Exploremetics
Journal of Innovative Engineering and Technology

Volume: 06 No: 01 | April -2025
ISSN (Online) 2636 – 590
ISSN (Print) 2636 - 591X

ENHANCEMENT OF INDUSTRIAL INTERNET OF THINGS (IOT) NETWORK QUALITY OF SERVICE USING MULTI-CHANNEL ROUTING ALGORITHM

Oluchi Lilian Enekwe[*1], James Eke[1]
1 Department of Electrical and Electronic Engineering, Enugu State University of Science and Technology
Author for correspondence: Enekwe O.L; **E-mail:** enekweliliano@gmail.com

Abstract -This study explores the development of a Multi-Channel Routing (MCR) algorithm for enhancing the Quality of Service (QoS) in Industrial Internet of Things (IIoT) networks. IIoT networks frequently encounter difficulties,including significant packet loss, high latency, and low throughput, which reduces their effectiveness in industrial settings. In order to ensure optimal channel use and congestion avoidance, the MCR algorithm was created to dynamically route packets using a shortest distance and cost-function method. Significant improvements were seen when network performance was compared with and without MCR. The average latency of the MCR-enabled IIoT network was 46.4 ms, which was 80.8% lower than the 243 ms of the baseline network. With MCR reporting 87.56% as opposed to 65.16% in the baseline network, throughput rose by 34.52%. Furthermore, the packet loss rate decreased from 4.55% to 0.87%, a decrease of 80.88%. These findings show that MCR efficiently improves network performance by facilitating quicker, more dependable data transfer. This study paves up opportunities for more investigation into MCR's scalability and integration with cutting-edge security protocols by demonstrating its potential as a strong remedy for QoS issues in IIoT systems.

Keywords: Multi-Channel Routing (MCR); Industrial Internet of Things (IIoT); Quality of Service (QoS); Network Performance; Latency

1. Introduction

The Industrial Internet of Things (IIoT) is a concept that refers to the integration of industrial processes with internet-connected devices and technologies (Brou and Janssen, 2015). It encompasses the use of sensors, data analytics, cloud computing, and machine learning to optimize and automate industrial operations. IIoT enables the collection and analysis of vast amounts of data from various sources within an industrial setting. This data can be used to improve efficiency, productivity, and safety in sectors such as manufacturing, energy, transportation, and agriculture (Onu et al., 2023).

According to Brou and Janssen (2015), one of the key advantages of IIoT is its ability to enable real-time monitoring and control of industrial processes. By connecting machines, equipment, and devices to a centralized system, operators can remotely assess performance, detect anomalies, and make timely adjustments to optimize operations (Ashish et al., 2017). IIoT also facilitates predictive maintenance, which helps to prevent equipment failures and minimize downtime. By analyzing data collected from sensors embedded in machinery, maintenance teams can identify potential issues before they occur, schedule repairs, and avoid costly breakdowns (Farooq et al., 2015). Furthermore, Mohit and Rakesh (2019) opined that IIoT plays a crucial role in enabling data-driven decision-making. By leveraging advanced analytics and machine learning algorithms, organizations can extract valuable

insights from the massive amount of data generated by IIoT devices (Mohamed et al., 2020). These insights can inform strategic planning, improve operational efficiency, and drive innovation (Oforji and Oju, 2018). However, the implementation of IIoT also presents challenges. Arakanksha (2016) and Gupta et al. (2010) revealed that security and privacy concerns are paramount, as the connectivity of industrial systems increases their vulnerability to cyber threats. Ensuring robust cybersecurity measures and data protection protocols is crucial to mitigating these risks.The quality of service in the industrial internet of things (IIoT) concept plays a crucial role in ensuring the efficient and reliable operation of industrial systems. The factors that determine the QoS in IIoT are reliability (Igbal et al., 2016;Ulagwu et al., 2021), security, scalability (Prasath et al., 2020), latency (Jamin et al., 2018), interoperability (Kizza, 2005), data integrity, and analytics (Mehryar et al., 2012). Overall, the quality of service in IIoT is crucial for ensuring reliable, secure, and efficient operations in industrial settings.

Today, the advancement in IIoT devices and the dynamic landscape of interconnectivity, coupled with the increased demand for real-time network security, optimal performance, and seamless maintenance through continuous network traffic analysis, has presented the need for Real-time Packet Inspection (RPI). According to Radu et al. (2017), RPI is a network surveillance approach that scans the network in real time to detect malicious activities tailored towards the confidentiality violation of the network. It is network data analysis approaches that delve deep into the packet features, and extract vital data from the application layer for analysis and detection of threats (Ghosh and Senthilrajan, 2019). This RPI is generally applied in the detection of multiple threat features, which include malware, Trojan, virus, phishing attack, and even expands to the detection of unauthorized transfer of sensitive data within a network.

Over the years, Machine learning (ML) has emerged as the dominant approach in solving various problems, such as pattern recognition, clustering, time series, and fitting tasks (Rishika et al., 2018). Its success can be attributed to the high success rate of its algorithms and their reliability when applied in real-world scenarios (Prasath et al., 2020). Notably, ML applications for addressing cyber threats have become a prevailing trend, with many algorithms employed for the classification and prediction of threats in IIoTs (Saravanan and Sujatha, 2018).

