International Journal of Computers and Informatics (IJCI)
Vol. (3), No. (10)

IJCI

المجلة الدولية للحاسبات والمعلوماتية
الإصدار (3)، العدد (10)

October 2024

# Challenges of Wireless Sensor Networks and their Solutions

**Leena Obaid, Roba Alhashmiy, Shahad Alsulami, and Atheer Majed**
College of Computer Science and Engineering, Taibah University, Madinah, Saudi Arabia

**Abdul Ahad Siddiqi**
Associate Professor, Department of Computer Science, College of Computer Science and Engineering, Taibah University, Madinah, Saudi Arabia
asadqi@taibahu.edu.sa

## Abstract

Wireless Sensor Networks (WSNs) have emerged as a critical technology with uses in the fields of smart cities, industrial automation, healthcare, and environmental monitoring. This research paper provides a thorough review of the challenges inherent in WSNs, with the intention of providing light on the challenges that practitioners and researchers have while setting up and maintaining these networks. The challenges involve several aspects, comprising data management, security, scalability, energy efficiency, and dependability. Security concerns: given that these networks' communication is open and wireless, maintaining data integrity and secrecy presents substantial issues. Furthermore, it is essential to guarantee data transmission dependability in dynamic, frequently severe situations. This research analyzes these challenges, looks at the methods and solutions that are currently being offered in the literature, and also points out areas that need more research and development in the area of wireless sensornetworks. Comprehending and resolving these obstacles is essential to realizing WSNs'complete potential and promoting

their extensive integration in various fields.

**Keywords:** WSNs, IoT, Challenges, Security, Routing, QoS.

## 1. Introduction

WSN refers to a group of sensor and routing nodes that can be deployed in various settings to forecast environmental factors like wind, temperature, and more. These networks gather and analyze data from small nodes before transmitting it to operators. Sensor networks find applications in diverse control systems, such as monitoring the environment, automating homes, detecting chemical and biological threats, deploying smart grids, conducting surveillance, and much more. Additionally, WSN plays a crucial role in aquaculture and the oil industry, encompassing tasks like data collection, offshore exploration, disaster prevention, tactical surveillance, and pollution monitoring.

Internet of Things (IoT) has emerged as a significant player in enhancing human life, alongside WSN. It has revolutionized the way we overcome social and physical barriers, providing ease and mobility to people, resulting in improved and equal opportunities, and access to information. IoT has a wide range of applications, including agribusiness, climate, clinical care, education, transportation, and finance. Researchers are drawn to IoT due to its potential in information and communication technology. Companies that have adopted this technology have become smarter, more competitive, automated, and sustainable in the global supply chain. In today's competitive marketplace, supply chains are struggling to keep up with each other. Therefore, IoT devices are an effective way to authenticate, monitor, and track products using GPS and other technologies. WSNs have emerged as a revolutionary technology in the field of IoT. These networks consist of a large number of autonomous sensor nodes that are capable of sensing, computing, and communicating with each other.

The primary purpose of WSNs is to collect and transmit data from the physical environment to a central base station or sink node. This data can then be processed and analyzedto extract useful information. WSNs are frequently utilized in distant locations where it is impractical for humans to intervene in post-deployment maintenance. Consequently, endeavorsare underway to improve their effectiveness and longevity. However, the deployment and operation of WSNs present several challenges that need to be addressed for efficient and reliable functioning. Numerous obstacles exist when it comes to deploying WSNs, including power consumption for long-distance deployment. However, thanks to advancements in automation trends and the development of applications, these obstacles are no longer hindrances for extensive remote deployment.

One of the main challenges in WSNs is routine. Since the nodes in a WSN are often deployed in a large area, it is essential to establish an efficient and reliable communication pathbetween the sensor nodes and the sink node. Various routing algorithms have been developedto achieve this goal, such as LEACH, AODV, and DSR. These algorithms consider factors likeenergy efficiency, network lifetime, and data delivery reliability. It is also important to ensuresecurity of WSNs. WSNs face security threats due to their distributed nature and resource- constrained sensor nodes. Ensuring data confidentiality, integrity, and authenticity is a significant concern. Security mechanisms such as encryption, authentication, and intrusion detection need to be implemented to protect against unauthorized access and attacks. Anotherchallenge in WSNs is data aggregation. Due to the large number of sensor nodes in a network,the amount of data generated can be overwhelming. Data aggregation techniques help in reducing the amount of data that needs to be transmitted by combining similar data from multiple nodes. This not only reduces the energy consumption but also improves the network scalability. Coverage is another critical challenge in WSNs. The sensor nodes need to be deployed in such

a way that they provide sufficient coverage of the monitoring area. Various coverage optimization techniques have been proposed to ensure that every point in themonitoring area is monitored adequately by the sensor nodes. WSN quality of service (QoS) isalso an important aspect to consider. QoS metrics such as reliability, latency, and throughput play a crucial role in determining the performance of a WSN. Ensuring QoS in WSNs is challenging due to the limited resources of the sensor nodes, such as energy, processing power,and memory.

## 2. Literature Review on Challenges Facing WSNs

This section of the paper provides a detailed account of the literature review conducted in connection with the challenges faced by WSNs.

