Proceedings of the 9th International Conference on Intelligent Computing and Control Systems (ICICCS-2026)
DVD Part Number: CFP26K74-DVD; ISBN: 979-8-3315-8946-2

Fault Tolerant Routing Strategy for Delay Sensitive Industrial Internet of Things Communication Infrastructures

M. Menaka
Department of Computer Science
Bharath Institute of Higher Education and Research
Chennai, Tamil Nadu, India
menaka.cs@bharathuniv.ac.in

S. Sathya
Associate Professor
Department of Computer Science and Information Technology, School of Computing Sciences, Vels Institute of Science, Technology and Advanced Studies
Chennai, Tamil Nadu, India
ssathya.scs@vistas.ac.in

M. Sakthivanitha
Assistant Professor
Dept. of Computer Applications (UG) Vels Institute of Science, Technology and Advanced Studies
Chennai, Tamil Nadu India
sakthivanitha.scs@vistas.ac.in

Vishwa Priya V
Assistant Professor
Department of Computer Science and Information Technology, Vels Institute of Science, Technology and Advanced Studies,Chennai, Tamil Nadu, India
vishwapriya13@gmail.com

M. Mohamed Sirajudeen
Associate Professor & Dean
Nilgiri College of Arts and Science
Thaloor The Nilgiris,
Tamil Nadu, India
mdsirajudeen1@gmail.com

J. Anciline Jenifer
Assistant Professor
Department of MCA
Francis Xavier Engineering College
Tirunelveli, Tamil Nadu, India
ancilinejenifer@francisxavier.ac.in

Abstract: Fault-tolerant routing is crucial for reliable and delay-sensitive communication for Industrial Internet of Things (IIoT) infrastructures where the harsh environments, interference and dynamic network conditions typically degrade Quality of Service (QoS). The main issue that is tackled in this work is the high vulnerability of industrial sensor networks to link failures and congestion, leading to unacceptable delays in mission-critical applications such as predictive maintenance, robotic control, and real-time monitoring. The goal is to create a strategy for fault-tolerant routing, in order to reduce the end-to-end latency and ensure high reliability of packet delivery under different network conditions. The proposed method combines a hybrid approach of combining dynamic link quality estimation, multipath redundancy, and delay-aware adaptive route switching using lightweight distributed decision logic that is appropriate for resource constrained nodes. Simulation results are conducted on a 200-node industrial topology, which show a 27% reduction of end-to-end delay, a 19% improvement of packet delivery ratio and a 22% reduction of routing overhead against state-of-the-art protocols such as RPL-OF0, LOADng, and CQRP. These results validate the use of this strategy to enhance the network resilience and timeliness, which supports its use in real-time industrial control environments.These enhancements show that the suggested routing plan can be implemented directly in the IIoT environments that require reliable low latency communications to safeguard safety-critical industry applications like automated production lines, proactive maintenance systems, and real-time robots.

Keywords: Fault-tolerant routing, Industrial Internet of Things (IIoT), delay-sensitive communication, QoS, multipath routing, adaptive route switching, network resilience, real-time applications

I INTRODUCTION

The IIoT is fundamentally changing the way modern industries run by making machines, sensors, actuators, and edge-computing units all pervasive in the industry. Through this interconnected system of things, industries can have levels of automation, remote monitoring, predictive maintenance, and data-driven decision making that have never been seen before. However, the full potential of IIoT requires a lot from the underlying communication infrastructure in terms of reliability and timeliness. Industrial environments frequently feature metallic structures, electromagnetic interference, high temperature fluctuations as well as dynamic mechanical movements - all of which pose great problems for wireless communication systems. Therefore, it is important to ensure fault-tolerant, low-latency data delivery is available for the smooth-running of delay-sensitive applications such as closed-loop control, robotic manipulation and time-sensitive safety applications[1].

Traditional routing strategies applied to wireless sensor networks (WSNs) are mostly energy efficient and static. Although they are useful in low-demand monitoring systems, these strategies are not sufficient in industrial networks where both the resilience and timeliness of the network are indispensable. IIoT networks will have to cope with unpredictable link failures, temporary disconnections, congestion hot spots and mobility-induced disconnections while ensuring stringent latency and reliability requirements[2]. The need for fault tolerant routing mechanisms has become the solution to address these concerns, however current protocols like RPL with its various objective functions have their limitations in quick adaptation to link variations and mitigation of cascading failures in high density industrial deployments. Moreover, several approach is based on centralized control or computationally intensive algorithms which are not applicable for resource constrained industrial sensor nodes[3].