According to Rashid and Samir (2023), while many studies have focused on addressing QoS challenges on IIoT, a holistic approach has not been proposed that considers the generated QoS constraints collectively and addresses their impact on IIoT. For instance, (Teng, 2022; Tanh et al., 2021; Sun et al., 2021; Malik et al., 2022; Alosaimi and Almutairi, 2023) all addressed quality of service constraints in the IIoT, with a major focus on security, without considering other quality of service parameters. Similarly, (Xu et al., 2018; Jyotsna and Nand, 2022; Subramaniam et al., 2023; Mazhar et al., 2023), all address QoS challenges in IIoT but leave a critical gap in security. This is because, as these devices continue to interconnect and interact, they are also susceptible to cyber threats and attacks. To this end, this paper proposes a solution that addresses the issues of QoS in IIoT. This will be achieved by developing an optimized routing solution that improves real-time data transfer between process design components, and also a reliable security solution for real-time deep packet inspection on the network.Collectively, the integration of this proposed solution will ensure that, holistically, QoS is actualized in IIoT while maintaining the integrity and safety of critical operations.

2. Research Methodology

The research methodology used for the study is expert consultation and a simulation approach. The techniques used for the realization of the research aim begin with a quality-of-service assessment test on a case

study of IIoT. From the network, data was collected to identify the security vulnerability on the network and the need for optimal quality of service during routing. To address the vulnerability problem on the network, an adaptive routing algorithm was proposed to further enhance QoS performance on the network. The QoS model proposed was integrated into the IIoT system using MATLAB and then tested using simulation. The performance was evaluated and validated using the cross-validation technique, with comparative analysis performed considering the network operational results without the proposed model.

2.1Data Collection

Earlier, primary data collection was used for the characterization process. In this case of secondary data collection, the Edge-IIoT set Cyber Security Dataset of IoT and IIoT was collected from the Kaggle repository and utilized for the study. The data was collected considering network attributes such as time, device ID, latency, motor speed, throughput, packet loss, jitter, and pressure. The data description was reported in Table 1.

Table 1: Data Description

S/N	Field Name	Data Type	Unique Values	Field Description
1	SourceID	Double	29	Unique identifier for the source
2	SourceAddress	Categorical	69 unique	Address of the source
3	SourceType	Categorical	8 unique	Type of the source
4	SourceLocation	Categorical	18 unique	Location of the source
5	DestinationServiceAddress	Categorical	64 unique	Address of the service destination
6	DestinationServiceType	Categorical	8 unique	Type of the service destination
7	DestinationLocation	Categorical	18 unique	Location of the service destination
8	AccessedNodeAddress	Categorical	149 unique	Address of the node that accessed the data
9	AccessedNodeType	Categorical	12 unique	Type of the node that accessed the data
10	Operation	Categorical	5 unique	Operation performed on the data
11	Value	Double	Integer	Value of the data
12	Timestamp	Double	Integer	Timestamp of the data
13	Normality	Categorical	8 unique	Normality of the data
14	Attributes	Data description		Data type

2.2 Data Transformation

Data transformation is a process used in this work to modify the data features and create a new representation that is most suitable for identification by machine learning algorithms. The feature transformation algorithm adopted for the data is principal component analysis (PCA) (Navin et al., 2013). This PCA was applied to reduce the dimension of the dataset while retaining the quality of features using the steps in Algorithm 1:

2.3 Algorithm 1: Principal Component Analysis (PCA) Algorithm

1. Input: Dataset X
2. Output: Reduced-dimensional data Y
3. Input: X, a dataset or data points.
4. For each feature, subtract the mean and divide by the standard deviation
5. Calculate the covariance matrix, C, of the standardized data X.
6. Compute the eigenvalues (λ) and eigenvectors (v) of the covariance matrix C
7. Define the number of components to keep, k.
8. Select the first k eigenvalues and their corresponding eigenvectors.
9. Calculate the new data Y by multiplying X by the selected eigenvectors.
10. End

2.4 Artificial Neural Network

Artificial Neural Network (ANN) is the machine learning algorithm utilized for the modelling of the deep packet inspection model (Sochima et al., 2025). The ANN is a made of

neurons which have weight and bias functions (Kekong et al., 2019). These neurons are interconnected in layers to formulate the network of neurons which are trained to generate the model for the deep packet inspection. The architectural model of a neural network was presented as Figure 2;

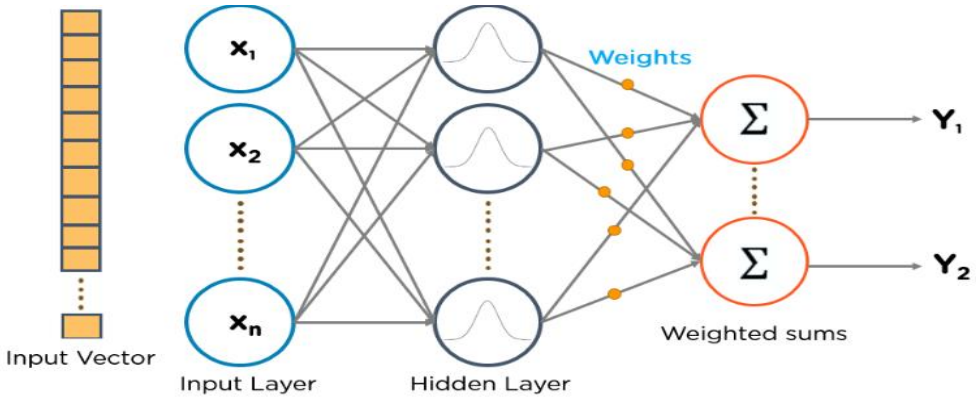

Figure 2: Architecture of Artificial Neural Network

Figure 2 presents the architecture of anartificial neural network, with the input vector, which is the input layer defined asX, while Xn is the number of vectors for the input, the interconnection of the neurons from the input layer forms the hidden layers, which are summed to produce the outputs Y. The ANN algorithm was utilized to train the neural network through the adjustment of hyperparameters of the neurons, such as momentum, learning rate, weight, and bias function (Haour et al., 2021). The algorithm, while adjusting these parameters in feed-forward propagation, monitors the gradient loss function of the neurons, and the back-propagation adjusts the hyperparameters until the neurons converge with a loss function value close to the set target value, which is usually approximately zero.

