International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 13 Issue: 04 | Apr 2026 www.irjet.net p-ISSN: 2395-0072

Reliability and Fault-tolerance Enhancement of Wireless Sensors Networks for Cyber Physical Systems: A Review

Islam B.M.Yousif [1], Yousif E.E.Ahmed [2], Sally D.Awadalkareem [3]

University of Gezira, Faculty of Engineering and Technology, Gezira State, Sudan

***

Abstract - *Wireless Sensor Networks (WSNs) play an important role in Cyber-Physical Systems (CPS) within Industry 4.0, supporting the interaction between physical and computational systems. WSNs are deployed in various environments to collect critical data and are expected to operate reliably for extended periods. However, achieving reliable communication is still challenging due to node failures, link disconnections, limited energy, and harsh conditions. This paper aims to review the main approaches used to enhance reliability and fault tolerance in WSN-based CPS. The study proposes a taxonomy that classifies existing work into main groups: reliability metrics, modeling and evaluation methods, enhancement techniques, protocols and open challenges. Several well-known protocols, including E2SRT, GARUDA, and RCRT are compared in terms of their strengths and limitations. Recent trends using machine learning and neural networks for fault detection and reliability improvement are highlighted. Results show that these approaches can improve performance and reduce cost, but their effectiveness depends on the network conditions. Overall, it is clear that no single method can achieve the best reliability in all situations; therefore, combining different techniques is often necessary. Finally, key open challenges are discussed, including the inherent trade-off between energy efficiency and high reliability, the need for robust mobility support and integration of lightweight security mechanisms that do not compromise fault tolerance.*

***Key Words*: Wireless Sensor Network (WSN), Cyber Physical System (CPS), Reliability, Fault Tolerance, Multipath Routing, Network Optimization, Energy Efficiency, Machine Learning.**

1. INTRODUCTION

The Industrial Revolution 4.0 represents a major transformation in modern industrial systems by integrating physical processes with intelligent computing technologies. Cyber-Physical Systems play a central role in enabling interaction between computational and physical components [1],[2]. Wireless Sensor Networks represent a fundamental infrastructure component of CPS, enabling real-time data collection, monitoring and communication across distributed environments, with extensive research addressing energy consumption, node reliability, and fault management [3],[4],[5].

WSNs consist of distributed sensor nodes communicating wirelessly to transmit sensed data to sink node [6]. Due to deployment in dynamic or harsh environments a failure may occur in node or link, these failures can affect system performance, leading to connection loss, data loss, and overall network degradation [7],[8]. Furthermore, the state of nodes and links changes over time, which directly affects system reliability over time as reported in several studies [9],[10]. As a result, significant research has been conducted on reliability modelling, message delay analysis and fault tolerance mechanisms in WSN including routing strategies, comparative protocol analysis, and structural classification [11],[12],[13],[14]. Recent approaches such as multipath routing with network coding and comparative fault detection in CPS have shown promising improvements in system robustness [15],[16].

Various real-world application of WSNs including environmental monitoring, healthcare and smart agriculture, are present in Figure-1.

Fig -1: WSN Application

Therefore, analysing and improving WSN reliability is critical for ensuring stable and efficient operation in CPS application [10]. The integration of WSNs and WSANs with in CPS architectures is illustrated in Figure-2. Many studies have focused on enhancing reliability through network design, communication protocols and fault tolerances techniques [11], [12], [13],[14].

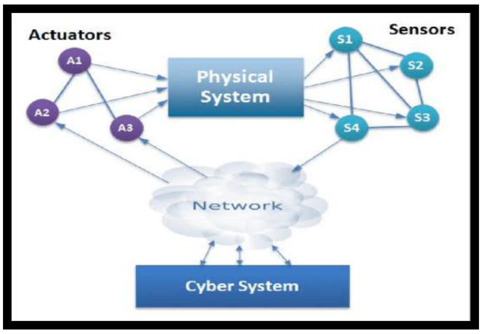

Fig -2: Cyber Generic Architecture

Cyber-Physical Systems (CPS) interact with Physical environments through Wireless Sensor Network (WSNs) and Wireless Sensor and Actuator Networks (WSANs) [17],[18]. As shown in the previous paragraph: reliability, fault detection and fault tolerance of WSNs play a critical role in ensuring overall CPS dependability. Figure-3 provides a system overview of how WSNs integrate with CPS platforms for fault detection and adaptive decision-making.

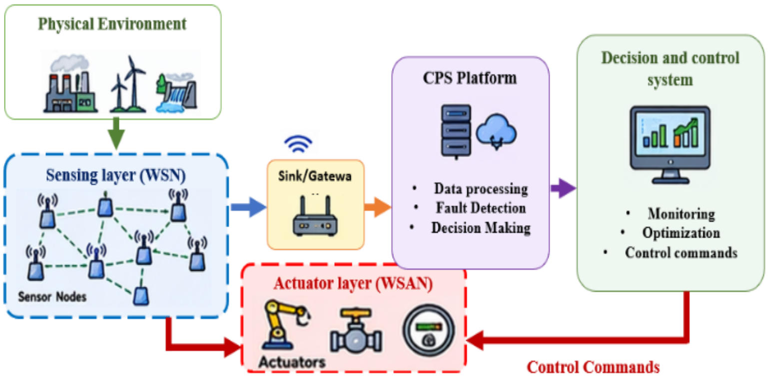

Fig -3: System overview in WSN in CPS

1.1 Cyber-Physical Systems

Cyber-Physical Systems (CPS) are integrated frameworks that enable advanced interaction between human-to-human, human-to-object, and object-to-object environments. CPSs rely heavily on continuous data acquisition and enhanced network connectivity to support efficient monitoring, control and optimization processes. With the integration of intelligent WSN, CPS are expected to become more reliable, Adaptive and secure in complex and dynamic environments [16],[19],[20].

A CPS is defined as a smart system that integrates computational component with physical to monitor and control a specific environment. In such systems, data integrity, availability and reliability are critical performance factors. WSNs represents fundamental communication infrastructure within CPS, enabling real-time sensing, data transmission, and actuation between physical and cyber components. Enhancing WSN reliability is essential to ensure CPS dependability, prolong network lifetime, and maintain stable system performance under varying operational condition [4],[13],[21].

1.2 Wireless Sensor Network (WSN)

Wireless sensor networks are becoming more popular, especially where direct physical connection between sensor and sink is difficult. The type of collected data by the sensor nodes determines how a WSN is monitored.

WSNs typically consist of hundreds or thousands of small sensor nodes distributed across a geographical area. These nodes communicate wirelessly with one another, forming a unified network to collect and transmit environmental data [6]. Also used in various applications, including environmental monitoring, healthcare industrial automation, and smart cities [6]. Each sensor node has limited energy, processing power, and storage capacity, which makes reliability a critical concern in WSN deployments.

