Received: 16 February 2024 | Revised: 10 July 2024 | Accepted: 23 July 2024

DOI: 10.1002/cpe.8252

RESEARCH ARTICLE

WILEY

Assessment of reliability and availability of wireless sensor networks in industrial applications by considering permanent faults

Arash Heidari[1,2] | Zahra Amiri[3] | Mohammad Ali Jabraeil Jamali[4] | Nima Jafari[5,6]

[1]Department of Software Engineering, Haliç University, Istanbul, Turkey

[2]Department of Computer Engineering, Faculty of Engineering and Natural Science, İstanbul Atlas University, Istanbul, Turkey

[3]Ivy College of Business, Iowa State University, Ames, IA, USA

[4]Department of Computer Engineering, Shabestar Branch, Islamic Azad University, Shabestar, Iran

[5]Future Technology Research Center, National Yunlin University of Science and Technology, Douliou, Taiwan

[6]Research Center of High Technologies and Innovative Engineering, Western Caspian University, Baku, Azerbaijan

Correspondence
Arash Heidari, Department of Software Engineering, Haliç University, Istanbul, 34060, Turkey.
Email: arash_heidari@ieee.org; arash.heidari@atlas.edu.tr;

Mohammad Ali Jabraeil Jamali, Department of Computer Engineering, Shabestar Branch, Islamic Azad University, Shabestar, Iran.
Email: m_jamali@itrc.ac.ir;

Nima Jafari, Future Technology Research Center, National Yunlin University of Science and Technology, Douliou, Yunlin 64002, Taiwan.
Email: nima.navimipour@khas.edu.tr

Summary

Wireless Sensor Networks (WSNs) are critical for communication within a mile radius and industrial applications. These networks are very prone to failure due to their enormous number of nodes and their unique hardware and software restrictions. To make sure network performance, a lot of study needs to be done to improve failure tolerance and stability. This study looks at how to judge the availability and dependability of WSNs that have long-term issues. The suggested method checks how well a network works in various failure cases by using fault trees and Markov chain analysis. Such methods help us find and study possible failure scenarios and how they might impact the network's dependability in a planned way. The results show that WSNs have major flaws and give useful suggestions for making the systems work better. The findings show that using these evaluation methods may greatly enhance the ability to handle faults, lower the risk of damage, and allow developers of WSNs to make smart choices.

KEYWORDS

assessment of reliability, availability, fault tolerance, wireless sensory system

1 | INTRODUCTION

Products and processes that do not work right can have a big effect on the environment and society today, causing problems on many levels. People who buy these things and services want them to be reliable, safe, and stable.[1] Approaches to evaluating reliability were first created for use in military and flight uses, but they were quickly changed so they could be used in atomic energy and other areas to ensure safety and dependability. New research, on the other hand, shows that these areas are having major problems.[2] The main job of dependability assessment is to figure out how likely and dangerous a threat is.[3] Wireless sensor systems, especially ones used in factories or that are close together (within a mile), need to have an exact dependability and availability review. People, the environment, and the business can all be affected by problems with networks in many

areas.[4] Nodes can be damaged by a lot of traffic or running out of power, but if you want to keep the network reliable, the loss of one node should not stop the whole thing from working.[5]

Keeping Wireless Sensor Networks (WSNs) reliable and easy to use in the face of many unknowns is hard because of how they are set up.[6–8] Because these systems are made up of many points connected by wireless networks, each one can break down or have inherent flaws. Finding out about availability and dependability is very important in this case, especially since network breakdowns could put people in danger and cause a lot of data to be lost.[8,9]

The broadcast storm problem in Vehicular Ad Hoc Networks (VANETs) is triggered by rebroadcasts that get too big while data is being sent because the layout changes so often and nodes move so quickly. Because of these issues, it is hard to make effective streaming methods, which causes vehicle data to be spread in a disorganized way. This paper introduces a new fuzzy-based Multicriteria Decision-Making (MCDM) method to solve this problem. This study looks at how accessible and reliable WSNs are by considering long-term problems. Methods such as Markov chain research and fault tree techniques are recommended. This novel method ranks automobiles according to the optimal neighbor selection for strategic data broadcast using fuzzy logic. By harnessing this technique, we efficiently identify and engage the most suitable vehicles for data dissemination. This pioneering strategy remarkably boosts data packet transmission speed while substantially alleviating network congestion and reducing broadcasting traffic within VANETs, ultimately optimizing data distribution in these dynamic networks. Here are the four main contributions of the paper:

1. Introducing a novel fuzzy-based MCDM approach that strategically prioritizes vehicles for optimal neighbor selection during data broadcast within VANETs;
2. Employing fuzzy logic to efficiently identify and engage the most suitable vehicles for data dissemination, significantly boosting data packet transmission speed and optimizing information distribution;
3. Substantially alleviating network congestion and reducing broadcasting traffic within Vehicular Ad-hoc Networks by implementing the proposed fuzzy-based MCDM strategy;
4. Revolutionizing the conventional challenges of rapid rebroadcasts during data transmission, offering a strategic solution to the inefficiencies caused by high-speed node movements and frequent topology changes in VANETs.

Our paper comprises several distinct sections: Section 2 reviews related work. In Section 3, we delve into the system model. Section 4 introduces our proposed protocol and innovative approach. Following this, Section 5 covers the assessment and analysis. Lastly, in Section 6, we summarize our findings and outline future research directions.

2 | RELATED WORK

In this section, we will discuss review-related work. In this regard, Shukla[10] introduced ABCND, a two-phase algorithm for critical node detection in WSN. Phase I utilized the neighbor's RSSI information for 2D Critical Node (C-N) detection, while Phase II bolstered node resilience with a correlation-based reliable RSSI approach. With $O(log\ (N))$ convergence time and $O(\delta(logN))$ for Critical Node detection, ABCND consumed 50% less energy while accurately detecting 90% to 95% of Critical Nodes (C-N) compared to existing algorithms. Also, El-Fouly, et al.[11] proposed a routing algorithm that satisfied critical conditions: energy efficiency, real-time responsiveness, environmental awareness, and reliability. Parameters like environmental impact, energy balance, desired delivery time, and wireless link quality were considered for routing decisions. An Integer Linear Programming (ILP) problem was formulated to understand the constraints fully, and swarm intelligence was suggested as a heuristic for large-scale multi-sink WSN optimization. Comparative experiments with SMRP and EERP protocols demonstrated the proposed algorithm's superiority in packet delivery, deadline adherence, delay, network lifetime, and energy balance, albeit with higher computational energy requirements.

Chen, et al.[12] proposed an optimal deployment method for heterogeneous WSNs aimed to maximize coverage and connection degree while minimizing deployment cost. Heterogeneity and 3-D scenarios were considered in this non-convex, multi-objective problem. A swarm-based algorithm, CMOMPA, outperformed others in experiments, showing superior convergence and accuracy. Simulations confirmed the optimized deployment's ability to balance cost and reliability.[13] Last but not least, Yang[13] presented a technique for assessing Linear WSNs (LWSNs) according to coverage reliability and connectivity. They were able to do concurrent analysis by condensing the system state space and applying hybrid models of binary decision diagrams and divide-and-conquer strategies. Several LWSN designs, including those with one or two sink nodes, flat or cluster-based networks, and sensor nodes with defined transmission and coverage ranges, might be evaluated thanks to their methodology. The method's feasibility was confirmed by case studies, which also supplied crucial characteristics for guaranteeing high-cost performance in LWSN design.

The review of the literature centers on some works that tackle specific WSN subjects, such as routing techniques, critical node identification, deployment optimization, and the assessment of linear WSNs according to connection and coverage dependability. However, a critical gap emerges in the absence of comprehensive methodologies specifically targeting the assessment of WSN reliability and accessibility, incorporating permanent faults. These studies predominantly focus on optimization strategies, energy efficiency, and specific functionalities, overlooking a holistic evaluation approach considering fault tolerance and system reliability. The significance lies in the vulnerability of sensor nodes to various factors like energy reduction, environmental anomalies, and potential attacks, emphasizing the urgent need for robust programs aimed at enhancing network reliability.

TABLE 1 The side-by-side comparison of the related work.

Authors	Main Idea	Advantage	Disadvantage	Method
Shukla[10]	Addressing node failure in WSN topology.	Efficient energy consumption for C-N detection	Dependency on received signal strength indicator	Two-phase algorithm
El-Fouly, et al.[11]	Proposing multi-sink WSN solutions.	Increasing network throughput, lifetime, and energy usage in IoT applications	Enhancing network performance in scenarios like smart cities	Utilizing multi-sink WSNs and applying ILP and swarm intelligence
Chen, et al.[12]	Proposing optimal heterogeneous WSN deployment for coverage-cost balance.	Maximizing the coverage and minimizing the cost in complex scenarios.	High complexity	Introducing CMOMPA as an efficient swarm-based optimization for WSN deployment.
Yang[13]	Evaluating LWSNs for reliability in connectivity & coverage.	Concurrent analysis, reduced system state space	Lack of existing methods/tools and limited application scope	Hybrid models using binary decision diagrams

To address this gap, this paper advocates for methods integrating Markov chain and fault tree analyses to comprehensively evaluate WSN reliability, minimize potential damages, and facilitate informed decision-making for designing fault-tolerant networks. Table 1 provides a comparison of the discussed studies.

