



Survey: Wireless Sensor Network

Prasant Kumar Pattnaik¹, Raghvendra Kumar², Priyanka Pandey³

¹School of Computer Engineering, Kalinga Institute of Industrial Technology University, Bhubaneswar, Odisha, India

²Department of Computer Science and Engineering, Lakshmi Narain College of Technology, Jabalpur, M.P., India

³Department of Computer Science and Engineering, Takshshila Institute of Engineering and Technology, Jabalpur, M.P., India

Email address:

patnaikprasantfcs@kiit.ac.in (P. K. Pattnaik), Raghvendraagrawal7@gmail.com (R. Kumar), pandeypriyanka906@gmail.com (P. Pandey)

To cite this article:

Prasant Kumar Pattnaik, Raghvendra Kumar, Priyanka Pandey. Survey: Wireless Sensor Network. *International Journal on Data Science and Technology*. Vol. 2, No. 2, 2016, pp. 31-35. doi: 10.11648/j.ijdst.20160202.13

Abstract: Target Coverage deals with the coverage of a specific set of targets by a set of sensor nodes. In this paper we address the target coverage problem, with the objective of maximizing the network life time and minimizing the energy consumption by a set of sensor nodes of a power constrained wireless sensor network deployed for monitoring of a set of targets with known locations. Here we consider that a large number of sensor nodes are dispersed randomly in close proximity of a set of objectives and send the sensed information to a central processing node. The sensor network life time is defined as the time interval each target is covered by at least one sensor node. A target can be covered by a sensor node if the Euclidean distance between the target and the sensor node is less than or equal to its sensor node's sensing range.

Keywords: WSN, Characteristics of WSN, Applications of WSN, Coverage Problem of WSN

1. Introduction

Recent advances in technologies made it technically and economically feasible to combine sensing, processing and communicating capabilities into small low cost sensor devices. Once these nodes get deployed, they self organize to form Wireless Sensor Network (WSN) and communicate via wireless links to perform a specific task of real world. Wireless sensor network are quickly gaining popularity due to this fact that they are potentially low cost solutions to a variety of real-world challenges. Availability of different sensor nodes with varieties of sensing capabilities results in hundred of applications including National Security [8], Habitat Monitoring, Environment observation and forecasting, Health Applications [8], Home and Office Applications. There fore WSN are becoming an active research field with numerous research activities carried out every year to explore and solve different constraints.

Wireless sensor networks have been experiencing more and more attentions in academia and industry in recent years, especially under the possibility of much more cheap sensors with certain computation and communication capability. WSNs can be used for many applications such as habitat monitoring, in-door monitoring, target tracking, and security surveillance, etc. However the reis a path before commercially deploying sensors, because WSNs have some problems to be overcome, for example, energy-conservation,

congestion control, reliability data dissemination, security, and management of a WSN itself. These problems of ten involve in one or several layers top-down from application layer to physical layer, and can be studies separately in each corresponding layer, or collaboratively cross each layer. For example, congestion control may involve in only transport layer, but energy-conservation may be related to physical layer, data link layer, network layer, and high layers. Some researchers recently turn the inattentions to transport control protocols, which are important for reliable data dissemination and energy-conservation for WSNs. Generally speaking, transport control protocols, especially for connection-oriented transport protocols, may include two main functions: congestion control and loss recovery. As for congestion control, it is firstly required how to detect whether or not congestion happens, and when and where it happens. Congestion can be detected through monitoring node buffer occupancy and link load. In traditional Internet, the method to weaken congestion are packet dropping at congestion point such as AQM, rate decreasing in source node such as AIMD in TCP, and routing techniques. For WSNs, it should be carefully considered how to detect congestion and how to overcome it, because sensor sare often with limited resources. These protocols must consider it simplicity and scalability to save energy and possibility to prolong the life-time of whole networks. For example, in order to weaken congestion, we can use end-to-end mechanism like TCP or