1.3 Problem statement

When sensor nodes are deployed in field environments, random failures may occur in either the nodes themselves or the links connecting them. These failures waste energy and other limited resources while simultaneously increasing maintenance complexity. Because node and link statuses change over time, reliability is not fixed but continuously vary. This dynamic nature creates a fundamental challenge for ensuring reliable WSN-based CPS operation.

1.4 Paper Contribution and Organization

This review contributes to the field by:

- It provides a structured, comprehensive review of WSN reliability for CPS
- It explains key concepts, analysis methods, and modeling approach.
- It offers a novel taxonomy for classifying reliability enhancement methods.
- It compares various protocols and techniques using summary tables
- It identifies open research challenges and future direction

The rest of this paper is organized as follows: Section 2 introduces fundamental concepts. Section 3 presents a taxonomy of reliability approaches. In Section 4 we discuss reliability enhancement methods and techniques. Section 5 presents a notation table. Section 6 reviews related work in organized way. Section7 looks at fault tolerance protocols. Section 8 talks about and lists open challenges. Section 9 concludes the paper.

2. FUNDAMENTALS

Before looking at specific reliability enhancement methods and protocols, it is useful to understand some basic concepts. This section defines what WSN reliability means, what fault tolerance and how simulation can help us understand systems.

2.1 WSN Reliability

As defined earlier WSN reliability can be defined as the probability that at least one active sensor node has a functional communication path to the sink node [22]. Mathematically this can be expressed as:

$$R_{WSN} = P\left(\bigcup_{i=1}^{m} Path_i \text{ } is \text{ } operational\right)$$

Assuming the paths are independent, the network reliability can be calculated as:

$$R_{WSN} = 1 - \prod_{i=1}^{m} (1 - R_{Path_i})$$

Table -1: Description Symbol

Symbol	Description
R_{WSN}	Overall WSN reliability
m	Number of possible paths from sensor nodes to the sink node
R_{Path_i}	Reliability of the $i-th$ path
$\prod$	Product operator (multiplication overall paths)

This formulation for WSN reliability: if at least one path is operational the network is considered reliable.

For a single path consisting of n nodes and l links, the path reliability is:

$$R_{path} = \prod_{j=1}^{n} R_{node}(j) \times \prod_{k=1}^{l} R_{link}(k)$$

Where:

$R_{node}(j)$ is the reliability of node j, and $R_{link}(k)$ is reliability of link k [5], [10].

WSN reliability is influenced by several factors, including energy, coverage, lifetime and connectivity is considered the most critical factor, especially in harsh environment. Figure-4 summarizes the main factors affecting WSN reliability: Energy, connectivity, Coverage and network lifetime.[4]

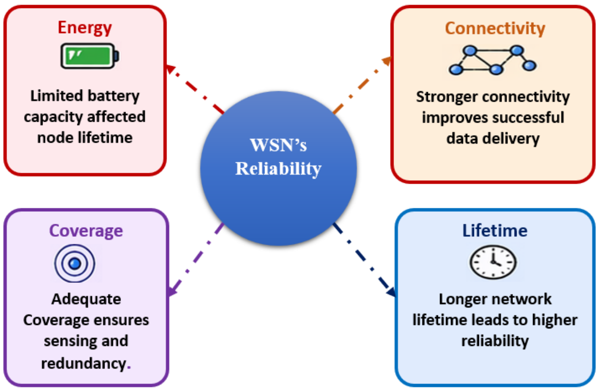

Fig -4: Factors Affecting WSN reliability

2.2 WSN's Fault Tolerance

Fault Tolerance (FT) is the ability of a system to maintain acceptable performance despite component failures, by detecting, isolating, identifying and recovering from faults. Also, FT is considered a key technique for enhancing reliability in Wireless Sensor Network. It enables the network to handle unexpected conditions such as hardware failures, software faults and network bottlenecks, while continuing to operate even when nodes fail randomly [23],[16].Due to harsh environment, limited energy resources and potential external disruptions, WSNs must be designed as robust systems to ensure reliable data delivery, as shown as Figure-5 [24].

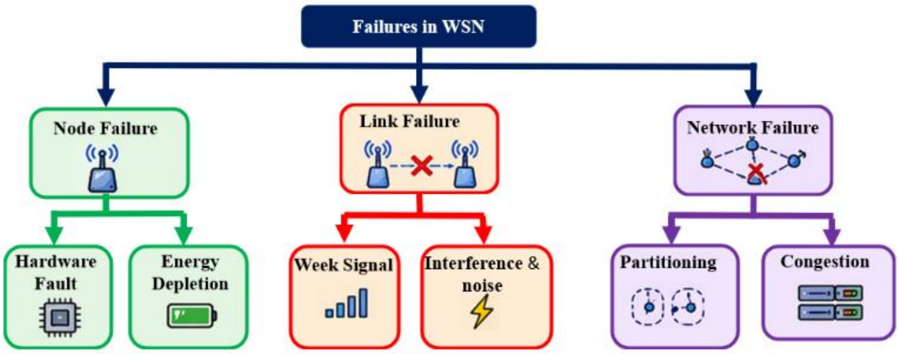

Fig -5: Classification of Failures

Fault tolerance improves reliability through techniques such as redundancy and retransmission; however, these approaches introduce trade-offs between system performance and resource consumption. The main mechanisms of fault tolerance include fault detection, fault recovery, identification and isolation of faults [25]– [27]. Table-2 summarizes the main fault tolerance mechanisms in WSN.

Table -2: Fault tolerance mechanisms in WSN

Mechanism	Function
Fault Detection	Identifying that a fault has occurred

Fault recovery	Restoring normal operation after a fault
Fault identification	Determining the type and location of the fault
Fault isolation	Separating faulty components from the rest of the network

2.3 Dynamic Systems and Simulation

Simulation is a powerful tool widely used in software engineering to visualize and understand of the system's dynamic behavior over time. It helps predict problems and system behaviors that may occur during runtime even at the early design stage. Simulating software architectures is critical, especially when using models that support dynamic reconfiguration. Such models allow researcher and developers to anticipate possible changes in system architectural configuration changes during runtime evaluate their impact in advance [28],[13].

3. TAXONOMY OF WSN RELIABILITY APPROACHES

This section provides a hierarchical taxonomy of WSN reliability approaches to better organize and understand the various methods and protocols discussed in this paper. This taxonomy is derived from a systematic analysis of the literature and is tailored to CPS applications. As shown in Figure, the taxonomy divides existing work into main groups that follow the logical flow of reliability research: what we measure, how we model and evaluate, how we achieve reliability, which protocols we use and what problems are still open.

