APPLICATION OF WIRELESS SENSOR NETWORKS FOR INDUSTRIAL AUTOMATION: TECHNOLOGY AND CHALLENGES

Deepak Sachan[1], K V V Raju [2], Subrata Biswas[3]

[1] Engineer
Technology Development Lab
BHEL Corporate R &D
Hyderabad 500093, INDIA
deepaksachan@bhelrnd.co.in

[2] Sr. Manager
Technology Development Lab
BHEL Corporate R &D
Hyderabad 500093, INDIA
kvvraju@bhelrnd.co.in

[3] General Manager
Technology Development Lab
BHEL Corporate R &D
Hyderabad 500093, INDIA
biswas@bhelrnd.co.in

ABSTRACT: Automated monitoring and control solution significantly increases the efficiency of the production process by expanding coverage area and dramatically reducing the maintenance costs. Automated solutions enhance both data acquisition scope and reliability, and facilitate growth and expansion through the deployment of highly scalable systems .A wireless sensor network is consisting of spatially distributed autonomous devices that uses sensors to monitor physical or environmental conditions. These autonomous devices, or nodes, combine with routers and a gateway to create a typical WSN system. The distributed measurement nodes communicate wirelessly to a central gateway, which provides a connection to the wired world where we can collect, process, analyze, and present the measurement data. To extend distance and reliability in a wireless sensor network, routers can be used to gain an additional communication link between end nodes and the gateway. By this way, wire for data communication is eliminated and installation of the system will become easy and even cost of the system is reduced when there are more number of points to be measured. The present paper illustrates about the state of the art of the technological review of the emerging WSN technology, its applications, challenges and its various security aspects.

Key Words: Wirless Sensor networks, Industrial Automation, Wireless Communication Protocol, Security Issues

1. INTRODUCTION TO WSN:

WSN (Wireless Sensor Networks) is an emerging technology which can increase the efficiency of the production by expanding the coverage area and dramatically reduce the cost of the installation and maintenance of the deployment of sensor networks at different power plant sites and other application areas. Automated solutions enhance both data acquisition scope and reliability, and facilitate growth and expansion through the deployment of highly scalable systems. However, until recently, the full potential of automated monitoring and control solutions was held back by limitations of conventional wired networks. Besides being costly wired solutions are simply not feasible in many remote, hazardous or hard-to-access and mission-critical locations. The emergence of wireless sensor networks made industry executives even more acutely aware of traditional wired networks' limitations.[1]

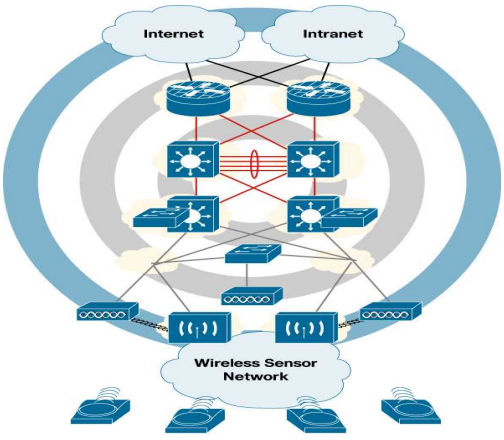

Fig1: *Wireless Sensor Network Overview [1]*

The arrival of Wireless Sensor Networks (WSN) brought liberation from wired limitations, but initially presented their own challenges. A basic WSN (wireless sensor network) is shown in Fig1. It mainly consists of following sections:

1. Wireless Sensor Node
2. Wireless Sensor Node Master Controller

The communication between sensor node and controller can take place through different wireless communication protocols e.g. IEEE802.15.4 IEEE802.15.4-based standards, such as Zig-Bee was designed to include features, like reliability and self-healing, support for a large number of nodes, fast and easy deployment, very long battery life(5-10 years), security, low cost, global inter-operability and vendor independence.

2. WHAT IS A SENSOR AND SENSOR NETWORK AND WHY WIRELESS SENSOR NETWORKS?

Sensors measure multiple physical properties and include electronic sensors, biosensors, and chemical sensors. These sensors can thus be regarded as **"the interface between the physical world and the world of electrical devices, such as computers"**. The counterpart is represented by actuators that function the other way round, *i.e.* whose tasks consist in converting the electrical signal into a physical phenomenon (*e.g.* displays for quantities measures by sensors (*e.g.* speedometers, temperature reading for thermostats).

