Computer Modeling in Engineering & Sciences

Tech Science Press

Doi:10.32604/cmes.2025.061318

ARTICLE

# Prioritizing Network-On-Chip Routers for Countermeasure Techniques against Flooding Denial-of-Service Attacks: A Fuzzy Multi-Criteria Decision-Making Approach

**Ahmed Abbas Jasim Al-Hchaimi[1], Yousif Raad Muhsen[2,3,*], Wisam Hazim Gwad[4], Entisar Soliman Alkayal[5], Riyadh Rahef Nuiaa Al Ogaili[6], Zaid Abdi Alkareem Alyasseri[7,8] and Alhamzah Alnoor[9]**

[1]Department of Electromechanical Systems Engineering, Thi-Qar Technical College, Southern Technical University, Basra, 61001, Iraq
[2]Department of Civil Engineering, Wasit University, Al Kut, 52001, Wasit, Iraq
[3]Technical Engineering College, Al-Ayen University, Thi-Qar, 64001, Iraq
[4]Department of Artificial Intelligence Engineering, College of Engineering, Alnoor University, Ninavah, 41012, Iraq
[5]Information Technology Department, Faculty of Computing and Information Technology at Rabigh King Abdulaziz University, Jeddah, 22230, Saudi Arabia
[6]Department of Computer Science, College of Computer Science and Information Technology, Wasit University, Al kut, 52001, Wasit, Iraq
[7]Information Technology Research and Development Center, University of Kufa, Najaf, 54001, Iraq
[8]College of Engineering, University of Warith Al-Anbiyaa, Karbala, 56001, Iraq
[9]Management Department, College of Business Administration (COBA), A'Sharqiyah University (ASU), Ibra, 400, Oman

*Corresponding Author: Yousif Raad Muhsen. Email: yousif@uowasit.edu.iq

Received: 22 November 2024; Accepted: 02 February 2025; Published: 03 March 2025

**ABSTRACT:** The implementation of Countermeasure Techniques (CTs) in the context of Network-On-Chip (NoC) based Multiprocessor System-On-Chip (MPSoC) routers against the Flooding Denial-of-Service Attack (F-DoSA) falls under Multi-Criteria Decision-Making (MCDM) due to the three main concerns, called: traffic variations, multiple evaluation criteria-based traffic features, and prioritization NoC routers as an alternative. In this study, we propose a comprehensive evaluation of various NoC traffic features to identify the most efficient routers under the F-DoSA scenarios. Consequently, an MCDM approach is essential to address these emerging challenges. While the recent MCDM approach has some issues, such as uncertainty, this study utilizes Fuzzy-Weighted Zero-Inconsistency (FWZIC) to estimate the criteria weight values and Fuzzy Decision by Opinion Score Method (FDOSM) for ranking the routers with fuzzy Single-valued Neutrosophic under names (SvN-FWZIC and SvN-FDOSM) to overcome the ambiguity. The results obtained by using the SvN-FWZIC method indicate that the Max packet count has the highest importance among the evaluated criteria, with a weighted score of 0.1946. In contrast, the Hop count is identified as the least significant criterion, with a weighted score of 0.1090. The remaining criteria fall within a range of intermediate importance, with enqueue time scoring 0.1845, packet count decremented and traversal index scoring 0.1262, packet count incremented scoring 0.1124, and packet count index scoring 0.1472. In terms of ranking, SvN-FDOSM has two approaches: individual and group. Both the individual and group ranking processes show that (Router 4) is the most effective router, while (Router 3) is the lowest router under F-DoSA. The sensitivity analysis provides a high stability in ranking among all 10 scenarios. This approach offers essential feedback in making proper decisions in the design of countermeasure techniques in the domain of NoC-based MPSoC.

**KEYWORDS:** NoC-based MPSoC security; flooding DoS attack; MCDM; FDOSM; FWZIC; fuzzy set

## 1 Introduction

### *1.1 Motivation*

The rapid proliferation of Internet of Things (IoT) platforms actress diverse applications such as smart cities, health care, and industrial automation has brought unprecedented levels of connectivity and data exchange [1,2]. At the core of these systems lies the Multiprocessor System-On-Chip (MPSoC) architecture (see Fig. 1), which integrates multiple processing elements to handle the varied workloads of IoT devices. Network-On-Chip (NoC) technology plays a critical role in managing communication among these processing elements, facilitating low-latency and high-bandwidth data transfer [3]. However, as IoT platforms grow in complexity, the reliance on third-party intellectual property (3PIP) cores and heterogeneous ones has exposed NoC-based MPSoCs to significant security risks, as shown in [2,4]. The biggest threat is the Flooding Denial-of-Service Attack (F-DoSA), where a malicious IP core floods the NoC with unnecessary traffic, leading to network congestion, degraded performance and potential system failure [5,6]. Given the critical nature of real-time processing in IoT applications, these is an urgent need for a robust and efficient approach to detect and mitigate such attacks while maintaining the system's performance and energy efficiency [5,7].

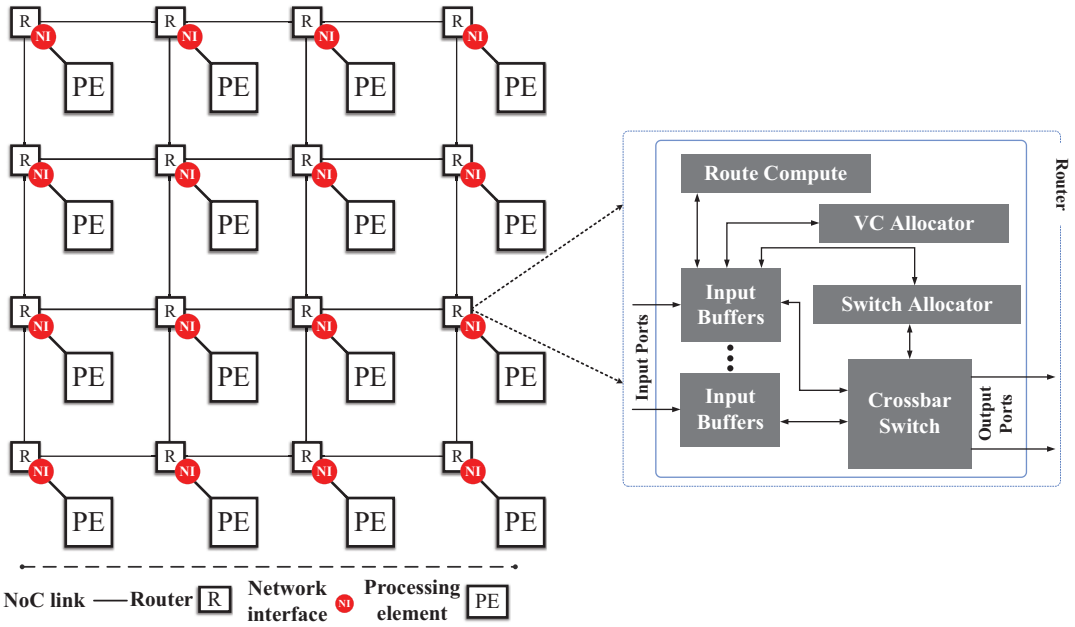


**Figure 1:** Typical NoC-based MPSoC platform in an IoT environment

### *1.2 Challenges*

Securing NoC-based MPSoC against threats like F-DoSA faces key challenges, such as the diversity of IoT traffic patterns blurs the distinction between normal and malicious behaviour, scalability demands computationally efficient detection, and evolving attack strategies require adaptable solutions. Machine Learning (ML) techniques have been used to address these issues using traffic features [8]. Timing-based features, for instance, have been exploited in attacks such as Earthquake and Prime + Probe Firecracker to

infer cryptographic keys and map processing elements. At the same time, trust-aware ML models analyze retransmission and latency to mitigate Hardware Trojans (HTs), as shown in [9,10].

Despite these advancements, the wide variety of NoC traffic features, such as flit latency, throughput, buffer usage and routing dependency, introduces challenges in determining which features are most impactful for security and performance optimization. Existing systemic security frameworks depend on feature-specific ML model approaches but lack a comprehensive approach to evaluate and prioritize traffic features for integration into a robust countermeasure technique and scalable NoC security mechanisms [11].

### *1.3 Research Gap*

Since the variety of traffic features employed in the ML-based NoC security approaches is rather vast, assessing such features and their ranking requires a systematic approach. On the one hand, prior research has identified specific features or threats associated with NoC traffic. However, there is currently no outfield approach to systemically rank and validate the importance of these features. This creates a gap for developing a Multi-Criteria Decision Making (MCDM) based approach to evaluate and prioritize NoC traffic features, enabling more effective and efficient AI-driven security solutions. On the other hand, previous research indicates that no study has yet integrated Single-valued Neutrosophic (SvN) with Fuzzy Decision by Opinion Score Method (FDOSM) and Fuzzy-Weighted Zero-Inconsistency (FWZIC) methodologies. Specifically, such integration into these decision-making frameworks would greatly strengthen their methodology and practical utility by providing a more precise and powerful means for dealing with uncertainty and inconsistency in complex, real-world problems. Bridging this gap is crucial for advancing theoretical understanding and practical application in On-Chip communication security.

### *1.4 Contribution*

The present paper aims to provide an integrated new approach for decision-making under uncertainty for ranking NoC router traffic feature alternatives. The proposed model integrates the Single-valued Neutrosophic-Fuzzy-Weighted Zero-Inconsistency (SvN-FWZIC) and Single-valued Neutrosophic-Fuzzy Decision by Opinion Score Method (SvN-FDOSM). More precisely, the implementation of the proposed methodology is based on a four-stage procedure that can be outlined as follows:

- Firstly, a group of experts identifies all relevant NoC-based MPSoC traffic features to be used as criteria and evaluates NoC routers as possible alternatives.
- Secondly, the SvN should be integrated with FDOSM, known as SvN-FDOSM, to overcome uncertainty issues and rank NoC routers' traffic features.
- Thirdly, the integration of SvN with Fuzzy-Weighted Zero-Inconsistency (FWZIC), known as SvN-FWZIC, will be extended to determine the significance per the criteria.
- Fourthly, implementing the MCDM method of group ranking based on extending SvN-FDOSM into Single-Valued Neutrosophic Weighted Einstein Averaging (SNEWA) operators.