3.1 Taxonomy Overview

Figure-6 present the complete taxonomy structure:

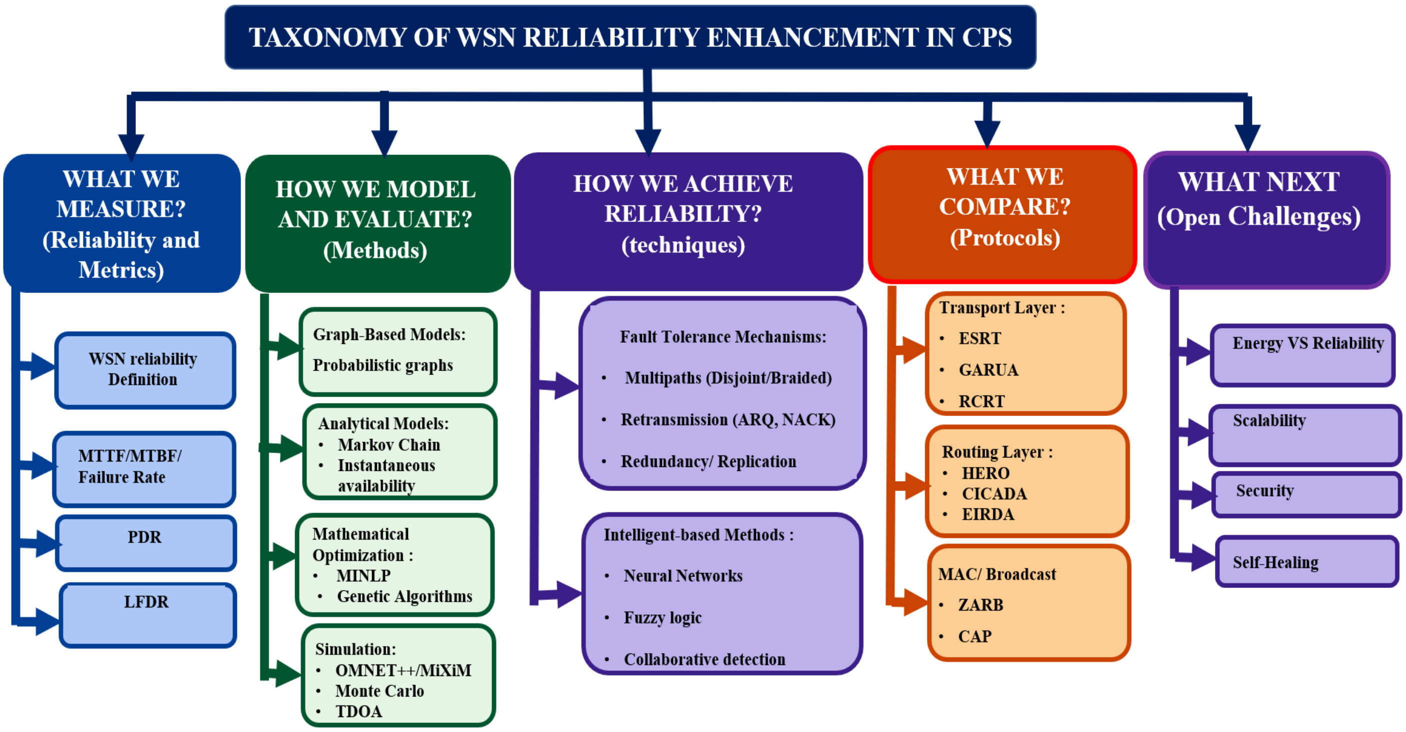

Fig-6: Taxonomy OF WSN Reliability Enhancement in CPS

3.2 Explanation of Taxonomy Parts

Part 1: what we measure- This category includes the fundamental definitions and quantitative metrics used to assess WSN reliability. These metrics provide a common basis for comparing different approaches and protocols.
Part 2: How we model and evaluate - This category covers the mathematical and computational approaches used to represents WSN behavior and compute reliability measures. It includes graph-based models, analytical methods, optimization techniques and simulation platforms.
Part3: How we achieve reliability- This category encompasses the practical methods and strategies implemented to improve WSN reliability. It includes fault tolerance mechanism and intelligence-based methods such as neural networks and fuzzy logic.
Part 4: which protocols we use- This category lists the specific protocols discussed and compared in this review, organized by their layer in the network stack: transport layer, routing layer and MAC/broadcast layer.
Part 5: what challenges remain open: This category identifies the unresolved research problems and future directions in the field, including the energy- reliability trade-off, scalability, security and self- healing capabilities.
This taxonomy is used throughout the remainder of this paper to organize the discussion of related work and to structure the comparative analysis of protocols.

4. RELIABILITY ENHANCEMENT: METHODS AND TECHNIQUES

Improving reliability is typically a step-by step process applied throughout all stages of WSN deployment, involving the definition of performance requirements, reliability targets and operating conditions based on Quality of Service (QoS) requirements and user needs [29] [30]. This section discusses various methods and techniques to improve WSN reliability. These include basic metrics, fundamental enhancement techniques and network optimization methods.

4.1 Reliability Metrics

As defined mathematically formulated in section 2.1, WSN reliability (R_{WSN}) is the probability that at least one path exists from sensor node to the sink node [22]. That section presented the fundamental network reliability equations.
In addition to network reliability, several other metrics are used to evaluate WSN performance. These metrics are divided into communication metrics, component metrics, and fault detection metrics, each is defined below with its mathematical formulation.

4.1.1 Communication metric

- **Packet Delivery Ratio (PDR):**

$$PDR = P_{recived} / P_{sent}$$

Where $P_{recived}$ is the number of packets successfully received, and P_{sent} is the total number of packets transmitted.

- **Path Reliability (R_{path}):** as introduced in Section2.1 For a single path consisting of n nodes and l links

4.1.2 Component Reliability Metrics

- **Mean Time to Failure (MTTF):** represents expected time before a node or component fails [31].

$$MTTF = T_{total} / N_{failures}$$

Where T_{total} is the total operating time and $N_{failures}$ is the number of failures.

- **Mean Time Between Failure (MTBF):** under the exponential failure distribution, it is inversely related to the failure rate (λ) [9],[31].

$$MTBF = 1/\lambda$$

- **Failure rate (λ):** is the frequency at which failures occur over time [31].

$$\lambda = 1/MTBF$$

- **Availability(A)**: the steady- state availability of a repairable components is [9],[32].

$$A = MTBF/(MTBF + MTTR)$$

Where $MTTR$ is the Mean Time to Repair.