Table 1 provides examples of the main sensor types and their outputs. Outputs are mainly voltages, resistance changes or currents. Table1 shows that sensors which measure different properties can have the same form of electrical signal.

Wireless sensor networks (WSNs) are perceived as the most appropriate approach to solve that issue and enable a wider development of machine-to machine (M2M) applications. Wireless sensor networking is a form of mesh networking, with self-forming and self-healing properties.

Physical property	Sensor	Output
Temperature	Thermocouple	Voltage
	Silicon	Voltage/ Current
	Resistance Temperature Detector(RTD)	Resistance
	Thermistor	Resistance
Force/ Pressure	Strain Gauge	Resistance
	Piezoelectric	Voltage
Acceleration	Accelerometer	Capacitance
Flow	Transducer	Voltage
	Transmitter	Voltage/ Current
Position	Linear Variable Differential Transformers (LVDT)	AC Voltage
Light Intensity	Photodiode	Current

Table 1: Examples of sensor types and their output

3. ARCHITECTURE OF WIRELESS SENSOR NETWORKS (WSN):

WSN are networks of nodes that sense and potentially also control their environment. They communicate the information through "wireless links enabling interaction between people or computers and the surrounding environment".

Fig 2 Typical WSN

The data gathered by the different nodes is sent to a sink or master controller, by means of different wireless communication protocol, which is connected to other networks (*e.g.* the Internet, Zig-bee) through a gateway. A WSN mainly consists of:

1. Master Control Unit (MCU) 2. Sensor Node

3.1 Master Controller Unit:

Master Control Unit (MCU) will collect the data from all the Sensor Nodes and logs data. It consists of a Microprocessor unit and an RF module (e.g.Zig-Bee) Fig 3.

Whenever MCU is switched on RF coordinator will detect all the sensor nodes which are on same network id. Once detected, Microprocessor unit will request data from the sensor nodes using different types of protocol over RF e.g. Zig-Bee

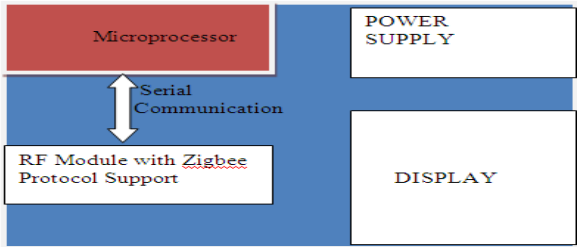

Fig 3: Master Control Unit

A basic MCU consists of:

a) Ethernet Micro Processor (e.g. RCM6700)
b) RF Coordinator
c) Graphical Display
d) Memory for logging data.
e) Keypad

MCU simultaneously communicate with sensor nodes and PC by following ways:

1) RF communication between the Master Control Unit and Sensor node. RF communication is used for data transfer of sensor values from node to MCU
2) Communication between PC and MCU is Modbus over Ethernet based.

3.2 Individual Wireless Sensor Node Architecture:

Sensor nodes are the simplest devices in the network. As their number is usually larger than the number of actuators or sinks, they have to be cheap. A sensor node typically consists of five main parts: one or more sensors gather data from the environment, the central unit in the form of a microprocessor manages the tasks, a transceiver (included in the communication module in Fig 4 communicates with the environment and a memory is used to store temporary data or data generated during processing, the battery supplies power to all parts with energy To assure a sufficiently long network lifetime (see Fig 4). Due to this, data processing tasks are often spread over the network, *i.e.* nodes co-operate in transmitting data to the sinks. Although most sensors have a traditional battery there is some early stage research on the

production of sensors without batteries, i.e. using similar technologies like passive RFID chips without batteries.

