International Journal of Engineering Sciences Paradigms and Researches Vol. 10, Issue 01, December 2013
(An Indexed, Referred and Impact Factor Journal)
ISSN (Online): 2319-6564
www.ijesonline.com

A Review on Wireless Sensor Network- Architecture, Applications and Attacks

Pulkit Berwal

Electronics and Communication Department
pulkit.berwal123@gmail.com

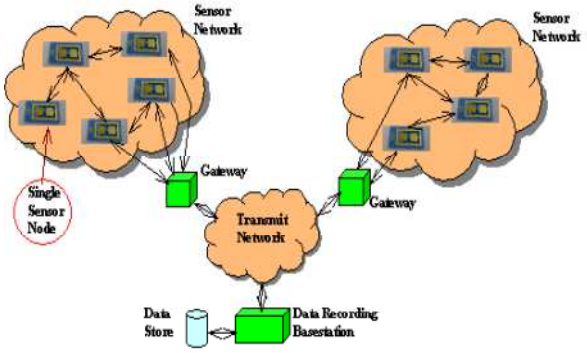
Abstract

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants., and to cooperatively pass their data through the network to a main location. The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. This paper deals with wireless sensor network as cluster sensor network, its applications and various platforms on which it can be implemented and about simulation of WSN. The emphasis of this paper is not to discuss some particular topic of WSN but discuss about its applications, platforms etc. in brief.

Keywords: *Sensor Network (WSN), Security, Attacks, Mesh Network, Star Network, Industrial Automation.*

1. Introduction

A **wireless sensor network (WSN)** consists of spatially distributed autonomous sensors. The more modern networks are bi-directional, enabling also to *control* the activity of the sensors. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer application, such as industrial process monitoring and control, machine health monitoring, environment and habitat monitoring, healthcare applications, home automation, and traffic control. The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from hundreds of dollars to a few pennies, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth.



The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding. In computer science and telecommunications, wireless sensor networks are an active research area with numerous workshops and conferences arranged each year.

2. Literature

A sensor network is denned as being composed of a large number of nodes which are deployed densely in close proximity to the phenomenon to be monitored. Each of these nodes collects data and its purpose is to route this information back to a sink. The network must possess self-organizing capabilities since the positions of individual nodes are not predetermined. Cooperation among nodes is the dominant feature of this type of network, where groups of nodes cooperate to disseminate the information gathered in their vicinity to the user.

Major differences between sensor and ad-hoc networks:

- Number of nodes can be orders of magnitude higher.
- Sensor nodes are densely deployed
- Sensor nodes are prone to failure.
- Frequent topology changes

• Broadcast communication paradigm
• Limited power, processing and power capabilities
• Possible absence of unique global identification per node. The authors point out that none of the studies surveyed has a fully integrated view of all the factors driving the design of sensor networks and proceeds to present its own communication architecture and design factors to be used as a guideline and as a tool to compare various protocols. After surveying the literature, this is our impression as well and we include it in the open research issues that can be explored for future work. The design factors listed by the authors:

2.1 Fault Tolerance:
Individual nodes are prone to unexpected failure with a much higher probability than other types of networks. The network should sustain information dissemination in spite of failures.

2.2 Scalability:
Number in the order of hundreds or thousands, Protocols should be able to scale to such high degree and take advantage of the high density of such networks.

2.3 Production Costs:
The cost of a single node must be low, much less than $1. Hardware Constraints: A sensor node is comprised of many subunits (sensing, processing, communication, power, location finding system, power scavenging and mobilize). All these units combined together must consume extremely low power and be contained within an extremely small volume.

2.4. Sensor Network Topology:
Must be maintained even with very high node densities.

2.5. Environment:
Nodes are operating in inaccessible locations either because of hostile environment or because they are embedded in a structure.

2.6. Transmission Media:
RF, Infrared and Optical, Power Consumption: Power conservation and power management are primary design factors.

3. Wireless Sensor Network Architecture

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

3.1. Star Network (Single Point-to-Multipoint)
A star network (Figure 1) 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 receive a message from the single base station; they are not permitted to send messages to each other. 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 network.

3.2. 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. 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 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.

3.3. Hybrid Star - Mesh Network
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. 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.

4. WSN Security

4.1 Requirements of WSN security

- Data Confidentiality- omission of data leaks to neighboring networks.
- Data Authentication- verification of sender/receiver.

Data Integrity - non altered transmission of data. Data Freshness- ensuring data is recent while allowing for delay estimation. WSNs are becoming a cost effective, practical way to go about deploying sensor networks. Large range of applications from civilian to military purposes pose different challenges as compared to traditional networks. Hence different mechanisms must be brought about.

4.2 Attacks on WSN

Spoofed, altered and replayed routing information
Selective Forwarding Sinkhole attacks.
Traffic Analysis Attacks: Take over the base station/nodes closest to base station
The Sybil attack: Defined as a "malicious device illegitimately taking on multiple identities."Originally used against peer to peer networks but may also be used to disrupt routing algorithms, data aggregation etc.

4.3 Challenges/Obstacles

* The existing infrastructure is already resource-starved.
- Communication bandwidth
- Power
- Computational power
* A typical sensor has a 16 bit 8 Mhz CPU with 10K RAM, 48K Program Memory and 1M flash storage.
* Preventing insider attacks.
* Sinkhole attacks and wormholes - no known countermeasures to apply after the protocol is designed.
* Building multi-hop routing topology - Nodes within one or two hops of the base station are attractive to intruders.
* Unreliable Communication:
#Unreliable Transfer: Packet-based routing of the sensor network is connectionless hence unreliable.
#Conflicts: Even if the channel is reliable, the communication may still be unreliable due to broadcast nature of WSN.
Latency:
Multi- hop routing, network conjunction and node processing can lead to better latency in the network.

