International Journal of Scientific Engineering and Science
Volume 1, Issue 11, pp. 75-81, 2017. ISSN (Online): 2456-7361

A Survey on Wireless Sensor Networks

Dr. N. Hariharan[1], Sreelekshmi S[2]
[1, 2]Dept. of Electronics and Communication Engineering, Adi Shankara Institute of Engineering & Technology, Ernakulam, Kerala, India

Abstract**—** *Wireless Sensor Networks is composed by the convergence of sensor, micro-electro-mechanism system and networks technologies. It consists of small nodes with sensing, computation and wireless communication capabilities. WSNs are used in different applications e.g. environmental monitoring, habitat monitoring, home automation, military application etc., and particularly in recent years with the help of sensors that are smaller, cheaper, and intelligent. The design of WSNs depends on the applications, and also it must consider factors such as the environment, the applications design objectives, cost, hardware, and system constraints. This paper focuses on the study of characteristics, communication architecture, challenges and open issues in WSN. The flexibility, fault tolerance, low-cost and rapid deployment features of the WSNs create many new and exciting application for remote sensing areas. In the future, this wide range of application areas will make sensor networks an integral part of our lives. The challenges and open research issues in WSN can be considered as a source of inspiration for future studies.*

Keywords**—** *Wireless Sensor Network, Architecture, WSN Standards & Technologies, Applications, challenges & issues, Attacks*.

I. INTRODUCTION

Wireless sensor networks (WSN) are composed of a large number of sensor nodes, communicate with each other through wireless transmission. Many feasible applications are proposed such as industrial sensor networks, volcano monitoring networks, habitat monitoring, health monitoring, and home automation etc. The organization of internal software and hardware should be in a manner that will allow them to work properly and be able to adapt dynamically to new environments, requirements and applications. Similarly, it makes sure to be general enough to be suited for as many applications as possible [1].

Sensors are being widely used in the health care applications where they may offer significant cost savings and enable new functionalities that can assist the elderly people living along in the house or people with chronic diseases on the daily activities. Applications of security in WSN include criminal and intrusion detection. However, having the limited bandwidth and power, sensor nodes is deployed typically, that will increase the challenges in the management and design of the sensor networks. Problems regarding the physical layer and data link layer are focused on low duty cycle, energy aware MAC protocols, dynamic voltage scaling etc.

Sensor nodes can be deployed either in an ad-hoc or a preplanned manner. An ad-hoc deployment is good for large uncovered regions where a network of a very large number of nodes can be deployed and left unattended to perform monitoring and reporting functions. Network maintenance such as managing connectivity and detecting failures is difficult in WSNs due to large number of nodes [1]. On the other hand, preplanned deployment is good for limited coverage where fewer nodes are deployed at specific locations with the advantages of lower network maintenance and management cost.

Figure 1 shows the architecture of the wireless sensor network where the sensor nodes are usually scattered in a sensor field. Each of these scattered sensor nodes has the capabilities to collect data and route data back to the sink. Data are routed back to the sink by a multihop infrastructure less architecture via the sink. The sink may communicate with the task manager node via Internet or satellite [8].

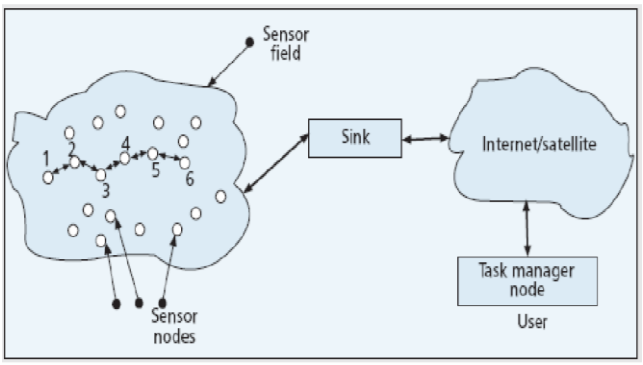

Fig. 1. WSN communication architecture [8].

A sensor node is formed by four main components such as a sensing unit, a processing unit, a transceiver unit and a power unit as shown in Figure 2. They may also have application dependent additional components such as a location finding system, a power generator and a mobilizer. Sensing units are composed of two subunits: sensors and analog to digital converters (ADCs). The analog signals produced by the sensors based on the observed phenomenon are converted to digital signals by the ADC, and then fed into the processing unit. The processing unit, which is generally allied with a small storage unit that manages the procedures that make the sensor node cooperate with the other nodes to carry out the assigned sensing tasks.

