

Energy Efficient Wireless Sensor Activities in Computer Networks

T. Bhuvaneswari¹

Research Scholar

Department of Computer Application

Dr. A.P.J. Abdul Kalam University, Indore, India

buvaneshvaribuvaneshvari879@gmail.com

Dr. Atul Dattatray Newase²

Research Supervisor

Department of Computer Application

Dr. A.P.J. Abdul Kalam University, Indore, India

dr.atulnewase@gmail.com

Abstract: A Wireless Sensor Network (WSN) can be described as a sophisticated ensemble of interconnected devices that collaborate to relay information collected from a designated observation area. This network architecture enables the transmission of data across various nodes, ultimately converging at a gateway that integrates the data into larger networks, such as wireless Ethernet. Essentially, a WSN consists of base stations and numerous nodes equipped with wireless sensors. Modern iterations of these networks support bi-directional communication, not only facilitating the collection of sensor data but also allowing for the remote control and adjustment of sensor operations. Initially spurred by military needs for comprehensive battlefield surveillance, the utility of wireless sensor networks has expanded significantly. Today, they are integral to a variety of both industrial and consumer contexts, ranging from monitoring and controlling industrial processes to assessing the condition of machinery in real time.

Keywords : Wireless Sensor Net, Bi-Directional, Machine Health Monitoring, Wireless Ethernet, Micro-Electro Mechanical Systems.

I. INTRODUCTION

Sensor networks are highly distributed networks of small, lightweight wireless nodes deployed in large numbers to monitor the environment or system by the measurement of physical parameters such as temperature, pressure or relative humidity. Building sensors has been made possible by the recent advances in micro-electro mechanical systems (MEMS) technology.

Each node of the sensor network consists of three subsystems, the sensor sub – system which sensor the environment, the processing subsystem which performs local computations on the sensed data, and the communication subsystem which is responsible for message exchange with neighboring sensor nodes. While individual sensors have limited sensing region, processing power, and energy, networking a large number of sensors gives rise to a robust, reliable and accurate sensor network covering a wider region. The network is fault-tolerant because many nodes are sensing the same events. Further, the nodes cooperate and collaborate on their data, which leads to accurate sensing of events in the environment. The two most important operations in a sensor network are data

dissemination, that is the propagation of data/queries throughout the network, and data gathering, that is the collection of observed data from the individual sensor nodes to a sink.

Finally some sensor – network specific issues such as energy – efficient hardware design, synchronization, transport layer protocols, security and real-time communication are discussed.

Application of Sensor Networks

Sensor nodes are used in a variety of applications which require constant monitoring and detection of specific events. The military applications of sensor nodes include battlefield surveillance and monitoring, guidance systems of intelligent missiles, and detection of attach by weapons of mass destruction such as chemical, biological or nuclear. Sensors are also used in environmental applications such as forest fire and flood detection, and habitat exploration of animals. Sensors can be extremely useful in patient diagnosis and monitoring. Patients can wear small sensor devices that monitor their physiological data such as heart rate or blood pressure. The data collected can be sent regularly over the

network to automated monitoring systems which are designed to alert the concerned doctor on detection of an anomaly. Such systems provide patients a greater freedom of movement instead of their being confined to a hospital. Sensor nodes can also be made sophisticated enough to correctly identify allergies and prevent wrong diagnosis.

Comparison with Ad Hoc Wireless Networks.

While both ad hoc wireless networks and sensor network consist of wireless nodes communicating with each other, there are certain challenges posed by sensor networks. The number of nodes in a sensor network can be several orders of magnitude larger than the number of nodes in an ad hoc network. Sensor nodes are more prone to failure and energy drain, and their battery sources are usually not replaceable or rechargeable. Sensor nodes may not have unique global identifiers, so unique addressing is not always feasible in sensor networks.

The main goals of data fusion are to reduce bandwidth consumption, media access delay, and power consumption for communication.