hop-by-hop back pressure like that in ATM networks or Frame Relay networks. The end-to-end approaches are very simple and robust, but it will bring with more on-going packets in networks. However, hop-by-hop approaches can quickly weaken congestion and bring with less on-going packets in networks, while it needs to change the behavior of each node on the way from source to destination. Since lesson-going packets can result in saved energy, there is a trade-off between end-to-end and hop-by-hop mechanism, which should be carefully considered when designing practical congestion control algorithms for WSNs. Packet loss is usual under wireless sensor networks due to bad quality of wireless channel, sensor failure, and/ or congestion. WSNs must guarantee certain reliability in packet-level or application-level through loss recovery in order to abstract correct information. Some critical applications need reliable transmission of each packet and thus packet-level reliability is needed. Other applications need only a proportion all reliable transmission of total packet and thus application reliability is needed. Any way, we first need to detect packet loss in order to correctly recover missing packets. The traditional method used in packet-switched networks can be used to detect packet loss for wireless sensor networks. For example, each packet can piggy back sequence number, and a receiver can detect loss though arbitrating the continuity of received sequence number during a time interval. After detecting packet loss, ACK and/ or NACK can be used to recover missing packets based on an end-to-end or hop-by-hop approach. Like that in congestion control, there is still a trade-off between end-to-end and hop-by-hop approach, which should be thought over. When designing transport control protocols for wireless sensor networks, we must consider energy-conservation at the same time. Intuitively, if there are few on-going packets and few re-transmissions, energy can be saved. Effective congestion control can result in few on-going packets and effective loss recovery approach can result in few re-transmissions. So congestion control and reliability guarantee can additionally save energy in a wireless sensor network. In a summary, the problem of transport control protocols for sensor networks is how to effectively control congestion and how to guarantee reliability while conserving energy as more as possible simultaneously.

1.1. Internet Protocol

The Internet Protocol is an unreliable, connectionless layer 3 protocol. That means that no connection setup is performed and it is not guaranteed that packets arrive at the destination. The Internet Protocol exists in two versions: IPv4 and IPv6. Version 4 is predominantly used as of 2011, but the adoption of IPv6 is continuously increasing. IPv6 was primarily introduced to solve the problem of the exhaustion of IPv4 addresses. Since IPv4 addresses are 32 bits long there are around 4 billion possible addresses. IPv6 on the other side features 128 bit long addresses which make a total of 1038 different addresses. This increase in addresses, however, did not come for free: The IPv6 header is double the size of an

IPv4 header, without extensions or options: 40 bytes vs. 20 bytes. In wireless sensor networks where most of the time only a few bytes are transferred and the link layer segment size is limited to a little more than 100 bytes, the 40 bytes of the IPv6 header alone would be too great of a head. For compression algorithms can reduce the IPv6 header's size to about 20 bytes. Should the packets still not fit in a link layer frame it can be fragmented using the low PAN protocol layer?

1.2. Transmission Control Protocol

The Transmission Control Protocol is a reliable, connection oriented protocol, in contrast to IP. It operates on layer 4 and establishes a connection between two TCP end points. Once the connection is established it needs to be managed. This management effort consists of making sure that all TCP segments are reliably transmitted from source to destination, detecting transmission errors, potential reordering of packets before delivering them to the destination process, detecting and reacting to network congestion, etc. Although these operations work very well on wired information systems and on wireless systems with no energy scarcity, they do not work well in WSNs. The reasons for that are the sensor nodes' limited resources and the high error rates in wireless networks. An end-to-end retransmission after a bite or was test much energy since the packet has to be sent and received over the whole path again. TCP's reaction to packet loss is not optimal as it is interpreted as network congestion and the sending rate is reduced. These are just two of the problems, which will be discussed in the following section, of operating TCP in a WSN.

1.3. Characteristics of Transport Protocols for WSNs

Transport protocols have been designed for WSNs into three categories:

1. Congestion control
2. Reliability
3. Congestion control and reliability

1.4. Congestion Control

One of the major challenges in wireless sensor network research is to curb down congestion in the network traffic, without compromising with the energy of the sensor nodes. Congestion affects the continuous flow of data, loss of information, delay in the arrival of data to the destination and unwanted consumption of significant amount of the very limited energy in the nodes. Generally the Congestion control is composed of three mechanisms:

1. Congestion detection
2. Congestion notification
3. Rate adjustment

1. Congestion detection:

Congestion detection refers to identification of possible events, which may build-up congestion in the network. A common mechanism is to use the queue length packet service time, or the ratio between packet service time and packet inter-arrival time at an intermediate node.

2. Congestion notification

Once congestion has been detected, congestion information should be propagated from the congested node to upstream traffic nodes and source node the approaches to notify congestion usually can be categorized into explicit congestion notification, and implicit congestion notification.

1.5. Implicit Congestion Notification

The congestion warning is embedded in the header of the normal data packets and the child nodes list their parent node to get the congestion information.