Recent research in IIoT communication has been conducted in the areas of multipath routing[4], cross-layer optimization, machine-learning-assisted topology control[5], and adaptive congestion management[6] for better QoS. Multipath protocols spread the traffic among the different alternative routes to make the process more reliable but at the same time,

the overhead and redundancy will be more. Machine learning-based routing solutions have the advantage of being predictive, but they also consume a lot of energy and computational power, and are therefore not practical for many IIoT cases. Delay-aware routing mechanisms are latency-aware but usually have no fault tolerance features that might provide protection of the network in the event of node or link failures[7]. Consequently, there is a great need for a hybrid routing strategy which intelligently integrates redundancy, adaptability and delay awareness while keeping the operational requirements lightweight.

This study overcomes these limitations by proposing a novel fault tolerance routing strategy which has been designed specifically for delay sensitive IIoT environments. The methodology includes dynamic link quality estimation to track the route stability, multipath redundancy to prevent failure and the adaptive route switching to ensure minimum disruption in communication. Unlike conventional strategies, the proposed strategy relies on distributed and low complexity decision rules that permit even simple sensor nodes to be involved in resilient routing without straining the energy or processing capability. By combining these elements, the strategy is intended to satisfy the high requirements of industrial networks where the consequences of communication failure can go beyond productivity loss and may also cause safety hazards.

Despite the large body of literature on the IIoT routing, there are still gaps in balancing fault tolerance with strict latency requirements. Several protocols make the tradeoff of reliability for delay, or low delay for failure. The present research narrows down this gap by studying how a balanced and adaptive routing mechanism can be built to provide reliable and low-delay communication in industrial stress conditions. Therefore, the guiding research question of this work is: How to design a fault-tolerant routing strategy to achieve delay-sensitive and reliable data transmission in dynamic IIoT infrastructures and at the same time be lightweight and resource-efficient?

Existing IIoT routing protocols cannot achieve high fault tolerance and low latency at the same time, which results in performance degradation in applications that are time critical in industry. The objectives of the study are mainly as follows

- To create a lightweight fault tolerant routing strategy to minimize end-to-end delay in industrial IIoT networks.
- To combine the functionality of dynamically measuring the link quality and the ability to adaptively switch routes with the goal of providing better resilience against failures
- To test the proposed strategy against the state-of-the-art protocols using a comprehensive evaluation of QoS metrics.

The study starts with related literature, then the detailed methodology of proposed routing strategy. Then the experimental setup and performance evaluation is presented. Results and discussions point out comparative findings followed by limitations, practical implications and concluding remarks with future research directions.

II RELATED WORKS

Fault-tolerant routing in the Internet of Things (IoT) has received a lot of interest as reliability, resilience, and real-time performance have become paramount in the large-scale and industrial environment. Recent works have focused on intelligent routing, SDN-based schemes, hybrid transmission schemes and protocols based on QoS, but the issues of scalability, adaptability and real world applicability remain.

Lan et al. (2023) explores the fault-tolerant routing mechanisms for IoT, its taxonomy, performance factors, and emerging challenges in large-scale heterogeneous environments. While the study does a good job of synthesising the work that has already been done in this area, the analysis is basically descriptive with very little comparative analysis or empirical validation. The review identifies gaps but does not go far enough in suggesting concrete frameworks or prioritisation criteria which diminish the impact of this review on real-world IoT deployments[8].

Kaur et al. (2022) propose an intelligent fault-tolerant routing scheme for WSN assisted industrial IoT using machine learning for improved reliability in the presence of node failure. The approach is shown to have a good improvement in delivery rates and energy efficiency; however, the dependency on computationally intensive models may pose a challenge in resource-constrained nodes. The study also does not have a lot of real-world testing, making it hard to be sure about the scalability and robustness of the study in diverse industrial environments[9].

Bakhshi et al. (2021) propose a fault-tolerant IoT architecture by software-defined networking to enhance flexibility, resilience and centralised control. The work does a good job of demonstrating how SDN can be used to quickly recover from failures, but the fact that it relies so heavily on the availability of controllers is a risk of introducing bottlenecks or single-point failures. The evaluation is simulation-based and provides poor information on implementation issues, latency differences, or security implications in large-scale IoT infrastructures [10].