4.1.3 Fault Detection Metric

- **Link Failure Detection Rate (LFDR):** quantifies the effectiveness of fault detection in identifying link failures [27].

$$LFDR = TP/(TP + FN)$$

Where TP= True Positive (correctly detected failures), FN= False Negatives (missed failures)

- **False Alarm Rate (FAR)**: measures the proportion of normal operations incorrectly classified as faults [33].

$$FAR = FP/(FP + TN)$$

Where FP=False Positive (false alarms), TN =True Negatives (correctly identified normal cases).
These metrics enable objective comparison of different designs, protocols and deployment strategies [31]

4.2 Reliability Enhancement Techniques

Several basic techniques can improve WSN reliability. Each has advantages and disadvantages that must be considered in context.

Redundancy (Fault Tolerance Approach): This technique involves adding extra hardware components or duplicating information. While redundancy normally increases design complexity and cost, in WSN it's often a built-in feature because multiple sensors naturally cover overlapping area. Hardware redundancy uses additional physical components, while information redundancy sends the same data multiple times through different paths [25] – [27].

Retransmission (ARQ): when a data packet is lost during transmission, the sender resends it. This approach is simple to implement but consumes additional energy and bandwidth. There is always a trade-off between reliable data delivery and efficient use of network resources [34].

Multi-path routing: instead of sending all data through a single path, the network distributes traffic across several alternative routes. This improves reliability because if one path fails, others can still deliver the data. However, maintaining multiple paths increases network overhead [34].

Source Coding: Data is encoded using special algorithms before transmission so that even if some portions are lost, the original message can still be reconstructed at the receiver. This technique also increases processing and transmission overhead [34].

Automatic Repeat Request (ARQ): similar to basic retransmission but often combined with error detection code to identify exactly which packets need to be resent, improving sufficiency [34].

4.3 Network Reliability Maximization Methods

If a communication network is found to be acceptable, it can continue operating without changes. However, if reliability is insufficient, corrective action is required. The simplest is adding more links between nodes, thus connections generally improve reliability. The network reliability maximization problem involves determining the best way to add links to achieve high reliability improvement [35]. This optimization problem can be addressed using different mathematical approaches depending on problem complexity, table-3 show these approaches

Table -3: reliability optimization methods

Method Type	Technique	Description
Exact Methods	branch and bound, dynamic programming	Provide optimal solutions
Meta-Heuristic Methods	Genetic Algorithm, Simulated Annealing, VNS (variable neighborhood search), Tabu Search	Find good solution quickly without optimality guarantee
Heuristic Methods	GRASP, path relinking, Scatter search	Handle complex problems with large solution spaces

These methods help decide where to add new links to achieve high reliability with minimal resource [36][30].

4.4 Comprehensive classification of techniques:

Table-4: reliability enhancement techniques.

Technique Type	Description	Advantages	Limitation
Routing-based	Uses multiple or optimized routing paths to ensure data delivery	Improves connectivity and reliability	May increase delay and complexity
Redundancy- based	Multiple nodes or paths	High fault tolerance and reliability	Increased energy consumption
Retransmission- based	Resends lost packets (ARQ)	Improves packet delivery ratio	Consumes bandwidth and energy
AI-based Methods	Uses ML, Neural Networks, Fuzzy Logic	Adaptive and intelligent decision- making	Requires training and computational cost
Optimization-based	Uses algorithm (GA, MINLP, etc.)	Finds near-optimal Solutions	Complex and time-consuming

5. NOTATION TABLE

Table5. The description of Abbreviation and full name

Table -5: notation table

Abbreviation	Full Name Description
WSN	wireless sensors network
CPS	Cyber physical system
WSAN	wireless sensors and actuator
GRASP	greedy randomized adaptive search procedures
MTTF	Mean-time-to-failure
MTBF	mean-time-between-fails
FT	Fault tolerance
DSN	distributed sensor network
NN	neural network
LFDR	Link Failure Detection Rate
PDR	Packet Delivery Ratio
MGN	modified gamma network
TDOA	time difference of arrival
E2SRT	event-to-sink reliable transport protocol
GARUDA	Achieving effective reliability for downstream protocol
NACK	negative acknowledgment
RCRT	rate-controlled reliable transport protocol
e2e	End-to-end
ZARB	ZigBee Acknowledgement-based Reliable Broadcast protocol
HERO	Hierarchical efficient and reliable routing protocol
CICADA	Cascading Information Retrieval by Controlling Access with Dynamic Slot Assignment protocol
CRT	Chinese Remainder Theorem
EIRDA	Energy Efficient Interest-based Reliable Data Aggregation protocol
CAP	contention access period protocol

6. RELATED WORKS

Many methods, algorithms and approaches have been developed for WSNs reliability analysis, modeling, evaluation, enhancement and optimization, and so much else to make WSNs more faults tolerable, in literature. This section explores the most common, recent and efficient contributions.

6.1 The Network Modeling

To understand and predict network reliability, researchers often create mathematical models. Reliability and message delay have been presented for network modeling. Two approaches are utilized to compute the reliability and expected message latency for arbitrary networks with random failure: enumerate network states and generate the shortest path. In addition, efficient (polynomial time) algorithms have been proposed for two concerns (disjoint pathways and interval graphs). After evaluating the failure probabilities of the sensors and intermediate nodes (nodes that transfer messages between sources and sinks), a probabilistic graph was utilized to model a distributed sensor network [11].

6.2 The DSN Reliability and Link Failures Detection

DSN reliability refers to the probability of an operational communication link between the sink node and at least one operational sensor in a target cluster.

Two algorithms compute this reliability and by using bidirectional connectivity graphs of a certain size and shortest-path routing methods.

The first algorithm: uses breadth-first-search to enumerate all states of the graph and find the length of the shortest path for each state.

The second algorithm: Instead of enumerating all network states, generates new paths by considering the two states of each vertex on the present path: failed and up (or operational). Their calculations show that when the sensor node range reduces, the average delay increases and reliability reduces [11], [37], [38].

In the WSN environment, a method for detecting wireless link failures between sensor nodes has been developed. A wireless sensor network uses the shortest wireless link or path to broadcast and receive packets from other sensor nodes [39]. There are two types of routes between two sensor nodes: weak and strong. Both nodes must have enough energy and must not be hostile or residual sensor nodes for the path or link between them to be strong [40]. If one of the nodes connecting them in the network environment lacks energy, a connection failure will occur. This is what causes the emergence and the occurrence of connectivity issues in wireless sensor networks [41]. After producing link failures between two nodes, the present **link failure detection approach** discovers the difficulties between them. As a result, packets in the network environment will be lost. As a result, expecting link failures or difficulties in wireless sensor networks is critical for reducing packet loss during network transmission or reception [42].

