International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Communication Protocols for Wireless Sensor Networks (WSNs): A Comprehensive Review

Pinki[1], *Sumit Dalal*[2], *Rohini Sharma*[3], *Sumiran*[4]

[1]Student, ECE, Sat Kabir Institute of Technology and Management, Bahadurgarh, Haryana
[2] Assistant Professor, ECE, Sat Kabir Institute of Technology and Management, Bahadurgarh, Haryana
[3]Assistant Professor and Corresponding Author, GPGCW, Rohtak, Haryana
[4] Assistant Professor, ECE, Sat Kabir Institute of Technology and Management, Bahadurgarh, Haryana

ABSTRACT:

Wireless Sensor Networks (WSNs) rely on efficient communication protocols to enable seamless data transmission and coordination among sensor nodes in diverse application scenarios. This paper provides an overview of key communication protocols designed specifically for WSNs, focusing on their characteristics, functionalities, and suitability for different deployment scenarios. We discuss protocols spanning multiple layers of the network stack, including MAC protocols for medium access control, routing protocols for data forwarding, transport protocols for message delivery, and network/security protocols for efficient and secure communication. Additionally, we explore localization protocols that enable accurate positioning of sensor nodes within the network. By understanding the strengths and limitations of these communication protocols, network designers can make informed decisions to optimize WSN performance and meet application requirements effectively.

Introduction:

Wireless Sensor Networks (WSNs) consist of spatially distributed autonomous sensors that cooperatively monitor physical or environmental conditions and transmit data wirelessly to a central location (Figure 1). Energy consumption is a critical factor in the design and operation of WSNs due to the limited energy resources of sensor nodes, which are often powered by batteries. Energy-efficient protocols are essential for maximizing network lifetime, reducing maintenance costs, and ensuring reliable data transmission. This comprehensive review explores the principles, mechanisms, and challenges associated with energy-based wireless sensor protocols[1].

In Wireless Sensor Networks (WSNs), "energy holes" [2] refer to areas or regions within the network where nodes deplete their energy rapidly due to heavy data forwarding or processing tasks, leaving other nodes with ample energy resources relatively unused. This non-uniform energy depletion can lead to network partitioning, where certain regions become isolated from others due to node failures caused by energy depletion. Energy holes can severely degrade network performance, leading to reduced coverage, increased latency, and diminished data delivery reliability. There are several reasons of energy holes: Nodes closer to the sink or base station often relay more data than nodes farther away. This non-uniform data traffic distribution can lead to some nodes exhausting their energy resources faster than others. Uneven distribution of sensor nodes can result in certain areas having more nodes than others. As a result, nodes in densely populated areas may deplete their energy faster than nodes in sparsely populated regions. Sensor nodes in WSNs typically rely on battery power, which is finite. Once a node's battery is depleted, it becomes non-functional, potentially creating a void in network connectivity. Inefficient routing protocols may contribute to energy holes by favoring certain paths over others, causing some nodes to handle more traffic than their counterparts. A lot of work has been done to improve the life of sensor networks. Various protocols have been developed to improve the life and efficiency of the sensor networks.

