

# A Study of Wireless Sensor Networks to Comprehend their Relevance to Different Applications

Jayashree Agarkhed<sup>1</sup>, Patil Yogita Dattatraya<sup>2</sup>, and Siddarama Patil<sup>3</sup>

<sup>1</sup> Computer Science and Engineering Department, Poojya Doddappa Appa College of Engineering, Kalaburagi, India

<sup>2</sup> Computer Science and Engineering Department, Sharnbasva University, Kalaburagi, India

<sup>3</sup> Department of E&CE, Poojya Doddappa Appa College of Engineering, Kalaburagi, India

<https://doi.org/10.26636/jtit.2020.139219>

**Abstract**—Wireless sensor networks (WSNs) have experienced enormous growth, both in terms of the technology used and their practical applications. In order to understand the features of WSNs that make the solution suitable for a specific purpose, one needs to be aware of the theoretical concepts behind and technological aspects of WSNs. In this paper, the significance of WSNs is illustrated, with a particular emphasis placed on their demands and on understanding research-related problems. A review of the literature available is presented as well. Detailed discussions concerning sensor node architecture, different types of sensors used and their relevance for various types of WSNs is presented, highlighting the need to achieve application-specific requirements without degrading service quality. Multipath and cluster-based routing protocols are compared in order to analyze QoS requirements they are capable of satisfying, and their suitability for different application areas is reviewed. This survey highlights the performance of different routing protocols, therefore providing guidelines enabling each of the routing techniques to be used, in an efficient manner, with factors such as specific network structure, protocol operation and routing path construction taken into consideration in order to achieve better performance.

**Keywords**—clustering, energy efficiency, multipath-based routing, wireless sensor network.

## 1. Introduction

WSNs are an evergreen technology due to the fact that they support different types of applications, which makes them perfectly suited for use in such areas as security and surveillance, environmental monitoring, health monitoring, factory process automation, home automation, as well as tracking animals, objects, vehicles, and humans [1], [2]. The sensors used in WSNs are very small and offer limited processing power and computing capabilities. These sensors may collect or process information, and transmit it to the sink node [3].

When sensors are deployed at remote and difficult-to-access locations, wireless communication is used to transfer the

data to a base station (BS). A battery is the primary source of power for a sensor node. Alternatively, power may be harvested using solar panels. Considerable amount of research has been conducted on the design of various data routing mechanisms, with strict WSN resource-related restrictions taken into consideration. The latest advances in the field of micro-electro-mechanical systems (MEMS) and the ever-changing application-related demands require that the manner in which all layers of a WSN protocol stack are designed be modified as well. Quality of service (QoS) demands pose a serious challenge while designing routing mechanisms that boost performance, due to the unique characteristics and specific features of WSNs.

### 1.1. Characteristics of WSNs

The routing protocols of a WSN are unique in order to satisfy the requirements of various applications. These include, for instance:

- limited resource availability (power, storage capacity, computing capacity),
- deployment in a hostile environment causes difficulty with recharging batteries of sensor nodes,
- self-organizing nature of sensor nodes causes frequent topology changes,
- heterogeneous nature of WSNs may cause interoperability problems,
- routing mechanism-based reconfiguration in the case of topology changes due to node failures, link breakups,
- scalability is an issue in massive network deployments,
- processing of unattainable operation is necessary in various application environments.

Common WSN-related research issues focus on ensuring high bandwidths, low energy consumption, QoS provisioning, node mobility, congestion control, congestion detection, congestion mitigation, reliability, end-to-end and hop-by-hop packet recovery, cache ACK/NACK, scalability, synchronization, data cache, data aggregation, computational overhead, availability, data security, and integrity [4], [5]. The provision of QoS support in WSNs while ensuring energy efficiency is an emerging area of research that needs to take into consideration numerous challenges [6].

The following WSN-related challenges have been identified while working on an efficient protocol design [7], [8]:

- **Limited resource constraints.** An efficient routing protocol needs to consider the energy status of the node, available bandwidth, storage, limited buffer size and computing capabilities in order to achieve high data rates with limited transmission power.
- **Heavy node-to-sink traffic.** This demands efficient utilization of available bandwidth and load balancing.
- **Redundant data transmission.** Data redundancy helps achieve reliability but increases power consumption.
- **Network dynamics.** Routing protocols need to periodically route packets which may suffer from a node or a link failure, and must establish links dynamically.
- **Node energy conservation.** Data transmission through the same path, retransmission of lost data and control messages depletes node energy.
- **Transmission power.** A heterogeneous environment with multimedia data demands minimization of transmission power.
- **Scalability.** The network has to attain desired performance levels, even with an increase in network size.
- **Time constraint transmission.** Critical and non-delay tolerant applications demand the transfer of data within a specified deadline.
- **Security.** For secure data transmission, several cryptographic, steganographic and other techniques are used.

Due to the many constraints in the traditional WSNs, new technologies need to be considered to overcome these and many other issues [9] and to offer a better understanding of the underlying sensor network.

The remaining part of the paper is constructed as follows. Section 2 presents details about sensor network architecture. Section 3 details the classification of WSNs based on node deployment type, delivery model, location, type, and nature. Section 4 specifies the applications of WSNs

and in Section 5, routing is discussed. Section 6 describes two broad routing categories and security aspects, while Section 7 presents the conclusions.

## 2. Sensor Network Architecture

WSNs consist of a vast number of sensor nodes that are distributed throughout the areas of interest, as shown in Fig. 1. WSNs comprise lightweight, low powered sensor nodes with the capability of acquiring, computing and communicating data (wirelessly). These sensor nodes communicate with each other and with the destination node that is also referred to as a base station or sink.

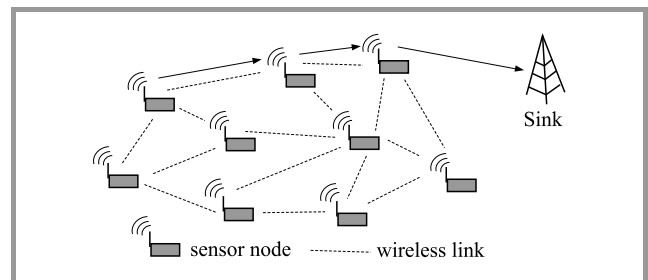


Fig. 1. Structure of WSNs.

Sensor nodes have some computing capability as well. They may be stationary or mobile, homogenous or heterogeneous. Homogenous sensor nodes are characterized by the same capacity in terms of power, computation and communication. Heterogeneous sensor nodes may perform sensing activities and other tasks, such as data relaying.

The basic components of sensor nodes are shown in Fig. 2.

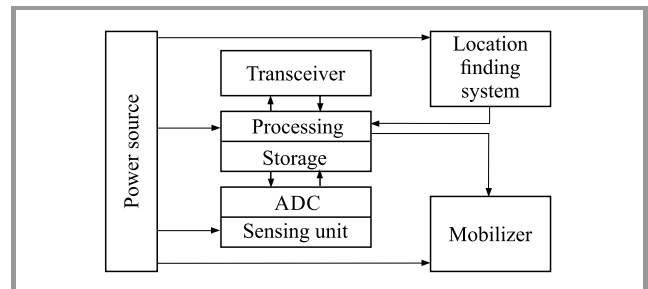


Fig. 2. Basic structure of sensor node.

