# Comparative Analysis of LEACH and AODV Routing Protocols for IoT-Enabled Wireless Sensor Networks: Toward Software-Defined Networking Integration

Shikha Verma[1] , Sunil Kumar [2]
[1] Associate Professor, Department of Computer Applications,
ABES Engineering College, Ghaziabad, India
[1]LGPR Postdoctrol Candidate at LUC Malayasia
Shikhasaxena83@gmail.com
[2] Associate Professor,Auro University,Surat
Sunil.kumar@aurouniversity.edu.in

**ABSTRACT**: The Internet of Things (IoT) is essential for automating and managing operations, which speeds up communication and processing. WSNs (WSNs), which are required to the majority of Internet of Things devices, are at their centre. Every Internet of Things device has sensors built into it so it can analyse data, sense its surroundings, and interact with other devices. Thus, WSNs is essential to the proper operation of IoT infrastructures. The comparative study of routing protocols created especially for Internet of Things applications in WSN is explored in this paper.
Keywords: Leach, WSN, IoT, AODV, Energy efficiency, SDN

**Introduction**

The "Internet of Things" (IoT) is the process of linking objects to the internet so they may be remotely controlled and monitored. The use of wireless technologies is the most often used method for reaching this level of connectivity. [1]. It is widely known that WSNs are transforming the networking industry. [2]. Sensor nodes are battery-powered, reasonably priced devices that are placed around a region to collect data, which they subsequently wirelessly send to larger "sink" nodes. Each of these sensors has the ability to communicate with the sink or with each other. The limited energy resources of individual nodes are a major issue for WSNs. [3]. For data gathered by sensors or other devices to be sent to the right location for additional processing, routing protocols are essential. After processing, this data can be used in a variety of ways to improve people's lives. Wireless sensor units or devices that communicate their readings to a base station while operating in a controlled manner make up WSN. Every single unit has a battery, but its energy supply is constrained.[4]. These devices usually have insufficient sensing and transmission ranges as well as minimal processing power. Since a node is used for several tasks like computation, networking, and sensing, how long it lasts depends on how lively its battery is. The tiny batteries used in sensor nodes are often neither rechargeable or interchangeable.

Although there are numerous ways to generate energy, these methods do not totally eliminate the need for effective energy management. Managing the extremely low battery power by using energy-efficient h/w and s/w protocols for WSNs is therefore one of the major problems.[24] WSNs are extensively utilized in many different applications, including as industrial machine monitoring, agricultural crop monitoring, military surveillance, remote patient monitoring, and ambient temperature monitoring and industrial machine monitoring, among others.[5]. While designing the WSN many issues such how the energy conserve, scalable up to whatever length, localizing and make them secure and most essential support routing, much study has concentrated on developing clustering with energy efficiency and methods of routing to decrease energy usage. For example, one study assessed whether the energy and temperature of each node's centrality were greater in order to choose the best cluster head.[6] [7].IoT is mostly dependent on WSNs, where sensors visit the environment on a regular basis and notify the base station (BS) right away if any events are detected. is used to load the collected data into the IoT Cloud in an IoT-based WSN. In certain configurations, the gateway might be the base station itself. Users can access data saved in the IoT Cloud remotely at any time.The features and difficulties of routing protocols will be covered in a later chapter, followed by a comparison of the many kinds of routing protocols.

**Characteristics and Challenges of Routing Protocols in IoT-based WSN**

Designing routing protocols for WSNs is a challenging problem because of several characteristics that distinguish them from wireless networks without infrastructure. Numerous routing challenges arise in wireless sensing networks.[26]

Resource Constraints: Because sensor nodes occasionally have limited power, memory, and processing capability, energy efficiency is a major concern. Assigning a universal identity system to a large number of sensor nodes is nearly impossible. Therefore, wireless sensor motes are unable to use typical IP-based protocols.

Scalability: Protocols must be scalable without compromising functionality because networks may have thousands or even hundreds of nodes.

Dynamic Topology: Because nodes frequently move or join the network, protocols must adapt to changing network topologies.