### *1.5 Objectives*

We aim to achieve the following objectives in the paper:

- Collecting the NoC-based MPSoC router data as an alternative using General Execution-driven Multiprocessor Simulator version 5 (GEM-5) based GARNET2.0 ruby simulator.
- To integrate FDOSM into a new fuzzy environment to improve the ranking accuracy of fuzzy decisions.
- To develop an advanced version of the FWZIC by extending it to the fuzzy environment based on a new consistency measure to improve the robustness and accuracy of the weightings.

- An aggregation operator is also developed to extend the SvN-FDOSM for group decision-making by efficiently utilizing multiple experts' opinions.

### *1.6 Significance and Implications*

To the best of our knowledge, no research has been done in the domain of NoC-based MPSoC security to evaluate and rank the NoC routers' traffic feature alternatives. The overall significance of this paper is to develop a new comprehensive approach capable of efficiently and effectively forming experts, examining and ranking alternatives while considering uncertain and ambiguous data and experts' confidence levels. This paper fills the gap in identifying F-DoSA attacks. It provides the foundation for further investigation of the integration of decision-making with ML to improve security in embedded systems. The paper has significant practical implications for expanding the understanding of IoT system dependability and potential vulnerabilities to enhance IoT dependability, especially in safety-critical applications for which immediate and accurate recognition of security threats is critical. Through this study, we seek to help advance improved and more secure NoC-based MPSoCs to adequately support the IoT systems domain's secure operation. In particular, the MCDM models in our study integrate FWZIC and FDOSM methodologies with an advanced fuzzy set to address fuzziness and uncertainty in MCDM and incorporate a more nuanced representation of vague information. Specifically, the model includes the SvN, which extends traditional fuzzy logic by introducing three distinct membership functions: Being true, indeterminate, and false. This structure displays the degree to which a criterion is satisfied or unsatisfied and the corresponding hesitation or uncertainty in this triadic form, often neglected in other fuzzy models.

#### *1.6.1 Why Using Machine Learning (ML) in NoC Security*

ML is used in NoC security due to its ability to offer flexible approaches for identifying levels of security threats, including DoS attacks and hardware Trojans. In today's system, NoCs, including those in IoT, encounter flexible and different traffic flows that rule base approaches cannot capture. Anomalies can be easily detected in real-time through these patterns, thereby improving the results of the ML models with low false positives. Moreover, using the presented ML approaches, it is possible to select and rank the features of traffic that are important for detection, allocate the resources more efficiently, and enhance the detection without a negative impact on the system performance. This makes ML a crucial mechanism for improving security in NoC-based environments. Table 1 lists the NoC traffic feature resulting from the proposed ML approaches in the NoC-based MPSoC architecture security context.

#### *1.6.2 Why Using FDOSM and FWZIC*

MCDM is a widely utilized method in expert systems and decision science for resolving issues involving several criteria. It specifically focuses on generating appropriate decisions using the existing data [12]. Additionally, MCDM methods can improve the quality of decisions via a more rational, obvious, and effective process than traditional ones, so the implementation of MCDM is rapidly gaining popularity [13]. One important issue concerning human decision-making is the inconsistency ratio that results from pair comparisons. Moreover, the problem involves an innovative approach to measure two measures that pose a considerable challenge. So, comparing criteria in pairs and using them as a scale was very time-consuming [14].

Several newly developed methods like Level-Based Weight Assessment (LBWA), Full Consistency Method (FUCOM), Objective Preference Analysis (OPA), and Distance-Based Ranking (DIBR) [15–17] attempt to overcome the deficiencies of traditional criteria weighting methods concerning fewer pairwise comparison requirements and consistency. FUCOM has strict conditions to ensure full consistency, and

LBWA leads to a stepwise procedure to simplify the process. Unfortunately, most of these methods fail to address uncertainty or subjectivity adequately. A comprehensive approach is essential to address these challenges effectively. Salih et al. [18] proposed the FDOSM as an MCDM solution, which offers several advantages. It significantly reduced the number of comparisons and ensured balanced and transparent decision-making scenarios, minimizing inconsistencies and mitigating imprecision while maintaining computational simplicity.

On the other hand, using FWZIC to weigh criteria is also an effective method, with a number of key advantages that give it great persuasiveness concerning decision-makers [19]. Among the most prominent of FWZIC's advantages is its capability to deal with inconsistencies in the decision process if this occurs, which is the common headache that can quickly mess up a decision's correctness and its portrait. Using fuzzy set theory and a zero-inconsistency approach, FWZIC can support the weighting of the criteria in the presence of inconsistencies. Another important benefit of FWZIC is reducing the time and effort needed to weight the criteria [13]. Unlike most other methods that require direct comparison of criteria, which can be time-consuming [20], this approach offers a different way of combining criteria. Therefore, the decision-makers can be more confident about the final decision based on systematic and uniform criteria weighting.

### *1.6.3 Why Using Single-Valued Neutrosophic (SvN)*

Fuzzy sets and their extensions, as intuitionistic and hesitant fuzzy sets, have supplied noteworthy improvements in handling uncertain and vague information. Nevertheless, these methods do not adequately represent the indeterminate information embedded in human cognition. In order to fill this gap, Smarandache proposed neutrosophic as a new area of philosophy that later led to a generalization of the Intuitionistic Fuzzy Set (IFS), called Neutrosophic Set (NS) [19]. Neutrosophic sets incorporate three membership functions: Consequently, they can deal with indeterminate and contradictory information through their truth, indeterminacy, and falsity. On top of this basis, Wang et al. presented the SvN, which is a practical and simplified form of a neutrosophic set [21]. The standard unit interval $\{0; 1\}$ is employed instead of the nonstandard unit interval of neutrosophic sets in SvN, enabling SvN to be applied in real-world decision-making problems. The adaptation provided by this tool allows decision-makers to better model and analyze problems with strategies of SvN, which can integrate truth, indeterminacy, and falsity to be examined in a structured and computationally manageable manner. SvN has extensive applications in many decision-making processes, such as supply chain management [22], medical diagnosis [23], and risk assessment [20]. In the domain of NoC-based MPSoC, decision-making is commonly made by identifying tradeoffs among the multiple conflicting criteria like power consumption, latency, throughput, and reliability. Although traditional fuzzy sets may be satisfactory for handling the vagueness of individual criteria, they cannot adequately represent the indeterminate states encountered when possessing incomplete design information or uncertain environmental conditions. However, FWZIC and FDOSM need to be extended with SvN because the SvN has a greater ability to manage uncertainty, indeterminacy, and vagueness in complex decision-making processes. The lack of an extension of the FDOSM and FWZIC approaches to the SvN is a methodological and practical gap that has to be filled.

This paper is structured as follows: Section 2 presents the literature review. Section 3 shows the steps of constructing the decision matrix, experts' panel selection, and research methodology framework. In Section 4, different evaluation results of decision matrix criteria and alternatives prioritizing have been discussed. Section 5 describes the results' validation using objective, sensitivity analysis, and Spearman coefficient statistical methods. Section 6 includes the results of compression with previously proposed MCDM methods. Section 7 shows the practical implications and future directions. Finally, Section 8 concludes this research paper.

## 2 Literature Review

### *2.1 Studies on ML in NoC Security*

F-DoSAs signify threats in the interconnected NoC-based MPSoCs, particularly in IoT applications where these are expected to provide real-time communication. These attacks mostly flood the NoC with duplicated data packets that affect the network utilization, availability of system resources and performance [24]. Using 3PIPs makes the NoCs more susceptible to such attacks than other networks because the control targets of many NoCs implement more complex services that depend on 3PIPs. Previous work studied other techniques for detecting and addressing these problems. However, the inconsistency in the traffic characteristics of NoC and the limited availability of resources in IoT applications are still issues.

While numerous F-DoSA detection methods exist, most lack adaptability and fail to prioritize NoC traffic features effectively under dynamic IoT conditions [25–27]. Contemporary approaches fail to employ the traffic features flexibly and instead use a set of twelve traffic features as the input, failing to consider that the importance of each of the features may vary depending on the situation. This may lead to suboptimal performance and excessive computational overhead, making it impractical for IoT applications [28].

**Table 1:** ML approaches in the context of NoC-based MPSoC: algorithms, selected features, objectives, and utilized simulators

| Article | ML approach | | DoS attack | | Network traffic features (criteria) | ML approach objective | Utilized simulator |
|---|---|---|---|---|---|---|---|
| | Name | Algorithm | Source | Category | | | |
| [29] | HT detection and localization approach | ANN | 3PIP, HT | Path collision DoS | T, L, UT, PC, PIR | Detection + Localization | NETRACE + 64 MPSoC ALPHA ISA + PARSEC Benchmark Tool |
| [30] | Runtime monitoring mechanism | KNN, LGB, DCT, XGB, NN, LRN, NBC | MIP | Flooding DoS | CCT, IFI, BWT, VCO, IP, OP, VI, TI, PI, PC, MP, HC, HR, CH, TID, VC, FT, FID | Detection | GARNET2.0 GEM5 |
| [31] | Cascaded ML model | KNN, SVM | HT | Path collision DoS | PI, PR, PNL, P, H | Detection | GEM5 |
| [32] | ML model | LR, DT, RF, RF, XGBOOST | – | – | PC, VC, FID, BU, | Detection | GARNET2.0 |
| [33] | Sniffer | ANN perceptron classification model | MIP | Flooding DoS | BWT, IFI, VCO | Localization | NOXIM + GEM5 |
| [34] | SWiNoC security mechanism | MLP, SVM, KNN, DT, J48 classifier | – | Jamming DoS | – | Detection | ASIC design flows with synopsys design compiler using 65-nm chip multiprocessor standard cell libraries |

Note: {Inter-Flit-Interval: IFI, Buffer Waiting Time: BWT, Virtual Channel Occupancy: VCO}; {Packet injected: PI, Packet Revived: PR, Packet Network Latency: PNL, Power: P, Hopes: H, Buffer Utilization: BU}; {Timing: T, Latency: L, Urination Temperature: UT, Packet Counts: PC, Injection/Ejection Rate: PIR}; {Out Port: OP, In Port: IP, Cach Coherence Type: CCT, Flit Id: FID, Flit Type: FT, Virtual Channel: VC, Traversal Id: TID, Current Hop: CH, Current Router: HR, Hop Count: HC, Max Packet: MP, Packet Count: PC, Port Index: PI, Traversal Index: TI, Vnet Index: VI}, Dynamic Confidence Interval (DCI) algorithm to detect malicious packets, and a novel Dynamic Security Credit Table}; {Multilayer Perceptron (MLP), Support-Vector Machine (SVM), K-Nearest Neighbors (KNN), Decision Tree (DT), J48 Classifier (a decision tree-based classifier)}.