The battery may be a disposable or a rechargeable power source. Since the nodes are deployed at a remote location, the design must ensure that the network is capable of functioning over long periods of time, with power preserved to extend the network lifetime [3].

The transceiver unit facilitates the radio link with neighboring nodes, or internally, within a subsystem of a nodes. This unit supports several operational states (sleep, idle or active) for efficient resource utilization. The transceiver unit may support different transmission media, such as radio frequency (RF), infrared, and laser [10].

The processing unit is the core element of a node that determines its computational and performance capabilities. It contains a microcontroller, a digital signal processor or field-programmable gate arrays (FPGAs). It performs various functions, such as turning the sensor on, converting data to the digital format, aggregating data, as well as processing data [11].

The sensing unit consists of a sensor and an analog-to-digital converter (ADC). It collects data from the environment. The ADC serves as an interface between the sensor and the processor [12].

The sensors are classified as physical, chemical and biological sensors:

- **Physical sensors** are used for measuring vibration, acceleration, ultra-sound, water level, stress, flex, bend, and strain.
- **Environmental sensors** are used to measure air temperature and humidity, soil humidity, humidity effect on leaves, wind direction and speed, air pressure, etc.
- **Gas sensors** allow to measure e.g. CO, CO<sub>2</sub>, CH<sub>4</sub>, NH<sub>3</sub>, O<sub>2</sub>, NO<sub>2</sub>, SH<sub>2</sub> and pollution levels.
- **Optical sensors** are used to measure sunlight, infrared and ultraviolet radiation. These sensors detect human presence using the IR spectrum. They are also used in agriculture, where sunlight, ultraviolet and radiation sensors measure the amount of energy and sunlight absorbed by plants.
- **Biometric sensors** perform electrocardiograms (ECG) and measure perspiration and pulse to prevent heart attacks.

Data sensed by the sensor node will be collected and routed to a more powerful node called the sink node.

### 3. Classification of WSNs

WSNs are categorized based on deployment type, delivery model, location of deployment, type and nature of node. Two deployment types are distinguished: deterministic and non-deterministic.

Non-deterministic deployment means that nodes are scattered randomly and creates an ad-hoc infrastructure, thus forming an unstructured WSN. Detecting sensor node failures and managing connectivity is difficult in unstructured WSNs. In this scenario, sensor nodes communicate with each other directly establish a link with BS.

Deterministic deployment allows the sensor nodes to be manually placed in a pre-planned manner at specific locations, in order to guarantee the coverage of a specific region and forming a structured WSN. In this scenario, data is routed through predetermined nodes.

Data is transferred using a specific data delivery model that is application dependent and classified as continuous,

query-driven, event-driven or hybrid (Fig. 3). In the continuous data delivery model, each node sends the data periodically. The event-driven model uses triggering based on a specific event determined in the target tracking application. In the query-driven model, data is transmitted in a reply to a query generated by the sink, in environment or habitat monitoring applications. The hybrid model combines the aforementioned features.

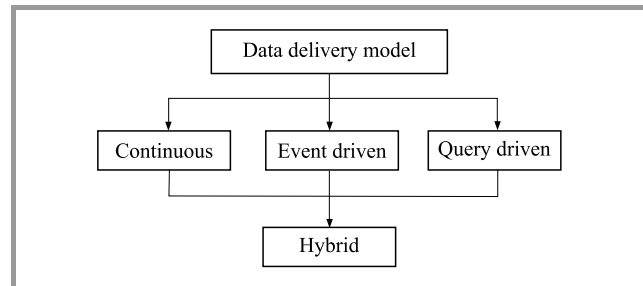


Fig. 3. Data delivery model.

WSNs are classified into different types based on the location of their deployment [2], [13]:

- **Terrestrial.** WSNs of this particular type rely on either ad-hoc or pre-planned deployment. In an ad-hoc deployment, the nodes are randomly dropped into the specific target area. Pre-planned implementation is based on an optimal placement grid;
- **Underground.** The network is formed by sensor nodes placed in mines or below ground to monitor underground conditions. The equipment required here has to support reliable communication through rocks, water, soil, etc.;
- **Mobile.** This network is formed by sensor nodes positioned in vehicles. Long propagation delays, limited bandwidth and signal fading are the most important issues here;
- **Body area.** Networks of this type are formed by the deployment of disposable, inside-the-body or on-the-body, low cost sensor nodes equipped with cameras.

Next, we may classify WSNs based on the type of nodes used.

In a homogenous network, all nodes have an equal capacity in terms of power, communication and computation. A heterogeneous network, in turn, may sense different parameters, such as humidity, temperature and pressure. Its sensors may also detect motion and capture images, videos, etc.

Finally, networks may be of the static variety, with nodes fixed at a predetermined location, or of the mobile variety, using frequent topology changes.

## 4. WSN Applications

WSNs are applied in a wide range of fields. Specific applications may be divided into two broad categories, as shown in Fig. 4 and summarized in Table 1 [14]–[24].

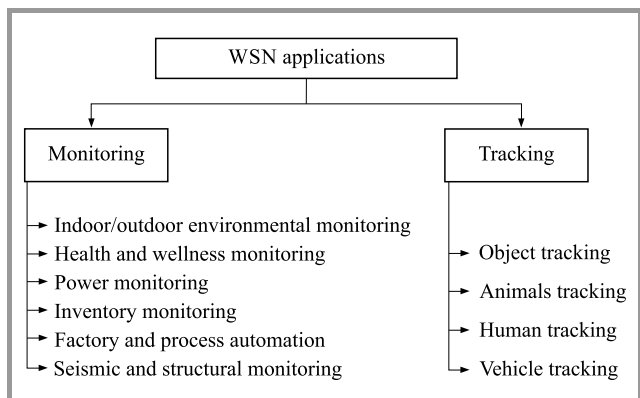


Fig. 4. WSN applications.

The performance of a WSN system may be evaluated by the use of a testbed, with specific performance parameters considered [9]. A WSN testbed is costly, difficult to design and time-consuming [25]. Hence, simulations may be performed using either an emulator or the simulator discussed in [26].

In consideration of the above, the design of a WSN depends, to a significant degree, on its specific application. It should also consider such factors as the environment, design objectives, hardware required, cost and overall system constraints [3], [27]. As WSN applications require the deployment of sensor nodes in a harsh environment, continuous functioning of the nodes is needed even in the event of a network infrastructure failure [4]. This necessitates that the network be designed in a proper manner, from deployment to data routing, with energy conservation being one of the most critical and challenging issues.

## 5. State-of-the-Art Routing

A vast literature survey concerning WSNs helps understand that an energy-efficient routing protocol is desirable in WSNs, as the lifetime of the network depends on the battery life of its sensor nodes. The essential energy conservation technique consists in choosing a proper network topology. Increased reliability [28] of the transmitted information may be achieved by routing it through a flexible path, with the ability to re-establish the route in the event of a node or link failure.