2.5 Training of the Neural Network

To train the neural network, the data was first imported into the network. This data was automatically split into training, test, and validation sets in the ratio of 70:15:15, and then the training set was used to train the neurons through the application of the back-propagation algorithm. While the algorithm adjusted the hyperparameters of the neurons, the regularization techniques applied dropout to ensure generalization of the model. This process continued iteratively until a loss function value of approximately zero was achieved. Other performance evaluation metrics, such as true positive, false positive, accuracy, positive prediction value, and false detection rate, are applied to analyze the model performance using the test and validation data samples, and then the results are all analyzed and reported in Chapter 4 of this work. At the end of the training process, a deep packet inspection model is generated.

2.6 Deep Packet Inspection (DPI) Model

The deep packet inspection model generated can detect features of normal packets from the plastic machine, as well as features of malware. When network data penetrates the access layer, the features of the packet are identified and transformed using the PCA algorithm. Then the deep packet inspection model classified the model into either Y_1 or Y2, as depicted in Figure 3. Where Y_1 is the output with threat features and Y_2 is the output without threat features. When threat features are classified as output from the network, they are immediately isolated from the transport layer through the access denial protocol.

3. Multi-Channel Routing For Enhanced Data Transfer

The Multi-Channel Routing (MCR) routing was proposed for optimal IIoT communication

to facilitate the transfer of information collected from the multiple sensor nodes to the server without issues of congestion. The MCR (Anguswamy et al., 2009; Hsu et al., 2022) is a smart routing technique formulated as an extension of weighted cumulative expected transmission time that considers the relationships between minimum hop counts and link quality for the routing of packets. MCR integrated end-to-end time of transmission and cost of switching for the path links by combining the average sum of transmission time from source to destination and then switching cost, while using a tunable parameter to influence the balance between the two factors. The MCR metrics for the computation of the overall cost of switching to a path are given as (Nji, 2008);

$$MCR = (1-\beta) * \sum_{i=1}^{n}\left(T_i + SC_{(ci)}\right) + \beta \max i \le j \le c Xj,\ 0 \le \beta \le 1 \quad (1)$$

Where β is a tunable parameter, n represents the number of hops on the path, T is the expected transmission time, and Xj represents the overall Ti cost on any jth channel within the available number of channels c. The probability $P_s(j)$ that the switchable interface will be a different channel (i, j) when a transmitted packet arrives on channel j is represented as;

$$P_s(j) = \sum_{\forall i 6=j}^{n} \text{InterfaceUsage}\ (i) \quad (2)$$

Where Interfaceusage (j) is the exponential weight of average channel j, which determines the time interval for switching when transmitting on channel j. The model in Equation 2 determined the probability of a switchable interface on diverse channels when a packet arrives. The switching cost j(SC(cj)) is given as;

$$SC(cj) = P_s(j) * \text{SwitchingDely} \quad (3)$$

Where the switching delay is the interface latency when a packet is transmitted on channel j. Overall, this MCR is a routing metric designed for multi-channel and channel-switchable wireless networks, proposing a metric that integrates end-to-end transmission time and switching costs for links over a path. The MCR metric, as defined by Equation 1, calculates the overall cost for a path by combining the weighted sum of T and switching costs, where a tunable parameter β influences the balance between the two factors. The probability of a switchable interface being on a different channel when a packet arrives (Ps(j)), computed through Equation 2, is crucial in determining the switching costs. The additional component in MCR, the Switching Cost (SC(cj)), is determined by multiplying Ps(j) with the switching delay (Equation 3). Notably, MCR offers an advantage by incorporating channel switching costs into routing metrics, allowing seamless integration with protocols like dynamic source routing and ad-hoc on-demand distance vector routing. The routing algorithm is presented as;

3.1 MCR routing algorithm for IIoT

1. Initialization
2. Set the tunable parameter β ($0 \le \beta \le 1$)
3. Apply Equation 1 for delay and switching cost for each channel
4. Determine the probability Ps(j) that a switchable interface will be on a different channel when a packet arrives on channel j using Equation 2
5. Compute the switching cost probability and delay of transmitted packet path using Equation 3.
6. Choose the path with the lowest cost# for the route of packet transmitted.
7. For packet transmitted from source =true
8. Switch interface to the same channel
9. End for
10. End