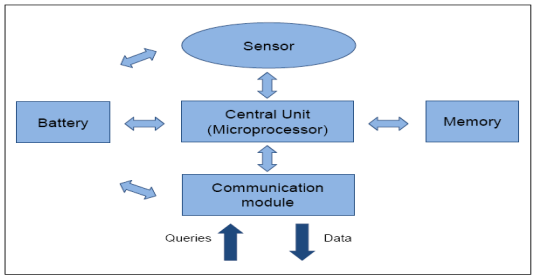

Fig4: Sensor Node Architecture

A functional block diagram of a versatile wireless sensing node is provided in Fig 5 modular design approach provides a flexible and versatile platform to address the needs of a wide variety of applications. For example, depending on the sensors to be deployed, the signal conditioning block can be re-programmed or replaced. This allows for a wide variety of different sensors to be used with the wireless sensing node. Similarly, the radio link may be swapped out as required for a given applications wireless range requirement and the need for bi-directional communications. The use of flash memory allows the remote nodes to acquire data on command from a base station, or by an event sensed by one or more inputs to the node. Furthermore, the embedded firmware can be upgraded through the wireless network in the field.

The microprocessor (Fig 5) has a number of functions including:

- Managing data collection from the sensors
- Performing power management functions.
- Interfacing the sensor data to the physical radio layer.
- Managing the radio network protocol.

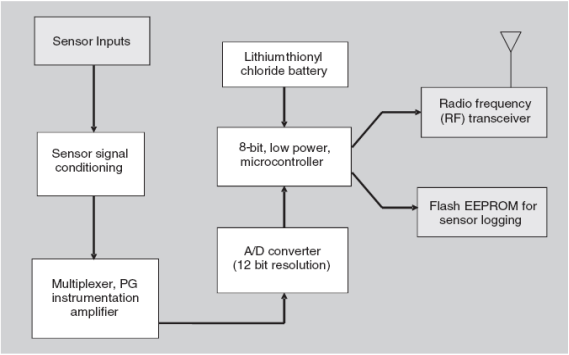

Fig5: Sensor Node Block Diagram

A key feature of any wireless sensing node is to minimize the power consumed by the system. Generally, the radio subsystem requires the largest amount of power. Therefore, it is advantageous to send data over the radio network only when required.

There can be many ways to transfer the data over radio link e.g. 802.11, Bluetooth, Wi-Fi, Zig-Bee etc (refer to section 5). This event-driven sensor data collection model requires an algorithm to be loaded into the node to determine when the data should be sent based on the sensed event. Additionally, it is important to minimize the power consumed by the sensor itself. Therefore, the hardware should be designed to allow the microprocessor to judiciously control power to the radio channel, sensor and sensor signal conditioner [13]. We can collaborate these individual nodes using different architectures (e.g. star, mesh, hybrid etc) to a sink or master controller to control the output as per the requirement.

4 TYPES OF WIRELESS SENSOR NETWORKS ARCHITECTURE:

There are a number of topologies available for radio communications networks. A brief discussion of the network topologies that apply to wireless sensor networks are outlined below. They are

1. Star Network
2. Mesh Network
3. Hybrid Network

4.1 Star Network (Single Point-to-Multipoint)

A star network (Fig 6) is a communications topology where a single base station can send and/or receive a message to a number of remote nodes. The remote nodes can only send or receives a message from the single base station; they are not permitted to send messages to each other.

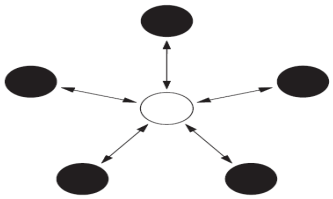

Fig6: Star Network

The advantage of this type of network for wireless sensor networks is in its simplicity and the ability to keep the remote node's power consumption to a minimum. It also allows for low latency communications between the remote node and the base station. The disadvantage of such a network is that the base station must be within radio transmission range of all the individual nodes and is not as robust as other networks due to its dependency on a single node to manage the entire network. [4,5]

4.2 Mesh Network

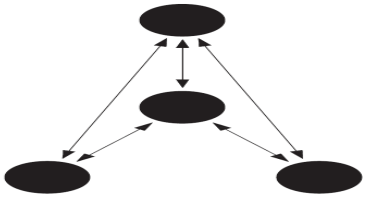

Fig7: Mesh Network

A mesh network allows for any node in the network to transmit to any other node in the network that is within its radio transmission

range (Fig 7). This allows for what is known as multi hop communications; that is, if a node wants to send a message to another node that is out of radio communications range, it can use an intermediate node to forward the message to the desired node. This network topology has the advantage of redundancy and scalability. If an individual node fails, a remote node still can communicate to any other node in its range, which in turn, can forward the message to the desired location. In addition, the range of the network is not necessarily limited by the range in between single nodes; it can simply be extended by adding more number of nodes to the system. The disadvantage of this type of network is in power consumption for the nodes that implement the multi hop communications are generally higher than for the nodes that don't have this capability, often limiting the battery life. Additionally, as the number of communication hops to a destination increases, the time to deliver the message also increases, especially if low power operation of the nodes is a requirement.

