: The Variable Bias blocks the circuitry and provides the amount of bias voltage required by the biased gas sensor between its reference and the working electrodes. The bias voltage can be programmed to be from 1% to 24% (there are 14 steps in total) of the supply, for the external reference voltage. The 14 steps can be programmed through I2C interface. The polarity of the bias can also be programmed.

Internal Zero: The internal Zero is the voltage at non-inverting pin of the TIA. The internal zero can also be programmed to be either 67%, 50% or 20%, of the supply, or by the external reference voltage. This provides both the sufficient headroom for a counter electrode of the sensor to swing, in case of the sudden changes in the gas concentration, and best use of ADC's full scale input range. The Internal zero is also provided through an internal voltage divider. And the divider is also programmed through the I2C interface.

Study of RF Wireless Sensors (9 of 23)

IBM

IBM ICE (Innovation Centre for Education)

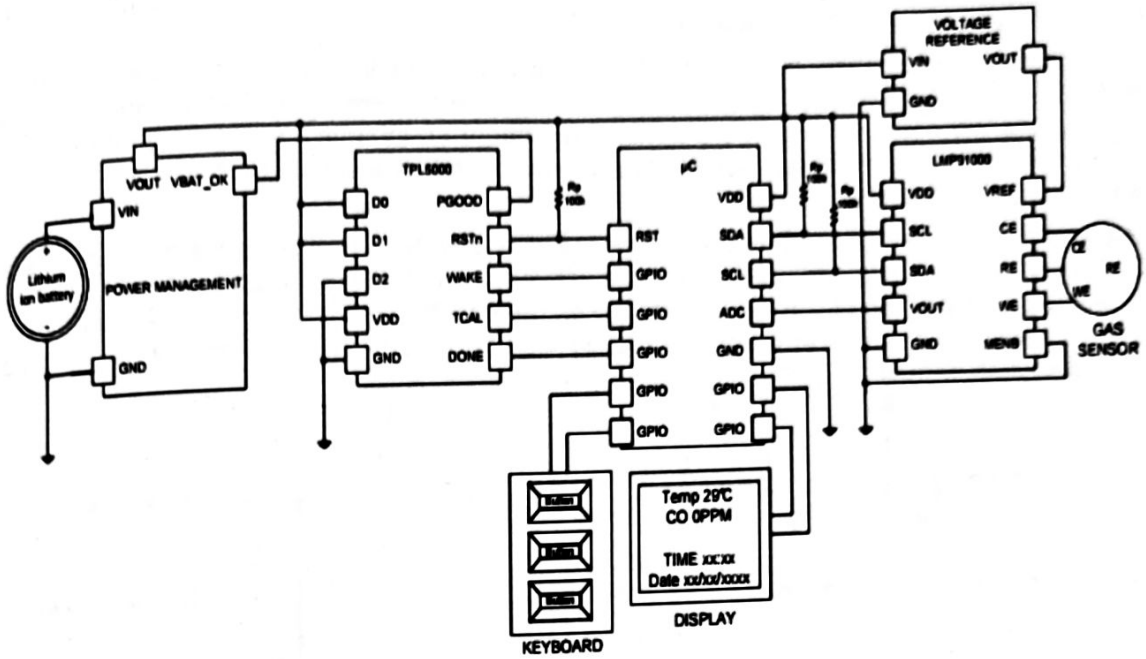


Figure 4-11. Study of RF Wireless Sensors (9 of 23)

Notes:

Temperature Sensor: An embedded temperature sensor can also be switched off during the gas concentration measurement to save power. The temperature measurement is to be triggered through I2C interface. The temperature output is also available at the VOUT pin till the configuration bit is reset. The output signal of temperature sensor is a voltage, referred to the ground of the LMP91000 (AGND)

Application and Implementation of the LMP 91000: The LMP91000 can be used in conjunction with the environment sensors to build a battery power environment monitors such as an air quality data-loggers, or wireless sensors. In this application due to monitored phenomena the micro-controller and a LMP9100 spend most of the time in idle state. In order to save the power and enlarge the battery life, the LMP91000 can also be put into deep sleep mode with Internal FET feature enabled. To optimize a current consumption of entire system, the acquisitions and in general the activities of the micro can be operated at set intervals with the TPL5000. The TPL5000 is the programmable timer with the watch-dog feature.

Design Requirements: The Design is driven by the low-current consumption constraint. The data are usually acquired on a rate which ranges between 1s to 10s. The highest necessity is the maximization of a battery life. The TPL5000 helps achieving that goal by which it allows putting the micro-controller in its lowest power mode. Moreover the deep sleep mode of the LMP91000 allows burning only some hundreds of nA.

Detailed Design Procedure: When the focal constraint is a battery, the selection of a low power voltage reference, the micro-controller and display is mandatory. The first step in a design is the calculation of power consumption of each device in the different mode of operations. An example is LMP91000; the device has the gas measurement mode, sleep mode and micro-controller in low power mode which is of normal operation.

The different types of modes offer the possibility to select the appropriate timer interval which respects the application constraint and maximizes the life of the battery.

Sensor Test Procedure: The LMP91000 has all hardware and programmability features to implement some test procedures. And the purpose of the test procedure is to:

- To test proper function of the sensor (status of health)
- To test proper connection of the sensor to LMP91000

The test procedure is very easy. And the variable bias block is a user programmable through a digital interface. A step voltage can be applied by the end of user to the positive input of A1. As the consequence of a transient current will starts flowing into a sensor (to charge its internal capacitance) and it will also be detected by the TIA. If the current transient is not yet detected, either a sensor fault or a connection problem is present.

The slope and the aspects of the transient response can also be used to detect the sensor aging (for example, if a cell that is drying and no longer it can efficiently conduct the current). After it is verified that a sensor is working properly, the LMP91000 needed to be reset to its original configuration. It is not required to observe a full transient in order to contain a testing time. All the needed information is included in the transient slopes (both edges).

Study of RF Wireless Sensors (10 of 23)

IBM

IBM ICE (Innovation Centre for Education)

Hall Effect Sensors

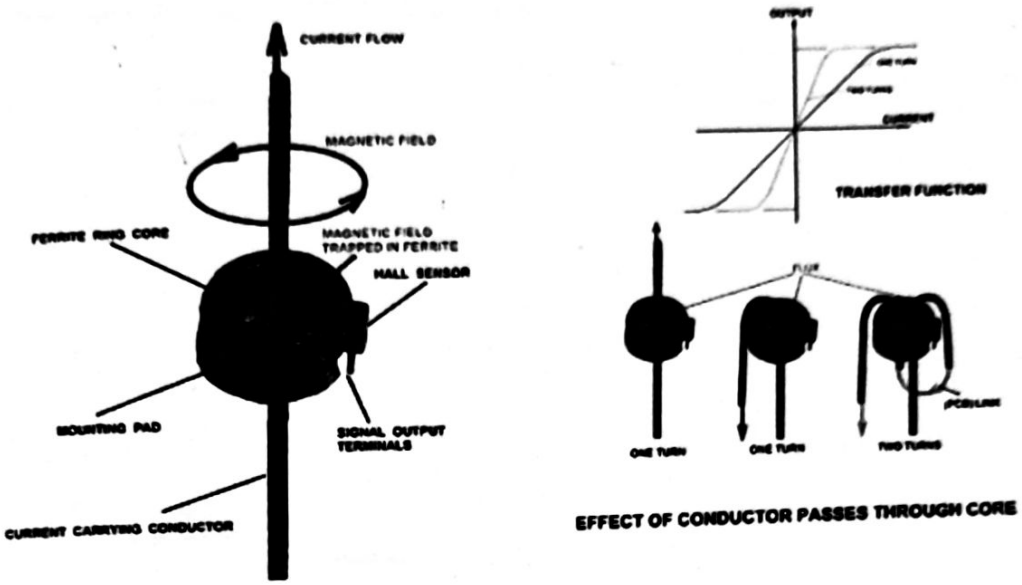


Figure 4-12. Study of RF Wireless Sensors (10 of 23)

Notes:

These sensors are used for detecting the position, acceleration or speed of an object by sensing the magnetic field which is generated by the object. Hall effect is a sensing technology that detects the presence and strength of the magnetic field. Hall Effect sensors can also measure the strength of the magnetic field as the indicator of distance or position without physical contact. These sensors are based on the theory of Hall Effect which is the production of a voltage difference (the Hall voltage) across an electrical conductor, which transverse to an electric current in a conductor and the magnetic field is perpendicular to the current.

There are two types of Hall Effect sensors are available in the market. They are;

- Analog Hall Effect Sensors
- Digital Hall Effect Sensors.

Advantages of the Hall Effect Sensors:

1. Solid state devices include signal conditioning and the protection logic.
2. Magnetic sensing is the highly repeatable operation (no mechanical wear or tear).
3. Contact is also not required for the operation.
4. Hall effect sensors are the immune to dust, dirt, air and RF noise.
5. Hall effect sensors are invariable over the wide temp range.

6. The devices are the pin-to-pin compatible and low cost (only 3 pins).

Example of Hall Effect Sensor:-

The DRV5013 device is the chopper-stabilized Hall Effect Sensor that offers the magnetic sensing solution with superior sensitivity the stability over temperature and the integrated protection features. The magnetic field is also indicated via the digital bipolar latch output. The IC has an open drain output stage with the 30mA current sink capability. The wide operating voltage ranges from 2.5V to 38V with the reverse polarity protection up to 22V makes the device suitable for the wide range of the industrial applications. Internal protection functions are also provided for the reverse supply conditions, load dump, and output short circuit or a over current.

Applications of the DRV5013 Digital Latch Hall Effect Sensor:

- flow meters
- Power tools
- Solenoid and Valve status
- Proximity sensing
- Tachometers
- Brush less DC motors

Study of RF Wireless Sensors (11 of 23)

IBM

IBM ICE (Innovation Centre for Education)

Humidity sensor → Principle

(1) Water vapor permeably electrode
(2) Humidity sensitive polymer
(3) Backplate electrode
(4) Basesubstrat
(5) Pin – capacitive measurement
(6) Pin – temperature measurement

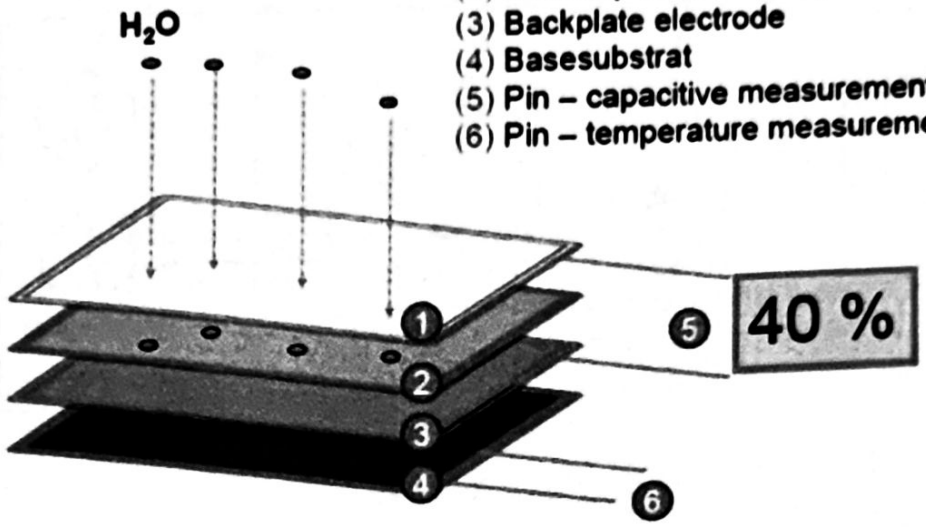


Figure 4-13. Study of RF Wireless Sensors (11 of 23)

Notes:

Relative humidity is a function of temperature. This sensor determines the amount of moisture or water vapor in the air. Integrated temperature sensors are also included in the Humidity Sensors.

This technology is been used in many applications including environmental monitoring in buildings and automobiles, warranty monitoring, process control, condensation/fog sensing and remote weather stations.

Example of humidity Sensors HDC 1000

HDC1000 is integrated humidity sensor and the temperature sensor with ±3% accuracy at very low power. The device measures its humidity based on the novel capacitive sensor. The humidity and temperature sensors are the factory calibrated. The innovative WLCSP (Wafer Level Chip Scale Package) also simplifies the board design with the use of an ultra-compact package. And the sensing element of the HDC1000 is placed on a bottom part of the device, which also makes the HDC1000 more robust against the dirt, dust, and also the other environmental contaminants. The HDC1000 is a functional within full of –40°C to +125°C is temperature range.

The main applications of these sensors are;

- White goods
- Wearable devices
- Printers
- Hand held Meters

- Medical devices
- Cargo shipping
- Automotive windshield Defog
- Smart thermostats and Room Monitors

Study of RF Wireless Sensors (12 of 23)

IBM

IBM ICE (Innovation Centre for Education)

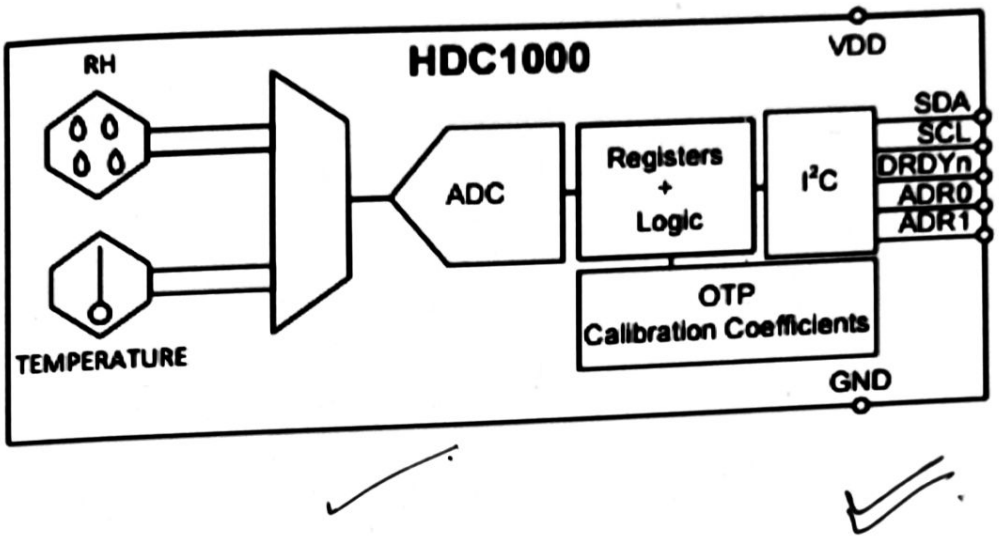


Figure 4-14. Study of RF Wireless Sensors (12 of 23)

Notes:

Description and functional diagram:

A HDC1000 is digital type of humidity sensor with an integrated temperature sensor that provides excellent measurement accuracy which is of very low power and the long term. The sensing element of the HDC1000 is placed on the bottom part of the device, which also makes the HDC1000 a more robust against dirt, dust, and other environmental contaminants. Measurement results can even be read out through the I2C compatible interface. Resolution is based on the measurement time and that can be 8, 11, or 14 bits for the humidity; 11 or 14 bits for the temperature.

Power Consumption: This device is suitable in battery or power harvesting applications. And in these applications the HDC1000 spends most of time in the sleep mode with a typical range of 110nA of the current consumption which is in sleep mode, and the averaged current consumption is minimal. Moreover its low consumption in the measurement mode minimizes any of the self-heating.

Voltage Supply Monitoring: The HDC1000 monitors the supply voltage level and also indicates when the voltage supply of HDC1000 is less than 2.8V. This information is useful in battery-powered systems is in order to inform the user for replacing the battery. This is reported in a TRES field (register address 0x00: bit) which is updated after the POR and after each measurement request.

Heater: The heater is the integrated resistive element that can also be used to test the sensor or to drive condensation off the sensor. The heater can also be activated by using HEAT, bit13 in the Configuration Register. And the heater helps in reducing the accumulated offset after the long exposure at high humidity

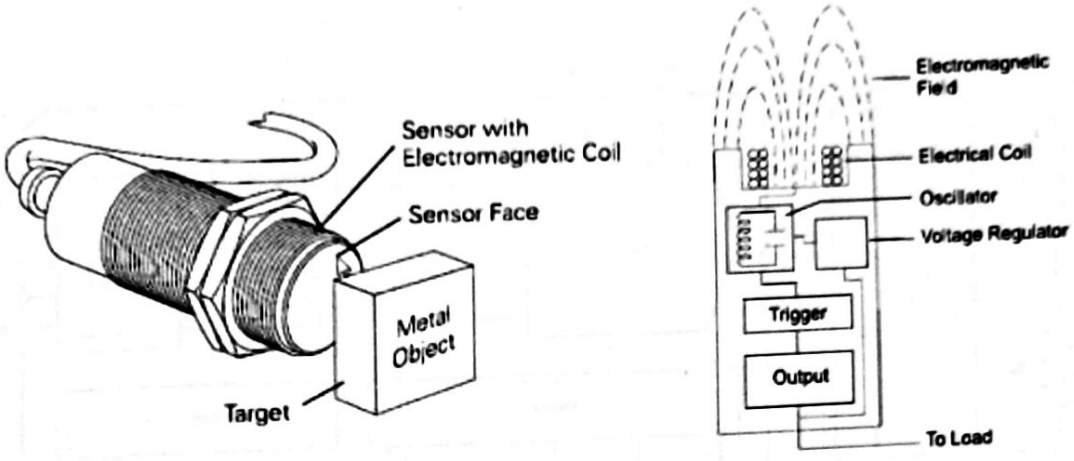
conditions. Once it is enabled the heater is to be turned on only in the measurement mode. To have the reasonable increase of the temperature it is also suggested to increase the measurement of data rate.

Device Functional modes: The HDC1000 has two types of modes of operation: sleep mode and measurement mode. And after a power up, the HDC1000 goes in sleep mode. In this mode, the HDC1000 waits for the I2C input including the commands to configure the conversion times, and read the status of the battery, triggers a measurement, and read measurements. Once it receives the command to trigger a measurement, the HDC1000 which moves from sleep mode to the measurement mode. In measurement mode, the HDC1000 also acquires the configured measurement and even sets a DRDYn line is low when the measurement is completed. After completing the measurement and settings the DRDYn low, the HDC1000 returns to sleep mode.

Study of RF Wireless Sensors (13 of 23)

IBM ICE (Innovation Centre for Education)

Inductive Sensors



Construction of a inductive proximity sensor

IOT011.0

Figure 4-15. Study of RF Wireless Sensors (13 of 23)

Notes:

Inductive sensor is a contact less sensing technology that can also be used to measure the position, motion, or composition of a metal or a conductive target as well as detects the compression, extension, or twist of the spring. Immunity to the environmental interferer such as oil, water or dirt allows sensing even in the very harsh environments.

LDCs (inductance to digital convert sensors) enables the own custom coils as sensors .These sensors can be used to detect the parallel resonance impedance and inductance of the sensor. The choice of the value which is to be used is depends on the application and system requirements. Inductive switches and Inductance to digital converters are the example of the inductive sensors. Inductive switches are used to proximity detection and event counting applications and for absolute position or motion sensing applications inductance to digital converters are used.

Examples of inductive sensors: LDC1614, LDC1000 are the inductance to digital converters and LMP91300 is an integrated inductive proximity sensor.