A transceiver unit is used to connect the node to the network. One of the most important components of a sensor node is the power unit. Power units are supported by a power scavenging unit such as solar cells [6].

International Journal of Scientific Engineering and Science
Volume 1, Issue 11, pp. 75-81, 2017. ISSN (Online): 2456-7361

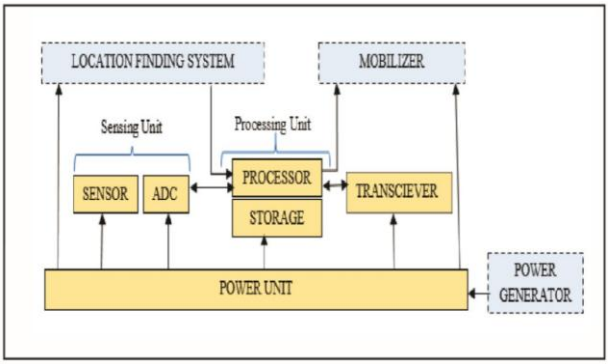

Fig. 2. Components of sensor node [6].

II. System Requirements

The characteristic requirements of a system comprising wireless sensor nodes [2] should be:

A. *Fault tolerant:* The system should be robust against node failure. Some beep mechanism should be incorporated to indicate that the node is not functioning properly.

B. *Scalable:* The system should support large number of sensor nodes to cater for different applications.

C. *Long life:* The node's life-time entirely defines the network's life-time and it should be high enough. The sensor node should be power efficient against the limited power resource. So it is difficult to replace or recharge thousands of nodes. The node's communication, computing, sensing, actuating operations etc. should be energy efficient.

D. *Programmable:* The reprogramming of sensor nodes in the field might be necessary to improve flexibility.

E. *Secure:* The node should support the following
- Access Control: To prevent unauthorized attempts to access the node.
- Message Integrity: To detect and prevent unauthorized changes to the message.
- Confidentiality: To assure that sensor node should encrypt messages, the node who having the secret key can only listen the message.
- Replay Protection: To assure that sensor node should provide protection against adversary reusing an authentic packet for network access, man in the middle attack can be prevented by time stamped data packets.

F. *Affordable:* the system should use low cost devices since the network comprises of thousands of sensor nodes, tags and apparatus. Installation and maintenance of system elements should also be significantly low to make its deployment realistic.

III. Protocol Stack of WSN

The protocol stack used by the sink and all sensor nodes [6]. This protocol stack combines power and routing awareness, integrates data with networking protocols, communicates power efficiently through the wireless medium, and promotes cooperative efforts of sensor nodes. Figure 3 show the protocol stack of WSNs which consists of application layer, transport layer, network layer, data link layer, physical layer, power management plane, mobility management plane, and task management plane. Depending on the sensing tasks, different types of application software can be built and used on the application layer. The transport layer helps to maintain the flow of data whether the sensor networks application requires it. The network layer takes care of routing the data supplied by the transport layer. The physical layer addresses the needs of a simple modulation, transmission and receiving techniques. The power, mobility and task management planes should observe the power, movement, and task distribution between the sensor nodes and these planes helps the sensor nodes to coordinate the sensing task and lower the overall power consumption.

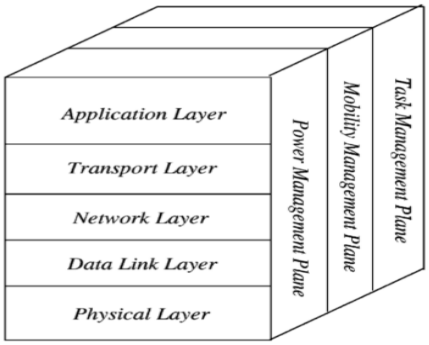

Fig. 3. The sensor networks protocol stack [6].

The power management plane manages how a sensor node uses its power. This is to avoid getting duplicated messages. Also, when the power level of the sensor node is low, the sensor node broadcasts to its neighbours that it is low in power and cannot participate in routing messages [6]. The remaining power is reserved for sensing. The mobility management plane should detects and records the movement of sensor nodes. So a route back to the user is always maintained, and the sensor nodes can also keep track of who are their neighbour sensor nodes. By knowing who the neighbour sensor nodes are, the sensor nodes can balance their power and task usage.