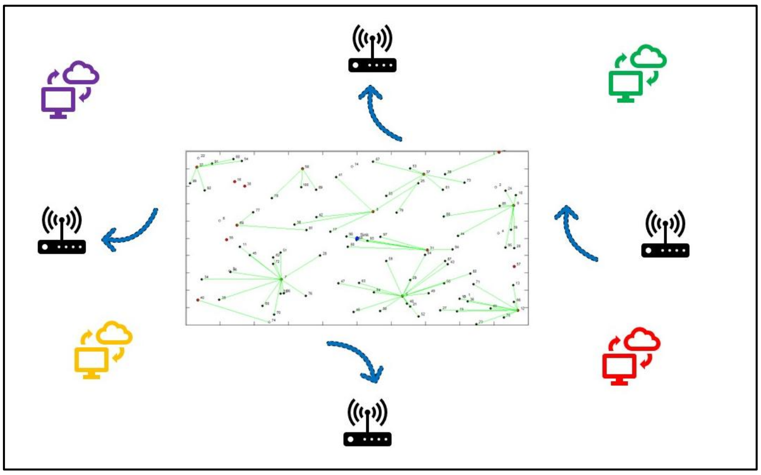

Figure 1: An instance of Wireless Sensor Network

CLASSIFICATION OF WIRELESS SENSOR NETWORKS PROTOCOLS

Wireless Sensor Networks (WSNs) utilize various protocols at different layers of the network stack to facilitate communication, data transmission, and coordination among sensor nodes. Here's an overview of some commonly used protocols in WSNs (Figure 2):

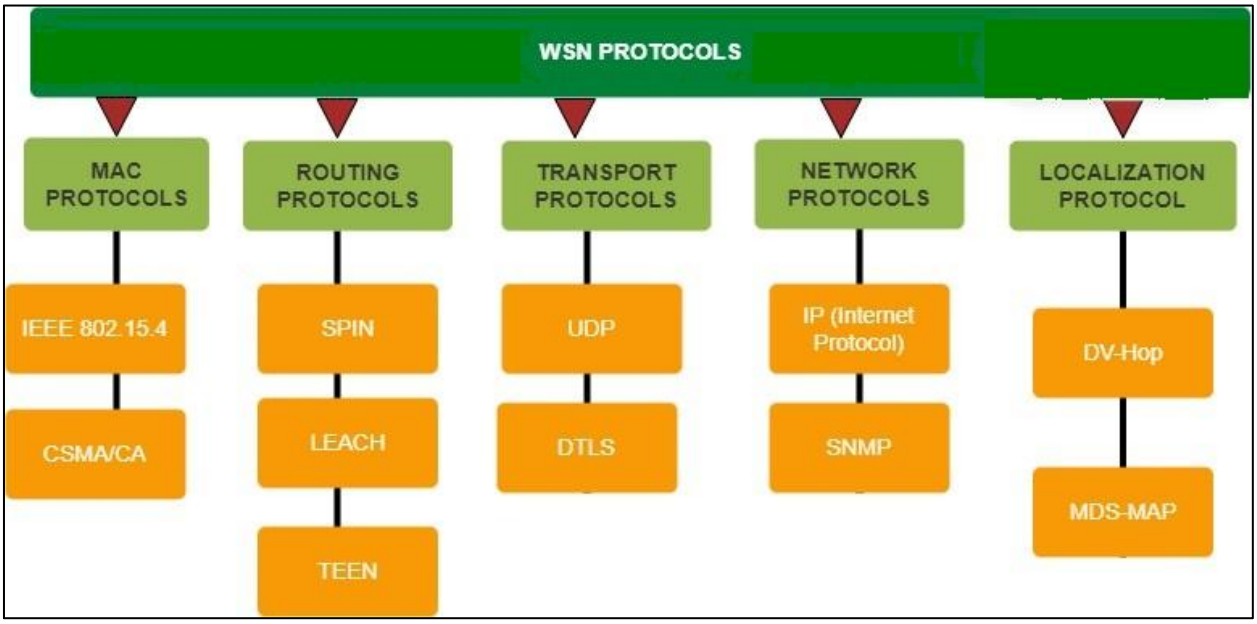

Figure 2: Types of WSN Protocols

MAC (Medium Access Control) Protocols:

- **IEEE 802.15.4**: This standard specifies the physical and MAC layers for low-rate wireless personal area networks (LR-WPANs). It provides mechanisms for channel access, addressing, and frame formats suitable for WSNs. MacMinBE, macMaxCSMABackoffs, and macMaxFrameRetries are medium access control (MAC) parameters that are compatible with the IEEE 802.15.4 standard for wireless sensor networks (WSNs). Such tuning is challenging because there are no straightforward and reliable models that describe how these factors affect packet delay, energy consumption, and the likelihood of a successful packet transmission. Furthermore, it is unclear how to modify the parameter using algorithms that can operate on nodes with limited resources in response to changes in the network and traffic regimes.