In the flat network topology (Fig. 5), all nodes perform identical functions [29] and communicate directly with the sink node, increasing transmission-related energy consumption and the communication overhead. Flat network topologies include, for instance, sequential assignment routing (SAR) [30], sensor protocols for information via negotiation (SPIN) [31] and greedy perimeter stateless routing

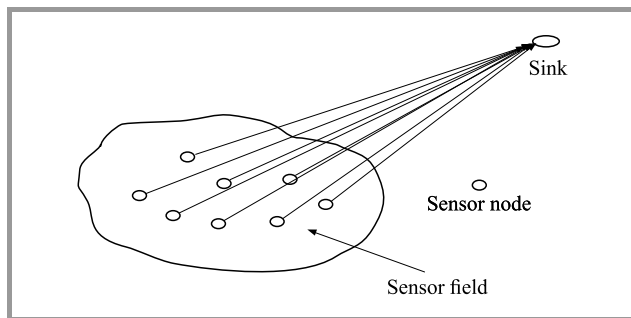


Fig. 5. Scheme of WSN with flat-based routing protocols.

(GPSR) [32]. All of them are based on application-related requirements and rely on star, mesh or tree topologies. Cluster-based routing (Fig. 6) is formed by subdividing a flat network into a set of a small individual clusters. Each cluster selects a node with the maximum energy level as its cluster head (CH), and all remaining nodes are considered to be respective cluster members (CMs). The primary task of the CH is to collect data from CMs within the cluster and to transmit the aggregated data to the next hop neighboring CH, until it reaches the BS [33]. Such an approach allows to save energy, as the CH is the only node that needs to be active all the time and the CMs are only used for sensing and may be periodically turned on and off to save energy. The role of the CH is assumed, alternately, by different CMs to avoid an early shutdown of a single CH due to it being continuously used for transmission purposes. Time-driven CH rotation is simple and offers a fixed cluster setup time. Time-driven CH rotation is a highly efficient solution.

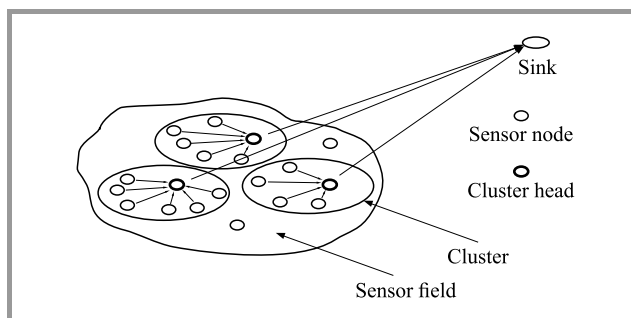


Fig. 6. An example of a WSN with cluster-based routing.

Reliability of information transmission is improved by multipath routing. This technique is used for balancing the load to avoid congestion, and to reduce the repeated route inquiries. It offers the lowest overall routing overhead and provides enhanced robustness against failure of a node, to achieve reliability and energy efficiency [34]. A lot of routing protocols are cluster-based or multipath-based in order to meet the service quality requirements. Designing a routing protocol in a manner that satisfies the requirements of a given application, simultaneously taking into consideration energy conservation and service quality, is a challenging task.

Table 1  
WSN applications

Application area	Monitoring	Tracking
Military	Friendly troop status [19], vehicles and their movements	Availability of equipment on the battle-field [20], [21]
Industrial control	Monitoring applications follows the data-driven model to monitor material flows, quality, and safety in order to reduce human-made errors and the cost of manufacturing [22]	Changes in plant security, machine processes, or mishandling by operator [23]
Surveillance	Used to monitor airports, public parks, and railway stations [24]	Tracking of intruders
Environmental	<ul style="list-style-type: none"> <li>• detect volcano eruptions [14],</li> <li>• detect forest fires by collaboration of solar-powered sensor nodes [15],</li> <li>• estimate floods by monitoring water level in rivers [16]</li> </ul>	<ul style="list-style-type: none"> <li>• identifying air pollution levels caused by increasing traffic volumes,</li> <li>• movement of birds, animals and insects</li> </ul>
Agriculture	Monitor water, humidity and temperature levels in order to achieve good quality farming produce [17]	Tracking the movement of animals
Health	Sensors monitor blood oxygen level, blood pressure, body temperature and the glucose level [18]	Assisting doctors in emergencies

The main objective of routing in WSNs is to conserve energy. Therefore, energy-efficient routing protocols are desired in WSNs, as the lifetime of the network relies on the battery life of each node. The well-known underlying protocol, referred to as low energy adaptive clustering hierarchy (LEACH) [35], allows CHs to communicate with sink directly. A cluster formed by a set of sensor nodes is based on the signal strength of the nodes and uses CH as a router-to-sink, with the constraint that a maximum of 5% of nodes may serve as CHs of a given network. LEACH offers lower energy consumption than direct communication, as it establishes a distributed system without any global knowledge. LEACH is not relevant for large size networks where selecting the CH is difficult. Its specific variant, LEACH-F, has a fixed number of clusters and alternately assigns the role of the CH to different nodes within the clusters. However, it does not support energy saving, meaning that it is not suitable for mobile applications.

An increase in the distance between the CH and the sink, in turn, increases communication cost and shortens network lifetime. Communication distance between the nodes is minimized by dividing the network into an optimal number of clusters, as specified in the optimal number of clusters algorithm (ONCA) [36]. Power-efficient gathering in sensor information systems (PEGASIS) is a technique that uses multi-hop routing by forming a chain of sensor nodes and selecting only one node to transmit to the sink, instead of multiple nodes, as in LEACH. It outperforms LEACH by aggregating data from the nodes. One drawback of PEGASIS is the increased delay caused by the chain formation process. This challenge is overcome by the hierarchical variety of PEGASIS. This version uses simultaneous trans-

mission of messages, which may lead to collisions that are avoided by the use of signal coding.

Chain-based CDMA-capable protocols support parallel transmission of data to minimize delay, but need dynamic topology adjustments to conserve energy [37]. A threshold-sensitive energy-efficient sensor network (TEEN) is an example of a hierarchical protocol that responds to a sudden change in the sensed attributes, such as temperature. It is useful in time-critical applications relying on networks operating in the reactive mode. The closest nodes from a given cluster communicate with each other and the process is repeated from the second level, until the base station is reached. The protocol uses either a soft or a hard threshold to trigger the sensor node to switch its transmitter on. Data transmission is controlled by varying these thresholds. TEEN is not useful for periodic reporting applications [38]. The adaptive threshold-sensitive energy-efficient sensor network protocol (APTEEN) captures periodic data and responds to time-critical events. The performance of TEEN is better than that of LEACH and APTEEN [39]. The hybrid energy-efficient distributed protocol (HEED) is useful in ad-hoc sensor networks. HEED assumes that all nodes have the same energy initially. Then, all nodes appoint themselves cluster heads based on their remaining power and based on the degree of a given node relied upon for cluster election. It is a cluster-based multi-hop routing protocol. HEED is characterized by good load balancing and uniform CH distribution. HEED does not offer balanced energy consumption due to the fact that a higher number of CHs is generated [40].

A useful way to save energy is to schedule data transmission processes that reduce the amount of sensing power and

preserve the quality of sensed data. One such algorithm, known as CIES, shares sensing error information and controls sensing errors through neighbor node coordination, therefore achieving high data accuracy and throughput [41]. It uses clustering and groups the sensor nodes into different clusters in order to meet scalability requirements, to balance the load in high-traffic networks, to minimize the size of the routing table at each node, and to efficiently utilize the communication bandwidth by relying on inter-cluster interaction with the CH [42].