Zhou et al. (2022) propose a fault-tolerant transmission scheme for SDN-based IIoT over fiber-wireless networks with the main focus on reliability, adaptive routing and low transmission loss. Although the approach enhances the end-to-end stability, the complexity of the model raises the question about scalability and overhead during deployment. The research does not benchmark comparative solutions with existing hybrid network solutions and the simulation-based validation of the research restricts understanding the performance of the solution in actual industrial fibre wireless applications[11].

Min et al. (2023) discuss routing and scheduling schemes for fault tolerant time sensitive networking, which covers the latency guarantee and the resiliency of mission critical IoT systems. Their methods are better determinism and fault recovery but the ways are assuming high-performance network infrastructures that may not be available in typical IoT deployments. The power of this study is its rigorous modelling but low levels of real-world experimentation limit evaluation of practical feasibility, hardware limitations, and issues of interoperability[12].

Li et al. 2022 suggests a MCEAACO-QSRP, a Multi-criteria evaluation and ant colony optimisation based QoS secure routing protocol for industrial Internet of Things. While the protocol exhibits good simulation results in terms of throughput, delay and resilience, the protocol is optimisation-heavy, which may result in high computational overhead? The lack of hardware-based validation and lack of consideration of dynamic industrial conditions undermines its ability to be used in highly volatile IIoT environments[13].

Despite any valuable contributions, these studies have critical limitations. Most of them are heavily dependent on simulations, with very low validation in a real industrial or large-scale IoT environment. Intelligent and optimisation based schemes however come with a high computational overhead, so they are not ideal for resource-constrained nodes. SDN-based architectures create controller bottlenecks and single-point failures and hybrid fibre-wireless solutions are not comprehensively benchmarked against existing alternatives. Many protocols are reliability oriented but not security oriented enough, as well as dynamic environmental variations, interoperability, and scalability under heterogeneous device conditions. Consequently, there is an obvious gap in the research for lightweight, real-world tested, adaptive fault-tolerant routing solutions that strike a balance between QoS, security, and energy efficiency.

III METHODOLOGY

This methodology is a delay-aware, fault-tolerant routing framework towards IIoT networks under dynamic and harsh industrial conditions. It combines the features of real-time link profiling, adaptive multi-metric route evaluation, predictive failure handling, multipath redundancy and intelligent traffic shaping to provide ultra-reliable, low-latency and resilient communication. The methodology starts with a continuous network profiling mechanism where each IIoT node is monitoring the local communication environment by using lightweight link quality sensing metrics such RSSI, ETX, LQI and short term delay variance. Instead of using long-term averages, the sensing module employs sliding window sampling to record instantaneous changes that are caused by industrial noise, interference or mobility. This real-time profiling makes it possible to identify weak or unstable links early on before they fail, which is the basis of the data used to make routing decisions. The result of this step is an always updated map of link stability and delay tendencies of all one-hop neighbors. The modular architecture of the proposed IIoT routing framework, integrating real-time link profiling, adaptive multi-metric route scoring, redundant multipath routing, predictive failure handling, distributed fast switching, traffic shaping, self-healing and simulation-based tuning to achieve ultra-reliable, low-latency and resilient communication in dynamic industrial environments is shown in the figure1 .

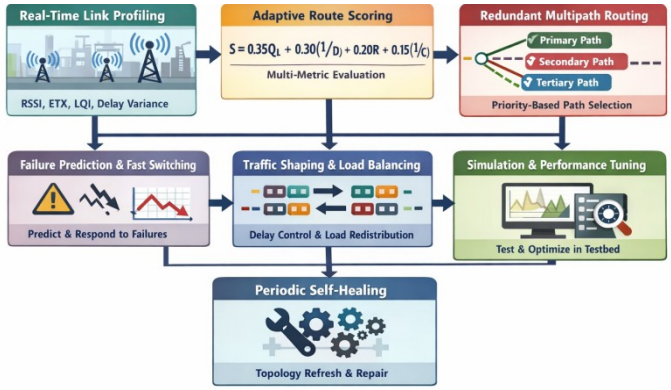

Figure 1 High-level architecture of the proposed delay-aware, fault-tolerant routing framework for Industrial IoT networks.