6.3 Machine learning and Neural Networks

Apply **Neural network (NN)** classifier in wireless networks with a given feature set that includes both weak and strong links between nodes. There are 100 sensor nodes in the simulation environment, each separated by 100 meters, with a total width and height of 1000 meters. Each node's baud rate is 150 B/Sec and the primary bandwidth is set to 100 MHz. In total, 15 connection failures occurred in the simulated environment within the simulation time duration. The performance of the proposed system is evaluated using the Link Failure Detection Rate, Packet Delivery Ratio and latency reports. In the network environment, the suggested system detects 14 out of 15 link failures. As a result, the link failure detection approach obtained 93.3 percent LFDR, 89.7% PDR, and 35.3 ms latency [33].

Fuzzy logic and other machine learning approaches are also recommended for improving WSN reliability and Operational efficiency [39],[48].

6.4 Analytical Methods

An Instantaneous Availability is a time varying measure. The proposed CPS reliability evaluation model based on instantaneous availability was developed using theories and simulations to analyze the variation of instant availability over time and the effect of some key parameters such as failure rate and repair rate on CPS reliability. The results show that the proposed method is more advanced than existing evaluation methods [32]. The reliability calculation method has been presented, using a reliability improvement technique based on **component replication**, to eliminate failures and effect failure as a parameter of the reliability of individual components [43]. Their result obtained reliability of the system is calculated as

0.9609. Random failures have also been included for classifying node failures, and link establishments have been identified using the disk connection model. Previous reliability research, such as [44],[45], has consistently overlooked the effects of energy consumption, environmental randomness, and interference. Using value-based optimization, more recent work addresses these gaps.

The **mixed-integer nonlinear programming (MINLP)** model is another mathematical optimization technique. It improves the reliability indices of distribution systems that are subject to economic and technological limitations. The results and studies have shown the effectiveness of the formulation [46].

Table -6: reliability optimization methods

Method name	Method Type	Key Details	Performance/outcome
Neural Network [33]	NN classifier for link failure detection	100 nodes,100 m spacing, 1000m x 1000m are, 150 B/Sec baud rate, 100MHz bandwidth	93.3% LFDR, 89.7% PDR, 35.3 ms latency (detected 14/15 failures)
Instantaneous Availability [32], [43]	CPS reliability evaluation model based on instant availability	Analyzes variation of instant availability over time,	More advanced than existing evaluation methods
Mixed-Integer Nonlinear Programming (MINLP) [46]	Mathematical optimization technique	Improves reliability indices of distribution systems under economic and technological constraints	Effective formulation proven by results

6.5 Reliability Evaluation Methods

For the reliability evaluation of the network, in a structural reliability analysis method, a genetic search algorithm was utilized to describe the statistical uncertainty of random variables, and it was developed using a robust and efficient strategy to search for the interval values of the reliability index in the optimization process [47]. Employed an adaptive formulation to improve the efficacy of the reliability approach. The Gamma network system, on the other hand, is far more reliable and fault-tolerant. The network's st-reliability (source-terminal reliability) has been examined, and the findings have been compared to most contemporary gamma networks in the literature. [48] Indicates that a MGN with fault tolerance improves reliability and reduces costs by 23%. (Reducing the number of stages also decreases the complexity of the network and thus decreases the latency of packet transmission). When it comes to analyzing reliability for WSNs, the reliability of K-coverage communication has been addressed using minimum spanning trees. In terms of reliability, the proposed approach is simpler and more effective.

The all-terminal reliability, which refers to the chance that all nodes in a network are linked, was used to evaluate the reliability of a wireless network in [49]. Also offered is a new way of increasing WSN performance. A network coding strategy has been employed to increase the WSN's transmission performance. The existing network coding multipath routing mechanism has been adjusted for a novel node selection to its residual power node in the research. For routing, this routing function was installed on the router. The MiXiM Framework library and the OMNET++ platform was then used.

Table -7: reliability evaluation methods

Technique	Application	Key Finding /Outcome
Genetic search algorithm for structural reliability analysis [48]	Describe statistical uncertainty of random variables; searches for interval values of reliability index	Robust and efficient strategy
Adaptive formulation [48]	Improves efficacy of reliability approach	Gamma network system is more reliable and fault-tolerant
Modified Gamma Network (MGN) [33]	Fault tolerance improvement	Improves reliability and reduces costs by 23%; Reduce stage ▶less

		Complexity ► lower latency
K-coverage communication reliability+ minimum spanning trees [35]	Reliability analysis for WSNs	Simpler and more effective approach
All- terminal reliability [35]	Probability that all nodes in a network are linked	Used to evaluate wireless network reliability
Network coding multipath routing [13]	Node selection based on residual power	Improves transmission performance: implemented on router using MiXiM +OMNET++

6.6 OMNET++ Platform and the MiXiM Framework

A software network simulation method was developed using the OMNET++ platform and the MiXiM Framework package. The suggested technique for selecting nodes and running network coding enhances the prior method in terms of WSN performance, such as reliability in [35]. In a five-node time difference of arrival localization approach, a new deployment sensor mechanism has been designed to ensure device availability in the case of a failure in a sensor. In every set of four nodes of the device, the uncertainty of two potential solutions for the four-sensor TDOA problem has been solved by increasing the distance between the two potential solutions at each target potential location [50].

7. FAULT TOLERANCE PROTOCOLS

This section looks at several protocols and compares them to improve fault tolerance and reliability in WSN.

7.1 Summary of Protocols

Table summarizes the main protocol, their core ideas, reliability focus, constraints and performance benefits.

Table -8: reliability and fault tolerance protocols

Protocol	Reliability Focus	Constraint	Performance	Core mechanism
E2SRT	Event to sink reliability	Unreliable link, Dynamic topology.	Reduced Energy consumption	Congestion control
GARUDA	Multiple-level reliability	Packet size transmission overhead	Better energy efficiency and Latency	Loss recovery through minimum recovery set
RCRT	End to end reliability	Hardware limitations, asymmetric link	Flexibility and efficiency in the network	recovery scheme based on NACK
ZARB	Broadcast reliability	Coverage delay	Improved Network efficiency	ACK packets broadcasting
HERO	Delivery of bidirectional	nodes constraints	Better Energy and life span	clustering techniques
Data fusion protocol	Information and transmission reliability	unreliable fusion structure	efficiency Energy	Information-weight fusion.
CICADA	End to end	Node Mobility	Higher Throughput,	Randomization and

improved protocol			lower delay, and power saving	overhearing
Simple CRT packet forwarding	Packets delivery	Channels that are unreliable, topology changes that are dynamic, and MAC overhead	Power saving	Algorithm for split packet based on (CRT)
EIRDA	Clustering	Security	Tolerance to fault, energy efficiency, and life span	beta-distribution function trust evaluation, aggregation, and routing.
contention access period protocol (CAP)	Reporting on events	Constraint on nodes	Tolerance to fault	Aggregation by collaboration
Collaborative distributed detection	Reliability of information	Faulty nodes	Tolerance to fault, efficiency on energy, and life span	Regression polynomial parameters are calculated, the intermediate data is assembled, and the final area 's status of event is determined.