The task management plane balances and schedules the sensing tasks given to a specific region. Not all the sensor nodes in that region are required to perform the sensing task at the same time. As a result, some sensor nodes perform the task more than the other sensor node depending on their power level. These management planes are needed for the sensor nodes to work together with a power efficient way, route data in a mobile sensor network, and share resources between sensor nodes.

IV. Classification of WSN

Presently many WSNs are deployed on land, underground and underwater. They face different challenges and constraints depending on their environment [1, 3].

A. Terrestrial WSN

Terrestrial WSN consists in a large number of low-cost nodes deployed on land in a given area, usually in an ad-hoc manner (e.g., nodes dropped from an airplane) [1]. In terrestrial WSNs, sensor nodes should be able to effectively communicate data back to the base station in a dense

environment. Since battery power is limited and usually non-rechargeable, terrestrial sensor nodes can be equipped with a secondary power source such as solar cells [3].

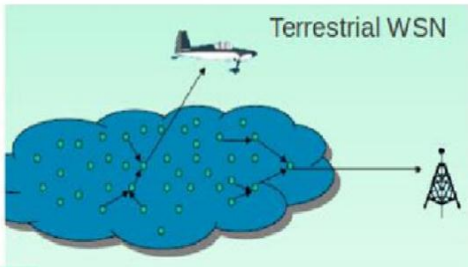

Fig. 4. Terrestrial WSN [1].

Energy can be conserved with multihop optimal routing, short transmission range, in-network data aggregation, and using low duty-cycle operations. Common applications of terrestrial WSNs are environmental sensing and monitoring, industrial monitoring, and surface explorations.

B. Underground WSN

Underground WSN consists of a number of sensor nodes deployed in caves or mines or underground to monitor underground conditions [3]. In order to relay information from the underground sensor nodes to the base station, additional sink nodes are located above ground. They are more expensive than terrestrial WSNs as they require appropriate equipments to ensure reliable communication through soil, rocks, and water.

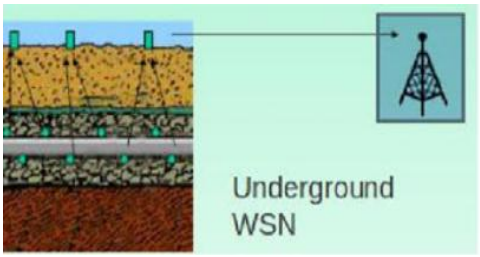

Fig. 5. Underground WSN [1].

Wireless communication have challenge in such environment due to high attenuation and signal loss. Moreover, it is difficult to recharge or replace the battery of nodes buried underground making it important to design energy efficient communication protocol for prolonged lifetime. Underground WSNs are used in many applications such as agriculture monitoring, landscape management, underground monitoring of soil, water or mineral and military border monitoring etc.

C. Underwater WSN

Underwater WSN consists of sensors deployed underwater, for example, into the ocean environment [1]. Such nodes being expensive, only a few nodes are deployed and autonomous underwater vehicles are used to explore or gather data from them. Underwater wireless communication uses acoustic waves that presents various challenges such as limited bandwidth, long propagation delay, high latency, signal fading problems etc. These nodes must be able to self - configure and adapt to extreme conditions of ocean environment. Nodes are equipped with a limited battery so which cannot be replaced or recharged requiring energy efficient underwater communication and networking techniques.

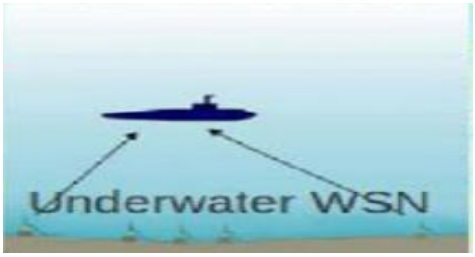

Fig. 6. Underwater WSN [1].

Applications of underwater WSNs include pollution monitoring, under-sea surveillance and exploration, disaster prevention and monitoring, seismic monitoring, equipment monitoring, and underwater robotics etc.

D. Mobile WSN

Mobile WSN consists of mobile sensor nodes that can move around and interact with the physical environment [1]. Mobile nodes can reposition and organize themselves in the network in addition to be able to sense, compute, and communicate. A dynamic routing algorithm must, thus, be employed unlike fixed routing in static WSN [3]. Mobile WSNs face various challenges such as deployment, mobility management, localization with mobility, navigation and control of mobile nodes, maintaining adequate sensing coverage, minimizing energy consumption in locomotion, maintaining network connectivity, and data distribution.