1.6. Explicit Congestion Notification

The source node uses special control messages to notify the involved sensor nodes of congestion

2. Wireless Sensor Node Architecture

Typically a Wireless Sensor Node consists of a sensing unit, a processing unit, a communication unit and a power unit, that is used for sensing there data, processing of the collected data and communicating with other connected nodes in the WSN, as shown in Figure 1. These nodes after deployment form the network to monitor the specific region of interest.

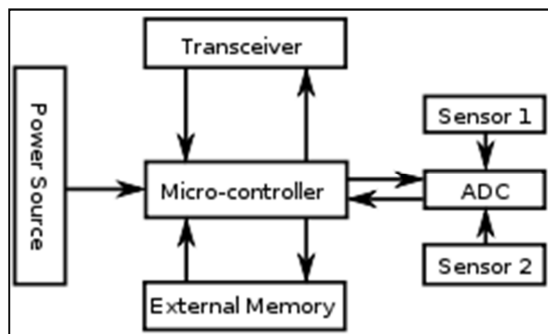


Figure 1. The Typical Architecture of Wireless Sensor Node.

Processor.

The processor performs tasks, processes data and controls the functionality of other components in the sensor node.

Transceiver.

The functionality of both transmitter and receiver are combined into a single device known as transceivers. The operation transmitting, receives, idle, and sleep. The idle state is when the transceiver is neither transmitting nor receiving, and the sleep mode is when it is turned off. The receive and idle states may require as much energy as transmitting, while the sleep state requires the less energy. Thus, it is better to completely shut down the transceiver rather than leave it in the idle mode when it is not transmitting or receiving.

External Memory.

Two categories of memory based on the purpose of storage are: user memory used for storing application related or personal data, and program memory used for programming

the device. Program memory also contain identification data of the device if present.

Power Source.

The sensor node consumes power for sensing, communicating and data processing more energy is required for data communication than any other process. Batteries, both rechargeable and non-rechargeable, are the main source of power supply for sensor nodes.

Sensors.

Sensors are hardware devices that produce a measurable response to a change in a physical condition like temperature or pressure. Sensors measure physical data of the parameter to be monitored. The continual analog signal produced by the sensors is digitized by an analog-to-digital converter and sent to controllers for further processing. A sensor node should be small in size, consume extremely low energy, operate in high volume, be autonomous and operate un attended, and be adaptive to the environment. As wireless sensor nodes are typically very small electronic devices, they can only be equipped with a limited power source

3. Characteristics and Constraints of WSN

Some of the unique characteristics and constraints of WSN includes:

- The sensor nodes are densely deployed in the specific region of interest.
- These nodes after deployment can automatically self-configure into a network
- The sensor network topology changes frequently.
- The nodes are usually battery powered.
- They are equipped with limited resources.
- They are prone to failures.
- They are application specific.

There for most sensor network design objectives include fault tolerance, scalability, self-configurability, production cost, hardware constraints, sensor network topology, and environment consideration sand power consumption.

Fault Tolerance: Individual nodes are pontoon expected failure with a much higher probability than other types of networks. The network should sustain information dissemination inspire of failures.

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.

Self Configurability: The sensor nodes after deployment should be able to automatically self-configure in to a network.

Production Costs: The cost of a single node must below.

Hardware Constraints: A sensor node is comprised of many subunits. All these units combined to gather must consume extremely low power and be contained within an extremely small volume.

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

Environment: Nodes are operating in inaccessible locations because of hostile environment.

Power Consumption: Power conservation and power management are primary design factors.

4. Coverage Problem of WSN

An important problem addressed in Wireless Sensor Network is Coverage Problem. It is basically concerned with a question: How efficiently the specific region of interest is being covered by the sensor nodes? This problem can be considered as a decision problem, whose goal is to determine whether every point in the service area of the sensor network is covered by atleast one sensor node. The cover age concept is a measure of the quality of service of the sensing function and is subject to a wide range of interpretation due to a large variety of sensors and applications. The objective is to have the region monitored by at least one sensor node.

The Coverage Problem may be broadly classified into the following main categories:

- Area Coverage Problem where the goal is to monitor a specific region or area.
- Target Coverage Problem where the goal is to monitor a specific set of targets or points.

In this paper we will be dealing only with the Target Coverage Problem which is concerned with the coverage of specific targets by the sensor nodes. These nodes require energy for performing the coverage task. Since, the sensor nodes are usually battery powered; there for judicious management of energy is an important concern so that coverage task can be performed for a maximum duration. In this paper, we propose an algorithm to perform the coverage task with minimum participation of sensor nodes to cover the targets, there by consuming minimum energy.