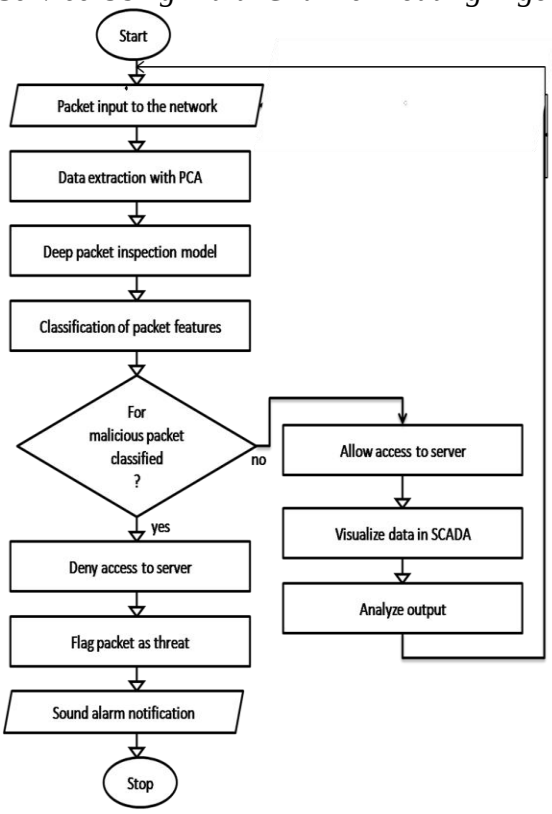

Figure 3: Flow chart of the DPI

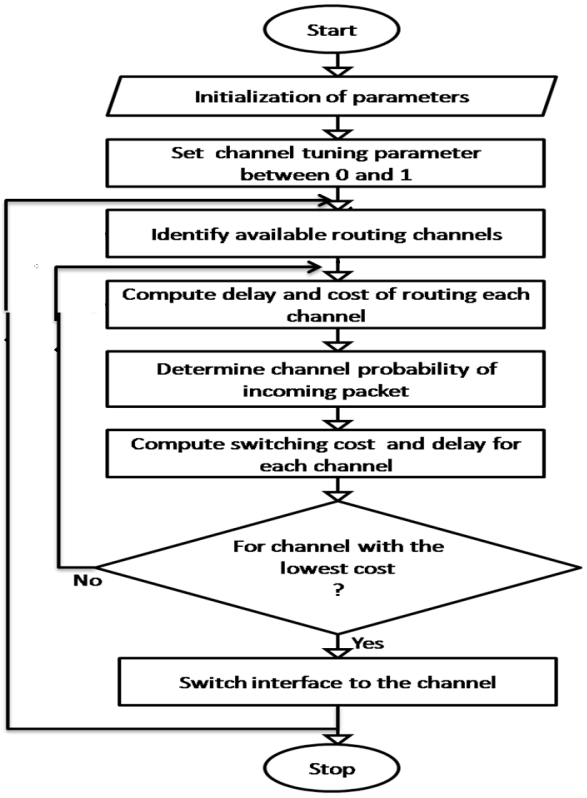

Figure 4: Flowchart of MCR Routing algorithm

The MCR flow chart in Figure 4 presents the operation of the routing algorithm. The channel tuning parameter's function β is set using values from 0 to 1. Then the entire routing paths within the network are identified and the cost of switching to each path and the overall end-to-end delay are determined using Equation 1. In addition, the probability that a transmitted packet is on a different path is computed, considering the average weighted sum of cost and delay in Equation 2. The path with the least cost and delay is then selected and switched to for the packet transmission process, and then the process continues in the same cycle.

4. System Implementation

The system implementation of the IIoT network with MCR involves setting up a simulation model that replicates real-world IIoT environments. In MATLAB, this canbe achieved by creating a network topology where devices such as sensors, controllers, gateways, actuators, and servers are represented as nodes, and communication links between them as edges. These edges are assigned weights that signify various network metrics such as bandwidth, latency, and signal quality across different channels. The simulation uses MATLAB graph function to create this topology in Figure 5, and packet routing is managed by dynamically choosing paths based on the channel's characteristics, optimizing for low latency or high throughput depending on the traffic requirements.

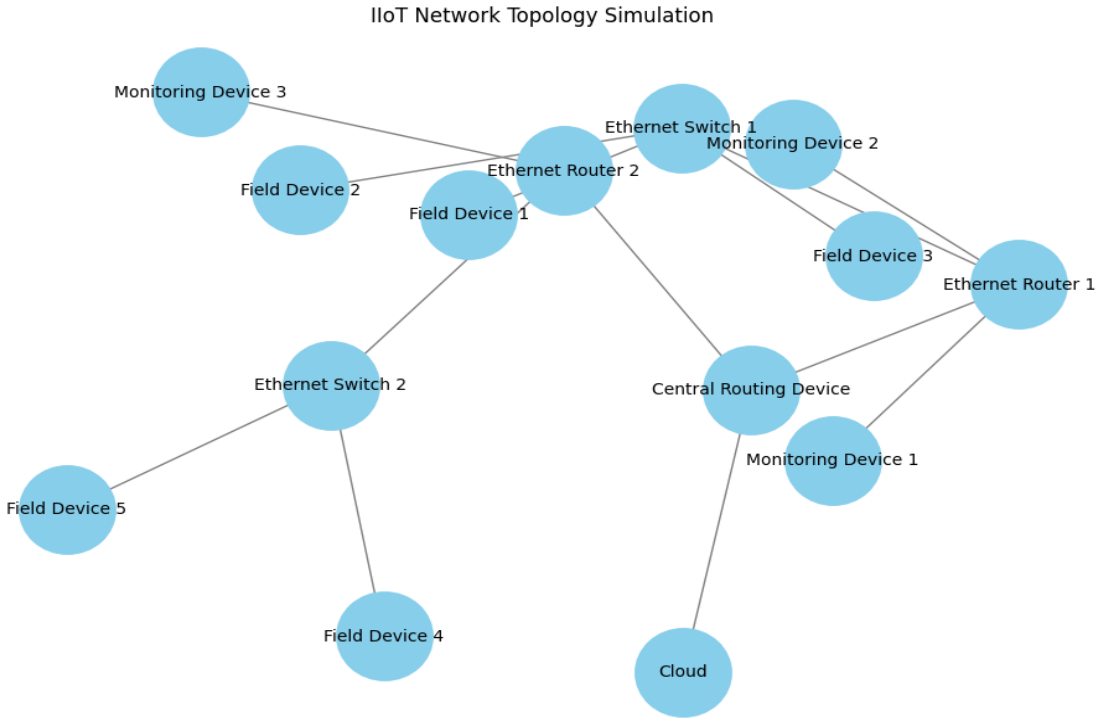

Figure 5: IIoT Network topology with Multi-Channel Routing

Figure 5 presents the IIOT Network Topology Simulation. This system connects various industrial devices such as field devices, monitoring devices, Ethernet routers, and switches. At the heart of the network is the Central Routing device, which manages the flow of data between connected devices. Field devices (such as sensors or actuators) are responsible for gathering data in real-time, often related to environmental or process conditions in an industrial setting. This data is sent through Ethernet routers and Ethernet switches, which manage communication and direct the flow of information. These routers and switches connect different parts of the network, ensuring that data reaches the intended destination, whether it be another field device, a monitoring device, or the cloud. Monitoring devices are critical for observing performance, and they rely on data from the field devices to track changes or detect anomalies.