In order to conserve energy, CH may schedule the cluster's activity by toggling between the node's active and sleep modes [43], [44]. The author in [45] presented a technique to optimize sensor node energy utilization by clustering, using a genetic algorithm. The paper [46] considered each sensor node's residual energy, the amount of energy used in sensing, the node's distance from the base station, and the number of neighboring nodes – all in order to identify an optimized, dynamic network structure.

Some of the routing protocols referred to above use single path routing, where each sensor node routes its data through the shortest path to the sink. Single-path routing may cause the routing path to break up due to the failure of the nodes and demands that a new route be established. It also increases energy consumption and the probability of a failure of a node which results in the packets being dropped and cause increased delay in the transmission to the sink. In such a case, it is desirable to avoid node failures by choosing an alternative routing path, thus forming multipath routing that increases the number of potential routes, guaranteeing robustness of transmission and increased throughput.

Single path routing does not offer a sufficient bandwidth for data transmission, as WSNs have a limited bandwidth capacity. Multiple routing paths facilitate simultaneous communication, and the aggregated bandwidth of the multiple routing paths is capable of satisfying significant bandwidth demand of any particular application. An increase in bandwidth overcomes delay and guarantees load-balanced energy utilization, along with increased network lifetime [47], [48]. Service differentiation deployed to differentiate and prioritize traffic flow is another mechanism relied upon to meet application-related requirements.

## 6. Classification of Routing Protocols

Based on extensive work on routing techniques in WSNs, routing protocols may be classified into the following broad categories: flat, hierarchical, location-based, multipath based, query-based, negotiation-based, QoS-based, coherence-based, proactive, reactive and hybrid.

The classification of routing protocols distinguishes also data-centric based, location-based, cluster-based, node mobility-based, multipath-based and service quality-based varieties [4]. The best routing protocol must offer the maximum residual energy of nodes, negligible packet drop rates, lower energy consumption, lower delays and load fairness.

### 6.1. Multipath Routing Protocols

One of the most significant advantages of multipath routing is that it minimizes route updates, balances the traffic and reduces the energy consumption of each sensor node. The comparison of multipath routing protocols presented in Table 2 highlights the strong points of the solution. In [49], the author proposed a maximally radio-disjoint multipath routing (MR2) that uses an incremental approach which helps choose alternate paths but leads to higher delays with increased overhead compared to hop count multipath routing (HCMR). HCMR is characterized by higher energy usage compared to the energy efficient interference-aware multipath routing (EEIAMR) protocol. It determines short alternate paths to minimize delay and energy consumption by relying on the large network size. With an increase in node count, MR2 and EEIAMR generate higher overhead compared to HCMR. Sensor protocol for information via negotiation (SPIN) provides robustness in the event of path failures, by relying on topology changes [44]. Reliable, real-time routing protocol (3R) considers both multipath and time constraints. This protocol [45] uses packet reception rate estimations to calculate the necessary number of forwarding paths. The disjoint path routing protocol [46] finds the first k-shortest route to the sink and sends periodic messages to keep these paths alive. Performance improvements and fault-tolerance are achieved by equal division of load among the nodes.

Table 2  
Multipath-based routing protocols

Protocol	Number of paths built	Interference awareness	Mean delay	Energy consumption	Over head
MR2 [49]	6–8	Yes	Higher	Lower	Higher
HCMR [9]	2–4	No	Lower	Higher	Lowest
EEIAMR [9]	1	Yes	Lowest	Lowest	Lower
SPIN [44]	1 or more	No	Higher	Lower	Lowest
3R [45]	More	No	Lowest	Higher	Lower
Disjoint path [46]	K	No	Lower	Higher	Higher

### 6.2. Cluster-Based Routing Protocol

In WSNs, the nodes are grouped into a cluster to enable load balancing, network scalability, to minimize the routing table size at the level of an individual node, to spare the communication bandwidth by inter-cluster interaction with CHs, and to ensure a stabilized network topology [45]–[48]. For energy conservation purposes, activities within the cluster are scheduled by the CH which toggles between sleep and active state of the nodes. Another advantage of clustering consists in the fact that CH aggregates data from all sensors in its respective cluster to reduce the count of packets to be sent [49]. Advantages of the cluster-based routing protocols are presented in Tables 3 and 4.

Table 3  
Cluster-based routing protocols with varying packet delivery ratio and end-to-end delay

Protocol	Feature supported	Delivery ratio	End-to-end delay
LEACH [11]	Minimizes energy consumption but incurs more delay by using large buffer size	Medium	Higher
CBEEQR [10]	Uses large buffer size, leading to lower packet drop rates	Increased	Lower
ONCA [12]	Increases network lifetime by dividing the network into an optimal number of clusters	Higher	Lower
TEEN [38]	Responds to a sudden change in a sensed attribute, based on a hard or soft threshold. Supports event-driven applications and is not suitable for periodic applications	High	Lower
APTEEN [39]	Captures data on a periodic basis and reacts to the time-critical events. Supports three types of queries historical, one-time and persistent	High	Lower

Table 4  
Cluster-based routing protocols with varying energy consumption

Protocol	Time [s]	Number of nodes alive	Routing type	Energy consumption
LEACH [5]	800	0	Proactive	High
	500	20		
Leach-C [36]	800	0	Proactive	Medium
	500	20		
TEEN with a hard threshold [37]	800	2	Proactive	Lower
	500	95		
TEEN with a soft threshold [38]	800	95	Proactive	Lowest
	500	100		

The majority of location-based protocols are not very energy efficient or reliable and sacrifice QoS requirements, which leads to transmission delays. They are not applied as frequently in healthcare, but may be useful for environmental monitoring or target tracking, provided that newly designed protocols place a greater emphasis on energy efficiency and reliability-related aspects. Cluster-based and mobility-based routing protocols are best suited for healthcare and military applications which require reliable transfers and a continuously operational environment. This requirement is met by mobile devices with batteries whose power capacity is higher compared to the conventional sensors.

Multipath based protocols are suited for military and medical applications, since they ensure high reliable data delivery rates. Appropriate cluster design and the selection of CH minimize energy consumption while communicating and aggregating messages and are highly significant design features. Data transmission is performed to conserve energy and achieve QoS with an efficient routing technique, in order to ensure efficient use of the sensor.

Application-related QoS requirements may be satisfied by assigning different priority levels to different types of applications, users, frames, data flows and packets through resource sharing. High quality of service is ensured by such parameters as delay, bandwidth, and packet loss [50]–[59].

Service quality takes into consideration hard and soft QoS factors. Routing protocols with hard QoS must meet strict requirements concerning delay, packet loss, and bandwidth. On the other hand, routing protocols with soft QoS may violate these provisions. Both hard and soft QoS are guaranteed through service differentiation. The two service differentiation models are the integrated service model (IntServ) [60] and the differentiated service model (DiffServ) [61]. They are presented, along with their key features, in Table 5.

Table 5  
Service differentiation model

Integrated service model	Differentiated service model
Service quality maintained on the per-flow basis	Service quality maintained on the per packet-basis
The approach relied upon reservation-based and is either data-centric or host-centric	The method used is reservation-less and relies on the multi-hop strategy to conserve energy
Cannot achieve guaranteed service quality due to the varying capacity of the channel, needs to maintain sensor state on the per-flow basis, scalability issues	Higher memory requirement due to the fact that each node acts as a source or intermediate node

The security of data sensed by a particular sensor is an issue that has been continuously gaining in importance. Security algorithms must not boost memory requirements and must not lead to increased power consumption during processing and transmission, as the sensor node suffers from resource constraints. The various security requirements include confidentiality, authentication, integrity, and availability [62]. The various cluster-based WSN protocols that apply different security methods to prevent different types of attacks, are presented in Table 6 and Table 7.