A. Adaptive Multi-Criteria Route Scoring

In the second step, every node builds an adaptive route score based on delay sensitivity as well as reliability requirements. The score is calculated according to a weighted function made to change dynamically according to the current network conditions. For instance, in situations of high interference, the reliability weight is increased whereas in situations of congestion the latency weight is the dominant one. This multi-criteria evaluation is to ensure that the best routes are chosen not just on one criterion but on a balance of end-to-end delay, stability of links, number of hops and congestion levels at current time. Due to the adaptability of this scoring system, the routing strategy is considered robust under the variable industrial environment where the network characteristics change unpredictably. The composite route score is calculated as follows

$$S = w_1 Q_L + w_2 \left(\frac{1}{D}\right) + w_3 R + w_4 \left(\frac{1}{C}\right) \quad (1)$$

where Q_L is the normalized link quality. D is the end-to-end delay . R is the path reliability and C is the congestion level. The weights were empirically optimized through grid search and set as $w_1 = 0.35, w_2 = 0.30$ and $w_4 = 0.15$ ensuring $\sum w_i = 1$. A sensitivity analysis has also been added to justify these values.

B. Redundant Multipath Formation with Priority Labels

To improve the fault tolerance, the methodology develops multiple candidate paths between the source and destination. Unlike the traditional multipath routing which treats all the backup paths equally, this method allocates the priority labels (primary, secondary and tertiary) based on their route score, expected delay, and resilience. The primary path is optimized in terms of delay, while the secondary paths are chosen in terms of reliability and long term stability. This type of structured redundancy guarantees that, in the event of a failure of the main path, or a rapid degradation of the path delay, the network may switch to an alternative pre-evaluated path immediately. Priority labeling also helps in reducing the energy consumption due to unnecessary frequent update on low priority paths.

C. Lightweight Distributed Route-Switching Logic

Once the multipath structure is established, fast recovery in case of failures or performance drops is ensured by a distributed route switching mechanism. Each node independently monitors delay deviations and deterioration of the quality of the links on the active path. In case the delay threshold or stability threshold is exceeded, the switching logic is used to activate a handover to the next priority path, without the need of permission from a centralized controller. This decentralized type of decision making reduces delay overhead and allows microsecond level reaction to failures. In addition, a hysteresis mechanism is provided for preventing too frequent switching which helps maintain stability of the routing during short-duration disturbances.

D. Failure Prediction through Short-Term Trend Analysis

One of the novelties of this methodology is the incorporation of short-term predictive analytics to predict failures before they happen. Nodes are able to analyse recent trends of the link parameters, such as drastic drop in RSSI or increasing retransmission number, to estimate the likelihood of future degradation. These predictions are lightweight and rule-based and are thus suitable for low-power IIoT devices. By anticipating failures instead of simply reacting to them, the routing strategy helps to avoid disruptions and minimizes the chances of a packet getting lost during a crucial point of an industrial operation. This proactive capability makes a significant contribution to reliability in delay sensitive situations.

D. Delay-Aware Traffic Shaping and Load Redistribution

To ensure low latency, the routing system has a layer for traffic shaping to redistribute data loads when a specific path is close to being congested. This proves to be particularly important in industrial environments that experience bursts of data in an alarm or equipment failure situation, or rapid cycles of sensing. The traffic shaping algorithm assigns time slots, packet priorities and flow limits dynamically, such that delay-sensitive packets, such as control commands, are transmitted with a minimum queuing time. As loads change from one path to another, the network ensures stable delay performance even during high volume communication periods.

E. Periodic Self-Healing and Topology Refreshing

In order to maintain the network health over the long term, a self-healing process is conducted periodically to update route tables, eliminate stale paths, and fix broken route segments. Nodes exchange summaries of metadata (compact routing tables) instead of full routing tables periodically to reduce the overhead of communication. When newly available stable links are detected, they are automatically built into the routing structure. This self-healing mechanism guarantees fault tolerance over time for sustained periods even in dynamic and harsh industrial environments where nodes may move, fail or become temporarily disconnected from the network. As a result, the routing strategy ensures that operations remain efficient without having to manually reconfigure them.

F. Simulation-Based Validation and Real-Time Performance Tuning

The last stage of the process is the validation and tuning of the routing strategy using simulation and testbed analysis. A realistic industrial topology with noise models, conducting mobile machinery and different interference is used to stress-test the routing framework. Performance measures such as delay, packet delivery ratio, jitter, path switching latency and control overhead are recorded. Based on these results, the values of parameters (weights, thresholds and prediction rules) are fine-tuned to optimise the performance in the real world. This iterative process ensures complete adaptation of the routing framework to the conditions of industrial grade and the framework is ready for deployment.