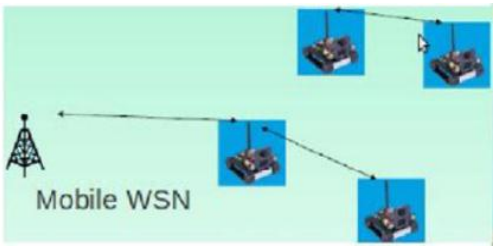

Fig. 7. Mobile WSN [1].

Primary examples of mobile WSN applications are monitoring (environment, habitat, underwater), military surveillance, target tracking, search and rescue. A higher degree of coverage and connectivity can be achieved with mobile sensor nodes compared to static nodes.

E. Multimedia WSN

Multimedia WSN consists of low cost sensor nodes equipped with cameras and microphones, deployed in a preplanned manner to guarantee coverage [1]. Multimedia sensor devices are capable of storing, processing, and retrieving multimedia data such as video, audio, and images. They must cope with various challenges such as high

bandwidth demand, high energy consumption, quality of service (QoS) provisioning, data processing, and compressing techniques, cross-layer design etc.

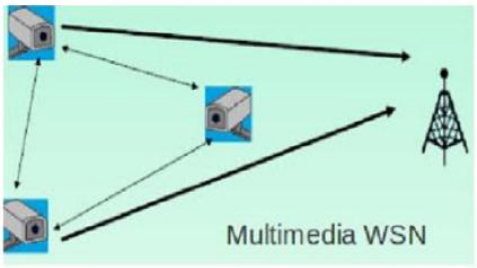

Fig. 8. Multimedia WSN [1].

It is required to develop transmission techniques that support high bandwidth and low energy consumption in order to deliver multimedia content such as a video stream. Though QoS provisioning is difficult in multimedia WSNs due to variable link capacity and delay, a certain level of QoS must be achieved for reliable content delivery. Multimedia WSNs enhance the existing WSN applications such as tracking and monitoring.

V. CHALLENGES IN WSN

A. Fault Tolerance

Some sensor nodes may be fails or blocked due to lack of power, physical damage, or environmental interference [1]. The failure of sensor nodes should not affect the overall task of the sensor network. The Medium Access Control (MAC) and routing protocols must accommodate the formation of new links and routes to the data collection base stations when nodes get fails. This may require actively adjusting transmit powers and signaling rates on the existing links to reduce energy consumption, or rerouting packets through regions of the network where more energy is available [7]. So, multiple levels of redundancy may be needed in a fault tolerant sensor network.

B. Scalability

The number of sensor nodes deployed in the sensing area should be in the order of hundreds or thousands, or more. Any routing scheme must be able to work with this huge number of sensor nodes [7].

In addition, the sensor network routing protocols should be scalable enough to respond to the events in the environment. Until there is an event occurs, most of the sensors can remain in the sleep state, with data from the few remaining sensors providing a coarse quality.

C. Transmission Media

In a multi-hop sensor network, communicating nodes are allied by a wireless medium. The conventional problems associated with a wireless channel (e.g., fading, high error rate) may also affect the operation of the sensor network [7]. In general, the desired bandwidth of sensor data will be low, on the order of 1-100 kbps. So related to the transmission media is the design of medium access control (MAC). Then one approach of MAC design for sensor networks is to use TDMA based protocols that conserve more energy compared to contention based protocols like CSMA.

D. Power Constraint of WSN

The wireless node be able to equipped with a limited power source [1]. There are a few scenarios in which replacement of power resources not viable. So, the lifetime of nodes strongly depend on depletion time of battery. In multihop network each node plays the dual role of data originator and data router [7]. The failures of some affect significant changes in topology and may requires the network re-organization. Data collection is continues process in most of the applications the power requirement of the sensor nodes and system becomes challenging and optimization of power utilized is another important and essential research issue. For the sensor node's accurate operation Ultra low power electronic circuits and dynamic power optimization algorithms are gaining attention of researchers to come up with new solutions.