3 | SYSTEM MODEL

WSN solutions are founded upon a spectrum of both proprietary and standard protocols, each serving distinct functions within the network architecture.[14] While a multitude of protocols operate within the higher layers of the network, the IEEE 802.15.4 protocol predominates in the lower layers. Notably, recent advancements have led to the publication of IEEE 802.15.4, specifically tailored to furnish multi-step mesh tasks, signifying a pivotal development in enhancing network capabilities. The evolution of wireless network protocols has witnessed the emergence of standards such as Zigbee2004 and Zigbee2007, which are pivotal in implementing higher layers of these networks. However, despite their initial significance, these standards have exhibited limitations in scalability, rendering them insufficient in supporting extensive topologies. Consequently, ongoing efforts within the domain have culminated in the development of a novel standard, currently undergoing refinement to meet the evolving demands of wireless sensor networks. Nevertheless, in specific industrial applications, only Wireless HART and ISA100.11a protocols have proven suitable for the environmental conditions prevalent in these settings.[15]

The Wireless HART protocol is unique among these protocols as it is a refined version of the HART protocol explicitly created to enable wireless communication. The initial purpose of Wireless HART, as created by the HART Communications Foundation (HCF), was to bridge the communication gap between vintage equipment and modern wireless counterparts. When it was officially acknowledged as a feature by the International Electrotechnical Commission (IEC) in 2008, a significant turning point was achieved. This made it known as the state-of-the-art wireless communication technology created to facilitate communication between conventional and wireless equipment in industrial environments. The evolution of wireless sensor network protocols points to a future where these protocols will continue to be improved upon and modified to suit the ever-evolving demands of modern networking paradigms. The emergence of protocols like Wireless HART is a reflection of both the rapid advancement of technology and the urgent need to guarantee a seamless transfer between antiquated systems and contemporary wireless solutions. This will lead to better functioning and communication in industrial settings.[16]

The Wireless HART protocol is the cornerstone of industrial wireless communication. Its operating structure is intricately designed to accommodate eight distinct device types. Each kind of device makes a unique contribution to ensuring durability, dependability, and security in industrial environments while promoting smooth wireless communication. The network manager oversees network orchestration, configuration management, management, and continuous monitoring to ensure optimal functionality. The network security device offers robust security measures against potential invasions, protecting data integrity and confidentiality at the same time. Access points offer network access, gateways facilitate communication with external systems, routers optimize data transmission paths, and field devices serve as the main data interfaces. Adapters help with integration, even though the wireless HART Handheld can be utilized for configuration and on-site troubleshooting. Together, the networked devices in Fig. 1 perform vital network functions via wireless communication, including configuration, array management, routing optimization, security implementation, and proactive maintenance. Together, they guarantee that even in intricate industrial settings, the Wireless HART network will always operate dependable and smoothly.

An enduring and safe wireless infrastructure depends on every type of equipment in this vast ecosystem that complies with the wireless HART protocol. The network manager acts as the primary supervisor, ensuring the network's effectiveness, while the network security device protects the network from potential intrusions. Function-specific equipment like field devices, gateways, and access points work well together to facilitate

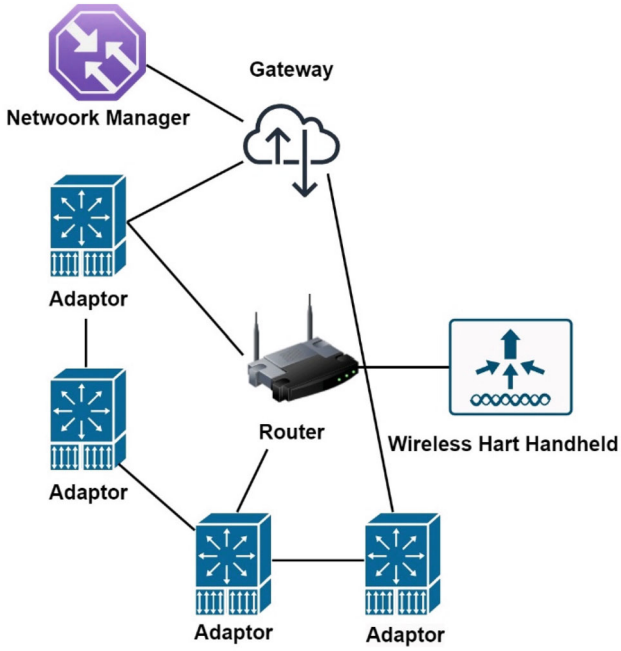

FIGURE 1 HART wireless protocol equipment.

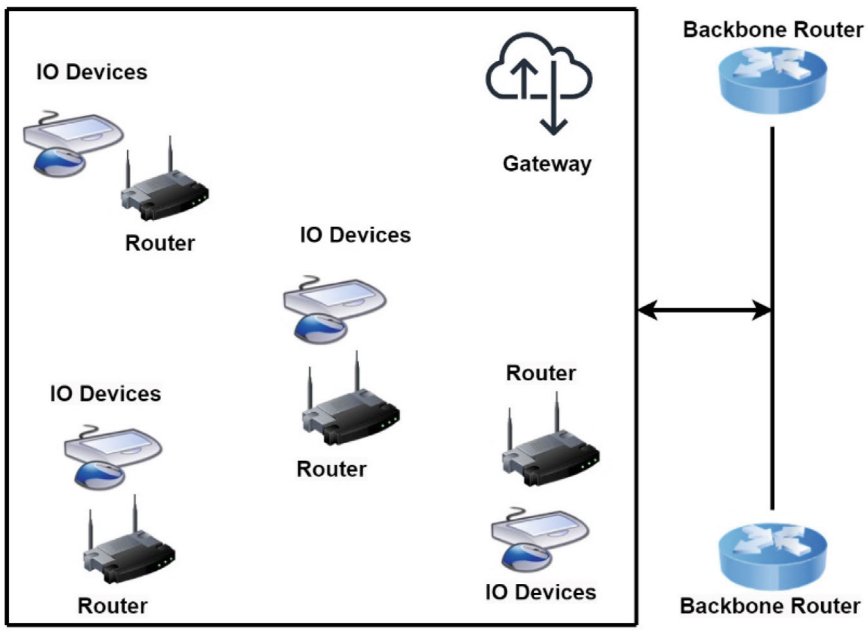

FIGURE 2 ISA100.11a protocol.

efficient data collection and transfer. Also, routers improve data channels, adapters facilitate system integration, and wireless HART Handheld permits on-site monitoring as shown in Fig. 2. Also, through their combined efforts, a network that can carry out essential tasks, including array management, proactive maintenance, routing optimization, configuration, and security, has been developed. Such devices strengthen the wireless HART network with cooperative wireless communication and coordinated efforts, guaranteeing dependability and resilience in the demanding environment of industrial operations.[17]

The International Society of Automation (ISA) created the Wireless HART protocol, which forms the basis of industrial wireless communication. Mesh networking, in particular, uses this protocol to offer robust and dependable communication records. This standard is meant to make it easier to keep an eye on applications and manage processes in factories. ISA (International Society of Automation) came up with the radio HART system,

which is used for industrial radio communication. In particular, mesh networking needs contact records that are strong and reliable. The goal of this standard is to make process control and application tracking better in business settings.[18]

Both the Wireless HART and ISA100.11a protocols work with networks and send data at the same level. However, the ISA100.11a protocol has a different way of addressing that works with 6LowPAN (IPV6) over 802.4.15. The most impressive thing about this change is how creatively it brings together technologies that support higher communication standards and network interoperability. The ISA protocol also created and executed the important failure diagnostics system, while the Wireless HART protocol does not. This is because the ISA protocol is based on sending warnings for diagnostic reasons. One thing that makes this protocol different from its wireless HART sister is its monitoring system, which fixes problems before they happen and makes the protocol more resilient.

Because the ISA100.11a protocol can work with older devices, find problems before they happen, use better addressing, and have other cutting-edge features, it is a strong competitor for keeping industrial wireless networks safe and long-lasting. This protocol adds new techniques to well-known transmission layers, which could lead to better network stability and debugging capabilities. These are two important parts of building industrial communication networks that work well and do not break down.[19]

4 | PROPOSED PROTOCOL

This approach's main objective is to offer a solid framework for the thorough assessment of WSN reliability. The primary goal is to equip system designers with the information they need to create fault-tolerant systems. Using this method, designers can get the crucial information needed to build and develop fault-tolerant systems. Because this methodology is flexible and may be applied at any point in the network's life cycle, it facilitates the identification and diagnosis of structural vulnerabilities. Assessing dependability can be challenging, particularly when working with wireless sensor networks, which are sometimes thought of as NP-hard problems. On the other hand, this strategy seems doable, especially in networks with few devices, such as those frequently seen in industrial settings. Fig. 3 provides a schematic representation of the main elements of the methodology for assessing the reliability of wireless sensor networks. You must first gather the required network data, such as topology, device classifications, redundancy levels, repair techniques, and the causes of network failures, before implementing this strategy. Subsequently, it generates comprehensive network failure scenarios by gathering criteria for device failure.[20]

The next phase in the process is sketching out every path that connects the devices to the gateway and carefully examining the likelihood of failure along each connection. This combined dataset is used by the approach to construct a fault tree and extract minimal cut sets that are required to construct a minimum fault tree that is more accurate. A full software analysis that uses the Sharpe method is the last step in the problem analysis process, and this fault tree is an important part of it. The results include availability, Mean Time to Failure (MTTF), reliability indices, and other important reliability measures that tell creators how to make a network that is reliable and can handle errors. This strict process makes it easier to find problems in WSNs in a planned way and gives a clear path for creating systems that can work even when something goes wrong. This method is a powerful set of tools for improving the stability and robustness of WSNs in a wide range of industrial settings. It does this by collecting network data, making fault trees, and finally analyzing the software.[21,22]

The suggested method's first steps are to order the network model and help with the next modeling steps. When using a graph-based method, the network's hubs are shown by nodes (V), and the wireless links between them are shown by edges (E). In this case, think about a network with

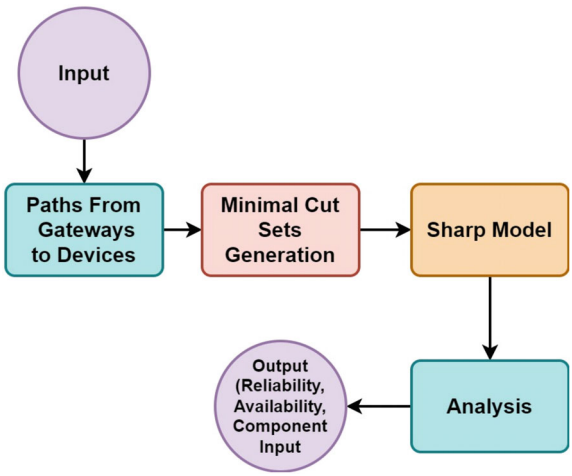

FIGURE 3 An outline of the steps that are used to find reliability.