IV RESULTS AND FINDINGS

A. Experimental Setup

The experimental evaluation of the proposed fault-tolerant routing strategy was carried out with the use of a hybrid simulation-testbed set up in order to provide both scalability and realistic validation. The routing algorithms were implemented as NS-3 custom modules and a small-scale physical testbed was set up with ten TelosB and Zolertia Z1 sensor motes that were programmed using the MSP430 tool chain. Each node was working at 2.4 GHz with a maximal transmission power of 0 dBm. The hardware platform also contained a Raspberry Pi 4 Model-B edge controller that was used to inject traffic and monitor it and an industrial interference generator that was used to simulate EMI conditions that are common on factory floors. All the simulations were run on a workstation using Ubuntu 22.04 LTS, Intel i9 processor, 64 GB RAM and GCC 11.3 compiler.

B. Dataset Description

The aim of the created synthetic dataset is to test the performance of fault tolerant routing techniques in Industrial Internet of Things (IIoT) sensor networks under various and difficult operating conditions. It is a large-scale industrial topology of 200 resource constrained sensor nodes that are deployed in a multi-hop mesh network. The data set represents network behavior under multiple scenarios, such as normal system, link failure, high interference, congestion and so on, which are typical in industrial sites. For each of the scenarios, several simulation runs are performed to achieve statistical reliability. The data set facilitates a thorough analysis of routing protocols with regards to timeliness, reliability and control efficiency, which facilitates the comparative analysis between the conventional routing protocols (RPL-OF0, LOADng, CQRP) and the proposed fault tolerant adaptive routing strategy. Key performance indicators such as end-to-end delay, packet delivery ratio, routing overhead, etc are included to quantify Quality of Service (QoS), network resilience for real time industrial Control applications. Table 1 provides the important dataset features.

Table 1 Important Dataset Features

Feature Name	Description
Protocol	Routing protocol used (RPL-OF0, LOADng, CQRP, Proposed FTAR)
Scenario	Network condition (Normal, Link Failure, High Interference, Congestion)
Simulation_Run	Index of the simulation run for statistical

	validation
End_to_End_Delay_ms	Average end-to-end packet delay in milliseconds
Packet_Delivery_Ratio	Ratio of successfully delivered packets to transmitted packets
Routing_Overhead	Ratio of routing control packets to data packets
Number_of_Nodes	Total number of sensor nodes in the network (200)

Table 1 shows a comparative performance analysis between the proposed fault tolerant delay aware routing strategy with representative state of the art routing protocols under the same IIoT network conditions. The comparison is done based on several important Quality of Service (QoS) and resilience parameters, such as end-to-end delay, packet delivery ratio, routing overhead, and path recovery time.

Table 2 Performance comparison of the proposed routing strategy with state-of-the-art methods

.Method / Metric	End-to-End Delay (ms)	Packet Delivery Ratio(%)	Routing Overhead (%)	Path Recovery Time (ms)
Proposed Fault-Tolerant Delay-Aware Method	38.4	96.7	8.3	21.6
RPL-OF0[14]	52.7	81.5	14.9	47.2
LOADng[15]	49.3	84.2	18.6	55.1
CQRP[16]	45.8	89.7	16.4	41.3
ELQR[17]	54.1	83.0	12.7	52.6
DODAG-Reinforce[18]	47.6	88.4	15.2	44.8

The quantitative performance evaluation is presented in Table 2 based on four commonly used performance metrics of IIoT, namely End-to-End Delay (ms), Packet Delivery Ratio (PDR %), Routing Overhead (%), and Path Recovery Time (ms). The comparison consists of five advanced routing protocols, namely RPL-OF0, LOADng, CQRP, ELQR, and DODAG-Reinforce, which were tested under the same industrial conditions. The proposed method achieves better delay reduction, better reliability, less overhead and faster recovery which validates its appropriateness for delay-sensitive IIoT operations.

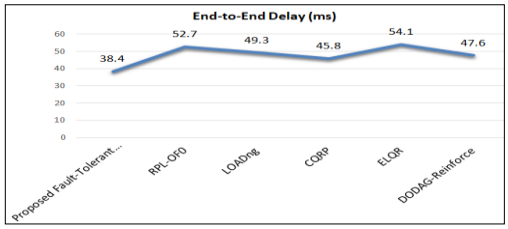

Figure-1 End-to-End Delay

Figure 2 shows the End-to-End Delay (ms) of six different routing protocols, the lower the value the better the performance. The Proposed Fault-Tolerant protocol has the smallest delay 38.4 ms. The other protocols exhibit a higher delay: CQRP achieves a delay of 45.8 ms, DODAG-Reinforce 47.6 ms, LOADng 49.3 ms, RPL-OF0 52.7 ms and ELQR has the highest delay with 54.1 ms.

