A Study of Challenging and Application in Wireless Sensor Networks

[1]Nalin Chaudhary
[1]Research Scholar
[1]Bhagwant University, Ajmer, India

Abstract: In this paper we are studding about challenging in wireless sensor networks. A wireless sensor network is composed of a large number of low-power, low-cost sensor nodes which are deployed close to an area of interest and are connected by a wireless RF interface. Wireless sensor networks (WSNs) contain hundreds or thousands of sensor nodes equipped with sensing, computing and communication abilities. Each node has the ability to sense elements of its environment, perform simple computations, and communicate among its peers or directly to an external base station.

This paper presents an exploratory summary of these challenges and constraints for the overall benefit of researchers working in this challenging area in the following paper. Sensor networks have many challenges, but its vast number of applications lures researchers to investigate more into it. A thorough investigation reveals that WSN is a multidisciplinary field.

***Index Terms* – Network, WSN, Node, Sensor, Challenges.**

I. Introduction

Main challenges for data interpretation and the formation of knowledge include addressing noisy, physical world data, and developing new inference techniques. Uncertainty in interpreted data can easily cause users not to trust the system. It is necessary to develop techniques that convert this raw data into usable knowledge in an energy efficient manner [3]. In order to support the lifetime requirements demanded, each node must be constructed to be as robust as possible. In a typical deployment, hundreds of nodes will have to work in harmony for years. To achieve this, the system must be constructed so that it can tolerate and adapt to individual node failure. Additionally, each node must be designed to be as robust as possible. System modularity is a powerful tool that can be used to develop a robust system. By dividing system functionality into isolated sub-pieces, each function can be fully tested in isolation prior to combining them into a complete application. To facilitate this, system components should be as independent as possible and have interfaces that are narrow, in order to prevent unexpected interactions. In addition to increasing the system's robustness to node failure, a wireless sensor network must also be robust to external interference. As these networks will often coexist with other wireless systems, they need the ability to adapt their behavior accordingly. The robustness of wireless links to external interference can be greatly increased through the use of multi-channel and spread spectrum radios [3]. It is common for facilities to have existing wireless devices that operate on one or more frequencies. The ability to avoid congested frequencies is essential in order to guarantee a successful deployment.

In the foreseeable future sensor networks have wide applicability from Observing scientific phenomenon to use in agricultural monitors and warehouse inventory management. In order tounderstand these scientific phenomenon, it is necessary for researchers to collect numerous measurementsof a scientific event in a geographic region. While these measurements can be obtained at a distance(remote sensing), there is often no substitute for observations made firsthand within the region of interest(in-situ). One form of technology that can accomplish such in-situ science is the Wireless Sensor Network (WSN). In WSNs a number of probe devices are distributed throughout a geographic region to observelocal scientific conditions. In addition to sensors, probes are equipped with computational resources for in-network data processing, as well as wireless transceivers for communication with neighboring probes.Recent advances in integrated circuitry, microelectromechanical systems (MEMS), communication andlow-cost, low-power design have fomented the emergence of these wireless sensors.

Time Synchronization is useful for better communication among the sensor nodes. The time synchronization problem is to synchronize the local clocks of sensor nodes in the wireless network [8]. Many applications of sensor networks need local clocks of sensor nodes to be synchronized, requiring various degrees of precision. Since all hardware clocks are imperfect, local clocks of nodes may drift away from each other in time. When a node in the network generates a timestamp to send to another node for synchronization, the packet carrying the timestamp will face a variable amount of delay until it reaches. This delay prevents the receiver from exactly comparing the local clocks of the two nodes and accurately synchronizing to the sender node. There are several reasons for addressing the synchronization problem in sensor networks. Some reasons are as following: Sensor nods are required to coordinate their operations to perform a particular task, Life time of network is depending on power. So to increase the life of network we need to use power saving schemes.

II. Challenging issues in WSNs

Before a WSN can be brought into real life, many problems need to be carefully resolved. More and more problems are discovered and solved over time. In this section, we itemize some typical ones that draw the most attention from researchers. Keep in mind that the following issues are needed to be attacked under the various constraints and limitations as mentioned in Section, which makes them exceedingly challenging [2].

2.1 Algorithm type

Energy is the most critical resource of a sensor since every operation requires a certain amount of energy while sensor is battery-driven but battery is not always replaceable. Thus, energy-efficiency should be and have been the foremost concern of any protocol designed for a WSN. Other limitations of a sensor that require thorough awareness when designing a WSN protocol include sensor's limited memory size, communication and computation capability, thus, algorithms for WSNs need to be simple but robust and fault-tolerant. That is also the reason why decentralized algorithm is always preferable (if it is not the only suitable ones) in WSNs. Some requirements that a "good" protocol aims to are simplicity, energy-efficiency, localized, distributed, and parallel type, scalability and flexibility to the enlargement of the network,robustness, fault-tolerance, and low communication overhead.

2.2 Topology control

For a prone-to-failure network as WSN, the sensors may malfunction at any time or any place for various reasons. It follows that the topology of a WSN is highly dynamic and unpredictable. For each kind of applications, an appropriate topology may be required.

