World Academy of Science, Engineering and Technology
International Journal of Information and Communication Engineering
Vol:6, No:12, 2012

Wireless Sensor Network: Characteristics and Architectures

Muhammad R Ahmed, Xu Huang, Dharmandra Sharma, and Hongyan Cui

***Abstract*—**An information procuring and processing emerging technology wireless sensor network (WSN) Consists of autonomous nodes with versatile devices underpinned by applications. Nodes are equipped with different capabilities such as sensing, computing, actuation and wireless communications etc. based on application requirements. A WSN application ranges from military implementation in the battlefield, environmental monitoring, health sector as well as emergency response of surveillance. The nodes are deployed independently to cooperatively monitor the physical and environmental conditions. The architecture of WSN differs based on the application requirements and focus on low cost, flexibility, fault tolerance capability, deployment process as well as conserve energy. In this paper we have present the characteristics, architecture design objective and architecture of WSN.

***Keywords*—**Wireless sensor network, characteristics, architecture.

I. Introduction

WIRELESS sensor network (WSN) a new technology for collecting data with autonomous task oriented sensors. Recently, this technology became more popular because of its application and cost. It consists of large number of low cost, low power and multifunctional sensors embedded with short range wireless communication capability that are deployed for monitoring the physical world. Sensor nodes are often called motes. The major components of a sensor nodes are a microcontroller, memory, transceiver, power source and one or more sensors to measure the physical phenomena. Sink in which all data is transmitted in an autonomous way has high capacity of storage and analysis power. The application of WSN includes battlefield surveillance, border monitoring, habitat monitoring, intelligent agriculture, home automation, etc. According to the applications the deployment strategy is decided [1]. When the environment is unknown or hostile such as remote harsh fields, disaster are as toxic environment the deployment usually done by scatter by a possible way, sometimes by small an aircraft. Thus the position of the sensor nodes may not be known in advance. In the post deployment the sensor nodes perform self-organization mechanism to set up the network by determining the neighbor and setting up the routing table by themselves in a autonomous way. A typical WSN is shown in Fig. 1.

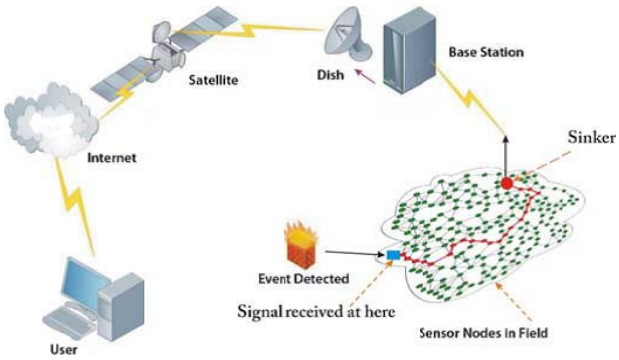

Fig. 1 A typical WSN [1]

Although WSN shares many properties with Wireless ad hoc network and may require similar techniques such as routing protocols but in certain cases it directly prohibit using the protocols proposed in wireless ad hoc network. Thus, the characteristics and architecture differs as well. To demonstrate this issue, the dissimilarities between the WSN and wireless ad hoc network are summarized: [2]

- The number of sensor nodes (hundreds or thousands nodes) in a WSN can be several orders of magnitude higher than the nodes in an ad hoc network.
- Sensor nodes are densely deployed, so multiple sensors can perform to measure the same or similar physical phenomenon.
- Sensor nodes are prone to failures because of battery exhaustion and hostile environment.
- The topology of a sensor network changes very frequently caused by node failure.
- Sensor nodes mainly use a broadcast communication paradigm, whereas most ad hoc networks are based on point-to-point communications.
- Sensor nodes are limited in power, computational capacities, and memory.
- Sensor nodes may not have global identification (ID) because of the large amount of overhead and large number of sensors.

For a functional WSN with maximum throughput with minimum energy in a hostile environment we need to have a good and autonomous system. In order to design such efficient system it is important to consider the characteristics of WSN and the purpose of application.

Muhammad R Ahmed is with the Faculty of Information Science and Engineering, University of Canberra, Australia (e-mail: muhammad.ahmed@canberra.edu.au).
Xu Huang is with Faculty of Information Science and Engineering, University of Canberra, Australia (e-mail: xu.huang@canberra.edu.au).
Dharmandra Sharma is with Faculty of Information Science and Engineering, University of Canberra, Australia (e-mail: dharmandra.sharma@canberra.edu.au).
Hongyn cui is with the School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, China (e-mail: cuihy@bupt.edu.cn).

Most importantly, WSN architecture may include the topology organization sink nodes and global view of the whole network. In the architectural design autonomy and adaptability is considered the main issue. WSN must have to be capable of operating in unattended, hostile environment with minimum maintenance and human interaction or administration.[3] Moreover, WSN has to operate by adapting the environmental changes. In the case of sensor nodes decrees the duty cycle to reduce the power consumption WSN need to operate without any significant changes.

The paper is organized as follows: section II is comprised of the significant characteristics of wireless sensor network followed by objective of architecture design in section III. This section covers what is important to consider in the architecture of WSN. The architecture of WSN is presented in the section IV followed by conclusion in section V.