  It is suggested to use a generalized Markov chain to represent these relationships using straightforward expressions without sacrificing accuracy. A restricted quantity of retransmissions, acknowledgments, unsaturated traffic, and packet size are taken into consideration. The adaptive algorithm for decreasing power consumption while ensuring reliability and meeting delay restrictions in packet transmission is then derived using the model. The IEEE 802.15.4 standard does not need to be modified in order for the technique to be implemented on network nodes[3]. It is simple to use the suggested adaptive MAC technique on sensor nodes by predicting the channel access probability and busy channel.
- **CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)**: A contention-based MAC protocol where nodes listen to the channel before transmitting to avoid collisions. The CSMA/CA and basic static routing protocol are incorporated into the planned wireless sensor node in order to prevent collisions during data transmission and to pass data throughout the wireless network. To evaluate the implementation's functionality and performance, some experiments are carried out. The outcome demonstrates that the nodes are able to identify the carrier when another device is transmitting and can correctly avoid collisions. Additionally, the experiment demonstrates how effectively the developed routing system forwards data within the network [4].

  The data fusion method makes use of the vast amount of data produced by the Internet of Things (IoT) to enhance the quality of services (QoS) that users have demanded. Usually, data fusion systems gather and combine information from multiple sensor nodes to improve the quality of the data (greater accuracy, precision, or a global view) on the subject of interest. In the particular scenario of a wireless sensor network (WSN) with a cluster-tree topology, channel access—typically controlled by the Carrier-Sens Multiple Access with Collision Avoidance (CSMA/CA) protocol—is the primary determinant of data transmission across nodes and the intermediary data fusion node (DFN). In order to satisfy the demands of WSN real-time data fusion applications and, specifically, to provide improved transmission channel management, an updated CSMA/CA is suggested. It considers a transmission time-delay, dynamically schedules the retransmission, and removes data packets planned after the predetermined time-delay, freeing up the channel for other nodes to use. Additionally, it maximizes the likelihood of obtaining data from every node within the given time-delay before moving forward with the fusion at the DFN level. With the help of the Contiki operating system, the suggested method attempts to gather data from every node in a predetermined amount of time. Simulation and experimental studies indicate that the WSN can reduce collisions, save energy, and increase the amount of data received in a short amount of time. Additionally, two simulated real-time data fusion applications—mobile localization and majority decision-making—are included to corroborate the findings. Utilizing the suggested improved CSMA/CA in both data fusion applications increases QoS in comparison to utilizing CSMA/CA as configured by Contiki [5].

Routing Protocols:

- **LEACH (Low-Energy Adaptive Clustering Hierarchy)**: an appreciated hierarchical routing technique for wireless sensor networks (WSNs) that elects cluster heads to gather data and send it to a base station in an effort to save energy. Numerous initiatives, including energy harvesting, mobile relays, and optimal sensor node deployment, have been made to extend the lifespan of the WSN [6]. The low-energy adaptive clustering hierarchy (LEACH) protocol has been a trailblazer in routing and clustering, helping to minimize the network's energy usage. This protocol creates numerous node clusters, each with a single cluster head (CH) node, using a hierarchical clustering-based routing technique. The CH node is in charge of compiling all information received and transferring it to the base station (BS) once member nodes in all groups provide their data to it. There is various multi-hop hierarchical clustering based protocols in addition to single-hop clustering.
- **TEEN (Threshold sensitive Energy Efficient sensor Network protocol)**: An energy-saving data-centric routing technique that modifies the sample rate in response to environmental events identified. TEEN, a hierarchical clustering protocol, connects sensor nodes to create clusters of nodes, every one of which is run by a CH. Data is gathered by this CH from its member node and forwarded to its upper CH node, which then aggregates and sends the data to the sink node. In this case, the time at which the CH disseminate threshold value for every cluster's member nodes changes [7].
- **SPIN (Sensor Protocols for Information via Negotiation)**: A family of protocols that enable energy-efficient data dissemination by negotiating data exchanges between neighboring nodes. The acronym for sensor protocol for information via negotiation is SPIN. This protocol's purpose is to eliminate shortcomings found in other protocols, such as flooding and communicating. The primary thesis is that data exchange, as perceived by the node, may need more resources than meta-data, which is merely a node-generated descriptor of the sensed data. Every node has a resource manager that keeps an eye on its resources and modifies their functionality as needed [8].
- **Directed Diffusion**: Data-centric protocol that enables energy-efficient data collecting by having nodes communicate attention and data along interest gradients. In networks with random and mesh topologies, the routing technique known as direct diffusion (DD) facilitates communication between source and sink nodes. Employing a data-centric methodology, this routing protocol allows nodes that are intermediate to compile data and forward it to a sink node. Researchers have succeeded in employing Passive Clustering (PC) in conjunction with DD to increase energy efficiency. By dividing the network into smaller clusters and implementing the DD protocol at the application layer, this approach guarantees lower energy costs, better latency, and a higher data transmission rate [9].