Study of RF Wireless Sensors (14 of 23)

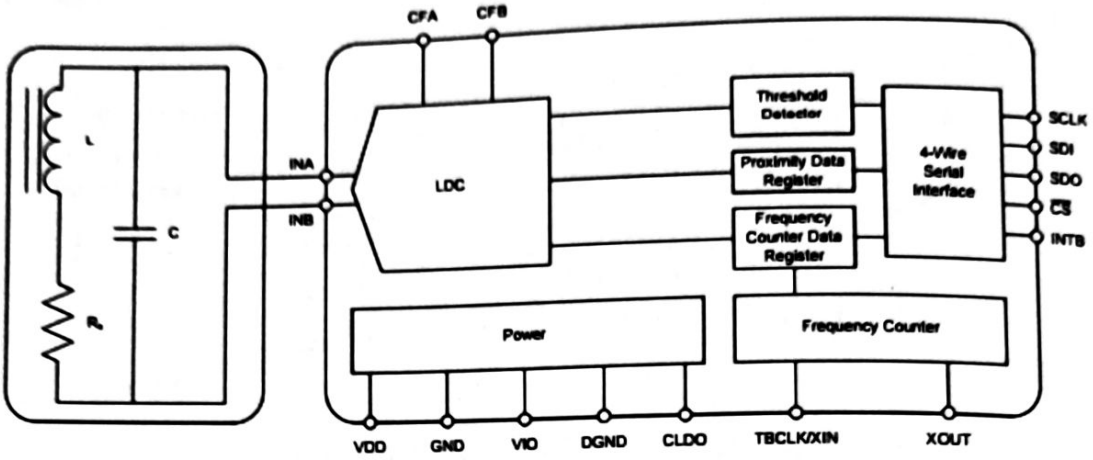


Figure 4-16. Study of RF Wireless Sensors (14 of 23)

IOT011.0

Notes:

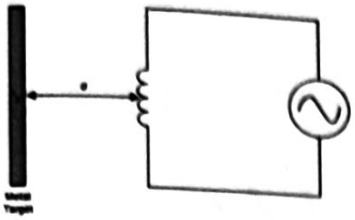
Working Function of LDC1000:

The LDC1000 is an Inductance-to-Digital Converter which measures the parallel impedance of an LC resonator. It also accomplishes this task by regulating the oscillation amplitude in the closed-loop configuration to a constant level, while monitoring the energy to be dissipated by the resonator. By monitoring the amount of a power injected into the resonator, the LDC1000 can also determine the value of Rp; it even returns this as the digital value which is inversely proportional to the Rp. The threshold detector block provides the comparator with hysteresis. With the threshold registers programmed and comparator is enabled, proximity data register is compared with the threshold registers and INTB terminal indicates the output. The device has the simple 4-wire SPI interface. The INTB terminal provides of multiple functions which are programmable with the SPI. The device has separate supplies for Analog and I/O, with an analog operating at 5 V and I/O at 1.8-5 V. The integrated LDO also needs a 56nF capacitor to be connected from CLDO terminal to GND.

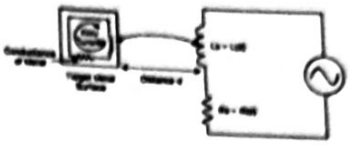
Study of RF Wireless Sensors (15 of 23)

IBM

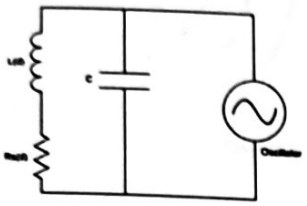
IBM ICE (Innovation Centre for Education)



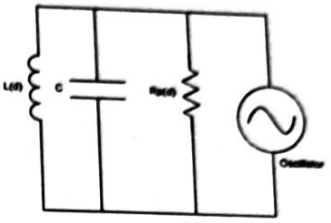
Inductor with metal target



Metal target modeled as L and R with circulating Eddy currents



LC tank connected to Oscillator



Equivalent Resistance of Rs in parallel with LC tank

Figure 4-17. Study of RF Wireless Sensors (15 of 23)

IOT011.0

Notes:

Inductive Sensing:

AC current flowing through a coil will generate an AC magnetic field. If the conductive material, such as a metal target, is brought into the vicinity of the coil, this magnetic field induces circulating currents (eddy currents) on a surface of the target. And these eddy currents are also a function of distance, size, and composition of the target. The eddy currents and then generate their own magnetic field, which also opposes the original field generated by the coil. This mechanism is best compared with a transformer, where the coil is a primary core and the eddy current is of secondary core. The inductive coupling between both the cores depends upon the distance and shape. Hence the resistance and inductance of a secondary core (eddy current), that shows up as a distant dependent of resistive and inductive component on a primary side (coil). The figures above show a simplified circuit.

Eddy currents are generated on the surface of a target which can be modeled as a transformer as shown in Figure. The coupling between the primary and secondary coil is a function of the distance and conductor's characteristics. In the above figure, the inductance Ls is the coil's inductance, and Rs is a coil's parasitic series resistance. The inductance L(d), which is the function of distance d, is a coupled inductance of the metal target. Likewise, R(d) is a parasitic resistance of the eddy current and is also a function of distance. Generating an alternating magnetic field with just an inductor will consume the large amount of the power. This power consumption can be reduced by adding the parallel capacitor, and turning it into a resonator as shown in the other figure. In this manner the power consumption is than reduced to the eddy and inductor losses Rs+R(d) only.

The LDC1000 doesn't measures the series resistance directly; instead of it measures the equivalent parallel resonance impedance Rp. This representation is equivalent to the one shown in the next figure, where the parallel resonance impedance Rp(d) is given by:

$Rp(d)=Ls+L(d)/[Rs+R(d)*C]$

Study of RF Wireless Sensors (16 of 23)

IBM

IBM ICE (Innovation Centre for Education)

Optical Sensors

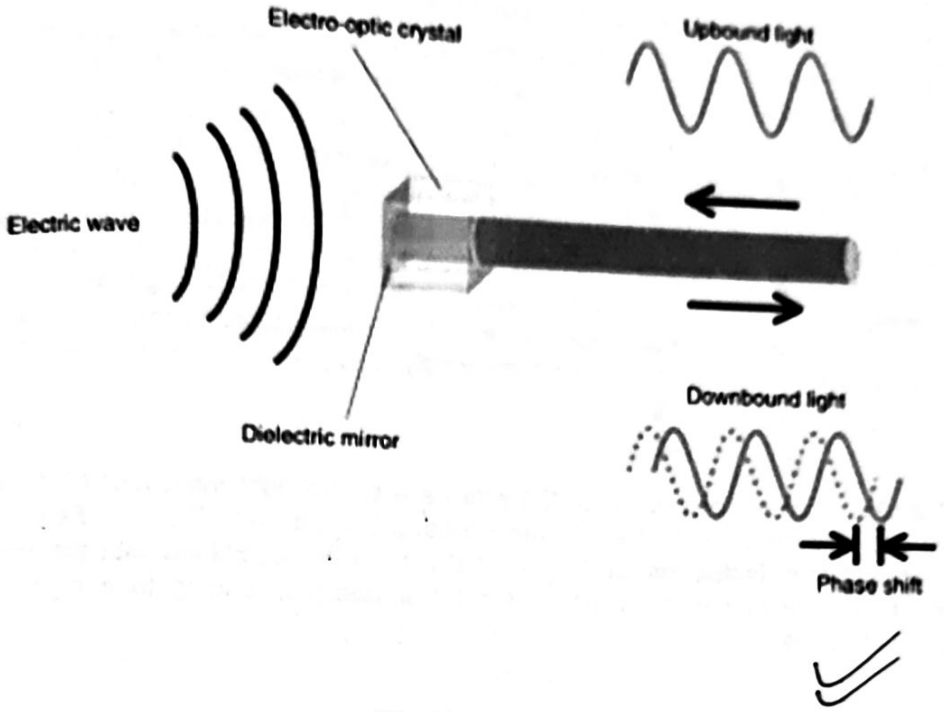


Figure 4-18. Study of RF Wireless Sensors (16 of 23)

IOT011.0

Notes:

Optical sensing is defined as conversion of light rays into electronic signals. The intensity of the light is measured or changes between one or more than one light beam is being measured. In its simplest form, sensing light intensity is used for the lighting control in everything from the tablets/phones to building automation and street lighting.

Optical sensing is used in the broad range of applications, and by monitoring the additional characteristics (spectrum, phase, geometry, and timing), of optical sensing enables an advanced applications such as chemical analysis, 3D mapping, medical scanning, and pulse oximetry. In its simplest form, sensing light intensity is also used for lighting controls in everything from tablets/phones to the building automation and street lighting. Optical sensing is also used in broad range of applications, and by monitoring an additional characteristics (spectrum, phase, geometry, or timing), and optical sensing enables advanced applications such as the chemical analysis, 3D mapping, medical scanning, and pulse oximetry.

Ambient light sensors, 3D time of full light, DLP advanced light control are the products of the optical sensors. Ambient light sensors are used to measure the intensity of light with a sensitivity tailored to match the human eye. 3D time of full light utilizes active IR illumination is used to measure the distance of objects which are in front of the sensor. DLP advanced light control is a programmable structured light enables projection of custom and adaptable patterns on the target object to sense physical measurements, and to analyze location or inspect a surface. OPT3001, DLP4500NIR and DLP500 are examples of optical sensors.

OPT 3001:

The OPT3001 is a type of sensor that measures the intensity of a visible light. The spectral response of the sensor tightly matches a photopic response of the human eye and includes the significant infrared rejection.

The OPT3001 is the single-chip lux meter, measuring the intensity of a light which is visible by the human eye. The precision spectral response and the strong IR rejection of the device which also enables the OPT3001 to accurately meter at the intensity of light as seen by the human eye regardless of the light source. The strong IR rejection also aids in maintaining the high accuracy when industrial design calls for mounting the sensor under the dark glass for aesthetics. The OPT3001 is designed for the systems that create a light-based experience for the human, and an ideal preferred replacement for the photo diodes, photo resistors, or other ambient light sensors with a less human eye matching and IR rejection.

Measurements can also be made from 0.01 lux up to 83k lux without manually selecting full-scale ranges by using a built-in, full-scale setting feature. This capability allows the light measurement over the 23-bit effective dynamic range.

The digital operation is flexible for the system integration. Measurements can be either continuous or a single-shot. The control and interrupt system features of autonomous operation, and allowing the processor to sleep while the sensor searches for the appropriate wake-up events to report through an interrupt pin. The digital output is reported over an I2C and SMBus (The System Management Bus is the single-ended simple two-wire bus for the purpose of a lightweight communication. Most commonly it is found in the computer motherboards for communication with power source for ON/OFF instructions) compatible, two-wire serial interface. And the low power consumption and low power-supply voltage capability of the OPT3001 enhances the battery life of battery-powered systems.

DLP4500NIR:

The DLP4500NIR digital micro mirror device (DMD) acts as a spatial light modulator (SLM) to steer the near-infrared (NIR) light and create patterns with the speed, precision and efficiency. Featuring the high resolution in the compact form factor, the DLP4500NIR DMD is often combined with the single element detector to replace expensive In GaAs array-based detector designs, leading to a high performance, cost-effective portable solutions.

Study of RF Wireless Sensors (17 of 23)

IBM

IBM ICE (Innovation Centre for Education)

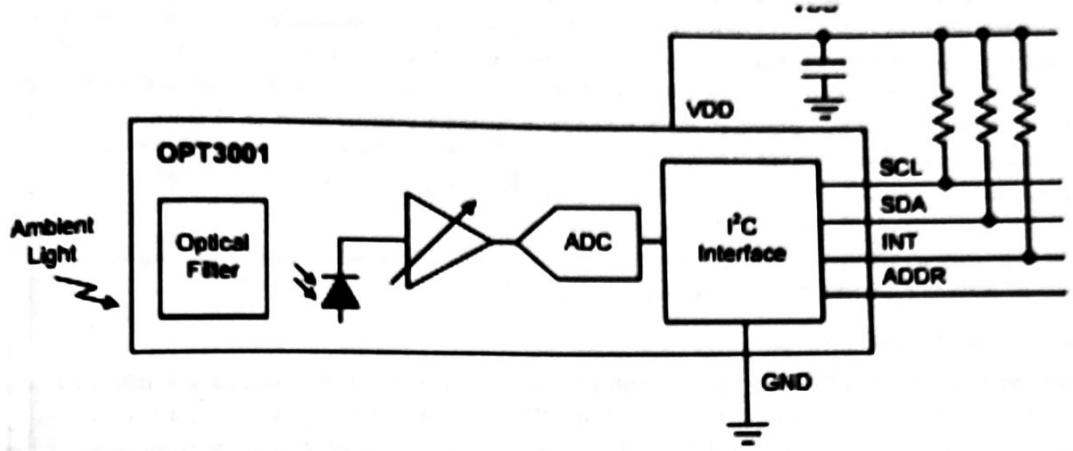


Figure 4-19. Study of RF Wireless Sensors (17 of 23)

IOT011.0

Notes:

Functional Description of OPT3001:

The OPT3001 measures an ambient light that illuminates the device. This device measures the light with a spectral response very closely matched to the human eye, and with a very good infrared rejection. The matching sensor of spectral response than the human eye response is so vital because ambient light sensors are used to measure and help to create ideal human lighting experiences. The strong rejection of infrared light, a human does not see it is crucial component of this matching. This matching makes an OPT3001 especially good for the operation of underneath windows that are visibly dark, but infrared transmissive.

The OPT3001 is a fully self-contained to measure an ambient light and report the result in the lux digitally over the I2C bus. The result can also be used to alert a system and then interrupt a processor with the INT pin. The result can even be summarized with the programmable window comparison and communication with the INT pin.

The OPT3001 can also be configured into an automatic full-scale, range-setting mode that will always select the optimal full-scale range to set for the lighting conditions. This mode frees a user from program that their software is for potential iterative cycles of measurement and even readjustment of the full-scale ranges until the optimal for any of the given measurement. The device can be commanded to operate continuously or in single-shot measurement modes. The device integrates its results over either the 100ms or 800ms, so the effects of 50-Hz and 60-Hz noise sources are from typical light bulbs are nominally reduced to a minimum. The device that starts up in the low-power shutdown state, such that the OPT3001 only consumes an active-operation power after being to programmed into an active state.

And the OPT3001 optical filtering system is not excessively so sensitive to non-ideal particles and micro-shadows are on the optical surface. This reduced sensitivity is also a result of the relatively minor device dependency on the uniform density of optical illumination of the sensor area for the infrared rejection. Proper optical surface cleanliness is always recommended for the best results on all optical devices.

Human Eye Matching:

The OPT3001 spectral response closely matches that of the human eye. If an ambient light sensor measurement is used to help and create a good human experience, or create the optical conditions that are optimal for a human, the sensor have to measure the same spectrum of a light that a human sees. The device also has an excellent infrared light (IR) rejection. This IR rejection is especially important because many of the real-world lighting sources have the significant infrared content that human do not see. If the sensor measures an infrared light that the human eye cannot see, a true human experience is not accurately represented. And furthermore, if the ambient light sensor is hidden underneath of a dark window (such that the end-product user cannot see a sensor) the infrared rejection of the OPT3001 significantly becomes more important because many of the dark windows attenuate visible light but transmit infrared light. This attenuation of the visible light and lack of attenuation of the IR light amplifies the ratio of the infrared light to visible light which illuminates the sensor. Results can also still be well matched to the human eye under this condition because of a high infrared rejection of the OPT3001.

Automatic Full-Scale Range Setting:

The OPT3001 has an automatic full-scale range setting features that also eliminates the need to predict and sets the optimal ranges for the device. In this mode, the OPT3001 automatically selects an optimal full-scale range for a given lighting condition. The OPT3001 has a high degree of result is matching between the full-scale range settings. This matching may eliminate the problem of varying results or the need for the range-specific, user-calibrated gain factors when the different full-scale ranges are been chosen. For further details, see an Automatic Full-Scale Setting Mode section.

Interrupt Operation, INT Pin, and the Interrupt Reporting Mechanisms:

The device has an interrupt of reporting system that allows the processor connected to the I2C bus to go to sleep, or otherwise ignores the device results, until a user-defined event occurs that requires a possible action. Alternatively, the same mechanism can be used with any of the system that can take the advantage of a single digital signal that indicates whether the light is an above or below levels of the interest. The interrupt event conditions are to be controlled by the high-limit and low-limit registers, as well as a configuration register latches and fault count fields. The results of comparing a result register with the high-limit register and low-limit register are referred to the fault events. The fault count register dictates that how many consecutive are of same result that fault events are required to trigger an interrupt event and also subsequently changes the state of the interrupt reporting mechanisms, which are of INT pin, a flag high field, and a flag low field. The latch field allows a choice between the latched window-style comparison and the transparent hysteresis-style comparison. The INT pin has an open-drain output, of which requires the uses of a pull-up resistor. This open-drain output allows multiple devices with the open-drain INT pins to be connected to the same line, thus creating the logical NOR or AND function between devices. The polarity of the INT pin that can be controlled with the polarity of interrupt field in a configuration registers. When the POL field is set to 0, the pin operates in an active low behavior so that pulls the pin low when an INT pin becomes active. When a POL field is set to 1, the pin operates in an active high behavior and becomes the high impedance, thus allowing the pin to go high when the INT pin becomes active.

Application and Implementation:

Ambient light sensors are used in the wide variety of applications that requires control as the function of ambient light. Because ambient light sensors nominally matches the human eye spectral responses, that they are superior to photodiodes when the goal is to create an experience for the human beings. Very common applications that include display optical-intensity control and industrial or home lighting control.

Study of RF Wireless Sensors (18 of 23)

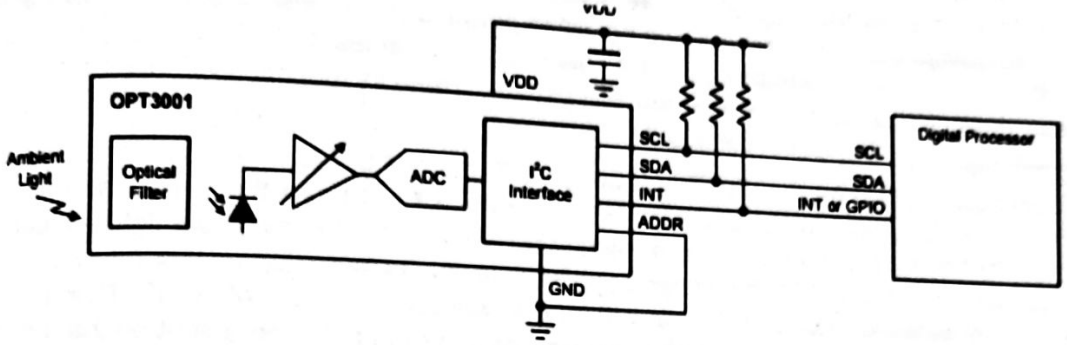


Figure 4-20. Study of RF Wireless Sensors (18 of 23)

Notes:

Two types of categories of interface are available in the OPT 3001.They are;

Electrical Interface:

The electrical interface is quite simple, as illustrated in Figure above. Connect the OPT3001 I2C SDA and the SCL pins to the same pins of an applications processor, a microcontroller, or the other digital processor. If that digital processor requires the interrupt results from the event of interest from the OPT3001, then connect the INT pin to either an interrupt or the general-purpose I/O pin of the processor. There are many multiple uses for this interrupt, by including signaling the system to wake up from the low-power mode, processing other tasks while waiting for an ambient light event of the interest, or alerting the processor that the sample is ready to be read. Connect pull up resistors between a power supply appropriate for digital communications and of the SDA and SCL pins (because they have open-drain output structures) also. If the INT pin is used, connect a pull up resistor to the INT pin. A typical value for these pull up resistors is 10kΩ. The resistor choice can also be optimized in conjunction to the bus capacitance for balancing the system speed, power, noise immunity, and other such requirements.

The power supply and the grounding considerations are discussed in the Power-Supply Recommendations of section. Although the spike suppression is integrated in the SDA and SCL pin circuits, uses the proper layout practices to minimize an amount of coupling into the communication lines. And one possible introduction of noise occurs from capacitive coupling signal edges in between the two communication lines among themselves. Another possible noise of introduction comes from the other switching noise sources present in the system, and especially for the long communication lines. In noisy environments, shield communication

lines are used to reduce the possibility of unintended noise of coupling into the digital I/O lines that could also be incorrectly interpreted.

Optical Interface:

The optical interface is a physically located within the package, of facing away from the PCB, as specified by the Sensor Area. Physical components, such as the plastic housing and a window that allows a light from outside of the design to illuminate the sensor, can help to protect the OPT3001 and the neighboring circuitry. Sometimes, a dark or opaque window is been used to further enhance the visual appeal of a design by hiding a sensor from view. This window material is typically a transparent plastic or glass. Any physical component that affects the light that which illuminates the sensing area of a light sensor also that affects the performance of that light sensor. Therefore, for the optimal performance, make sure to understand and controls the effect of these components. Design the window width and height to permit the light from a sufficient field of view to illuminate a sensor. For best the performance, uses a field of view for at least ±35°, or ideally ±45° or more. Understanding and designing a field view is been discussed further in the application report SBEA002, OPT3001 of Ambient Light Sensor Application Guide.