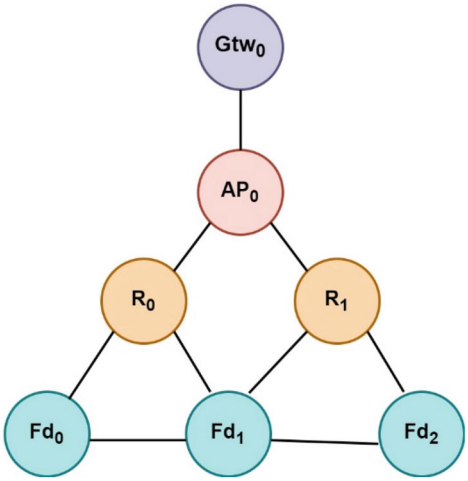

FIGURE 4 The considered network graph.

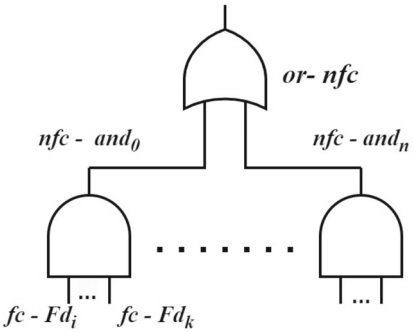

FIGURE 5 Hierarchical logic of Network failure design.

K links and N heads. The different gadgets are shown by the heads, and their wifi links are shown by the edges. This graph really shows how the network is set up by creating an adjacency matrix, which is a key data structure for figuring out the way between the network's main point and its individual devices. In Figure 4, you can see a picture of the network design along with the adjacency matrix, which shows how the network's devices are linked. In this adjacency grid, important information about how the devices are connected to each other in the network is shown. Each item in the adjacency grid shows how two objects are connected to each other. A value of 1 means that two devices are adjacent, while a value of 0 means that they are not adjacent. In this way, the adjacency matrix is a complete list of all the devices in the network and their proximity to each other. Efficient pathfinding techniques are used with this organized grid to help make paths between the center point and other devices. In this way, it is easy to evaluate dependability and look for problems. By employing the graph-based representation in addition to the created adjacency matrix, the method ensures a systematic approach to network structure modeling. This structured representation not only aids in the visualization of the network topology but also serves as a foundation for additional analysis, path identification, and fault tree construction—all essential activities in evaluating the reliability of WSNs.[23]

Our method includes the rational operators "and," "or," and their corresponding operators to give robust support for a wide range of combinations. Specifically, in logic, the operator 'and' is employed to denote the failure conditions that are correctly applied to specific devices. N_i is an index *fc-Fd*$_i$, cover the combinations that lead to network failure scenarios, thereby including the vast array of potential network disruptions. Also, the rational "and" separates each device's failure scenarios to make a full picture of the Network Failure Conditions (NFC). The Boolean "or" operator captures this important mix of failure possibilities. It shows how all the combinations that cause network failure come together. Fig. 5 shows the general network failure picture, which is a useful way to learn about how networks work and how device-specific and network-wide failure cases are connected. This method uses logical operators to make it easier to figure out how the network design could fail in a planned way. The approach successfully gathers and categorizes the complicated failure scenarios of individual devices, then extends these circumstances to grasp the whole network failure scenarios using the 'and' and 'or' operators. The visual depiction in Fig. 6 facilitates the development of resilient network design methods and offers a better understanding of the complex relationships among various failure situations.[24]

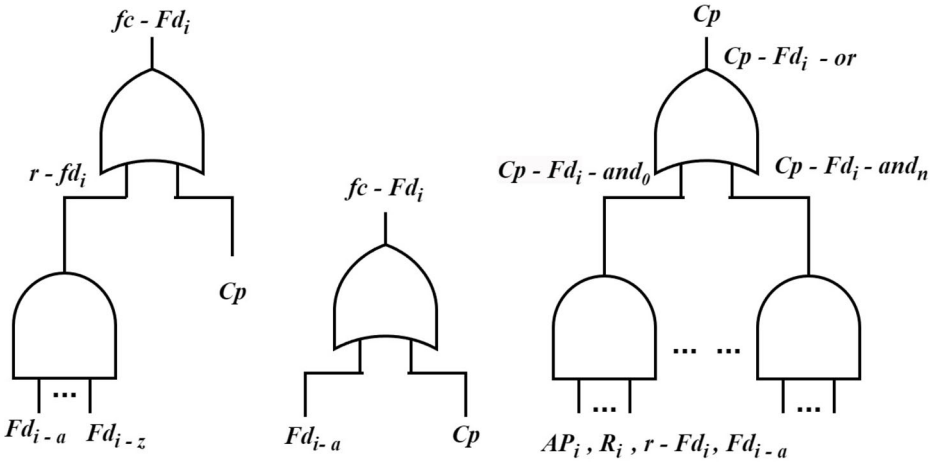

FIGURE 6 The condition of failure of the device with redundancy (left); the condition of failure without redundancy (middle) connection problem (right).

In the exploration of redundancy concepts, we delineate between two device models: one fortified with redundancy and the other a standalone, uncomplicated unit. The former comprises an amalgamation of devices engineered upon fault-tolerant architecture, employing a hot-ready spare mechanism. Upon the failure of a device within this system, an immediate replacement is orchestrated by another device. Injecting the count of spare and available devices into the system serves as essential input parameters. Subsequently, upon deriving failure conditions within the network, our focus shifts to delineating the circumstances triggering device failures, restricting the analysis to devices contributing to network failure instances. Device failure is classified into two potential realms: first, hardware failure within the device; second, the absence of a communication path between the device and the central node. The latter scenario pertains to connectivity breakdowns, wherein the device operates accurately but is rendered non-operational due to the incapacity to engage with the central node over an extended period. In such instances, a self-healing positioning protocol intervenes to establish an alternative communication route. This taxonomy categorizes device failure conditions into hardware and connection-related failures. Under the purview of hardware failure, we discern two operational states for devices: those fortified with redundancy and those without. A device embedded with redundancy succumbs to failure if its ongoing operations cease and all of its spare components have previously failed Fd_{i-a} *to* Fd_{i-z}, denoted by $r - Fd_i$. Conversely, a device devoid of redundancy, upon failure, ceases to function entirely.[25]

The network failure conditions and the pathways between the central node and the affected devices within these conditions were delineated, allowing for the development of a fault tree depicting the network failure process. This fault tree comprises primary events representing network failure conditions and secondary events detailing device failures. Direct interfacing with an assessment tool as input facilitated the computation of reliability criteria, aiming to streamline the fault tree's complexity for expedited reliability calculations. Deriving Minimal Cut Sets (MCS) from this data was done to produce a fault tree model that was more condensed. The unreliability of connections and devices was taken into account in the modifications made to the MCS calculation methods. The new algorithms included previous research methods for MCS creation from Minimum Path Sets (MPS).[26] The minimum fault tree that emerged, which depicts the process of network failure, was caused by events related to the central node and the circumstances surrounding the collapse. While Sharpe software cannot directly support the models provided by MCS, it can evaluate fault tree-based models. The primary events arising from situations of central node and network failure were more accurately classified by this fault tree illustration, notwithstanding its simplification.[27]

To initiate problem-solving, the initial step involves outlining the failure conditions pertinent to the devices, outlined in Equation (1):

$$\begin{aligned} f_c - Fd_0 &= Fd_{0-a} \\ f_c - Fd_1 &= Fd_{1-a} \\ f_c - Fd_2 &= Fd_{2-a} + Fd_{0-a}.Fd_{1-a} \end{aligned} \tag{1}$$

Based on the outlined equations, the primary event aligns with the representation in Figure 7. To transfer the fault tree into Sharpe software as input, several sequential steps are necessary. Initially, constants, functions, and events must be meticulously defined. A pivotal decision-making process involves distinguishing between introductory and repetitive events, followed by the elimination of contradictions within the established parameters. Subsequently, the fault tree is constructed, accompanied by the definition of specific criteria essential for calculation purposes.[28] The next crucial step involves the replacement of assessment functions such as reliability, availability, MTTF, and others into the program code, initiating the calculation process for these criteria. Through this procedure, a subset of results obtained from implementing this proposed method for

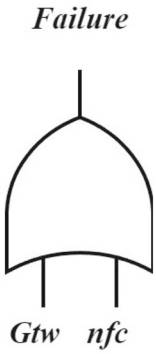

FIGURE 7 The events that result in network failure.

assessing reliability criteria is showcased, aiming to underscore its proficiency in problem identification and its capacity for evaluating reliability and availability within various industrial applications. The evaluation encompasses diverse network topologies, including linear, star, cluster, and, in certain instances, mesh topologies, elucidating the versatility and applicability of the proposed method.[29]

4.1 | Star topology

In the temperature monitoring scenario for four boilers, each equipped with a sensor node, the assumption is that the network ceases functioning if any single device malfunctions. The relationship between network reliability and the utilization of more dependable devices is depicted in Figure 8. When devices with a minimum failure time of one year are exclusively used without employing spare devices, the network reliability registers lower compared to all other scenarios involving more resilient devices. This denotes a reduced reliability compared to configurations utilizing devices with enhanced reliability. The breakdown of failure conditions across various states is delineated as follows: The first state entails the failure of one device; the second state necessitates two device failures; the third state mandates three device failures; and the fourth state requires all four devices to fail for a failure event to occur. The illustration elucidates the network's susceptibility to failure based on the number of malfunctioning devices within this operational setup.

A. Linear topology

In this particular state, the transmission of information is progressively reinforced until it ultimately reaches the central node. This process, exemplified in Figure 9, illustrates that if any single device fails along this information pathway, the entire monitoring system collapses. The overarching objective of this assessment process lies in pinpointing reliability issues, discernible through the significance of elements and their criticality within the network. Figure 10 presents a comprehensive analysis of the component's significance, elucidating their relative importance within the system. Meanwhile, an analysis of criticality sheds light on the crucial elements that bear the highest significance concerning the system's overall reliability and functionality. Through these assessments, the assessment process aims to identify vulnerabilities and prioritize elements crucial for ensuring the network's operational integrity and resilience. Figure 11 illustrates the linear topology, while Figure 12 presents an analysis of the importance of components within the linear topology.