7.2 Detailed of Protocols descriptions

E2SRT (Event- to -sink Reliability Transport Protocol) described in [51] to solve the 'over-demanding' event reliability problem and stabilize the network. In the presence of 'over demanding' event reliability, simulation results demonstrate that E2SRT beats ESRT in terms of both reliability and energy efficiency. Furthermore, it guarantees stable convergence in changing network situations.

GARUDA protocol, in [52], ensures that data has been delivered reliably from a sink node to multiple SNs in a point-to-multipoint fashion. It is a reliable protocol for limited delivery as well as for optimal assigning of locally specified servers. It also offers a bi-stage negative acknowledgment (known as the NACK scheme) based recovery mechanism.

Network congestion identification, transmission rate adaptation, transmission rate allocation, and end-to-end retransmission are the four essential components of RCRT protocol [53]. RCRT additionally employs a negative acknowledgment technique for data restoration in the event of an (e2e) data wastage.

The protocol ZARB was used in [54]. By intelligently processing broadcasted acknowledgments in WSN, it makes use of the acknowledgment process in multicast and broadcast transmission for secure transmission.

In [55], a protocol HERO is a routing protocol that takes advantage of hierarchical structural architecture by allowing reliable, stable, and multi-hop connectivity in both directions between nodes organized in different layers, allowing developers to create as many layers as they need in a WSNs Ad-hoc.

As indicated in [56], data fusion with the appropriate reliability protocol has been recommended for reduced energy usage and reliable transfer of collecting data in WSN. This algorithm technique for in-network processing, such as the fusion of data, is successful, but it can result from imbalances in information across nodes in the fusion of data hierarchy.

CICADA is a multi-layered protocol that has been utilized with mobile bodies in multi-hop networks, according to [57].

[58] Has implemented a simple packet forwarding based on the Chinese remainder theorem as a protocol that works by breaking packets using the CRT. The mechanism of splitting is useful for forwarding nodes that can't process or forward huge packets. The sink node is in charge of recombining all sub-packets and recreating the initial message if they are appropriately received.

[59] Suggested EIRDA protocol, which uses a static nature approach to establish clusters and distribute SNs equitably within each cluster.

Data could only be sent by any system when a slot CSMA/CA technique in the CAP protocol was completed in [60]. In the CAP, there are two types of data transfer models have been described. Downlink data should be carried indirectly, while uplink data should be transmitted directly, according to one viewpoint.

[61] Shows how collaborative distributed detection lowers network connection overhead and keeps the data fusion center from being overwhelmed by the sensory node's huge amount of raw data. Table 8 up and table 9 below compare and contrast some of the approaches, protocols, and procedures utilized in WSN to improve reliability.

7.3 Fault Tolerance Techniques:

Beyond specific protocols, several general techniques help achieve fault tolerance in WSN. Table 9 illustrates these techniques

Table -9: fault tolerance techniques

Technique	Description	Advantage	Disadvantage
Multipath disjoint [17],[62]	Creates completely separate, non-overlapping path	Can survive up to k-1 failure; high fault tolerance	High energy consumption
Multipath Braided [63]	Creates alternative paths that may share some node	Faster to discover than disjoint	Lower FT than disjoint
Retransmission [19]	Resends lost packets	Simple to implement	Waste's energy and bandwidth
Replication [54]	Sends multiple copies of each packet	Increases delivery probability	High communication overhead

Multipath routing is the most widely used fault-tolerance approach. It involves identifying a set of multiple routes between source nodes and sinks. While this approach provides load balancing and bandwidth aggregation benefits, it comes with higher power consumption and increased traffic load.

8. Discussion and open challenges

The primary open challenge remains the inherent trade-off between energy efficiency and high reliability. Moreover, most existing protocols assume static topologies, whereas future CPS applications demand robust support for mobility. Finally, the integration of lightweight security mechanisms that do not compromise fault tolerance remains a critical area for future investigation.

9. CONCLUSION

This paper reviewed WSN reliability and fault tolerance enhancing for CPS, by using comparing several methods based on the theory graph and simulations of Monte Carlo, clustering based on fuzzy logic, genetic algorithms, and nonlinear models. Also discuss network modeling, link failure detection, machine learning, analytical methods and many protocols. Fault tolerance techniques like disjoint and braided multipath, retransmission and replication were discussed. Finally, we listed open challenges: energy vs reliability, mobility, scaling, security, real-time needs, mixed networks. This work investigates reliability challenges in WSN-based CPS, reviews existing modelling and evaluation techniques and analyzes fault tolerance and reliability enhancement approaches

REFERENCES

[1] M. Uddin, H. Mo, and D. Dong, “A review on modelling, evaluation, and optimization of cyber-physical system reliability,” arXiv, 2025, pp.1-29
[2] M. S. Mahmoud and M. M. Hamdan, “Improved control of cyber-physical systems subject to cyber and physical attacks,” cyber-physical systems, vol. 5, no. 3, 2019, pp. 173-190.
[3] I. Kabashkin and J. Kundler, “Reliability of Sensor Nodes in Wireless Sensor Networks of Cyber Physical Systems,” Procedia Computer Science, vol. 104, 2017, pp. 380 – 384.

