Wireless Sensor Networks: Issues, Challenges & Solutions

Kavita Choudhary* & Dr. Seema Verma**
*Sr. Assistant Professor, Department of CSE, JIET, Jodhpur
**Associate Professor, Department of Electronics, Banasthali Vidyapith

Abstract:- **This electronic document Over the last decade, Wireless Sensor Networks have become an interesting area of research because of their numerous applications and the possibility of integrating them into more complex network systems. Wireless Sensor Network has such features that it has emerged as a promising tool for monitoring the physical world with wireless sensors that can sense, process and communicate. This paper provides an overview of WSNs, sensor architecture and the various issues encountered as challenges which need to be considered for research efforts. This paper also presents the possible solutions to the considered issues.**

I. Introduction

As we compare the past & recent years, the way how people communicate has changed. Due to advances in technology as well as the demands of applications, various classes of wireless networks have emerged such as Cellular Networks, Ad hoc Networks, Sensor Networks etc. **Cellular networks**, also termed as infrastructure dependent networks consist of mobile devices roaming an area that is divided into cells, with a base station located in every cell which serves the devices. **Ad-hoc networks**, termed as infrastructure independent are deployed without an existing infrastructure. Mobile devices communicate among themselves by relaying the message over many devices. **Sensor networks** consist of very small devices deployed in some areas to perform monitoring, tracking, and reports its finding to some central node.
Thus, *a wireless sensor network is an array of sensor nodes organized into a cooperative network, which communicates wirelessly and where each node consists of processing capability, multiple types of memories, a RF transceiver, a power source, and also accommodate various sensors and actuators.*

Architecture of WSNs:

A typical WSN architecture consists of a sensor field, which is in actual a physical environment where the sensor nodes or devices are deployed. These nodes communicate to a powerful BS that links them to a central manager for processing the sensed data.

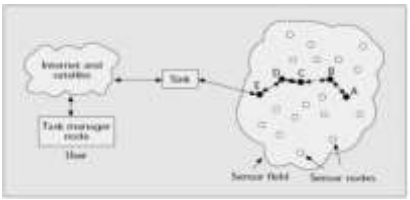

Fig 1. Architecture of WSNs

What actually does these sensors are composed of? A sensor device primarily has a sensing unit that performs the actual sensing tasks. The processing unit performs computations on the sensed data in conjunction with a storage unit and handles communication by running the operating system code and works collaboratively with other sensor nodes towards accomplishing the application objectives. The power management unit reduces the power consumption to the maximum extent possible.

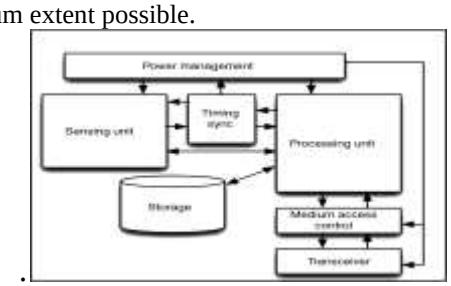

Fig 2. Components of a Sensor node

WSNs Characteristics:

- Sensor nodes are densely deployed and they are prone to failures.
- The number of sensor nodes can be several orders of magnitude higher than the nodes in an ad hoc network.

- The topology of a sensor network changes very frequently.
- Sensor nodes mainly use broadcast communication paradigm.
- Sensor nodes are limited in power, computation capacities, and memory.
- Sensor nodes may not have global identification (ID) because of the large amount of overhead and sensors.

Challenges & Issues in WSNs:

The major issues that affect the design and performance of WSNs are as follows:

Hardware Design:
Radio range is critical for ensuring network connectivity and data collection in a network as the environment being monitored may not have an installed infrastructure and thus the nodes may not establish connection for many days or may go out of range after establishing connection. So, Radio Range should be high. Memory Chips like flash memory is recommended as they are inexpensive and volatile. Power Consumption should be minimized and sensor nodes should be energy efficient since it determines their lifetime. For this, the node should shut off the supply when not in use. Platforms like Mica2, MicaZ, Telos, BT Node and Imotes and MIT μAMPS have been introduced.
Then what is next?
Different strategies to improve signal reception, design of low power, low cost sensors and processing units, schemes to conserve node power consumption, node optimization and simple modulation schemes need to be considered.

Operating System:
An operating system framework should be able to provide resource management as well as memory management in a constrained environment. A sensor node processes the extracted data and manipulates the data as per the requirement. This requires real time response, processing and routing of the data. So concurrency management is needed. An OS should be hardware independent and application specific. It should support multihop routing and user level abstractions. The OS should have inbuilt features to reduce the consumption of energy. The OS should be priority based. Various OS for sensor nodes like TinyOS, Mantis Operating System and Nano-Qplus have been already designed.