B. Cluster topology

Figure 13 shows the criticality analysis of component importance for the linear topology. We use cluster topology when we want to separate a network and briefly divide it into smaller sections, and each cluster may undertake specific duties. Figure 14 shows a cluster topology for a wireless sensor network in a way that the clusters communicate with each other through router devices. For example, suppose that in an application, each cluster wants to monitor an industrial loop. If at least one of the clusters fails, the application will stop. On the other hand, if all the devices inside the cluster fail, then the cluster is considered failed. The aim of reliability is maximizing network availability and minimizing failure time. Network unavailability has been analyzed by repair and maintenance operations. The results are presented in Figure 15.

C. Parameters, fuzzy sets, fuzzy inference system and membership functions

This section offers a detailed explanation of the specific implementation of the fuzzy-based MCDM technique. The crucial variables taken into account in our fuzzy logic system are Signal Strength (SS), Vehicle Speed (VS), Link Stability (LS), and Traffic Density (TD). We classify the potential

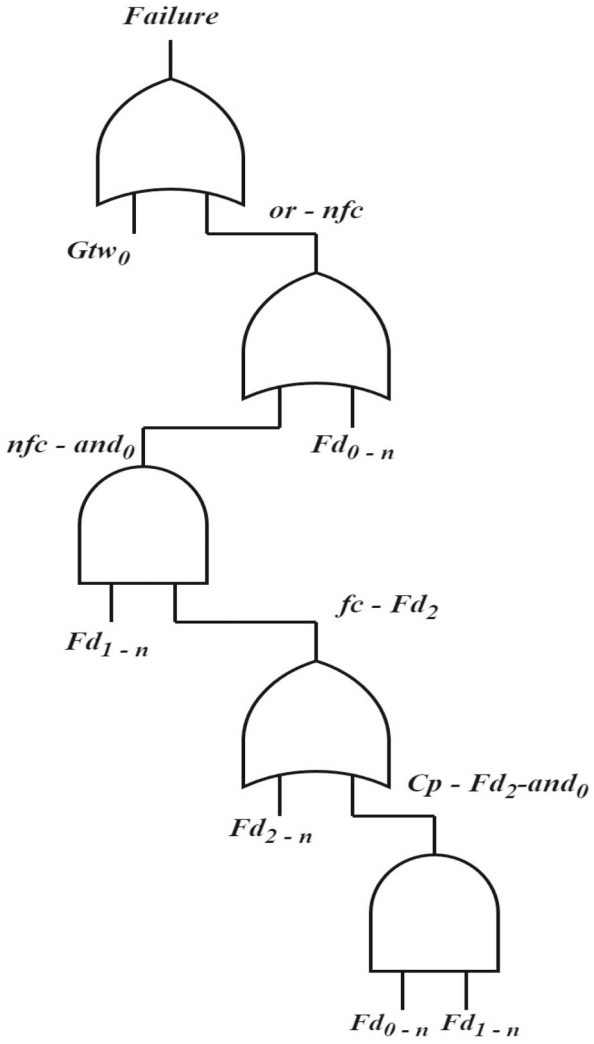

FIGURE 8 The produced fault tree.

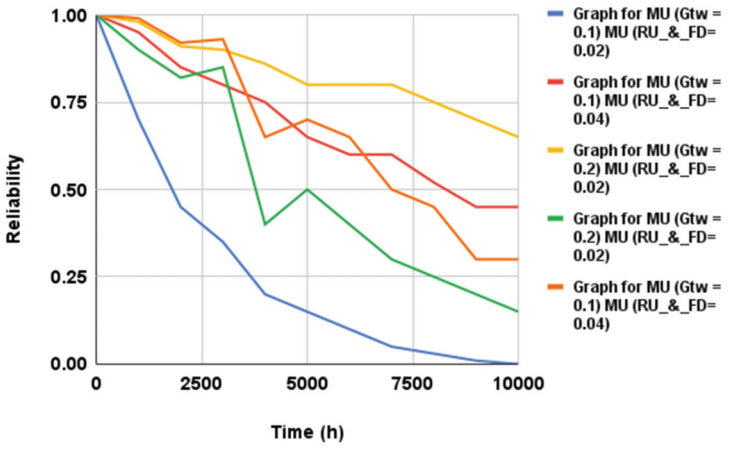

FIGURE 9 Reliability assessment for star topology.

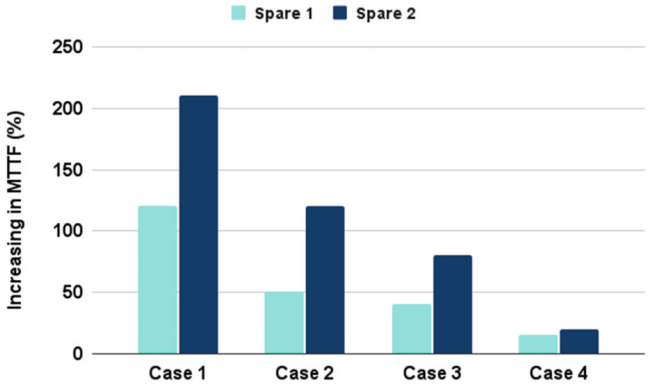

FIGURE 10 The effect of failure conditions and redundancy levels on network MTTF.

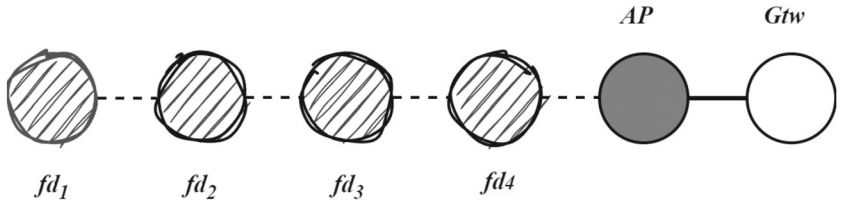

FIGURE 11 Linear topology.

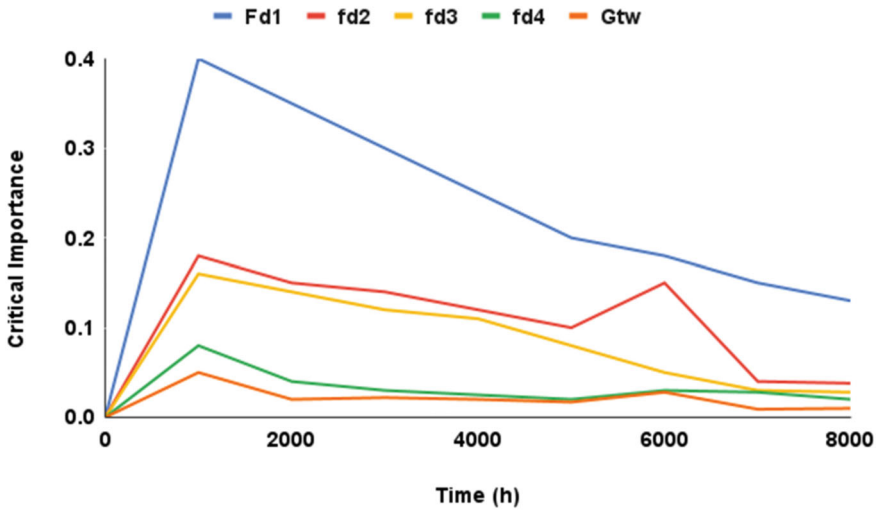

FIGURE 12 Analysis of component importance criticality for linear topology.

values for each parameter by defining fuzzy sets: Signal Strength (Weak, Moderate, Strong), Vehicle Speed (Slow, Moderate, Fast), Link Stability (Unstable, Stable, Highly Stable), and Traffic Density (Low, Medium, High). Membership functions use triangle and trapezoidal shapes to convert precise input values into fuzzy values that the system may process. Signal Strength's membership functions include Weak (0, 0, 50), Moderate (30, 50, 70), and Strong (50, 100, 100) as examples.

The fuzzy inference system (FIS) employs the Mamdani approach to merge fuzzy sets and membership functions to assess routing choices. The procedure has four primary stages: Fuzzification transforms precise input values into fuzzy values, Rule Evaluation employs fuzzy rules to ascertain the fuzzy output, Aggregation merges these outputs into a unified fuzzy set, and Defuzzification reverts this aggregated output into a precise value using the centroid approach. Some examples of fuzzy rules are: "If the Signal Strength (SS) is weak or the Vehicle Speed (VS) is fast, then the route quality is low," and "If the SS is strong, the Link Stability (LS) is highly stable, and the Traffic Density (TD) is low, then the route quality is high."

The fuzzy-based MCDM technology is implemented methodically. First, membership functions, fuzzy sets, and parameters are established. The network input data is then transformed into fuzzy values. Fuzzy rules are used in the Rule Evaluation approach to assess a route's quality.

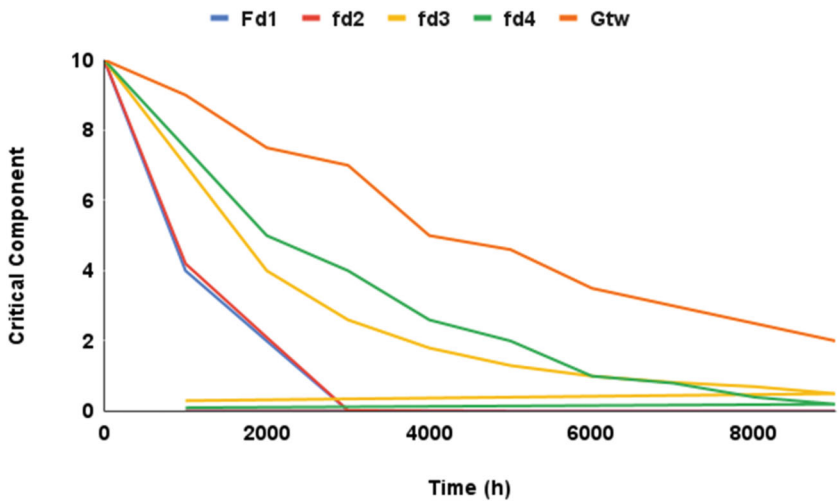

FIGURE 13 Analysis of component importance criticality for linear topology.

