IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, March 2023
Impact Factor: 7.301

A Review on Communication Protocols of Wireless Sensor Networks

Vismaya P N[1] and Dr. Binu G. S[2]
P.G Scholar, Department of ECE, NSS College of Engineering, Palakkad, Kerala, India[1]
Professor, Department of ECE, NSS College of Engineering, Palakkad, Kerala, India[2]

Abstract: *Wireless Sensor Networks (WSNs) are networks of small, low-cost, low-power, and wirelessly connected sensor nodes. These sensor nodes can be distributed over a large area and can collect data about the environment, such as temperature, humidity, light, sound, vibration, and motion. WSNs are useful in a variety of applications, including environmental monitoring, smart agriculture, healthcare, industrial automation, and security. They can be used to gather data in remote or hard-to-reach locations, and they can also be used to monitor large areas continuously and in real-time. The nodes in a WSN are typically battery-powered and have limited processing and communication capabilities. Therefore, energy efficiency is a critical concern in WSNs, and the nodes are designed to conserve energy wherever possible. Proper choice of Communication protocols are essential for energy conservation in Wireless Sensor Networks (WSNs).This paper discuss about various communication protocols and its types. They help to reduce idle listening time, minimize data transmission, optimize routing, and control transmission power. By using energy-efficient communication protocols, WSNs can achieve longer network lifetime, better data accuracy, and improved network performance.*

Keywords: Wireless sensor Networks(WSNs), Communication protocols, Energy conservation.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are a type of distributed network that consists of a large number of small, low-power, and inexpensive wireless sensor nodes. Each sensor node is equipped with sensing, processing, and communication capabilities and can be deployed in various environments, such as homes, buildings, industrial sites, and natural ecosystems. The nodes communicate wirelessly with each other to form a self-organizing and self-configuring network that can perform a variety of tasks, such as environmental monitoring, surveillance, and automation WSNs typically operate in an unattended and autonomous mode, where they collect data from their surroundings, process it, and transmit it to a base station or a sink node for further analysis and decision-making. The communication among the nodes is typically achieved through wireless links, such as radio frequency (RF) or infrared (IR) communication, using various network topologies, such as star, mesh, or tree. WSNs pose several unique challenges due to their constrained resources, such as limited processing power, memory, and battery life. Therefore, designing and deploying WSNs require careful consideration of various factors, such as power management, routing, data aggregation, and security. WSNs have a wide range of applications, including environmental monitoring, health monitoring, precision agriculture, smart homes and buildings, and industrial automation. They offer numerous benefits, such as cost-effectiveness, scalability, flexibility, and noninvasiveness. Therefore, WSNs are becoming increasingly popular and are expected to play a significant role in various domains, such as the Internet of Things (IoT), smart cities, and Industry 4.0.

The working of WSNs can be broadly divided into four stages:

1. **Sensing:** The sensing stage involves the acquisition of data by the sensor nodes. The sensor nodes use various sensors to measure the physical phenomena and convert them into electrical signals. The data collected by the sensors can be processed, aggregated, and compressed to reduce the amount of data transmitted over the network.
2. **Processing**: The processing stage involves the aggregation, fusion, and analysis of data by the sensor nodes. The sensor nodes can use simple algorithms to process the data locally and reduce the amount of data transmitted over the network. The sensor nodes can also perform complex computations such as signal

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, March 2023
Impact Factor: 7.301

processing and pattern recognition to extract meaningful information from the data.