The visible-spectrum transmission for the dark windows typically ranges between 5%to30%, but can be less than 1%. Specify the visible-spectrum transmission is as low as but not more than, necessary to achieve sufficient visual appeal because the decreased transmission decreases the available light for sensors to measure. The windows are made dark by either applying the ink to a transparent window material, or including a dye or the other optical substance within the window material of itself. This attenuating transmission is of in the visible spectrum of the window creates the ratio between a light on the outside of a design and the light that is measured by the OPT3001. Accurately for measuring a light outside of the design, which compensates the OPT3001 measurement and for this ratio an example is given in Dark Window Selection and the Compensation.

Ambient light sensors are used to help and create the ideal lighting experiences for humans therefore, and the matching of the sensor spectral responses to that of the human eye response is so vital. Infrared light is not visible to the human eye, and can also interfere with the measurement of visible light when the sensors lack infrared rejection. Therefore, the ratio of a visible light of interfering infrared light that affects the accuracy of any practical system that represents a human eye. The strong rejection of an infrared light by the OPT3001 allows the measurements consistent with human perception under the high-infrared lighting conditions, such as from incandescent, halogen, or sunlight sources.

Design Requirements:

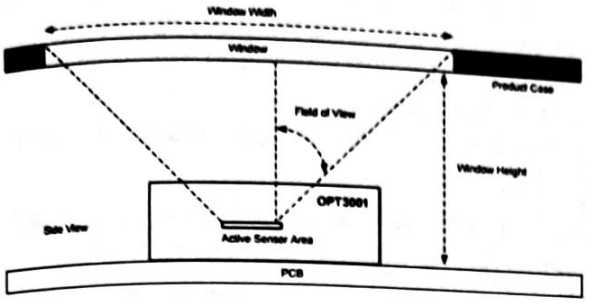
The basic requirements of this design are as follows:

- Sensor is hidden under dark glass so that sensor is not at all obviously visible. Note that this requirement is subjective to the designer preference.
- Accuracy of measurement of fluorescent light is 15%
- Variation in a measurement between the fluorescent, halogen, and incandescent bulbs (also known as the light source variation) is as small as possible.

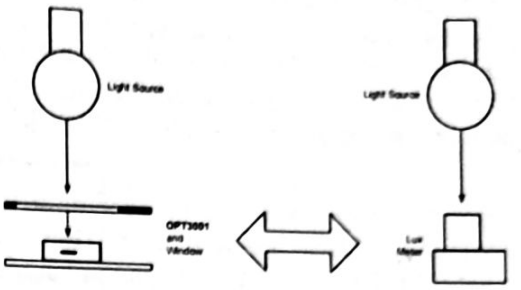
Study of RF Wireless Sensors (19 of 23)

IBM

IBM ICE (Innovation Centre for Education)



Product case and window over the OPT3001



Fixture with One Light Source Accommodating Either a Lux Meter or the Design (Window and OPT3001) in the Exact Same X,Y,Z Position

Figure 4-21. Study of RF Wireless Sensors (19 of 23) IOT011.0

Notes:

Design procedure

Optomechanical Design:

After completion of the electrical design, the next task used is the optomechancial design. Design a product case that includes a window to transmit the light from outside of a product to the sensor, as shown in below figure. Design the window width and the window height to give a ±45° field of view. A rigorous design of the field of view takes into account the location of the sensor area. The OPT3001 active sensor area is centered along with one axis of the package top view, but has a minor offset on the other axis of a top view. Window sizing and placement is discussed in more rigorous detail in the application report SBEA002, OPT3001: Ambient Light Sensor Application Guide Dark Window Selection and Compensation There are several approaches for selecting and compensating for a dark window. One of many approaches is the method described over here. Samples of many different windows are taken with various levels of darkness. Choose a window which is dark enough to optimize the balance between aesthetics of the device and sensor performance. Note that the aesthetic evaluation is a subjective opinion of a designer therefore it is more important to see the window on the physical design rather than refers to the window transmission specifications on paper. Make sure that the chosen window is not darker than absolutely it is necessary because a darker window allows less light to illuminate the sensor and therefore impedes the sensor accuracy. The window chosen for this applications example is dark and has less than 7% transmission at 550 nm. Figure above shows the normalized response of a spectrum. Note that the equipment used to measure the transmission spectrum is not capable for measuring an absolute accuracy (non-normalized) of the dark

window sample, but only the relative normalized spectrum. And also note that the window is much more transmissive to infrared wavelengths and longer than 700 nm than to visible wavelengths between the 400 nm and 650 nm. This imbalance between infrared and visible light decreases the ratio of a visible light to infrared light at the sensor. Although it is preferable to have a window to decrease this ratio as little as possible to (by having the window with a close ratio of visible transmission to the infrared transmission), the OPT3001 still performs well.

After choosing a dark window to measure an attenuating effect of the dark window for a later compensation. In order to measure this attenuation, firstly measure a fluorescent light source with a lux meter, later measure the same light with an OPT3001 under the dark window. To measure it accurately, it is important to use the fixture that can accommodate its lux meter or the design containing the OPT3001 and dark window, with a center of each of the sensing areas being in exactly the same X, Y, Z location, as shown in below Figure The Z placement of the design (distance from the light source) is on the top of the window, and not the OPT3001 itself.

The fluorescent light in this location measures a 1000 lux with the lux meter, and 73 lux with the OPT3001 under a dark window within the application. Therefore, a window has an effective transmission of the 7.3% for a fluorescent light. This 7.3% is a weighted average attenuation across an entire spectrum, weighted by the spectral response of the lux meter (or photopic response). For all the subsequent of OPT3001 measurements under this dark window, the following formula is applied. Compensated Measurement = Uncompensated Measurement / (7.3%).

Study of RF Wireless Sensors (20 of 23)

Pressure Sensor

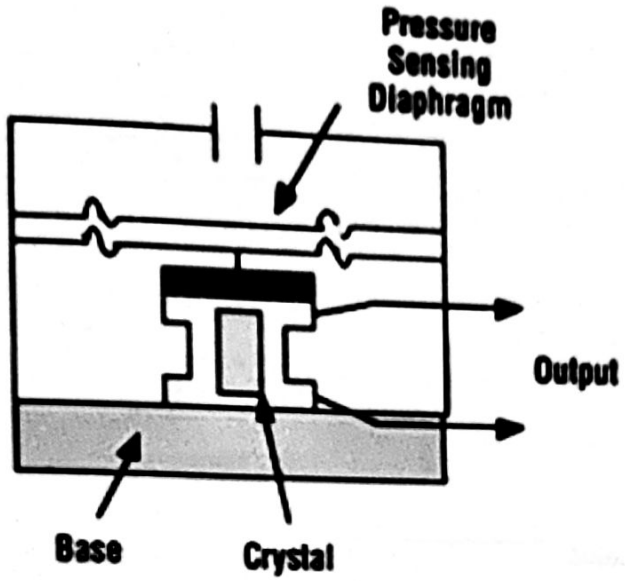


Figure 4-22. Study of RF Wireless Sensors (20 of 23) IOT011.0

Notes:

Pressure sensor is a signal conditioner which delivers the highly-precise and programmable solutions for accurately measuring the pressure. Measuring pressure precisely is very critical in number of industrial and commercial applications.

PGA400-Q1, PGA308 and PGA309 are examples of the pressure sensors.

PGA400-Q1 is an interface device for piezoresistive, strain gauge and capacitive sense elements. The device that incorporates the analog front end and that directly connects to the sense element and also the voltage regulators and oscillator. The device also includes the sigma-delta analog-to-digital converter of 8051 WARP core microprocessor and an OTP memory. Sensor compensation algorithms can be implemented in the software. The PGA400-Q1 also includes 2 DAC outputs.

1. pressure sensor signal conditioning
2. Level sensor conditioning
3. Humidity sensor signal conditioning the applications of the above sensor.

PGA308 is a programmable analog sensor signal conditioner. And the analog signal path amplifies the sensor signal and also provides the digital calibration for the offset and gain. Calibration is done via the 1W pin, a digital of One-Wire, UART-compatible interface. For the three-terminal sensor modules, 1W may be connected to VOUT and the assembly programmed through a VOUT pin. Gain and offset calibration parameters are to be stored on board in seven banks of the one-time programmable (OTP) memory. The power-on reset (POR) of OTP bank may be programmed a total of the four times.

The all-analog signal path contains of a 2×2 input multiplexer to allow electronic sensor lead swapping, a coarse offset adjusts, the auto-zero programmable gain instrumentation amplifier (PGA), of a fine gain adjust, a fine offset adjust, and the programmable gain output amplifier. The Fault Monitor circuitry which detects and signals sensor burnout, overload, and the system fault conditions. Over/under-scale limits and provides additional means for system level diagnostics. The dual-use DOUT/VCLAMP pin can be used for programmable digital output or as the VOUT over-voltage clamp.

PGA309 is the programmable analog signal conditioner designed for the bridge sensors. The analog signal path amplifies the sensor signal and provides digital calibration for the zero, span, zero drift, span drift, and the sensor linearization errors with the applied stress (pressure, strain, etc.). The calibration is also done via a One-Wire digital serial interface or through the Two-Wire industry-standard connection. The calibration parameters are to be stored in the external nonvolatile memory (typically SOT23-5) for eliminating the manual trimming and which achieves the long-term stability.

The all-analog signal path that contains a 2x2 input multiplexer, an auto-zero of programmable-gain instrumentation amplifier, linearization circuit, voltage reference, an internal oscillator, control logic, and an output amplifier. The programmable level shifting compensates for the sensor dc offsets.

The core of the PGA309 is the precision, a low-drift, no 1/f noise Front-End of a PGA (Programmable Gain Amplifier). The overall gain of a Front-End PGA + Output Amplifier can be adjusted from the 2.7V/V to 1152V/V. The polarity of input that can be switched through input multiplexer for accommodating the sensor with unknown polarity output. The Fault Monitor circuit detects and a signals sensor burnout, overload, and system of fault conditions.

1. bridge sensors
2. Remote 4-20mA Transmitters
3. Strain, load and weigh scales
4. Automotive sensors

These are the applications of the above sensor

Study of RF Wireless Sensors (21 of 23)

IBM

IBM ICE (Innovation Centre for Education)

Temperature Sensor

Figure 4-23. Study of RF Wireless Sensors (21 of 23)

Notes:

Temperature sensors leverage is of highly-predictable and linear properties of the silicon PN junction which derives temperature. Temperature sensors can also guarantee high accuracy while requiring a zero calibration in the end system. Temperature sensors offer the wide range of integration and a multi-channel of options to monitor external PN junctions such as the diodes, transistors, processors, ASICs, and FPGAs.

Temperature sensors are often used as a replacement for the thermistors for monitoring and protection, calibration, and the control. Temperature sensors can provide the greater linearity, lower power, a guaranteed accuracy, high programmability, and is built-in over-temperature detection and offer a wide range of analog and industry-standard interfaces.

The analog temperature sensors, digital temperature sensors and all temperature sensors are the different categories. TMP75B, LMT87 and TMP007 are some of the examples

TMP75B:

The TMP75B is the integrated digital temperature sensor with a 12-bit of analog-to-digital converter (ADC) that can be operated at a 1.8V supply, a pin and a register compatible with the industry-standard of LM75 and TMP75. This device is available in the SOIC-8 and VSSOP-8 packages, and requires no such type of external components to sense temperature. The TMP75B is a capable of reading the temperatures with a resolution of the 0.0625°C and is also specified over the temperature range of -55°C to +125°C.

The TMP75B features are SMBus and two-wire interface compatibility, and allows up to the eight devices on the same bus with the SMBus over temperature alert function. The programmable temperature that limits and

the ALERT pin allows a sensor to operate as the stand-alone thermostat, or an over temperature alarm for power throttling or system shutdown.

The factory-calibrated of the temperature accuracy and a noise-immune digital interface make the TMP75B the preferred solution for the temperature compensation of the other sensors and electronic components, without the need for additional system-level calibration or elaborate the board layout for distributed temperature sensing.

The TMP75B is ideal for the thermal management and protection of a variety of such as consumer, computer, communication, industrial and environmental applications.

- Server and Computer Thermal Management
- Telecommunication Equipment
- Video games consoles
- Office Machines
- Set-Top Boxes
- Power supply and Battery Thermal Protection
- Electrical Motor Driver Thermal Protection
- Environmental Monitoring
- Thermostat Control

Study of RF Wireless Sensors (22 of 23)

IBM

IBM ICE (Innovation Centre for Education)

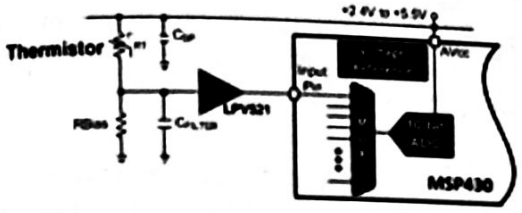


Fig A, Thermistor Solution

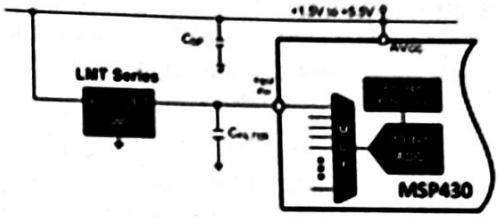


Fig B. Simplified solution using LMT Series

Figure 4-24. Study of RF Wireless Sensors (22 of 23) IOT011.0

Notes:

LMT87:

The LMT84-87 family is the precision analog of output temperature sensors that can operate at a supply voltage as low as the 1.5V and operates of between -50°C and 150°C. They are an effective and easy to use the replacement for NTC thermistors delivering more accurate and of more linear measurements while consuming of less power (Figure B).

The LMT87/LMT87-Q1 is precision CMOS of the integrated-circuit temperature sensors with the analog output voltage that is linearly and inversely proportional to the temperature. Its features make it suitable for many other general temperature sensing applications. It can operate down to 2.7V supply with the 5.4 µA power consumption. Multiple package options are including through-hole of TO-92 and TO-126 packages also allow the LMT87 to be mounted as on-board, off-board, to a heat sink, or on the multiple unique locations in same application. And a class-AB output structure that gives the LMT87/LMT87-Q1 strong output source and the sink current capability that can directly drive up to 1.1nF of capacitive loads. This means it is well suited to drive an analog-to-digital converter of sample-and-hold input with its transient of load requirements. It has an accuracy of specified in the operating range of −50°C to 150°C. The accuracy, of 3-lead package options, and few other features also makes the LMT87/LMT87-Q1 an alternative to the thermistors.

For devices with different average sensor gains and comparable accuracy LMT84/LM84-Q1, LMT85/LMT85-Q1 and LMT86/LMT86-Q1

1. Automotive Applications

2. Industrial Applications
3. White goods Appliances
4. Battery Management
5. Disk Drives
6. Games
7. Wireless Transceivers
8. Cell phones

TMP007:

The TMP007 is an infrared (IR) of thermopile sensors that measures a temperature of an object without contacting object. The integrated thermopile absorbs infrared energy which is to be emitted from the object in sensor field of view. The thermopile voltage is digitized and is provided as an input to the integrated math engine, along with a die temperature (TDIE). The math engine then computes a corresponding object temperature.

Default calibration and the thermal transient coefficients are to be stored in the built-in nonvolatile EPROM memory. Application specific values can even be stored for improved accuracy. An alert function is also available, and that can be programmed in either comparator or interrupt mode.

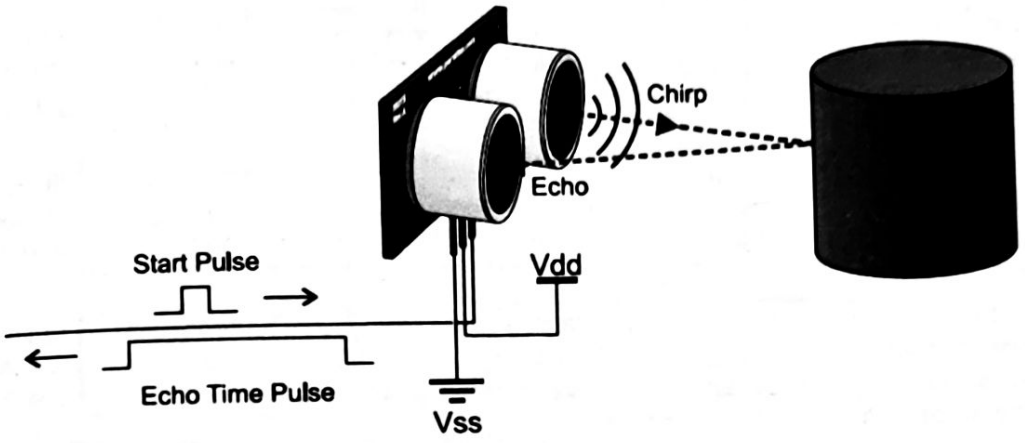
The TMP007 is a compatible with the I2C and SMBus interfaces, and allows up to eight devices on one bus. The Low power consumption along with low operating voltage is ideal for the battery-powered applications.

The TMP007 provides convenience, and non-contact thermal solutions for measuring temperature with the factory-supplied calibration. This device is also suitable for the industrial and consumer applications with the user-customized system calibration

- Non-contact Temperature Measurement
- Laptop and Tablet cases
- Batteries
- Heat sinks
- Skin
- Laser prints are the applications of the TMP007 Sensors.

Study of RF Wireless Sensors (23 of 23)

Ultrasonic sensors



IOT011.0

Figure 4-25. Study of RF Wireless Sensors (23 of 23)

Notes:

Ultrasonic sensing is the measurement of the time between an ultrasonic signal which is been sent and received. The interval between the two signals is also typically referred to as the time of flight (ToF). The speed of an ultrasonic wave is sensitive to the transmission medium (such as flow speed, temperature & concentration / purity).This technology used in the applications like

1. Distance to target either in a gas or fluid
2. Level of fluid in a tank
3. Flow speed of a gas or liquid
4. Temperature and concentration of a liquid or a gas

PGA450-Q1, TDC7200 and TDC1000-Q1 are examples of the ultrasonic sensors.

PGA450-Q1:

The PGA450-Q1 is a fully integrated interface device for ultrasonic transducers used in automotive park distance or object detection applications. It incorporates the system blocks such as voltage regulators, of 12-bit SAR ADC, an 8-bit microcontroller, a digital band-pass filter, a DAC, a dual NMOS low-side drivers, a low-noise amplifier, an oscillator, and the LIN 2.1 physical interface and protocol for interfacing.

The PGA450-Q1 possesses an 8-bit microcontroller and also OTP memory for the program storage and for processing the echo signal and even calculating the distance between the transducer and the object. This

data is to be transmitted through a LIN 2.1 communication protocol. The LIN 2.1 physical layer is slave-only and does not implement LIN wake-up features. All other LIN 2.1 features can be implemented in software.

- Automotive Park Distance
- Blind Spot Detection
- Object Detection Application is the applications of the above sensors.

TDC7200:

TDC7200 is a Time to Digital Converter (TDC) for ultrasonic sensing measurements such as water flow meter, gas flow meter, and the heat flow meter. When these are paired with the TDC1000 (ultrasonic analog-front-end), the TDC7200 can be a part of the complete TI ultrasonic sensing solution that includes the MSP430, power, wireless, and source code.

A Time to Digital Converter (TDC) performs the function of a stopwatch and measures the elapsed time (time-of-flight or TOF) between a START pulse and up to the five STOP pulses. The ability to measure from START to multiple STOPs gives user the flexibility to select which can STOP pulse yields for best echo performance.

The device has an internal self-calibrated time based on which compensates for the drift over time and temperature. Self-calibration enables time-to-digital conversion accuracy in an order of picoseconds. This accuracy makes the TDC7200 ideal for flow meter applications, where zero and the low flow measurements require the high accuracy.

When placed in the Autonomous Multi-Cycle Averaging Mode, the TDC7200 can also be optimized for the low system power consumption, making it ideal for battery powered flow meters. In this mode, and the host can go to sleep to save the power, and it can even wake up when it is interrupted by the TDC upon a completion of the measurement sequence.

1. Heat cost Allocators
2. Flow meter: Water Meter, Gas Meter, Heat Meter is the applications of the above sensor.

TDC1000-Q1:

The TDC1000 is of fully integrated analog front-end (AFE) for the ultrasonic sensing measurements of level, fluid identification/concentration, flow, and proximity/ distance applications are common in automotive, industrial, medical, and consumer markets. When it is paired with MSP430/C2000 MCU, power, wireless, and source code, TI provides a complete ultrasonic sensing solution.