5. Applications of wireless sensor network:-

5.1 Structural Health Monitoring

Smart Structures Sensors embedded into machines and structures enable condition-based maintenance of these assets. Typically, structures or machines are inspected at regular time intervals, and components may be repaired or replaced based on their hours in service, rather than on their working conditions. This method is expensive if the components are in good working order, and in some cases, scheduled maintenance will not protect the asset if it was damaged in between the inspection intervals. Wireless sensing will allow assets to be inspected when the sensors indicate that there may be a problem, reducing the cost of maintenance and preventing catastrophic failure in the event that damage is detected. In some cases, wireless sensing applications demand the elimination of not only lead wires, but the elimination of batteries as well, due to the inherent nature of the machine, structure, or materials under test. These applications include sensors mounted on continuously rotating parts, within concrete and composite materials [5], and within medical implants

5.2. Industrial Automation

In addition to being expensive, lead wires can be constraining, especially when moving parts are involved. The use of wireless sensors allows for rapid installation of sensing equipment and allows access to locations that would not be practical if cables were attached. An example of such an application on a production line is shown. In this application, typically ten or more sensors are used to measure gaps where rubber seals are to be placed. Previously, the use of wired sensors was too cumbersome to be implemented in a production line environment. The use of wireless sensors in this application is enabling, allowing a measurement to be made that was not previously practical. Other applications include energy control systems, security, wind turbine, health monitoring, environmental monitoring, location-based services for logistics, and health care.

5.3. Civil Structure Monitoring

One of the most recent applications of today's smarter, energy-aware sensor networks is structural health monitoring of large civil structures, such as the Ben Franklin Bridge (Figure 22.6.2), which spans the Delaware River, linking Philadelphia and Camden, N.J [9,10]. The bridge carries automobile, train and pedestrian traffic. Bridge officials wanted to monitor the strains on the structure as high-speed commuter trains crossed over the bridge. A star network of ten strain sensors were deployed on the tracks of the commuter rail train. The wireless sensing nodes were packaged in environmentally sealed NEMA rated enclosures. The strain gauges were also suitably sealed from the environment and were spot welded to the surface of the bridge steel support structure. Transmission range of the sensors on this star network was approximately 100 meters.

6. Future development

Most important aspect of WSN is security and the efficiency by vital deployment of batteries. The wireless sensor network product specially in industries will not get acceptance unless there is full proof security to the network. Most of the WSN protocols taking an account of security issues into account. Therefore a proper full proof security protocol must b designed by keeping in mind all the performance and the security issues for the secure WSN. 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.

7. Conclusion

WSN is very wide area for research. Further studies can be done in any topic like protocols, dead node detection and prevention. Currently proposed routing protocols for WSNs are insecure but vital. Link layer encryption and authentication mechanisms provide reasonable defense for mote-class outsider attacks. Cryptography is inefficient in preventing against laptop-class and insider attacks. Remains an open problem for additional research and development. The existing infrastructure is already resource- starved due to Communication bandwidth, Power and Computational power. So still there is need of developing more and more sensor networks which overcome these limitations.

References

[1] Arms, S.W., Townsend, C.P., Hamel, M. J.; "Validation of Remotely Powered and Interrogated Sensing Networks for Composite Cure Monitoring," paper presented at the 8th International Conference on Composites Engineering (ICCE/8), Tenerife, Spain, August 7-11, 2001.

[2] Arms, S.W., Townsend, C.P., Galbreath, J.H., Newhard, A.T.; "Wireless Strain Sensing Networks," Proceedings 2nd European Workshop on Structural Health Monitoring, Munich, Germany, July 7-9, 2004.

[3] Kohlstrand, K.M, Danowski, C, Schmadel, I, Arms, S.W; "Mind The Gap: Using Wireless Sensors to Measure Gaps Efficiently," Sensors Magazine, October 2003.

[4] A. 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.

[5] 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.

[6] C. Decker, M. Beigl, A. Krohn, U. Kubach, and P. Robinson. eSeal - a system for enhanced electronic assertion of authenticity and integrity of sealed items.In Proceedings of the Pervasive Computing, volume 3001 of Lecture Notes in Computer Science (LNCS), pages 254- 268. Springer Verlag, 2004.

[7] A. Perrig, R. Szewczyk, V. Wen, D. Culler, J.D. Tygar, SPINS: "security protocols for sensor networks", Proceedings of ACM MobiCom'01, Rome, Italy, pp. 189-199 (2001).

[8] L. Rizzo, "Effective erasure codes for reliable computer communication protocols," ACM Computer Communication Review, vol. 27, no. 2, pp. 24-36, (1997).

[9] A. Chandrakasan, R. Amirtharajah, S. Cho, J. Goodman,G. Konduri, J. Kulik, W. Rabiner, A. Wang, "Design considerations for distributed micro-sensor systems", Proceedings of the IEEE 1999 Custom Integrated Circuits Conference, San Diego, CA, pp. 279-286 (1999).

[10] D. Estrin, R. Govindan, J. Heidemann, S. Kumar," Nextcentury challenges: scalable coordination in sensor networks", ACM MobiCom'99, Washington, USA, pp. 263-270 (1999)