4.3 Hybrid Star – Mesh Network

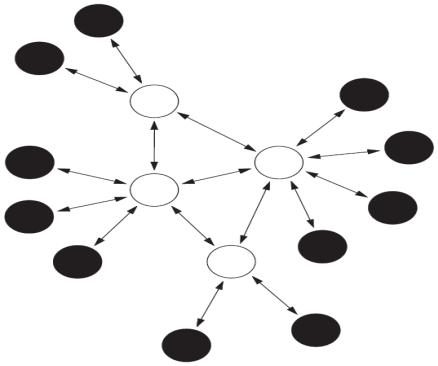

Fig8: Hybrid Star Mesh Network [4,5,6,7]

A hybrid between the star and mesh network provides for a robust and versatile communications network, while maintaining the ability to keep the wireless sensor nodes power consumption to a minimum (Fig 8). In this network topology, the lowest power sensor nodes are not enabled with the ability to forward messages. This allows for minimal power consumption to be maintained. However, other nodes on the network are enabled with multi hop capability, allowing them to forward messages from the low power nodes to other nodes on the network. Generally, the nodes with the multi hop capability are higher power, and if possible, are often plugged into the electrical mains line. This is the topology implemented by the up and coming mesh networking standard known as Zig-Bee[4,5].

These nodes and master controller can communicate through different wireless communication protocols.

5 RADIO OPTIONS FOR THE PHYSICAL LAYER IN WIRELESS SENSOR NETWORKS:

The physical radio layer defines the operating frequency, modulation scheme, and hardware interface of the radio to the system. There are many low power proprietary radio integrated circuits that are appropriate choices for the radio layer in wireless sensor networks, including those from companies such as Atmel, Micro-Chip, Micrel, Melexis, and ChipCon. If possible, it is advantageous to use a radio interface that is based on standards. A discussion of existing radio standards and how they may or may not apply to wireless sensor networks is given below:

5.1 IEEE802.11x:

IEEE802.11 is a standard that is meant for local area networking for relatively high bandwidth data transfer between computers or other devices. The frequencies used in 802.11x protocol are 2.4 GHz, 3.6 GHz and 5 GHz. The data transfer rate ranges from as low as 1 Mbps to over 50 Mbps. Typical transmission range is 300 feet with a standard antenna; the range can be greatly improved with use of a directional high gain antenna. Both frequency hopping and direct sequence spread spectrum modulation schemes are available. While the data rates are certainly high enough for wireless sensor applications, the power requirements generally preclude its use in wireless sensor applications.

5.2 Bluetooth (IEEE802.15.1 and .2)

Bluetooth is a personal area network (PAN) standard that is lower power than 802.11. It was originally specified to serve applications such as data transfer from personal computers to peripheral devices such as cell phones or personal digital assistants. Bluetooth uses a star network topology that supports up to seven remote nodes communicating with a single base station. The technology operates with three different classes of devices: Class 1, class 2 and class 3 where the range is about 100 meters, 10 meters and 1 meter respectively. Wireless LAN operates in the same 2.4 GHz frequency band as Bluetooth, but the two technologies use different signaling methods which should prevent interference. While some companies have built wireless sensors based on Bluetooth, they have not been met with wide acceptance due to limitations of the Bluetooth protocol including:

1) Relatively high power for a short transmission range.

2) Nodes take a long time to synchronize to network when returning from sleep mode, which increases average system power.

3) Low number of nodes per network (<=7 nodes per piconet).

4) Medium Access Controller (MAC) layer is overly complex when compared to that required for wireless sensor applications.

5.3 IEEE 802.15.4

The 802.15.4 standard was specifically designed for the requirements of wireless sensing applications. The standard is very flexible, as it specifies multiple data rates and multiple transmission frequencies. The power requirements are moderately low; however, the hardware is designed to allow for the radio to be put to sleep, which reduces the power to a minimal amount. Additionally, when the node wakes up from sleep mode, rapid synchronization to the network can be achieved. This capability allows for very low average power supply current when the radio can be periodically turned off. The standard supports the following characteristics:

1) Transmission frequencies, 868 MHz/902–928 MHz/2.48–2.5 GHz.

