Internet of Things - Unit 4

Participatory Sensing - Participatory sensing is the process whereby individuals and communities use ever- more-capable mobile phones and cloud services to collect and analyze systematic data for use in discovery. The convergence of technology and analytical innovation with a citizenry that is increasingly comfortable using mobile phones and online social networking sets the stage for this technology to dramatically impact many aspects of our daily lives.

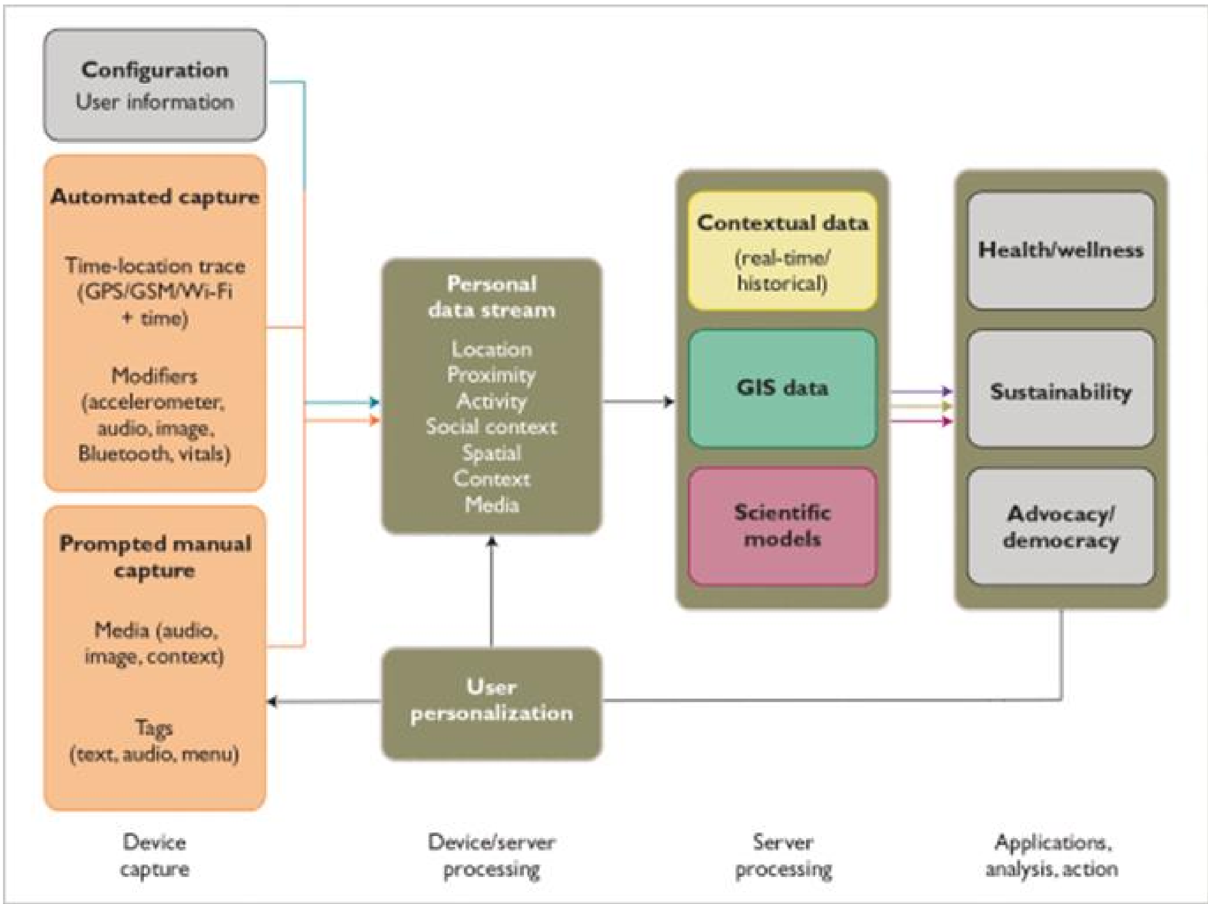
1. Applications and Usage Models

One application of participatory sensing is as a tool for health and wellness. For example, individuals can self-monitor to observe and adjust their medication, physical activity, nutrition, and interactions. Potential contexts include chronic-disease management and health behavior change. Communities and health professionals can also use participatory approaches to better understand the development and effective treatment of disease.