2.3 Routing

After sensors collect the information, enormous streams of information need to be made available to some data consuming centers. The question of how to efficiently, reliably, and securely route the data through a high-density network is also a challenging issue for sensor networks.

2.4 Data Management

A WSN is supposed to frequently collect information about the physical world, e.g., surrounding environment or objects. Information is exchanged on a multiple-source-multiple-destination basis and the number of sensors in a WSN is in the order of hundreds, thousands or even more. Thus, the amount of data collected by a WSN is extremely large. How to manage, process and route the data is truly a challenge. Researchers have considered the following sub-problems for this kind of issue: in-network data processing, data dissemination (multicast, unicast, broadcast) and aggregation (or converge cast).

2.5 Coverage

The primary function of a WSN is to watch over the physical world. To accomplish this function, it is compulsory to schedule, organize the network in such a way that it can effectively observe the interested environment or set of objects, and then collect information that it is desired and supposed to gather.

2.6 Security

It is no use if the sensed data of a WSN is illegally modified, blocked, or redirected to some illegal data centers. It is the responsibility of security protocols to protect the WSNs from such undesired actions. Because a WSN is usually an ad hoc wireless network and is usually deployed to an unattended and hostile region, attacks in sensor networks are relatively easy to carry out, but are exceptionally difficult to defend. Also, types of attacks in WSN are very multiform. Some aspects of security issues in WSNs are to guarantee the integrity, confidentiality of the data or to verify the authenticity of entities exchanging the data.

III. WSN APPLICATIONS

This section gives a nice survey on applications of Wireless Sensor Networks. Here, we briefly itemize some typical and promising applications of WSNs. More details can be found in [2, 3, 11].

3.1 Military applications

The autonomy, self-organization, self-configuration and portability characteristics of a WSN make it very suitable for military applications. It can be used:

- For commanders to monitor the status (position, quantity, availability) of their troops, equipment and ammunition.
- For battlefield surveillance or reconnaissance of opposing forces and terrain.
- For battle damage assessment.
- To target the enemy, to detect biological and chemical attack.

3.2 Environmental applications

It can be used:

- To monitor the condition/status of environment such as humidity, temperature, pressure and pollution in soil, marin and atmosphere.
- To detect a disaster such as forest fire, flood, tsunami, volcano activities that is about to happen.
- To track the movement, health condition of animal/insects etc.

3.3 Health applications

It can be used:

- To remotelymonitor/track/diagnose the condition/status (position, quantity, heart rate, blood pressure) of doctor, patient or drug, equipment, etc.
- To tele-monitor human physiological data (e.g. patient behavior), and the data will be collected and analyzed to detect early symptoms of a disease, and to find new treatment, etc.

3.4 Commercial applications

It can be used to detect/track/monitor vehicles, to manage/control inventory/warehouse, to support interactive devices, or to control environment of a building.

3.5 Scientific exploration

WSNs can be deployed under the water or on the surface of a planet for scientific research purpose.

3.6 Area monitoring

Area monitoring is a common application of WSNs. In area monitoring, the WSN is deployed over a region where some phenomenon is to be monitored. For example, a large quantity of sensor nodes could be deployed over a battlefield to detect enemy intrusion instead of using landmines. When the sensors detect the event being monitored (heat, pressure, sound, light, electro-magnetic field, vibration, etc), the event needs to be reported to one of the base stations, which can take appropriate action (e.g. send a message on the internet or to a satellite).

IV. WIRELESS SENSOR NETWORKS

Wireless sensor networks (WSNs) contain hundreds or thousands of sensor nodes equipped with sensing, computing and communication abilities. Each node has the ability to sense elements of its environment, perform simple computations, and communicate among its peers or directly to an external base station. The position of sensor nodes need not be engineered or predetermined. This allows random deployment in inaccessible terrains or disaster relief operations. On the other hand, this also means that sensor network protocols and algorithms must possess self- organizing capabilities. Another unique feature of sensor networks is the cooperative effort of sensor nodes. Sensor nodes are fitted with an onboard processor. Instead of sending the raw data to the nodes responsible for the fusion, they use their processing abilities to locally carry out simple computations and transmit only the required and partially processed data [11]. Various advantages or benefits of WSN are as follows:

- Easy to deploy,
- Enhanced flexibility,
- Reduced cabling,
- Mobility and ease of network configuration,
- Remote operation,
- Improving operability, visibility for energy management and occupancy,
- Location tracking of mobile equipments,
- Increased assets utilization and Low power,
- Reduced inventory,
- Reduced deployment costs, and
- Decreased maintenance costs.

A sensor node is made up of four basic components, as shown in Figure1.1 a sensing unit, a processing unit, a transceiver unit, and a power unit. They may also have additional application-dependent components such as a location finding system, power generator, and mobilize. Sensing units are usually 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 associated with a small storage unit, manages the procedures that make the sensor node collaborate with the other nodes to carry out the assigned sensing tasks. A transceiver unit connects the node to the network. One of the most important components of a sensor node is the power unit. Power units may be supported b y power scavenging units such as solar cells. There are also other subunits that are application-dependent. Most of the sensor network routing techniques and sensing tasks require knowledge of location with high accuracy. Thus, it is common that a sensor node has a location finding system. A mobilize ma y sometimes be needed to move sensor nodes when it is required to carry out the Assigned tasks [11].