TI's Ultrasonic AFE offers the programmability and flexibility to accommodate the wide-range of applications and end equipment. The TDC1000 can be configured for the multiple transmit pulses and frequencies, gain, and the signal thresholds for use with the wide-range of transducer frequencies of (31.25KHz to 4MHz) and the Q-factors. Similarly, the programmability of the receive path which allows ultrasonic waves to be detected over the wider range of a distances/tank sizes and through the various mediums.

Selecting different modes of the operation, TDC1000 can be optimized for the low power consumption, making it ideal for the battery powered flow meters, level instrumentation, and the distance/proximity measurements. The low noise amplifiers and comparator provides the extremely low jitter, enabling pico second resolution and accuracy for zero and low flow measurements.

1. Measurements through tanks of varying materials
2. Fluid level
3. Fluid identification or concentration
4. Flow metering :Gas, Water and Heat
5. Distance or proximity Sensing are the applications of above sensors.

Wireless Networks (1 of 19)

IBM

IBM ICE (Innovation Centre for Education)

Figure 4-26. Wireless Networks (1 of 19)

IOT011.0

Notes:

Bluetooth Technology:-

Bluetooth is an easy to use, short range and low bandwidth wireless networking technology. It uses the radio waves to send data .Bluetooth eliminates the need for cables by providing small form factor, low cost wireless solution that will also link computers, cell phones and many other electronics devices easily and quickly, expanding the communication capabilities. Bluetooth radio technology that operates in the license-free, global 2.4 GHz ISM frequency band and is very robust because of its adaptive frequency hopping technique, making it suitable for demanding the industrial, professional, medical and many other applications.

Data transmission in Bluetooth will be done through the low power radio waves. The communication frequency of the Blue tooth networks is 2.4GHZ.The, exact frequency is 2.402GHZ to 2.480GHZ. This frequency band has been set aside by the international agreement for the use of all such industrial, scientific and medical devices (ISM).

All the devices are taking the advantages of such type radio frequencies. Garage door openers, baby monitors and the cordless phones all make use of ISM band. Bluetooth and these other devices don't interfere with any one another as been a crucial part of the design process. Bluetooth devices avoid interfering with the other systems is by sending out the very weak signals which is of about 1milliwatt and by comparison most powerful cell phone can transmit the signal of 3watts.The range of the Bluetooth device is about of 32feet (10meters) because of the low power limits and it cuts the chance of interference between computer, mobile or television. Another advantage of Bluetooth is it doesn't require line of sight between

communicating devices because of the low power limits. The walls in house won't stop a Bluetooth signal, making the standard useful for controlling the several devices in the different rooms.

Simultaneously Bluetooth can connect up to eight devices with all of those devices in the same 10 meter radius, all are think that there may be a interference with another but it won't why because Bluetooth uses the technique called spread spectrum frequency hopping and which makes it rare for more than one device to transmit on the same frequency at the same time. A device will use 79 individual, and is randomly chosen frequencies within a designated range, changing from one to another on the regular basis in this technique. The transmitter changes the frequencies for 1,600 times every second that means more devices can make full use of a limited slice of the radio spectrum in case of the Bluetooth. Every Bluetooth transmitter uses a spread spectrum transmitting automatically it doesn't mean that two transmitters will always be on the same frequency at the same time. This same technique minimizes the risk that portable phones or the baby monitors will disrupt the Bluetooth devices, since any interference on the particular frequency will last only a tiny fraction of a second. An electronic conversation takes place, if Bluetooth-capable devices come within range of one another to determine whether they have the data to share or whether one may need to control the other. This electronic conversation happen automatically no need of command from user side. Once the conversation is occurred, devices whether they're a part of the computer system or a stereo form a network. Bluetooth system creates a personal-area network (PAN), or a piconet, that may fill a room or may encompass the no more distance than that between the cell phone on a belt-clip and a headset on your head. Once a piconet is been established, the members randomly hop frequencies in unison so they can even stay in touch with one another and avoid the other piconets that may be operating in the same room.

For example, there is an entertainment system with the stereo, a DVD player, a satellite TV receiver and television not only these but also cordless telephone and the personal computer. Each of these systems uses a Bluetooth and each of them forms own piconet to talk between with the main unit and peripheral in a modern living room. The cordless telephone has one of the Bluetooth transmitter in the base and another in the handset. And the manufacturer has programmed each unit with an address that falls into the range of addresses it has been established for a particular type of device. When the base is first turned on, it sends a radio signals asking for a response from any of the units with an address in a particular range. Since handset has an address in the range of which it respond, and a tiny network is formed. Now, even if one of these devices should receive the signal from another system, it will ignore it since it's not from within a network. The computer and entertainment system goes through similar routines, establishing networks among the addresses in range established by the manufacturers. Once the networks are been established, the systems begin talking among themselves. Each piconet hops of randomly through an available frequencies, so all the piconets are of completely separated from one another.

Now the living room has three separate networks which are to be established, each one made up of devices that must know address of the transmitters so that it should listen to and then address of receivers it should talk to. Since each network can change the frequency of its operation for thousands of times a second, it's unlikely that any of the two networks will be on the same frequency at the same time. And if it turns out that they are, then the resulting confusion will only covers a tiny fraction of the second, and software designed to correct for such type of errors weeds out of the confusing information and also gets on with network's business.

In any wireless networking setup, security is a concern. Devices can even easily grab radio waves which are out of the air, so people who send sensitive information over a wireless connection must need to take the precautions to make sure that those signals aren't intercepted. Bluetooth technology is not different but it's wireless and therefore susceptible to spying and a remote access, just like the Wi-Fi is susceptible if the network isn't secure. With the Bluetooth though automatic nature of a connection, which is a huge benefit in terms of a time and effort, is also a benefit to the people looking to send you data without your permission.

Bluetooth offers several security modes, and the device manufacturers to determine which mode to include in a Bluetooth-enabled gadget. In almost all cases, Bluetooth users can also establish the "trusted devices" so that can exchange data without asking permission. When any of the devices tries to establish the connection to the user's gadget, the user has to decide to allow it. Service-level security and the device-level security both works together to protect the Bluetooth devices from an unauthorized data transmission. Security methods also include authorization and identification procedure that limits the use of a Bluetooth services to the registered user and require that users which make a conscious decision to open a file or to accept the

data transfer. As long as these measures which are enabled on the user's phone or the other device, unauthorized access is unlikely. A user can even simply switch his Bluetooth mode to a "non-discoverable" and avoids connecting with any other Bluetooth devices entirely. If a user makes the use of a Bluetooth network primarily for only synching devices at the home, this might be a good way to avoid the any chance of a security breach while in public.

IBM

IBM ICE (Innovation Centre for Education)

Wireless Networks (2 of 19)

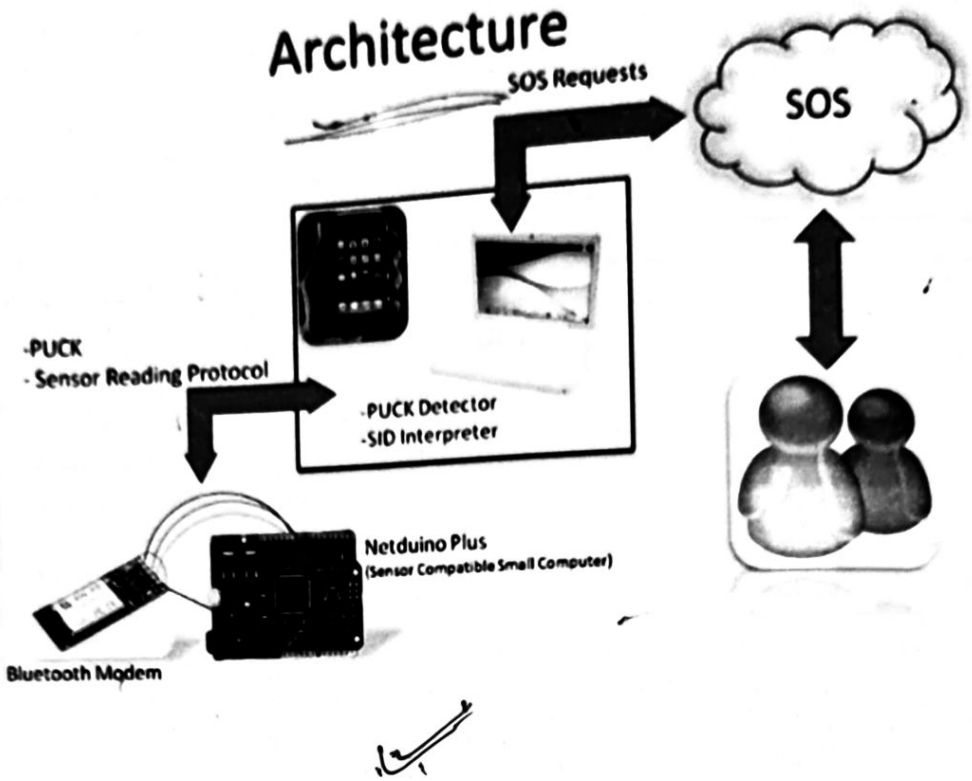


Figure 4-27. Wireless Networks (2 of 19)

Notes:

Still, early the cell-phone virus writers have taken advantage of the Bluetooth's automated connection process to send out the infected files. However, since most of the cell phones use a secure Bluetooth connection that requires an authorization and authentication before accepting data from an unknown device, of the infected file that typically doesn't get very far. When the virus is arrived in the user's cell phone, the user must have to agree to open it and then agree to install it. This has been so far stopped most cell-phone viruses from doing the much damage.

Other problems like "bluejacking," "bluebugging" and "Car Whisperer" have turned up as a Bluetooth-specific security issues. A Bluejacking involves Bluetooth users for sending the business card (just a text message, really) to the other Bluetooth users within a 10-meter (32-foot) of radius. If the user doesn't realize what the message is, he might even allow the contact to be added to his address book, and then the contact can send him messages that might even be automatically opened because they're coming from the known contact. Bluebugging is much problem, because it allows hackers to remotely access the user's phone and for using its features, including placing calls and sending the text messages, and so that the user doesn't realizes what is happening. A Car Whisperer is a piece of software that also allows hackers to send audio to and to receive audio from a Bluetooth-enabled car stereo. And like a computer security hole, these vulnerabilities are the inevitable results of technological innovation, and the device manufacturers are releasing firmware upgrades that address the new problems as they arise.

Blue tooth technology in IOT:-

PUCK over Bluetooth: The Open Geospatial Consortium (OGC) is an international industry consortium that has been supporting the geospatial interoperability since 1994, and has recently published a new standard, PUCK. PUCK is a standard defining a protocol for the RS232 and Ethernet connected instruments. Simply put, PUCK enables outside devices to access a sensor and including the sensor's datasheet, metadata, driver code and so forth. Bluetooth is a wireless technology standard which has an empowered devices to transfer data over short distances. By attaching a Bluetooth modem to the sensor, we can dramatically change our notion of the sensor networks. Since the Bluetooth modem transfers data to the serial port of the device its connected to, we can integrate a PUCK protocol, which was originally defined for communication over the cables, into Bluetooth. By combining the Bluetooth and PUCK, we have a standardized and automated way for the sensors to communicate wirelessly and real time. In summary, combining Bluetooth and PUCK has the following benefits:

- Sensor plug and play (very little or even no configuration is needed)
- Discoverable (sensors can even be discovered, paired and is consumed wirelessly)
- Flexible (the Bluetooth wireless capability allows users to install the sensors anywhere)
- Interoperable (based on the open and international standards)

For example, to implement PUCK over Bluetooth, select Netduino Plus as a sensor compatible of SBC (Single Board Computer) and BlueSMiRF Silver as a Bluetooth modem for the Netduino Plus. The user should first send a "GETCAPABILITIES" command to gather information about the sensors IDs, phenomenon IDs, and the unit of measurements. Next, the user sends a "GETREADING" command followed by the sensor ID and the number of readings which has been recorded on a device. These two commands and sensor description are defined in a SensorML file which is of a Sensor Interface Descriptor (SID) XML file recorded on the device memory.

Wireless Networks (3 of 19)

Figure 4-28. Wireless Networks (3 of 19)

Notes:

To describe a standardized wireless protocol for personal area networking or wireless personal area networking (WPAN) the term ZigBee is used. The protocol is the work of and property of the ZigBee Alliance, a consortium is of more than the 70 companies who have joined together to create and promote the new standard.

It has been designed to serve the diverse market of applications that require low cost, and low power wireless connectivity with more sophistication, this is the reason why the ZigBee is different from the other wireless standards. The standard focuses on low duty cycle connectivity and low data rate, a market segment not serviced well by existing standards. To afford interoperability between the devices manufactured by different companies a new protocol is promoted. It offers full wireless mesh networking capable for supporting more than 64,000 devices on the single network. It's been designed to connect the widest range of the devices, in any industry, into a single control network. ZigBee specification has the two implementation options or a Feature Sets: ZigBee and ZigBee PRO. The ZigBee Feature Set is been designed to support smaller networks with hundreds of the devices in a single network. The ZigBee PRO Feature Set is the most popular choice of the developers and specification is used for most Alliance developed ZigBee Feature Set, plus facilitates an ease-of-use and advanced support for the larger networks comprised of thousands of devices. Both Feature Sets are been designed to interoperate with each other, for ensuring long-term use and stability.

ZigBee is the hardware and software standard built on recently for ratified IEEE 802.15.4 standard. This important standard defines the hardware and software, which is been described in networking terms as a

physical (PHY), and the Medium Access Control (MAC) layers. The ZigBee Alliance has been added to Network (NWK) and application (APL) layer specifications to complete and it is called as a ZigBee stack.

The main characteristics of the ZigBee technology is

1. Global operation in the 2.4GHz frequency band according to the IEEE 802.15.4.
2. Regional operation in the 915MHz (Americas) and 868MHz (Europe).
3. Frequency agile solution is operating over 16 channels in the 2.4GHz frequency.
4. Incorporates power saving mechanisms for all the device classes.
5. Discovery mechanism with full application confirmation
6. Pairing mechanism with full application confirmation
7. Multiple star topology and inter-personal area network (PAN) communication
8. Various transmission options including broadcast Security key generation mechanism
9. Utilizes the industry standard AES-128 security scheme Supports Alliance standards (public application profiles) or the manufacturer specific profiles

Wireless Networks (4 of 19)

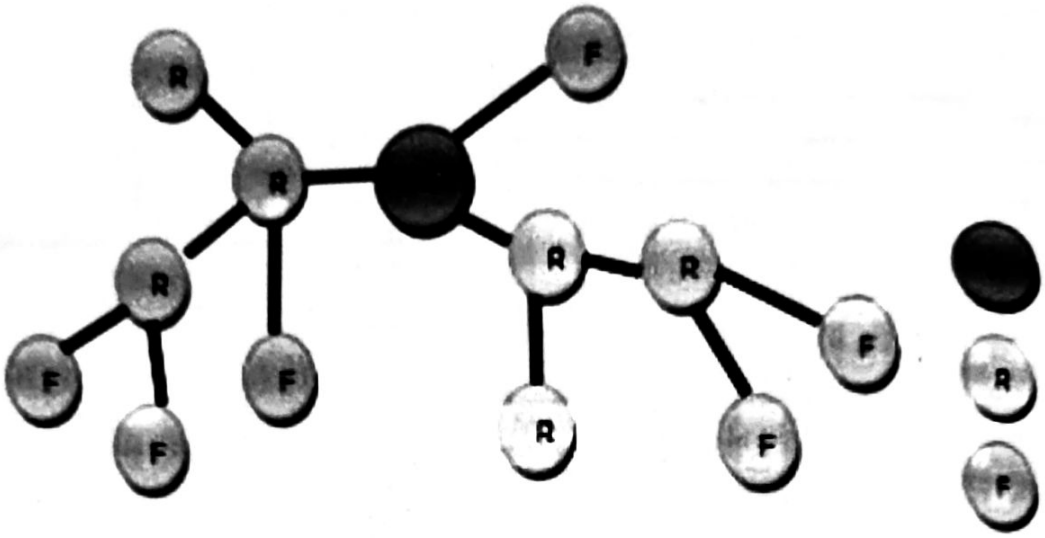


Figure 4-29. Wireless Networks (4 of 19)

Notes:

ZigBee Standard Devices Type:

There are two types of standard devices are available and can use in application such as lighting control, light sensor.

1. ZigBee logic Devices
2. ZigBee physical devices

ZigBee Logic Devices-

C- Coordinators

R-Routers

F- End devices

As shown in above figure there are 3 categorizes of nods in ZigBee system.

Router:

Router acts as the intermediate nodes, relaying data from other devices. Router can connect to an already existent network, is also able to accept the connections from other devices and be some kind of re-transmitters to the network. The Network may be extended through use of the ZigBee routers.

Coordinator:

There is exactly one coordinator in each network. It is also responsible for initiating the network and selecting the network parameters such as radio frequency channel, a unique network identifier and setting other operational parameters. It can also store the information about network, security keys.

End Devices:

End Device can be low-power /battery-powered devices. They can collect various information from the sensors and switches. They have sufficient functionality to talk to their parents (either the coordinator or a router) and cannot relay the data from other devices. This reduced functionality allows for the potential to reduce their cost. And they support better for the low power models. These devices do not have to stay awake for the whole time, while the devices are belonging to other two categories have to. Each end device can have up to 240 end nodes which are of separate applications are sharing the same radio.

Physical Devices:

Based on data processing capabilities, two types of the physical devices are provided in IEEE 802.15.4: Full Function Devices (FFD) and the Reduced Function Devices (RFD). Full Function Devices can perform all the available operations within a standard, including routing mechanism, coordination tasks and sensing task. The FFD plays a role of the coordinator or router or end devices (It can either be FFD or RFD depends on its intended application). A typical FFD in the ZigBee network will be powered from AC-fed mains supply, as it must always be and listening to the network. Reduced Function Devices, is on the other hand, implement a limited version of the IEEE 802.15.4 protocol. And the RFDs do not route the packets and must be associated with an FFD.

These are the end devices such as sensors actuators which are only doing limited tasks like recording the temperature data, monitoring lighting condition or controlling the external devices. The current ZigBee standard requires the FFDs to be always on, and in practice means that FFDs must be constantly powered. The Battery-powered FFDs have a lifetime on the order of a few days.

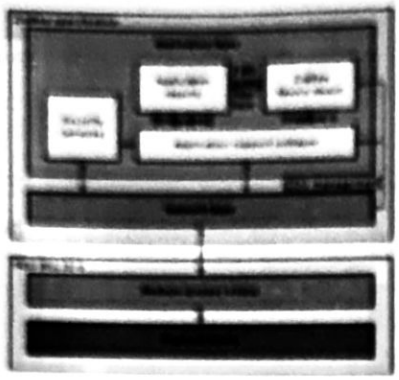
Access Modes:

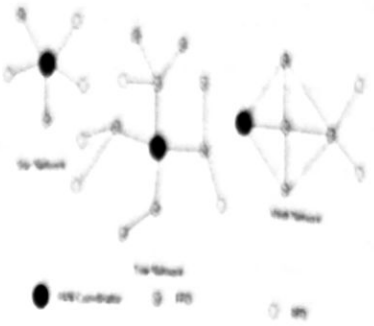
Two ways of multi-access in ZigBee protocol, are of Beacon and Non-beacon. In non-beacon enabled network, an every node in the network can send a data when the channel is free. In beacon enabled network, nodes can only transmit it in predetermined time slots. Here the PAN coordinator allocates a guaranteed time slots (GTS) for the each device; therefore devices will also transmit their data during their own slot. All the devices must get synchronized for this process. This can be achieved by sending a beacon signal. The coordinator is responsible to transmit the beacon signals and to synchronize the devices attached to it. Network in which the coordinator does not transmit the beacon signal is known as non-beacon network. It cannot have the GTS and contention free periods, because these devices are not synchronized. Battery life is better than the beacon enabled network, because the devices are wake up as less often.

Architecture of ZigBee Protocol:

As mentioned earlier 802.15.4 is important standard and it has Physical layer, MAC layer. Network and Application layer. The architecture and the functions of all layers are mentioned below.