The same systems can be used as tools for sustainability. For example, individuals and communities can explore their transportation and consumption habits, and corporations can promote more sustainable practices among employees.

In addition, participatory sensing offers a powerful “make a case” technique to support advocacy and civic engagement. It can provide a framework in which citizens can bring to light a civic bottleneck, hazard, personal-safety concern, cultural asset, or other data relevant to urban and natural-resources planning and services, all using data that are systematic and can be validated.

These different applications imply several different usage models. These models range from public contribution, in which individuals collect data in response to inquiries defined by others, to personal use and reflection, in which individuals log information about themselves and use the results for personal analysis and behavior change. Yet across these varied applications and usage models, a common workflow is emerging, as Figure 4.1 illustrates.



Benefits of IIOT

The IIoT can greatly improve connectivity, efficiency, scalability, time savings, and cost savings for industrial organizations. Companies are already benefitting from the IIoT through cost savings due to predictive maintenance, improved safety, and other operational efficiencies. IIoT networks of intelligent devices allow industrial organizations to break open data silos and connect all of their people, data, and processes from the factory floor to the executive offices. Business leaders can use IIoT data to get a full and accurate view of how their enterprise is doing, which will help them make better decisions.

IIOT Protocols

One of the issues encountered in the transition to the IIoT is the fact that different edge-of-network devices have historically used different protocols for sending and receiving data. While there are a number of different communication protocols currently in use, such as OPC-UA, the Message Queueing Telemetry Transport (MQTT) transfer protocol is quickly emerging as the standard for IIoT, due to its lightweight overhead, publish/subscribe model, and bidirectional capabilities.

Challenges of IIOT

Interoperability and security are probably the two biggest challenges surrounding the implementation of IIoT. As technology writer Margaret Rouse observes, “A major concern surrounding the Industrial IoT is interoperability between devices and machines that use different protocols and have different architectures.” Ignition is an excellent solution for this since it is cross-platform and built on open-source, IT-standard technologies.

Companies need to know that their data is secure. The proliferation of sensors and other smart, connected devices has resulted in a parallel explosion in security vulnerabilities. This is another factor in the rise of MQTT since it is a very secure IIoT protocol.

Future of IIOT

The IIoT is widely considered to be one of the primary trends affecting industrial businesses today and in the future. Industries are pushing to modernize systems and equipment to meet new regulations, to keep up with increasing market speed and volatility, and to deal with disruptive technologies. Businesses that have embraced the IIoT have seen significant improvements to safety, efficiency, and profitability, and it is expected that this trend will continue as IIoT technologies are more widely adopted.

The Ignition IIoT solution greatly improves connectivity, efficiency, scalability, time savings, and cost savings for industrial organizations. It can unite the people and systems on the plant floor with those at the enterprise level. It can also allow enterprises to get the most value from their system without being constrained by technological and economic limitations. For these reasons and more, Ignition offers the ideal platform for bringing the power of the IIoT into your enterprise.

Automotive IOT-With the number of networked sensors increasing across production, supply chains and products, manufacturers are beginning to tap into a new generation of systems that enables real-time, automatic interactions among machines, systems, assets and things. The pervasiveness of connected devices is finding applicability across multiple segments of manufacturing and “upply chain throughout the value chain. Following are the functions provided by Automotive IOT:

· Ability to view the status of the Assets at anytime, Anywhere & Faster service response from dealer.

· By hooking equipment into the IoT, original equipment manufacturers (OEMs) or dealers could use that stream of data to adjust preventative maintenance schedules based on actual wear and be able to better optimize uptime

· Understand, monitor, predict and control process variability

· Enhance equipment and process diagnostics capabilities

· IoT helps more hands-off way to track goods and the progress of work. RFID tags and readers can play a role in this by allowing materials, locations, or tooling to essentially talk with each other.

· Faster Response time and less operations cost for machine configuration requests that could be services remotely

large amount of transmit power from each node. This will quickly drain the battery of the nodes and reduce the system lifetime. How- ever, the only receptions in this protocol occur at the base station, so if either the base station is close to the nodes, or the energy required receiving data is large, this may be an acceptable method of communication.

Minimum transfer energy protocols- In these protocols, nodes act as routers for other nodes' data in addition to sensing the environment. These protocols differ in the way the routes are chosen. Some of these protocols only consider the energy of the transmitter and neglect the energy dissipation of the receivers in determining the routes. Depending on the real time costs of the transmit amplifier and the radio electronics, the total energy expended in the system might actually be greater using MTE routing than direct transmission to the base station.