II. Characteristics of WSN

WSN is currently used for real-world unattended physical environment to measure numerous parameters. So, the characteristics of WSN must be considered for efficient deployment of the network. The significant characteristics of WSN are described as follows [4]:

Low cost: in the WSN normally hundreds or thousands of sensor nodes are deployed to measure any physical environment. In order to reduce the overall cost of the whole network the cost of the sensor node must be kept as low as possible.

Energy efficient: energy in WSN is used for different purpose such as computation, communication and storage. Sensor node consumes more energy compare to any other for communication. If they run out of the power they often become invalid as we do not have any option to recharge. So, the protocols and algorithm development should consider the power consumption in the design phase.

Computational power: normally the node has limited computational capabilities as the cost and energy need to be considered.

Communication Capabilities: WSN typically communicate using radio waves over a wireless channel. It has the property of communicating in short range, with narrow and dynamic bandwidth. The communication channel can be either bidirectional or unidirectional. With the unattended and hostile operational environment it is difficult to run WSN smoothly. So, the hardware and software for communication must have to consider the robustness, security and resiliency.

Security and Privacy: Each sensor node should have sufficient security mechanisms in order to prevent unauthorized access, attacks, and unintentional damage of the information inside of the sensor node. Furthermore, additional privacy mechanisms must also be included.

Distributed sensing and processing: the large number of sensor node is distributed uniformly or randomly. WSNs each node is capable of collecting, sorting, processing, aggregating and sending the data to the sink. Therefore the distributed sensing provides the robustness of the system.

Dynamic network topology: in general WSN are dynamic network. The sensor node can fail for battery exhaustion or other circumstances, communication channel can be disrupted as well as the additional sensor node may be added to the network that result the frequent changes in the network topology. Thus, the WSN nodes have to be embedded with the function of reconfiguration, self-adjustment.

Self-organization: the sensor nodes in the network must have the capability of organizing themselves as the sensor nodes are deployed in a unknown fashion in an unattended and hostile environment. The sensor nodes have work in collaboration to adjust themselves to the distributed algorithm and form the network automatically.

Multi-hop communication: a large number of sensor nodes are deployed in WSN. So, the feasible way to communicate with the sinker or base station is to take the help of a intermediate node through routing path. If one need to communicate with the other node or base station which is beyond its radio frequency it must me through the multi-hop route by intermediate node.

Application oriented: WSN is different from the conventional network due to its nature. It is highly dependent on the application ranges from military, environmental as well as health sector. The nodes are deployed randomly and spanned depending on the type of use.

Robust Operations: Since the sensors are going to be deployed over a large and sometimes hostile environment. So, the sensor nodes have to be fault and error tolerant. Therefore, sensor nodes need the ability to self-test, self-calibrate, and self-repair

Small physical size: sensor nodes are generally small in size with the restricted range. Due to its size its energy is limited which makes the communication capability low.

III. Objectives of Architecture Design

WSN are widely considered as the new emerging technology underpinned by the different application. Because of its characteristics and nature it proposes numerous development challenges to make the sensor nodes. However, before any of the challenges can be properly addressed the sensor network must take place.[5] The network has to be designed and implemented, and it should have flexible mechanisms and the means for their efficient and convenient use. In order to do that the architecture design goals should take place. Some important objectives of WSN architecture design is as follows: [6]

Identifying Requirements of WSN Application: based on the target application necessities the quantitative analysis of the application need to be done, in order to facilitate and meet the accurate design.

Identifying Relevant Technological Trends: technology is growing exponentially with the help of microelectronics development. WSN is known to be heterogeneous and complex system. In such a complex system it is significant to consider the design cost and constrains in order to find the best fit for WSN with maximum power optimization based on the application.

Optimised Design: Sensor nodes are resource constrained. So, we have to design the network in such an optimised way that we can get maximum utilization of the sensor with minimum use of resources.

Design techniques and technology: based on the existing and upcoming technology the architecture need to be design. Among sensor nodes components the power supply and storage existing technology is considered to be mature technology. But ultra-low power wireless communication, sensors and actuators are upgrading almost every day and yet to make revolution. So, it is important to identify which technology can be used and which one need to be developed in the design phase of architecture.

Qualitative and quantitative analysis: existing technology, components and sensors need to be surveyed to do the qualitative and quantities analysis for effective and functional architecture of WSN.

IV. WSN Architecture

WSN is dynamic which can consist of various types of sensor nodes. The environment is heterogeneous in terms of both hardware as well as software. The sensor node construction focuses to reduce cost, increase flexibility, provide fault tolerance. Improve development process and conserve energy. The structure of sensor node consists of sensing unit (sensor and analog to digital converter), processing unit (processor and storage), communication unit (transceiver), and power supply unit. The major blocks shown in Fig. 2 a concise description of different unit is as follows:

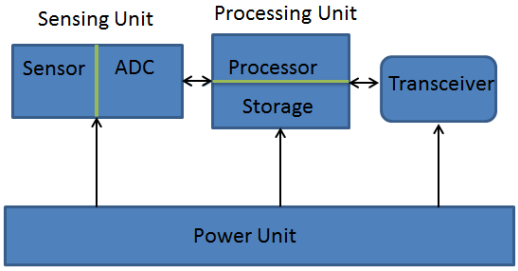

Fig. 2 Structure of a sensor node

Sensing unit: it is composed of collection of different types of sensor which is needed for measurement of different phenomenon of the physical environment. Sensors are selected based on its application. Sensor out is electric signal which is analog. So, analog-to-digital converter (ADC) is used to transform the signal to digital to communicate with the microcontroller.