Advancements in sensor network technologies are an enabler of the Internet of Things (IoT) – a technology that shapes the world anew by offering the ability to measure, infer and understanding environmental indicators. Recent developments and technological improvements have increased the efficiency and lowered the cost of devices, enabling

Table 6  
Cluster-based security protocols

Protocol	Security method	Type of security achieved	Computation overhead	Communication overhead
CHiMAC [63]	Message divided into two blocks and encrypted. Each block added to message with source, destination, and cluster ID	Authentication and integrity	High due to encryption and decryption	Lower due to clustering
Sybil attack model [64]	A malicious node uses all of its Sybil identities to join each cluster. RSSI and positioning using three points to defend against the novel attack has been considered	Detects 99.8% of Sybil nodes with 0.08% false detection rate	High	Lower
HMAC [65]	Hash-based message authentication code (HMAC) authentication followed by pair-wise key establishment used during data aggregation for two different types of node set up processes. It uses a pair-wise key generation process in which each node randomly generates a unique key with combining private and public key components	Authentication	Lower	Lower
KCLP [66]	To protect the location of the real source and the sink, a fake source and a fake sink have been used along with k-means clustering to elongate the routing path and to boost safety. The use of different routing patterns of the fake and the real packet has reduced network delay	Jamming attack, node collaboration	High	High
DH method [67]	Security guaranteed at each hop by using a binary hop count and end-to-end node authentication relying on Huffman coding. Dijkstra's algorithm finds the nodes with maximum energy level and optimum distance path	Message and node authentication. Integrity achieved by encryption	Medium	Lower

Table 7  
Different types of attacks

Type of attack	Classification into specific attack type	Description	Security methods applied
Common attack	Eavesdropping	Attacker retrieve information from transmitted data	Encryption technique and time stamp
	Message modification	Packet data modified while data in transmission	Provide authentication and identification of traffic, pushback
	Message replay	Adversary retransmit the contents and packet	
Denial of service attack [63]	Node collaboration	Some nodes act as maliciously and prevent message transmission to other nodes in the network	Use multiple disjoint routing paths and diversity coding
	Jamming attack	An adversary jams communication channel	
	Exhaustion power	Repeated packet request lead to depletion of battery power	
Node compromise attack	Node compromise	The attacker gain control of sensor node and launch attacks from compromised nodes	Trusted key server checks for node identification
Impersonation attack		Malicious node impersonates a legitimate node and uses its identity to mount an active attack such as Sybil [64] or node replication	BS or key server authenticates every node on the network
Protocol specific attack	Spoofed routing	Adversary spoof routing information by corrupting routing table content	Provide access to the authenticated node
	Selective forwarding	Selectively forwarding of packets that traverse a malicious node depending on some criteria	Use multiple disjoint routing paths
	Wormhole attack	Creation of wormhole that replays information from one location to other location	Each message is forwarded individually, choosing the next-hop node to be the neighbor closest to the ultimate destination
	Hello flood attack	Hello flood attack create false control packets	Check bi-directionality of the local links



their large-scale use in remote sensing applications. Our smartphones offer a diverse range of sensors as well and, consequently, they may operate a variety of mobile apps relevant for the IoT [68]. The most challenging task is to process huge amounts of data generated by sensors, taking into account security-related issues, energy and network limitations, as well as various types of uncertainties.

## 7. Conclusion

The architecture constrained sensor node for use in a different application domain demand an energy efficient routing protocol without losing service quality. From the compressive study of routing protocols, most of the location-based protocols are not much energy efficient, reliable, and sacrifice QoS requirements leading to a delay in transmission. Thus they are not appropriate for healthcare applications but can be useful for environmental monitoring or target tracking application if new protocols designed considering energy efficiency and reliability issues. Cluster-based and mobility-based routing protocols are best for healthcare and military applications. These applications require a reliable and continuously functioning environment that can be achieved by a mobile device equipped with a higher amount of battery power compared to conventional sensors like biosensors. Multipath-based protocols are suited for military and medical applications since they ensure reliable data delivery. Appropriate design of cluster and selection of CH minimize energy consumption during message communication and aggregation, which is one of the most significant design issues. To develop an efficient protocol, one must combine the best features of protocols of different routing categories.