### 2.1 Routing in WSNs:

Data moves along any network in the form of data packets. Each data packet contains aheader that contains information about the intended destination of the packet. As a packet travels to its destination, several routers may forward it multiple times. The function of the router is the process of determining a path in any network. And it performs this process millionsof times every second with millions of packets. When a data packet arrives, the router first looks up its address in a routing table. This is like a commuter consulting a bus schedule to findthe best bus route to their destination. The router then forwards or transmits the packet to the next point in the network. For example, when you visit a website from a computer in your office network, data packets first travel to the office network router. The router looks for the header packet and determines the destination of the packet. It then looks up its internal schedule and forwards the packet—either to the next router or to another device, such as a printer— within the same network. A computer network consists of several devices, called nodes, and paths or links between these nodes. Communication between two nodes in an interconnected

network can occur through several different paths. Also, routing is the process of choosing thebest path using some pre-defined rules. The routing creates efficiency in the network connection. Failure of network connections leads to long waiting periods for website pages toload for users [1]. It can also cause website servers to crash because they can't handle many users. Managing data traffic helps reduce network failure so that the network can use as muchof its capacity as possible without causing congestion. High levels of traffic can lead to congestion, affecting the router's performance and potentially causing delays in data transmission. Thus, efficient routing is an important aspect for all systems, without exception.One of the fundamental challenges of effective routing is the need to balance trade-offs between security, privacy, and efficiency. On the one hand, routing paths that are long or complex can compromise users' privacy by exposing their information. On the other hand, overly simplified routing paths can undermine network security and efficiency by increasing the risk of fraud and congestion. Regular security updates and configurations are critical to reducing the security threats that routers are vulnerable to, including unauthorized access, denial-of-service (DoS) attacks, and attempts to exploit vulnerabilities.

WSNs are utilized in a variety of industries, including the military, healthcare, agriculture, disaster relief, and others, to keep an eye on the local environmental conditions. And any defect in the routing may have a lot of detrimental effects. The dynamic nature of WSN networks refers to the constant changes and movements within the network. This includes nodes joining or leaving the network, as well as changes in the network topology dueto environmental factors or node failures. These dynamics pose challenges for maintaining reliable communication and efficient data transmission within the network. Also, multipath routing one way to improve routing efficiency and privacy is to use multiple paths for a singletransmission. By splitting the packet into several parts,

users can reduce the possibility of analysing the transmission log while increasing their chances of finding an efficient route [2].This leads to several negative effects on routing, including data duplication. In most sensor network applications, sensor nodes are densely spread over a region of interest and cooperate to accomplish a common, sensible task. Thus, data sensed by multiple sensors points usually has some level of correlation or redundancy. Consequently, the most common cause of outageissues is a network's failure and the lack of an alternate recovery routing path. Thereby

redundant network topologies—which include the use of redundant switches, routers, and links—help to establish backup channels for data transfer, guaranteeing that the network can function uninterrupted even in the event of a failure of a single component or link [3]. A rangeof protocols and technologies are utilized to provide recovery routing paths, including:

- **Routing Protocols:** In the event of a link failure, dynamic routing protocols such as EIGRP (Enhanced Interior Gateway Routing Protocol) and OSPF (Open Shortest PathFirst) can dynamically adjust to changes in the network.
- **Link-State Protocols:** In the event of a breakdown, routers can swiftly reroute traffic thanks to these protocols, which keep a thorough and current picture of the network.
- **Load Balancing:** In the event of a failure, traffic can be immediately diverted to an accessible path. Load balancing is a technique used by some systems to distribute trafficamong different paths.
- **Redundant Hardware:** If a component fails, an alternate path is guaranteed by employing physical redundancy, such as redundant switches, routers, or networkcables.

Recovery routing paths are intended to reduce downtime, preserve service availability, and guarantee data integrity in the event of unanticipated network events. This is especially important for mission-critical systems, where uninterrupted operation is vital.

The routing table is a crucial component that maps IP addresses to the next hop or exit interface, guiding the router on how to forward packets [4]. Large or inefficient routing tables can impact a router's ability to process and forward packets efficiently. Thus, routing table issues can lead to network problems, affecting the ability of routers to forward packets to their destinations efficiently. Routine maintenance and optimization of routing tables are important for optimal performance. The following is a list of some of the important problems that a routing table may encounter, along with solutions:

- **Incorrect Routes:** Issue: Packet misrouting may result because out-of-date or incorrect paths in the routing table. Solution: Utilize dynamic routing protocols or manual configuration to maintain accurate and current routing information, and update and review routing tables on a regular basis.
- **Route Aggregation Problems:** Issue: Larger routing tables might result from inappropriate aggregation or overly detailed routes, which can be inefficient.
- **Solution:** Reduce the number of entries in the routing table by implementing route summarization or aggregation; this will minimize routing table size and increase efficiency.
- **Routing Loops:** Issue: Packets can continuously travel between routers in a routing loop, which is caused by inconsistent or inaccurate routing information. Solution: Employ dynamic routing protocols that incorporate loop prevention measures. Examples of such protocols include the Split Horizon rule, Route Poisoning, and Hold-down timers.

International Journal of Computers and Informatics (IJCI)
Vol. (3), No. (10)
IJCI
المجلة الدولية للحاسبات والمعلوماتية
الإصدار (3)، العدد (10)
October 2024

Routing table problems can be quickly identified and resolved with the use of network monitoring tools. Other preventative measures include regular monitoring, appropriate documentation, and adherence to best practices in routing table maintenance.