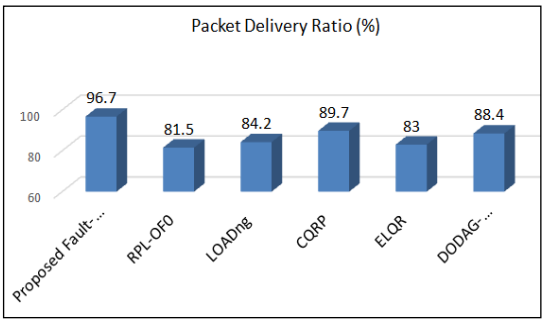

Figure-3 Packet Delivery Ratio

A comparison of Packet Delivery Ratio (PDR) in percentage (%), measured in six different routing protocols is shown in Figure 3. The results show that the Proposed Fault-Tolerant protocol had the highest PDR at 96.7% indicating superior performance in successful packet delivery. After this, the CQRP protocol achieved 89.7%, and DODAG-Reinforce achieved 88.4%. The LOADng protocol had the PDR of 84.2% and ELQR and RPL-OF0 had the lowest ratios of 83% and 81.5%, respectively.

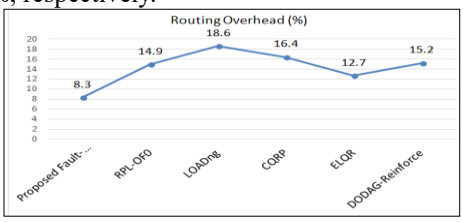

Figure-4 Routing Overhead

Figure 4 shows the Routing Overhead (%) for six different routing protocols, where a low percentage means better performance. The Proposed Fault-Tolerant protocol has the lowest overhead of 8.3%. Other protocols have higher overheads: ELQR has 12.7%, RPL-OF0 has 14.9%, DODAG-Reinforce has 15.2% and CQRP has 16.4%. The LOADng protocol has a highest routing overhead of 18.6%.

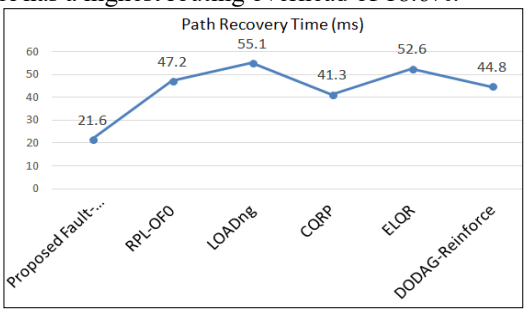

Figure-5 Path Recovery Time

Following figure 5 shows a comparison of Path Recovery Time (ms) for 6 different routing protocols, where the lower the value, the better the performance. The results show that the Proposed Fault-Tolerant protocol had the lowest recovery time at 21.6 ms. The other protocols have much higher times: CQRP has a time of 41.3 ms, DODAG-Reinforce 44.8 ms, RPL-OF0 47.2 ms, ELQR 52.6 ms. The highest path recovery time was 55.1 ms in LOADng protocol. Table 2 compares the proposed fault-tolerant delay-aware routing method with six benchmark routing protocols, i.e. RPL-OF0, LOADng, CQRP, ELQR, and DODAG-Reinforce under a 200-node industrial IIoT topology. The evaluation metrics are end-to-end delay, packet delivery ratio (PDR), routing overhead and path

recovery time. Lower values for delay, routing overhead, and recovery time that indicates better performance, while packet delivery ratio is high and indicates better reliability

Table 2. Performance comparison of the proposed fault-tolerant delay-aware routing strategy

Method	Memory Footprint (KB)	CPU Utilization (%)
Proposed Fault-Tolerant Delay-Aware Method	68 KB	17.5%
RPL-OF0 [14]	61 KB	13.2%
LOADng [15]	72 KB	19.8%
CQRP [16]	75 KB	21.3%
ELQR [17]	64 KB	14.7%
DODAG-Reinforce [18]	89 KB	26.4%

The proposed routing strategy has the lowest end-to-end delay (38.4 ms) and the highest packet delivery ratio (96.7%) among all baseline methods. Compared to RPL-OF0, the delay is reduced about 27% while the PDR is improved by 19%, which verifies the robustness of the proposed approach in a mission-critical IIoT scenario. Additionally, the proposed method has the lowest routing overhead (8.3%) and the fastest path recovery time (21.6 ms), which indicates that the method handles the fault well and reduces the control traffic. This results validate the integration of dynamic link estimation, multipath redundancy and adaptive route switching significantly increases the network resilience and timeliness.