These limitations underscore the need to develop the MCDM approach, which allows for the systematic evaluation of NoC traffic features and their relevance to DoS detection. This way, researchers could establish effective countermeasures with proper protection elements, considering the crucial features that are important in accurate and versatile detection models for different network environments. For example, The authors [35] developed a new effective means of DoS attack monitoring. Their work showed that they could design a circuit for PIR-based and PPL-based F-DoS attacks and indicated the possibility of using low power, energy and area while using low power to counter communication disruption. Similarly, the study [8] proposes a timing-based attack for reversing the MPSoC layout that achieved 100% accuracy for identifying processing element mappings across different NoC topologies and demonstrated the inefficiency of previously proposed countermeasures against latency-oriented reconnaissance attacks. In addition, in the context of cryptography, authors [36] discussed communication-based microarchitectural attacks like those attaining leftover noise covariance during cryptographic procedures in shared NoC resources. This study established that such attacks pose a large threat, as they can extract information through side channels; this confirms the need to safeguard the communication infrastructure in MPSoCs.

Furthermore, the article's authors [37] proposed a runtime anomaly detection framework that adopted machine learning models like linear regression, decision tree and support vector machine for F-DoS attack detection. The study also confirmed the precision accuracy of those models holding up under different NoC congestion patterns to prosecute attacks within actual real-time schemes without significant performance degradation. Altogether, these works abate and resume that the security and resilience improvement of NoC-based MPSoC for fresh threats remains a significant investigation direction. Besides, Sudusinghe et al. (2021) [30] used gradient boosting classifiers for DoS detection directly on the analyzed NoC traffic features. This method is less localized, and it is computationally costly. Hence, it cannot be used effectively in real-time low-power systems. Also, Siha et al. [33] suggested "Sniffer," an in-router monitoring system to monitor congestion anomalies at router input ports.

When it comes to implementation, this approach employs group decision-making in order to find out which of the proposed flooding attacks is probable, and it has problems with high variability that are common for modern IoT applications. Moreover, Sankar et al. (2024) [9] proposed a trust-aware routing technique for MPSoCs infected with Hardware Trojans (HTs). This model selflessly avoids using HTs in routing paths and minimizes packet retransmission and the latency it accompanies; this it achieved without significantly having to pay the price in the area and further power consumption. While useful, this learning technique targets HTs only indirectly, does not involve direct detection, and necessitates extensive routing changes. Besides, Nagalaxmi et al. (2024) [7] suggested a secure NoC approach built from Noekeon and RSA algorithms to be implemented in their 4 × 4 2D mesh NoC architecture. The experience takes advantage of Noekeon's side-channel resistance, RSA's efficient encryption, a 64% improvement in throughput, and a 51% reduction in latency. This method mainly employs high performance concerning the encryption aspect rather than the detection of DoS attacks.

Unlike prior methods that rely on static features or assume stable traffic, this paper introduces a tailored MCDM approach limiting adaptability in variable IoT settings. Using FWZIC for weighting and FDOSM for ranking enables real-time, precise F-DoSA detection with reduced computational demands, enhancing effectiveness in divers IoT environments.

### *2.2 Studies on FDOSM and FWZIC*

In 2022, authors of [37] demonstrated the utilization of FDOSM and Interval-Valued Pythagorean Fuzzy Sets to evaluate sign language recognition systems on wearable electronic devices. Besides, in recent research, FDOSM has been developed by Al-Hchaimi et al. [38,39] to evaluate countermeasure techniques against

Denial-of-Service and Timing Side-Channel attacks concerning the NoC-based MPSoC domain. This evaluation framework utilizes Fermatean-FDOSM and Criteria Importance Through Intercriteria Correlation (CRITIC). Three experts specializing in NoC-based MPSoC and IoT communications security served as a judgment panel to ascertain the criterion weights, providing their opinions on the importance of criteria in each DM. Additionally, two ranking approaches were employed for the alternatives in the DMs: individual and group rating. The F-FDOSM MCDM method obtained the final ranking of optimal countermeasure methods against integrated attacks. In addition, the authors of [40–42] delivered an integrated MADM evaluation framework to Rank Research-Based Microgrids (RB-MGs) by combining FWZIC and VIKOR processes. The evaluation identified 'installed power (KW)' and 'storage capacity (C3)' as fundamental criteria. At the same time, LIER-CIRCE attained the highest position according to this evaluation, and Ormazabal took the lead in 'storage capacity (C3)'. The assessment performed positive correlations against TOPSIS and MABAC methods but yielded negative correlations with Multi-Attribute Ideal Real-Anti Ideal Ratio Analysis (MAIRA). Using Triangular Spherical Fuzzy Numbers (TSFN), the authors proposed the APPSS method to handle uncertainties through preference and performance analysis processes. In assessing COVID-19's impact on India, this approach identified the 60–69 age segment as the most at-risk population category, thus helping policy leaders make decisions. In addition, Puška et al. [43] integrated FDOSM and linear Diophantine fuzzy logic with a medical waste generated by ten hospitals analysis through the Artificial Neural Network of their amount. Since the FDOSM used an external method to determine a weight for every criterion, various researchers have advocated that FWZIC should be used. The FWZIC method, introduced by article [44], was proposed to identify essential criteria weights while ensuring consistency. Later, many studies considered FWZIC a feasible replacement for the traditional MCDM methods used in different areas. The distribution of COVID-19 vaccines poses an MCDM challenge due to multiple criteria incorporations and substantial differences between these cores. This problem is a difficult one that requires an MCDM framework. Albahri et al. [13] employed a q-rung ortho-pair fuzzy framework to address these issues, incorporating FDOSM and FWZIC.

Furthermore, the introduction of the Cubic Pythagorean fuzzy set, designed to handle uncertainty, found application in Sign Language through Alamoodi et al. [14], who integrated it with FWZIC. Also, Alqaysi et al. [12] used the Interval type 2 trapezoidal-FWZIC technique (IT2TR-FWZIC) to allocate the correct weights to the nine polluting substances. Besides, Alamoodi et al. [45] applied FWZIC and Multi-Objective Optimization based on Ratio Analysis (MULTIMOORA) in evaluating oil companies. Despite previous efforts to address uncertainty and ambiguity in these extensions, some challenges remained. Finally, the authors of the study [46] suggested a new approach based on FPHFSs and MCDM techniques that rate Agri-food 4.0 supply chains (Agri4SC) using the criteria Supply Chain Visibility, Supply Chain Resource Integration and Sustainable Performance (SCV, SCRI, and SP) that take into account the uncertainties of the evaluation.

## 3 Research Methodology

This section contains an in-depth discussion of the methodologies utilized to create a new decision-making method for weighting traffic features and ranking routers of NoC-based MPSoC architecture, as shown in Fig. 2.

### *3.1 Dataset and Simulation Scenarios*

This study leverages a dataset inspired by Sudusinghe et al. (2021) [30], generated through simulations of a 3 × 3 mesh NoC architecture using the GARNET2.0 framework and the Gem5 simulator. The NoC configuration and simulation parameters are listed in Table 2. The captured dataset is normal as well.

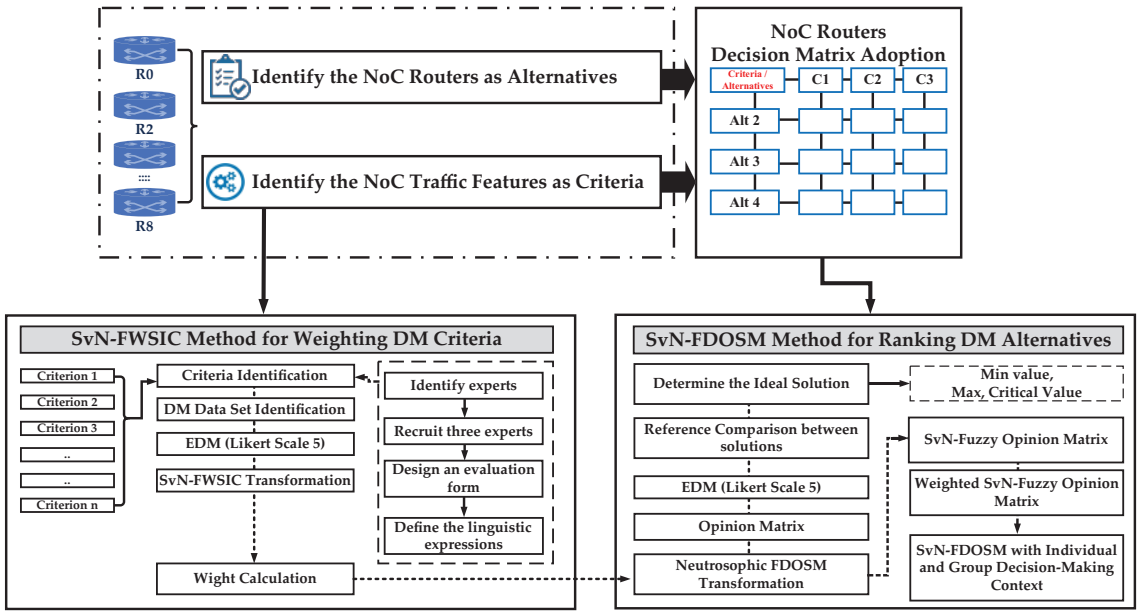


**Figure 2:** Research methodology

**Table 2:** Key parameters and configuration of the 3 × 3 NoC topology and simulation setup used for evaluating traffic features modelling attack scenarios

| Parameter | Description |
|---|---|
| **NoC topology** | 3 × 3 mesh topology using deterministic X-Y routing with wormhole switching and a 3-stage router pipeline. |
| **Router configuration** | Each router includes buffer write, route computation with virtual channel allocation, and link traversal. Each input port has four virtual channel buffers. |
| **Task mapping** | Tasks executed by IP cores with one malicious core injecting memory request packets targeting critical nodes. |
| **Processor and memory setup** | Each IP core operates at 1 GHz with a private L1 cache. Four memory controllers, placed at boundary nodes, provide equal access to off-chip memory. |
| **Traffic features** | Analyzed features include hop counts, enqueue times, packet injection rates, and virtual channel utilization. |
| **Attack injection rate** | The malicious core increases traffic by injecting packets 50% above the normal traffic rate. |
| **Benchmark used** | FFT benchmark from the SPLASH-2 suite, simulating normal and attack traffic scenarios. |

Attack traffic contains hop counts, traversal identifiers, number of packets, enqueue time, ingress/egress port, and virtual channel usage, as shown in Fig. 3. The analysis of these features allows the presentation of a clear picture of NoC functionality under different traffic scenarios.