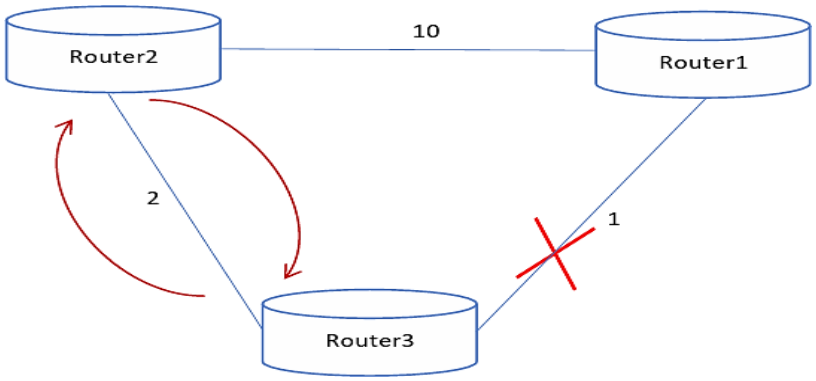



Figure (1): Example of Routing Loop

The batteries that power the wireless sensor nodes have a finite lifespan and are incrediblysmall. Therefore, maximizing network lifetime and minimizing energy consumption are the most important considerations when designing protocols and applications to achieve longevity and reliability. For this purpose, the limited energy resources of sensor nodes pose a significant challenge in the design of routing protocols. Efficient energy management techniques, such as node clustering and data aggregation, should be incorporated to prolong network lifetime [5]. This is another important consideration strong methods for node discovery and route maintenance must be used by the routing protocols to accommodate these changes and guarantee smooth communication. since this power supply failures are a common cause of network downtime. By using redundant power supplies, organizations can ensure that the network remains powered even if one power supply fails.

In a network setting, data backup and replication are essential for guaranteeing data availability, integrity, and recoverability. It is crucial to remember that routers, which are

network equipment primarily in charge of forwarding data packets between networks, usually do not deal directly with data replication and backup. Alternately, usually, servers, storage systems, or specialized backup appliances oversee these tasks. Routers are subject to hardwarefaults like any other electronic device, including broken parts, power supply problems, and overheating. And that leads to router hardware malfunctions, which can seriously impair a network's dependability and functionality. As essential parts of the network infrastructure, routers might experience a variety of hardware problems that can impair regular operations. Memory modules, CPUs, and interface cards are examples of components that frequently malfunction in hardware systems. Failures of memory modules may result in data loss or corruption, which will impair the router's capacity to efficiently store and process data. Further, performance issues or outright system breakdowns can be caused by CPU faults [6]. Also, failures of the interface cards may affect the router's capacity to connect to other networks or devices. Hardware failures can be lessened by implementing redundancy measures, such as hot-swappable components or dual power sources. To guarantee that routers in a network remain reliable, it is necessary to implement preventative maintenance, timely replacement ofmalfunctioning gear, and regular monitoring. These measures lead to reducing downtime, optimizing network performance, and enhancing whole network durability in the confronting of hardware challenges.

Router scalability also presents a unique challenge due to the inherent characteristics of sensor devices. WSNs comprise numerous tiny, resource-constrained sensors tasked with collecting and transmitting data wirelessly. As the network expands to accommodate a growingnumber of sensors, routers within the

WSN must grapple with the limitations of these resource-constrained devices. The challenge lies in maintaining efficient routing protocols and algorithms that can scale seamlessly with the increasing size of the network without compromising performance. Balancing the need for scalability while considering the energy constraints of sensor nodes is a critical aspect of addressing this challenge in WSNs, ensuringthat the network can effectively adapt to the dynamic nature of the environment it is monitoring.At last, routers are essential for maintaining smooth data transmission and communication inside a network. They can still face a variety of difficulties, though, which could negatively affect both their effectiveness and the network's general dependability. These challenges require proactive management and mitigation measures, ranging from hardware failures and routing table issues to security risks and setup errors. Overcoming these obstacles requires consistent upkeep, attention to best practices, and the installation of strong security measures.

Organizations can improve network resilience, lower downtime, and maximize the effectiveness of their communication infrastructure by methodically addressing router issues.

### 2.2 Challenge of Security of WSNs:

WSN security is currently a hot topic in WSN technology research. Due to their inherentvulnerabilities, wireless sensor networks have a significant impact on data availability, confidentiality, and integrity. The data gathered by the sensor node cannot be reliably and promptly transmitted to the destination sink node, particularly in the event of a network routing attack. Similar to conventional computer communication networks, a variety of attacks pose the biggest threat to the security of wireless sensor networks. In addition, wireless sensor networks are susceptible to denial-of-service attacks due to their energy-constrained sensor

nodes and radio characteristics that make it easier for attackers to launch passive and active attacks against the network. Sensor networks are also subject to monitoring, tampering, forging, and blocking attacks. The attack on wireless sensor networks might be classified to:[7]

### 2.2.1 Internal/External Classification

This table classifies WSN attacks into internal and outsider attacks.

Table (1): Internal and external attack classification [8]

| Internal | External | Internal /External |
|---|---|---|
| Collision | Eavesdropping | Node tampering |
| Replay attack | Basic jammers | Hardware hacking |
| Selective forwarding | Intelligentjamming | Spoofed/altered inf. |
| Black hole | Node replication | Hello flood |
| Sinkhole | | Energy drain |
| Sybil attack | | Desynchrony attack |
| Worm hole | | Attack on reliability |
| Data integrity | | Malicious code attack |
| | | Denial of service |
| | | Man in the middle |

### 2.2.2 Layer-based Classification:

This classifies the attack based on network layers. The below table summarize this classification.