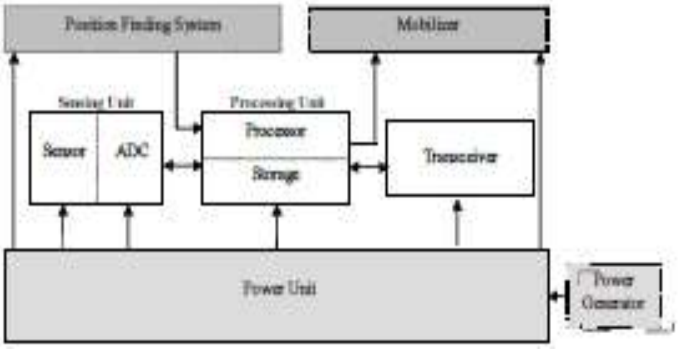

Fig. 1.1 The Components of a sensor node [11].

VI. CONCLUSION

A wireless sensor has not only a sensing component, but also capable of processing, communication, and storage. We are aware that communication poses a number of challenges in a sensor network design. This paper will be a useful scale for researchers to work on various challenges of WSN and application of WSN. Main challenges for data interpretation and the formation of knowledge include addressing noisy, physical world data, and developing new inference techniques. Uncertainty in interpreted data can easily cause users not to trust the system. It is necessary to develop techniques that convert this raw data into usable knowledge in an energy efficient manner. In order to support the lifetime requirements demanded, each node must be constructed to be as robust as possible.

As these networks will often coexist with other wireless systems, they need the ability to adapt their behavior accordingly. The robustness of wireless links to external interference can be greatly increased through the use of multi-channel and spread spectrum radio. It is common for facilities to have existing wireless devices that operate on one or more frequencies. The ability to avoid congested frequencies is essential in order to guarantee a successful deployment.

REFERENCES

[1] Jim Kurose and Keith Ross 2004.Computer Networking: A Top Down Approach Featuring the Internet. 3rd edition. Addison-Wesley.

[2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, 2002. A Survey on Sensor Networks. IEEE Communictions Magazine, pp 102-114.

[3] M. Cardei, M.T. Thai, Y. Li, and W. Wu, 2005. Energy-efficient target coverage in WSNs. In Proc. of IEEE Infocom.

[4] Computer Networks – Andrew S Tanenbaum

[5] Core Java 2 Volume 2-Advanced Features – By Cay S. Horstmann, Gary Cornell Sun Microsystems

[6] The Complete Reference Java 2 – By Herbert Schildt, Tata McGraw-Hill

[7] www.sun.java.com

[8] http://java.sun.com/docs/books/tutorial

[9] An introduction to Database Systems – By C.J. Date

[10] Akshaye Dhawan 2009. Distributed Algorithms for Maximizing the Lifetime of Wireles Sensor Networks. Doctor of Philosophy, Paper Under the direction of Sushil K. Prasad, December 2009,Georgia State University, Atlanta, Ga 30303. Available at:http://etd.gsu.edu/theses/available/etd.../Dhawan_Akshaye_200912_PhD

[11] Chinh Trung Vu, 2009. Distributed Energy-Efficient Solutions for Area Coverage Problems in Wireles Sensor Networks. Doctor of Philosophy, Paper Under the direction of Dr. Yingshu Li, August 2009, Georgia State University, Atlanta,Ga30303.

[12] Chee-Yee Chong and Srikanta P. Kumar 2003. Sensor Networks: Evolution, Opportunities and Challenges. Proceeding of the IEEE, vol. 91, no.8, Aug. 2003.

[13] R. Hahn and H. Reichl 1999. Batteries and power supplies for wearable and ubiquitous computing", in Proc. 3rd Intl. Symposium on Wearable computers.

[14] M. Cardei, J. Wu, N. Lu, M.O. Pervaiz 2005. Maximum Network Lifetime with Adjustable Range. IEEE Intl. Conf. on Wireles and Moble Computing, Networking and Communictions (WiMob'05), Aug.

[15] G. J. Pottie and W. J. Kaiser 2000. Wireles integrated network sensors. Communiction ACM, 43(5):51-58.

[16] P. Berman, G. Calinescu, C. Shah and A. Zelikovsky, "Power Efficient Monitoring Management in Sensor Networks," IEEE Wireles Communiction and Networking Conference (WCNC'04), pp. 2329-2334, Atlanta, March 2004.

[17] Brinza, D. and Zelikovsky, A 2006. DEEPS: Deterministic Energy-Efficient Protocol for Sensor networks", ACIS International Workshop on Self-Assembling Wireles Networks (SAWN'06), Proc. of SNPD, pp. 261-266, 2006.

[18] M. Cardei, J. Wu, "Energy-Efficient Coverage Problems in Wireles Ad-Hoc Sensor Networks", Computer Communictions Journal (Elsevier), Vol.29, No.4, pp. 413-420.