Clustering protocol -A final conventional protocol for wireless networks is clustering, where nodes are organized into clusters that communicate with a local base station, and these local base stations transmit the data to the global base station, where it is accessed by the end-user. This greatly reduces the distance nodes need to transmit their data, as typically the local base station is close to all the nodes in the cluster. Thus, clustering appears to be an energy-efficient communication protocol. However, the local base station is assumed to be a high-energy node; if the base station is an energy-constrained node, it would die quickly, as it is being heavily utilized. Thus, conventional clustering would perform poorly for our model of micro sensor networks.

Genetic Algorithm- a genetic algorithm (GA) is used to create energy efficient clusters for data dissemination in wireless sensor networks. A GA is used at the base station, which provides energy efficient solutions to the optimizer. This provides the base station with the ability to determine the best cluster formation that will give minimum energy consumption during run time. The base station analyses the current network condition and applies the GA after every iteration. The optimizer at the base station selects the best solution based on the acquired knowledge through the GA fitness function. The proposed fitness function is based on parameters such as energy consumption, number of clusters, cluster size, direct distance to sink, and cluster distance. Upon completion of iteration, the optimizer improves its decisions by receiving feedback, which is then used to adjust the weights of the parameters of the fitness function for the next iteration

Hierarchical Cluster-Based Routing (HCR) Protocol- In HCR nodes self organize into clusters and each cluster is managed by a set of associates called head-set. Using round-robin technique, each associate acts as a cluster head (CH).[3] The sensor nodes transmit data to their cluster heads, which transmit the aggregated data to the base station. Moreover, the energy-efficient clusters are retained for a longer period of time; the energy-efficient clusters are identified using heuristics-based approach.

Radio Frequency Identification Technology-Radio-frequency identification (RFID) uses electromagnetic fields to automatically identify and track tags attached to objects. The tags contain electronically stored information. Passive tags collect energy from a nearby RFID reader's interrogating radio waves. Active tags have a local power source (such as a battery) and may operate hundreds of meters from the RFID reader. Unlike a barcode, the tag need not be within the line of sight of the reader, so it may be embedded in the tracked object. RFID is one method for Automatic Identification and Data Capture (AIDC).

RFID tags are used in many industries, for example, an RFID tag attached to an automobile during production can be used to track its progress through the assembly line; RFID-tagged pharmaceuticals can be tracked through warehouses; and implanting RFID microchips in livestock and pets allows for positive identification of animals.

Wireless Sensor Network Technology-Wireless sensor network (WSN) refers to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment and organizing the collected data at a central location. WSNs measure environmental conditions like temperature, sound, pollution levels, humidity, wind, and so on.

These are similar to wireless ad hoc networks in the sense that they rely on wireless connectivity and spontaneous formation of networks so that sensor data can be transported wirelessly. Sometimes they are called dust networks, referring to minute sensors as small as dust. WSNs are spatially distributed autonomous sensors to monitor physical or environmental conditions, such

Unit -4

Topics to be covered

Sensor Technology, Participatory Sensing, Industrial IOT and Automotive IOT, Actuator, Sensor data Communication Protocols, Radio Frequency Identification Technology, Wireless Sensor Network Technology.

Sensor Technology

The Internet of Things (IoT) couldn’t exist without smart sensors, and the growing use of smart technology is already transforming how manufacturers implement the IoT. Smart sensors are also bringing more connectivity and analytics to the supply chain. There are some things to know about how and why this is happening.

First, smart sensors are the indispensable enablers of the IoT and the industrial IoT. Smart sensors, including radio frequency identification (RFID) tags, serve three broad purposes. They identify items, locate them and determine their environmental conditions, all of which have major implications for the supply chain and manufacturing. Smart sensors are particularly useful in plants or warehouses because they can keep track of temperature and humidity, log data for historical records and quality management, or be used as triggers for alarms or process management.

Second, smart sensors impact the supply chain by being embedded in products, which can help improve the manufacturing process or the products themselves. “ensors can live inside products to create “smart products” and new revenue sources from the enhanced features. They can also permeate the manufacturing process to monitor, control, and improve operations, or be added to logistics to streamline how products are delivered. There are a number of specific purposes of sensors, such as measuring temperature, humidity, vibrations, motion, light, pressure and altitude. Companies will need to develop new applications to take advantage of all the big data that the sensors are generating.