3. **Communication**: The communication stage involves the transmission of data between the sensor nodes and the base station. The sensor nodes can use wireless communication protocols such as ZigBee, Bluetooth, and Wi-Fi to transmit the data. The communication protocols used in WSNs are designed to conserve energy, increase network lifetime, and reduce data loss due to interference and node failure.
4. **Data Storage**: The data storage stage involves the storage of data by the base station or the sensor nodes. The data can be stored in a central repository for further analysis or used in real-time applications such as environmental monitoring and surveillance

II. IMPORTANCE OF ENERGY CONSERVATION IN WSN

Energy conservation is of utmost importance in Wireless Sensor Networks (WSNs) due to the following reasons:

1. **Limited power supply**: Sensor nodes in WSNs are usually powered by batteries or energy-harvesting mechanisms. These power sources have limited capacity and cannot be easily recharged or replaced. Therefore, it is crucial to optimize the energy consumption of sensor nodes to extend the network's lifetime.
2. **Energy consumption**: Sensor nodes in WSNs consume energy in various operations such as sensing, processing, and communication. Among these, communication is the most energy-consuming operation. Therefore, energy-efficient communication protocols and algorithms are necessary to reduce the energy consumption of WSNs.
3. **Network coverage**: WSNs are often deployed in remote or inaccessible areas, where it is difficult or impossible to replace or recharge the batteries of sensor nodes. Therefore, energy conservation is crucial to ensure that the network provides reliable coverage and operation over an extended period.
4. **Cost**: Replacing or recharging the batteries of sensor nodes can be expensive and timeconsuming, especially in large-scale networks. Therefore, energy conservation can reduce the operational costs of WSNs.
5. **Environmental impact**: Battery disposal and replacement can have a significant environmental impact. Therefore, energy conservation can reduce the environmental footprint of WSNs

By optimizing energy consumption, WSNs can achieve longer lifetimes, broader coverage, and lower operational costs while minimizing their environmental impact.

III. COMMUNICATION PROTOCOLS

Communication protocols play a crucial role in the performance and reliability of Wireless Sensor Networks (WSNs). Here are some of the reasons why communication protocols are important in WSNs:

1. **Energy efficiency**: Communication is one of the most energy-consuming operations in WSNs. Therefore, energy-efficient communication protocols can significantly improve the network's lifetime and reduce the operational costs of WSNs.
2. **Data reliability**: WSNs often operate in harsh and unpredictable environments, where sensor nodes can fail or lose connectivity. Communication protocols that can ensure reliable and error-free data transmission are essential to maintain the data quality and accuracy of WSNs.
3. **Scalability**: WSNs can consist of hundreds or even thousands of sensor nodes. Communication protocols that can support efficient and scalable communication among the nodes are necessary to ensure the network's proper operation.
4. **Security**: WSNs can be vulnerable to various security threats, such as eavesdropping, message tampering, and denial-of-service attacks. Communication protocols that can provide secure and authenticated communication among the nodes can enhance the network's security and protect against such threats.
5. **Interoperability**: WSNs can use different communication technologies and protocols, depending on the application requirements and constraints. Communication protocols that can support interoperability among the nodes and integrate with other communication systems are necessary to ensure the seamless operation of WSNs communication protocols are critical components of WSNs that can significantly impact their performance, reliability, and security. Therefore, designing and selecting appropriate communication protocols are essential for the successful deployment and operation of WSNs.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, March 2023
Impact Factor: 7.301

There are several types of communication protocols that are commonly used in Wireless Sensor Networks (WSNs). Here are some of the most widely used types:

1. **MAC Protocols**: MAC (Media Access Control) protocols define the rules for accessing the communication channel among the sensor nodes. They are responsible for managing the channel access and minimizing collisions and interference among the nodes. Examples of MAC protocols used in WSNs include S-MAC, T-MAC, and B-MAC.
2. **Network layer/Routing Protocols**: Network layer protocols define the rules for routing data packets among the sensor nodes in the network. They determine the optimal path for packet transmission based on various metrics, such as hop count, energy consumption, and reliability. Examples of network layer protocols used in WSNs include LEACH, HEED, and PEGASIS.
3. **Transport Layer Protocols**: Transport layer protocols provide end-to-end communication between the application layer and the network layer. They ensure reliable and efficient data transmission by implementing congestion control, flow control, and error recovery mechanisms. Examples of transport layer protocols used in WSNs include RAP and SCP.
4. **Security Protocols**: Security protocols provide mechanisms for protecting the communication among the sensor nodes from various security threats, such as eavesdropping, message tampering, and denial-of-service attacks. They provide authentication, encryption, and key management mechanisms to ensure secure communication. Examples of security protocols used in WSNs include TinySec, LEAP, and SPINS.
5. **Application Layer Protocols**: Application layer protocols define the rules for data exchange and interaction among the sensor nodes and the external applications or services. They specify the data formats, protocols, and interfaces for data collection, processing, and dissemination. Examples of application layer protocols used in WSNs include CoAP, MQTT, and AMQP