5. Result of Simulation

Multi-Channel Routing (MCR) is about finding the best way to send data packets through the IIOT network with multiple paths. First, a set parameter β to balance factors like speed and reliability is specified. Then, the time it takes and the cost of changing channels for each path are computed with Equation 1. Next, the probability that a switchable interface will be on a different channel when a packet arrives is determined, aiding in the decision-making process. Subsequently, the switching cost probability and delay of the transmitted packet path are computed, considering Equation 3. The path with the lowest overall cost is selected as the route for the packet transmission. If the packet is transmitted from the source, the interface is switched to the same channel. This process iterates until all packets have been transmitted, optimizing the routing process for efficiency and performance. To visualize the impact of this MCR routing on the IIOT network, Figures 6 and 7 present the routed packet by two separate Ethernet devices from two separate network control systems.

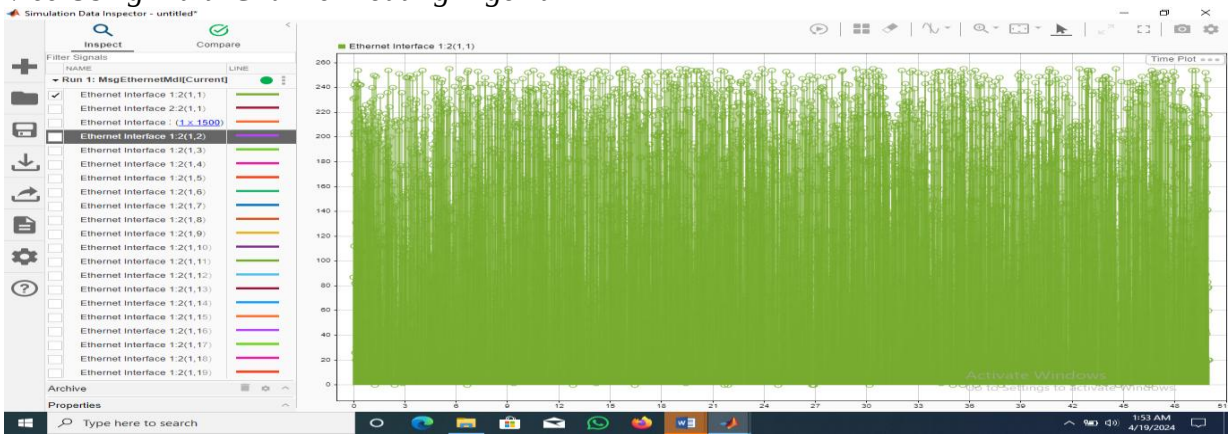

Figure 6: Routed Packet from Network 1

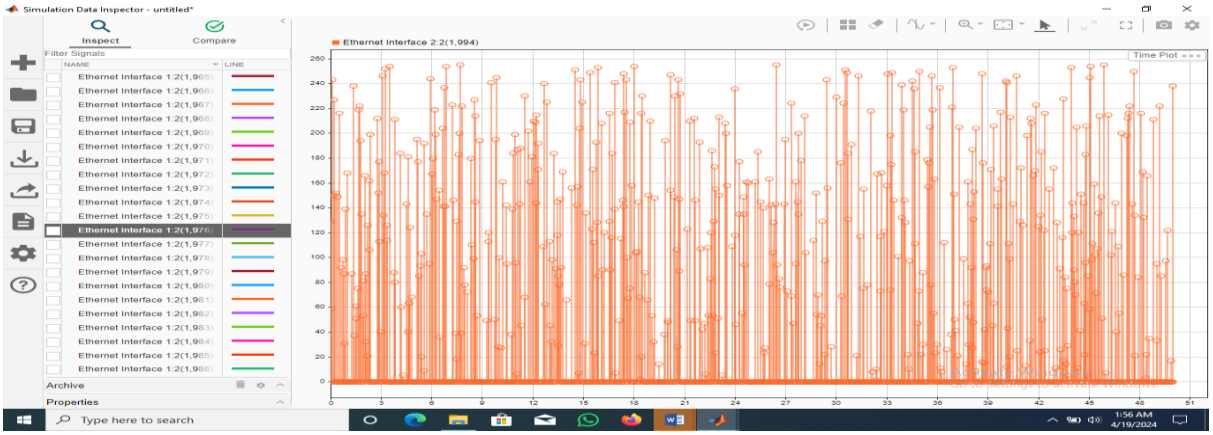

Figure 7: Routed Packet from Network 2

Figures 6 and 7 present the generated packet from the physical layer devices, such as the temperature sensor, pressure sensor, and level sensor, all transmitting signals to the programming logic controller via the Ethernet switch connected to the routing device. The router utilized the MCR to route the packet across channels with the lowest cost function and shortest path. Figure 8 presents the routed packets from the various network control systems along with the distributed routing device simulated with MCR.