## References

- [1] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey", *Computer Netw.*, vol. 52, no. 12, pp. 2292–2330, 2008 (DOI: 10.1016/j.comnet.2008.04.002).
- [2] R. Sachdeva and A. Singla, "Review on security issues and attacks in wireless sensor networks", *Int. J. of Adv. Res. in Comp. Sci. and Softw. Engin.*, vol. 3, no. 4, 2013 [Online]. Available: [http://ijarcsse.com/Before\\_August\\_2017/docs/papers/Volume\\_3/4\\_April2013/V3I3-0297.pdf](http://ijarcsse.com/Before_August_2017/docs/papers/Volume_3/4_April2013/V3I3-0297.pdf)
- [3] P. Y. Dattatraya and J. Agarkhed, "A review on various issues and applications in wireless sensor networks", *Int. J. of Sci. and Res.*, vol. 4, no. 11, pp. 2518–2522, 2015 (DOI:10.21275/v4i11.nov151773).
- [4] K. Akkaya and M. Younis, "A survey on routing protocols for wireless sensor networks", *Ad Hoc Netw.*, vol. 3, no. 3, pp. 325–349, 2005 (DOI: 10.1016/j.adhoc.2003.09.010).
- [5] P. Sharma, "A review of attacks on wireless sensor networks", *J. of Inform. Syst. and Commun.*, vol. 3, no. 1, pp. 251–255, 2012 [Online]. Available: [http://www.bioinfopublication.org/files/articles/3\\_1\\_53\\_IJSC.pdf](http://www.bioinfopublication.org/files/articles/3_1_53_IJSC.pdf)
- [6] D. Chen and P. K. Varshney, "QoS support in wireless sensor networks: A Survey", in *Proc. of the Int. Conf. on Wirel. Sensor ICWN'04*, Las Vegas, Nevada, USA, 2004, vol. 1, pp. 227–233 [Online]. Available: <http://www.cs.binghamton.edu/~kang/teaching/cs580s/qos-survey2.pdf>
- [7] R. Iyer and L. Kleinrock, "QoS control for sensor networks", in *Proc. IEEE Int. Conf. on Commun. ICC'03*, Anchorage, AK, USA, 2003, vol. 1, pp. 517–521 (DOI: 10.1109/ICC.2003.1204230).
- [8] D. Wei, S. Kaplan, and H. A. Chan, "Energy efficient clustering algorithms for wireless sensor networks", in *Proc. of the IEEE Int. Conf. on Commun. Worksh. ICC Workshops-2008*, Beijing, China, 2008, pp. 236–240 (DOI: 10.1109/ICCW.2008.50).
- [9] J. Agarkhed, P. Y. Dattatraya, and S. R. Patil, "Performance evaluation of QoS-aware routing protocols in wireless sensor networks", in *Proceedings of the First International Conference on Computational Intelligence and Informatics ICCII 2016*, S. C. Satapathy *et al.*, Eds. *AISC*, vol. 507, pp. 559–569. Springer, 2017 (DOI: 10.1007/978-981-10-2471-9\_54).
- [10] A. Jangra, "Wireless sensor network (WSN): Architectural design issues and challenges", *Int. J. on Comp. Sci. and Engin. (IJCSE)*, vol. 2, no. 9, pp. 3089–3094, 2010 [Online]. Available: <http://www.enggjournals.com/ijcse/doc/IJCSE10-02-09-076.pdf>
- [11] I. F. Akyildiz and M. C. Vuran, *Wireless Sensor Networks*. Wiley, 2010 (ISBN: 9780470036013).
- [12] R. Hawi, "Wireless sensor networks – sensor node architecture and design challenges", *Int. J. of Adv. Res. in Comp. Sci.*, vol. 5, no. 1, pp. 47–53, 2014 [Online]. Available: <http://www.ijarcs.info/index.php/Ijarcs/article/view/1980>
- [13] M. Jena and J. D. Abraham, "QoS provisioning issues in wireless multimedia sensor networks", 2009 [Online]. Available: <http://csjournals.com/IJITKM/Special/14.%20QoS%20Provisioning%20issues.pdf>
- [14] G. Werner-Allen *et al.*, "Deploying a wireless sensor network on an active volcano", *IEEE Internet Comput.*, vol. 10, no. 2, pp. 18–25, 2006 (DOI: 10.1109/MIC.2006.26).
- [15] J. Zhang *et al.*, "Forest fire detection system based on wireless sensor network", in *Proc. 4th IEEE Conf. on Indust. Electron. and Appl.*, Xi'an, China, 2009, pp. 520–523 (DOI: 10.1109/ICIEA.2009.5138260).
- [16] M. Pavani and P. T. Rao, "Real time pollution monitoring using Wireless Sensor Networks", in *Proc. of IEEE 7th Ann. Inform. Technol., Electron. and Mob. Commun. Conf. IEMCON 2016*, Vancouver, BC, Canada, 2016 (DOI: 10.1109/IEMCON.2016.7746315).
- [17] G. R. Mendez and S. C. Mukhopadhyay, "A Wi-Fi based smart wireless sensor network for an agricultural environment", in *Proc. of Fifth Int. Conf. on Sens. Technol.*, Palmerston North, New Zealand, 2011, pp. 405–410 (DOI: 10.1109/ICSensT.2011.6137009).
- [18] M. U. H. Al Rasyid, F. A. Saputra, and A. Christian, "Implementation of blood glucose levels monitoring system based on wireless body area network", in *Proc. IEEE Int. Conf. on Consum. Electron.-Taiwan ICCE-TW 2016*, Nantou, Taiwan, 2016 (DOI: 10.1109/ICCE-TW.2016.7521005).
- [19] D. Thomas, R. Shankaran, M. Orgun, M. Hitchens, and W. Ni, "Energy-efficient military surveillance: coverage meets connectivity", *IEEE Sensors J.*, vol. 19, no. 10, pp. 3902–3911, 2019 (DOI: 10.1109/JSEN.2019.2894899).
- [20] M. Rath, B. Pati, and B. K. Pattanayak, "Relevance of soft computing techniques in the significant management of wireless sensor networks", in *Soft Computing in Wireless Sensor Networks*, H. T. T. Binh and N. Dey, Eds. Chapman and Hall/CRC, 2018, pp. 75–94 (ISBN: 0815395302).
- [21] K. Ghosh, S. Neogy, P. K. Das, and M. Mehta, "Intrusion detection at international borders and large military barracks with multi-sink wireless sensor networks: An energy efficient solution", *Wirel. Pers. Commun.*, vol. 98, no. 1, pp. 1083–1101, 2018 (DOI: 10.1007/s11277-017-4909-5).
- [22] M. Faheem *et al.*, "Bio-inspired routing protocol for WSN-based smart grid applications in the context of Industry 4.0", *Trans. on Emerg. Telecommun. Technol.*, vol. 30, no. 1, 2018 (DOI: 10.1002/ett.3503).
- [23] J. Aponte-Luis *et al.*, "An efficient wireless sensor network for industrial monitoring and control", *Sensors*, vol. 18, no. 1, 182, 2018 (DOI: 10.3390/s18010182).
- [24] Z. Zhang, A. Mehmood, L. Shu, Z. Huo, Y. Zhang, M. Mukherjee, "A survey on fault diagnosis in wireless sensor networks", *IEEE Access*, vol. 6, pp. 11349–11364, 2018 (DOI: 10.1109/ACCESS.2018.2794519).


