Journal of King Saud University – Computer and Information Sciences 35 (2023) 651–681

HOSTED BY

Contents lists available at ScienceDirect

Journal of King Saud University – Computer and Information Sciences

journal homepage: www.sciencedirect.com

Data aggregation protocols for WSN and IoT applications – A comprehensive survey

Beneyaz Ara Begum [*], Satyanarayana V. Nandury

CSIR-Indian Institute of Chemical Technology, Hyderabad 500 007, India
AcSIR, CSIR-Indian Institute of Chemical Technology Campus, India

ARTICLE INFO

Article history:
Received 2 May 2022
Revised 21 December 2022
Accepted 8 January 2023
Available online 18 January 2023

Keywords:
Data aggregation protocols
IoT
WSN

ABSTRACT

Data aggregation involves the integration of correlated data generated by various wireless sensors and devices in WSN and IoT networks, in order to arrive at meaningful interpretation of the data sensed. It also serves as an efficient mechanism to optimize the resources like node energy, communication bandwidth and computation time, in WSN and IoT networks. The paper presents a brief overview of basic concepts related to WSN & IoT networks, data aggregation, and various optimization parameters used by the data aggregation protocols. A major contribution of the paper is to provide a comprehensive survey of various data aggregation protocols developed to address issues related to network topology, interference, fault-tolerance, mobility and security in WSN and IoT networks. Due to resource constraints, WSN and IoT networks are besieged with several competing requirements like latency, energy efficiency, data accuracy, data freshness, temporal correctness etc. The paper presents an in-depth discussion on these requirements, and the tradeoff strategies to be followed by data aggregation approaches to optimize these requirements. The paper highlights some of the gap areas in existing data aggregation approaches and suggests research solutions to amicably plug these gaps.

Contents

[*] Corresponding author.
E-mail addresses: nvs@csiriict.in (B.A. Begum), nandury@ieee.org (S.V. Nandury).

Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

https://doi.org/10.1016/j.jksuci.2023.01.008
1319-1578/© 2023 The Author(s). Published by Elsevier B.V. on behalf of King Saud University.

1. Introduction

Recent advances in wireless communications and the transition from 3G to 4G technology, had made it possible to connect *anything* to *everything* in a network. Due to this transition, Wireless Sensor Networks (WSNs) have now catapulted to a much larger application platform to manifest in the form of Internet of Things (IoT). With the advent of 5G services, WSN and IoT applications are expected to encompass several other application domains including big data driven applications. The rapid growth being witnessed in WSN and IoT networks can primarily be attributed to (a) the development of miniaturized sensors and actuators coupled with readily available high-speed internet services, and (b) the proliferation of smart devices into several application domains, particularly in remote sensing & data capture with the help of fog and cloud services.

At the core of this development is a miniaturized low-powered wireless sensor with embedded electronic interface to facilitate interaction with other wireless devices. The miniaturized wireless sensor has a built-in digital signal processor for conditioning of sensed data, transceivers for wireless communication, a battery to power various transactions and a microcontroller. To monitor a set of phenomena several such wireless sensors are deployed at various geographic locations in given region of interest. The wireless sensors coordinate amongst themselves to form a network of nodes and accomplish the defined task of aggregating the sensed data, and communicating the aggregated data to a sink or Base Station (BS) for further processing. Due to the large geographic spread, a wireless sensor resorts to multihop communication to establish a path to the BS, with the help of intermediary nodes acting as relay or Aggregator Nodes (AN). The ANs perform data aggregation and forward their aggregates to the next intermediary/AN in the path to the BS. The BS in turn forwards this information to a high-end computational platform for further processing.

Due to the presence of several low-cost miniaturized wireless sensors and devices, WSNs exhibit exceptional operational flexibility that helps them to form reconfigurable network structures to suit the application requirement. However, to maintain the low-cost advantage, the sensor nodes carry limited battery energy with low-end processing capabilities. Therefore, the wireless sensors forward their sensed data to the BS, which is endowed with better processing capability and has access to high-end processors. In order to optimize the battery energy, the wireless nodes indulge in short-range communications with other closely located sensor nodes. However, due to the close proximity of nodes, WSNs are often prone to radio interferences when two or more closely located nodes indulge in simultaneous transmissions.

With limitless opportunities for a wireless sensor node to get connected to other wireless sensors and internet-enabled devices, WSN has expanded its scope beyond the applications, which hitherto primarily centered around surveillance, intruder detection, remote monitoring of environment & industrial processes, defense, space, healthcare, agriculture etc.; to foray into application domains involving big data, data analytics and AI & ML applications. Data aggregation in such networks is confronted with several challenges particularly in the context of the five 'V's of big data viz. volume, velocity, value, veracity and variety. This poses several challenges to data aggregation and issues like (a) data integrity & data authentication, (b) data privacy preservation, (c) data accuracy & data correctness, (d) data redundancy & temporal data, etc., attain prominence while devising suitable data aggregation mechanisms and protocols. A holistic understanding of various underlying parameters that trigger competing requirements and the tradeoffs to optimize the network performance, is therefore necessary to address these issues. To this end, the paper presents a comprehensive survey of various data aggregation mechanisms and protocols developed by researchers' world-over to address issues related to network topology, interference, fault-tolerance, mobility, security and privacy. Further, the paper provides an in-depth discussion and analysis of various tradeoffs necessary for optimal performance of WSN and IoT networks with respect to the issues raised above.

There have been several other works that survey data aggregation in WSN and IoT networks, as shown in Table 1. Compared to other contributions that have surveyed WSNs, the main contributions of the paper are enumerated below:

- A comprehensive survey of data aggregation mechanisms and protocols developed for WSN and IoT networks in the context of their capability to address issues related to network topological structure, interference, fault-tolerance, mobility and security
- A comparison of the features, advantages and limitations of various data aggregation approaches and discussing their suitability for applications involving IoT networks
- Highlight the gap areas and challenges in the existing data aggregation approaches and the research challenges presently open for further research
- Discussion on optimization parameters and their competing requirements.
- Articulate the strategies to optimize the network performance in view of the competing requirements.

The paper is organized as follows: Section 2 presents a brief background on WSN and IoT networks, along with few definitions and terminology used in the paper. A brief discussion on various methods used for data compaction along with a classification of the data aggregation approaches is given in Section 3. A survey of various data aggregation protocols based on network topology is presented in Section 4. Data aggregation protocols that address issues related to interference, fault-tolerance, mobility (both node

Table 1
Brief overview of surveys conducted on data aggregation in WSN and IoT networks.

Publication	Focus and Highlights of the Survey	Scope and Limitations of the survey
Younis et al., 2014	• The survey focuses on tolerating node faults. • The paper provides a review of existing network topology management techniques and classification of fault-tolerance methods: proactive and reactive for tolerating/handling node failures in WSNs.	• The work does not survey of fault-tolerant data aggregation algorithms. • The survey is limited to node faults only. Process and interference faults are not addressed.
Jesus and Almeida, 2015	• The survey focuses on distributed data aggregation algorithms in WSN. • The paper provides an insight to problems related to distributed computing aggregation functions and distinct solutions to these problems. • The paper reviews different aggregation protocols based on communication taxonomy: hierarchy, unstructured and hybrid; and computation taxonomy: hierarchic, averaging, hash sketches, digests and counting.	• The survey does address interference, fault-tolerance, security and mobility issues in data aggregation. • Process faults were not addressed in the survey.
Rahman et al., 2016	• The focus of the survey is to compare few data aggregation techniques for WSN and IoT for various network topologies. • The paper provides a comparative study of few data aggregation algorithms like LEACH and LEACH-C with reference to parameters like energy dissipation, network lifetime, throughput, latency, etc.	• The scope of the survey is limited few network topologies and does not address interference, fault-tolerance, security and mobility issues. • Discussion on the applicability of the WSN based data aggregation algorithms for IoT networks is not addressed.
Lin et al., 2017	• The paper presents a comprehensive overview of IoT with respect to existing system architectures (viz., IoTSDN, three-layer and SOA) and inter-relationship with cyber physical systems. • Issues related to integration of fog/edge computing and IoT are surveyed. • The paper focuses on resource allocation, security and privacy	• The scope of the survey is limited to architecture, security and privacy issues. • The survey does address interference, fault-tolerance, and mobility issues in data aggregation.
Salman and Jain, 2017	• The paper focuses on presenting a survey of standards/protocols related to data link, routing, network and session layers in IoT networks. • Provides insight to different device management protocols and security protocols used in M2M and IoT applications.	• The scope of the survey is limited communication and security protocols in IoT networks. • Issues related to data aggregation, interference, mobility are not covered in the survey.
Ray, 2018	• The paper surveys existing IoT hardware platforms and wireless communication technologies/standards. • It also presents a survey of domain-specific IoT architectures: RFID, SOA and WSN, supply chain management and industry IoT.	• The scope of the survey is limited to communication protocols in IoT networks. • The survey does include issues related to fault-tolerance and mobility issues in data aggregation.
Kathjoo et al., 2018	• The paper focuses on providing a comparative study of the approach followed by WSN and IoT networks, with particular reference to the existing WSN standards: Zig Bee, WirelessHART and ISA-100.11a • It discusses the application requirements of WSN and IoT with respect to parameters: security, robustness, scalability, QoS, heterogeneity, autonomy, data processing, mobility and coverage.	• The study highlights the dissimilarities and similarities and in the approach followed by WSN and IoT in various communication protocols. • The differences in the data aggregation approaches followed by WSN and IoT do not find a place in the study.
Ni et al., 2019	• The work discusses the architecture of mobile edge computing (MEC) in IoT. • It explores the data processing capability of IoT to enhance data analysis of data-intensive applications with respect to parameters: data security & privacy through secure data aggregation, and data deduplication, and improve computational efficiency through offloading computation and services.	• The scope is limited to data aggregation and security issues in edge-enabled IoTs. • Issues related to data aggregation approaches that address networks of different topologies, interference and mobility are not covered.
Dehkordi et al., 2020	• The paper provides an in-depth survey on different types of data aggregation techniques and protocols based on topology and computational intelligence in terrestrial WSNs. • The survey also includes application challenges and routing protocols on Wireless Underground Sensor Networks (WUSNs), DA protocols for underwater WSNS (UWSNs) and protocols for WBANs (Wireless Body Area Networks).	• The scope of the survey is limited to surveying data aggregation approaches to terrestrial WSNs and underwater WSNS. • The survey does not include the data aggregation protocols for other applications.
Liu et al., 2020	• The paper presents a comprehensive review of secure data aggregation methods with respect to the security goals: anomaly-based, encryption-based, privacy, slicing etc. in WSNs. • It discusses some of the challenges that need to be addressed in secure data aggregation.	• The scope of the paper is confined to discussions and review on secure data aggregation approaches. • Data aggregation approaches for other issues are not discussed in the paper.
Xue et al., 2020	The paper presents a survey of edge computing, and architectural integration of Edge computing with IoT.	The survey does not cover issues related to data aggregation approaches in edge computing IoTs.

and BS mobility) and security, are discussed in Section 5 and Section 6. Section 7 discusses various optimization parameters and their inherent competing requirements. The gap areas in existing data aggregation approaches and future challenges are discussed in Section 8.

2. Definitions, overview of WSN and IoT networks

In this Section, we present a brief background on wireless sensors, WSN and IoT networks. Some definitions and terms used in the paper are given in Table 2**.**

A wireless sensor node is a small low-battery powered cost-effective sensing device equipped with a microcontroller, the sensing mechanism and radio transceivers for wireless communication. Due to the use of low-cost wireless sensors and internet-enabled devices, WSNs and IoT networks find applications in both social and strategic domains. Further, the ease of deployment of multiple wireless sensors and actuators networked together makes Wireless Sensor Networks (WSN) an attractive option for myriad application domains like: basic building blocks for IoTs for smart homes & smart cities, wireless body area sensor networks, remote monitoring of environment for pollution control & weather forecasting, surveillance and security for defense & space applications, industrial process automation & control, IoT enabled wearable body sensors placed in human body to monitor the health of a patient, wireless sensors and IoT devices placed at different locations to monitor the nutrients in the soil, pests, etc.(Durisic et al., 2012; Elijah et al., 2018; Gravina and Fortino, 2021; Kandris et al. 2020; Nandury and Begum, 2015).

Amongst the various unit operations performed by a wireless sensor, the specific energy consumption (energy per unit time) for radio transmission and reception operation is quite high,

Table 2
Terminology and Definitions.

Terminology	Definition and Description
Wireless sensor node (n_i)	A wireless sensor deployed in Sensor Deployment Region (SDR) is termed as a wireless sensor node. It has the capability to sense, process, compute and aggregate the data received from its neighboring sensor nodes.
Coverage	Sensing area covered by wireless sensors in the SDR.
Carrier Sense (CS) region	The unit disk centered around a source node with radius equal to its sensing range is called the CS region.
Wireless link $l_i(S_i , D_i)$	It is a unique edge for communication between a source node S_i and destination node $D_{i.}$
Distance $dist(n_i, n_k)$	The Euclidian distance between two nodes n_i and n_k in a Cartesian plane. It is also the shortest path between the two nodes.
Path	Path is a sequence of links/edges connecting nodes in a component. A unique path exists between any node in the component to the sink.
Parent node and Child node	The parent of node n_c is the unique node n_P that has an unique edge either directly to the sink or to the first node in its path to sink node. The node n_c is termed as the child node of n_P
Wireless Sensor Network (WSN)	A wireless network consisting of spatially distributed autonomous devices using sensors to monitor physical or environmental conditions such as temperature, sound, pressure, etc.
Sink node	It is the topological centre of the network to which all communications from the sensor nodes are routed.
Base Station (BS)	The BS is the node to which the sink nodes route their data. It is considered to be a node with limitless energy and acts as a gateway between the sink node (sink/topological center node) of the WSN and high-end computing platforms. Sink and BS are used interchangeably in the paper.
IoT platform	IoT platform is a cloud software that connects the sensors, gateways, end-user applications, or any other physical thing/devices enabled with network connectivity.
Transmission/Reception range (R_T)	R_T is the maximum distance between a source–destination pair (S_i, D_i), up to which the nodes can successfully communicate. Transmission range and reception range are synonymous and are used interchangeably.
Interference	Distortion of the signal received by destination node D_i due to noise and radio interference of concurrent transmissions from other unintended source nodes.
Interference range (R_I)	Maximum distance up to which unintended source nodes can interfere with the reception of a destination node. Generally, $R_I >$ R_T.
Successful transmission/reception	A transmission from S_i to its intended receiver D_i is successful if D_i can correctly decipher the data transmitted by S_i.
SINR threshold (β)	SINR is the minimum Signal to Interference + Noise Ratio required for successful reception of signal by an intended destination node. SINR is expressed in dB.
Path loss/gain exponent (α)	α is a parameter that indicates the rate at which the Received Signal Strength (RSS) decreases with distance due to the medium of signal propagation.
Intended and unintended nodes	In a link $l_i(S_i , D_i)$, S_i and D_i, are termed as intended source–destination pair of nodes. Any source node other than S_i is termed as the unintended source node of D_i. Similarly, any destination node other than D_i is termed as the unintended destination node of S_i.
Potential Interferer (PI)	Any unintended source node S_k which can potentially interfere with the reception of signals D_i, is termed as Potential Interferer (PI) of D_i. $l_k(S_k , D_k)$ is termed as the Potential Interfering Link (PIL) of $l_i(S_i , D_i)$.
Precedence relations	If the processing/computation of n_j needs to precede the processing/computation of n_i, then n_i and n_j, are said to have precedence relations.
Aggregator node (AN)	It is an intermediary node that aggregates the data received from its child nodes and forwards the aggregate to the root with the help of other intermediary nodes.
Data aggregation functions	The functions such as AVG, MIN, MAX, COUNT and SUM performed by the AN to aggregate the data received from its neighboring nodes.
Threshold energy	Threshold energy is the minimum energy that is required by a node to function as a healthy node while performing transmission, or a reception operation.
Residual energy	The residual energy is the energy possessed by a node n_i after the completion of transaction.
Faulty node	A faulty node is generally considered as the node whose residual energy is below the threshold energy required for transmission and reception operations
Minimum Latency Aggregation Scheduling (MLAS)	Minimum Latency Aggregation Scheduling (MLAS) algorithms aim to minimize the effect of wireless interference and collisions by scheduling non-interfering links to transmit simultaneously in the same time slot such that the total number of time slots used to aggregate the data is minimum.
Hidden Terminal (HT) problem	HT problem occurs when two source nodes inadvertently transmit in the same timeslot, oblivious of the fact that their transmissions might interfere with each other. Here the two source nodes are not within the CS range of each other.
Exposed Station (ES) problem	ES problem occurs when the source nodes either defer or back-off their transmissions, when they notice that other source nodes within their Carrier Sense (CS) range are transmitting, even if the transmissions do not interfere with each other.
Arborescence	It is a directed rooted tree with exactly-one directed path from each node to the root.

compared to other operations like performing aggregation and computation. While the specific energy consumed by a sensor for idling or remaining in *active* state, is significantly small, the total energy consumed by the sensor to remain in *active* state for long durations of time, is significantly high. To get over this problem, duty cycles (*sleep* and *active* states) are introduced, where a sensor node enters into *sleep* state to conserve its energy. However, for this strategy to be effective, the duty cycles need to be accurately determined.

The sensor nodes use their on-board processors to locally perform preliminary signal conditioning and pre-processing operations on the sensed data. The pre-processed information is converted into data packets and is routed to the sink node of the network with the help of neighboring nodes. The sink node collates the data received by its subsidiary nodes and forwards this information to the Base Station (BS). As there exists a direct one-to-one communication between the sink node and the BS, the sink node is often referred to as BS. However, in large WSNs there could be multiple sinks, and multiple BSs. In such cases the sink forwards its aggregate to its closest BS. For ease of understanding, unless otherwise specified, we use the terms sink node and BS interchangeably in this paper.

In most hierarchy-based network topologies, the sensor nodes located closer to the BS carry the additional burden of relaying the data received from lower level nodes to higher level nodes in the path to BS. As a result, the nodes closer to BS turn into hotspots, and a major portion of their battery-energy is consumed in relay operations. This phenomenon triggers issues related to load-balancing and faster depletion of energy of nodes closer to BS, which eventually leads to node/link failures. To reduce the number of relay transmissions and conserve the node energy, data compaction techniques like data compression, data fusion and data aggregation have become popular, which are discussed in Section 3.

2.1. Features of WSN

Compared to ad hoc networks, WSNs exhibit much closer coordination amongst the nodes in the network. The wireless nodes even though autonomous, are ordained to collectively cooperate to ensure that the sensed data is forwarded to the BS. To facilitate this, the nodes exploit some of the inherent features of WSN, as shown in Fig. 1.

2.1.1. Self-organizing network with flexible topology

The sensor nodes in WSN are capable of determining their geographical location either through an embedded GPS, or by estimating their locations relative to that of their neighbors. Due to this attribute, the sensor nodes in WSN have self-organizing capability and can configure themselves into connected networks. To route the sensed data to BS, the nodes self-organize themselves into tree, cluster, grid, mesh, etc. To illustrate this feature, consider the deployment pattern of wireless nodes as shown in Fig. 2(a). Depending on the application requirement, the nodes can organize themselves into tree, cluster, grid or mesh topologies as depicted in Fig. 2(b) to 2(e). The self-organization feature abstracts the underlying operations in establishing communication paths from BS to sensor nodes. The versatility of WSN presents an environment conducive to flexible network topologies, which can accommodate changes in application needs. The inherent redundancy of the WSN helps in determining multiple paths from any given node to the BS and therefore, failure of nodes may not significantly affect the functionality of the network. This feature was used to develop a self-healing approach, to tolerate node/link without the use of additional resources in Begum and Nandury (2022a). The nodes in the WSN also have the capability to accommodate new nodes, which synchronize seamlessly with their neighboring nodes without much degradation in the overall performance of the network.

2.1.2. Dense deployment and cooperative nature

Depending on the nature and ease of operation, the sensor nodes are strategically deployed to cover the SDR based on any of the following schemes *viz*., (a) strategically identifying deployment locations, (b) deployment at random locations, and (c) a mix of both schemes. The self-organizing nature of WSN makes it amenable to accommodate dynamic topological changes to pave way to newer WSN configurations. This feature enables the WSN administrators to densely deploy the sensor nodes in a given geographic location. However, as the network becomes dense, the BS may not be in a position to track & manage the network information flow from the sensor nodes. To get over this limitation, the sensor nodes share their localized information (node position, energy level) with their immediate or single-hop neighbors, and cooperate to perform the task of integrating or aggregating the sensed information.

2.1.3. Short-range broadcast and multihop routing

Sensor nodes in WSN are equipped with transceivers having omnidirectional antennas, which establish communication in a wireless mode with neighboring nodes on radio frequency (RF) medium. Constrained by energy, size and space limitations, the wireless sensors operate on miniature RF antennas. The energy expended by the nodes for RF transmission is relatively large compared to operations such as data processing, computing and generating control signals. Further, the farther a node transmits to reach its neighbor, larger is the energy it consumes. Therefore, in order to optimize battery-energy, the RF transceivers resort to short-range transmissions with their immediate one-hop neighbor nodes. To facilitate communication between BS and the nodes that are not within one-hop distance, multi-hop routing is established.

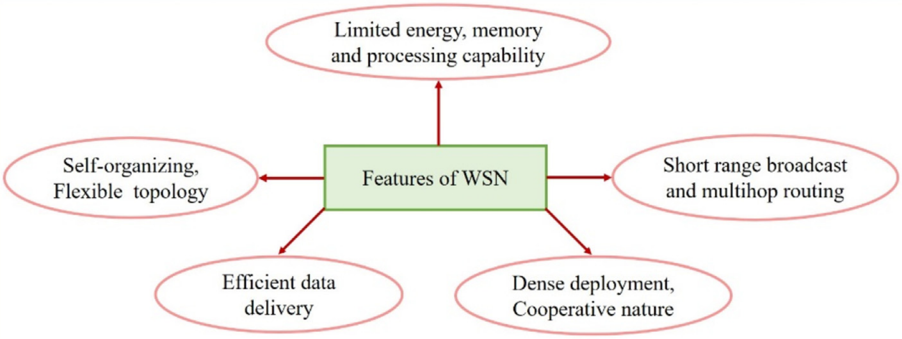

Limited energy, memory and processing capability
Self-organizing, Flexible topology
Features of WSN
Short range broadcast and multihop routing
Efficient data delivery
Dense deployment, Cooperative nature

Fig. 1. Features of Wireless Sensor Networks.

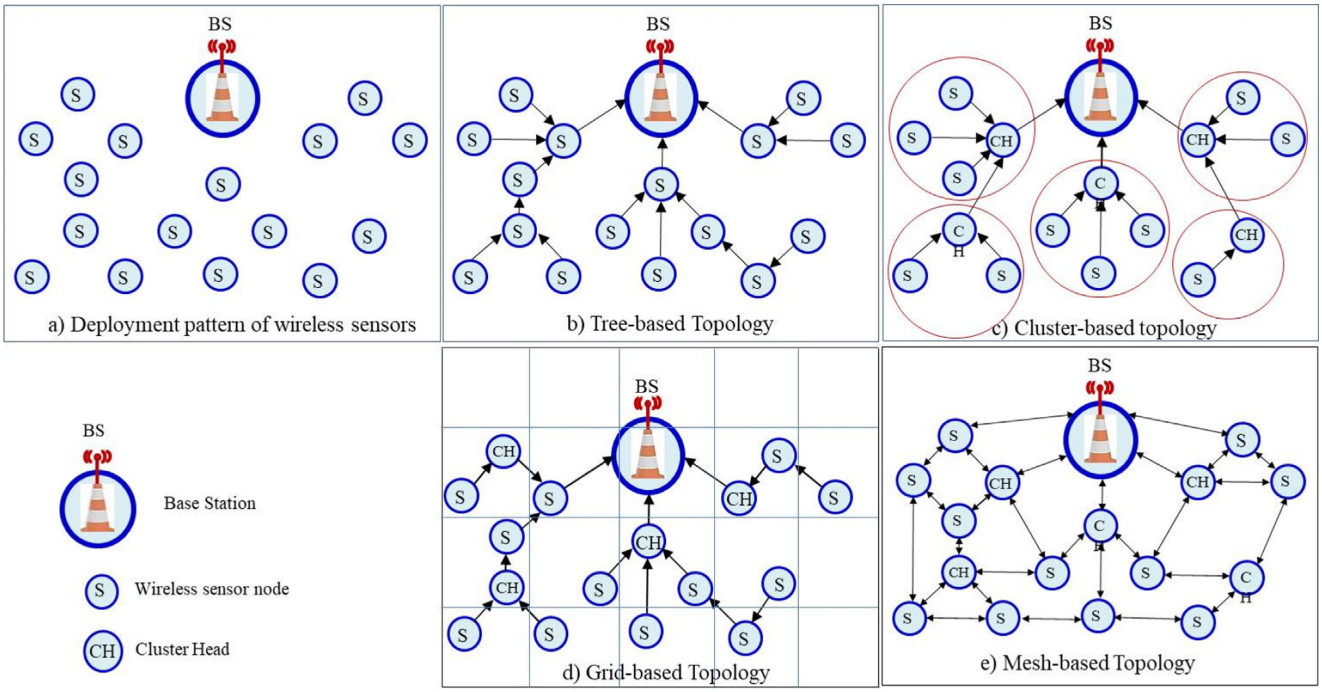


Fig. 2. Example of Self-organizing feature of WSN.