Table (2): Layer-based classification [8]

| Layer | Attack Types |
|---|---|
| Physical Layer | Tampering /destruction, Radiointerference, Jamming |
| Data Link Layer | Unfairness, Collision, Exhaustion,Interrogation, Sybil Attack. |
| Network Layer | Node Capture, Sybil, Sinkhole, Selective Forwarding / Black Hole, Hello Flood, Wormhole, (Altered, spoofed or Replay Routing Information), Acknowledgment Spoofing, Homing, Internet Smurf, Misdirection |
| Transport Layer | De-synchronization, flooding |
| Application Layer | Path-based DOS, overwhelm, deluge |

International Journal of Computers and Informatics (IJCI)
Vol. (3), No. (10)
المجلة الدولية للحاسبات والمعلوماتية
الإصدار (3)، العدد (10)
October 2024

## 2.3 Data Aggregation

Data gathering is the process of collecting information from the network's source or intermediate nodes. The process of aggregate the data from more than one node or sensor causea redundant information, which lead to bandwidth wasted if it is transferred to the sink node initsits current state. Additionally, it raises the nodes' energy consumption. Therefore, in order to extend the network lifetime, it is necessary to lower the energy consumption of nodes by reducing the number of packets that are transmitted. We call this procedure "data aggregation".This mode describes the architecture of data aggregation.

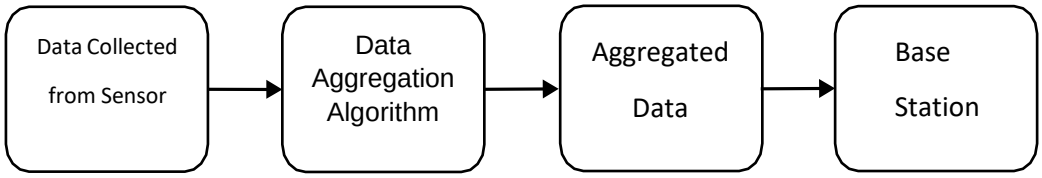



Figure (2): Data aggregation architecture

The main goal of data aggregation is to eliminate redundant data by using data aggregationfunctions to extract relevant information from the collected data such as MAX, MIN, MEAN,MEDIAN. [9]

International Journal of Computers and Informatics (IJCI)
Vol. (3), No. (10)
IJCI
المجلة الدولية للحاسبات والمعلوماتية
الإصدار (3)، العدد (10)
October 2024

### 2.3.1 Aggregation and Non-Aggregation Models

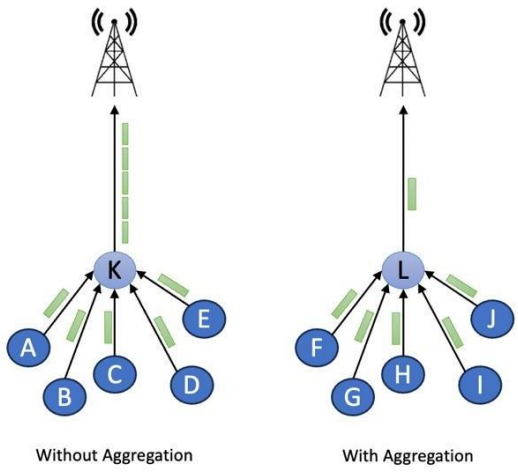



Figure (3): Non-Aggregation and Aggregation Models

The sensor nodes labeled (A, B, C, D, E, F, G, H, I, and G) in this figure are typical nodesthat gather data and relay it to the top node. The two sensor nodes (K, L) together constitute anaggregator of nodes that jointly sense and aggregate data. Both models contain five data packetstraveled through the network but the first one which doesn't use the aggregate concept forwardeach packet to the sink. While the aggregation model forward only one data packet to the sink.Based on these two models, it can be concluded that utilizing the data aggregation process decreased the quantity of data packets transmitted, extending the wireless sensors' overall lifespan. [10]

### 2.3.2 Data Aggregation Techniques According to Network Architecture

Data aggregation depends on network's type. Mainly it classified into two categories which are flat network and hieratical network. Each category will be discussed in detail.

#### 2.3.2.1 Flat Network

Because every sensor node in a WSN has an equal supply of power and operates in a similar manner, flat networks play a critical role in WSNs. In data aggregation, these kinds of networks necessitate data-centric routing, while the sink sends data packets to sensor nodes, much like in floods. Flooding sensors transmit response data packets back to the sink after carrying data that matches the data packets.

#### 2.3.2.2 Hierarchal Network

A common cause of the high energy consumption rates in flat networks is the strain that computing and communication in any form place on the sink. In the case of hierarchical networks, fewer data packets are sent to the sink because a unique node aggregates the data. As a result, the hierarchical networks—which include chain based, In-Network, Tree Based, and Cluster Based networks—perform better overall in terms of energy efficiency when they have this kind of structure. [11]

- **Chain Based Network Technique**

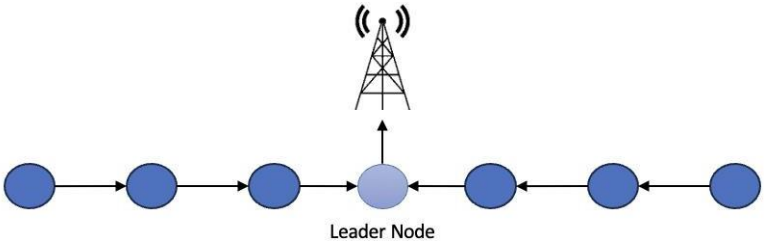
In order to move sensed data from the sensor nodes to their nearest neighbor rather than the cluster head, one or more chains are formed in this network. This method selects a leader to handle data aggregation and ultimately routes the data to the sink node. In addition to saving some energy, this process is distinguished by its straightforward topology and ease of implementation, as it eliminates the need for competition in selecting the cluster head.Ultimately, the sensor node only sends its sensed data to the node next to it. However, this technology has a number of drawbacks, such as a significant delay in data transmission becauseof the length of the chain and the number of hops required to transfer the data; additionally, there is an imbalance in the energy consumption by the sensing node because the leader

node's nearby node experiences more energy consumption due to excessive data traffic than the remote node, which has less data to transmit. Examples of this technique are PEGASIS (Power-Efficient Gathering in Sensor Information Systems) and EBCRP (Energy-Balanced Chain- Cluster Routing). The chain-based data aggregation method is depicted in Figure 4.