[4] Sh.Mehdiyev ," Assessing the Impact of Energy Consumption of Wireless Sensor Networks on the Fault Tolerance of Cyber-Physical Systems" , 2024, pp. 1–12.
[5] N. Babu and S. V. N. S. K. Kumar, "Comprehensive analysis on sensor node fault management schemes in wireless sensor networks," International Journal of Communication Systems, vol. 35, no. 18, 2022, pp.1-17.
[6] M. Majid, Sh. Habib, A.R. Javed, M. Rizwan, G. Srivastava, T. R. Gadekallu and J. C.-W. Lin, "Applications of Wireless Sensor Networks and Internet of Things Frameworks in the Industry Revolution 4.0: A Systematic Literature Review" Sensors, vol. 6, no. 22, 2022, pp.1-36.
[7] M. M´edard and S. S. Lumetta, "Network Reliability and Fault Tolerance," ResearchGate, pp.1-37, 2003.
[8] A. Choudhary, S. Choudhary and A. Mishra, "Review on Fault Tolerance in Wireless Sensor Network," International Journal of Computer Applications, vol.182, no. 45, 2019, pp.22-25.
[9] I. Silva, L. A. Guedes, P. Portugal and F. Vasques, "Reliability and Availability Evaluation of Wireless Sensor Networks for Industrial Applications," Sensors, vol. 12, no.1, 2012, pp. 806-838.
[10] A. Heidari, Z. Amiri, M. A. J. Jamali and N. Jafari, "Assessment of reliability and availability of wireless sensor networks in industrial applications by considering permanent faults," Concurrency and Computation: Practice and Experience, vol.36, no.27, 2024, pp.1-21.
[11] H. M. F. AboElFotoh, S. S. Iyengar and K. Chakrabarty, "Computing Reliability and Message Delay for Cooperative Wireless Distributed Sensor Networks Subject to Random Failures," IEEE Transactions on Reliability, vol.54, no. 1, 2005, pp.145-155.
[12] A. Sharma and S. Sharma, "A Comparative Review on Reliability and Fault Tolerance Enhancement Protocols in Wireless Sensor Networks," International Research Journal of Engineering and Technology (IRJET), vol. 03, no. 01, 2016, pp.622-626.
[13] Ms.S.G.Mungale, Dr.S.S.Shriramwar, Ms.D.Meshram, Dr.K.Raut , "Critical Review of Fault Tolerance Methods used in Wireless Sensor Networks" , Advances in Nonlinear Variational Inequalities, vol. 28 no. 5s ,2025, pp.521-556.
[14] G.H.Adday, S.K. Subramaniam, Z. A.Zukarnain and N. Samian, "Fault Tolerance Structures in Wireless Sensor Networks (WSNs): Survey, Classification, and Future Directions", Sensors, vol.22, no.16, 2022, pp.1-39.
[15] M. Abdurohman, "Improving the reliability of wireless sensor network (WSN) using modified network coding multipath routing," ComTech Computer Mathematics and Engineering Applications, vol.8, no. 3, 2017, pp.121-126.
[16] L.Piardi, A.S.d. Oliveira, P. Costa and P. Leitão, "Collaborative fault tolerance for cyber–physical systems: The detection stage", Computers in Industry, vol. 166, 2025, pp.1-12.
[17] N. Boulila, "Guidelines for Modelling Cyber-Physical Systems - A Three-Layered Architecture for Cyber Physical Systems," ResearchGate,2017, pp.1-15.
[18] S. Jain and L. Thakur, "Cyber Physical Systems: Theory and its Applications," International Journal of Innovative Science and Research Technology, vol. 8, no. 4, Apr. 2023, pp. 516-520.
[19] H. Ahmadi and R. Bouallegue, "Exploiting machine learning strategies and RSSI for localization in wireless sensor networks: A survey," International Wireless Communications and Mobile Computing Conference, (IWCMC) , 2017, pp.1150-1154.
[20] J. Ahn, J. Paek and J.Gil Ko, " Machine Learning-Based Image Classification for Wireless Camera Sensor Networks, " Proceedings - 2016 IEEE 22nd International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA) , 2016, pp. 1.
[21] M. A. Cifci, "Optimizing WSNs for CPS Using Machine Learning Techniques," Artificial Intelligence Paradigms for Smart Cyber-Physical Systems, 2021, pp.1-25.
[22] S. Lata, S. Mehfuz, S. Urooj, A. Ali and N. Nasser, "Disjoint Spanning Tree Based Reliability Evaluation of Wireless Sensor Network," Sensors, vol.20, no.11, 2020, pp.1-18.
[23] A. Sharma and S. Sharma, "A Comparative Review on Reliability and Fault Tolerance Enhancement Protocols in Wireless Sensor Networks," International Research Journal of Engineering and Technology (IRJET), vol. 03, no. 01, 2016, pp.622-626.
[24] C. WANG, C. CHUANG, Y. CHEN, and Y. CHEN, "On Cyber-physical Fault Resilience in Data Communication: A Case from a LoRaWAN Network Systems Design", ACM Journals, vol.8, no.3, 2024, pp.1-25.
[25] H. Mohapatra1 and A. K. Rath, "Fault-tolerant mechanism for wireless sensor Network," The Institution of Engineering and Technology, vol.10, no.1,2019, pp.23-30.
[26] R. Shukla, A. Kumar and V. Niranjan, "A Survey: Faults, Fault-tolerance & Fault Detection Techniques in WSN," 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 1761-1766
[27] L. Paradis and Q. Han, "A Survey of Fault Management in Wireless Sensor Networks," Journal of Network and Systems Management, vol.15, no.2, 2007, pp.171-190.
[28] W. Manzano, V. V. G. Neto and E. Y. Nakagawa, "Dynamic-SoS: An Approach for the Simulation of Systems-of-Systems Dynamic Architectures," The British Computer Society 2019, vol.63, no.5, 2019, pp.709–731.