2.1.4. Efficient data delivery models and addressing schemes

As the information sensed by a node meanders its way to the BS in the form of data packets, it is of prime importance to ensure: (a) that the sensed information is delivered in its pristine quality, (b) that the intermediary nodes do not consume much energy, and (c) timely delivery of packets without much delay or latency. To improve the efficiency with respect to the above three requirements, several data delivery models and addressing schemes were proposed, which are briefly described below:

Data delivery models: Based on the application, different data delivery models employed by WSN are enumerated below:

- **Event-driven:** In event-driven data delivery model, the sensed data is delivered to the BS only on the detection of an event. This delivery model finds applications in safety, security, intrusion detection, etc.; where it is critical for the BS to initiate appropriate response mechanism once an event is detected. Event-driven model is used in applications that are mission-critical, where detection of an event without any time delay is of prime importance. This model however, has to deal with good degree of redundancy if the event is detected and reported to the BS by multiple sensors. Further, if the event detection threshold levels are not well-defined, the sensor nodes tend to report low intensity signals to the BS, which may then raise false alarm.
- **Query-driven:** In query-driven applications, a query is initiated by the BS to retrieve specific data from sensor nodes. Only the nodes that satisfy the query, respond back to the BS. Most query-driven applications are interactive, query-specific, delay-intolerant and mission-critical. Unlike the event-driven model where the event data is *pushed* to the BS, in query-driven model, the event data is *pulled* by the BS through a *query-on-demand*. The BS may also use a query to reconfigure and manage the sensor nodes for purposes such as, software upgradation, reconfiguration of data transmission rates, etc., by sending out a *command* query to the nodes.
- **Continuous/Periodic:** In continuous/periodic applications, the sensors continuously monitor the environment and periodically relay the sensed data to BS at predefined time intervals. In time-critical applications, the data sensed is delay-constrained. For example, in real-time radar tracking applications, the information received at the BS loses its significance if the data is delivered after a threshold time limit. On the other hand, applications that routinely monitor the environment, say humidity; may not be time constrained and hence can accommodate time delays and sporadic loss of sensed data.
- **Hybrid:** This data delivery mechanism is mix of two or more data delivery models, where the nodes may resort to any data delivery mechanism depending on the nature of transaction to be performed.

Addressing scheme: For establishing communication amongst the nodes, the sensor nodes are provided with unique addresses, which act as their global identifiers. While MAC addresses help in resolving medium access contention, static assignment of addresses may not always be feasible if the network topology is dynamic in nature. As WSNs become larger, it is impractical for the network to access sensor data through non-unique node identifiers. Even if unique identifiers are used, the 64-bit MAC address may itself be larger than the packet payload. This results in large transmission overheads. To reduce these overheads, data-oriented naming schemes are used.

One of the important features of WSN, especially in the context of data aggregation is its data-centric addressing scheme. Unlike the traditional address-centric routing, where data is routed along the shortest path to the BS based on metrics such as least hop-count; in data-centric approach, the nodes are addressed based on the nature of data packets that they carry, rather than their physical address. A sensor node in data-centric approach tries to locate the aggregator which is most suitable to the data being aggregated. The address of an aggregator is primarily specified by a set of attributes that define the nature of data being aggregated, its routing path to BS, and other overheads. This facilitates more efficient routing of information from a data-centric node to its aggregator node.

2.1.5. Limited battery energy, memory, and computing power

WSNs gain their prominence in remote monitoring & control applications due to autonomous and miniaturized sensor nodes in the network. However, the miniaturized size-advantage comes at the cost of limitation in memory size, battery-energy and computational power of a sensor node. Compared to other wireless ad hoc networks, WSNs have stringent requirements on node energy and network lifetime.

2.2. IoT networks

Traditional WSNs were primarily developed for applications that involved monitoring remote and harsh terrains, where establishing a wired infrastructure was a major challenge. Later, due to easy access to satellite communication, the production of internet-enabled wireless sensors and devices started gaining ground. This has led to the development of applications where several internet-enabled sensors, *things* (devices), were integrated into a network, paving way to what is now being referred to as IoT networks. IoTs which were originally considered to be an off-shoot of WSNs, started assimilating the concepts developed for WSNs to address various issues related to network topology, data aggregation, interference, fault-tolerance, security, etc. With the onset of 4G and 5G technologies, IoTs expanded their scope and transgressed into application domains that network several thousands of *things* that keep generating humongous amounts of data. To harness the data generated IoT networks increasingly rely on cloud, fog and edge computing technologies. A brief overview of the features of IoT networks, and the prime distinctions between WSN and IoT networks are covered in this section. The features of IoT network are illustrated in Fig. 3.

IoT is an ensemble of several sensors, actuators and internet/Wi-Fi enabled devices in loosely coupled distributed network. Due to the loose coupling, IoT devices exhibit greater degree of autonomy and self-adaptation. The ease of integrating cross-domain technologies makes IoTs highly scalable that can encompass thousands of devices, making the IoT networks ubiquitous. The scalability of IoT networks is primarily due to their self-configuration and interoperable communication features.

A typical IoT application comprises a network of WSNs and IoT devices with internet, fog or cloud as the communication media as illustrated in Fig. 4, where several IoTs and WSNs are networked together via an internet cloud. While fitness trackers, smart watches and wearable biosensors form a part of IoT Node 1, smart home devices which collect data from IP cameras & smart TVs, smart speakers & smart locks, and HVAC are designated as IoT Node 2. A cellular network that tracks several smart devices connected to it is designated as IoT Node 3. Similarly, the IoT application has two WSNs, where their base stations are networked to other devices via an internet cloud as shown in the figure. Collectively, different constituent nodes of the IoT application function in a coordinated manner to fulfil a given mandate. The collected data can be sent to a remote data cloud for analytics. Few similarities and distinctions between WSN and IoT networks are given in Table 3.

3. Data compaction and data aggregation techniques

WSNs comprise large number of low-cost sensor nodes that have limited energy & processing capability, and low storage capacity. The nodes usually generate large amounts of data with high temporal coherency. A key strategy to leverage the low-cost advantage of the miniature devices, be it in WSN or IoT network, is to optimize the limited battery energy of wireless sensors by limiting the number of transmissions in the network. While the number of data packets generated by each node/device may be relatively small, the quantum of packets generated collectively by all nodes is significantly large. The transmission of such large quantum of packets by the intermediary nodes/devices either to BS as in case of WSN, or to an internet cloud as in case of IoTs; leads to multifold increase in the network traffic. Further, due to the deployment of large number of sensors to monitor the same phenomenon, for example, the use of thermocouple, thermistor and infrared sensors to monitor temperature; leads to redundancy in data (Gavel et al., 2021). Further, due to limited storage capacity, a sensor node/device may not have large enough buffer to accommodate the incoming data, which leads to packet drop once the buffer is full. Besides resulting in loss of data, it involves substantial load on network traffic as nodes are forced to retransmit the dropped packets. This results in faster energy drain out of nodes besides leading to undesirable consequences like increased latency. An effective mechanism to handle data is to aggregate,

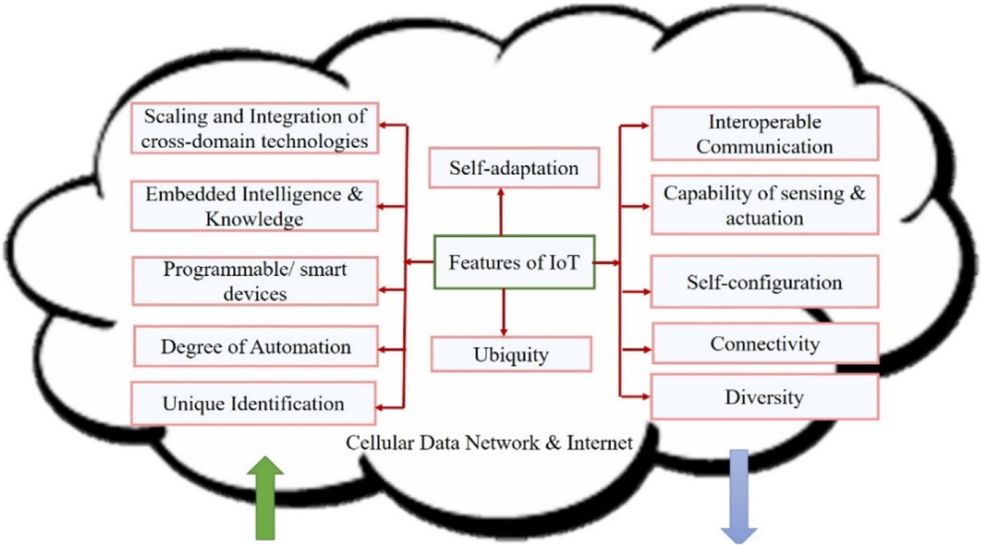

Scaling and Integration of cross-domain technologies
Embedded Intelligence & Knowledge
Programmable/ smart devices
Degree of Automation
Unique Identification
Self-adaptation
Features of IoT
Ubiquity
Interoperable Communication
Capability of sensing & actuation
Self-configuration
Connectivity
Diversity
Cellular Data Network & Internet

Fig. 3. Features of IoT.

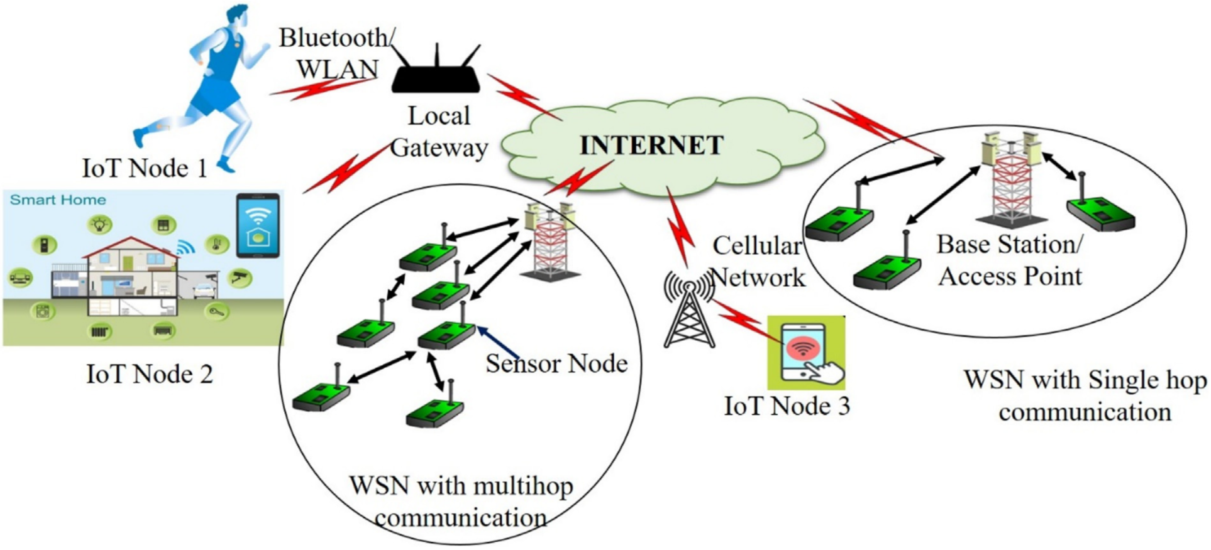


Fig. 4. Typical WSN and IoT application network.

fuse or compress the data at intermediary nodes before transmitting the compacted data to BS. Depending on the method used, data compaction can be classified as data aggregation, data compression and data fusion. The methods along with some key concepts are elaborated in this section. Three major data compaction techniques are data compression, data aggregation and data fusion, as illustrated in Fig. 5.

3.1. Data aggregation

Data aggregation involves integration of correlated or homogeneous data at intermediary nodes designated as aggregators, in order to arrive at meaningful interpretation of data sensed by various sensors/devices in the WSN/IoT. Here, data from multiple nodes are aggregated by ANs by performing appropriate aggregation functions like MIN, MAX, SUM, AVE, GREATER_THAN, etc., on similar or correlated data. After performing aggregation, the aggregator forwards the result also known as the *aggregate*, to the BS. For example, consider an application where sensors are deployed to record maximum temperatures observed in a given time interval. In such application, an aggregator node employs MAX function to determine the maximum temperature sensed, based on the information received from its neighboring nodes during a given time interval. The aggregator then forwards only the information related to the maximum temperature recorded in the given time interval to BS. This significantly reduces the number of packets transmitted to the BS. The primary objective of aggregation is to collate data, perform aggregation and forward meaningful information to BS. Besides reducing the number of data packets and easing the network traffic, data aggregation also reduces the latency and the power consumed by the nodes in the network (Krishnamachari et al., 2002).

The time at which data is aggregated, i.e. aggregation timing, is of great significance for true and accurate representation of data sensed by the network nodes. Timing is greatly impacted by the type of data delivery model and the data aggregation approach, whether centralized or in-network aggregation employed. The timing models and data aggregation approaches are described below.

3.1.1. Timing models for periodic data aggregation

Depending on the phenomenon to be monitored, the data delivery model employed can be periodic, aperiodic (query/event driven) or a hybrid of the two. Periodic data delivery in particular, impacts the freshness and accuracy of data delivered to the BS. While longer sampling time may apparently result in a well averaged-out value, too long a wait period may result in the aggregation of stale data or data which has outlived its value. Further, a longer wait period may also lead to an overlap of data between two successive periods. Therefore, proper time synchronization amongst the nodes is necessary to ensure that there is no overlap between fresh and stale data while performing aggregation. Time synchronization is of particular importance in periodic data delivery scheme, due to the fact that aggregation on a given set of data must be performed before the arrival of the next periodic data. The timing model defines how long an aggregator node needs to wait to receive data from its child node before performing aggregation. The timing models can be categorized as follows:

Periodic Simple Aggregation (PSA): In PSA, every parent node in the aggregation path waits for a predefined time period to receive data from its child nodes. Thereafter, the parent node aggregates the data received, including its own, and sends the aggregate to the next hop node. The maximum timeout period of a node is set, based on the time at which it has received its last packet from its child nodes.

Periodic Per-hop Aggregation (PPA): In periodic per-hop aggregation, the aggregator transmits its aggregate as soon as it receives data from all its child nodes, without waiting for timeout. To facilitate this, each parent node maintains information about the number of children it has. Similar to PSA, this approach too, is subjected to a longer delay if the parent node is not able to receive data from all of its child nodes before its timeout.

Periodic Per-hop Adjusted Aggregation (PPAA): In PPAA, a node's timeout depends on its position in the aggregation tree in each round. The parent node informs its children the time at which it expects to receive data from them. The child nodes schedule their transmission intervals to coincide with that of their parent's. Unlike PPA model, where the periods for all hops are assumed to be uniform across the network, this model makes provision for adjusting the node timeouts based on the time periods for each hop in the aggregation tree. The disadvantage of PPAA is increased delay if the transmissions of the child and parent nodes are not properly synchronized.

Table 3
Characteristics of WSN and IoT.

Characteristics	WSN	IoT Networks
Application domain	Primarily used for monitoring and data collection.	Serves numerous application including monitoring, data collection, control, communication, etc.
Network Components	Majority of nodes are wireless sensors. In addition, there can be few wireless/wired relay nodes and Base Stations.	Any internet-enabled device whether sensor, actuator, smart device can be a node in IoT network.
Number of nodes	Typically restricted to few wireless sensors to thousands.	Theoretically no limit to the number of devices connected.
Nature of data generated	The data generated by the wireless nodes are singularly in tune with each other. The wireless sensors generate limited amount of data.	Due to widely varying nature of IoT devices, diverse range of data is generated. The data generated by thousands of devices in an IoT network can be classified as big data.
Data packet Format	The sensors exchange data packets, which usually follow a uniform pattern.	There is no uniformity in the data packet format.
Volume, velocity and veracity of data	The volume and velocity of data generated is moderate. The data generated is largely authenticated.	In large IoT applications, the volume & velocity of data generated is humongous, and can be classified as big data. Data authentication is a major challenge
Network Topology	Adhoc, hierarchical, non-hierarchical, flat network of wireless sensors	Adhoc, largely heterogeneous, network of smart devices
Radio Channel access	CSMA-CD, CSMA-CA TDMA, TDMA/CDMA, LORA	CSMA-CD, CSMA-CA, TDMA, TDMA/CDMA, LORA
Communication	Wireless	Wireless, Internet, Edge computing, Fog/cloud computing
Security	The number of devices being limited, it relatively less complicated to build strong security features. However, if the wireless transmissions are not encrypted, WSNs are prone to security attacks.	All data transmissions are through internet, the application has the same security as the one provided by the ISP, which is usually high. If the transmissions are through fog/cloud, the security is very high. However, due to scalability of IoT network, the security may be compromised when a device that does not have built-in security features is integrated in to the network.
Interface to external world	BS or a set of BSs in a WSN form the gateway to external world.	The interface to the external world is through internet/web-enabled devices, with help of fog and cloud computing platforms.
Scalability	Moderate scalability	Highly scalable
Protocols	Proprietary, ZigBee, WirelessHART, ISA 100.11a**,** WiFi and mmWave (2.4 GHz, 5 GHz, 6 GHz Upper, 6 GHz Lower, 24 GHz, 60 GHz), LoRaWAN RF (868 MHz) LoRaWAN RF (900 MHz) 3G/4G/5G Mobile Data, Bluetooth Low Energy (2.4 GHz)	**Datalink Protocol:** IEEE 802.15.4e, EEE 802.11ah, WirelessHART (TDMA), Z-Wave Bluetooth Low Energy (2.4 GHz), ZigBee Smart Energy, DASH7, HomePlug. G.9959, IPv6, LTE-A, LoRaWAN RF (868 MHz, 900 MHz), NB-IoT, DECT/ULE, EnOcean, 3G/4G/5G Mobile Data **Network Layer Routing Protocols:** RPL, CORPL, CARP, E-CARP **Network Layer Encapsulation Protocol:** 6LoWPAN, 6TiSCH, 6Lo, IPv6 over G.9959, IPv6 over Bluetooth Low Energy **Session Layer Protocols:** MQTT, SMQTT, AMQP, CoAP, XMPP, DDS WiFi and mmWave (2.4, 5, 6, GHz Upper & Lower, 24 GHz, 60 GHz) (Kathjoo et al. (2018)
Autonomy of devices	Moderate	Highly autonomous
Deployment and coverage	The sensors are usually deployed through a predefined strategy. As WSNs are highly application oriented, the deployment strategy ensures maximum coverage.	As the communication is through internet, control on deployment and coverage does not exist.
Signal and Data Processing	While signal processing is performed by the sensors, data processing is performed at BS. Therefore, the computational capacity of the BS can be a limiting factor. Handling big data is therefore a serious Data Compaction challenge.	Signal and data processing is performed through internet and cloud, and hence the IoT devices need not carry high-end processors for computation. Good candidate for handling big data.
Mobility	Mobility is restricted, as sensor nodes rely on BS for all communication & high-end computation needs.	IoT devices rely on internet for communication & high-end computation needs. Therefore, the mobility can be high, subject to the availability of internet.
Performance metrics	Area coverage, network energy, end-to-end delay, throughput, received signal strength, bit-error-rate, packet-reception-ratio and network resilience to node faults and attacks.	Performance is analyzed in the context of applications like security, device connectivity and load conditions, functionality, quality and reliability, real-time decision making of IoT services.

Cascading Timers Aggregation (CTA): Cascading timers is another variation of PPAA protocol. It targets applications where periodic data is generated for continuous monitoring, for example, temperature, humidity, seismic activity, etc. In CTA, the position of a node in the routing hierarchy of the aggregation tree determines its timeout. The timeout of a child node is set before that of its parents. This causes a "cascading" effect, where data originating at the leaf nodes is clocked out first, to enable the parent node to perform aggregation and transmit the aggregate, before the timeout period of next higher level node. The net effect is that a "data wave" reaches the BS in one round of data collection. Cascading timers are triggered with an initial request from the BS. The request contains a hop count field which gets incremented as the request propagates to the leaf nodes.

3.1.2. Data aggregation approaches

Depending on the level of involvement of nodes in carrying out aggregation, there can be two types of data aggregation approaches: Centralized Data Aggregation (CDA) and In-network Data Aggregation (IDA).

In CDA the nodes periodically relay their sensed information to a solitary Centralized Aggregator (CA), which is responsible for aggregating the information it receives and transmitting the aggregate to BS. All intermediary nodes in the routing path to the CA act merely as relay nodes that forward the data packets they receive to the CA. CDA is simple to implement and is most suitable for small networks, where most nodes are within one hop distance from the CA. It is also desirable in applications where centralized control is a prime requirement. However, as all data packets are routed to the CA, the nodes closer to CA become traffic hot spots and may drain

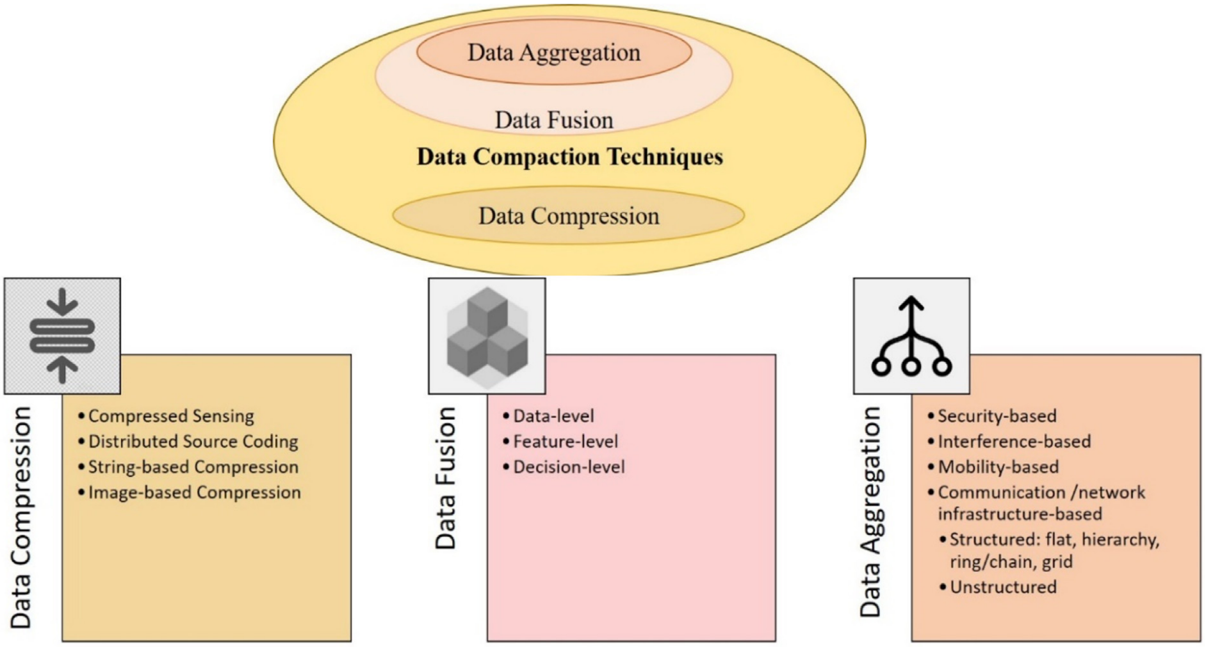


Fig. 5. Data Compaction Techniques.

out their energy prematurely. Therefore, in large networks the energy depletion rate of nodes is non-uniform and the WSN tends to become unreliable. Further, if CA fails, the WSN is prone to single-point failure. This is the main drawback of this approach.