Figure (4): Structure of chain approach

- **In-Network Approach**

A comprehensive method for gathering and processing data at intermediate nodes and routing information over multi-hop networks is called in-network aggregation.




Its primary goal is to lower the total power used during the operation. There are two types of known in-network aggregation:

1. Size-reducing aggregation: To reduce the size of the packets that are sent to the sink node, the data packets that are coming from sensor nodes via their neighboring nodes are combined and compressed.
2. Without any size reduction: When combining the packets of different neighbor nodes into a single packet, the data value is not processed in this instance.

   Data Routing In-Network Aggregation (DRINA) and Modified Data Routing In-Network Aggregation (M-DRINA) are a couple of instances of this kind of protocol.

- **Tree Based Approach**

The creation of Data Aggregation Trees (DAT) mandates the creation of minimal spanning trees for every data transmission. As seen in Figure 5, every node in the network hasa parent-child relationship with data directed in a bottom-up manner. While the parent nodes aggregate the data within the networks, the data flows from the leaf nodes towards the sink node. Tiny Aggregation (TAG) is one instance of this kind of protocol.

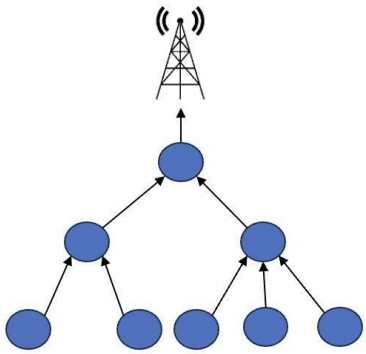


Figure (5): Structure of tree approach

- **Cluster Based Approach**

WSNs with cluster-based architecture have longer network lifetimes and improved energy efficiency. It reduces the number of messages sent to Base Station or the sink. We referto these as Cluster Head nodes (CHs) See Figure 6. A group of nodes in a network can choose to cluster in order to establish a good topology. A comprehensive set of neighbours can be selected based on various criteria, including density, energy, etc. A cluster is a categorized collection of nodes that has been named. They are collecting packets from non-cluster and managing and forwarding

them. This approach provides a functional network structure. [12]

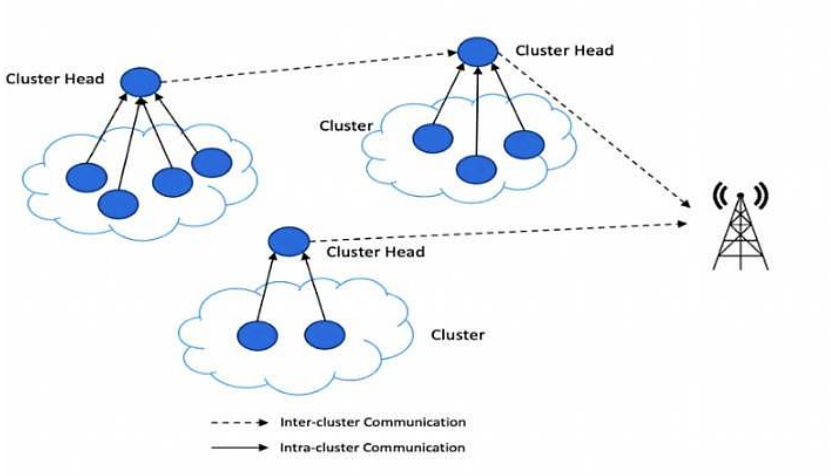



Figure (6): Structure of cluster-based approach

### 2.4 Challenge of Coverage of WSNs

Coverage is a significant challenge in WSNs and plays a crucial role in ensuring effectivemonitoring of the designated area. The deployment of sensor nodes must be carefully plannedto achieve sufficient coverage across the monitoring area. Researchers have proposed several coverage optimization techniques with the objective of ensuring that every point within the area is adequately monitored by the sensor nodes. Here are some key aspects related to coverage optimization in WSNs:

- **Node Placement**: The placement of sensor nodes is a fundamental aspect of coverageoptimization. Different strategies can be employed, such as random deployment, deterministic deployment, or hybrid approaches. Factors considered during node placement include sensor node density, deployment cost, energy efficiency, and coverage quality.

- **Coverage Models:** Coverage models are mathematical representations that define the extent to which a sensor node can cover a specific area. Various coverage models have been proposed, including distance-based models, probabilistic models, and directional
- models. These models help in estimating the coverage achieved by the sensor nodes and guide the deployment process.
- **Coverage Optimization Algorithms:** Numerous algorithms have been developed to optimize coverage in WSNs. These algorithms aim to find an optimal or near-optimal node placement that maximizes coverage while considering constraints such as limited energy resources, connectivity, and deployment cost. Examples of coverage optimization algorithms include Voronoi-based algorithms, genetic algorithms, and particle swarm optimization.
- **Energy Efficiency:** Energy efficiency is a critical consideration when optimizing coverage in WSNs. Sensor nodes typically operate on limited battery power, and energy consumption must be managed to prolong the network's lifetime. Coverage optimization techniques often consider energy-aware strategies, such as adjusting transmission power, node sleep scheduling, or energy-efficient routing protocols.
- **Coverage Hole Mitigation:** Coverage holes, which are areas lacking adequate sensor node coverage, can occur due to various factors such as node failure, obstacles, or uneven deployment. Coverage optimization techniques aim to identify and mitigate such coverage holes by repositioning nodes, adjusting transmission power, or incorporating additional nodes into the network. Researchers focus on optimizing coverage, deployment strategies, and node management to improve the efficiency and performance of these

networks. In this research we will introduce and briefly explain some of them.