Reliability: In the face of interference, node failures, and other challenges, it is essential to ensure correct data delivery. The generated data flow frequently contains significant duplication. because several sensor nodes can generate identical data during detection. Making the most of the available bandwidth and energy is therefore essential, as is utilizing the redundancy that the routeing protocols allow.

Heterogeneity: IoT-based WSNs often contain a variety of node types with a range of capabilities, necessitating adaptable routing solutions.

**Different Routing Protocols in IoT-based WSN and there comparative study**

Smart agriculture, air pollution, water pollution, and other issues are examples of IoT-based WSN applications.[11], air pollution monitoring, smart agriculture [11,13,14], health and environments [15,16], smart irrigation [17], smart cities and apartments, and smart wearables [18,19,20].For all implementations to function, multiple routing protocols are required.

**3.1** LEACH is a versatile, self-organizing clustering solution for WSNs (WSNs) that uses the cluster's head rotation mechanism to distribute energy burden evenly across the sensors. Sensor nodes in the target region aggregate together to form clusters, and the cluster head is selected based on these groupings. LEACH employs a random CH rotation mechanism to spread the load among multiple sensors rather than continuously depleting the power from a single sensor. A selected CH broadcasts an ad packet to inform neighboring non-Cluster Head nodes about its selection. The CH that received the strongest advertisement signal is informed to try to join by a non-Cluster Head node. Following the establishment of a cluster, the CH broadcasts a transmission schedule inside its cluster, allocating one data slot per cluster member every frame. A member of a cluster can only send during its designated slot. In the other spots, it turns off its radio. All of the cluster members' data is gathered by the CH, which then transmits an aggregate packet straight to the BS.This algorithm's primary feature is its cluster head selection on random basis , which rotates every round. or choosing the cluster head according to which sensor has the most energy Cluster. Data aggregation at the cluster head, which uses TDMA threshold values to connect with the sink or user directly.

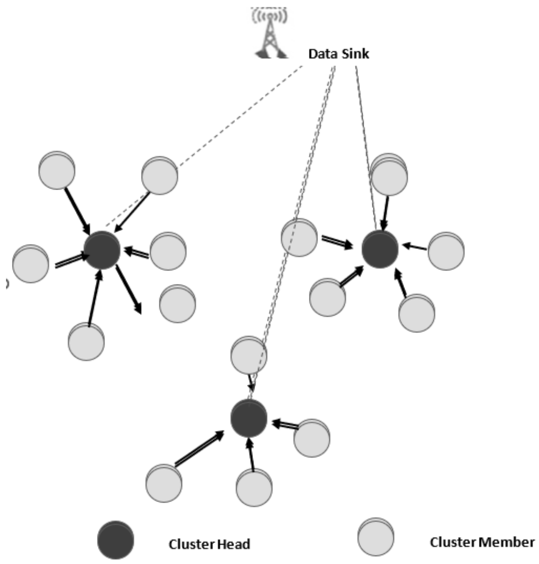


Fig. 1.  Network topology in WSN clusters.

LEACH offers some benefits, but it also has several disadvantages, such as the following:
Because LEACH cluster heads are selected at random, it is difficult to ensure that an appropriate counting and cluster head distribution would be employed.
Nodes with less energy will soon perish, and those with less energy strive to be the cluster's leader because they have more energy left.
This study provides a unique enhanced energy-efficient LEACH to address the problems with traditional approaches and achieve energy efficiency in the Cluster Head selection process [21][22].

**3.2 AODV (Ad hoc On-Demand Distance Vector):**

Ad-hoc on-demand distance vector is a popular classical routeing protocol that is frequently used with mobile ad hoc networks. AODV finds routes only when needed. When a node has information to send to a destination but does not have a valid routeing table entry, it broadcasts a Route Request (RREQ) packet to all of its neighbors [25].

After getting this RREQ, an intermediate node looks at a route to the designated destination as its local routeing table. If the search is successful, an RREP packet is generated and sent back to the start node via the reverse connection as a unicast message. The node establishes a reverse link to the node from whence the RREQ message was received and sent to all nodes RREQ packet if it cannot find a valid route to the destination. The destination node creates an RREP and sends it unicast return to the start node after receiving an RREQ packet. Each node that is in between adjusts its routeing database to set up a forward pointer upon receiving an RREP packet, then sends the RREP message to the next hop using the reverse pointer.