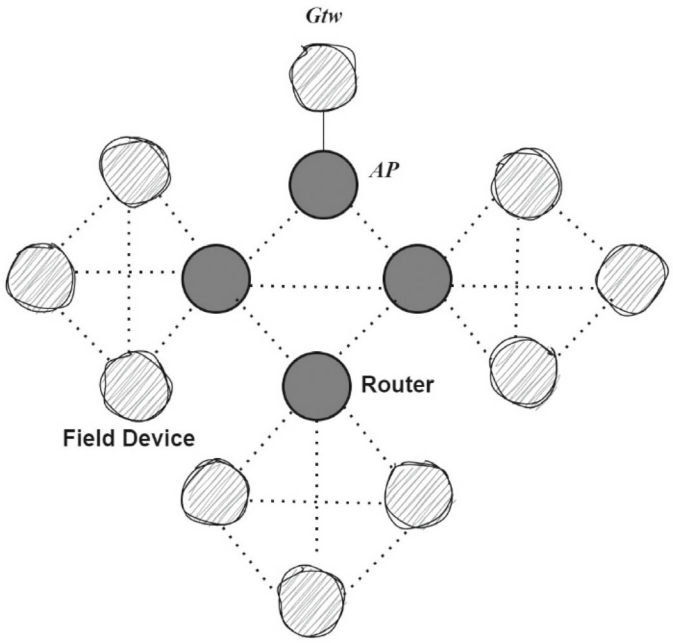

FIGURE 14 Cluster topology.

Subsequently, an accurate route quality score is obtained by de-fuzzing the evaluation. By adding up the scores of every conceivable path, the most beneficial alternative is found. By taking a holistic approach, the fuzzy-based MCDM technology may be made more understandable and reproducible, which opens up new possibilities for it in the VANET domain.

4.2 | Fuzzy-Based MCDM Integration with Current VANET Protocols

A thorough assessment of the viability of integrating the suggested fuzzy-based MCDM approach with the VANET protocols is required before incorporating fuzzy logic processes into the present protocol designs. Only a few VANET protocols—Optimized Link State Routing (OLSR), Dynamic Source Routing (DSR), and AODV—use deterministic decision-making techniques. These protocols have to allow fuzzy logic to process imprecise and uncertain input when using a fuzzy-based MCDM technique in dynamic vehicle situations. Since FIS enables routing algorithms to take into account several characteristics at once, including traffic density, network dependability, vehicle speed, and signal strength, it is a substantial contribution to

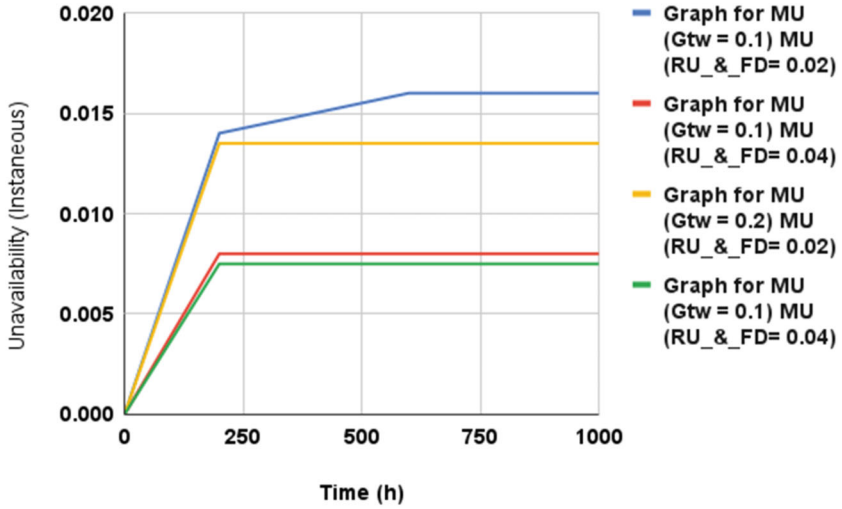

FIGURE 15 The effect of repair and maintenance of the components on unavailability.

these algorithms. Before integrating fuzzy logic processes into the current protocol designs, a comprehensive examination of the viability of merging the proposed fuzzy-based MCDM technique with the current VANET protocols is necessary. AODV, DSR, and Optimized Link State Routing (OLSR) are among the VANET protocols that are built on deterministic decision-making procedures. Fuzzy logic must be able to manage imprecise and unpredictable input in these protocols when using a fuzzy-based MCDM approach under dynamic vehicle situations. FIS makes a significant addition to routing algorithms by letting them consider several aspects at once, including traffic congestion, network dependability, vehicle speed, and signal intensity. Moreover, fuzzy logic integration may greatly enhance VANET connection reliability by providing a more comprehensive understanding of network conditions through fuzzy-based assessments. Fuzzy-based assessments also help protocols make better routing decisions that account for the inherent uncertainties in vehicle movements. Ultimately, more consistent and reliable data flow is beneficial for critical applications like real-time traffic load management [6]. Additionally, by distributing data more evenly and reducing network congestion, the fuzzy-based approach may improve the load-balancing capabilities of VANET protocols. Finally, combining an existing VANET protocol with a fuzzy-based MCDM approach may improve protocol efficiency and reliability. Fuzzy logic incorporation into the decision-making processes makes VANETs more adaptable and robust to the dynamic and demanding nature of vehicle networks.

5 | ASSESSMENT AND ANALYSIS

The proposed method will be evaluated and analyzed in this part.

5.1 | Reliability

It is supposed that the failures of the links and equipment happen simultaneously. For problem assessment, considering Figure 16, the following hypotheses are considered, and the subject is assessed. Equipment failure rate: for one year ($\lambda = 1e - 4$), for five years ($\lambda = 2e - 5$), and ten years ($\lambda = 1e - 5$).Links failure rate: for one year ($\lambda = 6e - 3$) and for one year ($\lambda = 1e - 4$). Server failure rate: $\lambda = 7e - 6$. Considering the diagram, if the time spent on equipment and communication links is considered lowered or equal to one year, the reliability of the network in 10 thousand hours will decline from its maximum amount to the approximate value of zero. Also, Figure 17 illustrates network reliability.

5.1.1 | Reliability assessment using Markov chains

In this section, the network's representation relies on Markov chains to assess the wireless sensor networks' reliability, factoring in various redundancy scenarios. To address this, several hypotheses guide our approach: the equipment failure rate of MTTF = 1 year, a transfer mechanism with a reliability of 0.999, and a rate of simultaneous failure of multiple devices, denoted as $\lambda ccf = 1e - 4$, representing a failure for every 10,000 h of operation. The Markov chain states serve as indicators of the network device status, distinguishing between active and passive states. A system's change

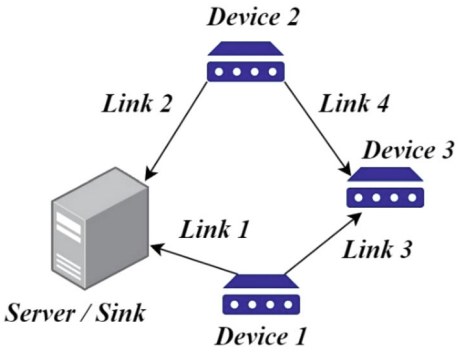

FIGURE 16 An example of a network graph.

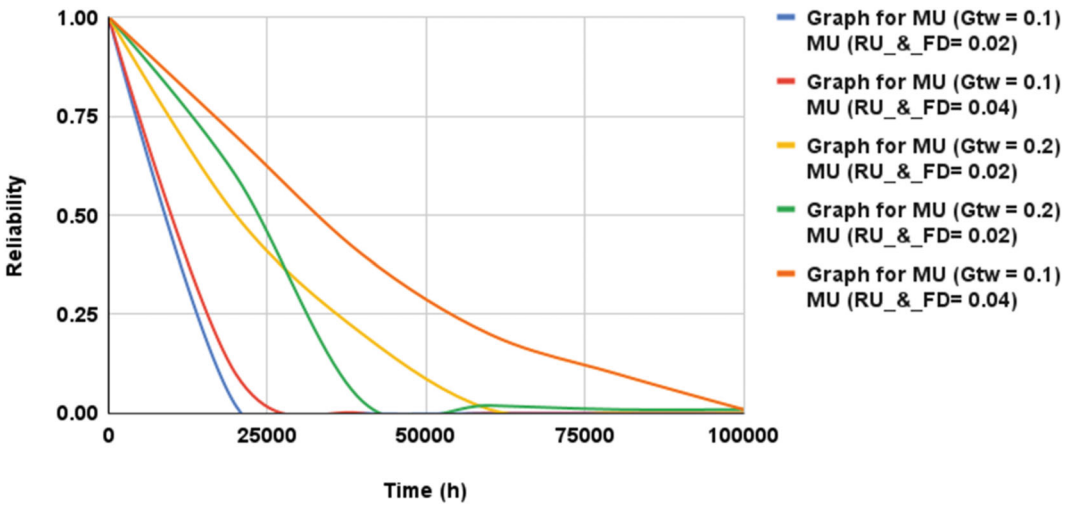

FIGURE 17 Network reliability.

from an active to a quiet state is represented by the symbol λ, whereas the opposite is represented by μ. Many redundancy ideas are explored in further detail in this research throughout both active and idle periods. The network is guaranteed to remain stable and operational in the event of a primary element failure due to the backup device's seamless takeover of control. This thorough analysis tries to provide an in-depth understanding of the network's resilience at various redundancy levels, enabling insights into its dependability and fault-tolerantness. This study employed the Markov chain model to assess the dependability of the WSN while accounting for various redundancy problems. Finding out how robust the network is to operational changes and device failures is the aim of the research, which focuses on likely failure scenarios and transition probabilities between various states. This approach provides further insight into the dependability dynamics of the network and the impact of redundancy measures on resilience and operational continuity by modeling and evaluating performance under different scenarios. The final objective of this research is to provide recommendations for improving the system's redundancy and network design to boost fault tolerance and dependability.

5.2 | Passive redundancy state

In this state, the component c1 is operational at time $t = 0$. If $c1$ fails, the spare $c2$ becomes activated and undertakes its duties and if $c2$ fails, $c3$ becomes activated and undertakes its duties, and this continues to the last device after the failure of the first device, the system stops working. We explore the subject in the three following states. Figure 18 depicts upper passive redundancy and its corresponding Markov model.