- [25] J. Polastre, R. Szewczyk, A. Mainwaring, D. Culler, and J. Anderson, "Analysis of wireless sensor networks for habitat monitoring", in *Wireless Sensor Networks*, C. S. Raghavendra, K. M. Sivalingham, and T. Znati, Eds. Boston: Springer, 2004, pp. 399–423 (ISBN: 9780387352695).
- [26] P. Y. Dattatraya and J. Agarkhed, "Simulation an art of performance evaluation in wireless sensor networks", in *Proc. Int. Conf. on Circ., Power and Comput. Technol. ICCPCT 2016*, Nagercoil, India, 2016 (DOI: 10.1109/ICCPCT.2016.7530235).
- [27] J. Agarkhed, B. S. Biradar, and V. D. Mytri, "Energy efficient QoS routing in multi-sink wireless multimedia sensor networks", *Int. J. of Comp. Sci. and Netw. Secur. (IJCSNS)*, vol. 12, no. 5, pp. 25–31, 2012 [Online]. Available: [http://paper.ijcsns.org/07\\_book/201205/20120505.pdf](http://paper.ijcsns.org/07_book/201205/20120505.pdf)
- [28] J. Agrakhed, G. S. Biradar, and V. M. Principal, "Energy efficient interference aware multipath routing protocol in WMSN", in *Proc. 2011 Ann. IEEE India Conf.*, Hyderabad, India, 2011 (DOI: 10.1109/INDCON.2011.6139615).
- [29] S. Randhawa and A. K. Verma, "Comparative analysis of flat routing protocols in wireless sensor networks: Which one is better?", in *Proc. 2017 Int. Conf. on Intell. Comput. and Control I2C2*, Coimbatore, India, 2017 (DOI: 10.1109/I2C2.2017.8321945).
- [30] J. N. Al-Karaki and A. E. Kamal, "Routing techniques in wireless sensor networks: a survey", *IEEE Wirel. Commun.*, vol. 11, no. 6, pp. 6–28, 2004 (DOI: 10.1109/MWC.2004.1368893).
- [31] L. Jing, F. Liu, and Y. Li, "Energy saving routing algorithm based on SPIN protocol in WSN", in *Proc. of Int. Conf. on Image Anal. and Sig. Process.*, Hubei, China, 2011, pp. 416–419 (DOI: 10.1109/IASP.2011.6109074).
- [32] B. Karp and H. T. Kung, "GPSR: Greedy perimeter stateless routing for wireless networks", in *Proc. of the 6th Ann. Int. Conf. on Mob. Comput. and Netw. MobiCom'00*, Boston, MA, USA, 2000, pp. 243–254 (DOI: 10.1145/345910.345953).
- [33] J. Agarkhed and Y. D. Patil, "Energy efficient service differentiated QoS aware routing in cluster-based wireless sensor network", *Int. J. of Hybrid Intell.*, vol. 1, no. 1, pp. 79–95, 2019 (DOI: 10.1504/IJHI.2019.099673).
- [34] Y. H. Robinson, E. G. Julie, and R. Kumar, "Probability-based cluster head selection and fuzzy multipath routing for prolonging lifetime of wireless sensor networks", *Peer-to-Peer Network. and Appl.*, vol. 12, pp. 1061–1075, 2019 (DOI: 10.1007/s12083-019-00758-8).
- [35] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks", *IEEE Trans. on Wirel. Commun.*, vol. 1, no. 4, pp. 660–670, 2002 (DOI: 10.1109/TWC.2002.804190).
- [36] H. A. Hussein and R. L. Johnston, "The DFT-genetic algorithm approach for global optimization of subnanometer bimetallic clusters", in *Frontiers of Nanoscience*, S. T. Bromley and S. M. Woodley, Eds. Elsevier, 2019, vol. 12, pp. 145–169, 2019 (DOI: 10.1016/B978-0-08-102232-0.00004-X).
- [37] S. Lindsey and C. S. Raghavendra, "PEGASIS: Power-efficient gathering in sensor information systems", in *Proc. of the IEEE Aerospace Conf.*, Big Sky, MT, USA, 2002, vol. 3, pp. 1125–1130 (DOI: 10.1109/AERO.2002.1035242).
- [38] A. Manjeshwar and D. P. Agrawal, "TEEN: A routing protocol for enhanced efficiency in wireless sensor networks", in *Proc. of the 15th Int. Paralle. and Distrib. Process. Symp. IPDPS 2001*, San Francisco, CA, USA, 2001, vol. 1, pp. 2000–2015 (DOI: 10.1109/IPDPS.2001.925197).
- [39] A. Manjeshwar and D. P. Agrawal, "APTEEN: A hybrid protocol for efficient routing and comprehensive information retrieval in wireless sensor networks", in *Proc. of the 16th Int. Paralle. and Distrib. Process. Symp. IPDPS 2002*, Ft. Lauderdale, FL, USA, 2002 (DOI: 10.1109/IPDPS.2002.1016600).
- [40] O. Younis and S. Fahmy, "Distributed clustering in ad-hoc sensor networks: A hybrid, energy-efficient approach", in *Proc. of 23rd Ann. Joint Conf. of the IEEE Comp. and Commun. Soc. INFOCOM 2004*, Hong Kong, China, 2004 (DOI: 10.1109/INFCOM.2004.1354534).
- [41] Q. Zhang *et al.*, "Collaborative scheduling in dynamic environments using error inference", *IEEE Trans. on Paralle. and Distrib. Syst.*, vol. 25, no. 3, pp. 591–601 (DOI: 10.1109/TPDS.2013.28).
- [42] M. Younis, M. Youssef, and K. Arisha, "Energy-aware routing in cluster-based sensor networks", in *Proc. of the 10th IEEE Int. Symp. on Model., Anal. and Simul. of Comp. and Telecommun. Syst.*, Fort Worth, TX, USA, 2002, pp. 129–136 (DOI: 10.1109/MASCOT.2002.1167069).
- [43] M. Adamou, I. Lee, and I. Shin, "An energy efficient real-time medium access control protocol for wireless ad-hoc networks", Report-University of York Department of Computer Science YCS, University of York, London, 2001.
- [44] T. Wu and S. Biswas, "A self-reorganizing slot allocation protocol for multi-cluster sensor networks", in *Proc. of the 4th Int. Symp. on Inform. Process. in Sensor Netw. IPSN 2005*, Boise, ID, USA, 2005 (DOI: 10.1109/IPSNS.2005.1440940).
- [45] M. Elhoseny, K. Elleithy, H. Elminir, X. Yuan, and A. Riad, "Dynamic clustering of heterogeneous wireless sensor networks using a genetic algorithm, towards balancing energy exhaustion", *Int. J. of Scient. Engin. Res.*, vol. 6, no. 8, pp. 1243–1252, 2015 [Online]. Available: <https://www.ijser.org/researchpaper/Dynamic-Clustering-of-Heterogeneous-Wireless-Sensor-Networks-using-a-Genetic-Algorithm-Towards-Balancing-Energy-Exhaustion.pdf>
- [46] X. Yuan, M. Elhoseny, H. K. El-Minir, and A. M. Riad, "A genetic algorithm-based, dynamic clustering method towards improved WSN longevity", *J. of Netw. and Syst. Manag.*, vol. 25, no. 1, pp. 21–46, 2017 (DOI: 10.1007/s10922-016-9379-7).
- [47] J. Agarkhed, G. S. Biradar, and V. D. Mytri, "Energy efficient QoS routing in multi-sink wireless multimedia sensor networks", *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 12, no. 5, pp. 25–31, 2012 [Online]. Available: [http://paper.ijcsns.org/07\\_book/201205/20120505.pdf](http://paper.ijcsns.org/07_book/201205/20120505.pdf)
- [48] J. Agarkhed, G. S. Biradar, and V. D. Mytri, "Adaptive multi constraint multipath routing protocol in wireless multimedia sensor network", in *Proc. of the Int. Conf. on Comput. Sci.*, Phagwara, India, 2012, pp. 326–331 (DOI: 10.1109/ICCS.2012.9).
- [49] C. B. Mudgule, U. Nagaraj, and P. D. Ganjewar, "Data compression in wireless sensor network: a survey", *Int. J. of Innov. Res. in Comp. and Commun. Engin.*, vol. 2, no. 11, pp. 6621–6632, 2014 [Online]. Available: [http://www.ijrcce.com/upload/2014/november/60\\_Data.pdf](http://www.ijrcce.com/upload/2014/november/60_Data.pdf)
- [50] D. Clark, R. Braden, and S. Shenker, "Integrated services in the internet architecture: an overview", RFC 1633, IETF, 1994 (DOI: 10.17487/RFC1633) [Online]. Available: <https://www.rfc-editor.org/info/rfc1633>
- [51] K. S. Kwak, S. Ullah, and N. Ullah, "An overview of IEEE 802.15.6 standard", in *Proc. of the 3rd Int. Symp. on Appl. Sci. in Biomed. and Commun. Technol. ISABEL 2010*, Rome, Italy, 2010 (DOI: 10.1109/ISABEL.2010.5702867).
- [52] G. Jolly and M. Younis, "An energy-efficient, scalable and collision-free MAC layer protocol for wireless sensor networks", *Wirel. Commun. and Mob. Comput.*, vol. 5, no. 3, pp. 285–304, 2005 (DOI: 10.1002/wcm.222).
- [53] A. Shehab, M. Elhoseny, and A. E. Hassanien, "An efficient scheme for video delivery in wireless networks", in *Quantum Computing: An Environment for Intelligent Large Scale Real Application*, A. E. Hassanien, M. Elhoseny, and J. Kacprzyk, Eds. SBD, vol. 33, pp. 207–225. Springer, 2017 (DOI: 10.1007/978-3-319-63639-9\_9).
- [54] G. Ottman, A. Bhatt, H. Hofmann, and G. Lesieutre, "Adaptive piezoelectric energy harvesting circuit for wireless, remote power supply", *IEEE Trans. on Power Electron.*, vol. 17, no. 5, pp. 669–676, 2002 (DOI: 10.1109/TPEL.2002.802194).
- [55] S. Li, J. Yuan, and H. Lipson, "Ambient wind energy harvesting using cross-flow fluttering", *J. of Appl. Phys.*, vol. 109, no. 2, 2011 (DOI: 10.1063/1.3525045).
- [56] A. Sarkar and T. S. Murugan, "Routing protocols for wireless sensor networks: What the literature says?", *Alexandria Engin. J.*, vol. 55, no. 4, pp. 3173–3183, 2016 (DOI: 10.1016/j.aej.2016.08.003).