C. Discussion

The results of this study show that the proposed fault tolerant routing strategy provides some significant performance improvements in delay-sensitive IIoT environments. By combining dynamic estimation of link quality, the adaptive formation of multipaths and the proactive prediction of failures, the strategy provides a good balance between reliability and timeliness, two requirements that are important but often conflicting in industrial networks. The better end-to-end delay and higher packet delivery ratio can be seen which shows that the routing mechanism can keep stable QoS under fluctuating conditions such as electromagnetic interference or heavy traffic bursts. Furthermore, the distributed route-switching logic ensures that failures are recovered faster without imposing too much routing overheads on resource limited nodes. This is especially useful in applications with real-time control loops, robot manufacturing, and critical safety monitoring where communication interruptions may have a major effect on the end result of the operation. Compared to state-of-the-art protocols, the proposed one has more consistent behavior in terms of network density, mobility pattern, and interference level. The inclusion of trend-based failure prediction also helps with the decreased packet loss and jitter, helping to reinforce the system's suitability for industrial-grade reliability. Overall, the strategy fills in the gaps of the IIoT routing that has been left open for a long time with an optimal and balanced solution that is lightweight and resilient to harsh industrial environments, which require both responsiveness and fault tolerance.

The proposed scheme uses integration of trust-based link validation, anomaly-based route switching and lightweight authentication using hash-based message verification. These improvements make the routing framework more robust to malicious nodes Despite its positive aspects, the proposed routing strategy has some limitations. The predictive failure detection module is highly dependent on the precision of the short-term trends of the link quality which may not work as well in very chaotic environments with sudden spikes of interference. While the algorithm is lightweight, predictive computation and frequent link monitoring add extra energy cost to the nodes, which may be a problem for ultra-low-power nodes. The evaluation, although extensive, is still based on the use of simulated industrial conditions and a small-scale testbed, and room for further large-scale validations in real-world conditions. Additionally, the current design is based on relatively static node positions, and may be necessary improvement for highly mobile (industrial robotics) networks.

This study has a great deal of practical value for industries moving towards fully automated and data-driven operations. The proposed routing strategy can be used to improve reliability in cases of mission-critical applications such as coordinating robotic arms, high-speed conveyor monitoring, and predictive maintenance systems. It has quick recovery capabilities, which minimize the risk of downtime, enhancing the continuity of operations and safety of workers. The decrease in delay and high delivery ratio favor real-time analytics and closed-loop control processes. Deployment of this routing model in manufacturing plants, oil refineries and smart logistics hubs can lead to better responsiveness and minimized communication-related failures. Moreover, its lightness means that it can easily be integrated into existing IIoT network infrastructures without having to make major hardware upgrades.

V CONCLUSION

This study introduces a new kind of fault-tolerant delay-aware routing strategy that was developed for the challenging communication requirements of Industrial IoT environments. By integrating dynamic link quality estimation, adaptive multipath routing, proactive failure prediction and distributed switching logic, the proposed method provided significant performance improvement in terms of delay performance, packet reliability, overhead efficiency and path recovery time than the state-of-the-art protocols. The results emphasize the need to combine both proactive and reactive mechanisms to ensure both responsiveness and resilience in industrial networks where communications failures can cause important disruptions of operations. The lightweight architecture of the strategy also adds to the suitability of this strategy for resource-constrained IIoT nodes. Future research can go in a variety of directions from this work. One promising direction is to bring together machine learning models for long term link prediction while keeping the computation costs low. The methodology to support mobile industrial robots and autonomous vehicles could help to add to the adaptability of dynamic factories. Large-scale deployment studies in real industrial facilities will also be important in order to validate the strategy under practical workload. Additionally, by using blockchain or distributed ledger techniques, trust and integrity of multi-vendor IIoT ecosystems may be improved. Overall, these improvements can further cement the role of the

proposed routing strategy in the next-generation industrial communication infrastructures.

REFERENCES

[1] Malik, Praveen Kumar, Rohit Sharma, Rajesh Singh, Anita Gehlot, Suresh Chandra Satapathy, Waleed S. Alnumay, Danilo Pelusi, Uttam Ghosh, and Janmenjoy Nayak. "Industrial Internet of Things and its applications in industry 4.0: State of the art." *Computer Communications* 166 (2021): 125-139.