[29] L. Venkatesan, S. Shanmugave and C. Subramaniam, “A Survey on Modeling and Enhancing Reliability of Wireless Sensor Network,” Scientific Research, vol.5, no.3, 2013, pp.41-51.
[30] Alfawaz, O., Khedr, A.M., Alwasel, B. and Osamy, W., “Reliability Evaluation for Chain Routing Protocols in Wireless Sensor Networks Using Reliability Block Diagram,” Journal of Sensor and Actuator Networks, vol.12, no.2, 2023, p. 537-571.
[31] Xing, Liudong. "Reliability modeling of wireless sensor networks: A review." Recent Patents on Engineering, vol.15, no.1, 2021, pp: 3-11.
[32] B. Rajasekaran and C.Arun, “Link Failure Detection and Classification in Wireless Sensor Networks using Classification Method,” International Journal of Innovative Technology and Exploring Engineering (IJITEE), vol.8, no.12, 2019, pp.1132 – 1135.
[33] S. Gupta and G.L. Pahuja, “Reliability Evaluation of Modified Gamma Network with Reduced number of Stages,” International Conference on Recent Trends on Electronics, Information, Communication & Technology, 2019, pp.190-194.
[34] S. Saqaeeyan and M. Roshanzadeh, “Improved Multi-Path and Multi-Speed Routing Protocol in Wireless Sensor Networks,” International Journal of Computer Network and Information Security, vol.4, no.2, 2012, pp.8-14.
[35] M. Nishino, T. Inoue, N. Yasuda, S. Minato and M. Nagata, “Network Reliability Optimization by Using Binary Decision Diagrams,” Further Exploring Communication Science, vol.16, no. 11, , 2018, pp.25-29.
[36] P. Festa, “A brief introduction to exact, approximation, and heuristic algorithms for solving hard combinatorial optimization problems,” IEEE, 2014, pp.1-20.
[37] H. Wang, J. Li, F. Shao, L. Fan, Z. Wang and Wei Lin," The Expected Path with Diameter Constraint in Wireless Sensor Network,” IEEE International Conference on Computer and Communications (ICCC) ,2015, pp.379-383.
[38] M. C. Golumbic, “Algorithmic Graph Theory and Perfect Graphs” London: Academic Press, 2014, pp.207-208
[39] Y. Gao, F. Xiao, J. Liu and R. Wang, “Distributed Soft Fault Detection for Interval Type-2 Fuzzy-model-based Stochastic Systems with Wireless Sensor Networks,” IEEE Transactions on Industrial Informatics, vol.15, no.1, 2018, pp. 334–347.
[40] W. Li, F. Bassi, D. Dardari, M. Kieffer and G. Pasolini, “Low-complexity distributed fault detection for wireless sensor networks,” IEEE International Conference on Communications (ICC), 2015, pp. 6712–6718.
[41] A. Mojoodi, M. Mehrani, F. Forootan and R. Farshidi, “Redundancy effect on fault tolerance in wireless sensor networks,” Global Journal of Computer Science and Technology, vol. 11, no. 6, 2011, pp. 35-40.
[42] R. N. Duche, N. P. Sarwade, “Sensor node failure or malfunctioning detection in wireless sensor network,” ACEEE Int. J. on Communications, vol. 3, no. 1, 2012, pp. 57-61.
[43] Y. Yang, S. Wang, M. Wen and W. Xu, “Reliability Modelling and Evaluation of Cyber-Physical System (CPS) Considering Communication Failures,” Journal of the Franklin Institute, vol.358, no.1, 2018, pp.1-26.
[44] N. Kumar, V. Kumar, T. Ali and M. Ayaz, “Prolong Network Lifetime in the Wireless Sensor Networks: An Improved Approach,” Arabian Journal for Science and Engineering, vol. 46, 2021, pp. 3631–3651.
[45] H. Koc, S. S. Shaik and P. P. Madupu, “Reliability Modeling and Analysis for Cyber Physical Systems,” 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), 2019, pp.0448-0451.
[46] A. Heidari, Z. Y. Dong, D. Zhang, P. Siano and J. Aghaei, “ Mixed-Integer Nonlinear Programming formulation for Distribution Networks Reliability Optimization,” IEEE Transactions on Industrial Informatics, vol.14, no. 5, 2017, pp.1-9.
[47] S. Xiang and J. Yang, “Reliability Evaluation and Reliability-Based Optimal Design for Wireless Sensor Networks,” IEEE Systems Journal, vol.14, no.2, 2019, pp.1-12.
[48] M. Bagheri, B. Keshtegar, S. Zhu, D. Meng, J. A. Correia and A. M. Jesus, “Fuzzy Reliability Analysis Using Genetic Optimization Algorithm Combined with Adaptive Descent Chaos Control,” ASCE-ASME J. Risk Uncertainty Eng. Syst, vol.6, no.2, 2020, pp.1-9.
[49] J.-H. Park, “All-terminal reliability analysis of wireless networks of redundant radio modules,” IEEE Internet Things, vol.3, no.2 ,2016, pp.219–230.
[50] J. D. González, R. Álvarez, N. P.-Fernández and H. Perez, “Local Wireless Sensor Networks Positioning Reliability Under Sensor Failure,” Sensor, vol.20, no.5, 2020, pp.1-15.
[51] S. Kumar, Z. Feng, F. Hu, and Y. Xiao, “E2SRT: Enhanced event-to-sink reliable transport for wireless sensor networks,” Journal of Wireless Communications and Mobile Computing, vol.9, no.10, 2009, pp.1301-1311.
[52] S. J. Park, R. Vedantham , R. Sivakumar, and I. F. Akyildiz “GARUDA: Achieving effective reliability for down- stream communication in wireless sensor networks,” IEEE Transactions on Mobile Computing, vol.7,no.2, 2008, pp. 214-230.
[53] J. Paek and R. Govindan, “RCRT: Rate-controlled reliable transport for wireless sensor networks,” ACM Transactions on Sensor Networks, vol.7, no.3, 2010, pp.1-45.
[54] T.W. Sung, T.-T. Wu, C.-S. Yang and Y.-M. Huang, “Reliable data broadcast for zigbee wireless sensor networks,” International Journal on Smart Sensing and Intelligent Systems, vol.3, no.3, 2010, pp.504-520.
[55] E. Canete, M. Diaz, L. Llopis and B. Rubio, “HERO: A hierarchical, efficient and reliable routing protocol for wireless sensor and actor networks,” Computer Communications, vol.35, no.11, 2012, pp.1392-1409.
[56] H. Luo, H. Tao, H. Ma, and S. K. Das, “Data Fusion with Desired reliability in wireless sensor networks,” IEEE Transactions on Parallel and Distributed Systems, vol.22, no.3,2011, pp.501-513.

[57] B. Braem, B. Latre, C. Blondia, I. Moerman and P. Demeester, “Improving reliability in multi-hop body sensor networks,” Second in Technologies and Applications, 2008, pp.342- 347.
[58] G. Campobello, A. Leonardi and S. Palazzo, “Improving energy saving and reliability in wireless sensor net- works using a simple CRT-based packet-forwarding solution,” EEE/ACM Transaction Networking, vol.20,no.1,2012, pp.191-205.
[59] H. Sethi, D. Prasad and R. B. Patel, “EIRDA: an energy efficient interest based reliable data aggregation protocol for wireless sensor networks,” International Journal of Computer Applications, vol.22, no.7, 2011, pp. 20-25.
[60] W. Yuan, S. V. Krishnamurthy and S. K. Tripathi, “Improving the reliability of event reports in wireless sensor networks,” Proceedings of the 9th International Symposium on Computers and Communications, vol.1, 2004, pp. 220-225.
[61] Z. ShuKui, G. ShengRong, C. ZhiMing and F. JianXi, “A reliable collaborative detection scheme of event-region in wireless sensor networks,” Proceedings of the International Symposium on Information Processing, 2009, pp.21-24.
[62] N. M. Hoang and V. N. Son, “disjoint and braided multipath routing for wireless sensor networks,” HCM City University of Technology, 2005, pp.1-7.
[63] C.-H. Yang, L.-W. Lin and C.-W. Chou, “A Routing Approach for Constructing Braided Multipath to Alleviate Congestion in WSNs,” International Journal of Emerging Trends & Technology in Computer Science (I JETTCS), vol. 5, no. 2, 2016, pp.200-207.
[64] H. Alwan, “QoS-Based and Secure Multipath Routing in Wireless Sensor Networks,” 2013, pp.1-156.