IV. MAC PROTOCOLS

The Medium Access Control (MAC) protocol is a communication protocol used in Wireless Sensor Networks (WSN) to enable communication between sensor nodes. he MAC protocol is responsible for managing the access of each sensor node to the wireless communication channel to ensure reliable and efficient data transmission.The MAC protocol in WSNs should address some unique challenges, such as energy efficiency, scalability, and low latency. Therefore, several MAC protocols have been developed to address these challenges and to provide the best performance according to the application requirements.

The Medium Access Control (MAC) protocol is of utmost importance in Wireless Sensor Networks (WSN) as it plays a critical role in managing the access to the wireless communication channel. Here are some of the key reasons why MAC protocols are important in WSN:

1. **Efficient use of limited resources:** In WSN, the resources such as energy, bandwidth, and computational power are limited. The MAC protocol helps to manage these resources efficiently by controlling the access of nodes to the wireless communication channel. By preventing collisions and minimizing idle listening, the MAC protocol ensures that the energy is used optimally, thus prolonging the lifetime of the network.
2. **Improved reliability:** In WSN, the transmission of data packets is often affected by interference, noise, and other external factors. The MAC protocol helps to improve the reliability of data transmission by regulating the access of nodes to the communication channel, minimizing collisions, and avoiding congestion.
3. **Scalability:** The MAC protocol plays a crucial role in maintaining scalability in WSN. With the increasing number of nodes in the network, the MAC protocol ensures that each node has a fair share of the communication channel without causing congestion.
4. **Low latency:** In some WSN applications, low latency is critical for real-time data transmission. The MAC protocol helps to reduce the latency by controlling the access of nodes to the communication channel and minimizing the waiting time for data transmission. It is critical to choose an appropriate MAC protocol that meets the specific requirements of the WSN application to ensure optimal performance.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, March 2023
Impact Factor: 7.301

4.1 MAC Protocols Types

A. SMAC

SMAC (Sensor Medium Access Control) is a power-efficient MAC protocol for wireless sensor networks (WSNs) that aims to reduce energy consumption and increase the network lifetime. SMAC is a contention-based protocol that uses a random back off algorithm to avoid collisions among nodes that are competing for the channel. SMAC divides time into fixed-size time slots, and each node is assigned a timeslot based on its unique identifier. During its assigned timeslot, a node can transmit data or receive data from other nodes. After the timeslot is over, the node enters a sleep mode to conserve energy until its next timeslot. To further reduce energy consumption, SMAC uses a duty cycling mechanism where nodes periodically wake up to check for any pending data transmissions or receptions. If there is no data to send or receive, the node goes back to sleep mode, thus conserving energy. SMAC also includes a neighbor discovery mechanism where nodes periodically broadcast hello messages to discover neighboring nodes and establish communication links with them. By using this mechanism, SMAC reduces the overhead of maintaining the routing tables, and it allows for efficient communication among nodes.

B. BMAC

BMAC (Berkeley Media Access Control) is a low-power, low-latency, and low-overhead MAC (Media Access Control) protocol designed specifically for Wireless Sensor Networks (WSNs). In a WSN, nodes are usually battery-powered and operate in a distributed manner, which means they have limited computational resources, memory, and battery power. As a result, designing a MAC protocol for WSNs requires addressing the challenges of energy efficiency, reliability, and low-latency communication. BMAC addresses these challenges by using a duty-cycle approach, where nodes alternate between sleep and active modes. In the active mode, a node listens to the channel for a short period of time to check for incoming packets. If a packet is detected, the node stays awake to receive the entire packet. If no packet is detected, the node goes back to sleep until the next active period. BMAC also uses a randomized back off scheme to avoid collisions and improve channel utilization. When a node wants to transmit a packet, it selects a random back off time before attempting to transmit. This reduces the probability of multiple nodes attempting to transmit at the same time, which could result in a collision and energy waste. Overall, BMAC is a lightweight, energy-efficient MAC protocol that is well-suited for WSNs. Its duty-cycle approach and randomized back off scheme help reduce energy consumption and improve reliability, while maintaining low-latency communication.