Radio Communication:
Low power consumption is needed to enable long operating lifetime by facilitating low duty cycle operation, local signal processing. Distributed Sensing effectively acts against various environmental obstacles and care should be taken that the signal strength is not reduced by reflection, scattering and dispersions. Multihop networking may be adapted to reduce link range & density of sensor nodes should be high.
Then what is next?
Low power consuming communication systems, CMOS circuit techniques, new architecture for integrated wireless sensor systems, modulation method and data rate selection need to be designed to make the communication more effective.

Architecture:
The main factor for currently limiting progress is lack of an overall architecture. To bridge the gap between raw hardware capabilities and a complete system, Software architecture is needed. A durable and scalable architecture would allow dynamic changes to be made for the topology with minimum update messages being transmitted. The architecture must provide precise control over radio transmission timing. The architecture must decouple the data path speed and the radio transmission rate.

Medium Access Schemes:
The MAC layer provides fine-grained control of the transceiver and allows on and off switching of the radio to conserve energy. A MAC protocol should avoid collisions from interfering nodes, over emitting, overhearing, control packet overhead and idle listening. The sensor network should adapt to the changes in the network size, node density and topology. A MAC protocol should include Message Passing. The MAC protocols should take care of Information Asymmetry. MAC Protocols should satisfy the Real-time requirements. Some are S-Mac (Sensor MAC), B-Mac, ZMAC, Time-MAC.
Then what is next?
By reducing the potential energy wastes at MAC layer, energy can be conserved. Fine tuning of the radio parameters is also required as it is the main source of energy consumption. MAC protocols should be more susceptible to the movement of nodes i.e. mobility at the MAC layer. Beside these all Optimization criteria such as latency, compliance with real time constraints or reliable data delivery for MAC protocols need to be considered.

Deployment:
Deployment of sensor network is a labor intensive and cumbersome activity. Node death due to energy depletion either caused by normal battery discharge or due to short circuits is a common problem. Deployment of sensor networks results in network congestion due to many concurrent transmission attempts. This occurs due to inappropriate design of the MAC layer or by repeated network floods. Another issue is the physical length of a link. Two nodes may be very close but still they may not be able to communicate due to physical interference while nodes which are far away may communicate with each other. Low data yield is another common problem in real world deployment.
Then what is next?
When radio antennas are deployed in physical phenomenon, it is required to improve the range and visibility of them and wrong sensor readings should be detected at the earliest, to reduce latency and reduce congestion.
Routing:
As energy efficiency is a very important criterion, we need to find various methods for discovering energy efficient routes and relaying the data from the sensor nodes to the BS. Routing Protocols should incorporate multi-path design technique. Path repair is desired in routing protocols whenever a path break is detected. The routing protocol should exploit redundancy to improve energy and bandwidth utilization. Routing Protocols should take care of heterogeneous nature of the nodes. Various type of routing protocols are SPIN, Rumor Routing, Direct Diffusion, LEACH, TEEN, GEAR, Sequential Assignment Routing SAR etc.
Then what is next?
Sensor networks are still at an early stage in terms of technology as it is still not widely deployed in real world. The current routing protocols need to be improved as they have their own set of problems. Much work is not reported on contention issues or high network traffic.

Transport Layer:
In sensor networks the loss of data, when it flows from source to sink is generally tolerable. But the data that flows from sink to source is sensitive to message loss. Traditional transport protocols such as UDP and TCP cannot be directly implemented in sensor networks for the following reasons:
1. The flow and congestion control mechanism cannot be applied for them.
2. Successful end to end transmissions of packets are not necessary in an event driven application.
3. Overhead in a TCP connection does not work well for an event driven application.
4. UDP has a reputation of not providing reliable data delivery and has no congestion or flow control mechanisms.
Another problem is failure of nodes due to battery depletion. Pump Slowly, Fetch Quickly (PSFQ) are one of the popular transport layer protocol.
Then what is next?
Developing transport protocols for sensor networks is itself a difficult task. Existing transport layer protocols assume that the network layer uses a single path routing and multi path routing is not considered. Since sensor nodes are placed in various types of environment, the data from different locations will have different priorities, thus transport protocols should consider priority while routing.

Middleware:
Middleware should provide an interface to the various types of hardware and networks supported by primitive operating system abstractions. This should provide new programming paradigm for application specific API's rather than dealing with low level specifications. This should include mechanisms to provide real time services by dynamically adapting to the changes in the environment and providing consistent data. This should support QoS considering constraints which are unique to sensor networks like energy, data, mobility & aggregation. Mate is one of the available middleware architecture.
Then what is next?
One needs to design developer friendly middleware architecture which is not only generic but also should take care of all the underlying hardware intricacies while helping to reduce the energy consumption and provide adequate quality of support.