Wireless Networks (5 of 19)





Network Layer:

Preamble	Start of packet Delimiter	PHY Header	PHY service data unit(PSDU)

Physical Layer;

Figure 4-30. Wireless Networks (5 of 19)

Notes:

The above figure shows the architecture of the ZigBee protocol.

Physical Layer:

The physical layer of IEEE802.15.4 standard it is closest layer to the hardware, which controls and communicate with the radio transceiver directly. And it handles all tasks involving the access to the ZigBee hardware, including initialization of hardware, a channel selection, link quality estimation, energy detection measurement and a clear channel assessment to assist the channel selection. Supporting three frequency bands, 2.45GHz band which using16 channels, 915MHz band which is using 10 channels and 868MHz band using a 1 channel. All three using Direct Spread Spectrum Sequencing (DSSS) access mode.

Physical Packet Fields;

1. Synchronization-preamble {32bits}
2. Start of packet Delimiter
3. PSDU length-PHY Header {8bits}
4. Data Field-PSDU {0 to 1016 bits}

MAC Layer:

This layer provides interface between the physical layer and network layer. This provides two services such as; MAC data services and MAC management service interfacing to the MAC sub Layer Management Entity

(MLME) Service Access Point called as (MLME-SAP). The MAC data service that enables the transmission and reception of the MAC protocol Data Units (MPDUs) across a PHY data service. The MAC layer is responsible for generating beacons and synchronizing devices to beacon signal in a beacon enabled services. It is also performing an association and dissociation function. It is defined as four frame structures, they are a Beacon frame, Data frame, Acknowledge frame, MAC command frame. Basically there are of two types of topology; star and peer to peer. The Peer to peer topology can take different shapes depends on its restrictions. The Peer to peer is also known as mesh, if there is of no restriction. Another form is tree topology. An Interoperability is one of the advantage of a ZigBee protocol stack. ZigBee has wide range of applications, so a different manufacturer provides the ZigBee devices. The ZigBee devices can also interact with each other regardless of the manufacturer (even if the message is encrypted).

Network Layer:

The Network layer interfaces between the application layer and MAC Layer. This Layer is responsible for the network formation and routing. Routing is the process of a selection of path to relay the messages to the destination node. This forms a network involving joining and leaving of the nodes, maintaining routing tables (coordinator/router), actual routing and address allocation. A ZigBee coordinator or router will perform the route discovery. And this layer Provides network wide security and allows the low power devices to maximize their battery life. From basic topologies, there are three network topologies which have been considered in IEEE802.15.4 are star, tree network and mesh.

Application Layer:

An application Layer is the highest protocol layer and it hosts the application objects. ZigBee specification separates an APL layer into three different sub-layers: the Application Support Sub layer, the ZigBee Device Objects, and Application Framework is having manufacturer defined Application Objects. The application objects (APO): Control and manages the protocol layers in the ZigBee device. It is a piece of software which controls the hardware. Each application objects assigned as unique end point number that the other APO's can use an extension to the network device address to interact with it. There can be up to 240 application objects in single ZigBee device. A ZigBee application must conform to an existing application profile which is from accepted ZigBee Alliance. An application profile defines message formats and protocols for interaction between the application objects. The application profile framework allows different vendors to independently build and sell ZigBee devices so that can interoperate with each other in a given application profile. ZigBee Device Object: The key definition of a ZigBee is the ZigBee device object, which addresses three main operations; service discovery, security and binding. The role of a discovery is to find nodes and ask about MAC address of coordinator/router by using unicast messages. This discovery is also facilitating a procedure for locating some services through their profile identifiers. So application profile plays an important role. The security services in this ZigBee device object have the role to authenticate and derive necessary keys for the data encryption. The network manager is implemented in the coordinator and its role is to select the existing PAN to interconnect. And it also supports the creation of new PANs. The role of binding a manager is for binding the nodes to recourses and applications also binding devices to channels.

Application support sub layer: Application Support (APS) sub layer provides an interface between the NWK and the APL layers through general set of the services provided by an APS data and management entities. The APS sub layer processes outgoing/incoming frames which are in order to securely transmit/receive the frames and to establish/manage the cryptographic keys. These upper layers issue primitives to the APS sub layer to use its services. The APS Layer Security includes the following services such as: Establish Key, Transport Key, Update Device, Remove Device, Request Key, Switch Key, Entity Authentication, and a Permissions Configuration Table. Security service provider: ZigBee provides a security mechanism for network layer and application support layers, each of which is also responsible for securing their frames. Security services include methods for the key establishment, key transport, frame protection and device management.

Wireless Networks (6 of 19)

Wi-Fi Technology

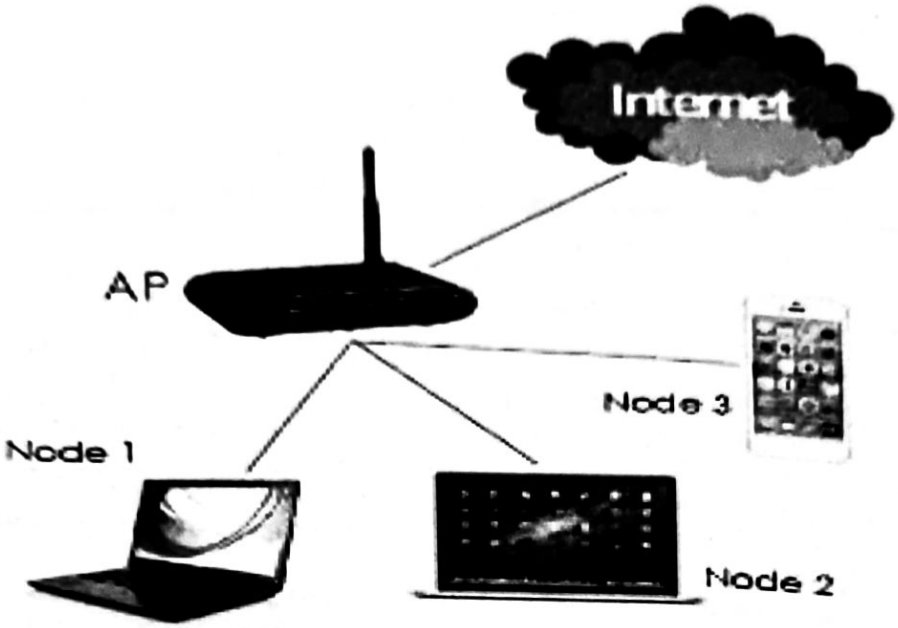


Figure 4-31. Wireless Networks (6 of 19)

Notes:

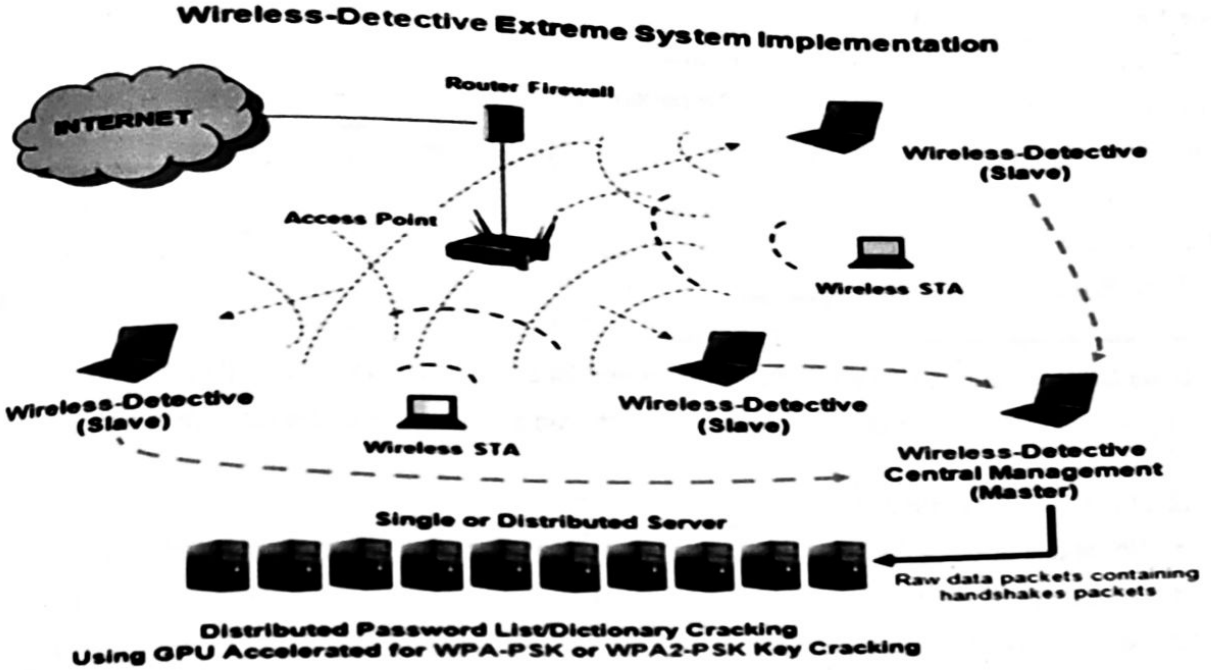
Wi-Fi is a Wireless technology that uses the radio frequency to transmit data through air. With the rise of a Wireless Fidelity (Wi-Fi), technology comes to rise of the hotspot public access Wireless Local Area Networks (WLANs) which allows anyone with a Wi-Fi capable notebook or a PDA to connect to the Internet or the corporate intranet in airports, hotels, coffee shops, or even campgrounds and the fast food restaurants. Wi-Fi hotspots are expected to have an important role in the future for provisioning of "anywhere, anytime" the connectivity. They are quickly being deployed at the locations that tend to attract the nomadic users, such as cafes, airports, hotels, and conference centres.

It contributes an alternative billing architecture for using *virtual prepaid tokens* (VPTs) and it experimentally evaluates its performance. The users buy VPTs at the point and time of access, using the third-party online payment server. Therefore, such an account is more flexible than the conventional pay-per-use account, which can be used only to purchase the access from a specific provider or a set of providers. Unlike physical prepaid tokens, VPTs allow a user to order and obtain the Internet access from a provider in less than the 15 s, even if a user has no previous or a subsequent relationship with that provider or the provider's aggregator. Simultaneous support for the captive-portal and 802.1x authentication allows hotspots to provide a recent Wi-Fi security improvement is to those clients whose configuration supports them, without disrupting the legacy clients. Improvements include mutual authentication between client and a hotspot and link-layer packet encryption and authentication with the dynamic per-session keys.Billing is often cited as a problem area that contributes to low hotspot utilization. The Existing billing methods have many drawbacks that turns away many potential users. Three of the most common methods are a subscription, pay-per-use account, and prepaid token.

Wireless Networks (7 of 19)

IBM

IBM ICE (Innovation Centre for Education)



IOT011.0

Figure 4-32. Wireless Networks (7 of 19)

Notes:

Even though subscriptions provide a steady revenue stream and convenience of the fixed price and single monthly payment to the user, Users may also be concerned about the provider reliability. Instead of a subscription, the users may set up a pay-peruse account with a provider. Pay-per-use accounts typically draw the funds automatically from one of the user's bank or the credit card accounts, when the user gains to access. Pay-per-use accounts can be less wasteful than the subscriptions to sporadic users. Moreover, a user may also occasionally need access in places that are not been served (directly or by agreement) by any of providers that serve areas more frequently visited by the user. In latter cases, the users may prefer prepaid tokens (PPTs). PPTs contain the id and password that are typically revealed by scratching the card and is activated after first use for a limited time. And a user does not need to set up any of the account to buy such a token; payment may be, e.g., by the cash or credit card. Prepaid tokens offer little risk to users. In many of the cases (e.g., at an airport), a vendor location may be inconvenient or not obvious. Moreover, a vendor location may be closed when the token is needed.

Experiments show that users arriving at a hotspot can buy a VPT and gain the full Internet connectivity in less than 15 seconds, it means much less time than it would take to buy and activate a physical token. VPTs can be used in the hotspots that employs a captive portal or 802.1x to authenticate users. Most current hotspots use the captive portal, but a 802.1x enables much better security. In particular, 802.1x enables mutual authentication between the user and hotspot and encryption keys at the link layer.

Wi-Fi Security Techniques

- Service Set Identifier (SSID)

- Wired Equivalent Privacy (WEP)
- 802.1X Access Control
- Wireless Protected Access (WPA)
- IEEE 802.11i

Service Set Identifier (SSID)

- SSID is been used to identify an 802.11 network
- It can be pre-configured or advertised in the beacon broadcast
- It is transmitted in to clear text
- Provide very little security

Wired Equivalent Privacy (WEP)

- Provide same level of the security as by wired network.
- Original security solution offered by the IEEE 802.11 standard.
- Uses RC4 encryption with a pre-shared keys and 24 bit initialization vectors (IV).
- Key schedule is generated by concatenating a shared secret key with the random is generated 24-bit IV.
- 32 bit ICV (Integrity check value).
  - No. of bits in key schedule is equal to a sum of length of the plaintext and ICV
- 64 bit preshared key-WEP
- 128 bit preshared key-WEP2
- Encrypt the data only between 802.11 stations. Once it enters into the wired side of the network (between access points) WEP is no longer valid.
- Security Issue with WEP
  - Short IV
  - Static key

- Offers a very little security at all

802.1X Access Control

- Designed as the general purpose network access control mechanism.

  -Not Wi-Fi specific

- Authenticate each client connected to an AP (for WLAN) or switch port (for Ethernet)
- Authentication is done with a RADIUS server, which "tells" the access point whether access to a controlled ports should be allowed or not
  - AP forces a user into an unauthorized state
  - user sends an EAP start message
  - AP return an EAP message requesting the user's identity
  - Identity is been send by user is then forwarded to the authentication server by AP.
  - Authentication server authenticate user and returns an accept message or reject message back to the AP.
  - If accept message is in return, the AP changes a client's state to authorized and normal traffic flows.

Wireless Networks (8 of 19)

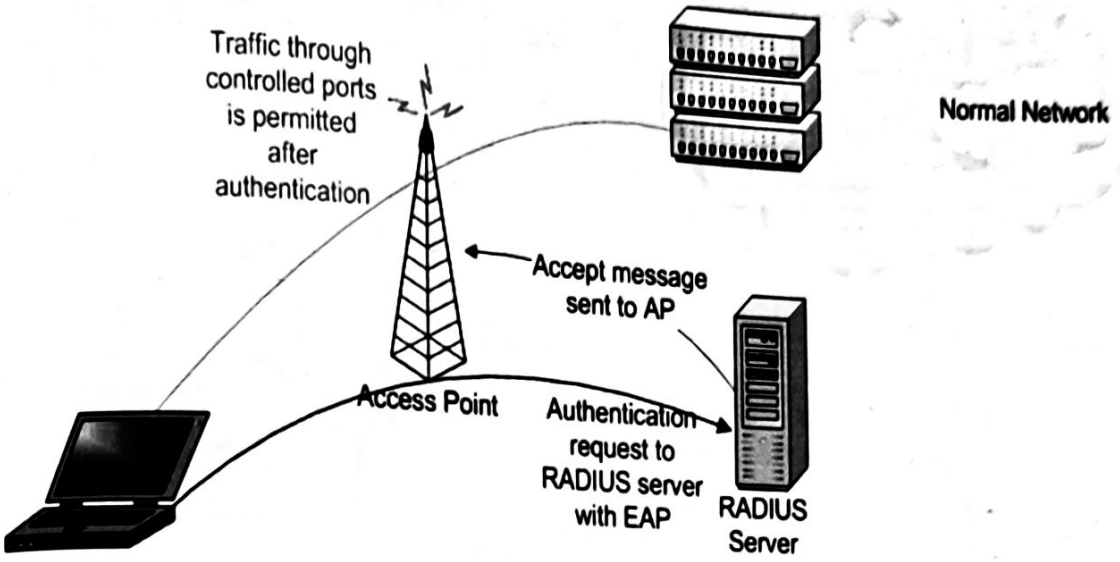


Figure 4-33. Wireless Networks (8 of 19)

IOT011.0

Notes:

Wireless Protected Access (WPA)

- WPA is specification of the standard based, interoperable security enhancements that strongly increase the level of a data protection and an access control for existing and future wireless LAN system.
- User Authentication
  - 802.1x
  - EAP
- TKIP (Temporal Key Integrity Protocol) encryption
- RC4, dynamic encryption keys (session based)
  - 48 bit IV
  - per packet key mixing function
- Fixes all the issues found from WEP
- Uses Message Integrity Code (MIC) Michael
  - Ensures data integrity
- Old hardware should be an upgradeable to WPA
- WPA comes in two flavors

- WPA-PSK
  - use pre-shared key
  - For SOHO environments
  - Single master key must be used for all users
- WPA Enterprise
  - For large organisation
  - Most secure method
  - Unique keys for the each user
  - Separate username & password for each user

Wireless Networks (9 of 19)

IBM

IBM ICE (Innovation Centre for Education)

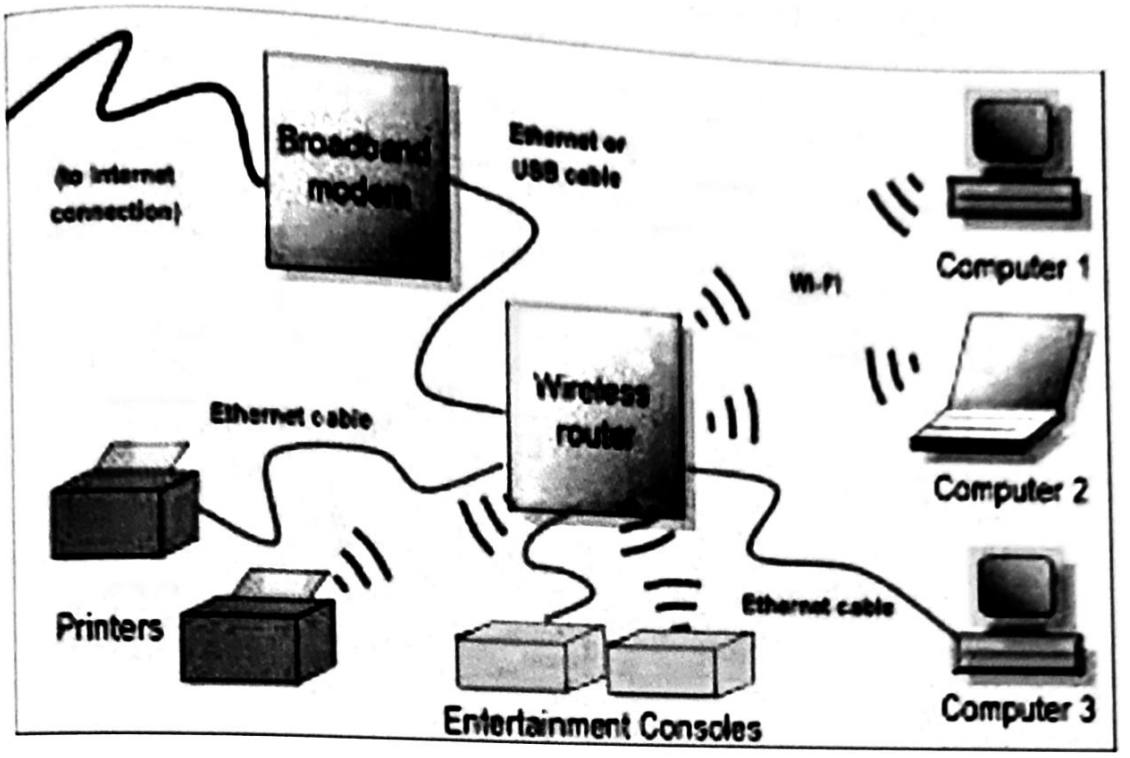


Figure 4-34. Wireless Networks (9 of 19)

IOT011.0

Notes:

How Wi-Fi Works?

To understand the wireless networking at its simplest level, think about a pair of walkie-talkies. These are a small radios that can transmit and receive radio signals. When someone talk into a Walkie-Talkie, theirr voice is picked up by the microphone, encoded onto a radio frequency and transmitted with the antenna. Another walkie-talkie can also receive the transmission with its antenna, decode the voice from the radio signal and drive a speaker. The two basic components of the Wi-Fi network or a computer device outfitted with a low-power radio and another radio-equipped gadget is known as an access point, which is wired to the Internet or a local network. The two communicates with each other over a free slice of a radio spectrum reserved for consumer use and inhabited by microwave ovens and cordless phones.