Processing unit: it consists of a processor (microcontroller) and storage (RAM). In addition it has operating systems as well as timer. The responsibility of the processing unit includes collecting data from various sources than processing and storing. Timer is used to do the sequencing for the sequence.

Communication unit: it uses a transceiver which consists of a transmitter as well as a receiver. The communication is performed through the communication channels by using the network protocol. Based on the application requirements and relevance in order to communicate it normally uses suitable method such as radio, infrared or optical communication.

Power unit: the task of the power unit is to provide the energy to the sensor node for monitoring the environment at a low cost and less time. The life of the sensor depends on the battery or power generator which is connected to the power unit. Power unit is required for the efficient use of the battery.

WSN communication architecture is a bit different from the conventional computer communication and computer network. The communication architecture can be classified in different layers. In order to get the maximum efficiency with limited resources and low overhead WSN does not adhere as closely to the layered architecture of OSI model of conventional network.

Nevertheless, the layered model is useful in WSN for categorizing protocols, attacks and defense. So, in contrast to the traditional seven layers it is reduced to the five layers [2] that include physical layer, Data link layer, network layer, transport layer and application later. The advantage of the layered model is conceptually similar functions are combined at one layer. Fig. 3 shows the communication protocol model of wireless sensor network.

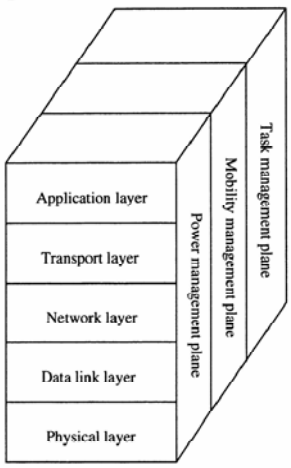

Fig. 3 Protocol Stack of WSN [2]

The physical layer addresses the hardware detail of wireless communication mechanism. This layer is responsible for frequency selection, carrier frequency generation, signal detection, modulation, and data encryption. The data link layer is concerned with the media access control (MAC) protocol. Since the wireless channel is susceptible to the noise and sensor nodes may be changing the location MAC protocol at the data link layer has to be power-aware and should have the capability of minimizing the collisions.[7] The network layer manages the routing the data supplied by the transport layer or between the nodes. Whereas the transport layer is able to maintain the data flow if the WSN application requires that. Various type of application can be implemented in the application depending the physical environmental sensing.

Orthogonal to the five layer Akyildiz et al. [2] defined three management plan named power, mobility and task management. These plans are responsible for monitoring the power, movement and task distribution among the sensor nodes. These management plans helps the sensor nodes to coordinate sensor tasks and minimize the overall power consumption.

V. Conclusion

In recent years, new technologies have shaped numerous military and commercial strategies in an unprecedented way. The wireless sensor network (WSN) technology is one such technology and has been attracting significant attention. In this paper we have presented the characteristics architecture of the wireless sensor network which will help the researchers and industry to design a functional WSN with maximum throughput using minimum resources with a low cost.

Acknowledgment

One of authors would like to thank the works has been partly supported by the project of No. 2009RC0124 and No. 2010ZX03004-002.

References

[1] X. Huang, M. Ahmed, D. Sharma, "Timing Control for Protecting from Internal Attacks in Wireless Sensor Networks", IEEE, ICOIN 2012, Bali, Indonesia, February 2012.

[2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E, Cayirci, "A Survey on Sensor Networks", IEEE Communications Magazine, August 2002.

[3] H. Karl, A, Willing, "Protocols and Architectures for Wireless Sensor Networks". New York: Wiley, 2005. 314−340, 2005.

[4] C. Buratti , A. Conti , D. Dardari and R, Verdone, "An Overview on Wireless Sensor Networks Technology and Evolution" , Sensors 2009, ISSN 1424-8220, pp 6869-6896, 2009.

[5] K. v. madhav , C ,rajendra and R. L. selvaraj, "A study of security challenges in wireless sensor networks", Journal of Theoretical and Applied Information Technology, 2010.

[6] J. Feng, F. Koushanfar, and M. Potkonjak, "Sensor Network Architecture", supported by the national science foundation under Grant No. NI-0085773 and NSF CENS Grant, 2005.

[7] T. He, J. A. Stankovic, C. Lu, T. Abdelzaher, "SPEED: A stateless protocol for real-time communication in sensor networks". In: Proc. of 23rd Int'l Conf. on Distributed Computing Systems. Rhode Island: IEEE Computer Society, 2003.