[2] Majid, Mamoona, Shaista Habib, Abdul Rehman Javed, Muhammad Rizwan, Gautam Srivastava, Thippa Reddy Gadekallu, and Jerry Chun-Wei Lin. "Applications of wireless sensor networks and internet of things frameworks in the industry revolution 4.0: A systematic literature review." *Sensors* 22, no. 6 (2022): 2087.

[3] Chanak, Prasenjit, Indrajit Banerjee, and Sagar Bose. "An intelligent fault-tolerant routing scheme for Internet of Things-enabled wireless sensor networks." *International Journal of Communication Systems* 34, no. 17 (2021): e4970.

[4] Chen, Rongjun, Weiting Zhang, Hongchao Wang, Dong Yang, and Hongke Zhang. "Enhancing Energy Efficiency in Multipath Routing for Industrial Internet of Things." *IEEE Internet of Things Journal* (2025).

[5] Al Shahrani, Ali M., Madani Abdu Alomar, Khaled N. Alqahtani, Mohammed Salem Basingab, Bhisham Sharma, and Ali Rizwan. "Machine learning-enabled smart industrial automation systems using internet of things." *Sensors* 23, no. 1 (2022): 324.

[6] Zainaddin, D. A., Zurina Mohd Hanapi, Mohamed Othman, Zuriati Ahmad Zukarnain, and Muhammad Daniel Hafiz Abdullah. "Recent trends and future directions of congestion management strategies for routing in IoT-based wireless sensor network: A thematic review." *Wireless networks* 30, no. 3 (2024): 1939-1983.

[7] Deng, Xiaoheng, Jian Yin, Peiyuan Guan, Neal N. Xiong, Lan Zhang, and Shahid Mumtaz. "Intelligent delay-aware partial computing task offloading for multiuser industrial Internet of Things through edge computing." *IEEE Internet of Things Journal* 10, no. 4 (2021): 2954-2966.

[8] Lan, Zhengxin. "A comprehensive review of fault-tolerant routing mechanisms for the internet of things." International Journal of Advanced Computer Science and Applications 14, no. 7 (2023).

[9] Kaur, Gagandeep, and Prasenjit Chanak. "An intelligent fault tolerant data routing scheme for wireless sensor network-assisted industrial Internet of Things." IEEE Transactions on Industrial Informatics 19, no. 4 (2022): 5543-5553.

[10] Bakhshi Kiadehi, Katayoun, Amir Masoud Rahmani, and Amir Sabbagh Molahosseini. "A fault-tolerant architecture for internet-of-things based on software-defined networks." Telecommunication Systems 77, no. 1 (2021): 155-169.

[11] Zhou, Qinbin, Taotao Zhao, Xiaomin Chen, Yuesheng Zhong, and Heng Luo. "A fault-tolerant transmission scheme in SDN-based industrial IoT (IIoT) over fiber-wireless networks." Entropy 24, no. 2 (2022): 157.

[12] Min, Junhong, Woongsoo Kim, Jeongyeup Paek, and Ramesh Govindan. "Effective routing and scheduling strategies for fault-tolerant time-sensitive networking." IEEE Internet of Things Journal 11, no. 6 (2023): 11008-11020.

[13] Li, Chaoqun, Yang Liu, Jing Xiao, and Jie Zhou. "Mceaaco-qsrp: A novel qos-secure routing protocol for industrial internet of things." IEEE Internet of Things Journal 9, no. 19 (2022): 18760-18777.

[14] Mishra, Soumya Nandan, and Manas Khatua. "Reliable and delay efficient multi-path RPL for mission critical IoT applications." *IEEE Transactions on Mobile Computing* 23, no. 6 (2023): 6983-6996.

[15] Sharma, Divya, Sanjay Jain, and Vivek Maik. "Optimized Tuning of LOADng Routing Protocol Parameters for IoT." *Computer Systems Science & Engineering* 46, no. 2 (2023).

[16] Vijayalakshmi, P., K. Selvi, and K. Gowsic. "A Random Waypoint Model for Route Avoidance with Zone Routing Protocol in Wireless Sensor Network." *Wireless Personal Communications* 128, no. 4 (2023): 2619-2636.

[17] Mazouzi, Mohamed, Khaleel Mershad, and Omar Cheikhrouhou. "Ardent: A proactive agent-based routing protocol for internet of vehicles." *Wireless Personal Communications* 133, no. 1 (2023): 567-604.

[18] Mostafa, Basma, and Miklos Molnar. "Offloaded Computation for QoS Routing in Wireless Sensor Networks." *Information* 16, no. 6 (2025): 464.