First of all the devices are called laptop or home pc or any network which want to access internet or connected to their network or to another office network. They want to insert wi-fi card which card give facilities to access wireless networking. They are firstly connected to the access point which gives the connection Gate to connect the internet after that than signals go to computer server which is been wired connected to the access point and computer server is connected to the internet server. Which provides the internet facilities to a computer or they are also using another office network through transmitter.

Now the question is that how they are converted signal to transmit data? In the small figure you saw that computer data combined with addressing and codes for the security. And this combined signals are send to transmitter and in the last antenna convert them into radio waves.

Wireless Networks (10 of 19)

AP-based topology

Figure 1-3 Typical WLAN

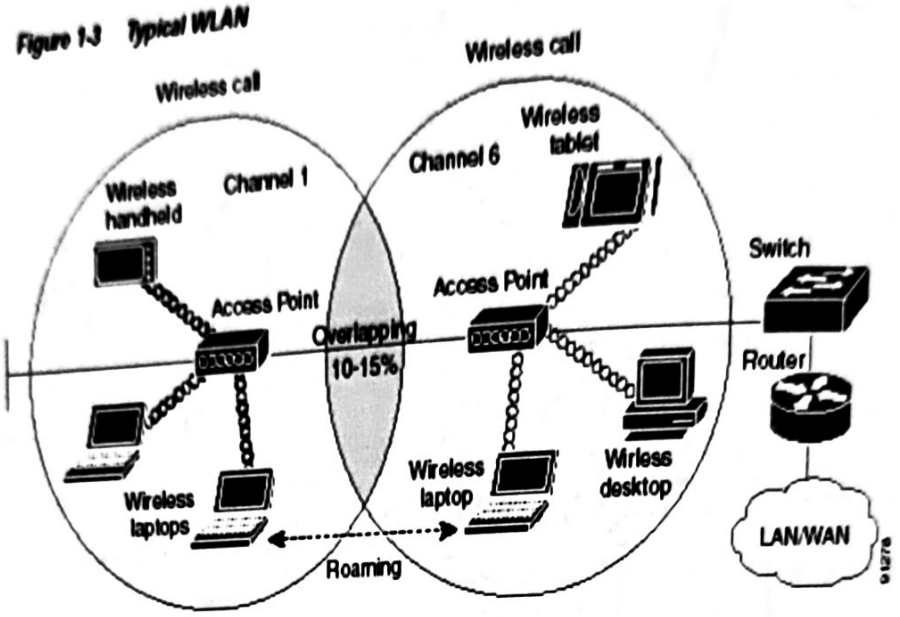


Figure 4-35. Wireless Networks (10 of 19)

Notes:

AP-based topology

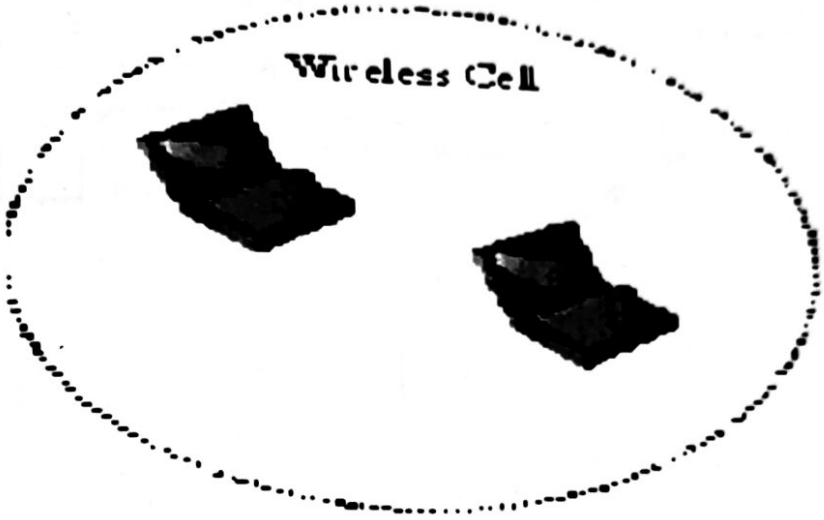
- The client communicates through an Access Point.
- BSA-RF coverage provided by an AP.
- ESA-It consists of a 2 or more BSA.
- ESA cell includes 10-15% overlap to allow roaming.

Wireless Networks (11 of 19)

IBM

IBM ICE (Innovation Centre for Education)

Peer-to-peer topology



IOT011.0

Figure 4-36. Wireless Networks (11 of 19)

Notes:

Peer-to-peer topology

- AP is not required.
- Client devices are within a cell and can communicate directly with each other.
- It is useful for setting up of the wireless network quickly and easily.

Wireless Networks (12 of 19)

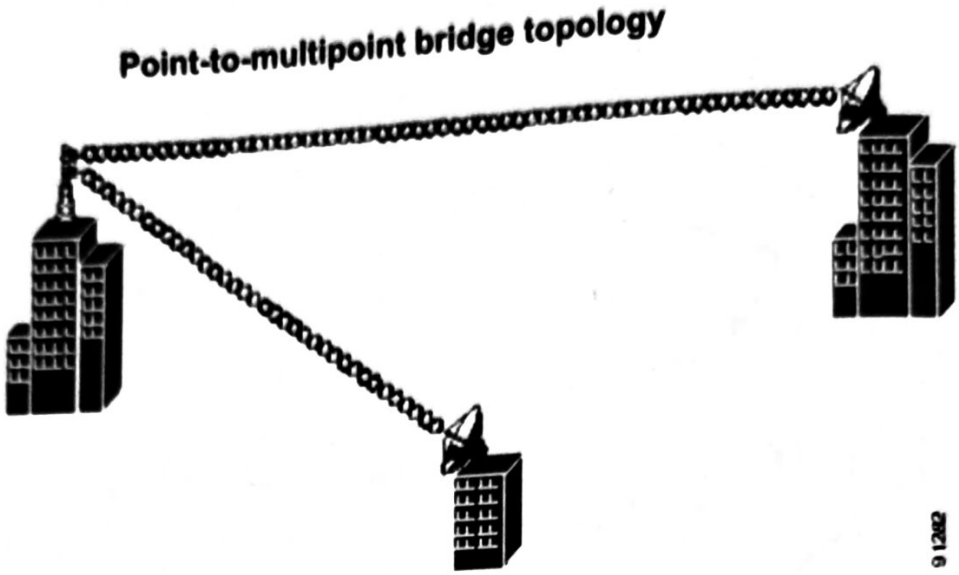


Figure 4-37. Wireless Networks (12 of 19)

Notes:

This is used to connect a LAN in one building to a LANs in the other buildings even if buildings are miles apart. These conditions receive a clear line of sight between buildings. The line-of-sight range varies is based on the type of wireless bridge and antenna used as well as the environmental conditions.

Advantages:

Flexible: With the wireless network you and your staff can have uninterrupted access to people, information and tools as you and they can move through the workplace with your mobile PC.

Responsive: As you change your business operations your wireless network can also change with you.

Customized: Your wireless network can be configured the way you want it can even combine with your current wired network.

Fast: From 11 to 54 Mbps throughput and advanced roaming capabilities and provide the reliable access to e-mail, the Internet, file sharing and other network resources are away from the desk.

Cost-effective: Expand and extend your existing network by simply adding more adapters and access points. Planning is of no brainer as you need to buy only what you need.

Secure: Current standards utilize 64-bit and 128-bit WEP encryption and helps to guard the network from intruders and protect data in transit. Add in technology and you have increased WLAN protection that is important for mission critical data.

In addition to the hard benefits of an increased efficiency, productivity, manageability and the cost savings, wireless networks will certainly make a Ëoe This is a technology savvy companyâ„¢ statement to the world.

Disadvantages

- Spectrum assignments and operational limitations are not consistent over worldwide.
- Power consumption is fairly high compared to the some other low-bandwidth standards.
- Wi-Fi networks have a limited range.
- Wi-Fi pollution, or an excessive number of an access points in the area, is especially on the same or neighbouring channel, can the prevent access and interfere with the use of other access points by others.

Limitations

- It has a limited bandwidth of about an 83.5 MHz.
- Frequency spectrum used by IEEE 802.11b is been shared by many other systems like microwave ovens, cordless phones etc. This frequency sharing causes the interference problem.
- Security techniques are not reliable yet.

Wireless Networks (13 of 19)

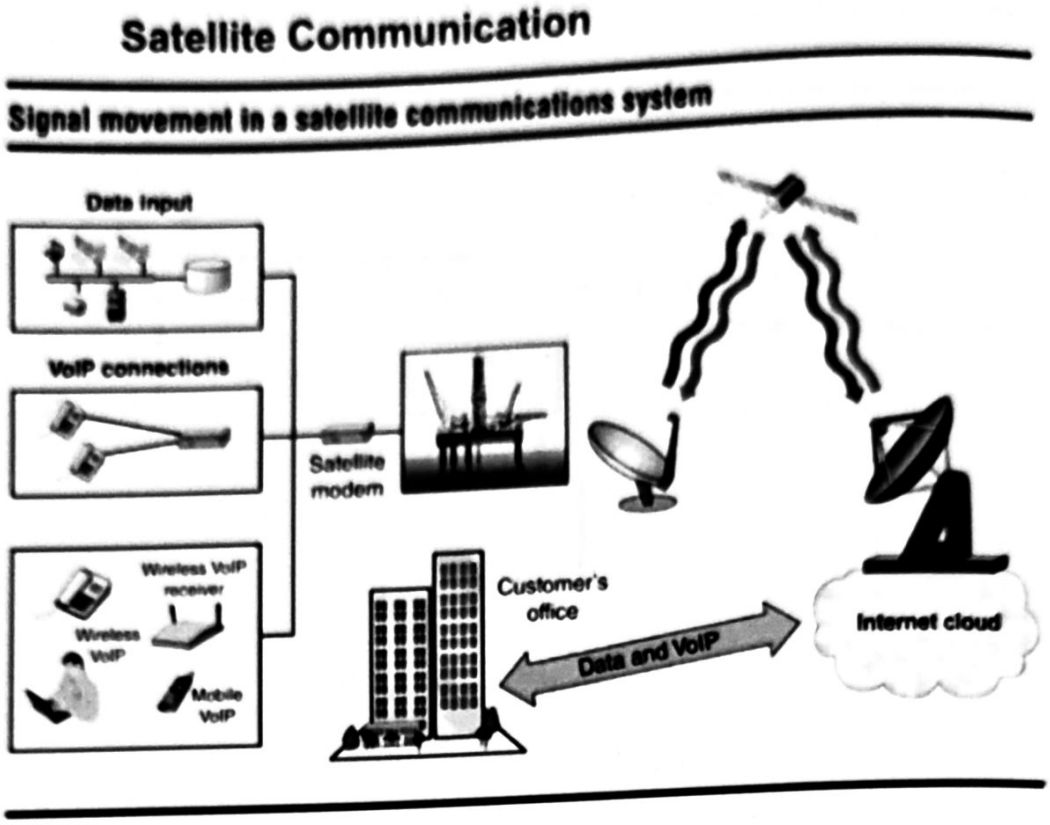


Figure 4-38. Wireless Networks (13 of 19)

Notes:

People need access to enterprise-class, a high-speed voice, video and data applications wherever they happen to be. Satellite connectivity is having power to drive the communications advance across the broad range of industries and geographies.

Whether it's ship-to-shore maritime communications, the Internet access for remote, rural classrooms, or vital data and communications for petroleum operations, the satellite applications meets a broad range of needs.

iDirect's communication platform enables any of the IP application to run reliably and efficiently over satellite.

iDirect's advanced technology provides organizations with immediate global reach by making mission critical communications possible in the most challenging and the diverse environments.

Communication satellites are used in a fixed or mobile wireless communications to receive and transmit radio signals from the orbiting satellite to another terrestrial location. There have been such advances in bandwidth utilization and reliability of the communications that satellite service now provide an affordable, always-on, high-speed, quality connectivity.

Global Coverage

In today's satellite communication can even deliver a terrestrial-grade experience with the voice, video, and data which can be accessed anywhere in the world. The Ubiquitous coverage can be obtained with a global network of the multiple satellites of all tying into one central network management system.

Reliability

Satellite networks are the dependable, providing a constant connectivity even when the terrestrial networks fail. With satellite networks, enterprises can even maintain business continuity with built-in redundancy and an automatic back-up service.

Security

Satellite networks already constitutes the private network. By adding encryption technology satellite can even provide more secure connection than the terrestrial networks, making it an ideal solution for the government, military and an enterprise VPN (virtual private network) solutions.

Scalability

The modularity of VSAT systems allows for a quick time-to-market and the fast upgrades. VSAT remotes can even be deployed rapidly and new remote locations are easily added to a network where the limited terrestrial infrastructure which exists simply by configuring bandwidth to the site and having a ground equipment installed.

Fast Deployment

Satellite technology is the ideal solution for a quick deployment, immune to the challenges are posed by the difficult terrain, remote locations, harsh weather, and terrestrial obstacles. In this the rapidly expanding market, and satellite allows a service provider to get to market quickly and efficiently and also provide an immediate connectivity in a disaster and the emergency relief scenarios.

Cost Savings

Satellite technology can deliver the communications infrastructure to areas where the terrestrial alternatives are of unavailable, unreliable or simply too expensive. Satellite allows the service providers to insure the scalability, profitability and maintaining the low operating expenses, while overcoming the lack of existing infrastructure.

How Satellite Works

A communication satellite is a satellite located in space for the purpose of the telecommunication.

There are three altitude classifications for the satellite orbits:

LEO-Low Earth Orbit

LEO satellites orbit are from 160-2000km above the earth, take approximately 1.5hrs for a full orbit and this only covers a portion of the earth's surface, therefore it requires a network or constellation of satellites to provide the global, continual coverage. Due to the proximity to Earth, the LEO satellites have a lower latency (latency is the time between the moment a packet is been transmitted and the moment it reaches to its destination) and require less amplification for the transmission.

MEO – Medium Earth Orbit

MEO satellites are located at above LEO and below GEO satellites and typically travel in an elliptical orbit over a North and the South Pole or in an equatorial orbit. These satellites are traditionally used for the GPS navigation systems and are sometimes used by the satellite operators for voice and for the data communications. MEO satellites require the constellation of satellites to provide a continuous coverage. Tracking antennas are needed to maintain link as the satellites move in and out of antenna range.

GEO – Geostationary Orbit

GEO satellites orbit at 35,786 km (22,282 mi) is above an equator in the same direction and is as speed as the earth rotates on its axis. This makes it appear for the earth station as fixed in the sky. The majority of a commercial communications satellites operate in this orbit; however it is due to the distance from the earth there is a longer latency.

Frequency Bands

There are four radio frequency bands of communication and military satellites operate within the:

C band – uplink 5.925-6.425 GHz; downlink 3.7-4.2 GHz

The C band can primarily use for voice and data communications as well as the backhauling. Because of its weaker power it requires the larger antenna, usually above 1.8m (6ft). However, due to a lower frequency range, it performs better under the adverse weather conditions on ground.

X band – uplink 7.9- 8.4 GHz, downlink 7.25 – 7.75 GHz

The X band is used mainly for the military communications and a Wideband Global SATCOM (WGS) systems. With relatively few satellites orbit are in this band, there is a wider separation between the adjacent satellites, making it ideal for Comms-on-the Move (COTM) of applications. This band is of less susceptible to the rain fade than Ku Band due to the lower frequency range, is resulting in a higher performance level under adverse to the weather conditions.

Ku band– uplink 14 GHz; downlink 10.9-12.75 GHz

Ku band is been used typically for the consumer direct-to-home access, a distance learning applications, retail and enterprise connectivity. The antenna sizes, are ranging from 0.9m -1.2m (~3ft), are much smaller than the C band because a higher frequency means that the higher gain can be achieved with small antenna sizes than C-band. The networks in this band are more susceptible to rain fade, especially in the tropical areas.

Ka band – uplink 26.5-40GHz; downlink 18-20 GHZ

Ka band is primarily used for the two-way consumer broadband and military networks. Ka band dishes can even be much smaller and typically range from the 60cm-1.2m (2' to 4') in diameter. Transmission power is much greater then compared to the C, X or Ku band beams. Due to the higher frequencies

Wireless Networks (14 of 19)

Energy Harvesting RF Networks

RF Harvesting Topologies-I

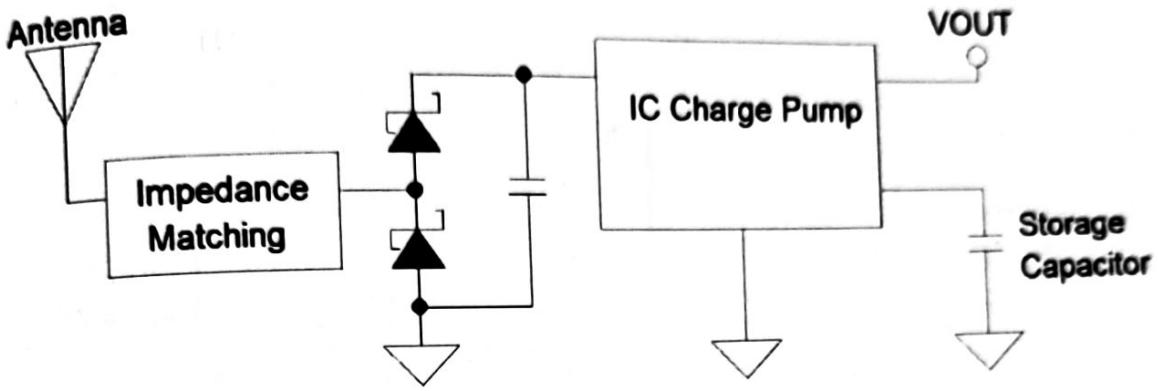


Figure 4-39. Wireless Networks (14 of 19)

Notes:

RF Harvesting Topologies-I

There are different RF harvesting topologies are available. Here we are mentioning two basic models;

The first type is a five-stage discrete Dickson RF charge pump implemented with Schottky barrier diodes. In this system it requires the external supervisory circuit to monitor the status of a storage capacitor and enable sensor node operation when the adequate charge has been collected. This supervisory circuit enables the node operation when the storage capacitor voltage reaches to 2.4V, and it disables operation at 1.8V, allowing the charge to recover.

Wireless Networks (15 of 19)

RF Harvesting Topologies-II

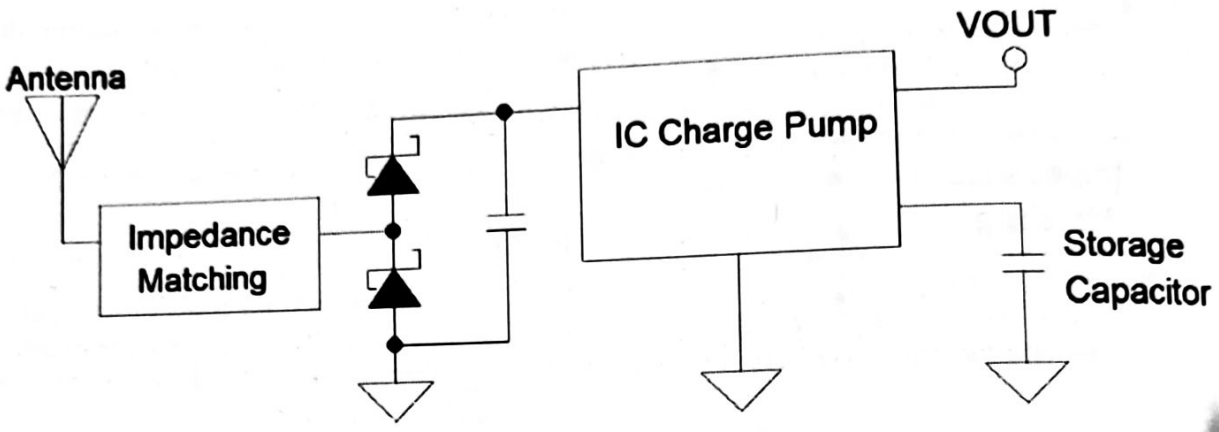


Figure 4-40. Wireless Networks (15 of 19)

IOT011.0

Notes:

The second type uses a discrete full wave rectifier (also with the Schottky barrier diodes) in conjunction with the low-voltage DC-DC integrated charge pump.