Until the start node receives the RREP, the procedure continues. When AODV was first released, it used recurrent HELLO messages to confirm that its neighbors' connections were legitimate. If a connection in an active route fails, a route error (RERR) message is sent. It is unicast return to the station that began the message and floods the associated routeing table entries for the all nodes in between. The stating node chooses the RREP packet with the fewest hops out of those it is expected to receive.[23]

**Features of AODV includes**

On-Demand Route Discovery: This strategy minimises extraneous control message overhead by only discovering routes when they are required.

Loop-Free Routeing: AODV uses sequence numbers to ensure that routes are not repeated and that the most recent route is always taken.
Route Maintenance: A route will be maintained as long as it is necessary. When a link fails, the protocol can quickly identify an alternate path or get in touch with the source.
Scalability: Because AODV scales well in networks with a large number of nodes, it is suitable for large IoT networks.
The route discovery process, which begins with a node and ends with another node, is based on the query and respond loop. Intermediate nodes along the route record the route information as route table entries. Control messages for route discovery and breaking include Route Request Message (RREQ), Route Reply Message (RREP), Route Error Message (RERR), and Hello Messages. Route Request (RREQ): When a route between the source and the destination is unavailable, a route request packet is sent over the network. The following table lists the parameters that are included in the route request packet:

| Source Address | Request ID | Source Sequence Number | Destination Address | Destination Sequence Number | Hop Count |
|---|---|---|---|---|---|

Table 1: Parameters of Route Request

The pair source address and request ID is used to identify the RREQ every duration the starting station transmits new one Request REQ and the request_ID is increased. When node receive the request message, every station verify the request_ID and start station addresses. The packet that is new is rejected if an RREQ packet with the identical pair of parameters already exists. A station lacking entrance route for the destination is one that rebroadcasts the RREQ with a higher hop counting parameter. A route reply messages are created and return to the start node if and only if station have a path with a sequence_number larger than or equal to RREQ.
Path Reply (RREP): When node discovers a correct path to the intended node, or if the intended node itself, it transmits an RREP message to the source. The following parameters are included in the route reply message:

| Source Address | Destination Address | Destination Sequence Number | Hop Count | Life Time |
|---|---|---|---|---|

Table 2: Parameters of Route Reply

Route Error Message (RERR): There is surveillance of the nearby nodes. Route error message that may be called as RERR on both sides of connection alerts the neighbouring nodes when an active route is lost.
Hello Messages: The purpose of the sent HELLO messages is to identify nearby nodes. The neighbourhood nodes communicate with each other directly. HELLO messages are sent in AODV to let the neighbours know that the link has been activated. Because of the short time to live (TTL) of one, these messages are not broadcast.
Route Discovery: The process of finding a node with which a source node wishes to interact begins when the source node lacks routeing information about the destination. As seen in figure 3, the procedure is started by broadcasting RREQ. Once the RREP message is received, the route is set up. Routeing information is updated with an RREP message of higher sequence number if multiple RREP messages with distinct routes are received.
Configuring a Reverse Path: Every node records the reverse path to the node when sending RREQ

signals. Once the destination node has been located, the RREP message proceeds along this path. Every node records the addresses of the neighbours from whom it receives RREQ packets.

Forward Path Setup: While an RREP message is being transmitted, a forward path is being set up. The path that is in reverse is utilised to convey the RREP message return to the start station. One could refer to this forward way as the reverse of the reverse path. The moment this forward path is configured, the data transfer begins. In a FIFO-queue, the packets that are locally buffered waiting for transmission are sent.