In-network data aggregation tries to address the limitations of CDA by providing multiple data aggregators distributed across the network. The aggregators nodes apply suitable aggregation functions on the data they receive from their child nodes and route the aggregate to BS. This reduces the network traffic overhead, as only aggregated data packets are routed to the BS, which results in longer network lifetime. Further, due to its decentralized approach, IDA is not prone to single point failure, and can be readily adapted to large WSNs.

3.2. Data fusion and data compression

Data fusion and data compression are approaches that strive to reduce the number of data communication packets. While data fusion compacts the data by integrating the *information* captured by sensor nodes, data compression treats the packets of information it receives as *textual data* before compressing it.

3.2.1. Data compression

Data compression techniques are employed to reduce the number of packets required to represent the sensed information. This technique is popularly used to save battery-energy of sensor nodes monitoring multimedia applications such as tracking, object localization and object detection, traffic surveillance, etc. Unlike data aggregation which aims to aggregate the *information* sensed by its subsidiary nodes, data compression attempts to compress the *data* it receives. Data compression comprises two phases; encoding and decoding. In the encoding or compression phase, a compressed version of the original data is generated by reducing its size through bit-reduction. The decoding/decompression phase attempts to reconstruct either the original data, or some approximation of it from the compressed version. Data compression algorithms can accordingly be categorized into two classes *viz.* lossless and lossy. Lossless compression algorithms reconstruct the original data, whereas lossy compression algorithms, reconstruct an approximation of the original data. Some of the well-known data compression algorithms are briefly described below.

String-based Compression Techniques: In this technique, the sensed data is treated as a string of characters on which text-data compression schemes are employed. A popular dictionary based encoding scheme is the LZW, where the algorithm scans each character in the input data stream and tries to match a substring in the dictionary. When such a string is found, the index of the longest matched substring in the dictionary is sent to the output data stream. If there is no match, the unmatched string is added to the dictionary. Here the sender and receiver agree on same initial dictionary. Information about new entries is derived from existing entries.

Image-based Compression Techniques: In this technique, the information sensed by a sensor node in a hierarchically organized WSN, is treated as an image represented in the form of a matrix of pixels. By applying wavelet transformations on the matrix, important features can be extracted and stored to reduce the size of information. The upstream nodes on receiving the compressed data apply the wavelet transmission technique to retrieve temporal and spatial data. Features having high correlation are then reduced in size by image-based compression techniques such as multi-resolution compression query framework.

Compressed Sensing Techniques: Compression is performed locally on each node, based on a randomly generated projection vector. In this technique, each node compresses its sensed data with the help of randomly generated non-adaptive linear projections. The nodes then transmit the compressed data or projection value to the BS. The BS generates a projection vector based on the node-address and combines it with the received projections from the source nodes to decompress the sensed data.

Distributed Source Coding Techniques (DSC): DSC tries to optimally compress the sensed data from correlated source nodes that neither communicate with each other, nor are co-located. For example, in multi-camera surveillance systems and in applications that require different sensors monitoring weather and seismic activities, data from correlated sensors are compressed by separate encoders. DSC techniques are based on the Slepian-Wolf coding theorem. As per this theorem, for a given set of data compression rates for both independent and identically distributed encoded data from multiple correlated sources, the original data is reconstructed losslessly by a joint decoder.

3.2.2. Data fusion

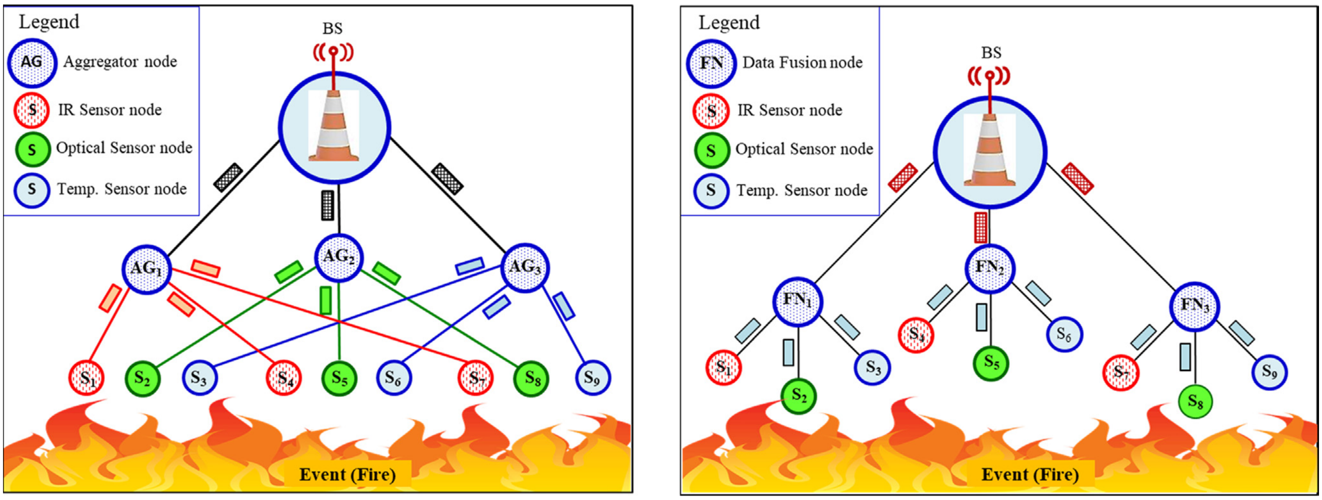
While data fusion and data aggregation and are often used interchangeably (Sridhar et al., 2007) data fusion is generally understood as a broad area that encompasses aggregation as well. Data fusion is a process by which, data from heterogeneous sensors are combined together to arrive at better correlations or inferences (Abdelgawad and Bayoumi, 2012).

To illustrate the functional differences of data aggregation and data fusion approaches, consider a WSN deployed to monitor the occurrence of fire in a forest as shown in Fig. 6(a) and (b). For better accuracy, and to pinpoint the location of fire, the WSN deploys three types of sensor nodes viz., (a) IR sensor to detect the location and spread of fire, (b) RTD/thermocouple sensor to detect the rise in temperature, and (c) optical sensor to act as a visual aid to validate the sensed data. Even though, all sensor nodes, in effect monitor the occurrence of fire, the sensing mechanisms and the purpose for which they are deployed are different. Due to the non-homogenous nature of the three sensors, the data sensed need to be aggregated separately. As illustrated in Fig. 6(a) the information from IR, Optical and RTD/thermocouple sensors are aggregated separately by aggregators AG$_1$, AG$_2$ and AG$_3$ respectively. The BS assimilates the aggregated data from different types of sensors, and determines the nature, spread and extent of fire. Unlike data aggregation, which aggregates homogeneous data, data fusion is capable of integrating data from different types of sensors. Accordingly, the fusion nodes FN$_1$, FN$_2$ and FN$_3$ fuse the data sensed by three types of sensors to infer the intensity and spread of fire as shown in Fig. 6(b). Therefore, the BS, need not carry out further analysis as the inference drawn by the FNs is reasonably complete.

3.3. Data aggregation in IoTs

Ready availability of high speed networks in the form of 4G and 5G technologies, and the market pull toward producing smart and internet-enabled devices has brought a paradigm shift in the way multiple devices are networked together on an internet cloud platform. Due to this shift, IoT networks are increasingly being used in diverse range of application domains. Having emerged as an extended version of WSN, the concepts developed for WSN can readily be assimilated into the IoT networks. Several data aggregation algorithms developed for WSNs are being tailored to suit the requirements of IoTs. The basic difference between data aggregation techniques employed for WSN and IoT, is the data generated by the nodes in respective networks. In WSNs the data generated by all nodes is singularly in tune with the intended application. Hence, the sensor nodes usually follow uniform data packet format for communication. However, in IoTs due to the diversity in the network devices, there are wide variations in the data format.

In large IoT applications the volume of data and velocity of data impinging on the network is humongous and can often be classified as big data. Further, the authenticity of data can at times be questionable. To handle such scenario, data aggregation mechanisms need to embrace the data handling concepts of big data. For collection of data, IoTs rely on a set of distributed ANs that forward their aggregates to multiple BSs (Fitzgerald et al., 2018). IoTs also rely on compressed sensing in applications where the IoT devices have embedded signal processing tools for data acquisition and signal reconstruction. Compressed sensing techniques can function efficiently in applications where the IoT devices have these advanced features (Zhang et al., 2021b). However, most real-life applications have mix of advanced as well as ordinary devices, where energy efficiency and recovery fidelity are often compromised. To get over this problem, a Light Weight Compressed Data Aggregation (LWCDA) algorithm, was developed in Amarlingam et al. (2018), where the network is fragmented into non-overlapping clusters of similar devices. Such clustering facilitates localized compressed sensing in clusters that have advanced devices, and leads to lower data transmission rates for exchange of data aggregates between the clusters. A major challenge in large IoT networks comprising heterogeneous wireless sensors and IoT devices, is the intermittent and random nature of task arrival rates. To model such application, Metzger et al. Metzger et al. (2019) present a detailed study on how to correlate the IoT network properties with different types of network traffic and task arrival rates, by assuming a Poisson distribution process. Based on their study,



(a) Data Aggregation (b) Data Fusion

Fig. 6. Data Aggregation and Data Fusion.

they propose few guidelines for optimizing the data aggregation process.

With ready availability of internet cloud services, IoT networks started utilizing low-latency fog devices. The fog devices which are located in close proximity with IoT edge networks, play a crucial role in optimizing computation & communication overheads, throughput and storage space (Ullah et al., 2020). Due to the presence of several heterogeneous devices that perform data aggregation utilizing the cloud services, the need to provide pervasive security and privacy are of prime importance. A popular scheme to preserve privacy during data aggregation is the data slicing approach (Pu et al., 2019). In this approach, the AN randomly slices its aggregate into n segments and performs symmetric encryption on each of the slices, retains one slice for itself and forwards the encrypted slice to other $n-1$ ANs in its group. A group node then adds up all slices and forwards the same to its group aggregator by employing homomorphic and AES encryption.

Advances in network infrastructure services in the form of cloud and 5G have resulted in manifold increase in the range and potential of WSN and IoT applications. With rapid proliferation of connected devices in the form of wireless sensors, mobile phones, IoT devices, etc. in all spheres of human activity, humongous amount of data is being shared across the network. To handle the voluminous amount of data being generated by the connected devices, data handling techniques such as AI & ML, deep learning, edge computing are increasingly being used (Zhu et al., 2021). Due to large variability in the devices used for IoT applications, centralized cloud computing may be a limiting factor to satisfy QoS for some data-driven applications. To address this limitation, there is a need to bring computing and storage resources closer (edge) of the IoT/sensor devices. Due to limited availability of storage space, IoT devices involved in processing big data utilize cloud services for data storage and data retrieval. However, frequent access to cloud leads to higher computational & communication overheads and faster depletion of node energy. Edge computing supports distributed data aggregation on one hand, and on the other facilitates localized computation. It ensures uniform availability of resources across all devices in the IoT network by bringing data storage resources to the edge of the network. This results in substantial reduction of computation and communication overheads leading to increased network lifetime (Lin et al., 2017; Xue et al., 2020; Ren et al., 2019; Ghosh and Grolinger, 2021).

3.4. Classification of data aggregation protocols and approaches

Data aggregation protocols define the standard operational procedures to (a) aggregate the sensed data based on aggregation function, (b) handle the communication of data & control messages, and (c) route the aggregates to the BS/internet cloud. The major objectives of data aggregation protocols are: to eliminate redundant data transmission from source nodes to BS/internet cloud, to maintain the accuracy of the data while performing aggregation, and to improve the lifetime of WSN/IoT. Considering the diversity of application and widely varying nature of operation, we classify the data aggregation protocols based on: (a) WSN/IoT topology, (b) interference and fault-tolerance models (c) security & privacy, and (d) mobility. A taxonomy of data aggregation protocols based on above classification is illustrated in Fig. 7.

4. Topology-based data aggregation protocols

The network topology has a large role to play in devising data aggregation strategies in WSN/IoT applications. In this section we review the data aggregation protocols for hierarchical and non-hierarchical based network topologies.

4.1. Data aggregation protocols based on flat networks

In Flat networks, there is no fixed topology or any hierarchy amongst the nodes. Although there are several variations, the sensor nodes in Flat topology-based WSN, are assumed to possess uniform capability in terms of their battery power, communication range and processing capability. However, the devices in IoT networks based on Flat topology have widely varying capabilities. Each node in this topology maintains the network state information (NSI) of its one-hop neighbors. Based on this information, the nodes coordinate to sequence and route their communications to the BS. Depending on the mechanism employed to avoid resource contention while communicating with their neighbors, the topology can be classified into: (a) Flooding, (b) Forwarding and (c) Data-centric routing schemes.

Flooding: In Flooding, every node broadcasts the data packet it receives to all its neighbors except the one from which it has received the data. This process is repeated until all nodes in the network receive a copy of the packet. While flooding is an effective mechanism to quickly disseminate the information, it suffers from problems like:

- Implosion: A node may receive several copies of the same data from multiple neighboring nodes.
- Overlapping: Two or more nodes may sense the same region of interest. Due to this, the nodes may receive similar information from multiple sensor nodes.
- Resource blindness: A node may unnecessarily use network resources for both receiving and sending data.

Forwarding: In forwarding scheme, the intermediary nodes maintain only one-hop neighbor information and data is forwarded to a randomly chosen neighboring node. This scheme reduces the overhead of maintaining end-to-end (from source to sink) routing information. In any given round, a node receives only a single copy of the data, and in the next round it forwards it to only one of its neighboring nodes. Thus, if there are n_s source nodes in the network, the fastest distribution rate is n_s nodes/round.

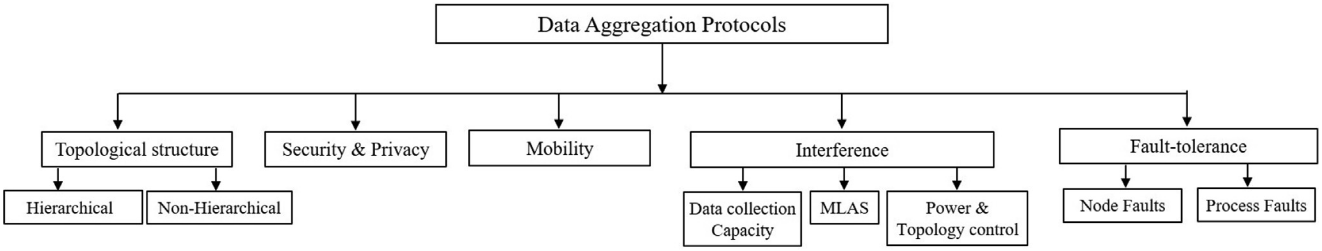


Fig. 7. A taxonomy of data aggregation protocols.

Although the data distribution rate is slow, the main advantage of this protocol is that the nodes dissipate energy at a slow rate. As the number of packets being transmitted is relatively small compared to Flooding approach, the Forwarding approach amicably addresses issues related to implosion, overlapping and resource blindness.

Data-centric: In Data-centric approach, data is aggregated regionally by a set of nodes in that region. On receiving a query from BS, the aggregator nodes in the region relay the aggregate to BS. Since the query carries attributes of the data to be aggregated, it can be directed to the nodes that can serve the query based on data-centric addressing scheme. This obviates the need to search through all the nodes in the network based on node identity. Amongst various data aggregation protocols for WSN with flat topology, SPIN (Sensor Protocols for Information via Negotiation) is the most popular (Heinzelman et al., 1999). SPIN protocol tries to address the deficiencies of flooding mechanism, viz. implosion, overlapping and resource blindness through negotiation and resource adaptation. A source node in SPIN advertises the data it proposes to transmit by broadcasting ADV message that contains a metadata, which is a high-level data descriptor with one-to-one mapping to the data sensed by the source node. The nodes that receive ADV message, study the metadata and respond with a REQ message only if they have interest in the data. Making use of DATA message, the source node on receipt of REQ from neighboring nodes, sends its information only to the nodes that have shown interest. This process is recursive and it terminates after all nodes that have responded to ADV message with REQ, transmit their DATA. Depending on the mechanism adapted by the nodes for negotiation, resource allocation, energy conservation, security etc., several variants of SPIN like SPIN-EC, M-SPIN, S-SPIN, SPIN-RL (Kulik et al., 2002; Rehena et al., 2011; Tang and Li, 2009) were proposed. Taking advantage of flat topology, SPIN and its variants accommodate minor topological changes to interact with any of its one-hop neighbors. This feature however, has not been exploited to its potential in IoT networks and SPIN has remained largely confined to WSNs.

4.2. Data aggregation protocols for Hierarchy-based networks.

In most hierarchy-based WSNs, the sensor nodes are located in different hierarchical layers in relation to the BS. The protocols exploit the self-organizing feature of the WSN to restructure the network into hierarchical topologies, such as chain, tree, grid, cluster, etc.

In chain-based data aggregation protocols, a chain-like structure is constructed between BS and the nodes. The linkages between the chain of nodes are established either centrally by the BS, or in a distributed manner by the nodes. Each node in the chain performs aggregation on the information received and transmits the aggregate to its nearest neighbor in the chain instead of directly sending it to BS. This conserves energy as the nodes need not transmit the data to the BS which is relatively far away. PEGASIS (Power-Efficient optimal chain-based data-GAthering protocol for Sensor Information Systems) follows greedy algorithm to organize the nodes in the form of a chain (Lindsey et al., 2002). A node far away from the BS initiates the construction of chain. If a chain is broken due to a dead node, the chain is reconstructed by bypassing the dead node. One amongst the chain of nodes is randomly elected as the leader and is assigned the task of communicating the aggregates to the BS. Thus, a leader once elected, it continues to lead the chain till all aggregates computed by the nodes in the chain reach the BS. Chain-based protocols, thus are simple and relatively easy to operate. However, these protocols may not be attractive in large networks.

Data aggregation protocols for tree-structured WSN rely on the construction of energy-efficient data aggregation trees, where the data is aggregated by the non-leaf nodes layer-by-layer along the path to the root node. The Tiny AGgregation (TAG) protocol and the Power Efficient Data gathering and Aggregation Protocol (PEDAP) are the most popular data aggregations protocols for tree-structured WSNs. TAG protocol is suitable for low-power wireless environments (Madden et al., 2002). In TAG, the BS initiates a query, and a tree is created in the order in which the query propagates through the network. The query semantics partition the time into fixed-sized epochs. TAG operates in two phases: distribution and collection phases. In the distribution phase, each node pushes a query to its child node and specifies the time interval during which the child node needs to respond back. In the collection phase, the parent node computes partial state record based on the information received from its child node, and transmits this aggregate to a higher order node in the hierarchical tree. The collection phase ensures that parents in the routing tree listen for longer period than their specified transmission interval. This is done to offset the clock synchronization mismatches if any. Further, to save energy, nodes that remain idle in a given interval of an epoch enters into a low power state.

In PEDAP (Tan and Korpeoglu, 2003) the BS initiates the construction of minimum spanning tree (MST). Data is aggregated by the intermediary nodes and the aggregate is routed along the edges of the MST to the BS. However, due to the workloads involved, the aggregator nodes deplete their energy faster than other nodes. To offset this, the construction of MST is periodically initiated after few rounds of aggregation, by taking into account the residual energy level of the nodes. Compared to PEGASIS, PEDAP performs better in applications where the BS is inside the sensing field, as the MST so formed has relatively less number of levels compared to the case where the BS is outside the sensing field. The root aggregator spends less energy for transmitting data to the BS, thus minimizing energy consumed and maximizing the network lifetime.

In grid-based data aggregation, the deployment region is geographically segmented into grids with multiple sinks. The sinks aggregate the data from the nodes mapped to a grid(s) closest to it. The sink that is centrally located is chosen as the primary sink (PS), which performs aggregation on the aggregates computed by its sub-ordinate sinks (Wang et al., 2013).

For large WSNs and IoT networks, the coordination amongst various nodes and devices networked in the form of either chain, tree or grid poses several complications. To get over these complications, the mechanism to group the nodes into clusters, or the ‘clustering approach’ has emerged as the most popular hierarchy-based protocols. In this approach, the WSN and IoT devices are grouped into hierarchical clusters, where the proximity of a cluster to its BS determines its level in the hierarchy. The formation of clusters is usually based on the geographical proximity of a set of nodes. The nodes in a cluster designate one amongst them as their Cluster Head (CH) to which they route their sensed data. To facilitate this, the cluster nodes network themselves into a star, tree, chain or grid topology. The CH aggregates the data received from its fellow cluster nodes and routes the aggregate to the BS. Depending on its proximity to the BS, the CH either directly transmits its aggregate to the BS or routes it through neighboring CH nodes. Due to the dual responsibility of performing data aggregation on one hand, and relaying the data received from its fellow CHs to the BS on the other hand, the CHs in cluster-based hierarchical network tend to deplete their energy much faster than other nodes in the network. To counter this, most data aggregation protocols centre their strategies on (i) optimal cluster formation, and (ii) on how to elect a CH with higher residual energy; so as to prolong the lifetime of the network. Based on the strategies used, the data aggregation protocols based on cluster hierarchy can be broadly into (a) adaptive cluster formation, (b) energy-efficient distributed clustering and (c) bio-inspired methods for clustering and CH selection; which are briefly enumerated below:

4.2.1. Adaptive clustering (AC)

In AC, the nodes that are in close proximity with one another form a cluster, with one of the node randomly chosen as the Cluster Head (CH) through an election process. The most popular amongst the protocols developed through AC approach are the Low Energy Adaptive Clustering Hierarchy (LEACH) protocol (Heinzelman et al., 2002). LEACH uses this method to form adaptive, self-configuring clusters with localized control, and application-specific data aggregation or compression techniques. One node in the cluster so formed, assumes the role of a CH, through an election process. The cluster nodes transmit their sensed data to the CH, which performs aggregation and routes the aggregate to the BS. Due to this, the computational and communication load of CH is much larger compared to other non-CH nodes. If the CHs are fixed for the entire network lifetime, they would eventually end up losing all their energy and the cluster collapses once the CH dies. To counter this, LEACH incorporates randomized selection of CH from time-to-time to ensure consistent energy dissipation among network nodes.

LEACH follows a dynamic clustering mechanism, where for each round of operation, a different set of clusters are formed. Each round comprises two phases, the first being the cluster formation phase and second, the data aggregation phase. In the cluster formation phase, the CHs implement CSMA mechanism to send advertisements to their neighbors. The neighboring nodes decide to associate with their closest CHs. Conflicts due to multiple associations are resolved randomly. The number of CHs required depends on communication versus computation tradeoff. Based on this consideration, an optimum number k of CHs is determined so as to cover the entire SDR. A lower value of k indicates that the cluster nodes are far away from their CH. Therefore, they need to expend more energy to transmit their data to the CH. On the other hand if k is large, the number of transmissions between the CHs and BS, and the associated communication overhead is quite large. On a relative scale, the cost (in terms of energy) for the construction of clusters in LEACH appears to be higher than the construction of an MST as in the case of PEDAP. However, since the cluster nodes communicate only with the CH during the entire lifetime of the cluster, the energy spent by them is much lower compared to the energy spent by nodes in PEDAP, where the MST is reconstructed periodically. Depending on the methodology adopted for cluster formation, CH selection and communication mechanism; several variants of LEACH were developed.

4.2.2. Energy-efficient distributed clustering

In this method of clustering, the cluster node is selected based on the node's residual energy. In the Hybrid Energy Efficient Distributed Clustering (HEED) protocol, all nodes are assumed to have similar functionality and possess discrete transmission power levels. Unlike LEACH, the node with maximum residual energy and minimum communication overhead is selected as the CH. The neighboring nodes are mapped based on their proximity to the CH. However, if a node falls in the range of two or more CHs, the CH with minimum intra-cluster communication overhead is chosen as its CH. Intra-cluster communication overhead is a function of cluster size and the transmission power required by each node to communicate to the CH. A node always opts for a CH that is closest to it, i.e., the one with minimum power to reach CH.

The clustering approach in HEED attempts to evenly distribute the energy consumption load among the nodes in order to extend the network lifetime. Thus, the primary objectives of HEED are to (i) enhance the network lifetime by even distribution of energy consumption load, and (ii) reduce the processing overhead by terminating the clustering process after finite number of iterations.