Transport Protocols:

Due to their distinct characteristics from typical wired networks, WSNs with extremely limited resources cannot use conventional transport layer protocols like TCP. In WSNs, a variety of applications' traffic is regarded as loss tolerant. The density implantation of sensor nodes and data aggregation properties in wireless sensor networks (WSNs) contribute to loss tolerance and directional dependability. In particular, for nearby sensors that are anticipated to produce significantly correlated data, the design of WSN transport layer protocols should take advantage of directional reliability to reduce the number of transmissions and reduce the computational cost by reducing the amount of data that needs to be aggregated [10].

- **UDP (User Datagram Protocol)**: Often used in WSNs due to its simplicity and low overhead, suitable for applications that prioritize low latency over reliability.
- **DTLS (Datagram Transport Layer Security)**: secures communication in wireless sensor networks (WSNs) by authenticating peers and encrypting data. Large volumes of perhaps sensitive data will be needed to travel across the public Internet due to the enormous number of sensors that are anticipated to be used in Internet of Things applications. This private information might include everything from a smart home's current security state to an older individual linked to smart monitoring' current health state. To link an internal or cloud-based server to the embedded sensors, a reliable and secure connection is necessary. Real-time data access will be made possible by the capacity to guarantee that the information produced by the sensor networks is safely broadcast to the central server[11]. A comparison is made between the widely used Transport Layer Security protocol and the less popular Datagram protocol. According to the study, when it comes to transmitting information from linked Wireless Sensor Networks over the Internet, Datagram Transport Layer Security is a strong substitute for Transport Layer Security.

Network and Security Protocols:

- **IP (Internet Protocol)**: Adapting IP for WSNs enables interoperability with existing networking infrastructure. A standard network layer protocol of the Internet architecture, Internet Protocol (IP) enables communication between heterogeneous networks. A router must adhere to this protocol in order for a network to be reachable via the Internet. Numerous intelligent sensing nodes with computing, networking, and sensing capabilities are included in wireless sensor networks. These intelligent sensors work together to collect pertinent data and display it to the user. Gateway-based or proxy-based techniques have been used to connect sensor networks to the Internet. In the past, a number of routing systems that deliberately discarded IP were developed. With significant input from the 6LoWPAN Working Group, new research, prototypes, and even tools for implementation demonstrate that it is feasible to combine the benefits of IP access with the difficulties of sensor networks [12].