2) Data rates of 20 Kbps (868 MHz Band) 40 Kbps (902 MHz band) and 250 Kbps (2.4 GHz band).

3) Supports star and peer-to-peer (mesh) network connections.

4) Standard specifies optional use of AES-128 security for encryption of transmitted data.

5) Link quality indication, which is useful for multi-hop mesh networking algorithms.
6) Uses Direct Sequence Spread Spectrum (DSSS) for robust data communications.

It is expected that of the three aforementioned standards, the IEEE 802.15.4 will become most widely accepted for wireless sensing applications. The 2.4-GHz band will be widely used, as it is essentially a worldwide license-free band. The high data rates accommodated by the 2.4-GHz specification will allow for lower system power due to the lower amount of radio transmission time to transfer data as compared to the lower frequency bands.[8,11]

5.4 ZigBee

The ZigBee Alliance is an association of companies working together to enable reliable, cost-effective, low-power, wirelessly networked monitoring and control products based on an open global standard. The ZigBee alliance specifies the IEEE 802.15.4 as the physical and MAC layer (Fig 9) and is seeking to standardize higher level applications such as lighting control and HVAC monitoring.

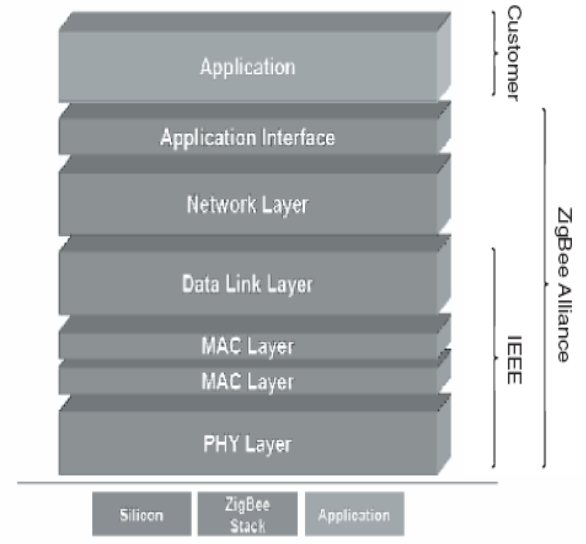

Fig9 : Zig-Bee Protocol

Zigbee works at 868 MHz in Europe, 915 MHz in the USA and Australia, and 2.4 GHz in most jurisdictions worldwide. Data transmission rates vary from 20 to 900 kilobits/second. It also serves as the compliance arm to IEEE802.15.4 much as the Wi-Fi alliance served the IEEE802.11 specification. The ZigBee network specification, to be ratified in 2004, will support both star network and hybrid star mesh networks. As can been seen in Fig 8, the ZigBee Alliance encompasses the IEEE802.15.4 specification and expands on the network specification and the application interface.[8,11]

5.5 IEEE1451.5

While the IEEE802.15.4 standard specifies a communication architecture that is appropriate for wireless sensor networks, it stops short of defining specific about the sensor interface. The IEEE1451.5 wireless sensor working group aims to build on the efforts of previous IEEE1451 smart sensor working groups to standardize the interface of sensors to a wireless network. Currently, the IEEE802.15.4 physical layer has been chosen as the wireless networking communications interface, and at the time of this writing the group is in the process of defining the sensor interface.

6. POWER CONSIDERATION OF A WSN:

One of the most important considerations for a wireless sensor network is power consumption. While the concept of wireless sensor networks looks practical and exciting on paper, if batteries are going to have to be changed constantly, widespread adoption will not occur. Therefore, when the sensor node is designed power consumption must be minimized. Fig 10 shows a chart outlining the major contributors to power consumption in a typical 5000-ohm wireless strain gage sensor node versus transmitted data update rate. Note that by far, the largest power consumption is attributable to the radio link itself.