Localization:
Determining the physical location of the sensors after they have been deployed is known as the problem of localization. The localization algorithm should be distributed since a centralized approach requires high computation at selective nodes to estimate the position of nodes. Localization algorithms should be robust enough to localize the failures and loss of nodes. It should be tolerant to error in physical measurements. Localization algorithm should be accurate, scalable and support mobility of nodes.
Then what is next?

It is required to design a system to track the location of valuable assets in an indoor environment so the maximum likelihood estimation in a distributed environment needs to be improved. Mobile assisted localization need to be designed with better localization accuracy.

Synchronization:
Time Synchronization in a sensor network aims to provide a common timescale for local clocks of nodes in the network. A global clock in a sensor system will help process and analyze the data correctly and predict future system behavior. Sensor nodes have higher degree of failures. Thus the synchronization protocol needs to be more robust to failures and to communication delay. The algorithm for sensor network clock synchronization needs to achieve multihop synchronization even in the presence of high jitter. Reference Broadcast Synchronization and Delay Measurement Time Synchronization protocol are used recently.
Then what is next?
Analytical models for multihop synchronization need to be built. The radio communication in the existing synchronization protocols are required to be improved.

Programming Paradigms:
Currently, programmers are too much concerned with low level details raising a need for programming abstractions. Programming models should help programmers in writing energy efficient applications. We need to reduce the run time errors and complexity since the applications in a sensor network need to run for a long duration without human intervention. Programming models should help programmers to write bandwidth efficient programs and should be accompanied by runtime mechanisms that achieve bandwidth efficiency whenever possible. TinyOS with Nesc and TinyGALS are examples for this category. Improving programming ease in languages such as Nesc and galsC itself provides tremendous opportunities for research.

Calibration:
Calibration is the process of adjusting the raw sensor readings obtained from the sensors into corrected values by comparing it with some standard values. Manual calibration is a time consuming, expensive and difficult task. Other objectives of calibration include accuracy, resiliency against random errors, ability to be applied in various scenarios and to address a variety of error models.
Then what is next?
Calibration techniques involving the various issues are required to be designed.

Data Aggregation & Dissemination:
Data gathering is the main objective of sensor nodes. Data Aggregation is defined as the process of aggregating the data from multiple sensors to eliminate redundant transmission and estimating the desired answer about the sensed environment, then providing fused information to the base station. Data dissemination is a process by which data and the queries for the data are routed in the sensor network. Sensor networks are inherently unreliable and certain information may be unavailable or expensive to obtain. So, eliminate redundant data transmission using meta- data negotiations. Improve clustering techniques for data aggregation to conserve energy of the sensors and network aggregation techniques to improve energy efficiency.
Then what is next?
Main focus is geared towards conserving energy. Other issues include improving security in data transmission and aggregation, handling tradeoffs in data aggregation, improving QoS of the data aggregation protocols.

Database Centric and Querying:
Sensor networks should be able to accept the queries for data and respond with the results. The data flow in a sensor database is different from the traditional database because of the following design issues and requirements:
1) The nodes are volatile since they may get depleted and links may go down at any point of time but data collection should be interrupted as little as possible.
2) Sensor data is exposed to more errors due to interference of signals and noise.
3) Sensor networks produce data continuously in real time, on a large scale; whereas a traditional database is mostly of static and centralized in nature.
4) Limited storage and scarce of energy is another constraint but a traditional consists of plenty of resources and disk space.
5) The low level primitives in the sensor networks are designed in terms of named data rather than the node identifiers.
Then what is next?
Sensor database include spatial-temporal querying, multi-query optimization, storage placement, a distributed long term networked data storage, low energy communication overhead, various ways of representing the sensor

data, processing and distributing query fragments, dealing with communication failures and designing various models for deploying and managing a sensor database systems are need to be designed.

Quality of Service (QoS):
Quality of Service (QoS) for sensor networks is defined as the optimum number of sensors sending information towards information-collecting sinks or a base station. Nodes may join, leave and rejoin and links may be broken at any time. Hence maintaining and re-establishing the paths dynamically, which is a problem in WSN, is not a big issue in wired networks. The QoS is difficult because the network topology may change constantly and the available information for routing is inherently imprecise. Traffic is unbalanced in sensor network since the data is aggregated from many nodes to a sink node. QoS mechanisms should be designed for an unbalanced QoS constrained traffic. Even though multihops reduce the amount of energy consumed for data collection the overhead associated with it may slow down the packet delivery. Also, redundant data makes routing a complex task thus affects QoS. QoS should be able to support scalability. Adding or removing of the nodes should not affect the QoS. One of the very first protocols which had QoS support was the Sequential Assignment Routing (SAR).
Then what is next?
Designing an appropriate QoS model, deciding how many layers need to be integrated, support for heterogeneous nodes, designing QoS model for specific applications, designing QoS based protocols to integrate them with other network like cellular, LANs and IP, and designing QoS via middleware layer.