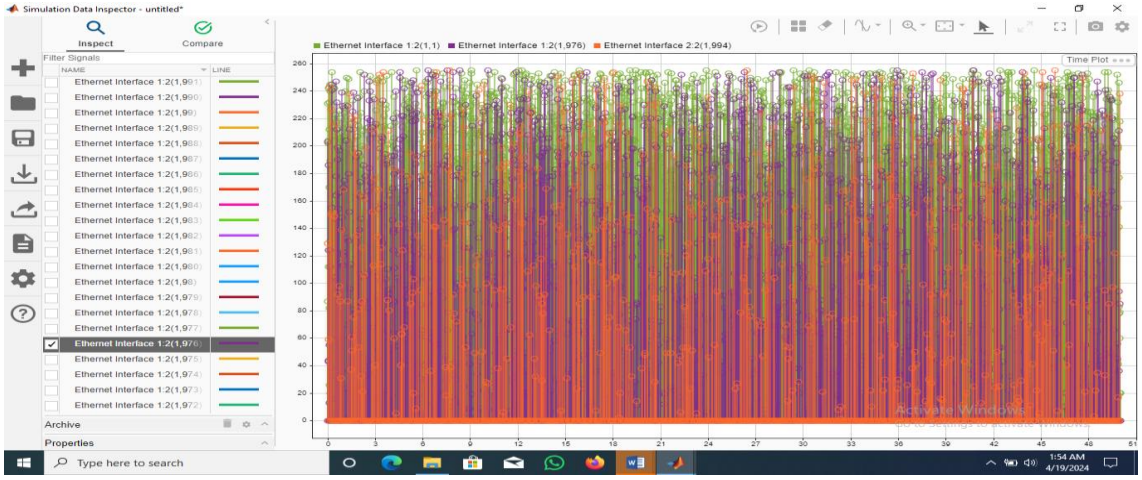

Figure 8: Result of routed packet from the three industrial network control systems

Figure 8 presents the routed packets from the three industrial network control systems. These packets generated from the respective network field devices are transmitted by the routing device on the network communication bus. During the process, the MCR was used to optimize the data transfer by selecting the optimal path, thereby managing the channel utilization factor, as packets are speedily transferred over the network channels. Figure 9 presents the result of the channel utilization factor during the inter-network control system communication process with MCR.

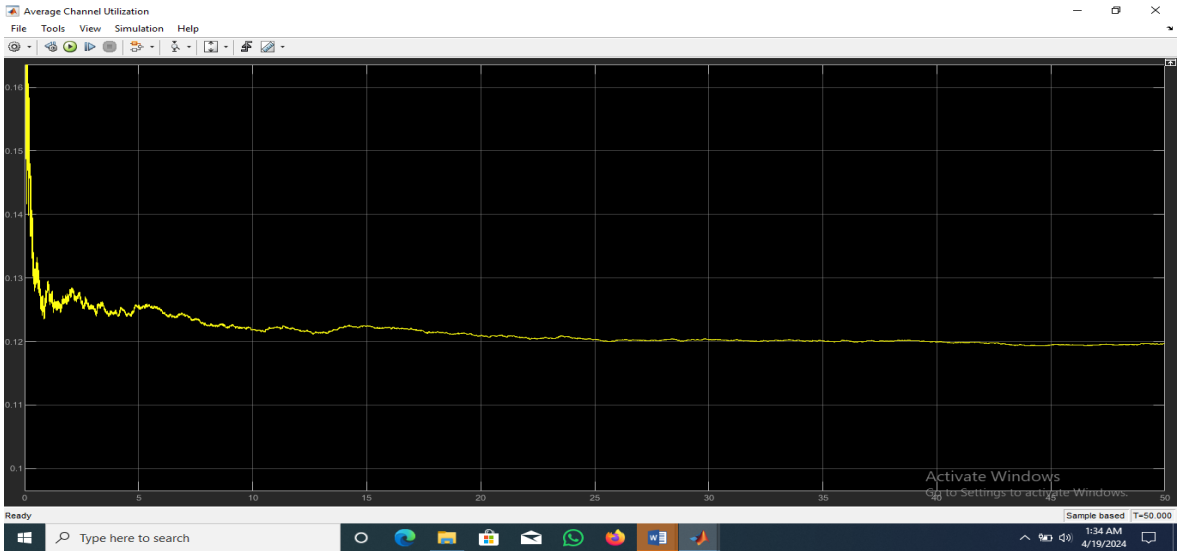

Figure 9: Channel Utilization Performance

Figure 9 showcases the channel utilization factor of the IIOT network with MCR. From the result, it was observed that during the communication process of the physical layer devices, the utilization factor remained consistently low at 0.126, which gives 12.6% channel utilization on average. This low utilization suggests that the Multi-Channel Router (MCR) effectively managed the data flow within the network, ensuring that each channel operated efficiently without becoming overwhelmed. It intelligently selects the most efficient paths for data transmission, minimizing congestion and ensuring smooth flow across the network.By optimizing routing paths and dynamically adapting to network conditions, the MCR facilitated smooth and reliable communication among the physical layer devices, thereby enhancing the overall performance and stability of the IIOT network. This highlights the crucial role of the MCR in mitigating congestion and maximizing the utilization of network resources, ultimately leading to improved efficiency and productivity in industrial environments.

5.1 Validation of the New IIOT Network with MCR

The approach utilized for the model validation is a comparative analysis of the new IIOT performance against the existing IIOT network with WAP-2 security and a static routing approach. In the data presentation, the network performance considering quality of service during communication is presented in Table 2.