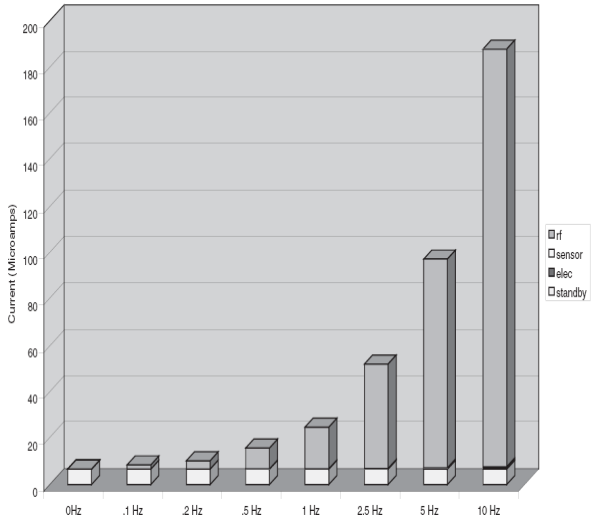

Fig 10: Power consumption of a 5000-ohm Strain gauge wireless sensor node[10]

There are a number of strategies that can be used to reduce the average supply current of the radio, including:

- Reduce the amount of data transmitted through data compression and reduction.
- Lower the transceiver duty cycle and frequency of data transmissions.

- Reduce the frame overhead.
- Implement strict power management mechanisms (power-down and sleep modes).
- Implement an event-driven transmission strategy; only transmit data when a sensor event occurs.

7. KEY CHALLENGES:

Industrial applications offer a broad scope for growth in wireless sensor use, but this growth cannot be achieved without overcoming some of the key challenges facing the market, as shown in Fig 11.

- ✓ Lack of adequate open bandwidth.
- ✓ Deployable network size and hopping challenge.
- ✓ Constantly evolving standards.

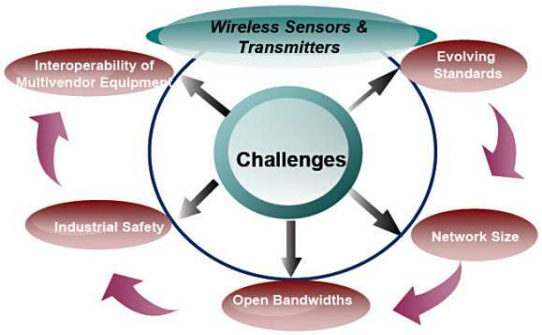

Fig 11: Key challenges for the wireless sensor market

Inter-operability is a major challenge for market participants. This is further exacerbated by the embedding of proprietary communication protocols and support software. Wireless communication technology is successful only if the equipment of different vendors can communicate. This multivendor interoperability environment is expected to be a long term challenge from a design standpoint for both sensor and test vendors. Also, equipment must have plug-and-play options for ease of use as well as to improve market acceptance.

Licensed bandwidths are a subject of disagreement in the market. Market leaders and large companies feel that the use of unlicensed bands interferes with the licensed ones and therefore should be completely eliminated. Presently most wireless sensor network devices operate in unlicensed bands such as 865 MHz and 2.4 GHz, and reliable communication can be affected by interference from other devices operating in the same frequency band. However, the majority of the market participants feel that the use of unlicensed bands is likely to bring in larger benefits accompanied by unrestricted growth as well as to provide equal opportunity to market participants operating on the same platform.

7.1 Key Hardware Issues:

Fig12. Hardware attributes most sought after by end users

There is no ideal wireless sensor or transmitter that could be used for all conceivable applications. In fact, each application determines what attributes the wireless transmitters should have.

Wireless sensors, transmitters, and networks are used for diverse applications with varying requirements and characteristics .Designers and the research community are developing a hardware design platform capable of supporting multiple applications. It is imperative for market participants to have a set of hardware platforms with different capabilities that cover the design space and cater to most market opportunities. A modular approach under which individual components of a sensor node can be easily exchanged is a solution for multiple applications (Fig 12). [11]

7.2Key Network Issues:

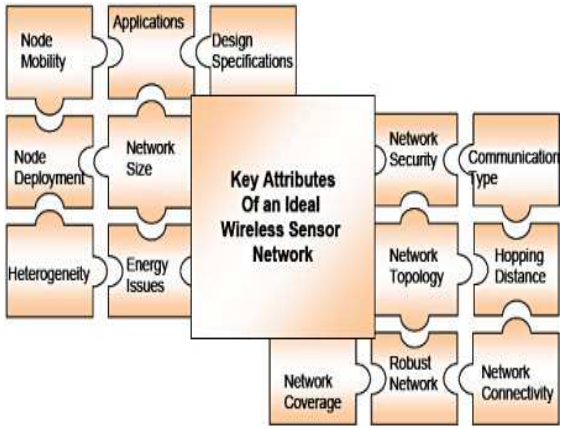

Fig 13. Key attributes of an ideal wireless sensor network

Because wireless sensor networking is built around low-power radios, the nodes that make up the network play a key role in wireless communication (Fig 13). From a physical perspective, the deployment of nodes may take several forms depending on the sensor application and the desired pattern of communication. Deployment may also be a one-time activity, where the installation and use of a sensor network are strictly separate activities. It can also be a continuous process where more nodes are deployed over the lifetime of the network.

Threat	Layer	Defense Techniques
Jamming	Physical	Spread-spectrum, lower duty cycle
Tampering		Tamper-proofing, effective key management schemes
Exhausting	Link	Rate limitation
Collision		Error correcting code
Route information manipulating	Network	Authentication, encryption
Selective forwarding		Redundancy, probing
Sybil attack		Authentication
Sinkhole		Authentication, monitoring, redundancy
Wormhole		Flexible routing, monitoring
Hallo flood		Two-way authentication, three-way handshake
Flooding	Transport	Limiting connection numbers, client puzzles
Clone attack	Application	Unique pair-wise keys

Table 2. Typical threats in WSN

The location of the wireless sensor nodes can also undergo changes over the life of the sensor system. This change of location can be either intentional as required by the system design or desired by the users or be due to external changes such as environmental changes. Mobility can be active or passive. Active mobility can be like an automotive application in which the mobile node must dynamically adjust its direction in accordance with the signal strengths between sensor nodes until it arrives at its desired location. Passive mobility involves a node attached to a moving object where the object is not under the control of the sensor node.

The application needs to determine the actual size of the network. The application can vary from a single sensor node to multiple sensor nodes. Again, the size of each sensor node can vary from a large box to a microscopically small particle.[11]

8 GENERAL SECURITY REQUIRMENT FOR WSN:

Because of the nature of wireless communications, resource limitation on sensor nodes, size and density of the networks, unknown topology prior to deployment, and high risk of physical attacks to unattended sensors, it is a challenge to provide security in WSNs. The ultimate security requirement is to provide confidentiality, integrity, authenticity, and availability of all messages in the presence of resourceful adversaries. To provide secure communications for the WSNs, all messages have to be encrypted and authenticated. Security attacks on information flow can be widespread. Modification of information is possible because of the nature of the wireless channels and uncontrolled node environments. An opponent can use natural impairments to modify information and also render the information unavailable. Security requirements in WSNs are similar to those of wireless ad hoc networks due to their similarities [12].

These security requirements can be provided by distribution mechanism with the requirements of scalability, efficiency key connectivity and resilience. Scalability is the ability to support large sensor nodes in the networks. Key distribution mechanism must support large network, and must be flexible against substantial increase in the size of the network even after deployment. Efficiency is the consideration of storage processing and communications limitations on sensor nodes. Key connectivity is the probability that two or more sensor nodes store the same key or keying material. Enough key connectivity must be provided for a WSN to perform its intended functionality. Resilience is about the resistance against node capture. Compromise of security credentials, which are stored on a sensor node or exchanged over radio links, should not reveal information about security of any other links in a WSN. Higher resilience means lower number of compromised links.

8.1 Typical Security Threats and Defense Techniques in Wireless Sensor Networks:

Communications over wireless channels are, by nature, insecure and easily susceptible to various kinds of threats. A large-scale sensor network consists of huge number of sensor nodes and may be dispersed over a wide area. Typical sensor nodes are small with limited communication and computing capabilities. These small sensor nodes are pervious to several key types of threats.

For a large scale sensor network it is impractical to monitor and protect each individual sensor from physical or logical attack. Threats on sensor networks can be classified into attacks on physical, link (MAC), network, transportation, and application layers [14]. Threats can also be classified based on the capability of the possible attacker, such as sensor-level and laptop-level.

Various threats, respective affected layer and defense technique has been shown in table2.