Third, the lower costs and more advanced capabilities of RFID tags are starting to enable wider and more effective use. The cost of RFID, which has come down dramatically, is in more than just the tag itself. To determine the true cost per use you have to include the software applications and deployment costs. The combination of lowered costs for tags and improved capabilities means that their value proposition has changed, and represents an opportunity for enterprises to rethink RFID.

A sensor is a device that detects and responds to some type of input from the physical environment. The specific input could be light, heat, motion, moisture, pressure, or any one of a great number of other environmental phenomena. The output is generally a signal that is converted to human-readable display at the sensor location or transmitted electronically over a network for reading or further processing.

Here are a few examples of the many different types of sensors:

In a mercury-based glass thermometer, the input is temperature. The liquid contained expands and contracts in response, causing the level to be higher or lower on the marked gauge, which is human- readable.

An oxygen sensor in a car's emission control system detects the gasoline/oxygen ratio, usually through a chemical reaction that generates a voltage. A computer in the engine reads the voltage and, if the mixture is not optimal, readjusts the balance.

Motion sensors in various systems including home security lights, automatic doors and bathroom fixtures typically send out some type of energy, such as microwaves, ultrasonic waves or light beams and detect when the flow of energy is interrupted by something entering its path.

A photo sensor detects the presence of visible light, infrared transmission (IR), and/or ultraviolet (UV) energy.

Fig 4.1 Participatory Sensing Model Workflow

2. Essential Components

Ubiquitous Data Capture

While empirical data can be collected in a variety of ways, mobile phones are a special and, perhaps, unprecedented tool for the job. These devices have become mobile computing, sensing, and communication platforms, complete with image, audio, video, motion, proximity, and location data capture and broadband communication, and they are capable of being programmed for manual, automatic, and con-text-aware data capture.

Because of the sheer ubiquity of mobile phones and associated communication infrastructure, it is possible to include people of all backgrounds nearly everywhere in the world. Because these devices travel with us, they can help us make sustainable observations on an intimately personal level. Collectively, they provide unmatched coverage in space and time.

Leveraged Data Processing and Management

In some cases, the data collected with a mobile device are enough to reveal an interesting pattern on their own. However, when processed through a series of external and cross-user data sources, models, and algorithms, simple data can be used to infer complex phenomena about individuals and groups. Mapping and other interactive capabilities of today's Web enhance the presentation and interpretation of these patterns for participants. Many applications will call for the comparison of current measures to past trends, so robust and long term storage and management of this data is a central requirement.

The Personal Data Vault

A common feature uniting these applications is the highly individualized, and therefore personal, nature of the data. By building mechanisms for protecting personal data directly into the emerging participatory sensing architecture’ we can create a healthy marketplace of content and services in which the individual has visibility and negotiating power with respect to the use and disposition of his or her personal data streams. By specifying standard mechanisms instead of standard policy, we enable support of diverse policies that are tailored to particular applications and users - this is the *narrow waist* of this participatory- sensing architecture. Without such architecture, critical applications will be encouraged to create bundled, vertically integrated, non-interoperable, and nontransferable vehicles for personal data streams, thereby making those streams opaque to their creators. By creating such a user-transparent architecture that places individuals and communities at the locus of control over information flow, we will simultaneously support participant rights and create a healthier market for competitive services.

To support this function, we propose the personal data vault. It decouples the capture and archiving of personal data streams from the sharing of that information. Instead of individuals sharing their personal data streams directly with services, we propose the use of secure containers to which only the individual has complete access. The personal data vault would then facilitate the selective sharing of subsets of this information with various services over time. Selective sharing may take the form of exporting filtered information from specific times of day or places in space, or may import service computations to the data vault and export resulting computational outputs. Essential to this scheme are tools to audit information flows and support meaningful usage. Finally, legal consideration is essential to protect and preserve the individual's control over his or her own data streams.

Industrial IOT - The IIoT is part of a larger concept known as the Internet of Things (IoT). The IoT is a network of intelligent computers, devices, and objects that collect and share huge amounts of data. The collected data is sent to a central Cloud-based service where it is aggregated with other data and then shared with end users in a helpful way. The IoT will increase automation in homes, schools, stores, and in many industries.

The application of the IoT to the manufacturing industry is called the IIoT (or Industrial Internet or Industry 4.0). The IIoT will revolutionize manufacturing by enabling the acquisition and accessibility of far greater amounts of data, at far greater speeds, and far more efficiently than before. A number of innovative companies have started to implement the IIoT by leveraging intelligent, connected devices in their factories.