Both LEACH and HEED have emerged as popular protocols for hierarchy-based networks and have attracted the attention of researchers to devise several variants. Few other popular hierarchical topologies including the variants of LEACH and HEED are briefly highlighted in Table 4.

4.2.3. Bio-inspired CH selection and clustering

In most hierarchy-based WSNs and IoT networks, the selection of CH plays an important role in network efficiency. The selection of CH is generally based on parameters such as (a) its proximity to the BS, (b) hop-distance of cluster nodes, (c) residual energy of the node under consideration, (d) computation and communication load, (e) cluster density, etc. If these parameters can be accurately determined, a multi-optimization function can be built, based on which CH selection can be made. However, these parameters are non-deterministic in nature due to highly diverse characteristics of the heterogeneous nodes in terms of energy requirements for computation & communication and dynamic behavior of the nodes in terms of mobility. Further, the parameters used to build the optimization function may have contrasting objectives. Therefore, the development of an optimization function to determine the CH may not be a viable proposition. To get over this problem, several bio-inspired techniques such as: Multi-objective Optimization Algorithm (SMS-EMOA), Non-dominated Sorting Genetic Algorithm (NSGA-II), S-Metric Selection Evolutionary and Multi-Objective Evolutionary Algorithm by Decomposition (MOEA/D) were used for selection of CH. In these approaches an initial fitness function is defined based on multiple optimization parameters of interest, and then the solution space is determined. The fitness function is determined iteratively, to determine the best fit (Miranda et al., 2019; Nayak et al., 2019; Wang et al., 2019; García-Nájera et al., 2011). Glow-worm Swarm Optimization (GSO)and Krill Heard algorithm, a bio-inspired technique was used to form clusters of unmanned aviation vehicles (Khan et al., 2019). In this technique, the residual energy level and motion of the unmanned vehicle were considered to be the prime parameters to determine the fitness function. Whilst the residual energy was considered to be the luciferin level, the motion is represented as lucipherase in the fitness function. After multiple iterations, the best fitness function is evaluated and the object (unmanned aviation vehicle) with best luciferin was selected as the CH. In terms of parameters such as cluster lifetime and residual energy, the CH selection based on this approach was found to be better than Germinal Centre and Ant Colony optimization approaches. Honey Bee algorithm (HBA) is another popular approach proposed for cluster formation and CH selection. In BeeWSN based clustering approach the nodes were considered to be the *source* of food for the bees, and the control packets used for communication in a network were considered to be the *onlooker bees* (Ahmad et al., 2018). The packets of data (other than control packets) transmitted across the network were considered to be the *employed bees*. Data collection represented the *necta*r to be collected by the *employed bees*. The *onlooker bees* were made responsible for identifying the best *source* of food (nodes) based on a fitness function, that considers quantity of food available (node energy) speed and direction (mobility and location of the node). Based on the evaluation of the best fitness function the node with optimal energy and closeness to other member nodes was selected as the CH. The study considered performance metrics based on (a) throughput at various mobility rates and node densities, and (b) end-end delay. In comparison with other approaches like new LEACH and ANP, the BeeWSN approach was found to be better.

Table 4
Data aggregation protocols based on hierarchical topology.

Protocols	Network Structure	Description and operational mechanism	Advantages and Limitations
HexDD (Erman et al., 2012)	• Virtual grid infrastructure and honeycomb tessellation. • Hexagonal grid with homogeneous nodes • Multiple sink with random mobility	• Query matching invokes data transmission in reverse path to BS. • Diagonal forwarding paths among source and BS pairs allow convergence of similar data at common border nodes. • Balanced traffic flows in all regions	• Suitable for Intelligent IoT • Reduced cost of data look-up and low latency • Borderlines and center cell nodes are hotspot nodes
hetHEED-1, 2, 3 (Chand et al., 2014)	• Cluster-based • In hetHEED-1 all sensor nodes have uniform energy levels. • In hetHEED-2 the nodes have two energy levels while in hetHEED-3, nodes have three energy levels.	CH selection considers node's residual energy and cluster node density.	Order of protocols in terms of network lifetime and minimal energy dissipation: hetHEED-3 > hetHEED-2 > hetHEED-1
hetHEED-FL-1, FL-2, FL-3 (Chand et al., 2014)	• Cluster-based • Do not require precise value of node's residual energy for CH election.	CH selection is based on fuzzy logic metrics like (i) residual energy (ii) node density and (iii) proximity of a node to BS.	Order of protocols in terms of network lifetime: hetHEED-FL-3 > hetHEED-FL-2 > hetHEED-FL-1
TCBDGA (Zhu et al., 2015)	• Tree cluster-based topology • Homogeneous and heterogeneous static nodes with a mobile sink and a static BS. • Advanved sensor nodes classified as Renedezvous Poins (RPs) and Sub-Rendezvous Points (SRP).	• Parameters for weighted trees: residual energy of 1-hop neighbor, number of its 2-hop neighbors, and distance to mobile BS. • RPs and SRPs act as local data aggregation points and stop points for the mobile sink. • RPs and SRPs are reselected after few rounds of data collection. • Mobile sink moves in the field periodically from the BS to collect data.	• Evenly distibutes network load • Balanced energy consumption and prolonged network lifetime. • Suitable for wide area applications, viz., industrial IoT involving massive amount of heterogeneous sensory data.
Energy Efficient Modified LEACH (Behera et al., 2018)	Cluster-based	• Nodes bid for CH selection by generating a priority value. • Predefined threshold energy limit is used for CH selection. • CH can re-assume the role as CH if its energy is greater than predefined threshold energy limit	• More suitable for IoT applications compared to traditional LEACH
Modified Leach (Nguyen et al., 2019) LA-RPL (Homaei et al., 2019)	• Cluster-based • Sensor nodes equipped with self-adjustable transmission range • Tree-structured network • Homogeneous static sensor nodes with one sink/BS, • Dynamic data aggregation approach • Sink node acts as root	• CH performs neighbors' discovery • Degree of CH is set to the maximum number of member nodes • Node-degree restriction on each parent node, to limit the number of child nodes depending on the network application type. • Nodes are equipped with learning automata to perform data aggregation and transmissions. • Data aggregation or direct data is decided on two factors: status and congestion of the received packets at a node. • Aggregation of some data packets at lower layer data aggregators do not allow aggregation of the same packets at higher layer data aggregators.	• Suitable for dynamic network • Adjustable transmission range ensures network connectivity. • Evenly distributed child nodes to balance network load • Avoids multi-step aggregation and reduces upward average delay. • Height of network tree is scalable. • Suitable for reduction of excessive exchanges and routing load in IoT.
LEACH-VA (Liang et al., 2019)	• Cluster-based, multi-hop routing with homogeneous sensor nodes for data collection, fusion, and forwarding and a BS. • Optimal number of CHs are selected.	• CHs act as regional point of the Voronoi Diagram. Nodes in same Vornoi form a cluster. • Uniform clusters and intra-cluster communication is less. • Uses ant colony optimization algorithm to select transmission path and reduce energy consumption due to long-distance/direct data transmission.	• Increased energy-efficiency per unit node per round and network lifetime compared to traditional LEACH. • Reduces network load. • Suitable for WSN-enabled intelligent IoT networks.
FOI-LEACH (Huo et al., 2020)	Heterogeneous networks with rechargeable field instruments.	Node's residual energy, rechargeable energy of nodes and proximity with BS is used as parameter for CH selection.	• Alleviates the hot spot problem and prolongs lifetime of network nodes. • Suitable for mobile IoT devices to enhance their routing capability.
MAI-LEACH (Vasan et al., 2021)	• Cluster-based, uses mobile agents for the collection of CH data.	• An enhancement of I-LEACH(improved-LEACH) • Improved clustering scheme based on optimal number of CH selection and mobile agents.	• Improved energy efficiency and throughput than I-LEACH • Prolonged network lifetime • Suitable for IoT applications with mobile agencies.
S-LEACH (Sectored LEACH) (Mohammed et al., 2022)	• Network region is divided into sectors. • Sectored network reduces transmission distance, limits sensing and transmitting area.	• Self-organized CH selection is based on the node's residual energy without BS contribution. • Ensures uniform energy consumption during distribution for CH.	• Sectored network minimizes energy consumption and prolongs network lifetime. • Use of Particle swarm optimization (PSO) algorithm and genetic algorithm (GA) techniques for node distribution can improve IoT network lifetime and attain high packet delivery ratio.

(*continued on next page*)

Table 4 (*continued*)

Protocols	Network Structure	Description and operational mechanism	Advantages and Limitations
EERP (Lokhande and Patil, 2022)	• Cluster-based, M2M network with static heterogeneous intelligent IoT devices and a single BS/medical center. • Uses LEACH protocol	• Clustering done autonomously to identify a node as CH and cluster member (CM). • Improved clustering process where legitimate nodes are identified based on trust score parameter. • Trust score for each node is calculated periodically.	• Suitable for tele-robotic surgery and M2M communication between medical devices. • Prolonged network lifetime and more energy-efficient and scalable than LEACH.

5. Addressing interference and fault-tolerance issues in data aggregation

In order to facilitate energy-efficient wireless communication, the low-cost sensor nodes resort to short-range communication. Due to this necessity, the closely located nodes in WSN are prone to radio interference while transmitting or receiving data from other nodes. In addition, due to the presence of large number of wireless devices, the WSN and IoT applications are prone to a variety of faults. The data aggregation protocols/algorithms that address issues related to interference and fault-tolerances are reviewed in this section.

5.1. Data aggregation techniques to address interference

Communication between two nodes is hampered if their signal transmissions are interfered due to ongoing transmissions between other closely located active nodes. Due to the interference phenomenon, noise is induced into the signal received and the destination node receives distorted/corrupt or *interfered* signal (Gupta and Kumar, 2000; Cardieri 2010; Begum and Nandury, 2015; Begum and Nandury, 2022b). The Protocol Interference (Pr_I) and Physical Interference (Ph_I) models have emerged as the most popular protocols to model interference in WSN.

The Pr_I model helps in defining the basic conditions in terms of Euclidean distance between a destination node and an active unintended source node, in order to avoid interference. As per this model, the minimum Euclidean distance between a destination node D_i and any other unintended active source node S_j for successful communication, must be greater than interference range R_I of D_i,. i.e. $dist(S_j, D_i,) \geq R_I$.

The Ph_I model helps in deriving schemes to estimate the minimum Signal to Interference plus Noise Ratio (SINR) threshold conditions for successful communication between a source–destination pair, amidst the presence of noise (background & network induced), path-loss/gain due to transmission medium and transmission power. For a source–destination pair (S_i, D_i), the power of the signal received by D_i is given by:

$$P_{D_i}(S_i) = P * min\left(1, dist(S_i, D_i)\right)^{-\alpha})$$

where $dist(S_i, D_i)$ is the Euclidean distance between S_i and D_i, and $\alpha \geq 2$ is the path-gain exponent. As per the Physical Interference model, the SINR threshold β for successful communication between (S_i, D_i), is given by:

$$SINR_{D_i}(S_i) = \frac{P_{D_i}(S_i)}{N_0 + \sum_{S_j \in N'} P_{D_i}(S_j)} \geq \beta$$

where $N_0 \geq 0$ is the varying background noise and S_j is the set of transmitting nodes N′ other than D_i i.e. $(N' \epsilon (N - D_i))$, that transmit in the same timeslot as that of S_i. The term $\sum_{S_j \in N'} P_{D_i}(S_j)$ is the network induced noise due to all other active nodes in the network.

The Pr_I and Ph_I models have emerged as the basic foundation on which several data aggregation algorithms that attempt to mitigate data corruption due to interference were developed. IoTs being an extended network of several wireless devices and WSNs, the data aggregation schemes developed for WSNs can readily be customized for IoT applications.

5.1.1. Classification of data aggregation techniques that address interference

To mitigate the effect of data corruption due to interference, data aggregation algorithms need to consider both pair-wise terminal interference, as well as cumulative/additive interference from other ongoing transmissions. The most popular approaches to handle pair-wise terminal interference are the transmitter-centric and receiver-centric approaches. In transmitter-centric approach, a transmission is considered to be successful if the distance between any two source nodes is more than the carrier-sense (CS) range. Therefore, the source nodes that are located within the CS range of each other are considered to be potential interferers. On the other hand, in receiver-centric approach, any source node that is within the interference range of a destination node is considered to be a potential interferer. Based on the two approaches, the potential interferers so identified are scheduled either in separate timeslots or on orthogonal frequencies. In cumulative/additive interference model, all nodes in the network are considered to be potential interferers. If the extent of interference caused by cumulative interference as estimated by Ph_I model is significant, the interfering transmissions need to be scheduled separately to minimize the interference. Based on these broad concepts several data aggregation approaches were developed that focus on reducing interference and improve aggregation efficiency, such as (a) enhancing data collection capacity, (b) minimizing latency to solve MLAS problem, (c) scheduling complexity and link coloring for link scheduling, (e) transmission power control, and (f) topology control. We present a brief review of algorithms to illustrate the methodology followed in mitigating interference in each of the above categories.

- Enhancing data collection capacity

The ability of a network to collect interference-free sensor data in a given time interval is termed as 'data collection capacity' and is expressed as number of non-interfering bits/second. This metric is often used to study the capability of a scheduling algorithm in maximizing the number of non-interfering concurrent transmissions. This metric is a measure of the capability of the algorithm in maximizing the collection of interference-free data aggregates at the BS with a minimum time delay. An in-depth study was conducted by Chen et al. Chen et al. (2012b) to establish theoretical lower and upper bounds of data collection capacity with and without aggregation, by considering Ph_I and Pr_I model and unit disk-graph models in arbitrary WSNs. The study assumed uniform transmission & interference ranges, data packet size and data transmission rate across all models. Further, the study assumed that there exist no spatial correlations amongst the sensed data. To calculate the upper and lower bounds, the study considered the paths $P_1, P_2, \cdots, P_z$ from the leaf nodes n_1, n_2,. . . , n_z to the BS. If Δ_i is the *maximum interference number* of path P_i from the leaf node n_i, the number of timeslots τ_i necessary to collect a data packet in the path is given by $\tau_i = \Delta_i|P_i|$, where $|P_i|$ is the path length expressed in the form of number of hop-counts in the path P_i. In order to estimate the total number of timeslots τ required to collect data from all nodes in the network, the study considered the maximum interference number of all paths $\Delta = max\{\Delta_1, \Delta_2, \cdots, \Delta_z\}$. Thus, $\tau = \Delta n$, where N is the number of nodes along all paths. For a packet size of b bits and transmission rate of W bits/sec, the length of each slot $t = b/W\ sec$, and the total delay D for collecting data from all nodes is given by $D = \tau t$, where τ is the sum of all timeslots. Thus, the study determined the data collection capacity C for all z paths $C = N * b/D = W/\Delta$. Therefore, the upper and lower bounds of data collection capacity of BFS-tree path scheduling algorithm is $\Theta(W/n)$ and upper-bound is $\Theta(W)$ under Pr_I model. However, with pipelined aggregation the sensors start aggregating snapshot data for the next round of data collection before the previous round aggregated data reaches the sink. The pipelined aggregation scheduling attains an upper bound delay rate of $\Theta(\sqrt{n(\log n)W})$ and collection capacity $= \Theta\left(\frac{n}{\log n}W\right)$. While the study develops the foundations to develop the data collection capacity, it does not provide mechanisms on how to ensure that there are no spatial correlations amongst the sensed data.

The Minimum Latency Collection Scheduling (MLCS) problem is used to arrive at the computational complexity of algorithms that determine an optimal data collection schedule. An and Cho (2015) discuss Hop-Based Collection Scheduling (HBCS) algorithm for the MLCS problem that can be applied to both graph model (collision-free graph model or 3-distance matching model) and the Ph_I model. HBCS algorithm starts by partitioning the network into sectors and then constructs an interference graph for generating an interference tree, along with a data collection tree (BFS- tree) rooted at the BS. The data collection tree is divided into number of subtrees. HBSC iteratively assigns timeslots to nodes in the subtrees based on interference graph, such that any two concurrently transmitting nodes are spatially separated by a distance of at least 3 R_T to allow data collection from all the other nodes without any collision or interference. To avoid interference, the transmission power is restricted and only the links with length less than $\left(\frac{P}{\beta N_0}\right)^{-1/\alpha}$ are considered for simultaneous transmissions. The latency of the algorithm is bounded by $O(n)$ time slots and can further be improved by employing data aggregation. A methodology to determine the theoretical upper and lower bounds of data collection capacity and delay in WSNs based on grid structure, with and without data aggregation, is presented in Chen et al. (2011). The study considered the cases where the sensor nodes are deployed either randomly or uniformly in the grid comprising single (multiple) sink(s).

- **Minimum Latency Aggregation Scheduling (MLAS)**

The MLAS class of algorithms aim to limit the number of timeslots to aggregate the data while attempting to avoid aggregation of interfered data (Li et al., 2014). Most MLAS algorithms rely on constructing CDS-based aggregation tree as discussed in Wan et al. (2004), to find an optimized schedule of transmission links that minimizes latency. Maximal Independent Set (MIS) based Connected Dominating set (CDS) was used to construct a virtual backbone for determining an optimal schedule (upper bounds and lower bounds of latency in time slots) for the design of constant-approximation data aggregation algorithms in WSNs. CDS reduces redundant connections, and limits the aggregation to nodes (connectors and dominator nodes) in the CDS. To address the MLAS problem Wan et al. (Wan et al., 2009) have developed three CDS-based centralized TDMA data aggregation algorithms (SAS, PAS and E-PAS) for achieving shorter latency, under the assumption that $R_I \geq R_T$. The study also derived the theoretical upper bounds for latency. Bagaa et al. (2012) have discussed two centralized TDMA data aggregation scheduling (DAS) approaches DAS-ST and DAS-UT using MIS-based CDS structure to solve MLAS problem under Pr_I model with $R_I = R_T$. The approach allows a wider scope for parent selection from any neighboring node irrespective of the node level (same, higher or lower levels) unlike CIAS and DIAS approaches where parent can be selected only if they at same or higher levels. In addition, the nodes already scheduled can also act as a parent node. Further, to reduce latency, the construction of aggregation tree and allocation of time slots can be taken up simultaneously. Centralized algorithms are not readily scalable. The BS needs to reconfigure the network, when there is a change in the network topology or in cases where either a new node has to be accommodated or when an existing node departs form the network. In comparison, distributed networks are scalable and the costs involved in communication and computation overheads are relatively low while accommodating changes in the network.

Time Division Multiple Access (TDMA) is a popular mechanism that facilitates multiple nodes to access the same frequency without interference, by segmenting the signal into multiple timeslots. A popular TDMA approach to address interference is to organize the network into a CDS-tree rooted at a topological center (different from sink). With CDS-tree as the backbone network topology, a TDMA based Centralized Improved Aggregation Scheduling (Centralized-IAS) approach was developed in Xu et al. (2011b). In this approach, each dominator in the CDS tree identifies the set of dominators that are two-hops away. The dominators higher in hierarchy, collect the data from the lower-level dominators with the help of connectors, to perform aggregation. This aggregate is then forwarded to higher-level dominators. The aggregation process progresses level-by-level in a bottom–up manner till the BS receives an aggregate of the data from all its sensor nodes. However, this approach is not scalable as it is totally dependent on the CDS tree structure. To counter this, a Distributed-IAS was developed to aggregate data in an inter-leaved manner. Each node in the CDS tree maintains information about its active neighbouring nodes within its interference range, that are in contention for a TDMA schedule. These nodes are termed as ready-competitor nodes. A node is permitted to transmit only if it does not interfere with its own set of ready-competitor nodes. In D-IAS, data transmission by dominatees and aggregation at dominators occurs in an interleaved manner. This results in an increase in the number of simultaneous transmissions leading to reduction in latency and average transmission times compared to C-IAS. The latency is bounded by maximum degree of the dominator nodes (dominator aggregation degree) in the CDS.

The problem of reducing collisions and signal interference is often modeled as a coloring problem on the interference graph. Link coloring is a graph-based approach that is commonly employed in interference graph to distinguish sets of disjoint active links that can be scheduled in a given timeslot. In this approach, each set of links in the network graph that can be scheduled together without causing interference are given the same color. Nodes with different colors in the graph are assigned separate timeslots. Huang et al. (Huang et al., 2021) discuss a shortest link scheduling algorithm under the Rayleigh fading model (SLSRF) with fixed transmission power at the sender nodes. The SLSRF partitions the wireless network area into hexagons and colors the hexagons with three different colors such that no two neighboring hexagons have same color. The source nodes of the links scheduled simultaneously are arranged in hexagons with the same color. SLSRF jointly takes into account Rayleigh fading model and Ph_I model constraints to transform the global information about additive interference into local interference. SLSRF simultaneously selects one link from each hexagon with the same color, and this selection process is executed one by one to avoid link conflicts. X. Xu, et al, develped a link scheduling algorithm under the Ph_I model to minimize the delay for activating a set of communication links and data aggregation (Xu et al., 2011c). A weighted-constant approximation approach was used to define the upper and lower bounds of latency in multi-hop wireless networks. X. Jio et al. presented two approximations algorithms for aggregation-based link scheduling CDAS and SDAS under Pr_I model for duty-cycled (active/sleep) multihop WSNs in Jiao et al. (2012). J. Ma et al. presented an energy-efficient link scheduling algorithm for both homogeneous and heterogeneous WSNs to allow spatial reuse in Ma et al. (2014). The ratio of interference to transmission range was varied from 2 to 4. Energy consumption caused by nodes' state transitions was reduced by using sleep scheduling such that the nodes become active only when they are in transmitting or receiving mode or performing aggregation.

The amount of time required to schedule the communication requests of a topology depends on interference measure. A perspective of the scheduling complexity and connectivity in arbitrary WSN topologies with respect to static interference in the Ph_I model was studied in Moscibroda et al. (2006a). The time required to schedule the communication requests depends on the measures taken to address interference. The work theoretically establishes an upper bound of complexity on the time required to actually schedule the communication requests, in connected topologies comprising both symmetric and asymmetric communication links.

- **Transmission power control and topology control**

Transmission power control and topology control are two popular approaches employed to prevent unwarranted interference between sensor nodes in WSN. Based on Ph_I model a distributed data aggregation algorithm for tree-structured topology was developed by Li et al. (Li et al., 2009), to generate an interference-free aggregation schedule. In this approach, the depth of the aggregation tree and the dominators node-degree, define the upper-bound latency of the aggregation schedule under the Ph_I model. The network is modeled as a graph G(n,δr) of n nodes, where $r = \left(\frac{P}{\beta N_0}\right)^{-1/\alpha}$ is the distance between two nodes. The network is partitioned into grids of length $l = \delta r/\sqrt{2}$, where the configuration parameter $\delta \epsilon (0, 1)$, and r is the maximum achievable transmission range under the Ph_I model with constant power assignment. A communication link is formed if the Euclidean distance between two nodes $\leq \delta r$. Any attempt to increase the transmission power to reach-out to distances greater than δr, interferes other active transmissions. Based on this rationale, a distributed synchronous message passing MLAS-algorithm with unicast communication is developed that avoids primary interference. The grids are colored with $\left[\frac{4\beta\tau P\cdot l^{-\alpha}}{\left(\sqrt{2}\right)^{-\alpha} P\cdot l^{-\alpha} - \beta N_0)} + 1 + \sqrt{2}\right]$ colors where $\tau = \frac{\alpha\left(1+2^{\frac{-\alpha}{2}}\right)}{\alpha-1} + \frac{\pi 2^{\frac{-\alpha}{2}}}{2(\alpha-2)}$. The sender and receiver of links are colored by their locations in the grid and links are scheduled with respect to grid color. To ensure that the random network is connected with high probability, the degree of each node is of the order of $O(\log n)$. As we know, the longer the link, the smaller is the path-gain, thus a smaller SINR can be obtained by its corresponding receiver. Therefore, a long link with length comparatively close to r is not a good candidate for transmission, since the SINR experienced at the receiver is very small. Further, it prevents multiple simultaneous transmissions. In brief, a shorter link is a better candidate for the transmission to lower the interference. Node with the shortest network radius (smaller hop count) is chosen as the topology center. BFS is executed by the topology center over the network to build a CDS backbone for aggregation tree. It solves the MLAS problem in $O(\Delta + r)$ time slots. The performance of the MLAS algorithm is further improved by adopting a greedy compressive scheduling strategy where links scheduled in different timeslots can be merged into a single slot, such that there is no interference among the scheduled links. Merging multiple links into a single timeslot not only reduces overall number of timeslots required for aggregation, but also lowers latency compared to the distributed algorithm.