A single stage full wave rectifier is used for the RF-DC conversion and this low DC voltage is provided to charge pump IC (example - Seiko S-882Z IC), which has a voltage sensitivity of 300 mV. This IC is of internal voltage supervisor by which it disables the output while it is collecting charge, by behaving nearly identical to the Type 1 supervisory circuit is including the use of 2.4V (enable) and 1.8V (disable) thresholds.

Power-Optimized Firmware:-

A firmware has to develop for the sensor node which provides sensor polling and a minimal radio communication stack. Common sense of the low-power firmware practices were employed, such as by avoiding CPU-intensive math operations, eliminating the unnecessary array copies or the initialization, and keeping call stacks short. Additionally, low-power sleep modes of the microcontroller and radio is also employed whenever possible.

Wireless Networks (16 of 19)

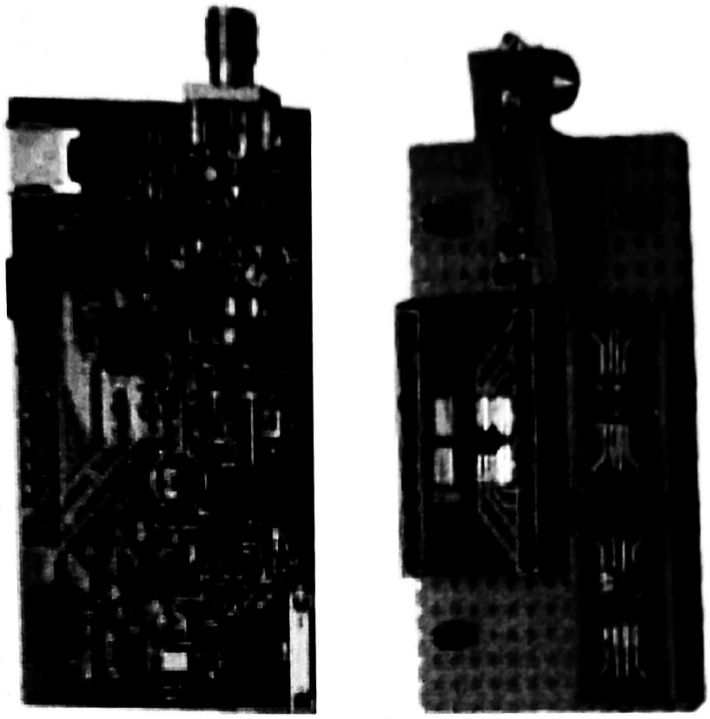


Figure 4-41. Wireless Networks (16 of 19)

Notes:

The two critical factors which have an impact on the practical usefulness of the RF harvesting sensor node are of operating sensitivity and per-operation energy. These are the two main optimization target is used during the design process.

Improve operating sensitivity: The minimum input power required for the operation depends on many factors, with one major factor being a magnitude of the quiescent current can even draw the storage capacitor and power management circuit during the charging state. In improving the sensitivity, it's also critical to minimize the leakage current of these devices.

Minimize operation energy: By reducing the amount of energy required to perform one Sense ? Process ? Transmit operation translates to more frequent operation and a better temporal resolution is in the collected data. Reducing the operation energy also allows for a smaller storage the capacitor value is to be used, lowering system cost and improving sensitivity and efficiency due to lower parasitic leakage of the smaller capacitors.

Most commonly used application is radio frequency identification tags in by which sensing device of wireless sends the radio frequency to a harvesting device which supplies just enough power to send back the identification information specific to an item of interest.

Energy Source	Classification	Performance (power density)	Weakness	Strength
Solar Power	Radiant Energy	100mW/cm^2	Require exposure to light, and low efficiency if device is in building	Can use without limit
RF Waves	Radiant Energy	0.02μW/cm^2 at 5Km from AM Radio	Low efficiency inside a building	Can use without limit
RF Energy	Radiant Energy	40μW/cm^2 at 10m	Low efficiency if out of line of sight	Can use without limit
Body Heat	Thermal Energy	60μW/cm^2 at 5°C	Available only when temperature different is High	Easy to build using Thermocouple
External Heat	Thermal Energy	135μW/cm^2 at 10°C	Available only when temperature different is High	Easy to build using Thermocouple

Figure 4-42. Wireless Networks (17 of 19)

Notes:

Other available Energy harvesting system for the Wireless sensors are: a solar power, electromagnetic energy, thermal energy, wind energy, salinity gradients, kinetic energy, biomedical, piezoelectric, pyroelectric, thermoelectric, electrostatic, blood sugar, tree metabolic energy. These can even be further classified into three: Thermal energy, Radiant energy, and Mechanical energy. Based on these, the above table is showing the comparison of the different and common energy scavenging techniques.

Wireless Networks (18 of 19)

Body Motion	Mechanical Energy	800μW/cm^3	Dependent on Motion	High power density, not limited on interior and exterior
Blood Flow	Mechanical Energy	0.93W at 100mmHg	Energy conversion efficiency is low	High power density, not limited on interior and exterior
Air Flow	Mechanical Energy	177μW/cm^3	Efficiency is low inside a building	High power density.
Vibrations	Mechanical Energy	4μW/cm^3	Has to exist at surrounding	High power density, not limited on interior and exterior
Piezoelectric	Mechanical Energy	50μJ/N	Has to exist at surrounding	High power density, not limited on interior and exterior

Figure 4-43. Wireless Networks (18 of 19)

Notes:

Beside the harvested energy for Sensor network, the consumption of a harvested power for the different mode of a network has to be look upon before choosing power harvesting source. A review of the some power consumption in some selected sensor nodes can be found in table below;

Wireless Networks (19 of 19)

Operating conditions	Manufactures			
	Crossbow MICAz [24]	Waspmote [25-26]	Intel IMote2 [27]	Jennic JN5139 [28]
Radio standard	IEEE 802.15.4/Zigbee	IEEE 802.15.4/Zigbee	IEEE 802.15.4	IEEE 802.15.4/Zigbee
Typical range	100m (outdoor), 30m (indoor)	500m	30m	1km
Data rate	250 kbps	250 kbps	250 kbps	250 kbps
Sleep mode (deep sleep)	15 µA	62 µA	390 µA	2.8 µA
Processor consumption	8 mA active mode	9 mA	31-53 mA	2.7+0.325 mA/MHz
Transmission	17.4 mA (+0 dBm)	50.26 mA	44 mA	34 mA (+3 dBm)
Reception	19.7 mA	49.56 mA	44 mA	34 mA
Supply voltage (Min)	2.7 V	3.3 V	3.2 V	2.7 V
Average power	2.8 mW	1 mW	12 mW	3 mW

Notes:

Computer connected to Internet

IBM

IBM ICE (Innovation Centre for Education)

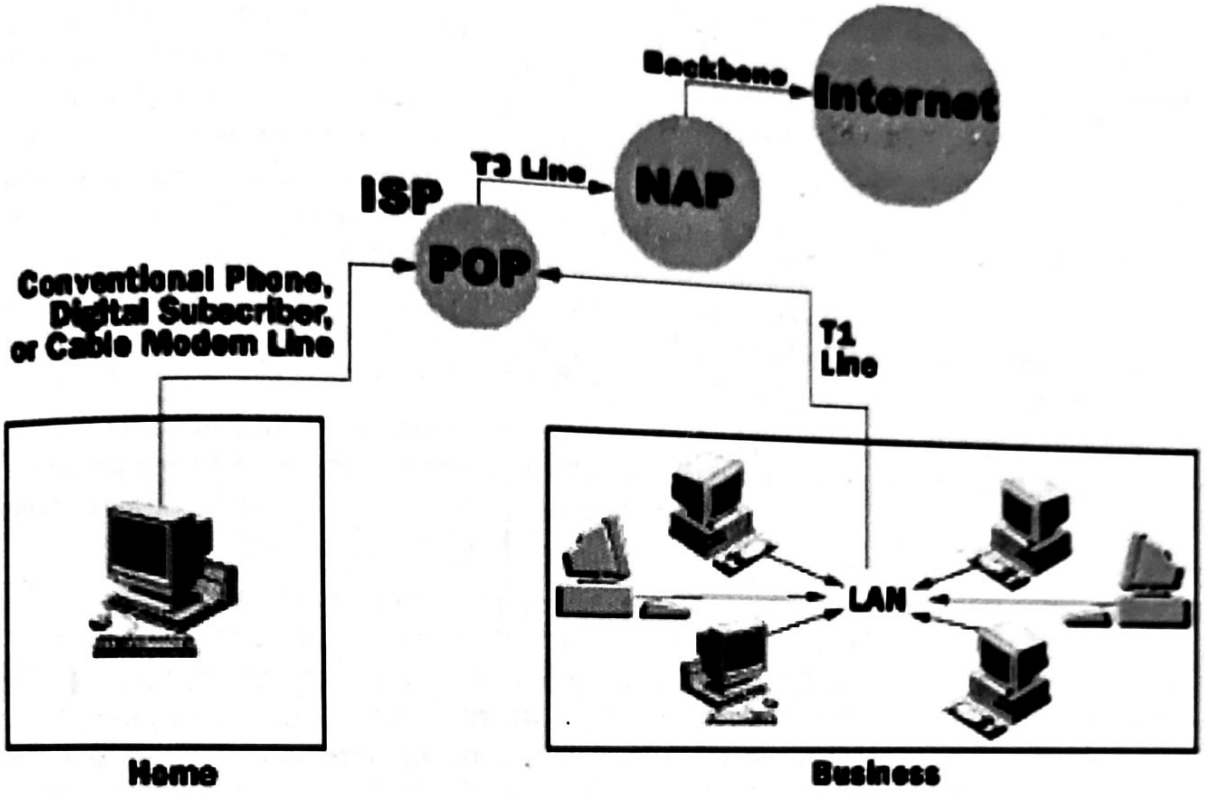


Figure 4-45. Computer connected to Internet

IOT011.0

Notes:

Communication between the computers started with an Electronic Data Interchange that made direct communication possible between two PCs. All the computers are connected to the Internet can even talk to each other. Use of mobile phones for connecting internet has been revolutionized the entire scenario. With Internet of Things the communication is extended via Internet among all the things that surround us.

Every computer that is connected to the Internet is part of a network, even the one in your home. For example, if you may use a modem and dial a local number to connect to an **Internet Service Provider** (ISP). At work, you may be a part of the **local area network** (LAN), but you most likely still connect to the Internet by using an ISP that your company has been contracted. When you connect to your ISP, you become part of their network. The ISP may even connect to a larger network and become part of their network. The Internet is simply a network of networks. Most of the large communication companies have their own dedicated backbones connecting various regions. In each region, the company has the **Point of Presence** (POP). The POP is a place for local users to access the company's network, and often through a local phone number or the dedicated line. The amazing thing here is that there is no overall controlling for network. Instead, there are the several high-level networks connecting to each other through **Network Access Points** or the NAPs.

IBM

Network Devices (1 of 2)

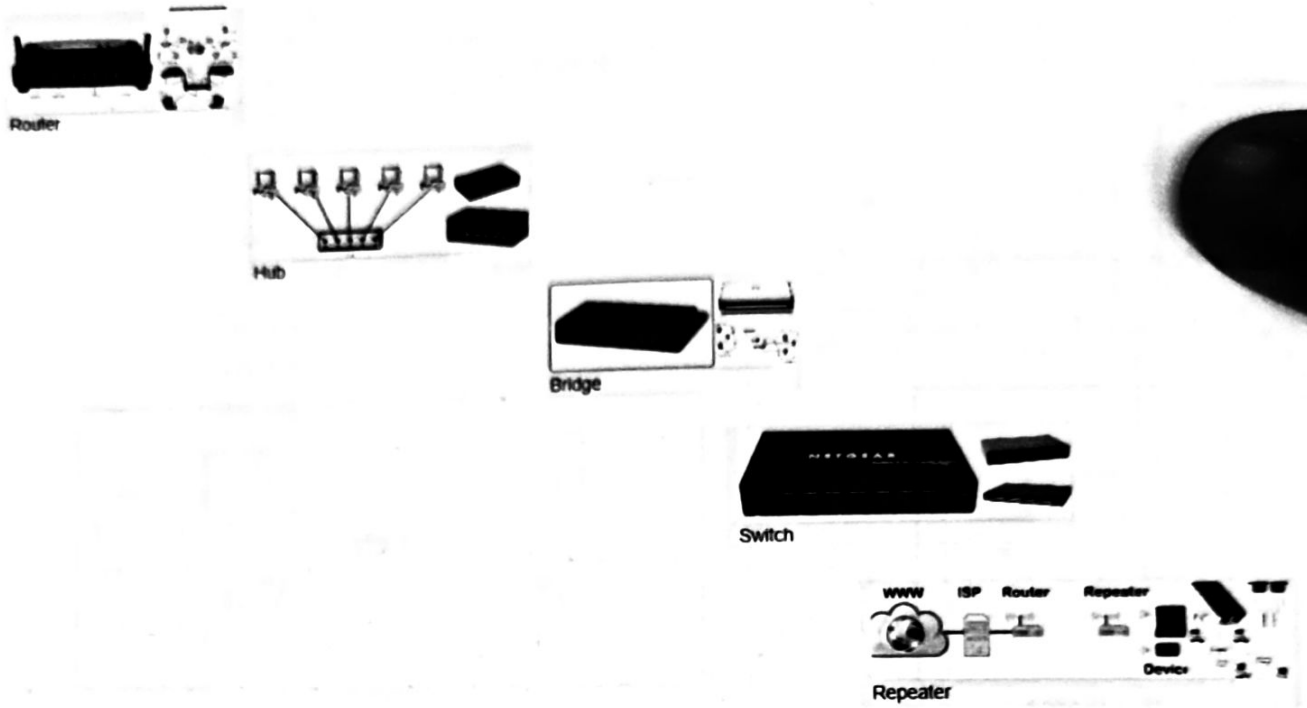


Figure 4-46. Network Devices (1 of 2)

IOT011.0

Notes:

- Network Devices:
- Hubs
- Switches
- Routers
- Gateways
- Firewalls

HUBS:

Hubs are simple network devices, and their simplicity is been reflected to their low cost. Small hubs with four or five ports (often referred to as work group hubs) cost is less than $50; with the requisite cables, they provide everything that is needed to create a small network. Hubs with more ports are also available for networks that require greater capacity. An example of a work group hub Computers connect to a hub through a length of twisted-pair cabling. In addition to the ports for connecting computers, even an inexpensive hub generally has the port designated as the uplink port that enables a hub that is to be connected to another hub to create the larger networks.

Most hubs are referred to as either the active or passive. *Active* regenerate a signal before forwarding it to all ports on the device and requires the power supply. Small workgroup hubs normally use an external power

adapter, but on a larger unit the power supply is built in. The *Passive* hubs, which are seen today are only on older networks, do not need any power and they don't even regenerate the data signal.

Regeneration of the signal aside, the basic function of a hub is to take the data from one of the connected devices and this is forwarded to all other ports on the hub. This method of the operation is inefficient because, in many cases, the data is been intended for only one of the connected devices.

Switches:

A *switch* is similar to a hub. Despite their similar appearance, the switches are far more efficient than hubs are far more desirable for the today's network environments. As with a hub, computers connect to a switch via a length of the twisted-pair cable. Multiple switches are often been interconnected to create larger networks. Despite their similarity is in appearance and their identical physical connections to the computers, switches offer significant operational advantages over the hubs. A hub forwards the data to all ports, regardless of whether the data is intended for the system connected to the port. Rather than forwarding a data to all the connected ports, a switch forwards data only to a port on which the destination system is to be connected. It looks at the Media Access Control (MAC) addresses of the devices connected to it to determine a correct port. A *MAC address* is a unique number that is stamped into every NIC. By forwarding data only to a system by which the data is addressed, the switch decreases the amount of traffic on each network link dramatically. In effect, the switch will literally channels (or *switches*, if you prefer) data between the ports.

Collisions occur on the network when these two devices attempt to transmit at the same time. Such collisions cause the performance of a network to degrade. By channeling a data only to the connections that should receive it, switches reduce the number of collisions that occur on a network.

As a result, the switches also provide significant performance and improvements over hubs. Switches can also further improve the performance over a performance of hubs by using a mechanism called *full-duplex.* On standard network connection, a communication between the system and the switch or hub is said to be *half-duplex*. In a half-duplex connection, the data can be either sent or received on the wire but not at the same time. Because switches manages dataflow on the connection, a switch can even operate in full-duplex mode it can send and receive the data on connection at the same time. In a full-duplex connection, the maximum of data through put is double that for the half-duplex connection for example, if 10Mbps becomes 20Mbps, and100Mbps becomes 200Mbps. As you can imagine, the difference in performance between the 100Mbps network connection and a 200Mbps connection is also considerable.

Switches use three methods to deal with the data as it arrives:

Cut-through: In the cut-through configuration, the switch begins to forward the packet as soon as it is been received. No error checking is performed on the packet, so packet is moved very quickly. The downside of cut-through is because of the integrity of a packet which is not been checked, and the switch can propagate errors.

Store-and-forward: In the store-and-forward configuration, the switch waits to receive an entire packet before beginning to forward it. It also performs the basic error checking.

Fragment-free: By building the speed advantages of cut-through switching, fragment-free switching works on by reading only the part of the packet which enables it to identify fragments of a transmission.

Routers:

Routers are an increasingly common sight in any of the network environment, from a small home office that uses one to connect the Internet service provider (ISP) to a corporate of the IT environment where racks of routers manage the data communication with disparate remote sites.

Routers make the internet working possible, and in view of this, they warranty the detailed attention. Routers are network devices that will literally route data around the network. By examining the data as it arrives, a router can even determine the destination address for the data; then, by using the tables of defined routes, the router determines a best way for the data to continue its journey.

Unlike bridges and switches, also use the hardware-configured MAC address for determining the destination of the data, routers use the software-configured network address to make the decisions. This approach makes the router more functional than bridges or switches, and it also makes them for more complex because they must work harder to determine the information.

The basic requirement for a router is it should have at least two network interfaces. If they are of LAN interfaces, the router can even manage and route information between the two LAN segments. More commonly, a router is used to provide the connectivity across wide area network (WAN) links.

Routers rely on two types of network protocols to make the routing

Routable Protocols and the Routing Protocols:

Routable Protocols:

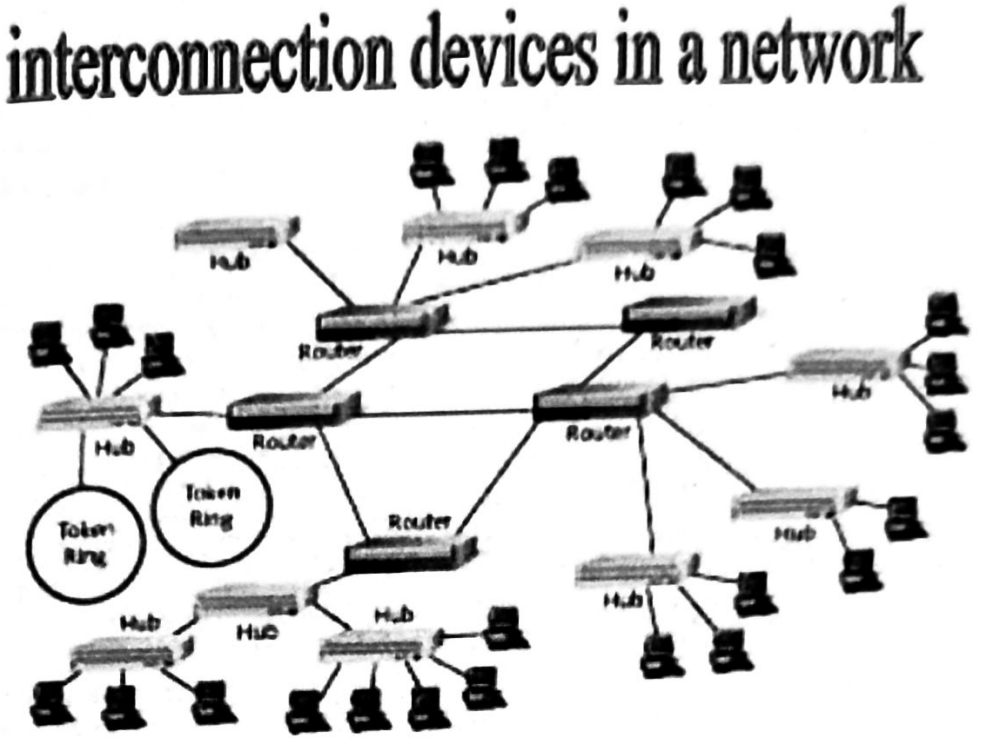
Large internet works need protocols that allow the systems to be identified by the address of a network to which they have been attached and by an address that it can uniquely identify them on that network. The network protocols which provides both of these features are said to be routable. Three routable LAN network protocols are available.