Issues and Challenges in Designing a Sensor Network

Sensor networks pose certain design challenges due to the following reasons:

- Sensor nodes are randomly deployed and hence do not fit into any regular topology. Once deployed, they usually do not regular topology. Once deployed, they usually do not require any human intervention. Hence, the setup and maintenance of the network should be entirely autonomous.
- Sensor networks are infrastructure-less. Therefore, all routing and maintenance algorithms need to be distributed.
- An important bottleneck in the operation of sensor nodes is the available energy. Sensors usually rely only on their battery for power, which in many cases cannot be recharged or replaced. Hence, the available energy at the nodes should be considered as a major constraint while designing protocols. For instance, it is desirable to give the user an option to trade off network lifetime for fault tolerance or accuracy of results.
- Hardware design for sensor nodes should also consider energy efficiency as a primary requirement. The micro-controller, operating system, and application software should be designed to conserve power.
- Sensor nodes should be able to synchronize with each other in a completely distributed manner, so the TDMA schedules can be imposed and temporal ordering of detected events can be performed without ambiguity.

- A sensor network should also be capable of adapting to changing connectivity due to the failure of nodes, or new nodes powering up. The routing protocols should be able to dynamically include or avoid sensor nodes in their paths.
- Real-time communication over sensor networks must be supported through provision of guarantees on maximum delay, minimum bandwidth, or other QoS parameters.

II. SENSOR NETWORK ARCHITECTURE

2.1 Layered Architecture

A layered architecture has a single powerful base station (BS), and the layers of sensor nodes around it correspond to the nodes that have the same hop-count to the BS.

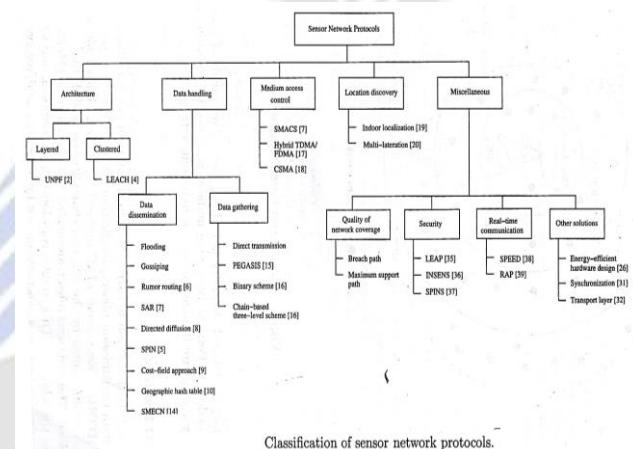


Figure 1. Classification of sensor network protocols.

Layered architectures have been used with in-building wireless backbones, and in military sensor-based infrastructure, such as the multi-hop infrastructure network architecture (MINA) [2]. In the in-building scenario, the BS acts an access point to a wired network, and small nodes form a wireless backbone to provide wireless connectivity. The users of the network have hand-held devices such a PDAs which communicate via the small nodes to the BS. Similarly, in a military operation, the BS is a data-gathering and processing entity with a communication link to a larger network. A set of wireless sensor nodes in accessed by the hand-held devices of the soldiers. The advantage of a layered architecture is that each node is involved only in short-distance, low-power transmissions to nodes of the neighboring layers.

Unified Network Protocol Framework (UNPF) : UNPF [2] is a set of protocols for complete implementation of a layered architecture for sensor networks. UNPF integrates three operations in its protocol structure: network initialization and maintenance, MAC, and routing protocols.

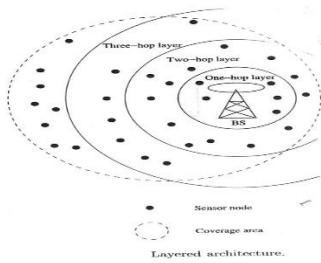


Figure 2. Layered architecture.

• Net work Initialization and Maintenance Protocol

The network initialization protocol organizes the sensor nodes into different layers, using the broadcast capability of the BS. The BS can reach all nodes in a one-hop communication over a common control channel. The BS broadcasts its identifier (ID) using a known CDMA code on the common control channel. All nodes which hear this broadcast then record the BS ID. They send a beacon signal with their own IDs at their low default power levels. Those nodes which the BS can hear form layer one since they are at a single-hop distance from the BS. The BS now broadcasts a control packet with all layer one node IDs. All nodes send a beacon signal again. The layer one nodes record the IDs which they hear, and these form layer two, since they are one hop away from layer one nodes. In the next round of beacons, the layer one nodes inform the BS of the layer two nodes, which is then broadcast to the entire network. In this way, the layered structure is built by successive rounds of beacons and BS broadcasts. Periodic beaconing updates neighbor information and alters the layer structure if nodes die out or move out of range.