E. Challenges in Real Time

WSN deal with real time data for applications like military and health services [1]. In many applications sensor data must be delivered within time constraints so that appropriate decision can be made or actions taken in time for the corrective measure is crucial. Most protocols either ignore real-time or simply attempt to process as fast as possible and wish that this speed is sufficient to meet deadlines. Some initial results exist for real-time routing but. It is important not only to develop real-time protocols for WSN, but also associated with the analysis techniques must be developed for the reliable and robust operation of the WSNs. Other functions that must meet the real-time constraints including: data fusion, data transmission, target and event detection and classification, query processing, and security.

F. Network Scale and Time-Varying Characteristics of WSN

Under harsh energy constraints, sensor nodes operates with limited computing, storage and communication capabilities [7]. Depending upon the application, the densities of the WSNs may vary widely, ranging from very sparse to very dense. In these sensor nodes the behaviour of the sensor nodes is dynamic and highly adaptive. As the need to self-organize and conserve energy the sensor nodes adjust the behaviour constantly in response to their current level of activity. Furthermore, the sensor nodes may be requires adjusting the behaviour in response to the erratic and unpredictable behaviour of wireless connections caused by high GH noise levels and radio-frequency interference, to prevent severe performance degradation of the application that have been supported.

G. Management at a Distance

Sensor nodes will be deployed at outdoor field such as a subway station. So it is difficult for the managers or operators to manage the network directly [7]. Thus the framework should provide an indirect remote control/ management system.

VI. ISSUES IN WSN

A. Wireless Network Layer Issues

The data transfer from WSNs are based on the standard layered architecture where each layer have issues as follows:

1. *Physical layer*

Physical layer is responsible for frequency being selected, generation of carrier frequency, modulation, data encryption, and signal deflection [7]. Types of sensors, distance between sensor nodes, path loss, reflection, absorption and scattering loss, interference i.e., co-channel and inter-channel interferences, modulation techniques, signal quality and strength are the main issues related to the physical layer data transfer.

2. *Data link layer*

Data link layer's major concern is to ensure interoperability amongst communication between nodes [4]. This layer deals with error detection and correction, flow control, multiplexing for WSN. Moreover, to create secure key during network deployment and maintenance, some scientist suggested the probable use of public key cryptography, and secure code distribution. Data frame detection, medium access, error control, and multiplexing of data streams are managed by data link layer. At MAC layer, the attacker can send or violate guaranteed time slots forcing the other sensors to retransmit the data multiple times for consuming power.

3. *Network layer*

Optimized path selection for the packet routing is the major responsibility of network layer. Network layer works for routing the data from node to node, node to sink, node to base station, node to cluster head and vice versa . Identification number based protocols and data centric protocols are used by WSN for routing mechanism [4]. Due to the broadcast nature of the transmission for WSN, secure routing protocol is an important requirement. Separate encryption and decryption techniques are utilized for secure routing. Forwarding of packets and the assignment of addresses is performed by network layer. At network layer, sending data long ways and disturbing the routing protocol can devastate global network performance [7]. The common examples include spoofing, altering, and replaying routing information. Black hole, sink-hole, Sybil, wormholes, hello flood, and acknowledgment spoofing are the attacks observed at the network later.

4. *Transport layer*

Transport layer is responsible for specifying the reliable transport of packets [4]. As external sensor network connected to the internet can aid the same Transport layer set up for the data transfer, however it is the main difficult issue in wireless sensor networks.

5. *Application layer*

Application layer is used to display ultimate yield by assure reliable data flow to lower layers. This layer is in charge of data collection, management and processing of the data by using the application software to obtain reliable data transmission [7]. At application layer, applications can be forced to do extensive computation which uses the limited memory of sensor nodes. The taxonomy of various types of faults and attacks elucidates that, there is a requirement of secure transmission of data or a mechanism where the identification of fraudulent nodes can be done which are behaving in an unpredictable manner.

B. Security Issues

The security issues are classified as primary and secondary issues [7]. The primary issues are Confidentiality, Integrity, Authentication and Availability. The secondary issues are Data Freshness, Self-Organization, Time Synchronization and secure localization

1. *Primary issues*

a. *Data confidentiality:-*

Confidentiality means that the ability to hide messages from an intruder in order to that any message communicated via the sensor network remains confidential [2]. This can be the most main problem in network security. A sensor node should not reveal its data to the neighbours [4].

b. *Data authentication:-*

Authentication guarantees the consistency of the message by recognizing its origin.

c. *Data integrity:-*

Data integrity in sensor networks are required to confirm the reliability of data and refers to the ability to confirm that the message has not been tempered with, altered, or modified [7]. While the network has confidentiality measures, there is still a clear stage that the data integrity has been cooperated by alterations. The integrity of the network is going to be in trouble when:-

- Any one node acts as malicious node in the network and also injects false data.
- Unbalanced conditions due to wireless channel basis damage or loss of data.

d. *Data availability:-*

Availability determines whether a node has the ability to use the resources and whether the network is available for the messages to communicate [5]. However, failure of the base station or cluster leader's accessibility will finally threaten the entire sensor network. Thus, availability is of main significance for maintaining an operational network.