C. TMAC

TMAC (Timing MAC) is another MAC protocol designed for Wireless Sensor Networks (WSNs) that addresses some of the limitations of traditional duty-cycle MAC protocols like BMAC. Like BMAC, TMAC is a low-power MAC protocol that uses duty cycling to save energy. However, TMAC differs from BMAC in how it schedules the active and sleep periods of the nodes. Instead of using a fixed duty cycle, TMAC schedules the active periods based on a global time slotting scheme. In TMAC, a coordinator node broadcasts the schedule for the active periods to all the nodes in the network. The schedule includes the start and end times for each active period, as well as the time slot duration. Each node in the network follows this schedule to determine when to turn on its radio to transmit or receive data. By using a global time slotting scheme, TMAC reduces the contention for the channel, which leads to better energy efficiency and reduced latency. TMAC also includes a mechanism for detecting collisions and handling them in a way that reduces energy consumption. Overall, TMAC is a more sophisticated MAC protocol than BMAC, with better energy efficiency and latency characteristics. However, it requires more coordination and management than BMAC, which may be a disadvantage in certain WSN scenarios.

V. ROUTING PROTOCOLS

Routing is a critical aspect of Wireless Sensor Networks (WSNs) as it enables sensor nodes to communicate with each other and with the base station or sink node. In WSNs, the sensor nodes are typically densely deployed in a large area to monitor physical phenomena or collect data. The nodes are typically energy-constrained, have limited computational resources, and have a low transmission range. Routing in WSNs involves the selection of an optimal path for data transmission between the source and destination nodes while optimizing different performance metrics such as energy efficiency, delay, reliability, and network lifetime. The importance of routing in WSNs can be highlighted as follows:

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, March 2023
Impact Factor: 7.301

1. **Energy efficiency:** Routing in WSNs can significantly impact the energy consumption of sensor nodes. The selection of an optimal path for data transmission can minimize the energy consumption of nodes by reducing the number of hops or by balancing the energy consumption among nodes. Energy-efficient routing can prolong the network lifetime and reduce the need for frequent battery replacement or recharging.
2. **Scalability:** WSNs can consist of a large number of sensor nodes, and routing algorithms should be scalable to support efficient data transmission in large-scale networks. Efficient routing algorithms can reduce the overhead of network control messages and enhance the scalability of WSNs.
3. **Data reliability:** Reliable data delivery is critical in many WSN applications, especially in mission-critical applications such as disaster management, military, and healthcare. Routing protocols that can ensure reliable data delivery by mitigating packet loss, error, or duplication can improve the data quality and increase the effectiveness of WSNs.
4. **Delay:** Some WSN applications require real-time data transmission, and routing algorithms can affect the delay in data delivery. The selection of optimal paths with minimal delay can enhance the responsiveness of WSNs.
5. **Fault-tolerance:** Sensor nodes can fail due to energy depletion, environmental factors, or hardware failure. Routing protocols that can handle node failures and reroute data to the destination can improve the fault-tolerance and reliability of WSNs.