Getting information around the Value Loop allows an organization to create value; how much value is created is a function of the *value drivers*, which capture the characteristics of the information that makes its way around the value loop. The drivers of information value can be captured and sorted into the three categories: *magnitude, risk,* and *time.*

Actuator-An actuator is a component of a machine that is responsible for moving or controlling a mechanism or system, for example by actuating (opening or closing) a valve; in simple terms, it is a mover. An actuator requires a control signal and a source of energy. The control signal is relatively low energy and may be electric voltage or current, pneumatic or hydraulic pressure, or even human power. The supplied main energy source may be electric current, hydraulic fluid pressure, or pneumatic (gas pressure). When the control signal is received, the actuator responds by converting the energy into mechanical motion.

An actuator is the mechanism by which a control system acts upon an environment. The control system can be simple (a fixed mechanical or electronic system), software-based (e.g. a printer driver, robot control system), a human, or any other input.

In typical IoT systems, a sensor may collect information and route to a control center where a decision is made and a corresponding command is sent back to an actuator in response to that sensed input.

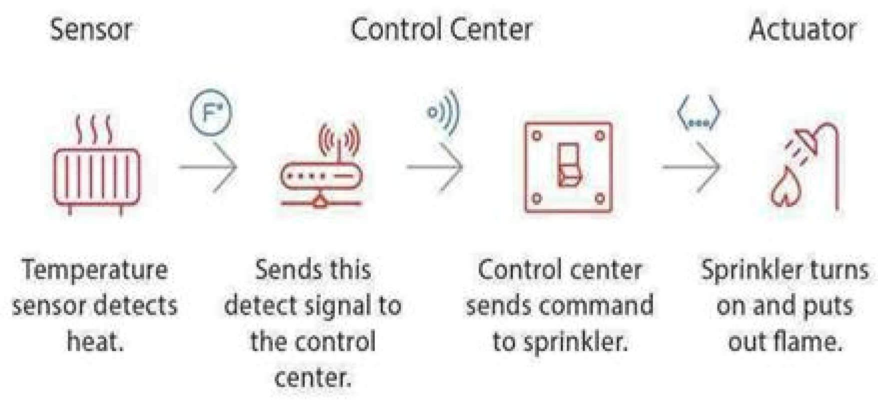


Fig 4.3 Sensor to Actuator Flow

There are many different types of sensors. Flow sensors, temperature sensors, voltage sensors, humidity sensors, and the list goes on. In addition, there are multiple ways to measure the same thing. For instance, airflow might be measured by using a small propeller like the one you would see on a weather station. Alternatively, as in a vehicle measuring the air through the engine, airflow is measured by heating a small element and measuring the rate at which the element is cooling.

Communications Protocols

Sensor data Communication Protocols-Wireless sensors networks are networks of tiny, battery powered sensor nodes with limited on –board processing storage and radio capabilities. Nodes sense and send their reports towards a processing centre which is called "sink". The design of protocols and applications for such network has to be energy aware in order to prolong the lifetime of the network, because the replacement of the embedded batteries is a very difficult process once these nodes have been deployed. the regular nodes sense the field, generate the data, and send them to associated nodes. Then the after performing some processes transmit them to the BS in a multi-hop approach. Eventually the user receives the data from the BS through the Internet.

Wireless sensor networks (WSNs) are composed of a huge number of sensor nodes. There are many applications for WSNs and depending on the application, different types of sensors are used, such as sensors measuring moisture, temperature, pressure and movement. WSNs have themselves characteristics that make them different from other types of networks. One for example is that the applicability of the networks is related to energy supply of the nodes, so energy conservation is one of the most important challenges in these networks. Different types of protocols for WSN are following:

Direct transmission protocols-Using a direct communication protocol, each sensor sends its data directly to the base station. If the base station is far away from the nodes, direct communication will require a

· Ability to view the entire population of connected products together marketing data and product trends

& increased trouble shooting ability for Manufacturer's tech support

· Real-time remote monitoring of performance

· Multi site monitoring improving the operational efficiency and reducing the site downtime

· Availability of real time data for the production environment and alerts generated to the local administrators mobile phone reducing the clean room downtime

· Full manufacturing & SCM traceability

· Predictive Maintenance and quality

Information value loop

The suite of technologies that enables the Internet of Things promises to turn most any object into a source of information about that object. This creates both a new way to differentiate products and services and a new source of value that can be managed in its own right. Realizing the IoT's full potential motivates a framework that captures the series and sequence of activities by which organizations create value from information: the Information Value Loop.