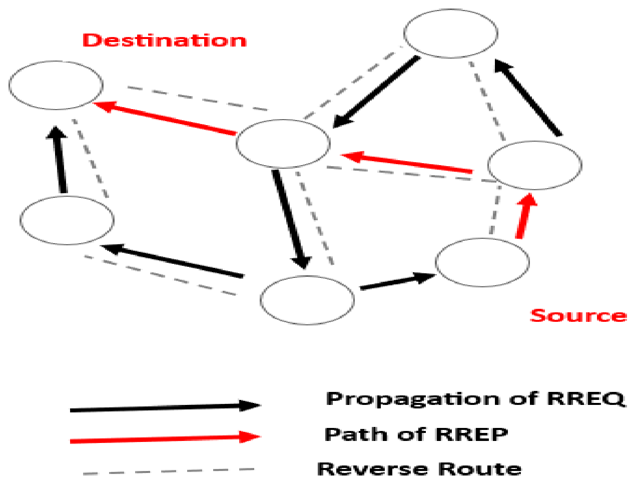


Figure 3. Discovery of Route

Although this protocol has numerous benefits, there are still certain difficulties, such as Route Discovery Latency: Since routes are discovered on demand, early route establishment delays may have an effect on real-time applications.

• Control Message Overhead: In highly dynamic networks, frequent route discoveries can still generate a significant amount of control message traffic even though AODV lowers overhead compared to proactive protocols.• Scalability Problems in Big Networks: The broadcast nature of RREQs in very large networks can cause more congestion and collisions, which could lower the protocol's efficacy.

| **Criteria** | **LEACH** | **AODV** |
|---|---|---|
| **Route Planning Technique** | Hierarchical (Cluster-Based) | Reactive (On-Demand) |
| **Structure of Network** | Clustered Hierarchical | Flat Structure |
| **Efficiency in Energy Use** | High | Variable |
| **The ability to scale** | Moderate | Moderate |
| **Latency** | Low to Moderate | Potentially High |
| **Reliability** | Moderate | High with Frequent Updates |
| **Security** | Vulnerable | Vulnerable to Specific Attacks |
| **Applications** | Energy-Constrained Environments | Dynamic and Mobile Networks |

Table1: Comparative study of LEACH,AODV

Existing routing protocols such as LEACH and AODV were originally designed for decentralized WSN architectures. With the rapid growth of IoT applications, centralized and programmable network management offered by SDN has emerged as a promising solution to overcome the limitations of conventional routing schemes. Consequently, SDN-based WSN architectures are gaining attention for improving traffic engineering, fault tolerance, and energy-aware routing in IoT environments.

**Conclusion**

Each routing protocol has pros and cons that make it suitable for specific IoT-based WSN scenarios. LEACH is ideal for energy-efficient applications since clustering can significantly reduce energy consumption. DAG-based routing and RPL are particularly effective in large, hierarchical networks where scalability, dependability, and energy efficiency are critical. Because on-demand routing offers advantages, dynamic, mobile networks with frequent topology changes are perfect for AODV. The optimal routing protocol depends on the specific requirements of the Internet of Things application, including the network's design, size, energy constraints, and need for security and reliability.SDN can viewed as an evolution of traditional WSN routing approaches.

**References:**

[1] O. Vermesan, P. Friess, P. Guillemin, R. Giaffreda, H. Grindvoll, M. Eisenhauer, M. Serrano, K. Moessner, M. Spirito, L.C. Blystad, E.Z. Tragos Internet of Things beyond the Hype: Research, Innovation and Deployment Building the Hyperconnected Society-Internet of Things Research and Innovation Value Chains, Ecosystems and Markets 2022

[2] F. Wu, L. Xu, S. Kumari, X. Li, J. Shen, K.K.R. Choo, M. Wazid, A.K. Das

[3] An efficient authentication and key agreement scheme for multi-gateway WSNs in IoT deployment J. Netw. Comput. Appl., 89 2017

[4] G. Bhukya Suresh A survey on enhanced energy efficient routing protocol of WSN for internet of things J. Univ. Shanghai Sci. Technol., 23 (7) 2021.