There are several types of routing algorithms used in Wireless Sensor Networks (WSNs) depending on the network topology, application requirements, and performance metrics. Some common types of routing algorithms used in WSNs are:

1. **Flat routing**: In flat routing, all sensor nodes are considered equal, and the data is transmitted from the source node to the sink node through multiple hops. Flat routing algorithms are simple and require low computational resources, but they may not be suitable for large-scale WSNs due to scalability and energy efficiency issues. Eg; Direct Diffusion (DD) , Rumor Routing , Gossiping
2. **Hierarchical routing**: In hierarchical routing, the sensor nodes are organized into clusters or groups, and a cluster head is responsible for aggregating and forwarding the data to the sink node. Hierarchical routing algorithms can reduce the energy consumption and enhance the scalability of WSNs by reducing the overhead of network control messages. Eg; Low energy adaptive clustering hierarchy (LEACH) ,Threshold sensitive energy efficient sensor network (TEEN) ,Stable election protocol (SEP) d. Distributed energy-efficient clustering (DEEC)
3. **Geographic routing:** In geographic routing, the data is forwarded to the next-hop node based on its geographic location. Geographic routing algorithms can minimize the energy consumption by reducing the number of hops and can handle node mobility efficiently. Eg; Greedy Perimeter Stateless Routing (GPSR), Geographic Distance Routing (GEDIR),Location-Aided Routing (LAR)
4. **Multipath routing**: In multipath routing, multiple paths are established between the source and destination nodes to enhance the reliability, fault-tolerance, and load balancing of WSNs. Multipath routing algorithms can improve the data delivery ratio and prolong the network lifetime by distributing the data traffic among multiple paths. Eg; Ad Hoc On-Demand Multipath Distance Vector(AOMDV), Multipath Forwarding Scheme for Unidirectional Link Networks (MFU),Energy-Aware Multipath Routing (EAMR)
5. **QoS-based routing**: In QoS-based routing, the data is transmitted based on Quality of Service (QoS) parameters such as delay, reliability, and energy consumption. QoS-based routing algorithms can meet the application-specific QoS requirements and enhance the network performance. Eg; QoS-Aware Routing Protocol (QARP),Quality-of-Service-Based Routing (QSR),Priority-Based Routing Protocol (PBRP)
6. **Energy-aware routing**: In energy-aware routing, the energy consumption of sensor nodes is considered while selecting the routing paths. Energy-aware routing algorithms can prolong the network lifetime by balancing the energy consumption among nodes and reducing the energy waste. Eg; Energy-Efficient Routing Protocol (EERP),Battery-Aware Routing Protocol (BARP),Stable Election Protocol (SEP).

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, March 2023
Impact Factor: 7.301

VI. TRANSPORT LAYER PROTOCOLS

Transport layer protocols in Wireless Sensor Networks (WSNs) are responsible for providing reliable and efficient end-to-end communication between the sensor nodes and the base station or other nodes in the network. They implement various mechanisms to ensure data integrity, flow control, congestion control, and error recovery. Here are some commonly used transport layer protocols in WSNs:

1. **Reliable Transport Protocol (RTP)**: RTP is a transport layer protocol that provides reliable data transmission between the sensor nodes and the base station. It uses sequence numbers, acknowledgments, and retransmissions to ensure data integrity and reliability. RTP can also support congestion control and flow control mechanisms to optimize the network performance.
2. **Sensor Protocol for Information via Negotiation (SPIN)**: SPIN is a transport layer protocol that uses a negotiation process to establish the communication between the sensor nodes and the base station. It provides reliable data transfer and efficient use of network resources by avoiding unnecessary retransmissions and reducing the overhead of acknowledgments.
3. **Sensor Control and Protocol (SCP):** SCP is a transport layer protocol that provides reliable data transfer and congestion control mechanisms for WSNs. It uses a feedback mechanism to adjust the data transmission rate based on the network congestion level and optimize the network throughput.
4. **Data Aggregation Transport Protocol (DATP)**: DATP is a transport layer protocol that provides efficient data aggregation and transmission in WSNs. It uses a hierarchical data aggregation mechanism to reduce the amount of data transmitted and conserve the network resources.
5. **Application Transport Protocol (ATP):** ATP is a transport layer protocol that provides efficient communication between the sensor nodes and the external applications or services. It supports different data formats and protocols to enable seamless integration with other communication systems and applications.