2. *Secondary issues*

a. *Data freshness:-*

Even if data confidentiality and data integrity are assured, there's a need to confirm the freshness of every message. Informally, data freshness suggests that the data is recent, and it ensures that no previous messages are replayed [5]. To resolve this issue, a nonce or another time-related counter is often extra into the packet to confirm data freshness.

b. *Self-Organization:-*

A wireless sensor network is usually an ad hoc network that requires every sensor node to be autonomous and flexible and sufficient and to be self-healing and self-organizing consistent with completely different situations [5]. There is no fixed infrastructure available for the aim of network management in a sensor network. This inherent feature brings an excellent challenge to wireless sensor network security. If self-organization is lacking in a sensor network, the injury

resulting from an attack or even the risky environment may be devastating.

c. Time synchronization:-

Most sensor network applications believe some kind of time synchronization [5]. Sensors might need to calculate the end-to-end delay of a packet as it travels between two pairwise sensors. An additional collaborative sensor network might need cluster synchronization for tracking applications.

d. Secure localization:-

The utility of a sensor network can believe its ability to accurately mechanically find every sensor within the network [5]. A sensor network designed to find faults can correct location information so as to pinpoint the location of a fault. Regrettably, an attacker will simply manipulate non secured location information by reporting false signal strengths, replaying signals.

VII. Wireless Sensor Network vs. Ad Hoc Network

A mobile ad hoc network (MANET), occasionally referred to as a mobile mesh network, could be a self-configuring network of mobile devices connected by wireless links. Every device in a MANET is liberal to move independently in any direction and so can modify its links to different devices frequently.

The distinction between wireless sensor networks and ad hoc networks is outlined below [5]:

- The number of sensor nodes in a sensor network can be several orders of magnitude beyond the nodes in an ad hoc network.
- Sensor nodes are heavily deployed.
- Sensor nodes are prone to failures.
- The topology of a sensor network changes recurrently.
- Sensor nodes mainly use broadcast communication paradigm, whereas most ad hoc networks are supported by point-to-point communication.
- Sensor nodes are restricted in power, computational capacities, and memory.
- Sensor nodes might not have universal identification (ID) because of the large quantity of overheads and huge number of sensors.
- Sensor networks are deployed with a selected sensing application in mind, whereas ad hoc networks are regularly created for communication purpose [5].

VIII. Application of WSN

The emergence of the WSN paradigm has triggered extensive research on many aspects of it [3]. The applicability of sensor networks has long been discussed with emphasis on potential applications that can be realized using WSNs. In this section, an overview of certain applications developed for WSNs is provided.

A. Military or Border Surveillance Applications

WSNs are becoming an integral part of military command, control, communication and intelligence systems [1].The need of rapid deployment and self-organization characteristics of sensor networks make them a very promising sensing technique for military applications. Since sensor networks are based on the dense deployment of disposable and low-cost sensor nodes, which makes the sensor network concept a better approach for battlefields [3]. Sensors can be deployed in a battle field to monitor the presence of forces and vehicles, and track their movements, enabling close surveillance of opposing forces.

B. Environmental Applications

The autonomous coordination capabilities of WSNs are employed in the realization of a wide variety of environmental applications. Some environmental applications of WSNs include tracking the movements of birds, small animals, and insects; monitoring environmental conditions that affect crops and livestock; temperature, humidity and lighting in office buildings; irrigation; large-scale earth monitoring and planetary exploration [3]. These monitoring modules could even be combined with actuator modules which can control, for example, the amount of fertilizer in the soil, or the amount of cooling or heating in a building, based on distributed sensor measurements.