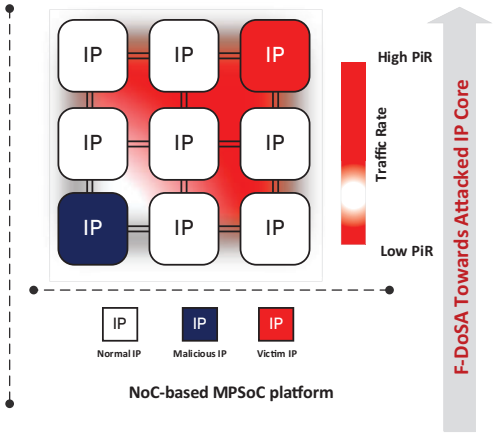


**Figure 3:** An illustrative example of F-DoSA involves a malicious IP core that targets a victim IP core. The heat map highlights elevated traffic activity concentrated around victim IP core

Normal simulation patterns depicted relatively fair traffic distribution across IP cores, while the attack simulations introduced injected malicious packets focused on particular nodes to mimic congestion and poor performance. To increase the reliability of the results, the traffic patterns were quite different, which excluded excessive focus on a specific configuration of the NoC. The decision matrix built from these simulations quantifies router performance based on criteria including, but not limited to, throughput, latency, energy consumption and congestion. Feature importance analysis also determined the priority of measurements towards NoC performance, emphasizing likely performance indicators. SPLASH-2 benchmarks and synthetic traffic patterns used for the validation confirmed the dataset's suitability for ranking routers and discovering significant traffic features essential for effective network operation. This approach forms a correct framework to assess the NoC traffic and router performances.

### *3.2 Phase 1: Decision Matrix Construction*

In this section, we describe the decision matrix (Table 3) resulting from the simulation process detailed in above (Section 3.1), which involved a 3 × 3 mesh topology NoC-based MPSoC platform in which each IP core was connected to a NoC router. The simulation results were collected for mixed NoC traffic scenarios under normal and F-DoSA conditions, where the Out-Port and In-Port columns in Table 3 reflect the flits take to leave a router which they enter a router, and both are encoded Integer (0-local, 1-north, 2-east, 3-south and 4-west). These values mimic flit movement across the NoC to assess traffic distribution and search for abnormalities (malicious traffic). Moreover, these counts, for example, 12, 14 or 11, represent the flit traffic on each port; this we use to analyze router activity and traffic under both normal and attack scenarios. Furthermore, the definitions of other features were obtained:

(i) Enqueue Time: This is when a packet is added to the input queue of a node in the network. In other words, it is when the packet starts its journey through the network.

(ii) Packet Count Decremented: This refers to the number of packets removed from a node's input queue and forwarded to the next node in the network. Each time a packet is forwarded, this count is decremented.

(iii) Packet Count Incremented: This is the opposite of the previous feature. It refers to the number of packets a node receives and added to its input queue. Each time a packet is received, this count is incremented.

(iv) Max Packet Count: This refers to the larger number of packets that can be placed in a node's input queue at any particular moment. When a new packet appears while the queue is full, it will be lost.
(v) Packet Count Index: This index shows a packet's location in an input queue within a node. It is used to monitor which packet will be sent next.
(vi) Traversal Index: This is an index of the ranking node in a network. It is used to decide which nodes a packet should be sent next.
(vii) Hop Count: This is the number of nodes a packet has visited. This count is increased every time a packet is forwarded to another node.

**Table 3:** Decision matrix

| | Features | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Router per NoC** | **Out-port** | **In-port** | **Enqueue time** | **Packet count decremented** | **Packet count incremented** | **Max packet count** | **Packet count index** | **Traversal index** | **Hop count** |
| **R0** | 12 | 14 | 8 | 3 | 5 | 4 | 4 | 7 | 7 |
| **R1** | 8 | 12 | 10 | 4 | 5 | 4 | 3 | 6 | 6 |
| **R2** | 8 | 11 | 9 | 4 | 6 | 4 | 3 | 5 | 5 |
| **R3** | 13 | 12 | 9 | 5 | 6 | 4 | 4 | 3 | 3 |
| **R4** | 11 | 10 | 8 | 4 | 5 | 4 | 3 | 6 | 6 |
| **R5** | 9 | 11 | 8 | 5 | 6 | 4 | 3 | 4 | 4 |
| **R6** | 8 | 10 | 9 | 4 | 6 | 4 | 3 | 5 | 5 |
| **R7** | 10 | 14 | 9 | 4 | 6 | 4 | 3 | 5 | 5 |
| **R8** | 11 | 13 | 9 | 4 | 5 | 4 | 3 | 6 | 6 |

Note: R: Router of NoC.

### *3.3 Phase 2: Criteria Weighting by SvN-FWZIC*

In the following subsections, we will elaborate on the five fundamental steps of the SvN-FWZIC approach:

**First Step:** The first definition stage is the set of evaluation definitions. This involves specifying the evaluation criteria, which will be discussed in the next step, whereby these experts evaluate them.

**Second Step:** The procedure of expert choice for the Structured Expert Judgment (SEJ) involves several crucial stages. Here are the five sub-steps engaged in this process:

- Identification of Knowledgeable Experts: The first step is to find individuals with knowledge related to that field of study. Such specialists are regarded as knowledgeable concerning the subject of assessment.
- Creation of an Expert Pool: Many experts are created when potential experts are identified. This pool should have at least three experts per subject. It should also be mentioned that studies [37] suggest an optimal size for the panel of experts at 3–5 people.

- Development of an Evaluation Model: The third sub-step establishes an assessment model of great importance to data collection. This model underpins the gathering of expert opinions and judgments.
- Assessment of Questionnaire Reliability and Validity: The experts chosen in the previous step are to evaluate the reliability and validity of a questionnaire. This procedure ensures that the questionnaire is reliable and efficient for collecting expert opinions.
- Importance Rating Using Likert Scale: Step 4 uses a five-point Likert scale to assess the degree of importance attributed to each criterion. This selection is made to reduce bias and improve the overall validity of the expert judgments.
- Conversion of Linguistic Scale to Numerical Scale: Finally, the linguistic scale evaluating the importance of a criterion used by experts is translated into a quantitative equivalent numerical one. This is done by using each expert qualitative input and converting it into a number, as represented in Table 4.
- These sub-steps provide for a structured and robust process of expert selection and assessment procurement, leading to the Structured Expert Judgment (SEJ) results from' reliability and validity.

**Table 4:** Five-point Likert scale

| Linguistic scoring scale | Numerical scoring scale |
|---|---|
| Not _important | 1 |
| Slight_important | 2 |
| Moderately_important | 3 |
| Important | 4 |
| Very_important | 5 |

**Third Step:** Expert decision matrix construction. An Expert Decision Matrix (EDM) is constructed in this step, consisting of the alternatives and criteria displayed in Table 5.

**Table 5:** Expert decision matrix (EDM)

| Criteria | $C1$ | $C2$ | ... | $Cn$ |
|---|---|---|---|---|
| E1 | I $(E1/C1)$ | I $(E1/C2)$ | ... | I $(E1/\mathrm{Cn})$ |
| ... | ... | ... | ... | ... |
| Em | I $(En/C1)$ | I $(\mathrm{En}/\mathrm{C2})$ | ... | I $(Em/Cn)$ |

Note: E1: Expert 1, C1: Criteria.

**Fourth Step:** The application of the SvN membership function is the next phase of the process. During this step, the fuzzy function associated with membership and defuzzification is applied to the EDM data. This procedure enhances the precision and effectiveness of the information, which is crucial, especially considering the challenge MCDM faces due to its inherent inclination toward strict preferences for each criterion (refer to Table 6). As previously mentioned, SvN-FWZIC is adept at addressing inconsistency and achieving high accuracy. The SvN can take on an objective form and is defined following Definitions 1, 2, and 3.

**Table 6:** Linguistic terms and their equivalent SvN

| Linguistic term | SvNs | | |
|---|---|---|---|
| Not _important | 0.1 | 0.9 | 0.9 |
| Slight_important | 0.3 | 0.75 | 0.7 |
| Moderately_important | 0.5 | 0.5 | 0.5 |
| Important | 0.8 | 0.15 | 0.2 |
| Very_important | 0.9 | 0.1 | 0.1 |

**Definition 1.** Following [47], let us consider a space of points or objects denoted as X, where each element in X is represented as x. Within this context, an SNS (Scalable Neutrosophic Set) in X can be described as S = {⟨x, t_S(x), f_S(x), k_S(x)⟩ | x ∈ X}, where the components t_S(x), f_S(x), and k_S(x) correspond to the truth-membership (with values satisfying 0 ≤ t_S(x) ≤ 1), indeterminacy-membership (with values satisfying 0 ≤ f_S(x) ≤ 1), and falsity-membership (with values satisfying 0 ≤ k_S(x) ≤ 1), respectively.

In the scenario where X consists of only one element, the SNS is simplified to an SNN (Scalable Neutrosophic Number), and it is denoted as S = ⟨t, f, k⟩, where t, f, and k represent the truth-membership, indeterminacy-membership, and falsity-membership, respectively.