Table 2: Validation Result of network performance with MCR

Time (min)	Packet data (Mbps)	Packet loss (%) with MCR	Throughput (%) with MCR	Latency (ms) with MCR	Packet loss without MCR (%)	Throughput without MCR (%)	Latency without MCR (ms)
03:10:00	778.24	0.947673	88.35455	39.25091	4.964	61	205.6
03:11:00	761.60	0.8295	87.20909	50.09455	4.345	67	262.4
03:12:00	808.96	0.850691	87.78182	39.44182	4.456	64	206.6
03:13:00	765.40	0.865773	86.82727	50.49545	4.535	69	264.5
03:14:00	737.28	0.846491	87.59091	51.92727	4.434	65	272.0
03:15:00	758.00	0.8862	87.20909	42.51545	4.642	67	222.7
03:16:00	737.28	0.8715	88.16364	40.58727	4.565	62	212.6
03:17:00	718.30	0.8505	87.59091	41.04545	4.455	65	215.0
03:18:00	788.48	0.828927	87.20909	50.15182	4.342	67	262.7
03:19:00	737.28	0.895745	87.4	52.04182	4.692	66	272.6
03:20:00	737.28	0.8694	88.16364	41.52273	4.554	62	217.5
03:21:00	757.76	0.8463	87.20909	50.51455	4.433	67	264.6
03:22:00	763.20	0.888491	88.35455	48.77727	4.654	61	255.5
03:23:00	737.28	0.906055	87.59091	52.00364	4.746	65	272.4
03:24:00	727.04	0.911782	87.20909	41.52273	4.776	67	217.5
03:25:00	737.28	0.8421	86.82727	46.65818	4.411	69	244.4
03:26:00	768.65	0.841718	87.4	40.56818	4.409	66	212.5
03:27:00	727.04	0.848591	87.20909	44.84455	4.445	67	234.9
03:28:00	778.24	0.947673	88.35455	39.25091	4.964	61	205.6
03:29:00	768.00	0.8295	87.20909	50.09455	4.345	67	262.4
03:30:00	808.96	0.850691	87.78182	39.44182	4.456	64	206.6
03:40:00	798.00	0.865773	86.82727	50.49545	4.535	69	264.5
03:41:00	737.28	0.846491	87.59091	52.00364	4.434	65	272.4
03:42:00	767.85	0.8862	87.20909	50.15182	4.642	67	262.7
03:43:00	737.28	0.8715	88.16364	48.22364	4.565	62	252.6
03:44:00	756.68	0.8505	87.59091	41.17909	4.455	65	215.7
03:45:00	788.48	0.828927	87.20909	50.15182	4.342	67	262.7
03:46:00	737.28	0.895745	87.4	39.44182	4.692	66	206.6
03:47:00	737.28	0.8694	88.16364	50.49545	4.554	62	264.5
03:48:00	757.76	0.8463	87.20909	52.00364	4.433	67	272.4
03:49:00	755.68	0.888491	88.35455	50.15182	4.654	61	262.7
03:40:00	737.28	0.906055	87.59091	48.22364	4.746	65	252.6
Avg.	756.6375	0.869084	87.56108	46.41477	4.552344	65.15625	243.125

Table 2 presents the comparative results of the network performance considering the network IIOT performance without MCR and the new IIOT with MCR. From the results, it was observed that when an average 756.63Mbps packet was transferred over the network from the physical layered components, the average latency with MCR was 46.4ms as opposed to 243ms in the network, giving a latency reduction percentage of 80.8%. Throughput reported with the MCR is 87.56% as against 65.16% in the network, thus giving an improvement of 34.52%. The packet loss rate with MCR was reported at 0.87%, as opposed to 4.55% in the network, thus giving a loss reduction rate of 80.88%. Overall, the results revealed that the IIOT network performed better with MCR than without MCR. The reason was that during the routing process with MCR, packets are routed using a dynamic channel selected based on the shortest distance and cost function, hence allowing instant transfer of packets without congested channels.

6. Conclusion

Developing and assessing the Multi-Channel Routing (MCR) algorithm to maximize Quality of Service (QoS) in Industrial Internet of Things (IIoT) networks was the goal of this study. The emphasis was on resolving important issues that impair IIoT network performance, such as excessive latency, substantial packet loss, and suboptimal throughput. The MCR algorithm was created to increase the efficiency and dependability of communication in industrial environments by combining cost-function-based routing with dynamic channel selection.

The MCR algorithm's examination revealed notable gains in performance. The comparison of outcomes of the IIoT network with and without MCR. The MCR-enabled network achieved an average latency of 46.4ms when transmitting an average packet of 756.63 Mbps, which is 80.8% lower than the baseline network's 243ms. The throughput with MCR was 87.56%, which was 34.52% higher than the 65.16% without MCR. Furthermore, MCR reduced packet loss by 80.88% as its packet loss rate was just 0.87%, far lower than the baseline network's 4.55% rate. These results show that by dynamically choosing uncongested channels, the MCR algorithm efficiently optimizes packet routing, allowing for quicker and more dependable data transfer.

In conclusion, by lowering latency, raising throughput, and minimizing packet loss, the MCR algorithm greatly improves IIoT network performance. Its capacity to dynamically route packets according to cost-function and shortest-distance computations guarantees effective use of network resources. These results support MCR's promise as a reliable approach to QoS improvement in IIoT settings. To further improve IIoT system performance, future research might examine its scalability in bigger networks and its integration with cutting-edge security protocols.

References

Alosaimi, S., & Almutairi, S. (2023). An intrusion detection system using BoT-IoT. Applied Sciences, 13(9), 1–15. https://doi.org/10.3390/app13095427

Arakanksha, C. (2016). Security issues of firewalls. International Journal of P2P Network Trends & Technology, 6(1), 4–9.

Ashish, K., Ansh, J., Deepak, B., & Pius, A. (2017). Internet of Things (IoT) and its applications. International Journal of Innovative Research in Technology, 3(12), 2349-6002.

Brou, P., & Janssen, M. (2015). Effect of the Internet of Things (IoT): A systematic review of the benefits and risks. 4th International Conference on Electronic Business (ICEB), 906–915.

Farooq, M. U., Mohammad, W., Sadia, M., Arjum, K.,& Talha, K. (2015). A review of the Internet of Things (IoT). International Journal of Computer Applications, 113(1), 1-7.

Ghosh, A., & Senthilrajan, A. (2019). Research on packet inspection techniques. International Journal of Scientific & Technology Research, 8, 2068–2073.

Gupta, B., Joshi, R., & Misra, M. (2010). Distributed denial of service prevention techniques. International Journal of Computer & Electrical Engineering, 5(6), 998–110.