### 2.4.1 Coverage Types

The initial step in the implementation of a wireless sensor network involves determining the specific area that needs to be monitored. Complete or comprehensive coverage implies that every point within the area of interest is within the sensing range of at least one sensor node. The ideal approach to achieve comprehensive coverage is to deploy the minimum number of sensor nodes necessary within the field. One proposal to achieve this is the concept of an r-strip construct, where each sensor is positioned at a distance of r from its neighboring sensor, ensuring comprehensive coverage. However, this solution is deemed impractical due to various limitations. Target coverage focuses on observing a fixed number of targets, particularly in military applications. In this particular research paper, the authors conducted extensive tests to detect, classify, and track targets while also aiming to conserve energy. Barrier coverage, on the other hand, involves detecting movement across a line of sensors, referred to as the maximal breach path. The authors of this study quantified the enhancement in coverage when additional sensors were introduced to the network. Other papers concentrate on developing algorithms related to barrier coverage. Sweep coverage, which can be seen as a variation of barrier coverage, addresses the challenge of monitoring a moving barrier.

### 2.4.2 Deployment

Sensor network deployments can be classified as dense or sparse, with dense deployments having a high number of sensor nodes in the field of interest and sparse deployments having fewer nodes. Dense deployments are used when multiple sensors are needed or when cost is prohibitive. Sensor nodes are typically static, while mobile nodes can relocate after deployment. One algorithm depends

on determining the optimal location for sensor nodes to provide maximum coverage, but it requires each node to be within the sensing range of anothernode. The other deployment algorithm communicates with neighbors and instructs them to move away until they are at a distance, maximizing coverage while maintaining connectivity. Some researchers introduce a method that aims to maximize coverage while minimizing sensormovement, but it requires a complex algorithm and may tax sensor nodes. Sensor network nodes can be deployed in predetermined locations or randomly located, with deterministic placement being easier to develop. Random deployments are typically dense, as additional sensors are needed for coverage if sensor nodes are stationary. Networks with mobile sensors typically start with random deployments, focusing on maintaining coverage while minimizingenergy consumption.

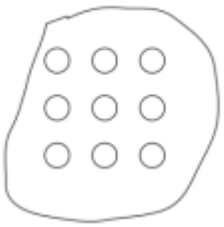


Figure (7): Deterministic Placement [21]

Figure (8): Random Placement [21]

### 2.4.3 Node Type

Sensor networks can be homogeneous or heterogeneous, with homogeneous groups having all nodes having the same capabilities and heterogeneous groups having more powerfulnodes. Cluster heads gather data from less powerful nodes. Algorithms require a homogeneousset of nodes, with nodes placed at precise distances based on identical sensing ranges. Some algorithms work for both homogeneous and heterogeneous networks. Some papers use a weighted Voronoi diagram to extend an energy-efficient network using homogeneous sensors,

proving their theories first with a homogeneous deployment and then with a heterogeneous deployment.

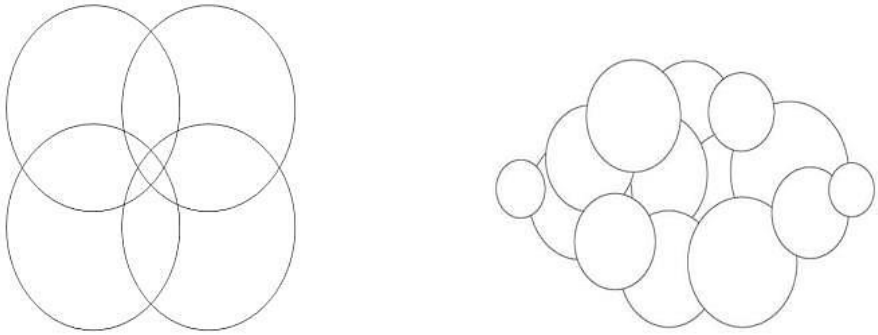


Figure (9): Homogeneous Placement and Heterogeneous Placement [21]

### 2.5 WSNs for IoT Applications

WSNs consist of small, low-cost sensors that are easy to deploy, making them part of the Internet of Things (IoT). Due to the cost of WSN, sensor nodes are easy to deploy in areas thatare hardly accessible to humans and can be controlled under severe conditions. This is thanks to their limited size and their communication capabilities.

WSN for IoT applications faces several challenges in terms of quality of service (QoS). QoS is defined as the ability of network elements to support a certain level of assurance for a specific service, enhancing performance and reliable data delivery [18] in a real-world scenario, QoS is paramount to the performance of the network. This includes various key termssuch as security, reliability, availability, throughput, latency, delay, jitter, maintainability, bandwidth, and energy consumption.

### 2.6 QoS in Real-Time Traffic

The real-time transformation system should have a QoS technique work at both

ends for the providence of maximum advantage. QoS execution works on 2 and 3 layers. The QoS canbe recognized through routers on layer 3. While layer 2 for the congestion and QoS. Data trafficis measured in the constant bit rate or variable bit ratio. Thus, the classification is based on thetype of incoming traffic received at the network edge router. There are three types of QoS models.