**Definition 2.** When comparing two SNNs [47], denoted as S_1 and S_2, the process can be described as follows:

$$p(S_1) > p(S_2), \text{ then } S_1 \succ S_2; \tag{1}$$

$$p(S_1) = p(S_2) \text{ and } q(S_1) > q(S_2), \text{ then } S_1 \succ S_2; \tag{2}$$

$$\boldsymbol{p(S_1) = p(S_2) \text{ and } q(S_1) = q(S_2), \text{ then } S_1 = S_2.} \tag{3}$$

$$\boldsymbol{p(S_i) = \frac{t_i + 1 - f_i + 1 - k_i}{3} \text{ and } q(S_i) = t_i - k_i (i = 1,2)} \tag{4}$$

**Definition 3.** The hypothesis posits that the following:

$S_j = \langle t_j, f_j, k_j \rangle (j = 1, 2, \cdots, n$ represents a collection of SNNs, where $S_j, \omega_j \in [0,1]$ and $\sum_{j=1}^{n} \omega_j = 1$. The subsequent operators for single-valued neutrosophic weighted averages are considered in this scenario. This study employed the SNEWA operators, as demonstrated in Eq. (5) [48].

$$\boldsymbol{\text{SNEWA}(S_1, S_2, \cdots, S_n)} = \left\langle \frac{\prod_{j=1}^{n}(1+t_j) - \prod_{j=1}^{n}(1-t_j)}{\prod_{j=1}^{n}(1+t_j) + \prod_{j=1}^{n}(1-t_j)}, \frac{2\prod_{j=1}^{n} f_j}{\prod_{j=1}^{n}(2-f_j) + \prod_{j=1}^{n} f_j}, \frac{2\prod_{j=1}^{n} k_j}{\prod_{j=1}^{n}(2-k_j) + \prod_{j=1}^{n} k_j} \right\rangle \tag{5}$$

**Fifth Step:** The weight coefficients for the evaluation criteria are determined in the Weight Computation phase. This involves utilizing the fuzzified data from the previous step to calculate the weight coefficients ($w_1, w_2, \ldots, w_n$) for the evaluation criteria. The following steps are taken to derive these coefficients:

Calculate the ratio of the fuzzified data using Eq. (6), specifically designed for SvN. These equations can be referenced in Table 7 for further details. Eq. (7) symbolizes the actual process of computing these weight coefficients.

$$\frac{\mathrm{Imp}(\widetilde{\mathrm{E1}}/C1)}{\sum_{j=1}^{n}\ \mathrm{Imp}\left(\widetilde{\mathrm{E1}}/C_{1j}\right)} \tag{6}$$

where $\mathrm{Imp}\left(\frac{\widetilde{E1}}{C1}\right)$ represent the fuzzy number of $\mathrm{Imp}\left(\frac{E1}{C1}\right)$.

**Table 7:** Linguistic terms and their equivalent SvN

| Linguistic term | SvNs | | |
|---|---|---|---|
| No_Difference | 0.1 | 0.9 | 0.9 |
| Slight_Difference | 0.3 | 0.75 | 0.7 |
| Difference | 0.5 | 0.5 | 0.5 |
| Very_Difference | 0.8 | 0.15 | 0.2 |
| Huge_Difference | 0.9 | 0.1 | 0.1 |

(ii) The average values are calculated to determine the ultimate fuzzy values of the weight coefficients for the evaluation criterion $(\tilde{w}, \widetilde{w2}, \ldots, \widetilde{wn})^T$. The Fuzzy $(\widetilde{\mathrm{EDM}})$ is employed to calculate the ultimate weight value of each criterion using the provided Eq. (7).

$$\widetilde{W_J} = \left(\sum_{i=1}^{m} \frac{\mathbf{Imp}\left(\overline{E_{tj}}/C_{tj}\right)}{\sum_{j=1}^{n}\ \mathbf{Imp}\ (\mathbf{E}(\mathbf{E_{tj}}/C_{tj})}\right)/m, \text{ for } \boldsymbol{i} = \mathbf{1, 2, 3, \ldots} \boldsymbol{m} \text{ and } \boldsymbol{j} = \mathbf{1, 2, \ldots n} \tag{7}$$

Fuzzy weights $\widetilde{w_J}$ are assigned to each criterion by dividing their ratio values by the total number of experts, $\widehat{Imp(E1/C1)}$ represent the fuzzy number of Imp (E1/C1), and $\sum_{j=1}^{n} \mathrm{Imp}(\mathrm{E}(\mathrm{E_{tj}}/C_{tj})$. It is the calculation of the total value of fuzzy numbers representing the importance assigned by the expert for each criterion.

### *3.4 Phase 3: Alternatives Ranking by SvN-FDOSM*

This section outlines the steps in the FDOSM approach for ranking NoC traffic features, as illustrated in the research methodology. The process of the FDOSM ranking method can be summarized into three distinct stages, as follows:

***Stage 1: Data Input***

The DM is constructed in the data input stage by considering the intersection of NoC traffic features criteria and routers as an alternative, as described in Table 1. This process results in the formation of NoC traffic features, which are structured based on (A × C) sets comprising $(\mathrm{A_1}, \mathrm{A_2} \ldots \mathrm{A_m})$ alternatives and $(\mathrm{C_1}, \mathrm{C_2} \ldots \mathrm{C_n})$ criteria. Eq. (8) visually represents this NoC traffic features DM format.

$$\mathrm{DM} = \begin{matrix} \mathrm{A_1} \\ \mathrm{A_2} \\ \vdots \\ \mathrm{A_m} \end{matrix} \begin{bmatrix} \mathrm{C_{11}} & \mathrm{C_{12}} & \ldots & \mathrm{C_{1n}} \\ \mathrm{C_{21}} & \mathrm{C_{22}} & \ldots & \mathrm{C_{2n}} \\ \vdots & \vdots & \vdots & \vdots \\ \mathrm{C_{m1}} & \mathrm{C_{m2}} & \ldots & \mathrm{C_{mn}} \end{bmatrix} \tag{8}$$

***Stage 2: Data Transformation***

This stage encompasses the following steps:

1. Determine the ideal solution by selecting each criterion's range of (min, max, critical) values using Eq. (9). The ideal value represents the maximum benefit and the minimum cost, and the critical value lies between them.

$$a_j^* = \begin{cases} \max\limits_{i=1,\ldots,m} a_{ij} & \text{if } C_j \text{ is a benefit attribute} \\ \min_{i=1,\ldots,m} a_{ij} & \text{if } C_j \text{ is a cost attribute} \\ cv_j & \text{otherwise} \end{cases} \tag{9}$$

2. Select a panel of specialists who possess a comprehensive understanding and substantial expertise in the field of research. This research required the participation of three experts.
3. Construct an opinion matrix utilizing the perspectives of the experts. The matrix facilitates a comparison between the ideal answer and alternative values for each criterion while also generating linguistic phrases that encapsulate the viewpoints of experts.
4. The opinion matrix can be converted into a numerical matrix using a linguistic Likert scale. The Likert scale allocates different degrees of significance to the criteria, as determined by the evaluations of experts. Using linguistic terminology plays a pivotal role in ascertaining the degree of importance within the evaluation process. The scale consists of five levels, ranging from "No Difference" to "Huge Difference," as described in Eq. (10) and Table 7.

$$Op_{Lang} = \{((\underset{ij}{\tilde{v}} \otimes v_{ij} | j \in J).|\mathrm{i} = 1, 2, 3 \ldots m)\} \tag{10}$$

This ⊗ refers to comparing the ideal solution and alternatives [18].

5. Apply the opinion matrix in Eq. (11) as the basis for expert opinions. Transform the matrix into a fuzzy opinion matrix using the SvN method, yielding the final output of this stage.

$$\mathrm{Op}_{\mathrm{Lang}} = \begin{matrix} \mathrm{A}_1 \\ \vdots \\ \mathrm{A}_\mathrm{m} \end{matrix} \begin{bmatrix} \mathrm{Op}_{11} & \cdots & \mathrm{Op}_{1\mathrm{n}} \\ \vdots & \ddots & \vdots \\ \mathrm{Op}_{\mathrm{m1}} & \cdots & \mathrm{Op}_{\mathrm{mn}} \end{bmatrix} \tag{11}$$

where the term ($\mathrm{Op}_{\mathrm{Lang}}$) denotes the decision maker's opinion.

***Stage 3: Data Processing***

1. This stage marks the conclusive step in ranking the fuzzy decision matrix.
2. There are two methods for ranking based on the opinions of individual and group experts [18].

$$\mathrm{SNEWA}_\omega\left(S_1, S_2, \cdots, S_n\right) = \left\langle \frac{\prod_{j=1}^n \left(1+t_j\right)^{\omega_j} - \prod_{j=1}^n \left(1-t_j\right)^{\omega_j}}{\prod_{j=1}^n \left(1+t_j\right)^{\omega_j} + \prod_{j=1}^n \left(1-t_j\right)^{\omega_j}}, \frac{2\prod_{j=1}^n f_j^{\omega_j}}{\prod_{j=1}^n \left(2-f_j\right)^{\omega_j} + \prod_{j=1}^n f_j^{\omega_j}}, \frac{2\prod_{j=1}^n k_j^{\omega_j}}{\prod_{j=1}^n \left(2-k_j\right)^{\omega_j} + \prod_{j=1}^n k_j^{\omega_j}} \right\rangle \tag{12}$$

The fuzzy opinion matrices' results are combined using Eq. (12) [47], and the defuzzification process is carried out using Eq. (13) [45], where the lower score corresponds to the highest effectiveness NoC router under the F-DoSA scenario.

$$\boldsymbol{s(A) = (t + 1 - f + 1 - k)/3} \tag{13}$$

## 4 Result and Discussion

In this section, we discuss the results obtained from the SvN-FWZIC and SvN-FDOSM in detail. These results are analyzed and interpreted to emphasize the performance and effectiveness of each method in tackling the desired decision-making challenges.

### *4.1 Results of Weighting*

The assessment scores and measurement weights for each criterion are shown below. The SvN-FWZIC result for the assigned weight of the NoC traffic features is also clarified using Eqs. (1)–(7). The evaluation and selection procedures were given to three specialists with more than 20 years of relevant expertise. Table 8 and Fig. 4 show the experts' relative weights for NoC traffic features criteria. Table 8 shows the weight of criteria extracted from NoC-based MPSoC routers' traffic features under heavy F-DoSAs. To find the impact of F-DoSAs on MPSoC routers' traffic feature, criteria such as Enqueue Time, Packet Count Decremented, Packet Count Incremented, Max Packet Count, Packet Count Index, Traversal Index and Hop Count were weighted based on their significance to network performance and security.