C. Agriculture

Using WSNs within the agricultural industry is increasingly common; using a wireless network frees the farmer from the maintenance of wiring in a difficult environment [3]. Gravity feed water systems can be monitored using pressure transmitters to monitor water tank levels, pumps can be controlled using wireless I/O devices and water use can be measured and wirelessly transmitted back to a central control center for billing. Irrigation automation enables more efficient water use and reduces waste. In agriculture, plant diseases are regularly monitored by WSN [1]. Plant monitoring with the image processing and sensor networks using Field Programmable Gate Array (FPGA) based control is the new method.

D. Health Care Applications

Wireless sensor networks can be used to monitor and track elders and patients for health care purposes, which can significantly relieve the severe shortage of health care personnel and reduce the health care expenditures in the current health care systems [3]. For example sensors can be deployed in a patient's home to monitor the behaviours of the patient. It can alert doctors when the patient falls and requires immediate medical attention. In addition, the developments in implanted biomedical devices and smart integrated sensors make the usage of sensor networks for biomedical applications possible [1].

E. Home Intelligence

Wireless sensor networks can be used to provide more convenient and intelligent living environments for human beings. For example, wireless sensors can be used to remotely read utility meters in a home like water, gas, electricity and then send the readings to a remote centre through wireless communication [3]. Moreover, smart sensor nodes and actuators can be buried in appliances such as vacuum cleaners, microwave ovens, refrigerators, and DVD players. These sensor nodes inside domestic devices can communicate with

each other and with the external network via the Internet or satellite. They allow end-users to more easily manage home devices both locally and remotely. Accordingly, WSNs enable the interconnection of various devices at residential places with convenient control of various applications at home.

F. Industrial Process Control

Networks of wired sensors have long been used in industrial fields such as industrial sensing and control applications, building automation, access control etc. However, the cost associated with the deployment and the maintenance of wired sensors limits the applicability of these systems. While sensor-based systems incur high deployment costs, manual systems have limited accuracy and require personnel. Rather, WSNs are a promising alternative solution for these systems due to their ease of deployment, high granularity, and high accuracy provided through battery-powered wireless communication units. Some of the commercial applications are monitoring material fatigue; monitoring product quality; constructing smart office spaces; environmental control of office buildings; robot control and guidance in automatic manufacturing environments; monitoring disaster areas; smart structures with embedded sensor nodes [3].

IX. CONCLUSION

Wireless Sensor Networks raise a growing interest in different domains and their possible applications are extremely versatile. The flexibility, fault tolerance, low-cost and rapid deployment characteristics of sensor networks create many new and exciting application areas for remote sensing. Security in WSN is important since it not only provides reliability to the system but also helps in sustaining the network. As wireless sensor networks are still a young research field, much activity is still ongoing to solve many open issues. As some of the main hardware problems, especially with respect to the energy supply and miniaturization, are not yet completely solved, wireless sensor networks are having certain short comings, which are to be solved. Energy constraints is an essential design issue. WSN represent a significant technology that attracts more and more considerable research attention in recent years and are expected to experience an enormous rise in next years are well.

REFERENCES

[1] P. Rawat, K. D. Singh, H. Chaouchi, and J. M. Bonnin, "Wireless sensor networks: a survey on recent developments and potential synergies," *The Journal of Supercomputing*, vol. 68, issue 1, pp. 1-48, 2014.

[2] V. Potdar, A. Sharif, and E. Chang, "Wireless sensor networks: A survey," *IEEE International Conference on Advanced Information Networking and Applications Workshops*, *WAINA'09*, 2009.

[3] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Computer Networks*, vol. 52, issue 12, 2008, pp. 2292-2330.

[4] A. R. Dhakne and P. N. Chatur, "Detailed survey on attacks in wireless sensor network," *Proceedings of the International Conference on Data Engineeringand Communication Technology*, pp. 319-331, Springer Singapore, 2017.

[5] C. V. Anchugam and K. Thangadurai, "Security in wireless sensor networks (WSNs) and their applications," *Information Fusion for Cyber-Security Analytics*, *Springer International Publishing*, pp. 195-228, 2017.

[6] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey," *Computer Networks*, vol. 38, issue 4, pp. 393-422, 2002.

[7] H. Rathore, "Case study: A review of security challenges, attacks and trust and reputation models in wireless sensor networks," *Mapping Biological Systems to Network Systems*, *Springer International Publishing*, pp. 117-175, 2016.

[8] L. Yong-Min, W. Shu-Ci, and N. Xiao-Hong, "The architecture and characteristics of wireless sensor network," *IEEE International Conference on Computer Technology and Development*, *ICCTD'09*, vol. 1., 2009.