- **SNMP (Simple Network Management Protocol)**: Facilitates management and monitoring of WSNs, allowing administrators to gather information and control sensor nodes remotely. The procedure of overseeing, maintaining, and regulating a network is known as network management. Traditional network administration relied on wired networks, which are bulky and inappropriate for wireless sensor networks with limited resources. Large-scale networks can be created with WSNs, yet managing each node separately is not feasible. Also, there is a significant overhead in management traffic due to the SNMP polling mechanism. Because management messages use up WSN resources, they can have an impact on the network's performance. Consequently, energy-efficient network management is a must for WSNs [13].
- **SPINS (Security Protocols for Sensor Networks)**: A suite of security protocols tailored for WSNs, providing services such as secure communication, data confidentiality, integrity, and authentication. Because of its high level of efficiency, sensor networks are the leading technology in wireless communication. Whether they are other networks or sensor networks, security is a crucial concern for all kinds of networks. Many researchers have attempted to physically develop sensor networks and nodes thus far, but their efforts have not yielded sufficient results to provide meaningful security for various connecting devices during communication operations. Because sensor networks operate in very resource-constrained environments, this study provides a model based on SPINS security building blocks. Simply SPINS security protocol can meet the specifications of the suggested framework. SNEP and TESLA are the two security building components that SPINS offers. Some special processing unit features, like the data controller unit and beacon message, are presented by this model. Although this security model is the most effective at achieving goals, the primary problems with sensor networks—namely, poor memory storage capacity, computation overhead, and a limited battery life—remain unresolved[14] .

Localization Protocols

Data collection and forwarding to a destination is a critical function of a sensor network. It is critical to understand where the data that has been acquired is kept. In WSNs, this kind of data can be collected through the use of localization techniques. One method of locating sensor nodes is localization. There has been a lot of work done in the intriguing field of sensor node localization research. Designing affordable, scalable, and effective localization methods for WSNs is very desirable. In this study, we address several localization approaches, sensor node design and its applications, and some potential avenues for future research. The process of estimating localization involves communicating the geometrical positioning or position of the localized and unlocalized nodes. The angle and separation between nodes are used to identify location.

- **DV-Hop (Distance Vector Hop Localization)**: A hop-based localization algorithm where nodes estimate their positions based on hop distances and anchor node positions. DV hop uses hop count to measure the distance between nodes. Throughout the network, at least three anchor nodes broadcast coordinates together with the number of hops. From neighbor to neighbor node throughout the network, the information spreads. Such information is received by adjacent node, which increases hop count by one. Unlocalized nodes can determine how many hops separate them from anchor nodes in this manner. The shortest path from one anchor node to another is determined by all anchor nodes, and unlocalized nodes do the same. The formula to compute average hop distance is as follows: hop count divided by the distance between two nodes.

  Unidentified nodes employ the hop count approach to determine the shortest distance between them and three or more anchor nodes in order to estimate their placements [15].
- **MDS-MAP (Multidimensional Scaling based MAP)**: Utilizes multidimensional scaling techniques to estimate node positions based on pairwise distance measurements. For localization in two-dimensional networks, MDS-MAP is one of the most effective methods and is often used as a reference by researchers. A group of methods called multidimensional scaling (MDS) are employed to lower the dimensionality of the data. MDS uses results visualization to highlight data's hidden structures [17]. The MDS algorithm produces 2D or 3D points as an output by using the distances between each pair of objects as an input[16]

CONCLUSION

The production of interruption-free and effective communication between source and destination nodes is greatly aided by routing protocols. The choice of an effective routing protocol has a major impact on a network's performance, service, and dependability. Ad hoc networks and wireless sensor networks require round-free protocols. There are numerous classifications for the routing protocols used in WSN. Multiple applications, varying reliability, packet-loss recovery, and congestion control should all be supported via transport layer protocols in WSNs. A generic transport layer protocol should be unaffected by the application. There are a lot of transport protocols, and each one is designed with a different purpose in mind. The amount of packet loss that WSN applications can withstand varies depending on their functions. Poor radio connectivity, traffic, packet collisions, running out of memory, and node failures can all cause packet loss. In data delivery, packet loss can lead to energy waste and a reduction in the quality of service (QoS). Throughput and energy consumption can be increased by identifying packet loss and appropriately recovering lost packets. Sensor nodes gather data from specific locations and process it in a variety of applications that use WSNs. Knowing the location of the data collection sites, however, is a crucial task. One method of locating nodes is called localization. While there are numerous ways for localization, it is preferable to use those that can manage the limited resources of sensor nodes. In this work, we have reviewed several protocols needed for functioning of WSN.