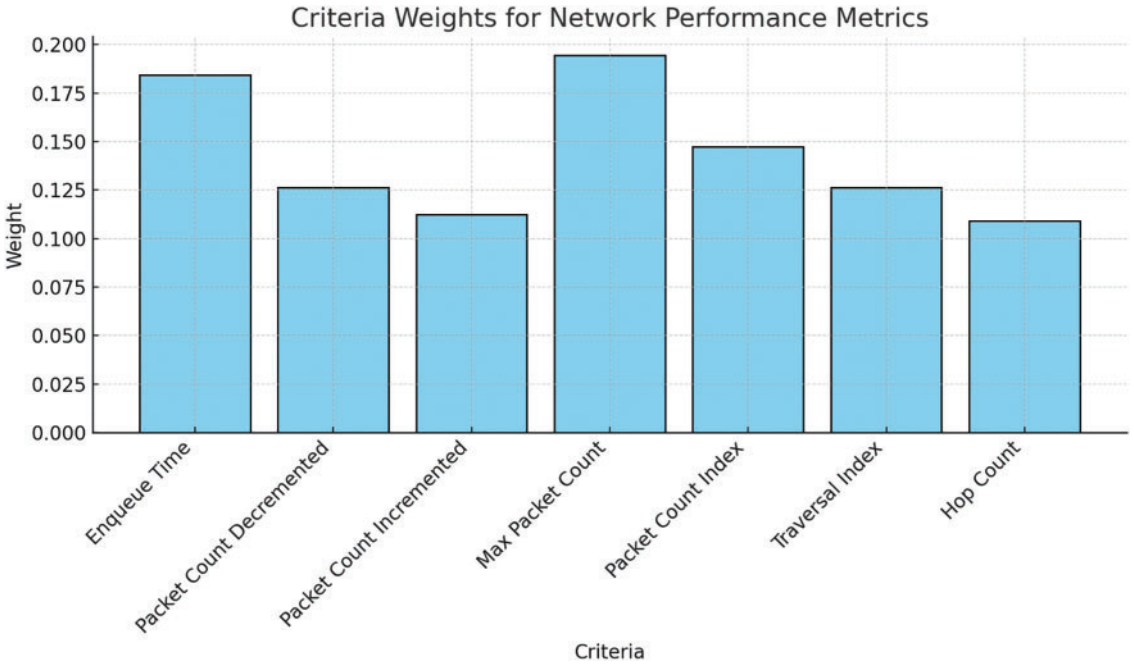


**Figure 4:** Importance of criteria weights in the utilized decision matrix

Additionally, the weights for Max Packet Count (0.1946) and Enqueue Time (0.1845) demonstrate their significant values and relevance in assessing the resilience of MPSoC systems under attack.

The measure of delay due to the time packets are spent in a queue is Enqueue Time, which is key as excessive amounts of queue time can cause significant processing delays that inhibit response time. In the same way, the Max Packet Count is similar to the threshold above which the system can handle packets, exceeding which can cause packet loss or congestion, leading to vulnerability to F-DoSAs. These two criteria are what engineering teams should optimize—by improving queue management strategies and packet handling algorithms to handle bursts, as illustrated in Fig. 4. Techniques including dynamic buffer resizing and implementing rate limiting for the packets' flow will control the packet flow based on the

data flow rate and guarantee efficient processing under the high load of the data flow. In addition, adaptive congestion control methods can also distribute traffic load over processing nodes, avoiding too many packets enqueueing to a processing node and max packet overload. This focus on high-weight criteria substantially strengthens MPSoC's resiliency to F-DoSAs, insulating the system from network congestion and latency spikes. The other criteria, Packet Count Decremented, Packet Count Incremented, Packet Count Index, Traversal Index, and Hop Count, are also equally as crucial, together with the high weight criteria Max Packet Count and Enqueue Time, in evaluating the effects and minimizing the impacts of the F-DoSAs on MPSoC. In addition, by monitoring these criteria in real time and adapting routing protocols, the system will be further fortified by balancing network load and reducing vulnerability to F-DoSAs. Focusing on all weighted criteria of this MPSoC improves its robustness, achieving better performance and resilience to malicious traffic patterns. The result of weight will be used with SvN-FDOSM to find the final rank of routers.

**Table 8:** Final criteria weight

| | Enqueue time | Packet count decremented | Packet count incremented | Max packet count | Packet count index | Traversal index | Hop count |
|---|---|---|---|---|---|---|---|
| **Criteria wight** | 0.1845 | 0.1262 | 0.1124 | 0.1946 | 0.1472 | 0.1262 | 0.1090 |

### *4.2 Results of Ranking*

In this part, we provide the findings and discussion from our analysis of the SvN-FDOSM experts' thoughts on NoC routers during the F-DoS attack. Experts record their collective judgments about the best possible solution to each criterion based on Eqs. (8) and (9) to make linguistically grounded comparisons between the best possible answer and other values for each criterion or alternative. Table 9 depicts the opinion matrix as reported by the three experts using the Likert five-point scale method.

**Table 9:** Opinion matrix of three experts

| NoC routers | Enqueue time | Packet count decremented | Packet count incremented | Max packet count | Packet count index | Traversal index | Hop count |
|---|---|---|---|---|---|---|---|
| | | | **Expert 1** | | | | |
| R0 | D | D | SD | SD | ND | ND | ND |
| R1 | ND | SD | SD | SD | SD | SD | SD |
| R2 | SD | SD | ND | SD | SD | D | D |
| R3 | SD | ND | ND | SD | ND | HD | HD |
| R4 | D | SD | SD | ND | SD | SD | SD |

(Continued)

**Table 9 (continued)**

| NoC routers | Enqueue time | Packet count decremented | Packet count incremented | Max packet count | Packet count index | Traversal index | Hop count |
|---|---|---|---|---|---|---|---|
| R5 | D | ND | ND | SD | SD | VD | VD |
| R6 | SD | SD | ND | SD | SD | D | D |
| R7 | SD | SD | ND | SD | SD | D | D |
| R8 | SD | SD | SD | SD | SD | SD | SD |
| **Expert 2** | | | | | | | |
| R0 | ND | D | ND | SD | SD | SD | SD |
| R1 | HD | ND | ND | SD | ND | ND | ND |
| R2 | SD | ND | SD | SD | ND | D | D |
| R3 | SD | SD | SD | SD | SD | HD | HD |
| R4 | ND | ND | ND | ND | ND | ND | ND |
| R5 | ND | SD | SD | SD | ND | VD | VD |
| R6 | SD | ND | SD | SD | ND | D | D |
| R7 | SD | ND | SD | SD | ND | D | D |
| R8 | SD | ND | ND | SD | ND | ND | ND |
| **Expert 3** | | | | | | | |
| R0 | SD | ND | ND | D | SD | HD | HD |
| R1 | HD | SD | ND | D | ND | VD | D |
| R2 | ND | SD | SD | D | ND | D | D |
| R3 | ND | D | SD | D | SD | ND | SD |
| R4 | SD | SD | ND | ND | ND | VD | VD |
| R5 | SD | D | SD | D | ND | SD | ND |
| R6 | ND | SD | SD | D | ND | D | D |
| R7 | ND | SD | SD | D | ND | D | D |
| R8 | ND | SD | ND | D | ND | VD | VD |

Note: D: Difference, SD: Slight_Difference, ND: No_Difference, VD: Very_Difference, HD: Huge_Difference.

Table 10 and Fig. 5 present the results of three experts who have ranked nine routers (R0 to R8) according to 7 criteria, following which their rankings are listed, and common differences in expert opinion are identified. Router R4 is continuously in the 1st rank (all experts). On the other hand, all of the experts rank router R3 last (9th is the consensus) due to underperformance.

**Table 10:** Individual results

| First expert | | | Second expert | | | Third expert | | |
|---|---|---|---|---|---|---|---|---|
| **Alternatives** | **Score** | **Rank** | **Alternatives** | **Score** | **Rank** | **Alternatives** | **Score** | **Rank** |
| R0 | 0.04647 | 3 | R0 | 0.01671 | 3 | R0 | 0.08997 | 5 |
| R1 | 0.08742 | 6 | R1 | 0.11049 | 7 | R1 | 0.12409 | 8 |
| R2 | 0.08156 | 4 | R2 | 0.08694 | 4 | R2 | 0.08910 | 3 |
| R3 | 0.17427 | 9 | R3 | 0.17470 | 9 | R3 | 0.14806 | 9 |
| R4 | 0.01135 | 1 | R4 | −0.22943 | 1 | R4 | 0.03017 | 1 |
| R5 | 0.13302 | 8 | R5 | 0.13241 | 8 | R5 | 0.09669 | 6 |
| R6 | 0.08910 | 7 | R6 | 0.08694 | 4 | R6 | 0.08910 | 3 |
| R7 | 0.08156 | 4 | R7 | 0.08694 | 4 | R7 | 0.09672 | 7 |
| R8 | 0.03245 | 2 | R8 | −0.08255 | 2 | R8 | 0.05736 | 2 |

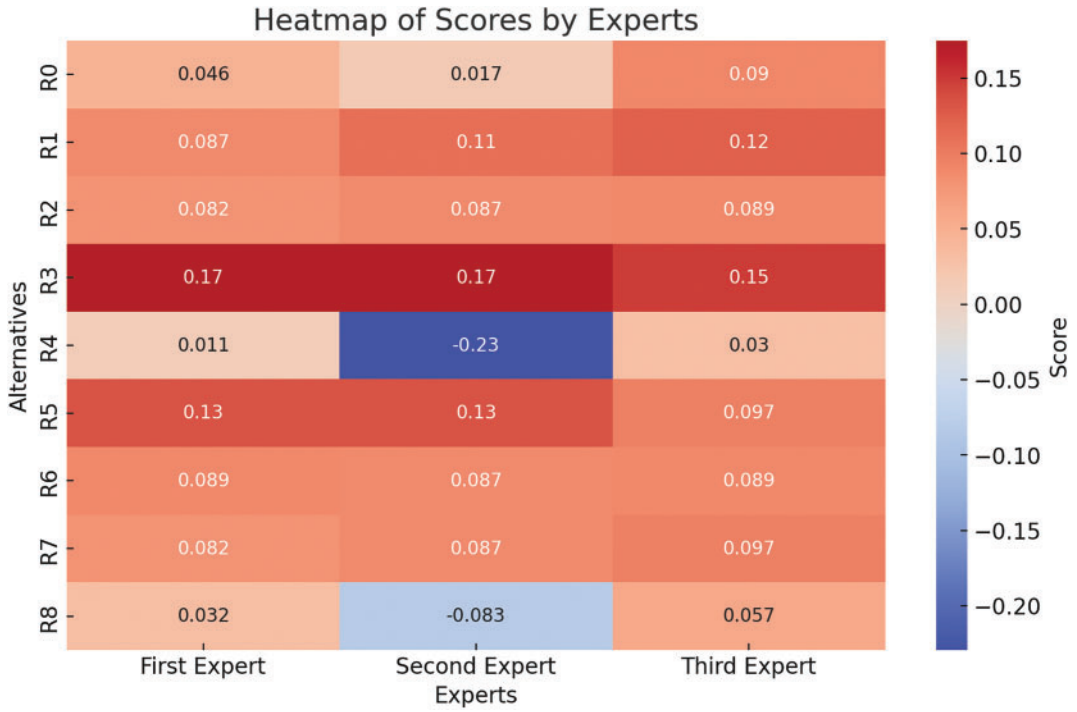


**Figure 5:** Heatmap showing the expert evaluation of alternatives (R0 to R8), where colour intensity represents the magnitude of scores assigned by each expert