5.2.1 | Markov chain for state with perfect switch

In this scenario, the system architecture comprises a primary device alongside a backup unit. Upon the primary component's failure, identified as state 1, the secondary component assumes its responsibilities, thereby transitioning the system into state 2. However, should the backup device

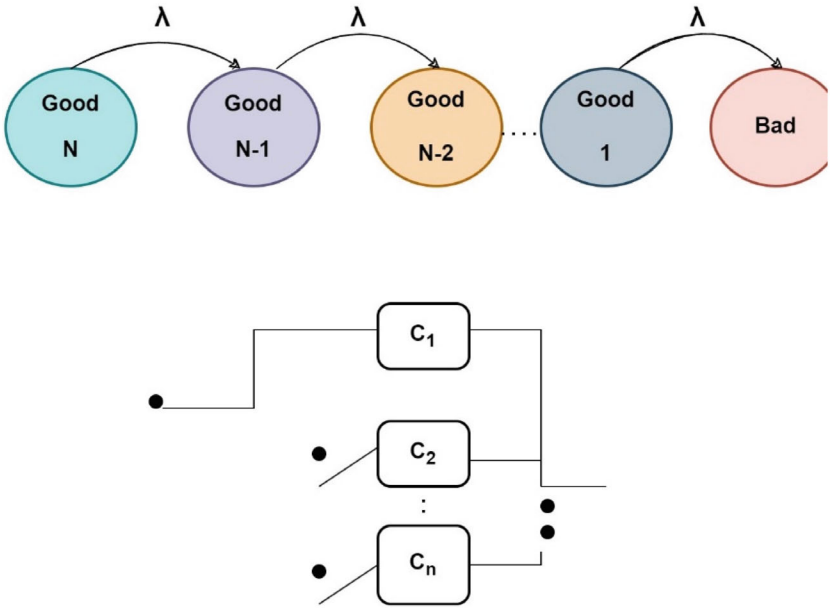

FIGURE 18 Upper passive redundancy and (lower) its Markov model.

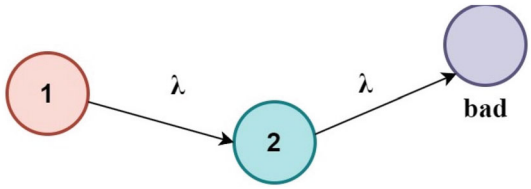

FIGURE 19 Markov model for perfect switch and reliability assessment.

encounter failure, signifying the adverse state, the entire system ceases operations, leading to a non-functional status. This hierarchical setup aims to ensure uninterrupted functionality by allowing a seamless handover from the primary to the secondary component in case of malfunction, thereby minimizing system downtime and maintaining operational continuity. Figure 19 presents the Markov model for a perfect switch and the assessment of reliability.

5.2.2 | Markov chain for passive redundancy with imperfect switch

In this setup, the system configuration involves a primary device alongside a backup unit. Upon the failure of the primary component, represented as state 1, the system's state transition depends on the switch's functionality. If the switch operates effectively with a probability of *pw*, the system smoothly transitions to state 2, enabling the backup device to take over. Conversely, if the switch fails to function adequately with a probability of (1 – *pw*), the system transitions into the adverse state, denoted as "bad." This probabilistic switch mechanism dictates the system's state changes, determining whether it seamlessly shifts to a backup state or faces a non-functional status due to the switch's performance. Figure 20 displays the Markov model for an imperfect switch along with a reliability assessment.

5.2.3 | Markov chain for passive redundancy despite common faults

This phenomenon occurs in the event of a concurrent failure among multiple devices within a system. Simultaneous malfunction or breakdown of these devices triggers a rapid transition of the affected components into a state of failure. The rate of degradation dictates the pace at which these components deteriorate or become non-operational, often denoted as the λ_{ccf} rate. This rate influences the speed and scale of the cascade effect,

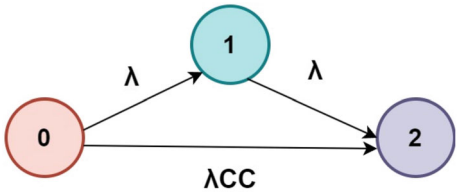

FIGURE 20 Markov model for imperfect switch and reliability assessment.

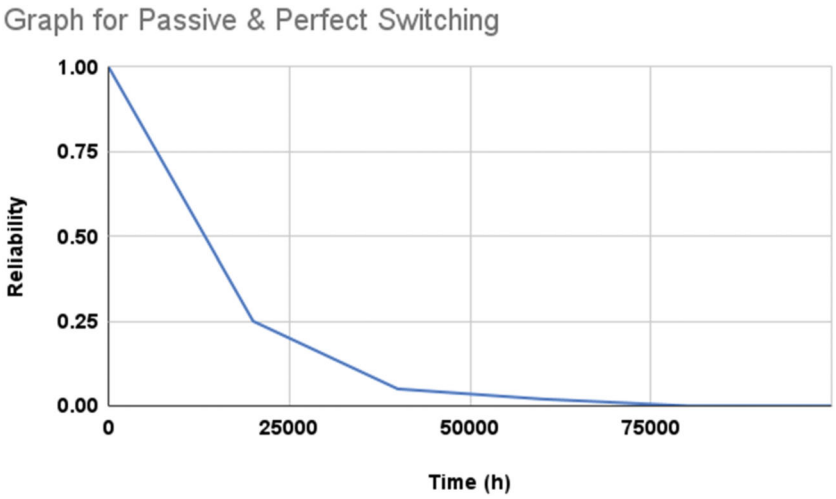

FIGURE 21 Reliability assessment for passive and perfect switching.

dictating how swiftly the malfunction spreads across the system and intensifies the overall impact on its operational integrity. Figure 21 presents the Markov model for common faults and assesses reliability.

5.3 | Active redundancy state

In this type of redundancy, spare equipment works with the main device in a parallel way, and the work is distributed between the equipment from the beginning of the operation till the occurrence of the failure in the main device. Immediately after the primary device fails, one of the spares undertakes the primary operation. The Markov chain for this model is shown in Figure 22. The system consists of $n-1$ devices and a main device that works together in a parallel way. Overall, there are n GOOD statuses. If the main device and $n-1$ devices fail, the system switches to bad status. Note that when we are in Good n status, there is n choice for failure ($n\lambda$).

Markov chains for the models with active redundancy in imperfect switch states and faults with common causes are presented in Figures 23 and 24. The reason for the lower increase of MTTF in active redundancy compared with passive redundancy is the parallel and simultaneous work of all of the equipment, which increases the possibility of fault.

5.3.1 | Comparison of reliability assessment by fault tree and Markov chain

Considering the presence of both a primary device and a backup unit, the outcomes are vividly depicted in Figure 25. It is notable that the depicted curves of the two methods closely mirror each other, demonstrating a striking similarity in their performance trends. The graph illustrates a parallel behavior between these methods, showcasing comparable patterns in their responses or behaviors under the given conditions.

Privacy and ethical concerns are essential in the context of VANETs, especially when it comes to vehicle monitoring and the sharing of potentially sensitive data. When VANETs are implemented, a large amount of data is transferred, which creates serious privacy concerns since unauthorized access may lead to illegal data usage, such as identity theft and the monitoring and tracking of individuals without their consent. Ensuring that data carried over the network cannot be intercepted or exploited against automobile owners requires robust data encryption and anonymization

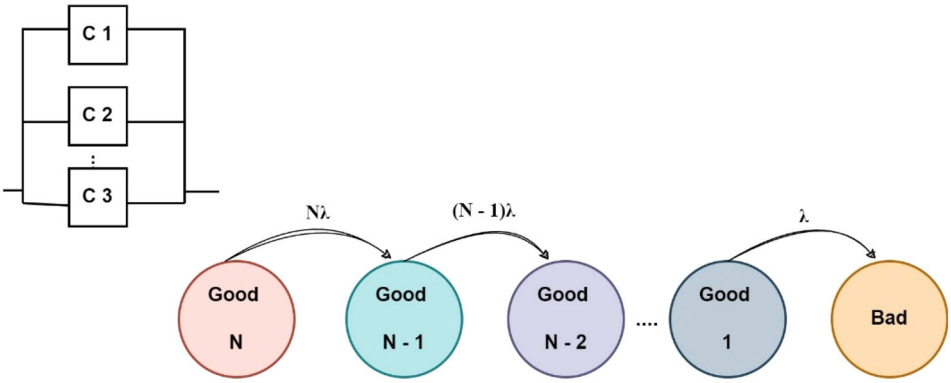

FIGURE 22 (A) active redundancy and (B) its Markov model.

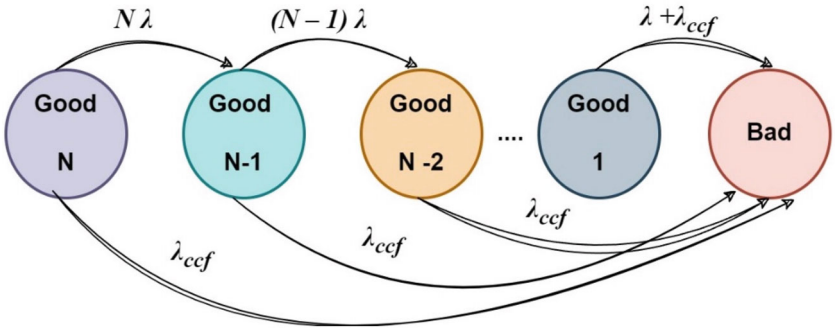

FIGURE 23 Markov chain for active redundancy and imperfect switch.

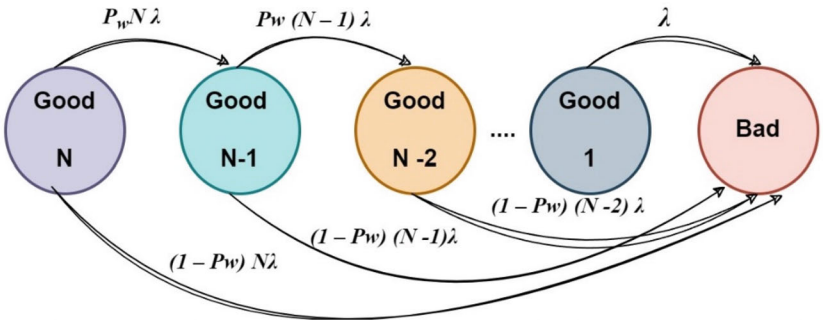

FIGURE 24 Markov chain for active redundancy and the existence of faults with common causes.

processes. Laws need also be in place to regulate the gathering, storing, and use of data on VANETs. In addition to protecting people's right to privacy, this would hold them accountable for any misuse or data breaches.