Security:
Security in sensor networks is as much an important factor as performance and low energy consumption in many applications. The basic security requirements are: Confidentiality to ensure information is well protected and not revealed to unauthorized parties; Authentication to verify the identity; Integrity; Message reply attack; Secure management is needed at the BS and Security mechanisms like encryption so that the overhead is minimized and should not affect the performance of the network.
Then what is next?
The security issues posed by sensor networks are an interesting field for research. Routing protocols having built in security features, a new symmetric key cryptography for sensor networks, secure data aggregation protocols, intrusion detection systems and security systems for multimedia sensors are needed to be designed.

II. Conclusion

The impact of wireless sensor networks on our day to day life can be preferably compared to what Internet has done to us. This field is surely going to give us tremendous opportunity to change the way we perceive the world today. In this paper we have identified a comprehensive list of issues associated with WSNs as well as the state-of-art and future direction in WSNs. But still a lot of work needs to be done in it in order to make it more mature and an acceptable technology.

References

[1] “A survey of Wireless Sensor Network technologies: research trends and middleware’s role” Eiko Yoneki and Jean Bacon, University of Cambridge Computer Laboratory, Cambridge CB3 0FD, United Kingdom.
[2] “Wireless Sensor Networks” F. L. LEWIS Associate Director for Research Head, Advanced Controls, Sensors, and MEMS Group Automation and Robotics Research Institute The University of Texas at Arlington 7300 Jack Newell Blvd. S Ft. Worth, Texas 76118-7115.
[3] “Sensor Networks: An Overview” Archana Bharathidasan, Vijay Anand Sai Ponduru, Department of Computer Science University of California, Davis, CA 95616
[4] “Chapter 13: Wireless Sensor Networks” Networking Fundamentals: Wide, Local and Personal Area Communications, by Kaveh Pahlavan and Prashant Krishnamurthy.
[5] “Wireless Sensor Networks” John A. Stankovic Department of Computer Science University of Virginia Charlottesville, Virginia 22904 June 19, 2006
[6] “Wireless Sensor Network Security: A Survey” John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary *Department of Computer Science, Wayne State University.*
[7] “Current and Future Trends in Sensor Networks: A Survey” Mokhtar Aboelaze* Fadi Aloul Dept. of Computer Science and Engineering York University; Toronto, ON. Canada Dept. of Computer Engineering American University of Sharjah Sharjah, UAE.
[8] “INSENS: Intrusion-Tolerant Routing in Wireless Sensor Networks” Jing Deng, Richard Han, Shivakant Mishra Department of Computer Science, University of Colorado, Boulder, CO 80309-0430.
[9] “Networking Issues in Wireless Sensor Networks” Deepak Ganesan, Alberto Cerpa, Wei Ye, Yan Yu, Jerry Zhao, Deborah Estrin.
[10] “Research Challenges for Wireless Sensor Networks” John A. Stankovic Department of Computer Science, University of Virginia.
[11] “Issues in Wireless Sensor Networks” Gowrishankar.S, G.Basavaraju, Manjaiah D.H, Subir Kumar Sarkar.
[12] “Wireless sensor networks: a survey” I.F. Akyildiz, W. Su*, Y. Sankarasubramaniam, E. Cayirci Broadband and Wireless Networking Laboratory, School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332, USA Received 12 December 2001; accepted 20 December 2001.
[13] “Wireless Sensor Networks: Energy Efficiency, Delay Guarantee and Fault Tolerance” Sinem Coleri Ergen, B.S. (Bilkent University, Ankara) 2000 M.S. (University of California, Berkeley) 2002.

[14] "Wireless Sensor Networks: Applications and Challenges of Ubiquitous Sensing" Daniele Puccinelli and Martin Haenggi, IEEE Circuits and Systems Magazine.
[15] "Wireless Sensor Networks - New Challenges in Software Engineering" Jan Blumenthal, Matthias Handy, Frank Golatowski, Marc Haase, Dirk Timmermann Institute of Applied Microelectronics and Computer Science Dept. of Electrical Engineering and Information Technology, University of Rostock, Richard-Wagner-Str. 31, 18119 Rostock, GERMANY
[16] "Middleware Challenges for Wireless Sensor Networks" Kay R¨omer, Oliver Kasten, Friedemann Mattern Department of Computer Science, ETH Zurich, Switzerland.