9 FIELDS OF APPLICATION OF WIRELESS SENSOR NETWORKS:

There are numerous different fields of application of sensor networks.

● Monitoring the structural integrity of civil structures by localizing damage for example in bridges

● Environmental control for power savings in heating, cooling, and lighting.

● Wireless health monitoring to unplug the patient from his hospital bed.

● Device monitoring to prevent accidents and failures, or limit their consequences.

● Outdoors monitoring to track telluric activity or pollution in the atmosphere.

● Logging for traceability and causal analysis.

● Triggers for M2M or alarms and alerts for open loop control.

While the enterprise might largely benefit from the introduction of additional wireless sensor systems, concerns might arise as they are integrated to the converged IT network.

10 FUTURE DEVELOPMENTS:

The most general and versatile deployments of wireless sensing networks demand that batteries be deployed. Future work is being performed on systems that exploit piezoelectric materials to harvest ambient strain energy for energy storage in capacitors and/or rechargeable batteries. By combining smart, energy saving electronics with advanced thin film battery chemistries that permit infinite recharge cycles, these systems could provide a long term, maintenance free, wireless monitoring solution.

11 CONCLUSIONS:

Wireless sensors can be deployed almost anywhere at a far lower cost than can a wired system. With the recent advances in embedded systems and wireless technology, the hardware used is becoming more inexpensive and more widely available. Also, since these devices comply with industry standards such as the ZigBee (IEEE 802.15.4) for radio communication.

The security of wireless networks remains a key concern. Certain proprietary protocols have been developed to prevent breaking into the network. However, multiple wireless networks operating simultaneously in a plant setting remains a concern due to increased signal interference. Despite the challenges mentioned earlier, wireless sensors are the future of communication and control networks in industrial settings. Their adoption in manufacturing plants, process control, power generation plants, test and measurement instrumentation, infrastructure, and medical devices is likely to experience exponential growth.

REFERENCES:

1. IEEE 802.11 Working Group (2007-06-12). IEEE 802.11-2007: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. ISBN 0-7381-5656-9.

2. Electric Power Research Institute (EPRI, 2008), The Green Grid - Energy Savings and Carbon Emissions Reductions Enabled by a Smart Grid, Technical Update, Palo Alto, CA.

3. European Commission (EC, 2006), European SmartGrids Technology Platform: Vision and Strategy for Europe's Electricity Networks of the Future, Brussels.

4. European Environment Agency (2009), "Environmental Terminology and Discovery Service (ETDS) –Business-As-Usual Scenario.

5. Chris Townsend, Steven Arms MicroStrain, Inc.

6. Lewis, F.L.,"Wireless Sensor Networks,"Smart Environments: Technologies, Protocols, and Applications, ed. D.J. Cook and S.K. Das, John Wiley, New York, 2004.

7. Townsend C.P, Hamel M.J., Arms S.W. (2001): Telemetered Sensors for Dynamic Activity & Structural Performance Monitoring, SPIE's 8th Annual Int'l Conference on Smart Structures and Materials, Newport Beach, CA.

8. Tiwari, A., Lewis, F.L., Shuzhi S-G.; "Design & Implementation of Wireless Sensor Network for Machine Condition Based Maintenance," Int'l Conf. Control, Automation, Robotics, & Vision (ICARV), Kunming, China, 6–9 Dec. 2004.

9. Arms, S.A., Townsend, C.P.; "Wireless Strain Measurement Systems – Applications & Solutions," Proceedings of NSF-ESF Joint Conference on Structural Health Monitoring, Strasbourg, France, Oct 3–5, 2003.

10. Chris Townsend, Steven Arms MicroStrain, Inc.

11. Wireless Sensor Use Is Expanding in Industrial Applications June 1, 2010 By: Dr. Rajender Thusu, PhD, Frost & Sullivan Sensors

12. K. Lu et al., "A Framework for a Distributed Key Management Scheme in Heterogeneous Wireless Sensor Networks", IEEE Transactions on Wireless Communications, vol. 7, no. 2, Feb. 2008, pp. 639-647.

13. OECD based on Verdone et al., 2008.

14 .Du, and H-H. Chen,"Security in Wireless Sensor Networks"IEEE Wireless Communications, vol. 15, no. 4, Aug. 2008, pp.60-66.

.].