First, best-effort service delivery model. It uses first-in-first out (FIFO) as queuing scheduling so there is no guarantee of reliability, throughput, and delay. Second, integrated service model (IntServ) uses a signaling protocol to notify the network of its traffic parametersand apply for a specific level of QoS before sending packets. The IntServ model uses the Resource Reservation Protocol (RSVP) for signaling. The RSVP protocol reserves resources such as bandwidth and priority on a known path, and each network element along the path must reserve required resources for data flows requiring QoS guarantee. IntServ has adaptability issues and is not generally acknowledged in sending [18]. Last, differentiated service model (DiffServ) classifies packets on a network into multiple classes and takes different actions for each class. When network congestion occurs, packets of different classes are processed based on their priorities, resulting in different packet loss rates, delay, and jitter. is the best choice QoS.

Packet loss in a network is primarily caused by congestion and delays within the packet information system queues. These queues, present at every output port, are essential for packetsto enter and leave the network. If the queues are empty or close to capacity, packets are immediately sent to the output line. However, if the queues are full due to high traffic, packetsare delayed until all preceding packets in the queue are sent, leading to an increase in the packetloss ratio.

The IntServ model, although facing adaptability issues and not widely used for

web-based communication, has been considered in this context by the authors [18]. However, DiffServ is preferred for execution due to its ability to assign resources to traffic groups instead of individual streams. The IntServ paradigm emphasizes the importance of service quality for all network hubs and utilizes the RSVP to negotiate and request specific quality of service requirements for applications, while also considering the limitations of this approach for larger systems. DiffServ is an alternative method for allocating network resources, described in RFC- 2475, that assigns resources to traffic groups rather than individual flows. It offers two forwarding groups: Assured Forwarding (AF) and Expedited Forwarding (EF). AF classes are assigned several assets, and packets within these classes are prioritized based on drop priority and blockage conditions. EF provides services with low jitter, loss, and delay, and is implemented using a priority queue.

The authors [18] suggested a model that aims to improve the performance of real-time collaborative data traffic by reducing packet delay and loss. It considers different types of data traffic, such as variable bit rate video traffic and constant bit rate internet protocol traffic and applies differentiated services-based QoS techniques. The model is implemented at the edge of the IP network, utilizing routers with multiple queues, including a dedicated line for signaling traffic, to prioritize and manage the different types of data traffic effectively. The method is to improve network performance for real-time traffic by guaranteeing QoS without over- provisioning constrained bandwidth. The model operates at the network's edge and is based on DiffServ, and it was validated using simulation-based testing. The results show that the proposed approach effectively reduces packet loss and delays, improving the quality of real- time traffic such as voice and video communication.

## 2.7 Congestion Avoidance in WSNs

Despite the progress made in WSNs, there are still challenges due to the limited computational capacity, storage, and power of sensors. To prolong the network's lifespan, it iscrucial to address energy-intensive tasks, such as routing. This means finding efficient ways todetermine the optimal paths for data transmission within the network to conserve energy and improve overall performance. In WSNs, the end-to-end delay consists of various components,including propagation delay, queuing delay, processing delay, medium access delay, and transmission delay. Queuing delay is particularly important for congestion avoidance in WSNs,as it is non-deterministic and can lead to increased end-to-end delay. To mitigate this, it is necessary to find node disjoint paths (paths with no common nodes) for each application in order to minimize the average queue length and reduce end-to-end delay.

Software Defined Network (SDN) is a promising solution for congestion avoidance inWSNs. In SDN, the network is viewed as a data plane that performs various functions like packet forwarding, while a centralized controller manages and configures the network. The controller acts as a central point, collecting information about the network's state and resourcesto make coordinated decisions and optimize network performance. The authors [19] utilize SDN to gain a global understanding of the entire WSN deployment. They propose an algorithm that uses graph-based techniques to select non-overlapping paths for each application, considering the diversity of communication paths. By integrating this algorithm into SDN-WISE, they aim to satisfy QoS requirements and prevent network congestion by identifying appropriate and efficient communication paths for multiple applications running on the same WSN. Path Finding Algorithm is used to compute all possible paths for each application, considering the source and destination nodes. The end-to-end delayis estimated

based on factors such as the number of hops, transmission delays, and propagation delays, which are influenced by packet size and communication technologies like 802.11 and Zigbee. Conflict Graph Algorithm is a tool used to identify the paths with the least conflicts between source and destination nodes in a wireless sensor network. To determine the best set of nodes, the graph is reduced by removing nodes with a high number of conflicts. Different measures of centrality, such as degree centrality, eigen-vector centrality, and page rank, are used to identify important nodes in the conflict graph. Calculate Cost Algorithm is used to calculate the cost of each path from a source to a destination in a network, taking into accountcommon nodes shared by different paths. The algorithm considers the estimated delay from thesource to the destination, the queuing delay induced by common aggregator nodes, and the packet arrival rate at those nodes. This cost calculation helps determine the optimal paths basedon minimizing delays and distributing loads in the network.

The authors [19] focus on ensuring timely data delivery while minimizing the increasein network queue length. The approach involves constructing a conflict graph based on the overlapping data dissemination paths of multiple applications and using graph theoretic algorithms to reduce conflicts and select the best combination of paths to satisfy QoS requirements. The algorithms outperformed existing methods by up to 34% and up to 14% worst in comparison to the optimal solution for various topologies and network sizes, but limitations include sparse graph connectivity and the need for path recalculation in the event of topology changes.