Transport layer protocols in WSNs provide reliable and efficient end-to-end communication and play a critical role in the network performance and reliability. The selection of the appropriate transport layer protocol depends on the application requirements, network topology, and resource constraints of the WSNs

VII. SECURITY PROTOCOLS

Wireless Sensor Networks (WSNs) are vulnerable to various security threats due to the nature of their deployment in open and hostile environments. Therefore, security protocols are essential to ensure the confidentiality, integrity, and availability of the data transmitted over WSNs.

Here are some reasons why security is essential in WSNs:

1. **Confidentiality:** WSNs are often used for collecting and transmitting sensitive information, such as environmental data, personal health data, and military intelligence. Security mechanisms such as encryption and authentication ensure that only authorized nodes can access and read this information, preventing unauthorized access and data theft.
2. **Integrity:** In WSNs, data integrity is crucial because any tampering or modification of data could lead to incorrect conclusions or actions. Security mechanisms such as digital signatures and message authentication codes help to verify the integrity of data, ensuring that the data is not altered during transmission.
3. **Availability:** Availability is critical in WSNs because the nodes rely on each other to function correctly. Security threats such as denial-of-service attacks can disrupt the network, making it unavailable for legitimate users. Security mechanisms such as intrusion detection systems and firewalls help to prevent such attacks, ensuring the availability of the network.
4. **Privacy:** WSNs are often used to collect personal information, and privacy is a critical concern in such scenarios. Security mechanisms such as anonymous routing and privacy-preserving data aggregation ensure that the personal information of users is protected, preventing unauthorized access and disclosure of information.
5. **Trust:** Trust is essential in WSNs because the nodes must be able to trust each other for accurate data transmission and routing. Security mechanisms such as secure key distribution and secure routing protocols help to establish trust between nodes, ensuring reliable and secure communication.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, March 2023
Impact Factor: 7.301

Some common security issues in WSNs:

1. **Denial-of-service (DoS) attacks:** DoS attacks aim to disrupt the normal operation of the network by flooding it with a large number of requests or messages, causing network congestion and making the network unavailable to legitimate users.
2. **Node compromise:** Sensor nodes can be compromised by attackers who gain unauthorized access to the node's resources and data, allowing them to control or manipulate the node and its data.
3. **Eavesdropping:** Eavesdropping attacks involve an attacker intercepting and monitoring the wireless communication between nodes to extract sensitive information such as passwords, personal information, or confidential data.
4. **Spoofing:** Spoofing attacks involve an attacker pretending to be a legitimate node in the network by forging its identity, allowing the attacker to gain unauthorized access to the network and its resources.
5. **Tampering:** Tampering attacks aim to modify the data being transmitted between nodes, leading to incorrect conclusions or actions. For example, an attacker could tamper with environmental data readings to cause a false alarm or damage.
6. **Routing attacks:** Routing attacks aim to disrupt the routing of data between nodes, leading to delays, data loss, or incorrect routing decisions.
7. **Physical attacks:** Physical attacks involve an attacker physically accessing the network or its components, leading to theft, damage, or destruction of the network.
8. **Insider attacks:** Insider attacks involve an authorized user within the network intentionally or unintentionally compromising the security of the network, leading to data theft or disruption of service.

Mitigating these threats requires the deployment of appropriate security mechanisms such as authentication, encryption, intrusion detection, and secure routing protocols, among others. It is essential to consider these security issues and deploy appropriate security measures when designing and deploying WSNs to ensure their reliable and secure operation
Some of the security protocols used in WSNs include:

1. **Encryption**: Encryption mechanisms can be deployed to protect the confidentiality of data transmitted between nodes. Symmetric and asymmetric encryption algorithms can be used to encrypt data and prevent eavesdropping attacks..
2. **Authentication**: Authentication mechanisms can be deployed to ensure that only authorized nodes can access the network and its resources. For example, digital certificates, passwords, and biometric authentication can be used to authenticate nodes..
3. **Access control**: Access control is used to restrict unauthorized access to the network. It can be achieved using various access control mechanisms such as MAC address filtering, firewalls, and intrusion detection systems.
4. **Key management**: Key management is used to generate, distribute, and store keys securely. It is an essential component of WSN security protocols.
5. **Secure routing protocols**: Secure routing protocols can be deployed to prevent routing attacks, such as selective forwarding, sinkhole, or Sybil attacks. Secure routing protocols use mechanisms such as node authentication, route authentication, and hop-by-hop encryption to prevent attacks.
6. **Intrusion detection**: Intrusion detection is used to detect and prevent any unauthorized access to the network. It can be achieved using various techniques such as anomaly detection, signature-based detection, and stateful protocol analysis.
7. **Physical security**: Physical security measures such as tamper-proof packaging, secure storage, and secure location of the nodes can also be used to enhance the security of WSNs.

VIII. APPLICATION LAYER PROTOCOL

In WSNs, the Application Layer Protocol is responsible for providing the interface between the sensor nodes and the end-users or applications. The main goal of the Application Layer Protocol is to ensure that the data collected by the sensor nodes can be used effectively by the end-user applications. The protocol defines the way in which the sensor nodes interact with the application layer and how the data collected by the sensor nodes is processed and transmitted to the end-users.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, March 2023
Impact Factor: 7.301

The Application Layer Protocol in WSNs is responsible for performing several key functions such as data aggregation, compression, filtering, encryption, and authentication. These functions are essential to ensure that the data collected by the sensor nodes is processed and transmitted efficiently and securely to the end-users.

There are several Application Layer Protocols used in WSNs, each designed for specific applications. Some of the commonly used Application Layer Protocols in WSNs include:

1. **Sensor Application Interface Protocol (SAIP)**: SAIP provides a standardized interface between the sensor nodes and the end-user applications.
2. **Sensor Query and Data Dissemination Protocol (SQDDP)**: SQDDP is used for querying and retrieving data from the sensor nodes.
3. **Sensor Network Management Protocol (SNMP):** SNMP is used for managing and monitoring the WSNs.
4. **Event Notification Protocol (ENP):** ENP is used for notifying the end-users of specific events that occur in the WSN.

The choice of Application Layer Protocol depends on the specific requirements of the application and the WSN. The Application Layer Protocol must be designed to ensure that the data collected by the sensor nodes is processed and transmitted efficiently and securely to the end-users.

IX. CONCLUSION

Wireless Sensor Networks (WSN) rely on communication protocols to transmit data between sensor nodes and the base station in an effective and reliable manner. There are several communication protocols for WSN, each with their own benefits and limitations. When choosing a communication protocol for a WSN, it is critical to take into account parameters like power consumption, data rate, range, security, and scalability. A robust and effective protocol can offer a solution for WSN applications by successfully balancing these variables. Based on the application's specific requirements, the communication protocol for WSN should be chosen, and the various aspects that influence the protocol's performance should be carefully considered.

REFERENCES

[1]. K. Sangeetha, J. Shanthini and S. Karthik, ”A Review on Energy Conservation Techniques in Wireless Sensor Networks,” 2018 International Conference on Soft-computing and Network Security (ICSNS), Coimbatore, India, 2018, pp. 1-5, doi: 10.1109/ICSNS.2018.8573621.

[2]. Giuseppe Anastasi, Marco Conti, Mario Di Francesco, Andrea Passarella, Energy conservation in wireless sensor networks: A survey, Ad Hoc Networks, Volume 7, Issue 3, 2009, Pages 537-568, ISSN 1570- 8705, https://doi.org/10.1016/j.adhoc.2008.06.003..

[3]. Kochhar, Aarti Kaur, Pardeep Singh, Preeti Sharma, Sukesha. (2018). Protocols for Wireless Sensor Networks: A Survey. Journal of Telecommunications and Information Technology. 1. 77-87. 10.26636/jtit.2018.117417.