• MAC Protocol

Network initialization is carried out on a common control channel. During the data transmission phase, the distributed TDMA receiver oriented channel (DTROC) assignment MAC protocol [3] is used. Each node is assigned a reception channel by the BS, and channel reuse is such that collisions are avoided. The nodes schedules transmission slots for all its neighbors and broad-casts the schedule. This enables collision-free transmission and saves energy, as nodes can turn off when they are not involved in a send / receive operation. The two steps of DTROC are channel allocation (the assignment of reception channels to the nodes) and channel scheduling (the sharing of the reception channel among the neighbors). DTROC avoids hidden terminal and exposed terminal problems by suitable channel allocation algorithms.

• Routing Protocol

Downlink from the BS is by direct broadcast on the control channel. The layered architecture enables multi-hop data forwarding from the sensor nodes to the BS. The node to which a packet is to be forwarded is selected considering the remaining energy of the nodes. This achieves a higher network lifetime. Existing ad hoc routing protocols can be

simplified for the layered architecture, since only nodes of the next layer need to be maintained in the routing table.

Clustered Architecture

A clustered architecture organizes the sensor nodes into clusters, each governed by a cluster-head. The nodes in each cluster are involved in message exchanges with their respective cluster-heads, and these heads send messages to a BS, which is usually an access point connected to a wired network. Clustered architecture where any message can reach the BS in at most hops. Clustering can be extended to greater depths hierarchically.

Clustered architecture is specially useful for sensor networks because of its inherent suitability for data fusion. The data gathered by all members of the cluster can be fused at the cluster-head, and only the resulting information needs to be communicated to the BS. Sensor networks should be self-organizing, hence the cluster formation and election of cluster-heads must be an autonomous, distributed process. This is achieved through network layer protocols such as the low-energy adaptive clustering hierarchy.

III. CONCLUSION

Sensor networks establish a ubiquitous distributed network that forms the backbone of an intelligent environment. These networks have a broad spectrum of applications, including intelligent building management, automated control in chemical manufacturing facilities, ecological habitat monitoring, and discreet operations in military contexts. Research in this field is primarily focused on addressing the core challenges of scalability, reliability, robustness, and power efficiency. The goal is to develop sensor networks capable of functioning effectively within highly constrained environments, thereby enabling their deployment in a diverse range of applications.

BIBLIOGRAPHY

1. I.F. Akyildz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A Survey on Sensor Networks," *IEEE Communication Magazine*, vol. no. 8, pp.102-114. August 2002.
2. J. Ding, "Design and Analysis of an Integrated MAC and Routing Protocol Framework for Large-Scale Multi-Hop Wireless Sensor Networks," *Technical Report*, Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore, July 2002.
3. "Integrated MAC and Routing Protocol Framework for Large Scale Multi-Hop Wireless Sensor Networks," Department of Electrical Engineering and Computer Science, Washington State University, <http://jaguar.eecs.wsu.edu/jding1/presentations/poster.pdf>.
4. W. Heinzelman, A. Chandrakasan, and Balakrishnan, "Energy-Efficient Communication Protocol for Wireless

- Microsensor Networks,” *Proceedings of HICSS 2000*, pp. 4-7, January 2000.
5. W.R. Heinzelman, J. Kulik, and H. Balakrishnan, “Adaptive Protocols for Information Dissemination in Wireless Sensor Networks,” *Proceedings of ACM MOBICOM 1999*, pp. 174-185, August 1999.
6. D. Braginsky and D. Estrin, “Rumor Routing Algorithm for Sensor Networks,” *Proceedings of ACM Workshop on Wireless Sensor Networks and Applications 2002*, pp. 22-31, September 2002.
7. K. Sohrabi, J. Gao, V. Ailawadhi, and G.J. Pottie, “Protocols for Self-Organization of a Wireless Sensor Network,” *IEEE Personal Communications Magazine*, vol.7, no 5, pp. 16-27, October 2000.
8. C. Intanagonwiwat, R. Govindan, and D. Estrin, “Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks,” *Proceedings of ACM MOBICOM 2000*, pp. 56-67, August 2000.
9. F. Ye, A. Chen, S. Lu, and L. Zhang, “A Scalable Solution to Minimum Cost Forwarding in Large Sensor Networks,” *Proceedings of IEEE ICCCN 2001*, pp. 204-309, October 2001.
10. S. Ratnasamy et.al., “GHT: A Geographic Hash Table for Data-Centric Storage,” *Proceedings of ACM Workshop on Wireless Sensor Networks and Applications 2002*, PP. 78-87, September 2002.