Two data aggregation algorithms Nearest-Neighbor Aggregation Scheduling (NN-AS) and Cell-AS, that attempt to limit the number of timeslots were developed in Li et al., (2014). The NN-AS algorithm follows a centralized approach to construct an aggregation tree in a phase-by-phase manner. A set of active transmission nodes is determined in each phase, based on which the aggregation tree is constructed. At every round of aggregation, a node in the transmission set establishes a link with the nearest neighbor node that is not linked to any other node. After each round, the transmission set is iteratively updated by removing the nodes that have already transmitted. The iterations terminate when the last remaining node in the transmission set successfully transmits the aggregated data to the BS. Cell-AS aggregates data from all sources in $O(\log^3 n)$. In large WSN and IoT applications it may not be possible to implement the NN-AS algorithm due to (a) the presence of large number of nodes, and (b) the need to have global information of all active nodes for determining additive interference. To counter this, the distributed Cell-Aggregation Scheduling (Cell-AS) algorithm segments the network into hexagonal cells, and a node that is closest to the BS is chosen as the Head Node (HN). Instead of forcing all nodes to store global interference information as in the case of NN-AS algorithm, the Cell-AS off-sets this need through strategic segmentation of the network based on link-length diversity, by exploiting non-linear power assignment strategy. To perform data aggregation, the HNs make use of the *pulling* mechanism to extract the data from the member nodes in the cell. The HNs then coordinate and pool in to larger hexagonals to aggregate the aggregates form each HN. This process is iteratively done till the aggregated data finally reaches the BS. The distributed Cell-AS algorithm under the Ph_I model in arbitrary topology networks takes $O(K)$ time slots, where K is the logarithm of the ratio between the lengths of the longest and shortest links in the network. However, to keep the network connected and to allow maximum coverage in the network, the transmission power at each node has to be large enough, which is not practically feasible. The assumptions pose some challenges for hardware design and is impractical when the network scales.

Lam et al (Lam et al., 2013) discuss weighted one-shot constant factor approximation algorithm with bounded maximum power to study the MLAS problem using the collision interference-free graph model and the Pr_I model. The approximation algorithm employs non-uniform power assignment scheme, and considers only the links that satisfy the SINR constraints. The algorithm has two phases of scheduling: cell-scheduling and backbone scheduling. In cell-scheduling phase, coloring approach is applied to cells for synchronizing the schedule amongst different cells in the network. A multi-level partitioning technique is used to generate local trees to perform data aggregation. In backbone scheduling phase, a virtual backbone tree is constructed to aggregate data from the roots of local trees to the BS. Coloring approach is adopted to schedule tree links based on their levels and colors. The latency is bound by $O(R + \chi)$ timeslots, where R is the network radius and χ is the link length diversity.

Topology control strategies aim to reduce the effect of radio interference by following a three pronged strategy of (a) reducing the transmission power of the source node to minimize the interference region, (b) by scheduling the transmissions when the neighboring nodes are in sleep mode, and (c) by devising topologies where the degree of nodes is low. An effective means to implement these strategies is to ensure that the energy consumption amongst the nodes is uniform across the network and to determine an optimal schedule so as to minimize the number of unintended reception of signals. Reducing transmission power can lessen the exposed terminal problem, but will aggravate the hidden terminal problem. But power control can still be a useful tool when it is jointly considered with other techniques for finding an overall solution to the two problems. As energy is the limiting factor for network lifetime, these strategies also lead to extension of network lifetime due the reduction in transmission power. However, these strategies will be successful only if network connectivity is preserved. A discrete-time Markov chain (DMTC) integrated analytical model is adopted to study the performance tradeoffs between delay latency, energy and fidelity of the aggregation jointly for in-network aggregation in an aggregation tree; and topology control is discussed in Erramilli et al. (2004). The DMTC model shows that medium to high event reporting load often leads to high fidelity levels, while shorter and denser aggregation/routing trees offer better delay-energy tradeoff as long as topology control is well-coordinated. However, the sleep schedule may generate unnecessary delays and lower the fidelity values in cases where a child node has data to transmit and the parent/aggregator is in sleep mode. In such cases, topology control through active/sleep schedules may interfere with aggregation and offset any benefits from aggregation performance degradation. Li et al. Li et al. (2005) present three approaches to construct efficient spanning tree topologies: Interference-based local minimum spanning tree (LMST), Relative Neighborhood Graph (RNG) and Euclidean Minimum Spanning Tree (EMST)), with adjustable transmission power range using weighted.

WSNs often encounter Exposed Station (ES) and Hidden Terminal (HT) problems, whenever two or more source nodes indulge in simultaneous transmissions. If the problems are not adequately addressed, ES results in loss of throughput, while HT leads to interfered signals, Lowering the transmission power can avoid the ES problem, but it aggravates the HT problem. However, transmission power control can be powerful tool to address both ES and HT problems if an optimal tradeoff power is arrived at.

Whilst several models have been developed as an off-shoot of the Pr_I and Ph_I models to understand conditions under which the communication between two nodes are subjected to interference, several gap areas exist in the form of addressing issues related to (a) interference avoidance, (b) exposed station, (c) source back-off problem, (d) hidden terminal problem, (e) identification of potentially interfering source nodes to an on-going transmission, and (d) facilitating the determination of Interference-Fault Free Transmission (IFFT) schedule. To amicably address these issues, Begum and Nandury (Begum and Nandury, 2015; Begum and Nandury, 2022b) developed a Composite Interference Mapping (CIM) model which determines a comprehensive map of all Potentially Interfering Links (PIL) to all active source–destination pairs in the WSN or IoT application. The CIM map not only facilitates the determination of an IFFT schedule, but also addresses the ES, back-off and HT problems. Based on CIM model, three IFFT data aggregation scheduling algorithms were developed viz., (i) IFFT-STDMA and IFFT-ESTDMA for topology-free, and (ii) LL-IFFT-ESTDMA for tree-structured WSNs. With the help of interference maps generated by the CIM model, the active links are grouped into sets of non-interfering links, and each set is allocated a separate timeslot by making use of the TDMA approach. As the algorithms have precise knowledge of the potentially interfering links, they succeed in arresting the generation and propagation of *interference-laden* corrupt data across the network. Besides this, the IFFT algorithms maximize the number of concurrent transmissions in a given timeslot.

Protocol and Physical Interference models continue to be the primary foundation on which different data aggregation schemes were developed to address interference in WSN and IoT networks. The protocols and algorithms developed differ widely based on the application network, the approach and the complexity & performance metrics. Few such select works are reviewed in Table 5.

5.1.2. Data aggregation techniques to address interference in IoT

IoT networks typically comprise several heterogeneous sensors, actuators and devices that are autonomous and stand-alone. Interference free data aggregation is a major challenge in such networks, as the aggregation protocols need to deal with different wireless technologies like Bluetooth, Wi-Fi, mmWave, ZigBee, LoRaWAN, etc.; operating on a varied range of bandwidth and frequency bands in the RF Spectrum. The rate of data transfer in an IoT network comprising several network segments with overlapped bandwidth and frequency spectrum, invariably depends on the segment that is most sluggish. Such networks are prone to interference if the devices are located within the interference range of each other. Further, due to the presence of heterogeneous devices each driven by its own protocol, the data aggregation schemes developed specifically for homogeneous WSNs are not readily implementable in IoT networks. To address this, several Interference Management Mechanisms (IMM) were developed which can be broadly categorized into (a) those that isolate mutually interfering transmissions through resource partitioning, and (b) those that use signal processing techniques to facilitate interference-free concurrent transmissions. Whilst the first category may lead to poor spectrum efficiency due to resource partitioning, the success of the second category depends on the availability of Channel State Information (CSI). To address issues related to narrowband IoT and mitigate interference in such scenarios, Z. Li et al. (Li et al., 2019) have developed IMMs that generate an Interference Steering Signal (ISS). The ISS steers the interference imposed to be orthogonal to the original intended signal and thus negates the effect of interference on the intended receiver.

Due to the use of multiple frequency bands, data transmissions in one segment of the IoT network may interfere with the communication in other segments, even if the two segments are not directly connected. Further, any external device (microwave heating device) which is not a part of the IoT network, might cause interference to communications within the network, if their frequencies of operation are not spatially separated. Furthermore, detection of such external devices is quite complicated, especially if such devices are proprietary in nature and use non-standard, device specific frequencies. When interference is detected, the receiving device drops the data packet and the transmitting device initiates re-transmission of its data. Multiple such trials lead to faster depletion of the device's energy. On the other hand, if signal interference is not detected, corrupt data is aggregated. This has a cascading effect, as the corrupt data aggregates proliferate into the network, severely compromising data integrity and accuracy. To get over this problem, the IoTs may limit their transmissions to cellular bands operating in a controlled RF environment. Besides being expensive, this approach impacts the autonomy of IoT network. Another solution to this problem is to extend the CIM model (Begum and Nandury, 2022b) to determine sources of interference both within and outside the IoT network. The Time-Division Multiple Frequency (TDMF) approach introduced in Begum and Nandury, (2015) can then be used to schedule the interfering

Table 5
Data aggregation protocols based on interference models for WSN and IoT.

Algorithm(s)/Model(s) with Objective	Description and Features	Performance Metrics
CONVERGECAST (Kesselman and Kowalski, 2006) **Objective:** To minimize data collection time and energy Follows Protocol interference model	• Considers GPS enabled homogeneous (uniform power) nodes equipped with collision detection capability. • Randomized distributed algorithm • Tradeoff between energy consumption and latency is studied.	• Latency in terms of the number of time-steps: $O(\log n)$ and in line topology, latency is $(n-1)$ time steps. • Consumes at most *O(n log n)* times the minimum energy.
PLS and **LPS** (Moscibroda and Wattenhofer, 2006b) **Objective:** To study scheduling complexity for scalable scheduling for large-scale worst-case networks. Physical interference (SINR) modelCommunication backbone is spanning tree Considers arbitrary WSN with non-linear power assignment	• Two algorithms: Poly Logarithmic Scheduling (PLS) and Linear Power Assignment (LPS). • PLS employs a power assignment scheme where the nodes choose nearest active neighbor based on power level. • LPS partitions the network into grid-cells. In each time-slot, it selects one link in each such cell for scheduling. • The transmitting nodes that maintain an interference-free distance between each other are scheduled in the same time slot.	• PLS latency for strongly connected graph $O(\log^4 n)$ slots. • Uniform LPS, latency bound is $O(g(V).\log n)$ slots, where $g(V)$ is number of non-empty length classes of nearest neighbor forest links.
FIRST-FIT AGGREGATION SCHEDULING Huang et al. (2007) **Objective:** To solve MLAS problem in large-scale dense WSN. Follows Protocol interference model	• Considers Maximal Independent Set based BFS tree rooted at BS. • Assumes $R_I = R_T$ with uniform power assignment • BS divides the network into layers and the nodes are scheduled layer-by-layer using first-fit approach.	• Latency when $R_I = R_T$, 2 $3R + \Delta - 18$ time slots • Larger the Δ shorter is the latency
SAS (Sequential Aggregation Scheduling), **PAS** (Pipeline Aggregation Scheduling) and **E-PAS** (Enhanced PAS) (Wan et al., 2009) **Objective:** To solve MLAS problem in synchronous multihop networks. Follows Protocol interference model.	• Considers $R_I \geq R_T$ with uniform power assignment • Inward arborescence • CDS backbone induced by a BFS ordering of vertices. • Determines 3 data aggregation schedules based on SAS, PAS and E-PAS that have identical interference and transmission ranges. • SAS, PAS and E-PAS determine a Maximal Independent Set (MIS) by BFS ordering of vertices to implement CDS for routing.	Latency in terms of time slots: • SAS:$15R + \Delta - 4$ • PAS: $2R + O(\log R) + \Delta$, • E-PAS:$1 + O(\log R/3\sqrt{}R))R + \Delta$
CDAS and **DDAS** (Xu et al., 2009) **Objective:** To minimize latency in dense networks Adapts to dynamic networks with fixed CDS and uniform power assignment	• Assumes $R_I = \Theta(R_T)$ with CDS backbone for BFS-based aggregation tree. • Presents two algorithms: Centralized-Data Aggregation Scheduling (CDAS) and Distributed DAS (DDAS) • CDAS uses a bottom-up layer-by-layer approach, while DDAS allows dominators to be scheduled greedily once they collect data from their dominates, without waiting for other dominators.	• Latency is at most $16R + \Delta - 14$ time-slots. • Lower-bound of latency for $R_I = R_T$ is $max\{\log n, R\}$. • Energy efficiency of DAS is not studied.
CONNECT (Orsson and Mitra, 2012) **Objective:** To connect arbitrary point set into a strongly connected diagraph and to address MLAS problem Follows Physical Interference Model	• For better connectivity and energy conservation, oblivious power assignment scheme is adopted. • Schedules both one-way and two-way half-duplex communication in same slot. • For small link length diversity, the utility of oblivious power assignments was found to be effective.	• Latency in symmetric bidirectional model is Ω (n) slots. • Latency in asymmetric bidirectional is $O(\log n)$ slots. • Any structure with oblivious power assignment requires $n/2$ slots.
EMA-SIC (Li et al., 2013) **Objective:** To arrive at an optimum latency-energy tradeoff in arbitrary multihop WSN. Nodes have differential power levels up to maximum distance *R* Needs information on the relative position of each dominatee w.r.t. to its dominator.	• Considers CDS backbone for the data aggregation tree • Each dominator encircles itself with a disk radius R_T and fills it with equal size hexagonal • Alleviates inter-hexagon interferences by separating concurrent transmitters with a predefined distance • Successive Interference Cancelation SIC technique reduces latency. Cell-AS for smaller networks has reduced latency compared to EMA-SIC	• Reduced maximum aggregation latency • Asymptotically optimal latency-energy tradeoff compared to Cell-AS • Latency upper bound by $O(D)$ timeslots. • Reduced energy consumption approximation, $O(\Delta^{\alpha-1})$
FAST (Yousefi et al., 2015) **Objective:** To minimize time latency of MLAS. Distributed data aggregation protocol for fixed tree-based topology	• Employs connected 3-hop dominating sets (C3DS) • Nodes use uniform power assignment • Backbone nodes employ waiting policy to schedule arrivals • Simultaneous construction of aggregation tree and scheduling • Dominator nodes negotiate with child nodes to schedule transmissions	• Latency of distributed TDMA-based FAST is upper-bound by $12R + \Delta - 2$ time slots. • Performance improves with increase in network density
1 K and nK models (Fitzgerald et al., 2018) **Objective:** To have energy-optimal data aggregation and extended lifetime in IoT edge networks. Follows Physical interference model with Fog nodes/gateway as network backhaul.	• Employs Mixed Interference Programming (MIP) formulated data aggregation models: 1 K model and nK model, where K is number aggregated measurements • 1 K aggregation model uses reverse arborescence • Examines tradeoffs between minimal total energy usage and min–max per-node energy usage.	• For small networks, energy usage is similar for the 1 K and nK cases • In nK, energy consumption increases faster as the network increases in size • Unreliable for redundant data transmitted to multiple receivers over multiple redundant paths
ASIoT (An et al., 2019) **Objective:** To solve MLAS problem in IoT networks. Broadcast communication and use of non-overlap-	• Uses Collision (Interference) model similar to Protocol interference model where CDS is the communication backbone.	• Latency is approximated to be $\leq\Delta - 1 + 15 * D$ timeslots, D is network diameter $\leq 2R$.

Table 5 (*continued*)

Algorithm(s)/Model(s) with Objective	Description and Features	Performance Metrics
ping frequencies Different transmission power for each node	• After scheduling dominatees, the dominators and connectors in the CDS tree are scheduled iteratively using modified First-Fit scheduling algorithm	• Suitable for environmental monitoring IoT applications
NOMA-TST (Moussa and Zhuang, 2020) **Objective:** To provide energy efficient and delay-aware channel access. Considers 2-hop network comprising layers of cellular BSs and cellular network with numerous homogeneous IoT devices.	• NOMA-TST framework supports large-scale cellular IoT communications • Data aggregators aggregate and relay data from IoT devices to BSs by employing successive interference cancellation. • Frequency is partitioned into orthogonal sub-channels of equal bandwidth and packet generation is modeled as M/G/1 queue • Uses SINR model with no noise, where the messages with SIR greater than a threshold are received and decoded.	• Data aggregators consume less energy • Increase in network density, energy consumption is either stable or decreases • Improved end-to-end delay • Better than OMA-based cluster-based approach • Resolves inter-cluster and intra-cluster interference
IA-ORA (Lin et al. 2020) **Objective:** Optimal aggregate throughput in ultra-dense multi-cell random access IoTs. Each cell has one access point (AP) and numerous IoT devices No cooperation is assumed among the APs. Considers a quasi-static fading model	• Employs ultra-dense TDD K-cell slotted-ALOHA with decentralized transmission of signals. • Each user signal must satisfy-two threshold conditions: (a) signal power to the destined AP is sufficiently large and (b) small interference leakage power to other Aps • Transmitting nodes requires channel state information	• K-fold increase aggregate throughput, $\frac{K}{e}(1-\epsilon)\log(snr\log n)$, $0<\epsilon<1$, $K\geq 1$, when compared with conventional opportunistic random access protocols. • Resolves inter-cell and intra-cell interference with opportunistic transmission
1-D PPP & 2-D PPP (Nabil et al., 2022) **Objective:** To model spatial and temporal characteristics of SINR in Large-scale hexagonal grid-based IoT network. Considers synchronous time-triggered traffic where the devices possess uniform transmission power with multipath fadingEmploys Universal frequency reuse scheme and synchronized duty-cycle	• SINR characterization uses two spatiotemporal PPP models: Parallel 1-D PPP and Parallel 2-D PPP • IoT devices are distributed on parallel lines with equal inter-line separation while the gateways were placed on hexagonal grids • Based on data granularity, device density, and mutual interference, IoT devices are modelled as spatially interacting PH/PH/1 queues • Rate-sensitive SINR packet are stored and sent in FIFO manner • Uses directional antenna and channel inversion power control to speedup data aggregation and to minimize total average latency.	• Optimal number of packet segments minimizes delay and improves transmission success probability • Directional antennas improve reliability and delay • Path-loss power control marginally degrades the network performance • Uses stochastic geometry and queueing theory to study the tradeoff

transmissions in spatially separated frequencies. Advanced communication back-bone technologies like 5G are expected to address interference more amicably compared to 4G technology.

5.2. Fault-tolerant data aggregation techniques

The use of miniaturized low-cost devices is one of the hallmark advantages of WSN and IoT applications. However, to maintain this advantage, the sensor and IoT devices are forced to carry limited battery, storage and computational capacities. This makes the network susceptible to node/link failures, packet drop and interference faults (Begum and Nandury, 2022b). Therefore, to build a robust framework, the WSN and IoT networks need to be equipped with mechanisms that detect & isolate faults and diagnose them, in order to initiate recovery & reconfiguration activities to tolerate these faults. In this section few works on fault detection & diagnosis and fault-tolerance are briefly outlined.

5.2.1. Fault detection & diagnosis

Fault Detection is an essential pre-requisite for any data aggregation mechanism. A common mechanism to detect faults is to periodically assess the health status of the sensor nodes. A watch-dog timer is often used to detect node faults, where the nodes periodically broadcast "I AM ALIVE" message to proclaim that they are healthy. Non-receipt of such message from a node is an indication for its neighbors that the node is dead or faulty. The use of watch dog nodes is another popular approach, where some nodes categorized as watch dogs keep monitoring the status of their neighboring nodes. Watch dog nodes are also used to detect any unauthorized intrusions in the network (Hasan and Mouftah, 2017).

In large WSNs and IoT applications it may not be practical to adopt a centralized fault-detection mechanism. To detect permanent node faults and faulty processing units in such applications, a system level distributed fault algorithm is proposed in Saha and Mahapatra (2011).

To avoid degradation in service, Mahapatro and Khillar (2012) present a distributed approach to detect faulty nodes in the network. The approach provides a method for detecting both hard as well as soft faults, which are either permanent, transient or intermittent. A distributed fault diagnosis method based on comparisons between the sensed data and the data received by other sensor nodes is discussed in Lee and Choi (2008). However, for the comparisons to be reliable, it is necessary to consider (a) time redundancy delays and (b) drift and calibration errors of the sensors. Time delay redundancy is eliminated by implementing a sliding window scheme, where each sensor node maintains a table comprising the status of its neighbors. Drift and calibration errors can be detected by a BIT (Built-In Test) diagnosis method, where the sensors keep executing BIT to correct their readings, by spatially correlating them with the readings of other sensors deployed in the network. Based on the mean variation between the observed sensor readings and the operating range (minimum and maximum), the performance of degradation of sensors can be estimated.

5.2.2. Tolerating process faults and node/link faults

Whilst it is relatively simple to detect hardware faults, detection of faults arising due to sensor malfunction, interference faults, process faults, etc., are more complex. Such faults usually manifest as corrupt data, which are difficult to detect, as in most cases these faults occur due to externally driven events. If such faults go undetected, the aggregator nodes keep aggregating corrupt data, which has a cascading effect and faulty data soon pervades the entire network. Besides detection, these faults need to be isolated to pinpoint the source of faults, and diagnosed to understand the root-cause, in order to prevent degradation of network services like data transfers and communication between nodes.

In large dynamic WSN and IoT applications, process-fault detection is quite challenging, as the sharing of network status information amongst several autonomous sensors, actuators and devices is an unviable proposition. To address this, machine learning approaches are increasingly being used, where learning algorithms are used to train the fault-detection model by initially feeding the algorithm with test data sets (Laiou et al., 2019; Yadav et al., 2021). The response of these algorithms to the test data is captured in the form of support vectors, which helps in iteratively tuning the test data sets for more accurate detection of faults.

The application of Support Vector Machine (SVM), is increasingly being used as a fault-detection tool in large WSNs and IoT applications. SVM is a supervised learning tool that segments the data sets into multiple classes by iteratively generating hyperplanes till an optimal hyperplane that accurately divides the classes is determined (Kamalesh and Kumar, 2017; Jan et al., 2021). Jan et al. (2021) proposed the use of a fault detection block in the sensor itself that transforms the sensed data into a low-dimensional feature vector for the SVM to classify the data as normal or faulty. To address fault management and recovery issues, Kamalesh and Kumar (2017) divide the network into clusters, where the node with maximum degree of connectivity is selected as the CH. The SVM helps the CH to identify the outliers in the data received from its cluster nodes and classifies them as faults if the data is too far away from the hyperplane.

The concept of maintaining a backup parents set for every node in the network is discussed in Zhang et al. (2012). The backup parent set of a node comprises a list of nodes that are within one-hop distance from its grandparent. In the event of failure of a parent node, the child nodes of a faulty parent randomly select one of the nodes in their backup parent set as their new parent. Based on this concept, a TDMA-based fault-tolerant scheduling algorithm was developed. However, this approach may lead to resource contention if the same backup node is selected by multiple child nodes. Further, this approach also limits the number of alternate pathways to the BS, as it disregards the nodes outside the backup parent set that could lead to the BS.

Fault-diagnosis helps in understanding the cause and nature of faults, which helps in formulating appropriate fault-tolerant mechanisms. If the nature of fault is related to node failure, a popular fault-tolerant approach is to reconfigure the network topology by eliminating the faulty node or faulty link, and re-allocate the tasks assigned to the faulty node to an alternate node (Younis et al., 2014). However, in applications where the order in which data is aggregated across the network is of great significance, such reconfigured network severely compromises data accuracy. Further, if the application is driven by real-time constraints, the data is of no significance if the sensors that generate time-critical data find themselves at the far-end of the reconfigured network structure.

To counter this, Begum and Nandury (Begum and Nandury, 2022a) have proposed the use of component graph theory to reconfigure the network. In this approach, the whole network is considered to be component, and when a node or a link turns faulty, the component graph is fragmented into smaller components. Each node in the network maintains a list of alternate parents, through which they can be connected to the root, if their parent node fails. In the event of the failure of a node, the components at the bottom end of the tree are connected back to the components that lead to the topology centre with the help of alternate parents. This approach preserves precedence relations and honors the real-time constraints.