Transmission Control Protocol/Internet Protocol (TCP/IP): TCP/IP was developed in the 1970s by the Department of a Defense, which it needs a protocol to use on its WAN. TCP/IP's flexibility, durability, and functionality meant that it has soon became the WAN protocol of choice and also became the standard for LANs most of the networks use TCP/IP in some of the fashion, even if the main LAN protocol is something other than TCP/IP. Working with TCP/IP," provides complete coverage of a TCP/IP.TCP/IP is a protocol suite comprised of numerous individual protocols. Within TCP/IP, the two routing protocols used over here are the Routing Information Protocol (RIP) and Open Shortest Path First (OSPF). RIP is the distance-vector routing protocol, and the OSPF is a link-state routing protocol.

Network Devices (2 of 2)

IBM

IBM ICE (Innovation Centre for Education)



IOT011.0

Figure 4-47. Network Devices (2 of 2)

Notes:

Internet work Packet Exchange/Sequenced Packet Exchange (IPX/SPX):

It is created by Novell for use on NetWare networks, IPX/SPX is the routable protocol that was popular for many years. Today, even the Novell acknowledges that TCP/IP is the network protocol of a choice and so has to be moved away from IPX/SPX and toward the pure TCP/IP environment. In fact, the last few versions of a Novell NetWare have used the TCP/IP as the default protocol and allowed the IPX/SPX is to be enabled if needed.

Like TCP/IP, IPX/SPX is also the protocol suite. Within IPX/SPX, by the Net Ware Link State Protocol (NLSP) and the Routing Information Protocol (RIP) manage routing. RIP uses the distance-vector route-discovery method, which calculates the routes based on the number of hops. The NLSP uses a link-state route discovery method to build the routing tables.

AppleTalk: AppleTalk is a full-featured protocol is designed to be used with the Macintosh computer systems. AppleTalk which has been around since the early 1980s and is been widely deployed in Apple networks. Like TCP/IP and IPX/SPX, AppleTalk is the protocol suite. Within the suite, a Routing Table Maintenance Protocol (RTMP) provides the routing functionality. RTMP is the distance-vector routing protocol is similar to the RIP, and which is used by IPX/SPX and TCP/IP.

Routing Protocols:

- Two types of Routing Protocols are available they are
- Link State Protocol

- Distance Vector Protocol

Distance-Vector Protocols

With the distance-vector routing protocols, each router communicates with all the routes it knows about to all other routers to which it is been directly attached (that is, with its *neighbors*). Because each router in the network knows only about the routers to which it is been attached, but it doesn't know how to complete the entire journey; instead, of it knows only how to make the next hop. *Hops* are the means by which a distance-vector routing protocols determine the shortest way to reach the given destination. Each router constitutes the one hop: so if a router is four hops away from another router, there are three routers, or the hops, between itself and the destination. Distance-vector protocols can also use a time value known as a *tick*, which it enables the router to make a decision about which path is quickest if choice is given than more than one (a common situation on networks with the redundant links).

The frequency with which routers have to send route updates it depends on the routing protocol is being used, but it is usually between 10 and 60 seconds. At every update, the entire routing table of the sender is been sent to other connected routers. When the other routers receives the information, and they check it against the existing information if there are any of the changes, they alter through their routing tables accordingly. This constant update cycle is one of the problem of the distance-vector routing protcols because it can lead to the large amounts of network traffic. Furthermore, after such an initial learning period, the updates must (hopefully) be irrelevant the chances of the network topology is changing for every 30 seconds or so are slim, and that type of network, some troubleshooting maybe in order.

When a change does occur on the network, it may take some time for all the routers to learn of the change. The process of an each router is learning about the change and updating its routing tables is known as *convergence*. In a small network, the convergence might not take long; but in larger networks, those with, say, more than 20 routers, it might take some time to complete.

Rather than cause of routers to wait for the updates, it can configure triggered updates, which are sent when a topology change is been detected. Using triggered updates can significantly improve the convergence speed of distance-vector–based networks hold-down timers are used to improve convergence. A hold-down timer prevents a router from trying to make too many changes and too quickly. When a router receives a change about a route, it makes the change and then applies a hold-down timer to change. The hold-down timer will prevent the further changes from being made to that route within the defined time period. Hold-down timers are been particularly useful when an unreliable router keeps going on and off the network. If hold-down timers are not been applied, updates to the routing tables on routers would continually be changing, and the network might never converge.

Link State Protocol:

A router that uses a link-state protocol differs from a router that it uses a distance-vector protocol because to build a map of the entire network and then holds that map in the memory. On a network that uses a link-state protocol, so that routers can send out link-state advertisements that contain information about what type of networks they have been connected to. The LSAs are sent to every router on the network, thus enabling the routers to build up their complete network maps. When the network maps on each router are complete, the routers will update each other at a given time, it is just like with a distance-vector protocol, but the updates occur much less frequently with the link-state protocols than with the distance-vector protocols. The only other circumstance under which updates are sent is a change in the topology is been detected, at which point the routers must use LSAs to detect the change and update their routing tables. This mechanism, is combined with the fact that the routers hold the maps of entire network, makes convergence on a link state based network that occur very quickly.

Although it might seem to be like link-state protocols are an obvious choice over the distance-vector protocols, routers on a link-state based network require the more powerful hardware and more RAM than on the distance-vector–based network. Not only doing the routing tables and also have to be calculated, but they must even be stored. A router that uses distance-vector protocols need only to maintain a small database of the routes are accessible by the routers to which it is directly connected. A router that uses the link-state protocols that must maintain a database of the routers in the entire network.

Two of the most popular link-state of routing protocols are the Open Shortest Path First (OSPF) and NetWare Link State Protocol (A.K.A NetWare Link Services Protocol) (NLSP). The former is been used on TCP/IP networks, and the latter is used on networks that use IPX/SPX.

A router can be either the dedicated hardware device or a server system that has at least two network interfaces installed in it. And all common network operating system offers the capability to act as routers which are part of their functionality. Dedicated hardware routers also offer greater performance levels than server-based solutions, but they have such disadvantage of offering a limited range of the features for their cost.

The following are some of the advantages of a dedicated hardware routers:

1. Typically faster than server-based routers.
2. Generally more reliable than server-based routers.
3. Easier to harden against the attacks than server-based routing solutions.

The following are some of the disadvantages of a dedicated hardware routers:

1. More expensive than server-based router solutions extra functionality must have to be purchased.
2. Often require specialized skills and knowledge to manage them.
3. Limited to a small range of possible uses.

The capabilities of a router depend on the features it has. The basic router may route only one of the protocol between two network interfaces of the same type. A more advanced router may even act as a gateway between the two networks and two protocols. In addition, it may offer the firewall services, security and authentication, or remote access functionality such as the virtual private networking.

Gateways:

The term gateway is been applied to any device, system, or software application that can also perform the function of translating the data from one format to another. The key feature of a gateway is that to convert the format of data, not even the data itself.

The functionality of the Gate ways are in many ways a router that can route data from an IPX network to an IP network is, also technically, a gateway. The same can be used for translational bridge that, as described earlier in this chapter that it converts from an Ethernet network to the Token Ring network and back again. Software gateways can be found everywhere. Many of the companies use an email system such as Microsoft Exchange or Novell GroupWise. These system transmits the mail internally in a certain format. When email is needed to be sent across the Internet to users by using a different email system, the email must be even converted to another format, usually to the Simple Mail Transfer Protocol (SMTP). This conversion process must be performed by a software gateway.

Another good (and often is used) example of a gateway which involves the System Network Architecture (SNA) gateway, of which it converts the data format which is used on a PC to that used on an IBM mainframe or the minicomputer. A system that even act as an SNA gateway which sits between the client PC and the mainframe and also translates requests and replies from both directions. The function of a gateway is very specific, but how the gateway functionality is been implemented is not. No matter what they use, but gateways slow the flow of data and can therefore potentially become the bottlenecks. The conversion from one data format to another data it takes time, so the flow of data through a gateway is always slower than the flow of data without one.

A Channel Service Unit/Data Service Unit (CSU/DSU) acts as the translator between the LAN data format and the WAN data format. Such type of conversion is necessary because technologies used on WAN links are different from those used on LAN. Some consider a CSU/DSU as a type of a digital modem but unlike a normal modem, which changes the signal from digital to analog, the CSU/DSU changes the signal from one digital format to another.

Firewalls:

Firewalls are an essential part of the network's design. A *firewall* is the networking device, either hardware or software based, that can even control access to your organization's network. Thus the controlled access is

designed to protect data and resources from the outside threat. To do this, firewalls are been typically placed at entry/exit points of a network. For example, a firewall might be placed on between an internal network and the Internet. After the firewall is in place, it can even control access in and out of that point. Although the firewalls typically protect internal networks from public networks, they are also been used to control the access between specific network segments within a network. For example, place a firewall between the Accounts Department and a Sales Department. As mentioned, firewalls can be implemented through a software or through the dedicated hardware device. The Organizations implement software firewalls through the network operating systems (NOS) such as a Linux/Unix, Windows servers, and a Mac OS servers. The firewall is configured on the server to allow or to permit the certain types of network traffic. In the small offices and for regular home use, the firewall is commonly been installed on the local system and configured to control the traffic. Many third-party firewalls are available.

Hardware firewalls are used in networks for all the sizes today. Hardware firewalls are often a dedicated network devices and these can be implemented with very little configuration and protects all the system behind it from outside sources. Hardware firewalls are readily available and are often combined with the other devices today. For example, many broadband routers and wireless access points have the firewall functionality built in. In such a case, the router or WAP may even have a number of ports available to plug systems into.

Device Configuration and Management

IBM

IBM ICE (Innovation Centre for Education)

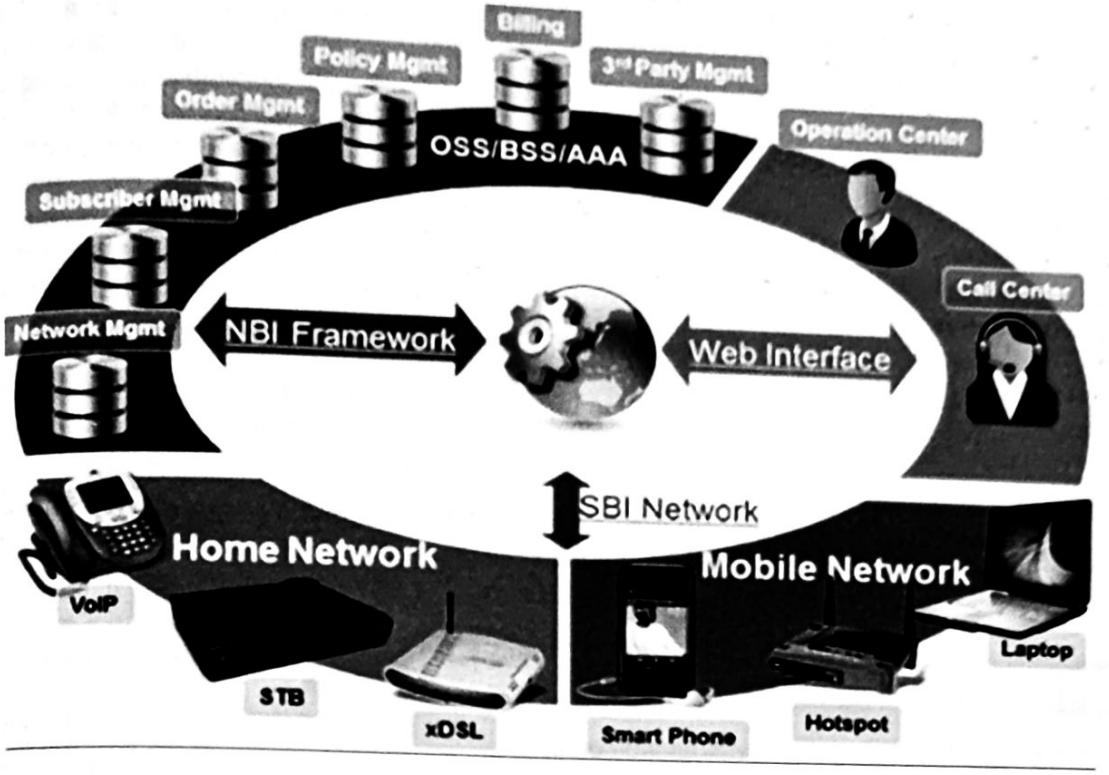


Figure 4-48. Device Configuration and Management

IOT011.0

Notes:

Connectivity is a way of life that drives expectations of real-time, convenience-driven automation.

Those expectations are propelling the advances in connected cars, home automation, mobile health and a variety of vertical industries, all enabled by transformations in machine-to-machine (M2M) communications.

Device on boarding encompasses several tasks that are essential to the M2M solutions, by including interoperability testing (IOT), provisioning and firmware upgrades. Today, M2M device on boarding often involves the complex manual processes that drives up the cost and increase the likelihood of errors. The prevailing practice is to tailor the applications to capabilities of their specific devices. This approach ties applications to devices and makes it difficult to mix and match with old and new devices. In mainstream the consumer world, we can see increasing standardization and consolidation of the device capabilities and the applications that can run on a wide range of devices. To bring the M2M to mainstream, the industry must consolidate a protocol choices and use this consolidation to create the streamlined IOT processes that can characterize the devices and their capabilities. These processes must even allow the consumers and operators to use the devices of their choice and without having to engage in custom testing or multiple iterations.

Network operators have home and the mobile device management expertise that can help reduce the complexity which is associated with the M2M fragmentation and device on boarding. Each year, they add and upgrade support for hundreds of consumer devices and activate millions of the device instances on their networks in a highly reliable and secures fashion. In doing so, they can navigate and manage a diverse set of the standards and device-specific protocols. The knowledge they gain in performing the activities is readily

applicable to the M2M applications. The path to broader the M2M success which lies in bringing this device management expertise to M2M-specific functions. The Network operators has a clear opportunity to encourage the shift toward a more scalable of M2M business model. The addition of support for the M2M device management functions are such as provisioning, configuration, firmware upgrades and the analytics will give operators the means to scale and streamline the M2M operations and reduce support costs.

An operator can benefit in several key ways by complementing to its network connectivity capabilities with standards-based device management as the service is offering. For instance, an operator can even gain the better understanding of what types of devices are attached to the network and how these devices use the connectivity. This knowledge will enable the operator to manage its network more effectively. A standards-based platform can even support the end-to-end service assurance and also device diagnostic capabilities, both of which will help the operator to troubleshoot the problems and provide meaningful service level agreements (SLAs) to the customers. Moreover, standards-based solutions can even empower an operator to bring much more devices under management. Since the unmanaged devices are untrusted by definition, the ability for managing more devices will help the operator to secure and retains the trust of more consumers and enterprises. Standards will also allow operator to adapt the behavior of generic devices to meet the needs of a specific verticals. This will reduce the needs for the customized devices and allow the operator to reach to a broader customer base. Open APIs can even add to the benefits which are offered by standards. By embracing open APIs, an operator can gain the ability to offer ready access to useful the data and support common service and the application lifecycle management functions. These new capabilities will increase their value to certain enterprises, governments and the M2M industry as a complete system.

Number of platforms are available in the real time world for this M2M device management here is the example of some M2M platforms are explained.

Examples are given below;

Mformation's machine-to-machine device management solution IMPACT:

- Mformation IMPACT Service Manager
- Open Mobile Alliance (OMA) standards-based server
- In-network installation or cloud-hosted solution
- Multi-tenant architecture with hardened partitions
- Scalable support for hundreds of millions of endpoints on a single instance
- Robust administration interface with scheduling and reporting
- Automatic detection of devices as they attach to the network
- Progressive view of actions, messages, and transactions
- Automated notification system
- Restful Web-services APIs for easy integration
- Free form addressing allows devices to be addressed with IP or phone number
- Mformation IMPACT Gateway
- Supports Lightweight M2M
- Adaptive Layer to address non-standard devices
- Manages standards translation
- Support for standard and non-standard protocols

Exchange Information without human Intervention

IBM

IBM ICE (Innovation Centre for Education)

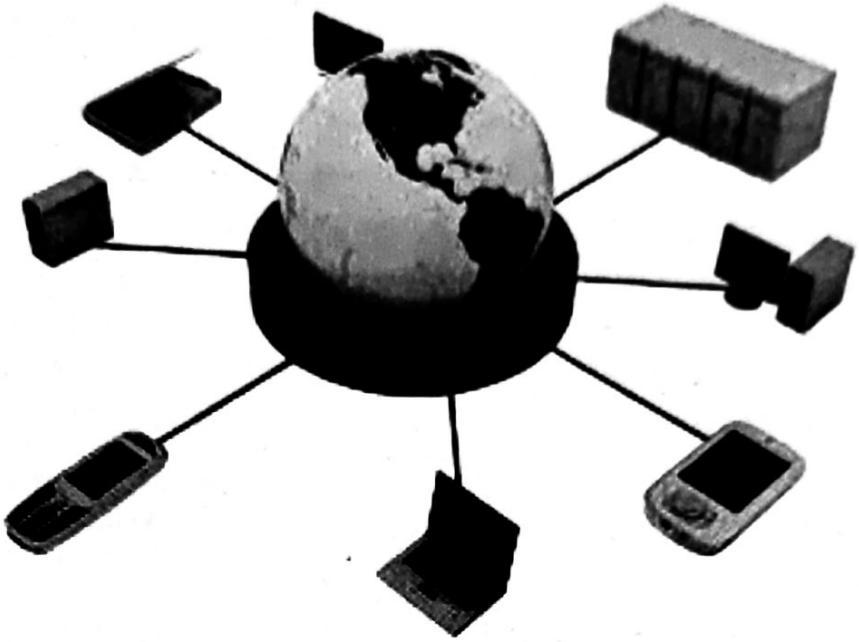


Figure 4-49. Exchange Information without human Intervention

IOT011.0

Notes:

Electronic Data Interchange-

The direct exchange of information from one computer to another without human intervention. For example; a buyer computer can place an order automatically when stock levels get low and the sellers computer can process the order, issue invoice and arrange delivery.

It is recommended for the organizations to automate with the exchange of orders, invoices and shipment information with their trading partners it is difficult to transform information quickly. For some businesses, due to the volume of information and complexity it is extremely very difficult to participate in the B2B automation process. Some companies needlessly spend resources manually mailing or by emailing the PDFs to their customers rather than integrating directly between systems.

PDF documents can be difficult or even for time consuming to retrieve the necessary information by software without the human intervention and also when processing into your back office system. By manually processing and adjusting documents create the additional expenses, time and errors. With" **Smart PDF Connect"** customers are been able to process, translate and integrate the PDF documents automatically with back office system with the 100% accuracy, regardless of the ERP system.

Quicker Processing and More Accurate Delivery

Automating the exchange of documents through the email and PDF, by reducing the margin of error, and also lowering the processing time is a huge advantage for you and to your trading partners to finish the work

quickly. Faster processing often means the shipments leave the warehouse quicker which even results in being as easier to do the business and faster time to market.

User-Friendly Dashboard

All PDF documents are been accepted, processed and routed through the environment directly integrated with your ERP-system. After turning on the application, all orders, invoices and other documents (EDI and non-EDI) can be tracked live, reprocessed in real-time and is been delivered through the same environment within short span of time.

Smart PDF Connect Benefits:

- By enabling the Trading Partners with a solution that don't have the B2B Integration Solutions.
- Quickly and accurately process the PDF documents without any manual work.
- Easily process large documents as quickly as possible.
- Reducing repetitive, manual work and margin of errors.
- It is of 100% accuracy when translating PDF documents into the back office system.
- Compatible with all the ERP Systems.
- Save time and reduce costs.
- Accept and Process PDFs 24/7.