For Router R0, the ranking result varies a bit; the first and second experts rank it 3rd, but the third expert ranks it 5th. While R0 performs well overall across criteria, this slight shift seems to suggest a small change of perspective. Although all experts rank Router R1 in 6th to 8th place, this indicates a stable but not too high evaluation, with some experts believing it to be less competitive than the routers lying ahead of them. Routers R2 and R6 show more interesting anomalies. The first and second experts rank R2 as 4th. However, the third expert ranks it in 3rd place, owing perhaps to different weights given to some criteria that different experts prioritize, as shown in Fig. 5. Like R6, there are also rank variations observed, in that 7th place was

reported by the first expert and 4th place is highlighted by the second and third experts, suggesting that R6 may not be tracked well for all necessarily, but could perform well in particular areas preferred by the latter two experts. Although low in the ranking (8th), it has a small improvement in the score of the third expert, to indicate some of its strengths being overwhelmed by its lower overall ranking. Lastly, Router R8 also shows the closest consensus among experts, constantly ranked between 2nd and 3rd.

In addition, there is disagreement amongst the panel of experts; for instance, expert 1 ranked 'R6' lower than experts 2 and 3, while expert 2 ranked it higher. Therefore, we need to unify the opinions of experts. Finally, Table 11 provides a convention of the results of the three experts' efforts to reach a consensus utilizing a group decision-making approach.

**Table 11:** Group ranking results based on SvN-FDOSM

| | **Group of experts** | |
|---|---|---|
| R0 | 0.05105 | 3 |
| R1 | 0.10733 | 7 |
| R2 | 0.08586 | 4 |
| R3 | 0.16567 | 9 |
| R4 | −0.0626 | 1 |
| R5 | 0.12079 | 8 |
| R6 | 0.08838 | 5 |
| R7 | 0.08840 | 6 |
| R8 | 0.00241 | 2 |

The final theoretical ranking results of nine routers (R0 to R8) are provided using the SvN-FDOSM-SNEWA to aggregate evaluations of individual experts into one group decision in Table 10. This is a group decision-making approach in which expert's opinions are aggregated to minimize personal biases and ultimately decide whether a router is good or bad at a collective level. Router R4 is the top-ranked option in the final rankings with an assigned score of −0.0626. It shows that this router meets a critical standard that the entire group values. Router R8 comes next in R4, ranking 2nd with a minimal positive score of 0.00241, which can be considered moderate. Coming in the 4th position is Router R2 with a score of 0.08586, and Router R6 takes the 5th position by scoring 0.08838, preceded in the 3rd position with a score of 0.05105 by Router R0. From this pattern, we speculate that these routers have some properties that always make them good but not necessarily the best for every type of connection. Router R7 consumed the 6th place (score 0.08840), Router R1 consumed the 7th place (0.10733), and Router R5 with the 8th place (0.12079), which shows that these routers have performance limitations according to aggregated criteria by experts. Finally, Router R3 finishes the rankings with the lowest, 9th, and a score of 0.16567. This means that this router has the lowest rankings in the entire group due to consistently poor performance concerning other routers in the criteria the group evaluated.

As shown in Table 10, the group decision approach smooths out fluctuations in individual expert rankings and gives a clearer overall ranking of the routers. This also clarifies routers on which expert group members have strong consensus with high performance ('R4') and those seen as less effective ('R3') to help decision-makers hone in on options that resonate with correlated preferences and performance goals elicited by the expert group. After the order of the alternatives has been identified, there is an urgent need to evaluate the accuracy of these results.

## 5 Validation

Rapid solutions are required for issues with the generalizability of results, and validation provides this. The objective, sensitivity analysis and Spearman correlation coefficient validation approach will be applied. Combining several opinion matrices into a single, unified one and then using that matrix to rank the NoC traffic features. (1) The group's decision results in the opinion matrix are used to sort the NoC traffic features in the opinion matrix. (2) The sorted groups are then divided into equal sections. The mean (x) for each group is then used to infer the results of the group's decision-making, as illustrated in Eq. (14) and Table 12 below:

$$\overline{\boldsymbol{x}} = \frac{\mathbf{1}}{\boldsymbol{n}} \sum_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{x_i} \tag{14}$$

where $\overline{\boldsymbol{x}}$ refers to the arithmetic mean.

**Table 12:** The objective validation result

| Group | Mean |
|---|---|
| 1st group | −0.0030 |
| 2nd group | 0.08755 |
| 3rd group | 0.13124 |

The mean of every group is calculated. The comparison implies that the first group's arithmetic mean should be smaller than or equal to the second group's mean. Similarly, the outcomes of the second group must be less than or equal to those of the third group. Table 12 displays the result of objective validation.

This result demonstrates that groups extended depending on the SvN-FDOSM-SNEWA outcomes to assess and compare the NoC-based MPSoC are true. The second validation method was sensitivity analysis. To enhance the robustness and reliability of the presented methods, sensitivity analysis was conducted, starting with systemically varying the criteria weights to see the effects of the variation on alternatives ranking. The researchers first determined the most relevant criterion. Based on the result provided in Table 8, an analysis was conducted on the weighting of criteria, concluding that "Max Packet Count" is the most influential aspect that should be considered. We increased its weight by 0.5, which is in line with previous academic investigations. Fig. 6 depicts ten probable outcomes based on the study of seven criteria. The weights allocated to the remaining criteria were derived using Eq. (15).

$$w_n : (1 - w_{z1}) = w_n^* : (1 - w_{z1}^*) \tag{15}$$

Fig. 6 presents the sensitivity analysis results conducted to evaluate the influence of changing the weights allocated to the criterion on the ranks of different alternatives. The ranks in the "original" are presented according to the first set of criterion weights. The ranks are displayed in columns labelled scenario 1 to scenario 10 after the weights have been adjusted according to different circumstances. By comparing the rankings in various weights, we can easily observe the final ranks and evaluate how changing the weights provided to the criterion affects them. The objective of performing a sensitivity analysis is to assess the robustness and stability of the rankings by examining how changing the weights affects the relative positions of the alternatives. For instance, in the second scenario, the weights have been altered in a way that is different from the original weights, resulting in a change in the ranks of certain alternatives. Figure is a visual evaluation of rankings in various situations, helping researchers or decision-makers understand how changes

in criteria weights influence the rankings. The final result shows a slight modification in the overall sequence, thus demonstrating the effectiveness of the weighing and ranking strategy.

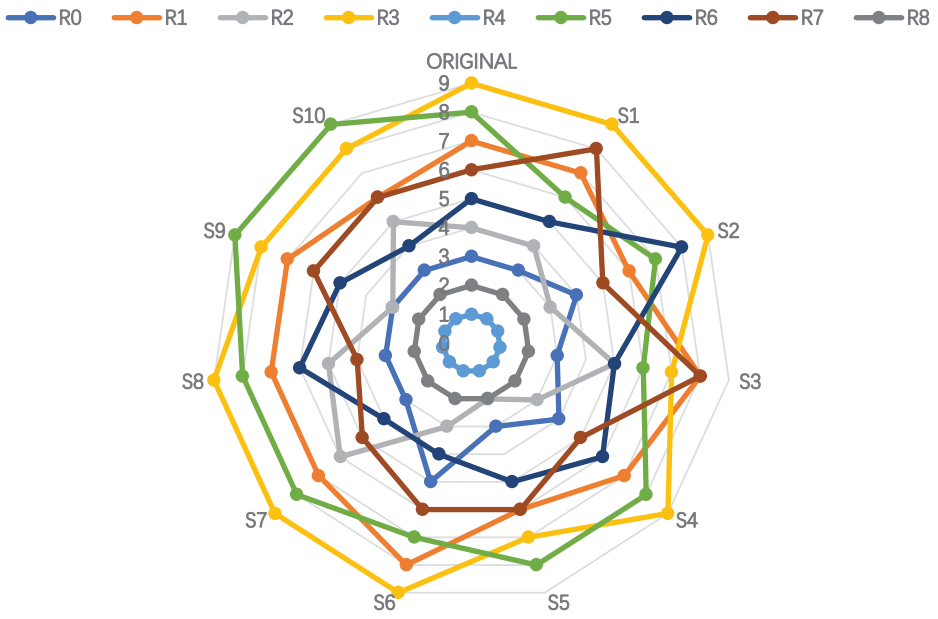


**Figure 6:** Sensitivity analysis

The Spearman technique (Eq. (16)) is used as a third validation method in this study to evaluate the connection between the scenarios. The relative importance of these elements is established by applying a specific calculation, which then determines their ranking. By utilizing Spearman's rank correlation, researchers may gain useful insights into the relative relevance and influence of different aspects under investigation. The Spearman rank correlation coefficient quantitatively measures the consistency of rankings between various scenarios. It is a statistical measure of the degree of correlation between the rankings of each scenario and an original ranking. A high Spearman correlation coefficient (close to 1) shows the model is consistent in ranking in the presence of weight variations; in other words, the model is resilient. Fig. 7 shows the Spearman's rank correlation.

$$r_s = 1 - \frac{6 \sum_i d_i^2}{n^3 - n} \tag{16}$$

For instance, the Spearman correlation coefficient we obtained was always above 0.87, even with the variation of weights up to 20%, indicating that the proposed methods behave well. The relative importance of these elements is established by applying a specific calculation, which then determines their ranking. By utilizing Spearman's rank correlation, researchers may gain useful insights into the relative relevance and influence of different aspects under investigation. Results are shown in Fig. 7 for the ranking of alternatives, where the lowest value was 87%, and the highest value was 100%. Moreover, not only does this sensitivity analysis confirm the stability of the FWZIC and FDOSM methods, but it also confirms their effectiveness in ensuring reliable rankings. The insights of this analysis allow decision-makers to use the methods in dynamic or uncertain settings with surety that the results are robust to reasonable changes in the input parameters.