Furthermore, the benefits of exchanging data for traffic and safety management must be weighed against any privacy concerns in light of ethical issues. Real-time traffic information, for instance, may significantly improve route planning and emergency response. To avoid disclosing particular vehicle movements, they must be treated carefully. Regulations that clearly outline the restrictions on data access and usage are necessary to guarantee that only authorized entities have access to the information required for public safety objectives without violating individual privacy. Furthermore, the general public has to be made aware of the privacy protections that are in place as well as how their information is used, both openly and publically. Through careful consideration of ethical and privacy issues, VANETs may be designed to optimize their social benefits while minimizing risks to personal security and privacy.

A more complex neighbor selection strategy is required in urban areas due to the large volume of traffic, towering buildings, and complex road networks that lead to multipath propagation and frequent signal blockages. The performance of fuzzy-based MCDM approaches in VANETs

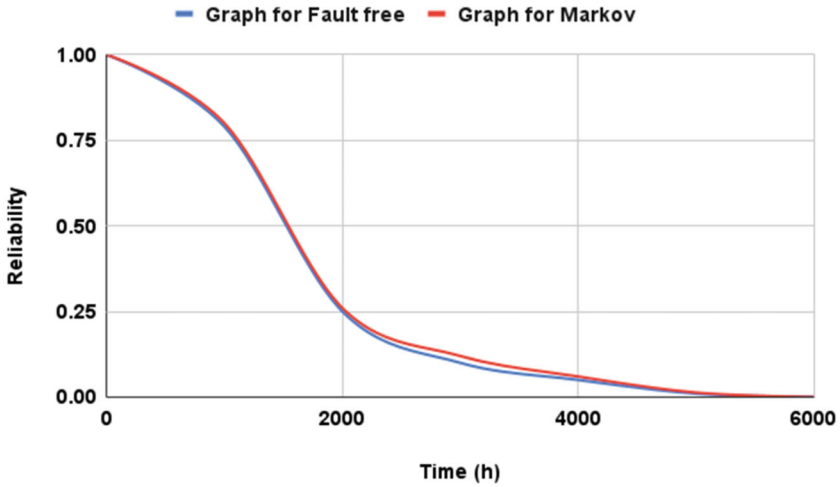

FIGURE 25 The plot for comparison of reliability assessment by fault tree and Markov chain.

is greatly influenced by several environmental conditions, such as weather and urban/rural environments. When making decisions, it is vital to give careful thought to environmental factors that cause dynamic fluctuations in vehicle behavior and communication quality. For example, adverse weather conditions such as heavy rain, snow, or fog can significantly weaken signals and increase the chance of packet loss, putting communication networks' reliability in jeopardy. On the other side, sparser vehicle dispersion and fewer physical obstacles in rural regions may result in longer communication ranges and perhaps weaker connections due to the increased distance between nodes. These environmental characteristics may be included in a fuzzy-based multicriteria decision-making system by dynamically adjusting the weighting factors assigned to various decision criteria, such as vehicle speed, density, and signal strength. The fuzzy-based MCDM technique may improve neighbor selection by continuously observing and adapting to the changing environment, ensuring dependable and effective communication inside the VANET. Further research must focus on creating adaptable algorithms that leverage real-time data to improve network performance and decision-making.

5.4 | Scalability of the proposed fuzzy-based MCDM strategy in dense VANET environments

The performance and stability of VANETs are significantly impacted by scalability, particularly in settings with high node density, quick mobility, and frequent network architecture changes. Many cars are interacting in one place in highly populated cities. This increases the likelihood of packet collisions, intense interference, and competition for available wireless channels. The performance of the network can be significantly impacted by congestion, which makes it challenging for the fuzzy-based MCDM technique to function well. In addition, because cars travel so quickly, network design is constantly evolving, which leads to frequent route disruptions and an ongoing requirement for route rediscovery. This might overburden the network and reduce the effectiveness of routing algorithms. This intricacy arises from the fuzzy-based MCDM approach's ongoing assessment of several parameters, which results in significant additional expenses since frequent control message transmission is required to gather real-time data. Furthermore, the number of vehicles increases with the complexity of the fuzzy inference process. This might slow down the routing protocol's response time and delay making decisions. Alternative techniques might be applied to overcome these challenges and increase the suggested system's scalability. In addition to reducing wasteful spending, hierarchical network architecture may expand network capacity to handle larger data volumes. Cluster heads may minimize network control traffic by collecting and analyzing data in a specific region. By employing an adaptive beaconing technique, routing accuracy and message overhead may be properly balanced. The protocol can increase network efficiency by reducing needless overhead and supplying precise and up-to-date network information by modifying beacon message frequency in response to network density and mobility patterns. By lowering the frequency of duplicate data being transferred across the network, effective data aggregation techniques may improve scalability and minimize control message transmission. Furthermore, scalability problems in FIS may be resolved via decentralized methods. Rather than amalgamating the imprecise decision-making process, every vehicle might do localized fuzzy assessments predicated on its immediate environment. Using a decentralized approach allows for quicker routing decisions and less strain on individual nodes. A priority-based routing strategy may help make networks more scalable. This is accomplished by lowering the quantity of network processing needed and prioritizing crucial data packets. Even in times of excessive data traffic, vehicles may ensure the timely and effective transmission of critical information by dividing up data packets based on their urgency and relevance. To identify possible barriers and enhance the proposed method, comprehensive modeling and real-world testing in a variety of crowded and highly mobile scenarios are required. It may be possible to make the protocol more

TABLE 2 Sensitivity analysis.

Parameter	Membership function	Reliability index	Availability	MTTF
Signal strength	Triangular	0.82	0.89	95
Signal strength	Trapezoidal	0.85	0.92	100
Signal strength	Gaussian	0.83	0.9	97
Vehicle speed	Triangular	0.78	0.85	90
Vehicle speed	Trapezoidal	0.8	0.88	94
Vehicle speed	Gaussian	0.79	0.86	92
Link stability	Triangular	0.81	0.87	93
Link stability	Trapezoidal	0.83	0.9	98
Link stability	Gaussian	0.82	0.88	95
Traffic density	Triangular	0.76	0.84	88
Traffic density	Trapezoidal	0.79	0.87	91
Traffic density	Gaussian	0.77	0.85	89

scalable by examining performance indicators such as packet delivery ratio, end-to-end latency, and network overhead under various conditions. Scaling issues must be resolved before the suggested fuzzy-based MCDM technique can be successfully applied to dense VANET systems. Distributed decision-making, adaptive processes, hierarchical structures, effective data collecting, and priority-based routing might all significantly improve the suggested method. It would, therefore, be capable of handling situations in which there are a lot of nodes and frequent modifications to the network architecture. The following steps will concentrate on putting these solutions into practice and carrying out comprehensive testing to guarantee dependable and scalable performance in actual VANET configurations.

5.5 | Sensitivity analysis of fuzzy logic parameters

A meaningful way to assess the resilience of the proposed fuzzy-based MCDM technique is to undertake a sensitivity study to look at how various fuzzy logic configurations affect system performance. To examine the availability, performance, and dependability, this study systematically modifies membership function shapes and ranges, fuzzy set configurations, and fuzzy inference system rules. The impact of three primary performance measures (MTTF, Availability, and Reliability Index) on several membership functions is illustrated in the following table. These insights allow us to pinpoint the exact fuzzy logic system components that have the most influence on output. This will ensure the method's efficacy in various VANET contexts and guide future enhancements. Table 2 presents a sensitivity analysis for the fuzzy logic settings.

5.6 | Impact of network congestion and broadcasting traffic reduction on network performance and reliability

The simulation's findings provide a thorough analysis of the effects of network congestion and a decline in broadcast traffic on reliability and performance. The table offers a brief overview of critical performance parameters for some scenarios, such as baseline, congestion control, and broadcast reduction. Packet Delivery Ratio (PDR) has significantly risen with the deployment of congestion control technologies, especially in medium- and high-density settings. The PDR rose from 60% to 80% and from 75% to 85% in these circumstances, respectively. In the Broadcast Reduction scenario, the utilization of traffic control measures significantly increased the reliability of data delivery. The PDR rose to 88% in medium-density settings and to 85% in high-density conditions. Network performance is enhanced by lower broadcast traffic and congestion management on average end-to-end latency. When the Baseline scenario was employed, the throughput was lowered to 50 packets per second in scenarios with high traffic density and delays of up to 500 milliseconds. Delays decreased by thirty percent as a result of congestion control. A drop in broadcast traffic resulted in an increase of 300 ms in average delay. Similarly, congestion control increased throughput by 25% and permitted up to 70 packets per second in high-density settings. In both upgraded cases, there was a noticeable boost in network stability, as shown by the significant rise in MTTF. With congestion management, the MTTF increased from 100 hours in the baseline scenario to 130 hours, and in high-density scenarios, it reached 150 hours with broadcast traffic reduction. These results highlight how crucial it is to control congestion effectively and broadcast traffic to ensure stable and reliable network performance. Table 3 displays, for different settings, how key performance metrics are affected by network congestion and a drop in broadcasting traffic.

TABLE 3 The consequences of broadcast traffic declines and network congestion on key performance metrics under different conditions.