The restructuring of network graph into Connected Dominating Set (CDS) tree is popularly used in WSN for energy optimization. This approach has been also used to develop several fault-tolerant data aggregation protocols (Feng et al., 2011). In this approach, a CDS data aggregation tree is constructed, where the data is aggregated from the leaf nodes to the dominators, level-by-level in a hierarchical manner. Nodes vulnerable to failure are identified and an amendment strategy to reconfigure the network is worked out so as to reduce the number of nodes affected due to the failure of these vulnerable nodes. However, success of this approach largely depends on the coverage offered by the scheduling algorithm and the amendment strategy. Further, network reliability studies need to be carried out to analyze the effect of failure on the connectivity of the nodes and data aggregation process. Lee et al. (2004) have discussed use of Weibull probability density function to model a node's reliability for resolving wear-out failures.

To handle large variations in the nature of IoT devices, a cluster based approach for data communication is preferred instead of direct routing of to the BS. However, this strategy is prone to multiple failures if one or more CHs fail. To offset this, Lin *et al.* (Lin et al., 2019) propagate the concept of using a virtual CH instead of a physical wireless node that acts as a sensor. The virtual CH also acts a backup node if one or more neighboring nodes fail. Retrieval of data from a CH is relatively simple, and the aggregates from the virtual CHs are obtained through flow-graph modeling.

Fog and cloud services are increasingly being used for IoT applications for utilizing data storage and computational resources. However, these applications may sometimes experience loss of data due to intermittent bandwidth or a momentary lapse in connectivity. In such eventuality, the application may be made fault-tolerant by making a prudent estimate assumption of the missing data from past record of mean and variance, without compromising privacy (Lu et al., 2017; Khan et al. 2021).

6. Data aggregation protocols based on mobility, security and privacy

Ready availability of internet and cloud computing platforms, has facilitated the recent spurt in mobile sensors and IoT devices. With the market for wearable devices and GPS enabled automobiles, WSNs are increasingly catering to applications that demand data aggregation of mobile nodes. With any-thing and every-thing being connected, network security has emerged as a major concern for WSN. Data aggregation protocols developed to address mobility and security issues in WSN and IoT applications are discussed in this section.

6.1. Data aggregation protocols to address mobility in WSN and IoT applications

Data aggregation schemes that address mobility need to consider any of the three scenarios where: (a) the BS or sinks are mobile (b) nodes are mobile and (c) both nodes and BS are mobile. Telecommunications through cell phones is most popular application where the sensor nodes are mobile. The cell phone device has several sensors like GPS, vibration sensor, touch sensor, to name a few. Communication between these mobile sensors is facilitated by BS in the form of static cell-towers.

In applications where the wireless sensors are deployed in harsh un-manned terrains spread over large a geographic area, mobility of nodes is a major challenge. Besides this, the placement of multiple communication towers (BS) in the deployment region of interest may not be a viable option. In such applications, mobile agents are usually employed. The mobile agents visit the static sensor nodes periodically to collect data and perform data aggregation. To optimize the path length, Rendezvous Points (RP) are strategically located, where each RP acts like a virtual CH. The mobile agents instead of visiting each and every node, visit the RP and collect data from the nodes located within one-hop distance from the RP, which substantially reduces the tour length (Zhu et al., 2015; Prashanth and Nandury, 2019). Fan Ye et al. (2005) have developed a Two-Tier Dissemination Protocol TTDD, for applications with static sensor nodes and mobile sinks. The mobile sinks at the lower tier forward aggregated queries to the data dissemination nodes in the higher tier. The dissemination nodes forward the processed queries to the mobile BS. Erman *et al.* (Erman et al., 2012) proposed a virtual grid with honeycomb tessellation to cover the entire WSN area in applications with mobile BS. The diagonal forwarding paths between a static sensor and a mobile BS allow convergence of similar data at common border nodes. While the hexagonal tessellation achieves traffic flow balance across all regions, the nodes in border line and those lying in the central line turn into hot-spots, to serve as the main limitation of this approach. To offset this, the size of the hotspot hexagonals need to be adjusted based on the network traffic load. In the Mobile Sink based Routing Protocol (MSRP), a mobile BS determines the CHs based on a specified distance threshold and residual energy threshold posseessed by a node (Basumatary, and Barma, 2019). The CHs aggregate the data from their static cluster nodes and forward the aggregate to its mobile BS. This approach is more suitable to delay-tolerant WSNs with limited number of nodes and may encounter severe limitations when applied to IoTs. The Data Quality Maximization (DQM) protocol (Xu et al., 2011a) is applicable for BSs with predictable trajectory. The protocol proposes a three-tiered network, where the middle tier acts as the gateway between the sensor nodes in the bottom tier and the mobile BSs in the top tier. The gateway uploads the stored aggregates to the mobile BS when it passes through the intersection of trajectory and transmission range of gateway, or is nearer to the gateway. Due to its middle tier, DQM is relatively more energy efficient than MSRP. However, the protocol does not mitigate the hot-spot problem and is suitable only for delay-tolerant applications.

Table 6
Mobility related data aggregation protocols.

Protocol	Features	Advantages/Limitations and Applicability for IoT
CLCP (Alkhamisi et al., 2016)	• Cluster-based and CH acts as aggregator node • Distributed cross-layer scheme for data aggregation in mobile ad-hoc environments • Support for query-based search • Node with highest CL_factor is selected as CH selection. • CL_factor parameters: residual energy and average distance of cluster members	• Suitable for IoT/Smart-city applications • Ensures failure tolerance and operates in both network and application layer • Reduced traffic load and energy saving • High latency
ME-IoT (Hanady et al., 2018)	• Cluster-based topology with homogeneous sensors and a BS • MEs (mobile element) have high power capability and act as CHs • Sensor nodes can directly reach each other and to the BS • MEs are connected to IoT wirelessly • Frequency of MEs entering the WSN network in a given time period may be uniform or non-uniform or no MEs • Switching of aggregation from ME dependent technology to regular WSN technology where there are no MEs	• Improves energy efficiency of WSN and maintain data accuracy • Prolongs network lifetime using IoT technology and MEs • Ensures data aggregation is independent of the presence of the MEs. • Suitable for WSN-enabled IoT network
TPEG (Lai et al., 2018)	• Hierarchical one-hop vehicle to infrastructure (V2I) or multi-hop vehicle to vehicle (V2V) transmissions • Based on "store-carry-forward" routing in delay-tolerant network • Integrates fog nodes with VANETs (vehicular adhoc networks) • Fog nodes apply-two-level threshold adjustment (2LTA) scheme • Sensing operators are classified into low cost sensing (LCS) mode and high cost sensing (HCS) mode • Three phase of operation: monitoring phase, event-checking phase and data upload phase	• 2LTA adaptively adjusts the threshold to upload data for decision making • Prevents unnecessary message transmissions. • Efficiently senses and gathers data • Cost of message transmissions can be reduced with data aggregation and compressive sensing • Used for monitoring road condition and periodic sensing • Suitable for smart cars and intelligent transportation systems (ITS)
FERA (Lai et al., 2019)	• Mobile environment • Hierarchical data collection and processing • Three-layer filter-based request answering framework: vehicular nodes, the edge nodes and the cloud. • Adaptively implements pull/push strategies. • Data/Readings flow: vehicular nodes to edge nodes, and from edge nodes to cloud • Query/Request Flow: Cloud to edge nodes, and down from edge nodes or ordinary nodes	• Combines the fog computing and vehicular sensing • Suitable for vehicular ad hoc networks/smart city applications • Adaptively adjusts the states of filters to match the cost ratio and achieve better performance • Filters in vehicular nodes and edge nodes suppresses unnecessary push of data readings
TTDD-QL (Wang and Hsu, 2020)	• Hierarchical grid structure, multi-hop and multicast routing, • Stationary sensor nodes with mobile sinks • Two-tier query aggregation/query traversal: higher-tier has dissemination nodes and lower-tier comprises BSs • Immediate dissemination node aggregates queries from BSs • Upstream dissemination node receives aggregate queries and directs processed query data streams to BSs • Dissemination nodes have soft-states timer • Applies Q-learning in TTDD to determine energy efficient path between the BS and the dissemination node	• Reduced communication overhead • Supports mobility of BSs • Balances the overhead due to periodic upstream update messages • Suitable for use in IoT applications with mobile IoT-edge devices
TSVA-CP-ABE (Zhang et al., 2021a)	• Applicable to applications driven by smart mobile crowd sensing platform. • Follows a cipher text policy where the encryption and decryption policy is frame based on a set of attributes. • Nodes with encrypted data are authorized to share the decryption access with other nodes of their choice. • Authorized edge nodes perform data aggregation	• The utility of TSVA-CP-ABE is optimal only if the devices have smart sensing features. • Use of edge computing reduces the energy overheads for computation and communication • Suitable for application with context-awareness and temporal constraints. • The protocol provides highly secure communication.

In large WSN and IoT applications, both sensor nodes and BS are mobile. In such applications, data aggregation is carried out through fog or cloud computing. Some of the recent works on data aggregation schemes to address mobility are presented in Table 6.

6.2. Data aggregation protocols to address security in WSN and IoT applications

WSNs form the primary backbone for applications related to surveillance, strategic sectors like defense & space and a host of IoT applications. Since security is a major requirement for these applications, WSNs are expected to preserve the privacy of data and secure all transactions both within and outside the network. As most sensors and devices in the network are anonymous & autonomous, and are often dynamic and loosely coupled to the network, they are vulnerable attacks from malicious entities. Due to involvement of a wide variety of sensors & devices, WSN and IoT applications are prone to security lapses. Further due to resource constraints WSNs and IoTs become easy targets to sinkhole, Sybil, wormhole, jamming and eavesdropping attacks. Therefore, providing QoS related to network security in terms of (a) device authentication & authorization, (b) data encryption & decryption, and (c) data confidentiality & privacy has emerged as major challenge for secure data communication (Khatib, 2020; Yousefpoor et al., 2021). Most firewalls designed for wireless communication can readily be used for providing QoS related to node/device authentication & authorization in WSN and IoTs. Similarly, most encryption and decryption methods can be readily implemented in these applications. However, for secure data aggregation, protocols that address data confidentiality & privacy need to be specially devised for WSN and IoT applications.

The hop-by-hop data aggregation security approach encrypts and decrypts data at each aggregation node while ensuring data integrity and authentication. However, the data confidentiality cannot be ensured and hence, the relayed data is more vulnerable to malicious attacks. Further, the hop-by-hop approach assumes that all the network nodes use computationally intensive cryptographic algorithms. However, this assumption is unrealistic in resource-constrained WSNs. As a result, the hop-by-hop approach is largely limited to applications that do not have resource constraints. The data aggregation protocols to address security are reviewed in this section.

The Secure Information Aggregation Protocol (SIA) (Przydatek et al., 2003) considers a WSN with static homogeneous sensor nodes. It is to be noted that Merkel hash tree are increasingly being used to encode blockchain data for quick verification and to maintain security of the data. The BS in SIA initiates the construction of Merkel-hash tree to ensure node authentication and data integrity while performing data aggregation. SIA prevents malicious and stealth aggregate manipulation attacks. SIA can be extended to larger WSNs by including multiple BSs acting as aggregators. However, to implement SIA for IoT applications, provision need to be made accommodate node mobility.

Concealed Data Aggregation (CDA) protocol and its variants CDAP (CDA with Privacy homomorphism) and RCDA (Recoverable CDA) (Parmar and Jinwala, 2016) aim to provide end-to-end privacy preservation in a concealed manner. The CDA protocol that was originally conceived for a network of homogeneous nodes, eliminates the need to store privacy keys. It employs the Domingo-Ferrer's probabilistic symmetric privacy homomorphism scheme to prevent passive adversary eavesdropping. CDAP protocol is extended for use in network of heterogeneous nodes, where end-to-end concealment of data, confidentiality and secure data aggregation are provided through privacy homomorphism. The RCDA protocol uses aggregated signature and Elliptic Curve (EC)-ElGamal algorithm for data authenticity, integrity and end-to-end confidentiality (Chen et al., 2012a). RCDA is applicable for networks comprising both homogeneous as well as heterogeneous nodes. In RCDA-HOMO, the CH gathers all ciphertext-signature pairs created by homogeneous cluster nodes and sends the aggregate to BS. In RCDA-HETE, the intra-cluster traffic is encrypted with pairwise private keys and inter-cluster traffic between CHs is aggregated and encrypted with signatures. RCDA is not suitable for networks that are scalable.

Another data aggregation protocol that makes use of EC-ElGamal algorithm with Homomorphic Encryption (HE) is the Sen-SDA introduced in Shim and Park (2015). Sen-SDA considers a cluster based three-tiered WSN topology comprising heterogeneous node. The CHs of each cluster collect and verify time-stamped ciphertext-signature pair of their member nodes before transmitting the aggregates to the BS, i.e., data freshness is preserved. The CHs and BS execute batch verification using Binary Quick Search (BQS) technique to check signature validity. Due to batch verification, end-to-end confidentiality and hop-by-hop authentication is maintained, which prevents forgery attacks by a compromised node. However, an issue of concern for this protocol is its relatively higher communication and computational costs on resource-constrained nodes due to asymmetric encryption. Further, due to its rigid three-tier structure, it may not be suitable for IoT applications that demand more flexibility in topological structure.

The Secure Hierarchical In-network Aggregation (SHIA) protocol in Chan et al. (2006) is able to prevent any manipulation of aggregated data by limiting the adversary activity. The network is structured as a directed tree with homogeneous sensor nodes and single BS. The BS broadcasts a query to initiate construction Merkel hash-based aggregation tree. The nodes perform symmetric-key encryption, decryption and collision-resistant cryptographic hash computations and independently verify correctness of their contributions to the aggregate (without assuming data correlation). Message Authentication (MAC) codes are used to verify consistency of data at the remote user.

The Energy-efficient Secure Pattern Data Aggregation (ESPDA) protocol (Cam et al. 2006) provides secure data aggregation through the Non-blocking Orthogonal Variable Spreading Factor - Block Hopping (NOVSF-BH) mechanism, by randomly assigning data blocks to different time slots in every session. ESPDF is applicable to homogeneous cluster-based WSNs. The CHs transmit distinct aggregates in encrypted form to the BS. To improve data confidentiality, coded patterns are applied at the CHs and the messages are time-stamped to guarantee data freshness, data integrity and authenticity. The nodes follow a sleep-active mode, which helps in mitigating transmission of redundant data, besides conserving energy. Most NOVSF-BH codes increase the slot assignment overhead and hence, may not be suitable for IoT applications that require low latency. Other data aggregation protocols that addresses security in homogeneous cluster-based WSNs are (a) Cluster-based Private Data Aggregation (CPDA), and (b) Slice-Mix-AggRegaTe (SMART) (He et al., 2007). In CPDA each cluster uses algebraic properties of polynomials to determine the intermediate aggregates. The computational overhead in CPDA is commensurate with the size of the cluster - larger the cluster size, larger the overhead. Due to hop-by-hop encryption of intermediate aggregates, data privacy is maintained. In SMART protocol, each node hides its private data by slicing it into encrypted pieces. This reduces the computational overhead encountered in CPDA. Both CPDA and SMART achieve higher data accuracy in aggregated result without data loss/collision. However, both the protocols are not resilient to data manipulation and corruption attacks. Further, the higher computational overhead may be a detrimental factor for application of CPDA to large IoT applications.

The wireless body sensor network (WBSN) technology is an application of IoT in healthcare, where data security and privacy are of prime importance. The data collected via IoT-enabled wireless body sensors is vulnerable to a variety of internal and external attacks. One solution is to encrypt or sign the collected data to provide confidentiality and integrity, but the computational complexity hinders the application in the real IoT-based healthcare devices. Although there have been some attempts to provide secure and efficient IoT schemes, there is a lack of achieving secure data analysis in modern healthcare. To counter this, Rezaeibagha et al. (Rezaeibagha et al., 2021) proposed a cryptographic accumulator based on authenticated additive homomorphic encryption, which can securely collect and aggregate data from wearable devices without compromising the privacy. The encrypted data can be used for analysis in an encrypted form so that privacy of the data is maintained.

Transfer of data between various devices in WSN and IoT applications predominantly happens in a multihop manner, where each relay node holds the incoming data for a finite interval of time till the data is aggregated or forwarded to the next node in the path to BS. Due to this, WSN and IoT applications are susceptible to issues related to privacy violation. Whilst aggregation of data from various nodes in a network is a prime requirement, the value of the aggregation process diminishes if privacy is not preserved. Several privacy preserving data aggregation algorithms were developed which are surveyed in Kaosar and Yi (2011). Large WSN or IoT applications often operate on different bandwidths, with various levels of access to fog and cloud services. Further, the inter-node and inter-cloud communications may be constrained due to intermittent and restrained bandwidth. Whilst some devices are endowed with bandwidth abundance, other devices may operate in a bandwidth impoverished environment. As the devices share their bandwidth and data with other devices, the applications potentially get besieged with faults and issues related to data privacy. To this end, Grining et al. (Grining et al., 2019) developed a fault-tolerant data aggregation protocol that demonstrates a provable level of data privacy even amidst the failure of several devices.

WSN and IoT applications are often driven by the need to aggregate time series data, where data privacy and aggregation accuracy are equally significant. However, most approaches to address these issues assume an application that has a fully Trusted Authority (TA). C. Xu et al. (Xu et al., 2022) develop a privacy preserving algorithm for aggregation of time series data that is applicable to semi-trusted scenarios. In addition, algorithm tolerates faults that arise due to gaps in periodicity of data transmission by the sensor nodes and IoT devices and in data aggregation functions, without compromising the accuracy.

The Recoverable Privacy-preserving Integrity assured Data Aggregation (RPIDA) protocol (Yang et al., 2015) proposes a query-based tree topology comprising heterogeneous nodes. RPDIA uses the Hash-based Message Authentication Code (HMAC) where every transmitting node runs an encryption algorithm that uses Privacy Homomorphism (PH) scheme to encrypt the data. A set of keys to the encrypted data are shared with the receiving nodes. To provide end-to-end privacy, a hash algorithm is used to transform the message. This protocol prevents eavesdropping and detects attacks from malicious nodes and masqueraders. Another protocol that uses the HMAC to provide end-to-end privacy preservation is the Security Energy Saving Data Aggregation (SESDA) (Cui et al., 2018), where the network has powerful high-end sensors functioning as CHs. The CH share separate symmetric key with each of its member nodes to preserve the privacy. Similarly, each CH maintains a separate key with the BS. This helps the BS to verify the integrity of the aggregates that it receives from the CH, thus, providing two-level security to the network to prevent bogus and malicious data packets. Each data transmission carries a time stamp to ensure data freshness. SESDA uses Okamoto-Uchiyama HE to guarantee end-to-end privacy and data confidentiality. It also prevents eavesdropping, false data injection and unauthorized aggregation. SESDA can readily be applied to large WSN and IoTs. Some of the recent data aggregation protocols that address security are surveyed in Table 7.

7. Competing requirements and tradeoffs

To leverage the low-cost advantage of miniaturized wireless sensors & devices, data aggregation in WSN and IoT networks encounter several issues: (a) optimal utilization of resources like battery energy and data storage space, (b) reduction in communication and computation overheads, (c) optimum coverage and connectivity, (d) enhancing data accuracy (e) reducing delay latency, etc. Resource constraints like battery energy carried by the nodes and limited communication and computational power, etc., force the data aggregation algorithms to arrive at optimal tradeoffs between several competing requirements. Amidst these competing requirements, the data aggregation protocols need to address the QoS requirements that provide assurance to parameters such as: network sensing & coverage, network lifetime & longevity, network reliability & availability, data aggregation accuracy & time criticality, etc. (Kale and Nene, 2019). In addition to above requirements, IoT networks need to consider other challenges such as (a) massive scaling of network architectures, (b) handling issues related to volume, velocity and veracity in big data, (c) robustness amidst open computing platforms, (d) security and privacy (Stankovic, 2014). However, in order to address these issues, a deeper understanding of the underlying optimization parameters like energy efficiency, network lifetime, delay latency, interference, freshness, etc., in resource constrained environments is necessary.

7.1. Competing requirements and optimization parameters

We discuss the role of the above parameters in bringing about optimization in some of these competing requirements in this section.

7.1.1. Coverage, connectivity and capacity

The ability of sensor node or an IoT device to sense or detect various transactions in its neighborhood can be termed as the *coverage*. In WSN and IoT networks, coverage is a measure of the monitoring capability of the network in a defined field of interest, while *capacity* is a measure of the volume of traffic a network can successfully handle in a given time (Tripathi et al., 2018). Whilst it is desirable to have a large coverage area for a stand-alone sensor, it might be counterproductive for IoT networks, which are essentially a conglomerate of several WSNs. When the network coverage is large, it results in higher connectivity. However, the active sensor nodes in one WSN segment of the IoT network might be forced to receive unintended transmissions from source nodes in neighboring WSN segment. This results in faster energy depletion, as the nodes keep receiving unintended transmissions, leading to higher network traffic and latency and lower network lifetime. Besides this, it also results in the propagation of interfered signals in the network, which significantly reduces the number of successful transmissions. Thus, the capacity of the network is lowered. On the other hand, if the coverage is small, the interference effect is minimized and the capacity of the network to facilitate successful communication increases. In the absence of interference, data link protocols like Sigfox and LoRaWAN, used by low-power IoT devices like smart phones, smart electric meters and other common smart appliances, perform appreciably well (Vejlgaard et al., 2017). However, the network connectivity gets hampered, due to which, the

Table 7
Overview of data aggregation protocols for security.

Protocol	Model	Description, Features	Applicability to IoT
MODA (Zhang et al., 2018a)	• Supports both homogenous and/or heterogeneous nodes networked as a tree. • Raw data transformed into vectorized data by differential encoding. • Each node forwards encrypted data with vectorized mapping value to parent aggregator. • Implements asymmetric key elliptic curve ElGamal based additive HE for data integrity. HE enables cipher text aggregation and end-to-end security.	• Differential encoding preserves the order, value and context of the data. • The two variants of MODA, RODA (enhanced RandOm selected encryption based Data Aggregation) and CODA (COmpression-based Data Aggregation) aim to reduce the communication overheads. • Whilst RODA is relatively low in security features, CODA has lower data aggregation accuracy. • Suitable for data mining WSNs.	• Data mining feature of MODA makes it attractive for IoTs. • Tradeoffs between security, communication cost of MODA and its two variants needs to assessed during their implementation.
LBOA (Zhang et al., 2019)	• LBOA is a location-aware data aggregation scheme that comprises three entities: User, Cloud Service Provider (CSP), and Location-Sensitive Device (LSD). • LBOA is implemented in location-specific resource constrained applications. • The LBOA scheme returns the maximum value of sensory data by applying one-way chain, order-preserving encryption.	• Public encryption algorithms • Secure outsourced aggregation task in the IoT • Outsourcing data aggregation based on device location to a third-party service provider overcomes the energy and bandwidth limitation of sensing devices. • Preserves data confidentiality and ensures verifiability.	Due to the presence of large number of location specific devices in IoTs, outsourcing aggregation task may work out to be a viable option without compromising on security issues for location-critical scenarios viz., smart homes, intelligent transportation, and smart city.
PPHDA (Tang et al., 2019)	• PPHDA protocol aims to preserve the privacy of patient healthcare data. • The hierarchical framework of PPHDA comprises 3-layers: data collection layer, data aggregation layer and service layer. • It operates on 5 entities: (i) TA (ii) patients with healthcare device; (iii) healthcare centers; (iv) cloud server; and (v) data users.	• Data collection layer securely collects data from healthcare center via a cloud server. • Noise addition into the health data preserves differential privacy. • Combines Boneh-Goh-Nissim cryptosystem and Shamir's secret sharing to provide data obliviousness security and fault tolerance • Guarantees privacy to the contributing patients health data from multiple sources.	PPHDA with its high security features and lower computation, communication and storage overheads makes it suitable for e-healthcare IoT systems.
CBDA (Hu et al., 2020)	• Organizes the nodes into a tree structure where the leaf nodes get connected to each other in the form of a chain. • Nodes in the chain acts as an aggregator. • Tail nodes in the chain fragment the aggregated data to preserve data privacy.	• CBDA injects fake fragments to the sliced aggregates to deter the attacks. • Fake fragments deliberately injected can be detected while integrating the fragment aggregates • Prevents eavesdropping and collusion attacks.	Due to its ability to prevent malicious attacks and eavesdropping and the privacy preserving feature, CBD can be used for highly critical IoT or Industrial IoT applications.
FESDA (Saleem et al., 2020)	• Uses fog computing to aggregate data from homogeneous Smart electric Meters (SM) with the help of fog nodes in a hierarchical network. • Each SM has separate HMAC secret key. • SM data is encrypted using a modified Pallier encryption.	• FESDA ensures data privacy and is resilient to false data injection attacks. • Fog computing offers relatively low communication and computation overheads. • Preserves privacy of the SM data with Pallier cryptosystem.	Lower communication and computation costs and SM data privacy makes FESDA a ready-to-use in Smart Grid IoT network.
LVPDA (Zhang et al., 2020)	• LVPDA supports a hierarchical 3-tiered topology with four entities: (i) Control Center/cloud server, (ii) TA, (iii) Edge Server (ES) and (iv) Smart IoT devices. • Control centre generates aggregation requests and edge server performs aggregation on reports generated from IoT devices. • Paillier HE and online/offline signature schemes • Outsources time-consuming operations to the edge servers.	• Signatures scheme guarantees privacy, confidentiality and integrity verification during data aggregation. • Employs q-strong Diffie-Hellman (q-SDH) to prevent Existential Unforgeable Chosen Message Attack (EU-CMA) and guarantee the data integrity. • Implements Double Trapdoor Chameleon Hash (DTCH) function for signature scheme. • Outsourcing of tasks reduces load on smart IoT devices.	• With q-SDH, two or more unrelated IoT devices can jointly establish a security key. • Three-tier involving cloud computing, edge computing and smart devices, LVPDA has ready applications in IoT.
EEDAM (Ahmed et al., 2022)	• Supports a decentralized cluster topology, where the clusters are formed based on a fuzzy similarity matrix. • Uses secure edge computing devices. • Integrated blockchain mechanism is employed by the cloud server. • On demand trusted service by the edge servers.	• Depending on the fuzzy similarity matrix, a designated CH performs data aggregation. • Data integrity and security are provided through validation of the edge through blockchain mechanism. • Secured edge services with minimum delay.	• Secure data aggregation for IoT applications. • Use of block-chain technology helps in creating inherently secure data structures.
ES-PPDA: (Chen et al., 2022)	• Supports a hierarchical network topology consisting of heterogeneous nodes. • Entities of ES-PPDA: cloud servers, Edge Servers (ES), smart IoT devices (SDs) and TAs (or other control centers). • ES acts as an aggregator and processes encrypted data.	• SDs collect private data generated by sensors and transmits encrypted data to CC via an ES. • Implements Pallier homomorphic encryption. • M/G/1 queuing to govern the task arrivals reduces wait time and increases reliability and channel access	• Provides privacy preserving solutions for edge-based XasS (Anything as a service) architecture. • Guarantees data security and integrity. • Low-priority packets have more latency compared to high-priority packets.

nodes resort to multihop communication. This leads to higher latency, and additional communication & computation overheads. Therefore, coverage and capacity are key optimizing parameters in WSN and IoT networks (Aggarwal and Nasipuri, 2019).