[5] Rawat, P.; Chauhan, S. Clustering protocols in WSN: A survey, classification, issues, and future directions. *Comput. Sci. Rev.* 2021

[6] Heinzelman, W.R.; Chandrakasan, A.; Balakrishnan, H. Energy-efficient communication protocol for wireless microsensor networks. In Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, Maui, HI, USA, 7 January 2000

[7] Dionisis, K.; Nakas, C.; Vomvas, D.; Koulouras, G. Applications of WSNs: An up-to-date survey. *Appl. Syst. Innov.* 2020

[8] Ju, X. Energy-efficient routing sensing technology of WSNs based on Internet of Things. *J. High Speed Netw.* 2021

[9] Marek, K.; Bijok, T.; Sciuto, G.L. Design and Modeling of Intelligent Building Office and Thermal Comfort Based on Probabilistic Neural Network. *SN Comput. Sci.* 2022

[10] Pedro, C.; Martinez, J.; Rodriguez-Molina, J.; Cuerva, A. Integration of wearable devices in a WSN for an E-health application. *IEEE Wirel. Commun.* 2013

[11] Alduais, N.A.M.; Abdullah, I.; Jamil, A. An efficient data collection algorithm for wearable/mobile tracking system in IoT/WSN. In Proceedings of the 2018 Electrical Power, Electronics, Communications, Controls and Informatics Seminar (EECCIS), Batu, Indonesia, 9–11 October 2018

[12] Fatemeh, S.; Souri, A.; Baker, T.; al Ridhawi, I.; Aloqaily, M. PriNergy: A priority-based energy-efficient routing method for IoT systems. *J. Supercomput.* 2020

[13] Zin, M.C.; Gopal, L.; Aung, Y.L. WSN-based reconfigurable water quality monitoring system in IoT environment. In Proceedings of the 2017 14th International Conference on Electrical

Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), Phuket, Thailand, 27–30 June 2017

[14] Santanu, M.; Nguyen, H.A.D.; Ha, Q.P. IoT-enabled WSNs for air pollution monitoring with extended fractional-order Kalman filtering. *Sensors* 2021

[15] Lo Sciuto, G. Air pollution effects on the intensity of received signal in 3G/4G mobile terminal. *Int. J. Energy Environ. Eng.* 2019

[16] Giacomo, C.; Sciuto, G.L.; Monforte, P.; Napoli, C. Cascade feed forward neural network-based model for air pollutants evaluation of single monitoring stations in urban areas. *Int. J. Electron. Telecommun.* 2015

[17] Khalid, H.; Din, I.U.; Almogren, A.; Islam, N. An energy efficient and secure IoT-based WSN framework: An application to smart agriculture. *Sensors* 2020, *20*, 2081. [Google Scholar]

[18] Sushanth, G.; Sujatha, S. IOT based smart agriculture system. In Proceedings of the 2018 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India, 22–24 March 2018

[19] Maryam, S.; Sadeghi-Niaraki, A.; Choi, S.; Islam, S.M.R. Performance analysis of IoT-based health and environment WSN deployment. *Sensors* 2020

[20] Alamelu, J.V.; Mythili, A. Design of IoT based generic health care system. In Proceedings of the 2017 International Conference on Microelectronic Devices, Circuits and Systems (ICMDCS), Vellore, India, 10–12 August 2017

[21] Sabrine, K.; el Houssaini, D.; Kammoun, I.; Kanoun, O. Precision irrigation: An IoT-enabled WSN for smart irrigation systems. In *Women in Precision Agriculture*; Springer: Cham, Switzerland, 2021

[22] Heinzelman, W., Chandrakasan, A., and Balakrishnan, H., "Energy-Efficient Communication Protocols for Wireless Microsensor Networks", Proceedings of the 33rd Hawaaian International Conference on Systems Science (HICSS), January 2000.

[23] Lim C. A Survey on Congestion Control for RPL-Based WSNs. *Sensors*. 2019; 19(11):2567. https://doi.org/10.3390/s19112567

[24] Khedr, A.M.; Osamy, W.; Ahmed, S.; Abdel-Aziz, S. Privacy preserving data mining approach for IoT based WSN in smart city. *Int. J. Adv. Comput. Sci. Appl.* 2019, *10*, 555–563.

[25] G Yin, G Yang, W Yang, B Zhang, W Jin. An energy-efficient routing algorithm for wireless. In. International Conference on Internet Computing in Science and Engineering (ICICSE'08), IEEE, China; 2008.

[26] Ehsan S, Hamdaoui B. A survey on energy-efficient routing techniques with QoS assurances for wireless multimedia sensor networks. IEEE Communications Surveys & Tutorials. 2012;14(2), PP. 265-278.