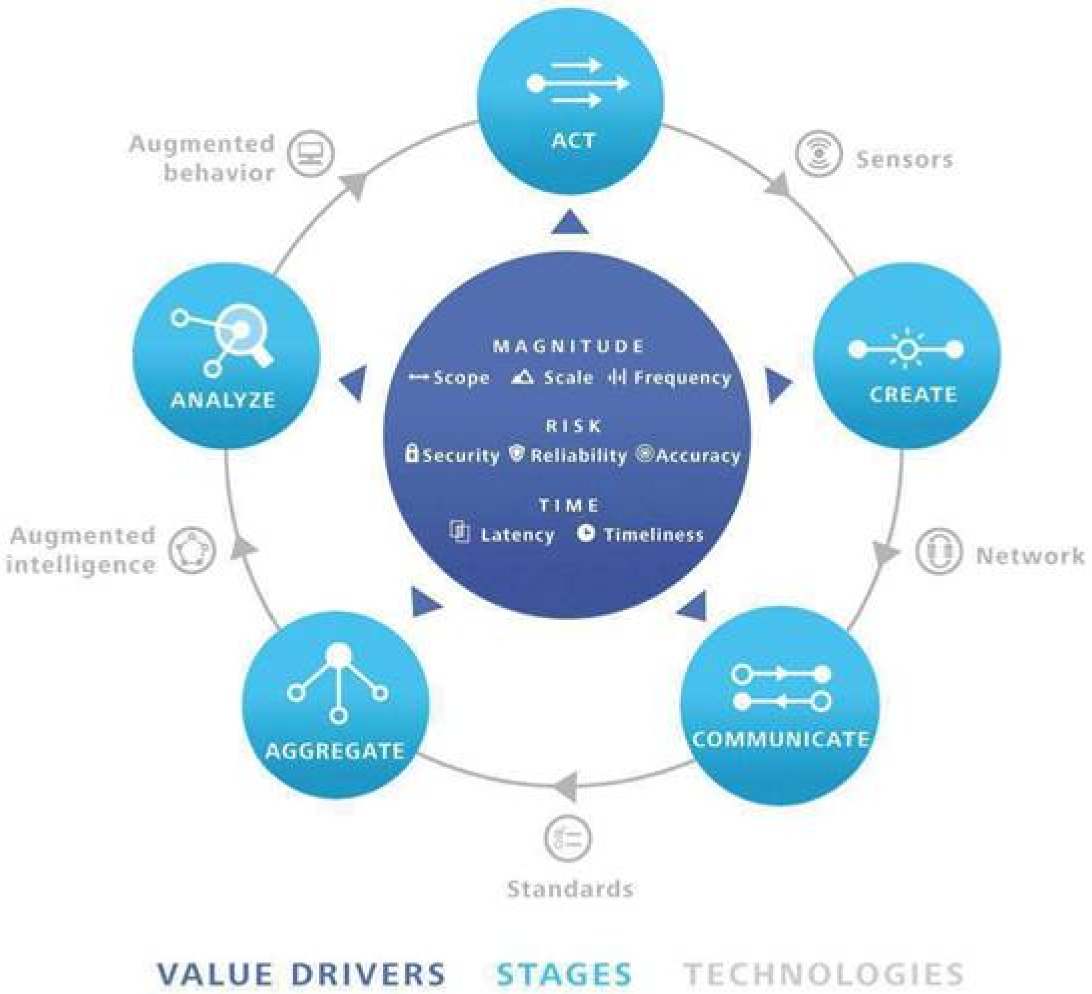


Fig 4.2 Information value loop

For information to complete the loop and create value, it passes through the loop's *stages*, each enabled by specific *technologies*. An *act* is monitored by a *sensor* that *creates* information, that information passes through a *network* so that it can be *communicated*, and *standards*—be they technical, legal, regulatory, or social—allows that information to be *aggregated* across time and space. *Augmented intelligence* is a generic term meant to capture all manner of analytical support, collectively used to *analyze* information. The loop is completed via *augmented behavior* technologies that either enable automated autonomous action or shape human decisions in a manner leading to improved action.

as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main locations. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

A wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to monitor physical or environmental conditions. A WSN system incorporates a gateway that provides wireless connectivity back to the wired world and distributed nodes (see Figure 1). The wireless protocol you select depends on your application requirements. Some of the available standards include 2.4 GHz radios based on either IEEE 802.15.4 or IEEE 802.11 (Wi-Fi) standards or proprietary radios, which are usually 900 MHz.