7.1.2. Data accuracy, data freshness, delay latency and temporal correctness

The term *data accuracy* has different connotations depending on the application where the term is used. In wireless communications, data accuracy is usually understood as the closeness of the data received by a destination node, to the actual data sensed by a source node. In WSNs and IoTs, data accuracy is a measure of the closeness of the data computed by an aggregate function with the actuals, as sensed by the nodes. In most applications, data accuracy is evaluated based on the three parameters (a) sensing mechanism accuracy – how accurately a phenomenon is sensed, (b) data transmission accuracy – how accurately the sensed data is transmitted without any distortions, and (c) aggregation accuracy – how accurately the aggregation function is executed. Further, to maintain data accuracy, the AN needs to perform the aggregation function only after it receives data from all its subordinate source nodes. However, in applications where an aggregator node receives data from different source nodes at different time intervals, the AN is forced to wait for long durations if there is a delay in the reception of data from some of its source nodes. This results in delay latency. However, in order to reduce latency, if the AN performs aggregation without receiving data from all nodes, data accuracy is compromised.

In addition to delay latency, the AN also encounters issues related to *data freshness* which is a measure of how recent the data being aggregated is. This issue arises when the AN is forced to wait due to a delay in transmission by its subsidiary nodes. During this wait period, other nodes might transmit fresh data updates to the AN. If the AN now performs aggregation, it leads to poor data accuracy. In time critical applications, no matter how accurate the data aggregate is, it is of no significance if the data is not computed within a time deadline. Under these real-time constraints the data aggregation schemes need to devise appropriate tradeoff strategies to balance data accuracy, data freshness, delay latency and temporal correctness (Nguyen et al., 2021).

7.1.3. Energy efficiency and network lifetime

WSNs and IoT networks operate under resource constrained environments. To model the energy resource status of various sensors and components of the network, most approaches assume that the energy consumption is uniform across the network. However, this assumption is far from reality, since the models are not equipped to factor the energy expended by the nodes: (a) due to data retransmissions whenever a data packet is dropped, (b) idling during network congestion, (c) sharing the load of faulty nodes, etc. Further, there is wide variation in the energy consumption pattern of various heterogeneous devices of the network, with each device following its own protocols and energy overheads. Therefore, an application-specific approach need to be followed while determining the energy efficiency.

Energy efficiency is a critical parameter to estimate the Network LifeTime (NLT), which is a measure of the overall health of the network. NLT is usually expressed as the number of aggregation rounds the network can survive till a defined percentage of nodes become dysfunctional due to energy drain out. As a substantial proportion of communication load is due to data retrieval and data storage operations, caching scheme can be employed to reduce this load. In this scheme frequently used information is cached by the nodes. The nodes share the cached data with its neighboring nodes to reduce the communication overhead. However, the identification of the information to be cached determines its efficacy (Jorge et al., 2019; Zhang et al., 2018b).

IoT networks which depend on fog and cloud computing, consume considerable energy to access the cloud services, which can substantially bring down the energy possessed by the IoT sensors and devices. To this end, the present day IoT networks use edge computing as a tool to reduce the energy load on communication and computational overheads. Edge computing facilitates the availability of computational and storage resources at the edge of the network (Ghosh and Grolinger, 2021; Wang et al., 2022). As a result, the energy consumed on communication & computational overheads is substantially reduced. However, to access edge and cloud computing platforms, the sensors and IoT devices need to be equipped with additional hardware/software resources. Therefore, considering the costs involved in the use of these additional resources, data aggregation algorithms need to arrive at an optimal tradeoff between NLT and energy efficiency.

7.2. Tradeoffs and optimization

Some of the popular strategies for optimization in WSN and IoT networks are (a) node clustering, (b) transmission power control, (c) effective management of *sleep* state of nodes, (d) assigning fair band width to address network congestion, (e) bio-inspired optimization techniques for selection of CH, (f) use of edge, fog and cloud computing platforms, etc (Moulik et al., 2019). In event-driven applications, the occurrence of an event is unpredictable and hence there can be occasions when a network may encounter sudden increase in the events. An effective strategy to manage such occurrences, and prevent congestion hotspots is to employ a demand-driven band width assignment strategy, where the nodes with higher traffic loads are assigned a *fair* amount of bandwidth (Miller et al., 2005; Raman and James, 2019; Yarde et al., 2019). The Fairness Aware Congestion Control (FACC) protocol applies a probabilistic function based on a packet-drop threshold to estimate the traffic load at critical/intermediary nodes (Yarde et al., 2019). To estimate how busy a channel is likely to be in a given time interval, a channel *busyness ratio* is determined by considering the total length of busy periods in a defined time interval. Smaller the busyness ratio of an intermediary node, lower is the traffic load, while a higher busyness ratio indicates node-congestion, which needs to be eased by fair allocation of bandwidth. Unlike FACC, which considers how busy a channel is (busyness ratio), the Priority-based Congestion Control Protocol (PCCP) centers its strategy on (a) estimating the traffic flow in a channel by determining the *congestion degree,* defined as the ratio the packet inter-arrival time, to the time taken to service the packets, and (b) a priority index to indicate the importance of the node. Based on the two parameters, a weighted-fairness priority index is determined to allocate the bandwidth, in order to reduce congestion and improve energy-efficiency.

8. Conclusion and areas for future research

Some of the gap areas in the current approaches on data aggregation, which can well become areas for future research are presented below.

Estimation of residual energy: Data aggregation approaches based on CH or head node selection, like LEACH, HEED, PEGASIS, PEDAP etc., tacitly assume that the residual energy of each node in the network is known apriori. However, this assumption is far from reality, and it is extremely difficult to model the energy consumption pattern of various heterogeneous devices in the network. Though -some attempts were made to estimate the residual energy by developing models that try to piggyback the state information on control packets, they cannot be used to determine node residual energies in large WSN and IoTs. For these networks we propose the use of Bio-inspired learning (Huo et al., 2020; Miranda et al., 2019; Nayak et al., 2019; Wang et al., 2019; García-Nájera et al., 2011; Khan et al., 2019; Ahmad et al., 2018; Esmaeili and Jamali, 2016) and fuzzy based algorithms to dynamically estimate the residual energies. The learning algorithms need to factor the transmission loads, network congestion, number of transactions performed, active and sleep states of each node in the network, to arrive at a reasonable estimate of residual energies.

Efficient management of duty cycles and routing protocols to optimize energy consumption: The duty cycles in most MAC based protocols are usually governed by extraneously imposed SYNC control messages. This forces a node to stay *awake* even if it is not receiving any signal. In large WSNs and IoTs there can be substantial energy savings if the sleep schedules of the nodes in the network are intelligently coordinated. We propose the use of AI & ML and bio-inspired techniques to dynamically determine the sleep schedule of a node by estimating the transmission loads of its neighbours. To factor the deviations if any in the estimate, an upper bound for the sleep state can be evaluated. Based on this upper bound, the node can switch to *awake* state to receive transmissions if necessary.

In most applications, Data Centric (DC) and Address Centric (AC) routing schemes are used in isolation. However, due to the heterogeneity of IoT networks, there can be large variation in the nature of nodes located in a particular segment. To leverage the advantage of both AC and DC routing in IoT networks, we propose the development of an intelligent hybrid model where DC routing is used in closely packed nodes and AC routing in other segments.

As the number of transactions in IoT networks is quite large and non-deterministic in nature, resource optimization throws open several research challenges. Development of traditional heuristic approaches to address these challenges may be quite tedious. We propose the use of bioinspired techniques to develop fuzzy classifiers, appropriate membership & fitness functions; for clustering, CH selection, determination of low-latency paths, and intelligent usage of duty cycles to optimize the energy consumption.

Optimum utilization of network resources: Energy and bandwidth are the prime resources for WSN and IoT networks. Most FACC schemes do not consider the criticality of a node in the data aggregation process while allocating bandwidth. As a result, the near-sink nodes which are critical to the data aggregation process are not given a higher priority. We propose the determination of a criticality index that defines the priority of a node. The FACC algorithms can use the criticality index while allocating bandwidths.

In addition to the approaches stated above to conserve energy, *intelligence on the edge*, is turning out to be a popular to tool to reduce latency and energy, storage & communication loads (Ni et al., 2019, Martinez et al., 2017). To exploit the full potential of edge, fog and cloud computing technologies, we propose to integrate the NextGen technologies like 5G, IPV6 for seamless exchange of data for data aggregation, and for providing QoS guarantees.

Failure detection models: Most works on fault-tolerance in WSN do not specifically address issues related to failure detection. Instead, they attempt to develop fault-tolerant strategies on the assumption that failures are known or, are already detected. However, for these approaches to be more effective, an attempt must be made to (a) track the failures in real-time, and (b) carryout root-cause analysis; in order to prevent the occurrence of such faults. The use of Artificial Neural Networks (ANN), Fuzzy Neural Nets (FNN), Bayesian Networks (BN) and SVM have emerged as some of the most popular fault detection tools in WSN and IoT networks (Lo et al., 2019). However, these tools have their own limitations. SVM can work admirably well even with limited training data. However, in applications where the support vectors are large in number, its efficiency is compromised. ANN is computationally intensive and is prone to overfitting problem. BN, which relies on tree construction is of limited use in non-hierarchical networks. Domain expertise is necessary for FNN to be effective. Considering these limitations, a concerted research effort to develop new AI & ML and bio-inspired algorithms to leverage the strength of these tools is necessary.

8.1. Conclusion

A comprehensive review of the contributions made by the researchers' world over in data aggregation in WSN and IoT networks is presented in the paper. A comparative study of survey papers on WSN and IoT networks with particular reference to their focus, scope, areas covered and limitations, were discussed to highlight the contribution of our survey. While presenting a brief overview of the features of WSN and IoT networks, we discussed some of the similarities and distinctions between the two networks. Data compaction techniques are effective tools to reduce the data processing load in a network. We have discussed various data compaction techniques like data compression, data aggregation and data fusion and highlighted their relative merits and demerits. We discussed in detail the data aggregation process and various timing models of data aggregation in the paper. Based on the approach followed in aggregating data, we classified the data aggregation approaches, and presented a taxonomy of the approaches based on this classification. We have presented an in-depth survey of data aggregation protocols based on their ability to address issues related into topology, interference, fault-tolerance, security and mobility. In data aggregation approaches based on topological structure, we discussed various protocols developed for hierarchical and non-hierarchical topologies. A comparison of various protocols and algorithms was presented to highlight their operational mechanism, advantages and limitations. We presented a similar comparative study of the approaches followed in data aggregation protocols that address interference, fault-tolerance, security and mobility. While discussing the data aggregation protocols, we have presented a study on their applicability to IoT networks. Some of the advanced techniques like bio-inspired learning algorithms used in the development of data aggregation algorithms were discussed in the paper. We have discussed at length the competing requirement and tradeoffs necessary to optimize various resources like node energy, communication bandwidth, communication and computational capability, etc. We also discussed the tradeoffs necessary for various optimization parameters like latency, data accuracy, temporal correctness, data freshness, network lifetime, network coverage, connectivity and capacity. We highlighted few gap areas in the present research approaches and suggested research directions to plug the gap areas identified.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Abdelgawad, A., Bayoumi, M., 2012. Data Fusion in WSN. Resource-aware data fusion algorithms for wireless sensor networks. Lecture Notes in Electr. Eng. 118, 17–35.

Aggarwal, S., Nasipuri, A., 2019. Survey and performance study of emerging LPWAN technologies for IoT applications. In: IEEE 16th Int. Conf. on Smart Cities: Improving Quality of Life Using ICT & IoT and AI (HONET-ICT), pp. 069–073.

Ahmad, M., Ikram, A., Wahid, I., Inam, M., Ayub, N., Ali, S., 2018. A bio-inspired clustering scheme in wireless sensor networks: BeeWSN. Procedia Comput. Sci. 130, 206–213. https://doi.org/10.1016/j.procs.2018. 04.031.

Ahmed, A., Abdullah, S., Bukhsh, M., Ahmad, I., Mushtaq, Z., 2022. An energy-efficient data aggregation mechanism for IoT secured by Blockchain. IEEE Access 10, 11404–11419. https://doi.org/10.1109/ACCESS.2022.3146295.

Alkhamisi, A., Nazmudeen, M. S. H., Buhari, S. M., 2016. A cross-layer framework for sensor data aggregation for IoT applications in smart cities. 2016 IEEE Int. Smart Cities Conference (ISC2), pp. 1-6, doi: 10.1109/ISC2.2016.7580853.

Amarlingam, M., Mishra, M., Rajalakshmi, P., Sumohana, Channappayya, S., Sastry, C. S., 2018. Novel Light Weight Compressed Data Aggregation using sparse measurements for IoT networks. J. Network Comput. Appl. 121.

An, M.K., Cho, H., 2015. Efficient data collection in interference-aware wireless sensor networks. J. Networks 10 (12), 658–667.

An, M. K., Cho, H., Zhou B., Chen, L., 2019. Minimum latency aggregation scheduling in internet of things. Int. Conf. on Computing, Networking and Communications (ICNC), pp. 395-401. doi: 10.1109/ICCNC.2019.8685660.

Bagaa, M., Derhab, A., Lasla, N., Ouadjaout, A., Badache, N., 2012. Semistructured and unstructured data aggregation scheduling in wireless sensor networks. In: Proc. IEEE INFOCOM'12, pp. 2671– 2675.

Basumatary, H., Barma, M.K.D., 2019. Analysis of mobile sink based routing protocols in wireless sensor networks. Int. J. Comput. Intell. IoT 2 (3) https://ssrn.com/abstract=3358300.

Begum, B.A., Nandury, S.V., 2015. Composite interference mapping model for interference fault-free transmission in WSN. In: Proc. of Int. Conf. on Advances in Comput., Commun. and Informatics, pp. 2119–2125.

Begum, B.A., Nandury, S.V., 2022a. Component-based self-healing approach for fault-tolerant data aggregation in WSN. IEEE Access 10, 73503–73520.

Begum, B.A., Nandury, S.V., 2022b. Composite Interference Mapping Model to Determine Interference-Fault Free Schedule in WSN. IEEE Access 10, 107505–107525. https://doi.org/10.1109/ACCESS.2022.3211654.

Behera, T.M. et al., 2018. Energy-efficient modified LEACH protocol for IoT application. IET Wireless Sens. Syst. 8 (5), 223–228.

Cam, H., Ozdemir, S., Nair, P., Muthuavinashiappan, D., Ozgur Sanli, H., 2006. Energy-efficient secure pattern based data aggregation for wireless sensor networks. J. Comput. Commun. 29 (4), 446–455.

Cardieri, P., 2010. Modeling interference in wireless ad hoc networks. IEEE Commun. Surveys Tuts. 12 (4), 551–572. 4th Quart.

Chan, H., Perrig, A., Song, D., 2006. Secure hierarchical in-network aggregation in sensor networks. In: Proc. of 13th ACM Conf. on Comput. and Commun. Security, pp. 278–287.

Chand, S., Singh, S., Kumar, B., 2014. Heterogeneous HEED protocol for wireless sensor networks. Wireless Personal Commun. 77, 2117–2139. https://doi.org/10.1007/s11277-014-1629-y.

Chen, C., Lin, Y., Lin, Y., Sun, H., 2012a. RCDA: Recoverable concealed data aggregation for data integrity in wireless sensor networks. IEEE Trans. Parallel Distrib. Syst. 23 (4), 727–734. https://doi.org/10.1109/TPDS.2011.219.

Chen, S., Tang, S., et al., 2012b. Capacity of data collection in arbitrary wireless sensor networks. IEEE Trans. Parallel Distrib. Syst. 23 (1).

Chen, S., Wang, Y., Li, X.Y., et al., 2011. Capacity of data collection in randomly-deployed wireless sensor networks. Wireless Netw. 17, 305–318. https://doi.org/10.1007/s11276-010-0281-z.

Chen, Q., Wu, L., Jiang, C., 2022. ES-PPDA: an efficient and secure privacy-protected data aggregation scheme in the IoT with an edge-based XaaS architecture. J. Cloud Comp. 11 (20). https://doi.org/10.1186/s13677-022-00295-5.

Cui, J., Shao, L., Zhong, H., Xu, Y., Liu, L., 2018. Data aggregation with end-to-end confidentiality and integrity for large-scale wireless sensor networks. Peer-to-Peer Netw. Appl. 11 (5), 1022–1037. https://doi.org/10.1007/s12083-017-0581-5.

Dehkordi, S.A., Farajzadeh, K., Rezazadeh, J., et al., 2020. A survey on data aggregation techniques in IoT sensor networks. Wireless Netw. 26 (2), 1243–1263. https://doi.org/10.1007/s11276-019-02142-z.

Durisic, M. P., Tafa, Z., Dimic, G., Milutinovic, V., 2012. A survey of military applications of wireless sensor networks. 2012 Mediterranean Conference on Embedded Computing (MECO), pp. 196–199, Bar, Montenegro.

Elijah, O., Rahman, T.A., Orikumhi, I., Leow, C.Y., Hindia, M.N., 2018. An overview of Internet of Things (IoT) and data analytics in agriculture: Benefits and challenges. IEEE Internet Things J. 5 (5), 3758–3773. https://doi.org/10.1109/JIOT.2018.2844296.

Erman, A.T., Dilo, A., Havinga, P., 2012. A virtual infrastructure based on honeycomb tessellation for data dissemination in multi-sink mobile wireless sensor networks. J Wireless Commun. https://doi.org/10.1186/1687-1499-2012-17. Netw., 2012 (art Id 17.

Erramilli, V., Matta, I., Bestavros, A., 2004. On the interaction between data aggregation and topology control in wireless sensor networks. 2004 1st Annu. IEEE Commun. Society Conf. on Sensor and Ad Hoc Communications and Networks, pp. 557-565, doi: 10.1109/SAHCN.2004.1381958.

Esmaeili, M., Jamali, S., 2016. A Survey: optimization of energy consumption by using the genetic algorithm in wsn based internet of things. CiiT Int. J. Wireless Commun. 8 (2).

Fan Ye, H.L., Cheng, J., Lu S., Zhang, L., 2005. TTDD: Two-tier data dissemination in large-scale wireless sensor networks. J. of Wireless Networks, 11, 161–175. Springer Science + Business Media, Inc.

Feng, Y., Tang, S., Dai, G., 2011. Fault-tolerant data aggregation scheduling with local information in wireless sensor networks. IEEE Tsinghua Sci. Technol. 16 (5), 451–463.

Fitzgerald, E.E. et al., 2018. Energy-optimal data aggregation and dissemination for the internet of things. IEEE Internet of Things J. 5 (2), 955–969.

García-Nájera, A. et al., 2011. Analysis of the multi-objective cluster head selection problem in WSNs. Appl. Soft Comput. 112.

Gavel, S., Charitha, R., Biswas, P., et al., 2021. A data fusion based data aggregation and sensing technique for fault detection in wireless sensor networks. Computing 103, 2597–2618. https://doi.org/10.1007/s00607-021-01011-y.

Ghosh, M., Grolinger, K., 2021. Edge-cloud computing for internet of things data analytics: embedding intelligence in the edge with deep learning. IEEE Trans. Ind. Inf. 17 (3), 2191–2200.

Gravina, R., Fortino, G., 2021. Wearable body sensor networks: State-of-the-art and research directions. IEEE Sens. J. 21 (11), 12511–12522. https://doi.org/10.1109/JSEN.2020.3044447.

Grining, K., Klonowski, M., Syga, P., 2019. On practical privacy-preserving fault-tolerant data aggregation. Int. J. Inf. Secur. 18, 285–304.

Gupta, P., Kumar, P.R., 2000. The capacity of wireless networks. IEEE Trans. Inf. Theory 46 (2), 388–404.

Hanady, M.A., Bader, A.A., AlRoumi, E., 2018. Usage of mobile elements in internet of things environment for data aggregation in wireless sensor networks. Comput. Electr. Eng. 72, 789–807. https://doi.org/10.1016/j.compeleceng.2017.12.028.

Hasan, M.M., Mouftah, H.T., 2017. Optimization of Watchdog Selection in Wireless Sensor Networks. IEEE Wireless Commun. Lett. 6 (1), 94–97. https://doi.org/10.1109/LWC.2016.2633990.

He, W., Liu, X., Nguyen, H., Nahrstedt, K., Abdelzaher, T., 2007. PDA: Privacy-preserving data aggregation in wireless sensor networks. 26th IEEE Int. Conf. on Comput. Commun., pp. 2045–2053.

Heinzelman, W.B., Chandrakasan, A.P., Balakrishnan, H., 2002. An Application-specific protocol architecture for wireless microsensor networks. IEEE Trans. Wireless Commun. 1 (4), 660–670.

Heinzelman, W.R., Kulik, J., Balakrishnan, H., 1999. Adaptive protocols for information dissemination in wireless sensor networks. In: Proc. of 5th Ann. ACM/IEEE Int. Conf. on Mobile Comput. and Netw., pp. 174–185.

Homaei, M.H., Salwana, E., Shamshirband, S., 2019. An enhanced distributed data aggregation method in the Internet of Things. Sensors (Basel) 19 (14), 3173. https://doi.org/10.3390/s19143173. PMID: 31323905; PMCID: PMC6679339.

Hu, S., Liu, L., Fang, L., Zhou, F., Ye, R., 2020. A novel energy-efficient and privacy-preserving data aggregation for WSNs. IEEE Access 8, 802–813. https://doi.org/10.1109/ACCESS.2019.2961512.

Huang, S.C., Wan, P., Vu, C.T., Li, Y., Yao, F., 2007. Nearly constant approximation for data aggregation scheduling in wireless sensor networks. In: Proc. of IEEE INFOCOM, pp. 366–372.

Huang, B., Yu, J., Ma, C., et al., 2021. Shortest link scheduling in wireless networks under the Rayleigh fading model. J. Wireless Com. Network 135. https://doi.org/10.1186/s13638-021-02011-4.