Harbor M.C., Eneh I.I., Ebere U.C. (2021). Nonlinear dynamic control of anan autonomous vehicle under slip using an improved back-propagation algorithm. International Journal of Research and Innovation in Applied Science (IJRIAS); Vol. 6; Issue 9; https://rsisinternational.org/journals/ijrias/DigitalLibrary/volume-6-issue-9/62-68.pdf

Jamin, G., Uwe, B., Michael, F., Paul, F., Oliver, K., Frank, L., & Lukas, R. (2018). A detailed analysis of IoT platform architectures: Concepts, similarities, and differences. Springer Publisher, 80–101.

Jyotsna, & Nand, P. (2022). Novel DLSNNC and SBS-based framework for improving QoS in healthcare-IoT applications. International Journal of Information Technology, 14(4), 2093–2103.

https://doi.org/10.1007/s41870-022-00922-z

Kizza, J. M. (2005). Computer network security. Springer Engineering, 2(2), 268–276.

Malik, R., Singh, Y., Sheikh, Z., Anand, P., Singh, P., & Workneh, T. (2022). An improved deep belief network IDS on IoT-based network for traffic systems. Hindawi Journal of Advanced Transportation, 1–17. https://doi.org/10.1155/2022/7892130

Mazhar, T., Malik, M., Mohsan, S., Li, Y., Haq, I., Ghorashi, S., Karim, F., & Mostafa, S. (2023). Quality of Service (QoS) performance analysis in a traffic engineering model for next-generation wireless sensor networks. Symmetry, 15, 1–24. https://doi.org/10.3390/sym15020513

Mehryar, M., Rostamizadeh, A., & Talwalker, A. (2012). Foundations of machine learning. The Press Cambridge, Massachusetts.

Mohamed, L., Nabil, K., Kalid, E., Abdellah, E., & Mohamed, F. (2020). IoT security: Challenges and countermeasures. Procedia Computer Science, 117, 503–508.

Mohit, K. S., & Rakesh, K. S. (2019). Internet of Things (IoT) applications & security challenges. International Journal of Engineering Research & Technology, 7(12), 2218-2231.

Oforji, J. C., & Oju, O. (2018). Internet of Things and its applications. International Journal of Computer Science and Mathematics Theory, 4(2), 2545-5699.

Onu, P., Anup, P., & Charles, M. (2023). Industry 4.0 and smart manufacturing Industrial Internet of Things (IIoT): Opportunities, challenges, and requirements in manufacturing businesses in emerging economies. Procedia Computer Science, 217(2), 856–865.

Kekong P.E, Ajah I.A., Ebere U.C. (2019). Real-time drowsy driver monitoring and detection system using a deep learning based behavioural approach. International Journal of Computer Sciences and Engineering 9 (1), 11-21

Prasath, J.S., Ramachanraih, U., Prabhuraj, S., & Muthukumaran, G. (2020). Internet of Things- based hybrid cryptography for processing data security. Journal of Mathematics and Computer Science, 10(6), 2208–2232.

Radu, V., Casian, C., Laurențiu, M., & Ion, B. (2017). Network traffic anomaly detection using shallow packet inspection and parallel K-means data clustering. Available at: https://sic.ici.ro/wp-content/uploads/2017/12/SIC_2017-4-Art.2.pdf

Rishika, M., Jyoti, S., & Kavita, K. (2018). Internet of Things: Vision, application, and challenges. International Conference on Computational Intelligence and Data Science, 132, 1263–1269.

Saravanan, R., & Sujatha, P. (2018). A state of the art techniques on machine learning algorithms: A perspective of supervised learning approaches in data classification. Second International Conference on Intelligent Computing and Control Systems (ICICCS), 945–949. https://doi.org/10.1109/ICCONS.2018.8663155

Sochima V.E. Asogwa T.C., Lois O.N. Onuigbo C.M., Frank E.O., Ozor G.O., Ebere U.C. (2025)"; Comparing multi-control algorithms for complex nonlinear system: An embedded programmable logic control applications; DOI: http://doi.org/10.11591/ijpeds.v16.i1.pp212-224

Subramaniam, M., Vedanarayanan, V., Mubarakali, A., & Priya, S. (2023). Reinforcement learning to improve QoS and minimizing delay in IoT. Intelligent Automation & Soft Computing, 36(2), 1603. https://doi.org/10.32604/iasc.2023.032396

Sun, N., Li, T., Song, G., & Xia, H. (2021). Network security technology of intelligent information terminal based on mobile Internet of Things. Mobile Information

Systems, 8, 1–9. https://doi.org/10.1155/2021/6676946

Tanh, N., Tri, N., & Trung, M. (2021). The solution to improve information security for IoT networks by combining lightweight encryption protocols. Indonesian Journal of Electrical Engineering and Computer Science, 23(3), 1727–1735. https://doi.org/10.11591/ijeecs.v23.i3

Teng, D. (2022). Industrial Internet of Things anti-intrusion detection system by neural network in the context of Internet of Things for privacy law security protection. Wireless Communications and Mobile Computing, 1–17. https://doi.org/10.1155/2022/7182989

Ulagwu-Echefu A., Eneh .I.I. Ebere U.C. (2021). Enhancing realtime supervision and control of industrial processes over wireless network architecture using model predictive controller. International Journal of Research and Innovation in Applied Science (IJRIAS); vol 6; Issue 9.https://rsisinternational.org/journals/ijrias/DigitalLibrary/volume-6-issue-9/56-61.pdf

Xu, H., Yu, W., Griffith, D., & Goimie, N. (2018). A survey on Industrial Internet of Things: A cyber-physical systems perspective. NIST Author Manuscript IEEE Access, 1–21. https://doi.org/10.1109/access.2018.2884906