—

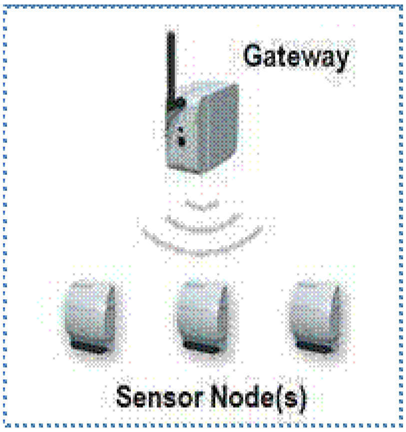


Fig 4.4 WSN Components, Gateway, and Distributed Nodes

Potential Applications-Engineers have created WSN applications for areas including health care, utilities, and remote monitoring. In health care, wireless devices make less invasive patient monitoring and health care possible. For utilities such as the electricity grid, streetlights, and water municipals, wireless sensors offer a lower-cost method for collecting system health data to reduce energy usage and better manage resources. Remote monitoring covers a wide range of applications where wireless systems can complement wired systems by reducing wiring costs and allowing new types of measurement applications. Remote monitoring applications include:

- Environmental monitoring of air, water, and soil
- Structural monitoring for buildings and bridges
- Industrial machine monitoring
- Process monitoring
- Asset tracking

WSN System Architecture

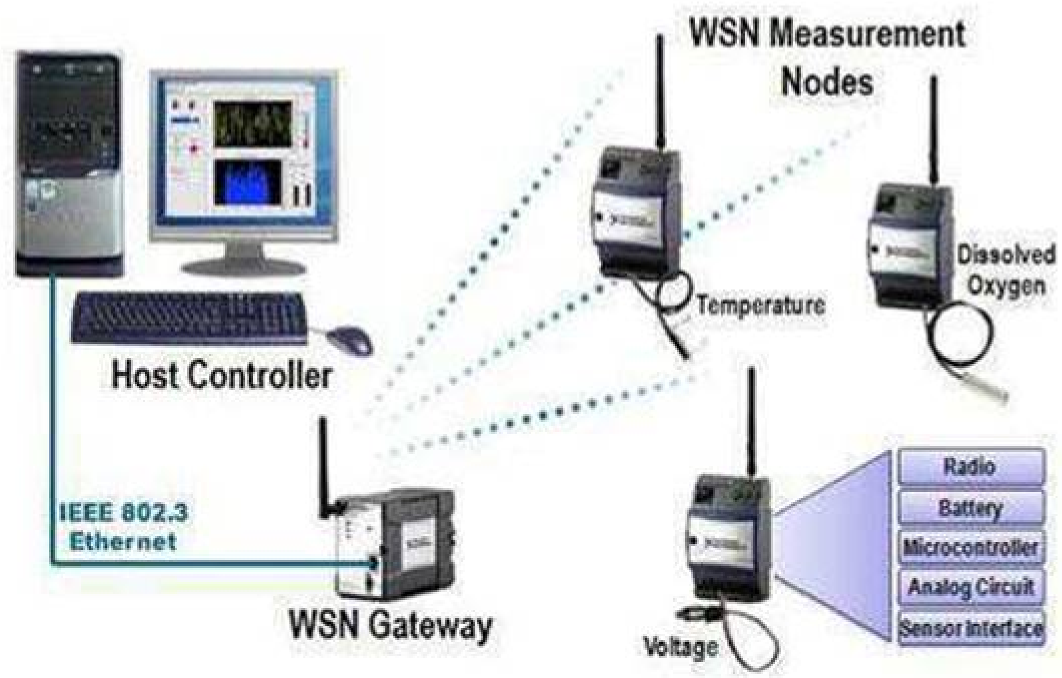


Fig 4.5. WSN System Architecture

Wireless technology offers several advantages for those who can build wired and wireless systems and take advantage of the best technology for the application. To do this, you need flexible software architecture like the NI Lab VIEW graphical system design platform. Lab VIEW offers the flexibility needed to connect a wide range of wired and wireless devices.