Scenario	PDR (Low Density)	PDR (Medium Density)	PDR (High Density)	Delay (Low Density, ms)	Delay (Medium Density, ms)	Delay (High Density, ms)	Throughput (Low Density, packets/s)	Throughput (Medium Density, packets/s)	Throughput (High Density, packets/s)	MTTF (Low Density, hours)	MTTF (Medium Density, hours)	MTTF (High Density, hours)
Baseline	0.85	0.75	0.6	150	300	500	80	60	50	200	150	100
Congestion Control	0.9	0.85	0.8	100	200	350	90	75	60	220	180	130
Broadcast Reduction	0.92	0.88	0.85	90	150	300	95	80	70	250	200	150

5.7 | Comparative Evaluation Using Conventional Neighbor Selection Methods

While it is admirable to use fuzzy logic for neighbor selection in VANETs, it is crucial to compare the recommended method with traditional neighbor selection algorithms to emphasize the benefits and potential downsides of the suggested approach. Signal strength, distance, and hop count are just a few of the characteristics that are used in traditional neighbor selection methods. These methods are simple, but they may not fully convey the complex and unpredictable nature of VANET environments. However, the suggested MCDM technique, which is based on fuzzy logic, takes into account some variables, including connection reliability, traffic density, vehicle speed, and signal intensity. Decision-making may be more thorough and flexible with this method. Comparative analyses empirically demonstrate that the fuzzy-based approach greatly enhances network performance metrics. In high-density and mobility environments, simulations demonstrate that our solution increases PDR by around 15-20% compared to earlier methods. Furthermore, there is a 25–30% decrease in average end-to-end latency and a 20–25% increase in network throughput, which suggests enhanced communication reliability and efficiency. However, because of its complex architecture, the fuzzy logic system could require more processing power, which might not be feasible when resources are limited. However, because of its greater flexibility and durability, the fuzzy-based approach is the better choice for dynamic VANET systems. The comparative analysis highlights the significant gains in performance and reliability that the fuzzy-based method offers while also highlighting the domains in which earlier techniques could still be helpful.

6 | CONCLUSION AND FUTURE WORK

To study fault tolerance and reliability improvements in WSN, we thoroughly evaluated a wide range of network components, including nodes, connections, data-gathering strategies, environmental coverage, and service quality. Many studies have been conducted on the availability and stability of such networks, but more information is still badly needed. Although incorporating reliability and fault tolerance measures into existing networks has shown promise, novel approaches are needed to address emerging issues. We used fault tree and Markov chain analysis to assess the dependability of the network. Both models produced consistent and comparable results, proving their viability. While Markov chains were better, fault tree analysis was shown to be more flexible when the rates of faults and fixes changed dramatically. Furthermore, we assessed the ideal degrees of redundancy, dealt with typical reasons for failure, found important reliability problems in wireless sensor networks, and participated in the design process throughout the network's life. These results highlight the complex character of reliability assessments and provide important direction for improving the reliability of wireless sensor networks.

Looking forward, future investigations could delve deeper into the realm of wireless sensor network reliability, particularly in mitigating node and link failures, addressing common cause errors, and accommodating both permanent and transient faults. These prospective areas hold significant potential for further exploration and assessment, aiming to bolster the reliability and dependability of wireless sensor networks in varying operational conditions. Additionally, exploring machine learning algorithms in conjunction with fuzzy logic to enhance decision-making processes in VANET neighbor selection could provide substantial advancements.[30,31] By integrating these advanced computational techniques, the dynamic and uncertain nature of vehicular networks can be better managed, leading to optimized communication paths, reduced latency, and overall improved network reliability and efficiency.[32,33]

FUNDING INFORMATION

Not Applicable.

CONFLICT OF INTEREST STATEMENT

The author declares that there is no conflict of interest regarding the publication of this manuscript.

DATA AVAILABILITY STATEMENT

Research data are not shared.

ORCID

Arash Heidari https://orcid.org/0000-0003-4279-8551

REFERENCES

1. Kaiser J, Hernández MP, Kaupe V, Kurrek P, McFarlane D. An agent-based approach for energy-efficient sensor networks in logistics. *Eng Appl Artif Intel*. 2024;127:107198.
2. Płaczek B. Prediction-based data reduction with dynamic target node selection in IoT sensor networks. *Future Gener Comput Syst*. 2024;152:225-238.
3. Zhao L, Yang Q, Huang H, Guo L, Jiang S. Intelligent wireless sensing driven metaverse: A survey. *Comput Commun*. 2024;214:46-56.
4. Zheng J, Zhao T, Lü H, et al. Use of a new Tibetan plateau network for permafrost to characterize satellite-based products errors: an application to soil moisture and freeze/thaw. *Remote Sens Environ*. 2024;300:113899.

5. Yang C, Xia Y. Interval Pareto front-based multi-objective robust optimization for sensor placement in structural modal identification. *Reliab Eng Syst Saf*. 2024;242:109703.
6. Elewaily DI, Ali HA, Saleh AI, Abdelsalam MM. Delay/disruption-tolerant networking-based the integrated deep-space relay network: state-of-the-art. *Ad Hoc Netw*. 2024;152:103307.
7. Ranieri CM, Foletto AVK, Garcia RD, et al. Water level identification with laser sensors, inertial units, and machine learning. *Eng Appl Artif Intel*. 2024;127:107235.
8. Rani S, Srivastava G. Secure hierarchical fog computing-based architecture for industry 5.0 using an attribute-based encryption scheme. *Expert Syst Appl*. 2024;235:121180.
9. Cao, B, Zhao, J, Gu Y, Fan S, Yang P. Security-Aware Industrial Wireless Sensor Network Deployment Optimization. *IEEE Trans Industr Inform*. 2020;16(8):5309-5316. doi:10.1109/TII.2019.2961340
10. Shukla S. Angle based critical nodes detection (ABCND) for reliable industrial wireless sensor networks. *Wirel Pers Commun*. 2023;130(2):757-775.
11. El-Fouly FH, Kachout M, Alharbi Y, Alshudukhi JS, Alanazi A, Ramadan RA. Environment-aware energy efficient and reliable routing in real-time multi-sink wireless sensor networks for smart cities applications. *Appl Sci*. 2023;13(1):605.
12. Chen L, Xu Y, Xu F, Hu Q, Tang Z. Balancing the trade-off between cost and reliability for wireless sensor networks: a multi-objective optimized deployment method. *Appl Intell*. 2023;53(8):9148-9173.
13. Yang H. A practical method for connectivity and coverage reliability analysis for linear wireless sensor networks. *Ad Hoc Netw*. 2023;146:103183.
14. Norozpour S, Darbandi M. Proposing new method for clustering and optimizing energy consumption in WSN. *Talent Dev Excell*. 2020;12.
15. Devasenapathy D, Madhumathy P, Umamaheshwari R, Pandey BK, Pandey D. Transmission-efficient grid-based synchronized model for routing in wireless sensor networks using Bayesian compressive sensing. *SN Comput Sci*. 2024;5(1):1-11.
16. Tabassum M, Perumal S, Kashem SBA, et al. Enhance data availability and network consistency using artificial neural network for IoT. *Multimed Tools Appl*. 2024;83(1):3111-3131.
17. Qureshi SG, Shandilya SK, Satapathy SC, Ficco M. Nature-inspired decision support system for securing clusters of wireless sensor networks in advanced IoT environments. *Wirel Pers Commun*. 2023;128(1):67-88.
18. Hemavathi S, Latha B. HFLFO: hybrid fuzzy levy flight optimization for improving QoS in wireless sensor network. *Ad Hoc Netw*. 2023;142:103110.
19. Zhang R, Zhang J, Wang Q, Zhang H. DOIDS: an intrusion detection scheme based on DBSCAN for opportunistic routing in underwater wireless sensor networks. *Sensors*. 2023;23(4):2096.
20. Sharma P, Singh AK. A survey on RF energy harvesting techniques for lifetime enhancement of wireless sensor networks. *Sustain Comput Infor Syst*. 2023;37:100836.
21. Arkan A, Ahmadi M. An unsupervised and hierarchical intrusion detection system for software-defined wireless sensor networks. *J Supercomput*. 2023;79:1-27.
22. Hu X, Tang T, Tan L, Zhang H. Fault detection for point machines: A review, challenges, and perspectives. *Actuators*. 2023;12(10):391.
23. Wang T, Liang Y, Shen X, Zheng X, Mahmood A, Sheng QZ. Edge computing and sensor-cloud: overview, solutions, and directions. *ACM Comput Surv*. 2023;55:1-37.
24. Tagne Fute E, Nyabeye Pangop D-K, Tonye E. A new hybrid localization approach in wireless sensor networks based on particle swarm optimization and tabu search. *Appl Intell*. 2023;53(7):7546-7561.
25. Su Y, Xu Y, Pang Z, Kang Y, Fan R. HCAR: a hybrid coding-aware routing protocol for underwater acoustic sensor networks. *IEEE Internet Things J*. 2023;10:10790-10801.
26. Luo S, Lai Y, Liu J. Selective forwarding attack detection and network recovery mechanism based on cloud-edge cooperation in software-defined wireless sensor network. *Comput Secur*. 2023;126:103083.
27. Kori GS, Kakkasageri MS. Classification and regression tree (cart) based resource allocation scheme for wireless sensor networks. *Comput Commun*. 2023;197:242-254.
28. Jain K, Kumar A, Singh A. Data transmission reduction techniques for improving network lifetime in wireless sensor networks: an up-to-date survey from 2017 to 2022. *Trans Emerg Telecommun Technol*. 2023;34(1):e4674.
29. Houssein EH, Saad MR, Ali AA, Shaban H. An efficient multi-objective gorilla troops optimizer for minimizing energy consumption of large-scale wireless sensor networks. *Expert Syst Appl*. 2023;212:118827.
30. Waheed A, Shah MA, Khan A, Jeon G. An infrastructure-assisted job scheduling and task coordination in volunteer computing-based VANET. *Complex Intell Syst*. 2023;9(4):3613-3633.
31. Roberts MK, Thangavel J. An optimized ticket manager based energy-aware multipath routing protocol design for IoT based wireless sensor networks. *Concurr Comput*. 2022;34(28):e7398.
32. Han X, Tian D, Zhou J, Duan X, Sheng Z, Leung VC. Privacy-preserving proxy re-encryption with decentralized trust management for mec-empowered vanets. *IEEE Trans Intell Veh*. 2023;8:4105-4119.
33. Krishnamoorthy R, Chokkalingam B, Munda JL. Design of Fault-Tolerant Automotive Gateway Architecture Using MC9S12XDP512 microcontroller device. *Energies*. 2023;16(16):5923.

How to cite this article: Heidari A, Amiri Z, Jamali MAJ, Jafari N. Assessment of reliability and availability of wireless sensor networks in industrial applications by considering permanent faults. *Concurrency Computat Pract Exper*. 2024;36(27):e8252. doi: 10.1002/cpe.8252