5. Applications of WSN

The original motivation behind the research into WSN was military application. As the cost for sensor nodes and communication networks have been reduced, many other potential applications have emerged. The following area few fields including military application where Wireless Sensor Networks have a great contribution:

- National Security

Wireless sensor networks can be an integral part of military command, control, communications, computing, intelligence, surveillance, reconnaissance and targeting systems. The rapid deployment, self-organization and fault tolerance characteristics of sensor networks

- Environment observation, Habitat Monitoring and forecasting

Some environmental applications of sensor networks include tracking the movements of birds, small animals, and insects; monitoring environmental conditions that effect crops and lives tock; irrigation; macro instruments for large-scale Earth monitoring and planetary exploration; chemical/biological detection; precision agriculture; biological, Earth,

and environmental monitoring in marine, soil, and atmospheric contexts; forest fire detection; meteorological or geo physical research; flood detection; bio-complexity mapping of the environment; and pollution study

- Health Applications

Some of the health applications for sensor networks are providing interfaces for the disabled; integrated patient monitoring; diagnostics; drug administration in hospitals; monitoring the movements and internal processes of insects or other small animals; tale monitoring of human physiological data; and tracking and monitoring doctors and patients inside a hospital

- Home Applications.

As the technology advances, smart sensor nodes and actuators can be buried in appliances, such as vacuum cleaners, micro-wave ovens, refrigerators, and VCRs These sensor nodes inside the domestic devices can interact with other and with the external network via the Internet or Satellite. They allow end users to manage home devices locally and remotely more easily.

- Commercial Applications

Some of the commercial application share monitoring material fatigue; building virtual key boards; managing inventory; monitoring product quality; constructing smart office spaces; environmental control in office buildings; robot control and guidance in automatic manufacturing environments; interactive toys; interactive museums; factory process control and automation; monitoring disaster area; smart structures with sensor nodes embedded in side; machine diagnosis; transportation; factory instrumentation; local control of actuators; detecting and monitoring car thefts; vehicle tracking and detection; and instrumentation of semiconductor processing chambers, rotating machinery, wind tunnels, and anechoic chambers

6. Conclusion

In this paper, we have discussed about Wireless Sensor Network, its characteristics, constraints and applications. Coverage of the specific region of interest is an important issue of Wireless Sensor Network.

References

- [1] M. Cardei, M. T. Thai, Yingshu Li and Weili Wu, "Energy-Efficient Target Coverage in Wireless Sensor Networks," 24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM2005), Pp: 1976-1984, vol. 3, 13-17 March 2005.
- [2] M. Cardei and J. Wu, "Energy-Efficient Coverage Problems in Wireless Ad-hoc Sensor Networks", Computer Communications Journal (Elsevier), Vol. 29, No. 4, pp: 413-420, Feb. 2006.
- [3] Zongheng Zhou, Samir R. Das, Himanshu Gupta. "Connected K-Coverage Problem in Sensor Networks", Proceedings of the International Conference on Computer Communications and Networks (ICCCN2004), October 11-13, 2004, Chicago, IL, USA 2004, pp-373-378.

- [4] J. Carle and D. Simplot, "Energy Efficient Area Monitoring by Sensor Networks", IEEE Computer, Vol 37, No 2 (2004), pp 40-46.
- [5] S. Slijepcevic, M. Potkonjak, "Power efficient organization of wireless sensor networks", IEEE International Conference on Communications, vol. 2, pp 472-476, Helsinki, Finland, June 2001.
- [6] K. Kar and S. Banerjee, "Node Placement for Connected Coverage in Sensor Networks", Proc. Of Wi Opt 2003: Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (2003).
- [7] Yu Gu, Jie Li, Baohua Zhao, and Yusheng Ji, "Target Coverage Problem in Wireless Sensor Networks: A Column Generation Based Approach," in Proceedings of 6th IEEE International Conference on Mobile Ad-hoc and Sensor Systems (2009).
- [8] I.F. Akyildiz, W. Su, Y. Sankara subramaniam and E.Cayirci, "A Survey on Sensor Networks", IEEE Communications Magazine, (Aug.2002), pp 102-114.
- [9] S. k. Padi and P. K. Pattnaik, "A Novel Distributed Protocol For Randomly Deployed Clustered Based Wireless Sensor Network", Journal of Theoretical and Applied Information Technology, Vol 15. No. 1, 2010.
- [10] X.-Y. Li, P.-J. Wan and O. Frieder, "Coverage in Wireless Ad-hoc Sensor Networks", IEEE Transactions on Computers, Vol 52(2002), pp 753-763.