REFERENCES :

[1] R. Sharma and D. K. Lobiyal, “Intelligent water drop based coverage-connectivity and lifespan maximization protocol for wireless sensor networks,” *Recent Patents Eng.*, vol. 13, no. 3, 2019, doi: 10.2174/1872212112666180521082955.

[2] R. Sharma, “Impact of energy holes problem on ad-hoc routing protocols,” *World Rev. Entrep. Manag. Sustain. Dev.*, vol. 16, no. 1, pp. 63–75, 2020.

[3] P. Park, C. Fischione, and K. H. Johansson, “Adaptive IEEE 802.15. 4 medium access control protocol for control and monitoring applications,” *Wirel. Netw. Based Control*, pp. 271–300, 2011.

[4] A. S. Budi, E. Setiawan, and H. Fitriyah, “Implementation of CSMA/CA and Simple Routing Protocol on Arduino and nRF24L01 as a Solution for Affordable Wireless Sensor Node,” in *2019 International Conference on Sustainable Information Engineering and Technology (SIET)*, 2019, pp. 159–163.

[5] A. Achroufene, M. Chelik, and N. Bouadem, “Modified CSMA/CA protocol for real-time data fusion applications based on clustered WSN,” *Comput. Networks*, vol. 196, p. 108243, 2021.

[6] R. Sharma and D. K. Lobiyal, “Energy based proficiency analysis of ad-hoc routing protocols in wireless sensor networks,” in *Conference Proceeding - 2015 International Conference on Advances in Computer Engineering and Applications, ICACEA 2015*, 2015. doi: 10.1109/ICACEA.2015.7164829.

[7] A. Sharma, K. Bhatia, and R. Sharma, “A Detailed Overview of Life Cycle Enhancing Approaches for WSN,” 2023.

[8] K. Rani, K. Bhatia, S. Bhadola, and R. Sharma, “A THOROUGH REVIEW OF WSN ROUTING PROTOCOLS,” *Cent. ASIAN J. Math. THEORY Comput. Sci.*, vol. 3, no. 7, pp. 22–24, 2022.

[9] N. S. Samaras and F. S. Triantari, “On direct diffusion routing for wireless sensor networks,” in *2016 Advances in Wireless and Optical Communications (RTUWO)*, 2016, pp. 89–94.

[10] J. Jones and M. Atiquzzaman, “Transport protocols for wireless sensor networks: State-of-the-art and future directions,” *Int. J. Distrib. Sens. Networks*, vol. 3, no. 1, pp. 119–133, 2007.

[11] R. Fisher and G. Hancke, “DTLS for lightweight secure data streaming in the internet of things,” in *2014 Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*, 2014, pp. 585–590.

[12] P. A. C. S. Neves and J. J. P. C. Rodrigues, “Internet protocol over wireless sensor networks, from myth to reality,” *J. Commun.*, pp. 189–196, 2010.

[13] J. Kim, H. Jeon, and J. Lee, “Network management framework for wireless sensor networks,” in *Communication and Networking: International Conference, FGCN 2010, Held as Part of the Future Generation Information Technology Conference, FGIT 2010, Jeju Island, Korea, December 13-15, 2010. Proceedings, Part I*, 2010, pp. 76–84.

[14] F. Ullah, T. Mehmood, M. Habib, M. Ibrahim, and S. Zulfikar, “SPINS: security protocols for sensor networks,” in *Proceedings of the International Conference on Communication Engineering and Networks (IPCSIT’11)*, 2011.

[15] Q. Huang and S. Selvakennedy, “A range-free localization algorithm for wireless sensor networks,” in *2006 IEEE 63rd Vehicular Technology Conference*, 2006, vol. 1, pp. 349–353.

[16] B. Risteska Stojkoska, “Nodes localization in 3D wireless sensor networks based on multidimensional scaling algorithm,” *Int. Sch. Res. Not.*, vol. 2014, 2014.