WSN Network Topologies-WSN nodes are typically organized in one of three types of network topologies. In a star topology, each node connects directly to a gateway. In a cluster tree network, each node connects to a node higher in the tree and then to the gateway, and data is routed from the lowest node on the tree to the gateway. Finally, to offer increased reliability, mesh networks feature nodes that can connect to multiple nodes in the system and pass data through the most reliable path available. This mesh link is often referred to as a router.

—

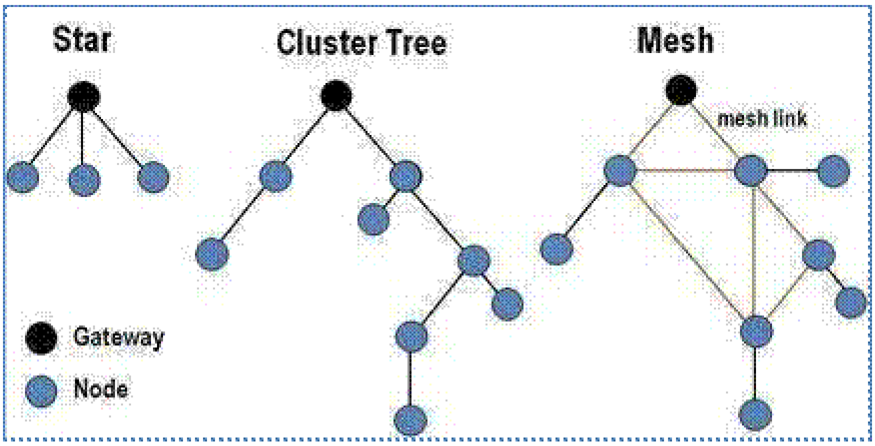


Fig. 4.6. Common WSN Network Topologies

Components of a WSN Node-A WSN node contain several technical components. These include the radio, battery, microcontroller, analog circuit, and sensor interface. When using WSN radio technology, you must make important trade-offs. In battery-powered systems, higher radio data rates and more frequent radio use consume more power. Often three years of battery life is a requirement, so many of the WSN systems today are based on ZigBee due to its low-power consumption.

The second technology consideration for WSN systems is the battery. In addition to long life requirements, you must consider the size and weight of batteries as well as international standards for shipping batteries and battery availability. The low cost and wide availability of carbon zinc and alkaline batteries make them a common choice. To extend battery life, a WSN node periodically wakes up and transmits data by powering on the radio and then powering it back off to conserve energy. WSN radio technology must efficiently transmit a signal and allow the system to go back to sleep with minimal power use. This means the processor involved must also be able to wake power up, and return to sleep mode efficiently. Microprocessor trends for WSNs include reducing power consumption while maintaining or increasing processor speed. Much like your radio choice, the power consumption and processing speed trade-off is a key concern when selecting a processor for WSNs. This makes the x86 architecture a difficult option for battery-powered devices.

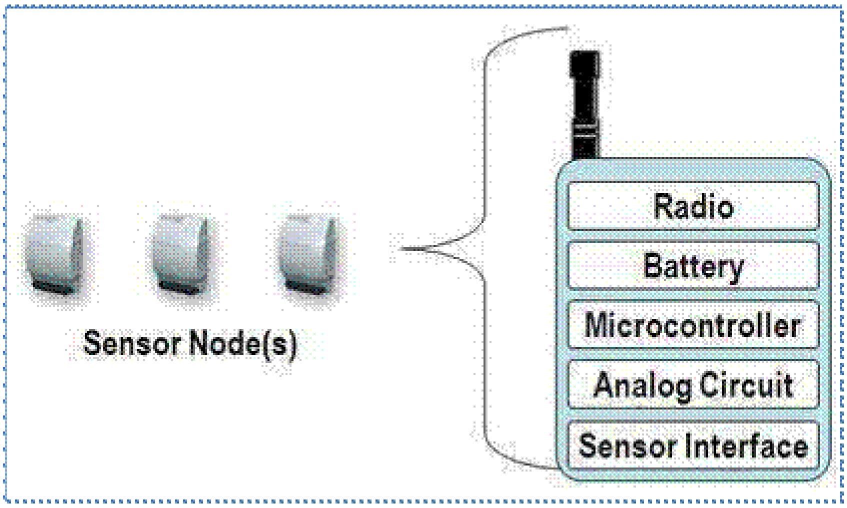


Fig 4.7 WSN Sensor Node Components