- [57] A. Ahmed, K. A. Bakar, M. I. Channa, K. Haseeb, and A. W. Khan, "A trust aware routing protocol for energy constrained wireless sensor network", *Telecommun. Syst.*, vol. 61, no. 1, pp. 123–140, 2016 (DOI: 10.1007/s11235-015-0068-8).
- [58] F. T. Zuhra, K. A. Bakar, A., Ahmed, and M. A. Tunio, "Routing protocols in wireless body sensor networks: A comprehensive survey", *J. of Netw. and Comp. Appl.*, vol. 99, pp. 73–97, 2017 (DOI: 10.1016/j.jnca.2017.10.002).
- [59] W. Rehan, S. Fischer, M. Rehan, and M. H. Rehmani, "A comprehensive survey on multichannel routing in wireless sensor networks", *J. of Netw. and Comp. Appl.*, vol. 95, pp. 1–25, 2017 (DOI: 10.1016/j.jnca.2017.07.006).
- [60] R. Braden, D. Clark, and S. Shenker, RFC 1633: "Integrated services in the Internet architecture: an overview, June 1994. Status: Informational", IETF, 1994 [Online]. Available: <https://tools.ietf.org/html/rfc1633>
- [61] E. Davies, M. A. Carlson, W. Weiss, D. Black, S. Blake, and Z. Wang, "An architecture for differentiated services", RFC 2475, IETF, 1998 (DOI: 10.17487/RFC2475) [Online]. Available: <https://tools.ietf.org/html/rfc2475>
- [62] S. Prasanna and S. Rao, "An overview of wireless sensor networks applications and security", *Int. J. of Soft Comput. and Engin. (IJSC)*, vol. 2, no. 2, pp. 538–540, 2012 [Online]. Available: <http://www.ijscce.org/wp-content/uploads/papers/v2i2/B0648042212.pdf>
- [63] H. A. Alrubaish and R. Zagrouba, "Cluster-based hierarchical message authentication code to secure data dissemination in wireless sensor network (CHIMAC)", *Int. J. of Appl. Engin. Res.*, vol. 14, no. 9, pp. 2084–2088, 2019 [Online]. Available: [https://www.ripublication.com/ijaer19/ijaerv14n9\\_02.pdf](https://www.ripublication.com/ijaer19/ijaerv14n9_02.pdf)
- [64] M. Jamshidi, E. Zangeneh, M. Esnaashari, A. M. Darwesh, and M. R. Meybodi, "A novel model of sybil attack in cluster-based wireless sensor networks and propose a distributed algorithm to defend it", *Wirel. Pers. Commun.*, vol. 105, no. 1, pp. 145–173, 2019 (DOI: 10.1007/s11277-018-6107-5).
- [65] B. E. Manjunath and P. V. Rao, "Balancing Trade off between Data Security and Energy Model for Wireless Sensor Network", *Int. J. of Elec. and Comp. Engin.*, vol. 8, no. 2, pp. 1048–1055, 2018 (DOI: 10.11591/ijece.v8i2.pp1048-1055).
- [66] G. Han, H. Wang, M. Guizani, S. Chan, and W. Zhang, "KCLP: A k-means cluster-based location privacy protection scheme in WSNs for IoT", *IEEE Wirel. Commun.*, vol. 25, no. 6, pp. 84–90, 2018 (DOI: 10.1109/MWC.2017.1800061).
- [67] T. A. Alghamdi, "Secure and energy efficient path optimization technique in wireless sensor networks using DH method", *IEEE Access*, vol. 6, pp. 53576–53582, 2018 (DOI: 10.1109/ACCESS.2018.2865909).
- [68] J. Agarkhed, Y. D. Patil, and Shilparani, "A survey on Internet of Things towards issues and challenges", *J. of Innov. in Comp. Sci. and Engin.*, vol. 7, no. 1, pp. 18–21, 2017 [Online]. Available: <https://www.indianjournals.com/ijor.aspx?target=ijor:jicse&volume=7&issue=1&article=004>



**Jayashree Agarkhed** is currently working as a Professor at the CSE Department of PDAACE Kalaburagi, affiliated to VTU. She obtained her M.Tech. in CSE in 2003 and Ph.D. in 2013, both from VTU. Her main research areas are in wireless sensor networks, multimedia information networks, artificial intelligence, cloud computing,

and the Internet of Things. She has published more than 150 scientific articles in top-tier journals and has contributed to numerous conferences and book chapters. She is an author of 2 books in the field of computer science.

 <https://orcid.org/0000-0003-3365-6498>

E-mail: [jayashreeptl@yahoo.com](mailto:jayashreeptl@yahoo.com)


Department of CSE

Poojya Doddappa Appa College of Engineering  
Kalaburagi, India



**Patil Yogita Dattatraya** is currently working as an Associate Professor at the Computer Science and Engineering Department of Sharnbasva University, Kalaburagi, and is pursuing a Ph.D. from Poojya Doddappa Appa (PDA) College of Engineering, Kalaburagi, affiliated to Visvesvaraya Technological University (VTU), Bela-

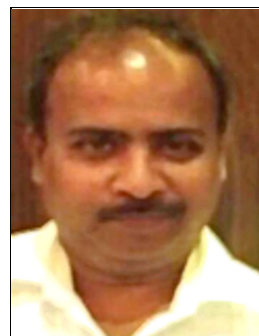
gavi. She obtained her B.E. from the Pune University and an M.Tech. in Computer Science and Engineering in 2010 from VTU. Her research focuses on wireless sensor networks, multimedia communication, cloud computing and the Internet of Things.

 <https://orcid.org/0000-0001-6478-3348>

E-mail: [agyogita@gmail.com](mailto:agyogita@gmail.com)


Department of CSE

Sharnbasva University  
Kalaburagi, India



**Siddarama R. Patil** received his B.E. degree in Electronics and Communication Engineering from Gulbarga University, Gulbarga, Karnataka, India, M.Tech. in Telecommunication Engineering, and Ph.D. from the Indian Institute of Technology (IIT), Khargpur, India, in 1990, 1999 and 2009, respectively. Currently, he is a Profes-

sor in the Electronics, Communication and Engineering Department and Dean Academics of Poojya Doddappa Appa College of Engineering, Gulbarga, Karnataka, India. His current research includes information theory and coding, turbo codes, LDPC codes, iterative decoding algorithms, wireless sensor networks, mobile ad hoc networks and cognitive radio.

 <https://orcid.org/0000-0002-7798-1359>

E-mail: [pdapatil@gmail.com](mailto:pdapatil@gmail.com)

Department of E&CE

Poojya Doddappa Appa College of Engineering  
Kalaburagi, India