Huo, J., Deng, X., Mohammed Al-Neshmi, H.M., 2020. Design and improvement of routing protocol for field observation instrument networking based on LEACH protocol. J. of Electrical and Computer Engineering, 2020 (art. Id. 8059353). doi: 10.1155/2020/8059353.

Jan, S.U., Lee, Y.D., Koo, I.S., 2021. A distributed sensor-fault detection and diagnosis framework using machine learning. Inf. Sci. 547, 777–796. https://doi.org/10.1016/j.ins.2020.08.068.

Jesus, P., Almeida, P.S., 2015. A Survey of distributed data aggregation algorithms. IEEE Commun. Surveys Tuts., 17(1), 381-404, 1st Quart. doi: 10.1109/COMST.2014.2354398.

Jiao, X., Lou, W., Wang, X., et al., 2012. Data aggregation scheduling in uncoordinated duty-cycled wireless sensor networks under protocol interference model. Ad-Hoc and Sensor. Wirel. Netw 15.

Jorge, A.G. de Brito et al., 2019. Topology control optimization of wireless sensor networks for IoT applications. In: WebMedia'19: Proc. of 25th Brazillian Symp. on Multimedia and the Web, pp. 477–480. https://doi.org/10.1145/3323503.3361718.

Kale, P., Nene, M.J., 2019. Data Aggregation Trees with QoS in Sensor Networks. IEEE 5th Int. Conf. for Convergence in Technology (I2CT), pp. 1–5.

Kamalesh, S., Kumar, P.G., 2017. Data aggregation in wireless sensor network using SVM-based failure detection and loss recovery. J. Exp. Theoret. Artif. Intell. 29 (1), 133–147. https://doi.org/10.1080/0952813X.2015.1132262.

Kandris, D., Nakas, C., Vomvas, D., Koulouras, G., 2020. Applications of wireless sensor networks: an up-to-date survey. Appl. Syst. Innov. 3 (1), 14. https://doi.org/10.3390/asi3010014.

Kaosar, M.G., Yi, X., 2011. Privacy preserving data gathering in wireless sensor network. In: Network security, administration and management: Advancing technology and practice. IGI Global, USAc, doi: 10.4018/978-1-60960-777-7.ch012.

Kathjoo, M.Y., Khanday, F.A., Banday, M.T., 2018. A Comparative study of WSN and IoT. 2nd Int. Conf. on Advances in Electronics, Computers and Communications (ICAECC), pp. 1–5. doi: 10.1109/ICAECC.2018.8479420.

Kesselman, A.A., Kowalski, D.R., 2006. Fast distributed algorithm for converge cast in ad hoc geometric radio networks. Parallel Distrib. Comput., 578–585

Khan, A., Aftab, F., Zhang, Z., 2019. BICSF: Bio-inspired clustering scheme for FANETs. IEEE Access 7, 31446–31456. https://doi.org/10.1109/ACCESS.2019.2902940.

Khan, H.M., Khan, A., Jabeen, F., Rahman, A.U., 2021. Privacy preserving data aggregation with fault tolerance in fog-enabled smart grids. Sustainable Cities Society 64 (102522). https://doi.org/10.1016/j.scs.2020.102522.

Khatib, M., 2020. Wireless Mesh Networks - Security, Architectures and Protocols. M. Khatib, S. Alsadi (Eds.), London, United Kingdom. https://www.intechopen.com/books/7322 10.5772/intechopen.74910.

Krishnamachari, B., Estrin, D., Wicker, S., 2002. The impact of data aggregation in wireless sensor networks. In: Proc. of 22nd Int. Conf. on Distributed Computing Systems Workshops, pp. 575–578.

Kulik, J., Heinzelman, W.R., et al., 2002. Negotiation-based protocols for disseminating information in wireless sensor networks. Wireless Netw. 8, 169–185.

Lai, Y., Lin, H., Yang, F., Wang, T., 2019. Efficient data request answering in vehicular ad-hoc networks based on fog nodes and filters. Futur. Gener. Comput. Syst. 93, 130–142.

Lai, Y., Yang, F., et al., 2018. Fog-based two-phase event monitoring and data gathering in vehicular sensor networks. Sensors 18 (1), 82.

Laiou, A. et al., 2019. Autonomous fault detection and diagnosis in wireless sensor networks using decision trees. J. Commun. 14 (7).

Lam, N.X., An, M.K., Huynh, D.T., Nguyen, T. N., 2013. Scheduling problems in interference-aware wireless sensor networks. 2013 Int. Conf. on Computing, Networking and Commun. (ICNC), 2013, pp. 783–789, doi: 10.1109/ICCNC.2013.6504188.

Lee, M., Choi, Y., 2008. Fault Detection of Wireless Sensor Networks. Computer Commun. 31 (14), 3469–3475.

Lee, J., Krishnamachari, B., Kuo, C.C.J., 2004. Impact of energy depletion and reliability on wireless sensor network connectivity. In: Proc. of SPIE & Security, Digital Wireless Commun. VI, 5440, pp. 169–180. doi: 10.1117/12.542491.

Li, H. et al., 2014. Latency-minimizing data aggregation in wireless sensor networks under physical interference model. J. Ad Hoc Networks 12, 52–68.

Li, X., Moaveni-Nejad, K., Song, W., Wang, W., 2005. Interference-aware topology control for wireless sensor networks. 2005 2nd Annu. IEEE Commun.Society Conf. on Sensor and Ad Hoc Commun. and Netw., pp. 263–274, doi: 10.1109/SAHCN.2005.1557081.

Li, X.Y., Xu, X., Wang, S., Tang, S., Dai, G.J., Zhao, J.Z., Qi, Y., 2009. Efficient data aggregation in multi-hop wireless networks under physical interference model. IEEE 6th Int. Conf. on Mobile Adhoc and Sensor Systems (MASS'09), pp. 353–362.

Li, Z., Liu, Y., Shin, K.G., Liu, J., Yan, Z., 2019. Interference Steering to Manage Interference in IoT. IEEE Internet of Things J. 6 (6), 10458–10471.

Li, C., Wu, D., Yu, Q., Lau, F., 2013. Aggregation latency-energy tradeoff in wireless sensor networks with successive interference cancellation. IEEE Trans. Parallel Distrib. Syst. 24 (11), 2160–2170. https://doi.org/10.1109/TPDS.2012.314.

Liang, H., Yang, S., Li, L., et al., 2019. Research on routing optimization of WSNs based on improved LEACH protocol. J. Wireless Comm. Network, 194. https://doi.org/10.1186/s13638-019-1509-y.

Lin, J., Chelliah, P.R., Hsu, M., Hou, J., 2019. Efficient fault-tolerant routing in IoT wireless sensor networks based on bipartite-flow graph modelling. IEEE Access 7, 14022–14034. https://doi.org/10.1109/ACCESS.2019.2894002.

Lin, H., Kim, K.S., Shin, W.-Y., 2020. Interference-aware opportunistic random access in dense IoT networks. IEEE Access 8 (93472–93486), 2020. https://doi.org/10.1109/ACCESS.2020.2996221.

Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., Zhao, W., 2017. A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. IEEE Internet Things J. 4 (5), 1125–1142. https://doi.org/10.1109/JIOT.2017.2683200.

Lindsey, S., Raghavendra, C., Sivalingam, K.M., 2002. Data gathering algorithms in sensor networks using energy metrics. IEEE Trans. Parallel Distrib. Syst. 13 (9), 924–935.

Liu, X., Yu, J., Li, F., Lv, W., Wang, Y., Cheng, X., 2020. Data aggregation in wireless sensor networks: From the perspective of security. IEEE Internet Things J. 7 (7), 6495–6513. https://doi.org/10.1109/JIOT.2019.2957396.

Lo, N.G., Flaus J.M.C., Adrot, O., 2019. Review of machine learning approaches in fault diagnosis applied to IoT systems. Int. Conf. on Control, Automation and Diagnosis (ICCAD), pp. 1-6. doi: 10.1109/ICCAD46983.2019.9037949.

Lokhande, M.P., Patil, D.D., 2022. Enhancing the energy efficiency by LEACH protocol in IoT. Int. J. Comput. Sci. Eng. 5 (1), 1–10. https://doi.org/10.1504/ijcse.2022.120783.

Lu, R., Heung, K., Lashkari, A.H., Ghorbani, A.A., 2017. A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT. IEEE Access 5, 3302–3312. https://doi.org/10.1109/ACCESS.2017.2677520.

Ma, J., Lou, W., Li, X.-Y., 2014. Contiguous link scheduling for data aggregation in wireless sensor networks. IEEE Trans. Parallel Distribut. Syst. 25 (7), 1691–1701. https://doi.org/10.1109/TPDS.2013.296.

Madden, S.R., Franklin, M.J., Hellerstein, J.M., Hong, W., 2002. TAG: A Tiny aggregation service for ad-hoc sensor networks. ACM SIGOPS Operat. Syst. Rev. 36 (SI), 131–146.

Mahapatro, A., Khillar, P., 2012. Transient fault tolerant wireless sensor networks. Science Direct Procedia Technol. 4, 97–101.

Martinez, I.S.H., Daza, J., Salcedo, I.B.S.R., 2017. IoT application of WSN on 5G infrastructure. 2017 Int. Symposium on Networks, Computers and Communications (ISNCC), pp. 1–6. doi: 10.1109/ISNCC.2017.8071989.

Metzger, F. et al., 2019. Modeling of aggregated IoT traffic and its application to an IoT cloud. Proc. IEEE 107, 679–694.

Miller, M. J., Sengul, C., Gupta, I., 2005. Exploring the energy-latency trade-off for broadcasts in energy-saving sensor networks. In: Proc. of 25th IEEE Int. Conf. on Distrib. Comput. Syst. (ICDCS), pp. 17–26.

Miranda, K., Zapotecas-Martínez, S., López-Jaimes, A., García-Nájera, A., 2019. A comparison of bio-inspired approaches for the cluster-head selection problem in WSN. In: Shandilya, S., Shandilya, S., Nagar, A. (Eds.), Advances in Nature-inspired Computing and Applications. EAI/Springer innovations in Communication and Computing. Springer, Cham. https://doi.org/10.1007/978-3-319-96451-5_7.

Mohammed, F.A.B., Mekky, N., Suleiman, H.H., Hikal, N.A., 2022. Sectored LEACH (S-LEACH): an enhanced LEACH for wireless sensor network. IET Wireless Sens. Syst. 12 (2), 56–66.

Moscibroda, T., Wattenhofer, R., 2006b. The complexity of connectivity in wireless networks. In: IEEE Ann. Joint Conf. of the IEEE Computer and Commun. Soc. - INFOCOM, pp. 1–13.

Moscibroda, T., Wattenhofer, R., Zollinger, A., 2006a. Topology control meets SINR: the scheduling complexity of arbitrary topologies. In: Proc. 7th ACM Int. symposium on Mobile ad hoc networking and computing (MobiHoc'06). Association for Computing Machinery, New York, NY, USA, 310–321. https://doi.org/10.1145/1132905.1132939.

Moulik, S., Misra, S., Chakraborty, C., 2019. Performance evaluation and delay-power trade-off analysis of zigbee protocol. IEEE Trans. Mob. Comput. 18 (2), 404–416. https://doi.org/10.1109/TMC.2018.2836456.

Moussa, H.G., Zhuang, W., 2020. Energy- and delay-aware two-hop NOMA-enabled massive cellular IoT communications. IEEE Internet Things J. 7 (1), 558–569. https://doi.org/10.1109/JIOT.2019.2951584.

Nabil, Y., Sawy, H.E., Al-Dharrab, S., Mostafa, H., Attia, H., 2022. Data aggregation in regular large-scale IoT etworks: Granularity, reliability, and delay tradeoffs. IEEE Internet Things J. 9 (18), 17767–17784. https://doi.org/10.1109/JIOT.2022.3160970.

Nandury, S.V., Begum, B.A., 2015. Smart WSN-based ubiquitous architecture for smart cities. In: Proc. of Int. Conf. on Advances in Comput., Commun. and Informatics, Kochi, 2015, pp. 2366–2373.

Nayak, P., Kavitha, K., Khan, N., 2019. Cluster head selection in wireless sensor network using bio-inspired algorithm. TENCON 2019, 1690–1696. https://doi.org/10.1109/TENCON.2019. 8929440.

Nguyen, T.N., Ho, C.V., Le, T.T.T., 2019. A topology control algorithm in wireless sensor networks for IoT-based applications. In: 2019 Int. Symposium on Electrical and Electronics Engineering (ISEE), pp. 141–145.

Nguyen, T.-D., Le, D.-T., Vo, V.-V., Kim, M., Choo, H., 2021. Fast sensory data aggregation in IoT networks: collision-resistant dynamic approach. IEEE Internet Things J. 8 (2), 766–777. https://doi.org/10.1109/JIOT.2020.3007329.

Ni, J., Lin, X., Shen, X.S., Mar, A., 2019. Toward edge-assisted internet of things: from security and efficiency perspectives. IEEE Netw. 33 (2), 50–57.

Orsson, M.H., Mitra, P., 2012. Wireless connectivity and capacity. Symp. Discrete Algorithms (SODA), 516–526.

Parmar, K., Jinwala, D.C., 2016. Concealed data aggregation in wireless sensor networks: A comprehensive survey. Comput. Netw. 103, 207–227. https://doi.org/10.1016/j.comnet.2016.04.013.

Prashanth, J.S., Nandury, S.V., 2019. A cluster–based approach for minimizing energy consumption by reducing travel time of mobile element in WSN. Int. J. Comput. Commun. Control 14 (6), 691–709. ISSN 1841–9836, e-ISSN 1841–9844.

Przydatek, B., Song, D., Perrig, A., 2003. SIA: Secure information aggregation in sensor networks. In: Proc. of the 1st Int. Conf. on Embedded networked sensor Syst. (SenSys '03), pp. 255–265.

Pu, Y., Luo, J., Hu, C., Yu, J., Zhao, R., Huang, H., Xiang, T., 2019. Two secure privacy-preserving data aggregation schemes for IoT. Wireless Commun. Mobile Comput. 2019, 1–11.

Rahman, H., Ahmed, N., Hussain, I., 2016. Comparison of data aggregation techniques in internet of things (IoT). 2016 Int. Conf. on Wireless Communications, Signal Processing and Networking (WiSPNET), 2016, pp. 1296-1300. doi: 10.1109/WiSPNET.2016.7566346.

Raman, C.J., James, V., 2019. FCC: fast congestion control scheme for wireless sensor networks using hybrid optimal routing algorithm. Clust. Comput. 22, 12701–12711.

Ray, P.P., 2018. A survey on internet of things architectures. J. of King Saud University – Computer and Information Sciences, 30(3), 291-319. doi: 10.1016/j.jksuci. 2016.10.003.

Rehena, Z., et al., 2011. A modified SPIN for wireless sensor networks. 3rd Int. Conf. on Commun. Syst. and Netw. (COMSNETS 2011), pp. 1–4.

Ren, J., He, Y., Huang, G., Yu, G., et al., 2019. An edge computing based architecture for mobile augmented reality. IEEE Netw. 33 (4), 162–169.

Rezaeibagha, F., Mu, Y., Huang, K., Chen, L., 2021. Secure and efficient data aggregation for IoT monitoring systems. IEEE Internet Things J. 8 (10), 8056–8063. https://doi.org/10.1109/JIOT.2020.3042204.

Saha, T., Mahapatra, S., 2011. Distributed fault diagnosis in wireless sensor networks. IEEE Int. Conf. on Process Automation, Control and Comput., 1–5

Saleem et al., 2020. FESDA: fog-enabled secure data aggregation in smart grid IoT network. IEEE Internet Things J. 7 (7), 6132–6142. https://doi.org/10.1109/JIOT.2019.2957314.

Salman, T., Jain, R., 2017. A survey of protocols and standards for the internet of things. Adv. Comput. Commun. 1 (1).

Shim, K., Park, C., 2015. A secure data aggregation scheme based on appropriate cryptographic primitives in heterogeneous wireless sensor networks. IEEE Trans. Parallel Distrib. Syst. 26 (8), 2128–2139.

Sridhar, P., Madni, A.M., Jamshidi, M., 2007. Hierarchical Aggregation and Intelligent Monitoring and Control in Fault-Tolerant Wireless Sensor Networks. IEEE Syst. J. 1 (1), 38–54.

Stankovic, J.A., 2014. Research directions for the internet of things. IEEE Internet Things J. 1 (1), 3–9. https://doi.org/10.1109/JIOT.2014.2312291.

Tan, H.O., Korpeoglu, I., 2003. Power efficient data gathering and aggregation in wireless sensor networks. ACM SIGMOD Rec. 32 (4), 66–71.

Tang L., Li, Q.L., 2009. S-SPIN: a provably secure routing protocol for wireless sensor networks. 2009 Int. Conf. on Commun. Software and Netw., pp. 620–624. doi: 10.1109/ICCSN.2009.8.

Tang, W., Ren, J., Deng, K., Zhang, Y., 2019. Secure data aggregation of lightweight E-healthcare IoT devices with fair incentives. IEEE Internet Things J. 6 (5), 8714–8726. https://doi.org/10.1109/JIOT.2019.2923261.

Tripathi, A., Gupta, H.P., Dutta, T., Mishra, R., Shukla, K.K., Jit, S., 2018. Coverage and connectivity in WSNs: A survey, research issues and challenges. IEEE Access 6, 26971–26992. https://doi.org/10.1109/ACCESS.2018.2833632.

Ullah, A. et al., 2020. Fog-assisted secure healthcare data aggregation scheme in IoT-enabled WSN. Peer-to-Peer Netw. Appl. 13, 163–174.

Vasan, S., Kalra, N., Kumar, R., Dhiman, G., 2021. Mobile agent assisted I-leach clustering protocol for IoT application. In: Materials Today: Proceedings, Apr. 2021. https://doi.org/10.1016/j.matpr.2021.03.257.

Vejlgaard, B., Lauridsen, M., Nguyen, H., Kovacs, I.Z., Mogensen, P., Sorensen, M., 2017. Interference impact on coverage and capacity for low power wide area IoT networks. 2017 IEEE Wireless Communications and Networking Conference (WCNC), pp. 1–6. doi: 10.1109/WCNC.2017.7925510.

Wan, P.J. et al., 2004. Distributed construction of connected dominating set in wireless ad hoc networks. Mobile Netw. Appl. 9 (2), 41–149.

Wan, P., Huang, S.C., Wang, L., Wan, Z., Jia, X., 2009. Minimum latency aggregation scheduling in multihop wireless networks. ACM Mobile ad hoc Netw. Comput., 185–194

Wang, N.C. et al., 2013. Grid-based data aggregation for wireless sensor networks. J. Adv. Comput. Networks 1 (4), 329–333.

Wang, X., Garg, S., Lin, H., Kaddoum, G., Hu, J., Hossain, M.S., 2022. A secure data aggregation strategy in edge computing and blockchain empowered internet of things. IEEE Internet Things J. 9 (16), 14237–14246. https://doi.org/10.1109/JIOT.2020.3023588.

Wang, N., Hsu, W., 2020. Energy efficient two-tier data dissemination based on Q-learning for wireless sensor networks. IEEE Access 8, 74129–74136. https://doi.org/10.1109/ACCESS.2020.2987861.

Wang, Z., Ong, Y.-S., Sun, J., Gupta, A., Zhang, Q., 2019. A generator for multiobjective test problems with difficult-to-approximate pareto front boundaries. IEEE Trans. Evol. Comput. 23 (4), 556–571. https://doi.org/10.1109/TEVC.2018.2872453.

Xu, C. et al., 2022. Privacy-preserving and fault-tolerant aggregation of time-series data with a semi-trusted authority. IEEE Internet of Things J. 9 (14), 12231–12240. https://doi.org/10.1109/JIOT.2021.3135049.

Xu, X., Wang, S., Mao, X., Tang, S., Li, X.Y., 2009. An improved approximation algorithm for data aggregation in multi-hop wireless sensor networks. ACM workshop on Foundations of wireless ad hoc and sensor Netw. and Comput., pp. 47–56.

Xu, X., Liang, W., Wark, T., 2011a. Data quality maximization in sensor networks with a mobile sink. 2011 International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS), Barcelona, pp. 1–8. doi: 10.1109/DCOSS.2011.5982160. IEEE.

Xu, X., Lou, W., Liu, X., Tang, S., 2011c. Delay efficient link and aggregation scheduling under physical interference model. 2011 IEEE Eighth Int. Conf. on Mobile Ad-Hoc and Sensor Systems, pp. 421–429. doi: 10.1109/MASS.2011.49.

Xu, X., Li, X.Y., Mao, X., Tang, S., Wang, S., 2011b. A delay-efficient algorithm for data aggregation in multihop wireless sensor network. IEEE Trans. Parallel Distrib. Syst. 22 (1).

Xue H., Huang, B., Qin, M., Zhou H., Yang, H., 2020. Edge computing for internet of things: A survey. In: Int. Conf. on Internet of Things, pp. 755–760.

Yadav, S. A., T. Poongodi, T., 2021. A review of ML based fault detection algorithms in WSNs. 2021 2nd Int. Conf. on Intelligent Engineering and Management (ICIEM), London, UK, pp. 615–618, doi: 10.1109/ICIEM51511.2021.9445384.

Yang, L., Ding, C., Wu, M., 2015. RPIDA: Recoverable privacy-preserving integrity-assured data aggregation scheme for wireless sensor networks. KSII Trans. Internet Inf. Syst. 9 (12).

Yarde, P., Srivastava, S., Garg, K., 2019. A delay abridged judicious cross-layer routing protocol for wireless sensor network. IEEE 4th Int. Conf. on Computer and Commun. Systems (ICCCS), pp. 634–638.

Younis, M., Senturk, I.F., Akkaya, K., Lee, S., Senel, F., 2014. Topology management techniques for tolerating node failures in wireless sensor networks: A survey. J. Comput. Netw. 58, 254–283.

Yousefi, H. et al., 2015. Fast aggregation scheduling in wireless sensor networks. IEEE Trans. Wireless Commun. 14 (6), 3402–3414.

Yousefpoor, M.S., Yousefpoor, E., Barati, H., Barati, A., Movaghar, A., Hosseinzadeh, M., 2021. Secure data aggregation methods and countermeasures against various attacks in wireless sensor networks: A comprehensive review. J. Network Comput. Appl. 190. https://doi.org/10.1016/j.jnca.2021.103118.

L. Zhang et al., 2012. Fault-tolerant scheduling for data collection in wireless sensor networks. 2012 IEEE Global Commun. Conf., pp. 5345–5349.

Zhang, Z., Lung, C., Lambadaris, I., St-Hilaire, M., 2018. IoT data lifetime-based cooperative caching scheme for ICN-IoT networks. 2018 IEEE International Conference on Communications (ICC), pp. 1–7.

Zhang, T., Song, X., Xiongfei, L., Zheng, H., Han, Y., Kai, Q., 2021a. Towards time-sensitive and verifiable data aggregation for mobile crowdsensing. Hindawi Security Commun. Netw. 2021. https://doi.org/10.1155/2021/6679157.

Zhang, P., Wang, J., Guo, K., Wu, F., Minc, G., 2018a. Multi-functional secure data aggregation schemes for WSNs. Adhoc. Networks 69, 86–89.

Zhang, M., Zhang, H., Yuan, D., Zhang, M., 2021b. Learning-based sparse data reconstruction for compressed data aggregation in IoT networks. IEEE Internet Things J. 8 (14), 11732–11742.

Zhang, J., Zong, Y., Yang, C., Miao, Y., Guo, J., 2019. LBOA: Location-Based Secure Outsourced Aggregation in IoT. IEEE Access 7, 43869–43883. https://doi.org/10.1109/ACCESS.2019.2908429.

Zhang, J., Zhao, Y., Wu, J., Chen, B., 2020. LVPDA: A lightweight and verifiable privacy-preserving data aggregation scheme for edge-enabled IoT. IEEE Internet Things J. 7 (5), 4016–4027. https://doi.org/10.1109/JIOT. 2020. 2978286.

Zhu, C., Wu, S., et al., 2015. A tree-cluster-based data-gathering algorithm for industrial WSNs with a mobile sink. IEEE Access 3, 381–396.

Zhu, G., Xu, J., Huang, K., Cui, S., 2021. Over-the-air computing for wireless data aggregation in massive IoT. IEEE Wirel. Commun. 28 (4), 57–65. https://doi.org/10.1109/MWC.011.2000467.