## 3. Conclusion

Examining challenges pertaining to WSNs has shed light on several important areas. Onemajor issue that has been identified is routing, which emphasizes the need for

effective algorithms to optimize data transmission paths. Security issues highlight how important it is tohave strong encryption and intrusion detection systems in place to protect sensitive data in WSNs. One important factor to keep in mind when reducing energy use and improving network efficiency is data aggregation. In addition, resolving coverage problems is necessary toguarantee that sensor nodes sufficiently observe the environment of interest. It is critical to address the interoperability and scalability issues that arise as WSNs advance toward integration with the IoT. The achievement of a strong and effective IoT ecosystem will be made possible by the smooth integration that will result from successfully navigating these challenges. The focus of this study is on the complex interrelationships among wireless sensornetworks' problems. Since these networks are dynamic and play a critical role in the larger IoTslandscape, effective solutions must be comprehensive. To ensure the sustainable developmentof wireless sensor networks and their integration with emerging technologies, future research endeavours should keep exploring these challenges and promoting innovation and advancements.

## References

1. Z. Mammeri, Reinforcement learning based routing in networks: Review and classification of approaches, IEEE Access, vol. 7, pp. 55916–55950, 2019.
2. S. Alaparthi, S. R. Parvataneni, C. S. Vaishnavi, P. Sathvika, M. Chandrika, and P. Sharanya, “Dynamic source routing protocol—A comparative analysis with AODV and dymo in ZigBee based wireless personal area network,” in Proc. 6th Int. Conf. Signal Process. Integr. Netw. (SPIN), Noida, India, 2019, pp. 1042–1046.
3. A. Agrawal, V. Singh, S. Jain and R. K. Gupta, "Gcrp: Grid-cycle routing protocol for wireless sensor network with mobile sink", AEU - International Journal of Electronics and Communications, vol. 94, pp. 1-11, 2018.
4. Yao, J.; Zhang, K.; Yang, Y.; Wang, J. Emergency vehicle route-oriented signal coordinated

control model with two-level programming. Soft Comput. 2018, 22, 4283– 4294.

5. Wang,J.; Gao, Y.; Liu, W.; Sangaiah, A.K.; Kim, H.J. An Improved Routing Schema with Special Clustering using PSO Algorithm for Heterogeneous Wireless Sensor Network. Sensors 2019, 19, 671.
6. J. Wang, Y. Gao, W. Liu, A. K. Sangaiah and H.-J. Kim, "Energy efficient routing algorithm with mobile sink support for wireless sensor networks", Sensors, vol. 19, no. 7,2019.
7. Huanan, Z., Suping, X., & Jiannan, W. (2021). Security and application of wireless sensor network. Procedia Computer Science, 183, 486-492.
8. Elsadig, M. A., Altigani, A., & Baraka, M. A. (2019). Security issues and challenges on wireless sensor networks. Int. J. Adv. Trends Comput. Sci. Eng, 8(4), 1551-1559.
9. Kaur, M., & Munjal, A. (2020). Data aggregation algorithms for wireless sensor network:A review. [1]Ad hoc networks, 100, 102083.
10. Abdalkafor, A., & Aliesawi, S. (2022). Data aggregation techniques in wireless sensors networks (WSNs): Taxonomy and an accurate literature survey. AIP Conference Proceedings, 2400(1), AIP Conference Proceedings, 2022, Vol.2400 (1).
11. Saeedi, I. D. I., & Al-Qurabat, A. K. M. (2021, March). A systematic review of data aggregation techniques in wireless sensor networks. In Journal of Physics: Conference Series (Vol. 1818, No. 1, p. 012194). IOP Publishing.
12. Ibrahim, D. S., Mahdi, A. F., & Yas, Q. M. (2021). Challenges and issues for wireless sensor networks: A survey. J. Glob. Sci. Res, 6(1), 1079-1097.
13. D. Davis and V. Vokkarane, “Failure-aware protection for many-to-many routing in content centric networks,” IEEE Trans. Netw. Sci. Eng., no. 99, pp. 1–16, 2019.
14. Huanan, Z., Suping, X., & Jiannan, W. (2021). Security and application of wireless sensor network. Procedia Computer Science, 183, 486-492.
15. M. A., Altigani, A., & Baraka, M. A. (2019). Security issues and challenges on wireless sensor networks. Int. J. Adv. Trends Comput. Sci. Eng, 8(4), 1551-1559
16. K.J.PaiandJ.M.Chang,“Dual-cists: Configuring a protection routing on some cayley

networks," IEEE/ACM Trans. Netw., vol. 27, no. 3, pp. 1–12, 2019.

17. Gulati, K., Boddu, R. S. K., Kapila, D., Bangare, S. L., Chandnani, N., & Saravanan, G. (2022). A review paper on wireless sensor network techniques in Internet of Things (IoT). Materials Today: Proceedings, 51, 161-165.
18. Mazhar, T., Malik, M. A., Mohsan, S. A. H., Li, Y., Haq, I., Ghorashi, S., ... & Mostafa,
19. S. M. (2023). Quality of Service (QoS) Performance Analysis in a Traffic Engineering Model for Next-Generation Wireless Sensor Networks. Symmetry, 15(2), 513.
20. Khan, A. N., Tariq, M. A., Asim, M., Maamar, Z., & Baker, T. (2021). Congestion avoidance in wireless sensor network using software defined network. Computing, 103, 2573-2596.
21. Majid, M., Habib, S., Javed, A. R., Rizwan, M., Srivastava, G., Gadekallu, T. R., & Lin,
22. J. C. W. (2022). Applications of wireless sensor networks and internet of things frameworks in the industry revolution 4.0: A systematic literature review. Sensors, 22(6),2087.
23. Raymond Mulligan, "Coverage in Wireless Sensor Networks: A Survey," p. 27, 13 April 2010.