[4]. Joseph Polastre, Jason Hill, and David Culler. 2004. Versatile low power media access for wireless sensor networks. In Proceedings of the 2nd international conference on Embedded networked sensor systems (SenSys ’04). Association for Computing Machinery, New York, NY, USA, 95–107. https://doi.org/10.1145/1031495.1031508

[5]. Ye, Wei Heidemann, John Estrin, Deborah. (2002). An energyefficient MAC protocol for wireless sensor networks. Proceedings - IEEE INFOCOM. 3. 1567-1576 vol.3. 10.1109/INFCOM.2002.1019408. .

[6]. Mehran Abolhasan, Tadeusz Wysocki, ErykDutkiewicz, A review of routing protocols for mobile ad hoc networks, Ad Hoc Networks, Volume 2, Issue 1, 2004, Pages 1-22, ISSN 1570-8705,

[7]. Khatarkar, Sarika Kamble, Rachana. (2013). Wireless sensor network mac protocol Smac and tmac. Ind. J. Comput. Sci. Eng.. 4. 304-310.

[8]. Gupta, Anuj Sadawarti, Harsh Verma, Anil. (2011). Review of Various Routing Protocols for MANETs. International Journal of Information and Electronics Engineering. 1. 251-259. 10.7763/IJIEE.2011.V1.40.

[9]. Ndia, John. (2018). A Survey of WSN Security protocols. International Journal of Applied computer Science (IJACS). I. 1-11.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, March 2023
Impact Factor: 7.301

[10]. Stangaciu, Valentin Stanciu, Madalina Lupu, Loredana Micea, Mihai Cretu, Vladimir. (2017). Application layer protocol for IoT using wireless sensor networks communication protocols. 430-435. 10.1109/ICUMT.2017.8255160. .

[11]. Jones, Justin Atiquzzaman, Mohammed. (2007). Transport Protocols for Wireless Sensor Networks: State-of-the-Art and Future Directions. Int J Distrib Sens Netw. 3. 10.1080/15501320601069861.

[12]. J. Grover and S. Sharma, "Security issues in Wireless Sensor Network — A review," 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 2016, pp. 397-404, doi: 10.1109/ICRITO.2016.7784988.

[13]. Musthafa, Sameena G.S, Dr. (2021). Mobility Characteristics and Routing Protocols For Wireless Sensor Network With Mobile Sink - Energy Perspective.

[14]. Khriji, Sabrine El Houssaini, DhouhaKammoun, Ines Kanoun, Olfa. (2018). Energy-efficient techniques in wireless sensor networks: Technology, Components and System Design. 10.1515/9783110445053- 017.

[15]. Parvathy S and Dr. BinuGS,Energy Efficient Management Approach For Wireless Sensor Network,s International Journal of Advanced Research in Science, Communication and Technology (IJARSC),Volume 2, Issue 7, May 2022

[16]. Jamal N Al-Karaki and Ahmed E Kamal. Routing techniquesin wireless sensor networks: a survey. IEEE wireless communications, 11(6):6–28, 2004.

[17]. Manap, Z., Ali, B.M., Ng, C.K. et al. A Review on Hierarchical Routing Protocols for Wireless Sensor Networks. Wireless Pers Commun 72, 1077–1104 (2013). https://doi.org/10.1007/s11277-013-1056-5

[18]. A. Kanavalli, D. Sserubiri, P. D. Shenoy, K. R. Venugopal and L. M. Patnaik, "A flat routing protocol for sensor networks," 2009 Proceeding of International Conference on Methods and Models in Computer Science (ICM2CS), New Delhi, India, 2009, pp. 1-5, doi: 10.1109/ICM2CS.2009.5397948.

[19]. M. Bhalla, N. Pandey and B. Kumar, "Security protocols for wireless sensor networks," 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), Greater Noida, India, 2015, pp. 1005-1009, doi: 10.1109/ICGCIoT.2015.7380610.

[20]. Cedric Ramassamy, Hac ´ eneFouchal, Philippe Hunel. Impact of Ap- ` plication Layers over Wireless Sensor Networks. 12th international conference on innovative Internet community services (I2CS 2012), Jun 2012, Trondheim, Norway