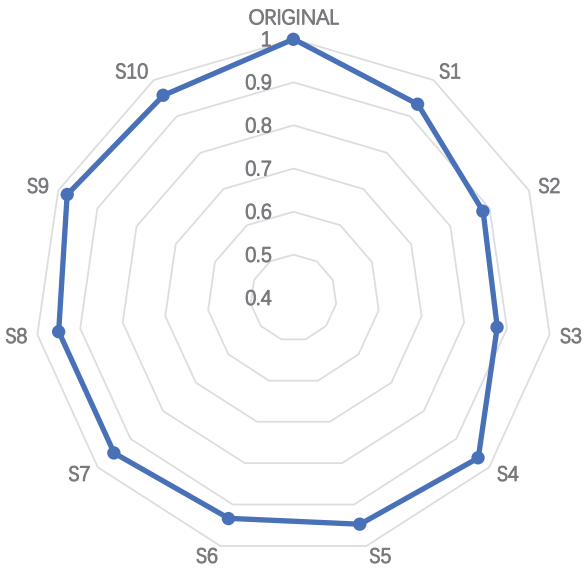


**Figure 7:** Spearman's rank correlation

## 6 Comparison Analysis

Multiple widely recognized MCDM algorithms operate on SvN numbers. This section compares these algorithms, focusing on SvN-FDOSM-SNAWA, which has been preferred over other approaches. The comparison highlights the resilience of SvN-FDOSM-SNAWA. To begin, TOPSIS is a well-known MCDM methodology that has been extensively used in various applications and is considered one of the top methods. However, the basic form of TOPSIS is affected by uncertainty, and an extension called fuzzy SvN number TOPSIS (SvN-TOPSIS) [49] has been developed using the same SvN fuzzy number employed in SvN-FDOSM-SNAWA. SvN-TOPSIS incorporates SvN fuzzy numbers to address uncertainty, but it retains the fundamental drawback of the original TOPSIS, which requires external sources to provide preference weights. In the same way, the SvN integration with VIKOR is used to address uncertainty [22].

SvN-FDOSM-BM outperforms SvN-TOPSIS in several aspects: 1) Handling missing data. 2) Dealing with immeasurable criteria. 3) Generating criteria weights. 4) Normalizing data involves unifying data from different scales and types in the decision matrix. 5) Determining the ideal solution (best value under the same criterion) and measuring the distance between the ideal solution and other alternatives. 6) Managing ambiguous or unclear data (fuzziness). Table 13 shows the compassion.

**Table 13:** Comparison with SvN-TOPSIS and SvN-VIKOR

| No. | Comparison issue | SvN-FDOSM | SvN-VIKOR | SvN-TOPSIS |
|---|---|---|---|---|
| 1 | Handling missing data | √ | × | × |
| 2 | Dealing with immeasurable criteria | √ | × | × |
| 3 | Generating criteria weights | × | × | × |
| 4 | Normalizing data | √ | √ | √ |
| 5 | Determining the ideal solution | √ | × | × |
| 6 | Managing ambiguous or unclear data | √ | √ | √ |

These details are presented in Table 13, which demonstrates that SvN-FDOSM-SNAWA shows greater resilience compared to SvN-TOPSIS and SvN-VIKOR for assessing and benchmarking routers. Furthermore, while TOPSIS addresses ambiguous information and normalization with a limited scope (n = 2/6), SnV-FDOSM-SNWEA tackles all of the challenges mentioned above comprehensively, except weighting criteria (n = 5/6).

Similarly, the classic AHP (Analytic Hierarchy Process) is a well-known MCDM approach that suffers from ambiguity and uncertainty in its original form. The SvN was utilized to augment this approach and overcome the latter problem. SvN-AHP was introduced as an extension to address uncertainty. However, SvN-AHP [50] still has limitations compared to SvN-FWZIC, including the number of comparisons required, nature of comparisons, rank task, inconsistency issues, and the rank process. These problems are listed in Table 14.

**Table 14:** Comparison between SvN-FDOSM and SvN-AHP

| No. | Comparison issue | SvN-FWZIC | SvN-AHP |
|---|---|---|---|
| 1 | Number of comparisons | (n – 1) The comparison minimum number is 1 | [n (n – 1)/2] |
| 2 | Nature of comparisons | Similar quantities | Several quantities have been used in this weight situation, whereas the exact amounts have been used in the ranking process. |
| 3 | Rank process | Easier | Complicated |
| 4 | Inconsistency problem | Solved | The most challenging task at hand. |
| 5 | Feedback from experts | It takes less time. | It takes more time. |
| 6 | Final rank | It's a higher degree of rationality and alignment with the perspective DM. | It is reliant on assigning weights to the decision criteria. |

Considering these comparisons, it becomes evident that SvN-FWZIC is more robust than SvN-AHP for evaluating and benchmarking, which is why it was used in our work.

## 7 Practical Implications and Future Directions

In the context of the practical implications, the results of this work offer valuable insights for designing countermeasure strategies for F-DoSA in NoC-based MPSoC architecture systems. This paper identifies Max Packet Count as the most significant traffic feature in the study to show that it should best be used in developing mechanisms for invasion detection. The routers' ranking, especially Router 4 as the best performing and Router 3 as the worst performing, provides practical information that could enhance routing algorithms and router hardware in real-world NoC practice. Such outcomes are highly desirable for IoT platforms since improving the platform's tolerance to F-DoSA is relevant to vital industries, including healthcare, autonomous systems, and smart infrastructure. Nevertheless, the study also recognizes some limitations, such as the sensitivity nature of FDOSM to the number of experts, which may lead to bias

or computational time. Further, concerning uncertainty, the elements described in SvN-FWZIC and SvN-FDOSM offer the validation of the uncertainty element; however, it is also possible to use other approaches based on fuzzy sets, such as Intuitionistic Fuzzy Sets or Pythagorean Fuzzy Sets. The research also provides a concrete methodology for the analysis of NoC routers. Still, in future, one can consider the analysis of adaptive defence measures, other approaches to aggregation, such as Bonferroni, or a study of the algorithms at larger systems or the different types of more sophisticated attacks. These improvements would extend the potential of the practicality of the results of this research, especially in providing security for communication in IoT-based MPSoC systems for smart cities, healthcare Internet of Things, and industrial automation.

Alternatively, as a future direction for enhancing FDOSM for Practical Applications, some samples of applications include the usage of higher-order fuzzy sets such as M-Polar or cloud-based surroundings for enhanced ambiguity treatment and adaptive mechanisms as real-time protection means of dynamic threats. Managing uncertainty using other aggregation methods like Bonferroni will likely improve the existing results, and extending the approach to larger NoC systems will promote its effectiveness. Industrial applications include smart city protection, IoT data of the healthcare sector, and reliability of industrial automation.

## 8 Conclusion

The research endeavours encompassed an extensive evaluation of NoC-based MPSoC traffic features under F-DoSA. The evaluation process was conducted utilizing pioneering multiple-criteria decision-making methods known as SvN-FWZIC and SvN-FDOSM, which offered a novel approach to assessing the effectiveness and suitability of various NoC routers. The research methodology was structured into three phases, each serving a specific purpose. These phases were visually represented in Fig. 2, facilitating a clear understanding of the research process. The first phase involved the construction of a decision matrix for the 9 NoC routers as alternatives and seven traffic features as criteria. In the second phase, a meticulous process of criteria weighting was conducted using the SvN-FWZIC method. This step aimed to assign appropriate weights to the decision-making criteria, considering their relative significance and impact. By employing the SvN-FWZIC method, comprehensive and well-balanced weighting criteria were used in the third phase. The result of this phase indicates that the Max Packet Count with a weight value (0.1946) is the highest importance criterion, while the Hop count is the lowest criterion with a weight value (0.1090). Moreover, the third phase involved ranking NoC routers using the SvN-FDOSM method. This method, tailored specifically for evaluating NoC routers within MPSoCs-based IoT, provided a systematic and robust approach to prioritizing and comparing the NoC routers. The final result of this study shows that R4 was in the first step, while R3 was the worst.

A rigorous validation process was implemented to ensure the reliability and validity of the evaluation results. The key contribution of this research lies in developing and proposing an evaluation framework that addresses the complex challenge of selecting the optimal NoC router that affects the context of MPSoCs-based IoT. In addition, this investigation offered a new version by combining SvN with FDOSM and FWZIC to overcome uncertainty issues in weighting and ranking. This research expanded the understanding of communication security in MPSoCs-based IoT. It provided a practical and effective framework for researchers and practitioners to make informed decisions regarding the NoC router testing during the F-DoS attack scenario. Some limitations of the proposed extension are considered. However, the effectiveness of FDOSM is extremely sensitive to the number of experts. Bias may result from only a limited number of experts, and a large number can increase computational complexity and make it harder to get consensus. Second, the model uses SvN as it provides a means to capture truth, indeterminacy, and falsity. However, such capabilities of capturing uncertainty and incomplete knowledge could be replicated using any fuzzy sets generalization, like Intuitionistic Fuzzy Sets (IFS) or Pythagorean Fuzzy Sets (PFS). In addition, other

methods of aggregation can used with FDOSM and FWZIC, such as Bonferroni. For future research directions, investigate adaptive defence mechanisms. In addition, different fuzzy set techniques, including M-Polar, D number, and cloud environment, may be executed with FWZIC and/or FDOSM to explore the ability of these kinds of fuzzy sets to address the ambiguity issue.

**Acknowledgement:** None.

**Funding Statement:** The authors received no specific funding for this study.

**Author Contributions:** The authors confirm contribution to the paper as follows: Ahmed Abbas Jasim Al-Hchaimi: conceptualization, methodology development, supervision and oversight, and drafting the manuscript; Yousif Raad Muhsen: data collection and preparation, statistical analysis, and manuscript review and editing; Wisam Hazim Gwad: literature review, methodology refinement, writing—review & editing; Entisar Soliman Alkayal: experimental design, data validation and visualization; Riyadh Rahef Nuiaa Al Ogaili: approach analysis, implementation, testing, and results interpretation; Zaid Abdi Alkareem Alyasseri: formal analysis and results interpretation; Alhamzah Alnoor: resources and materials contribution and final review and approval of manuscript. All authors reviewed the results and approved the final version of the manuscript.

**Availability of Data and Materials:** The dataset used in this project, which includes NoC traffic data for both normal and malicious simulation scenarios, will be made available upon request to the corresponding authors.

**Ethics Approval:** Not applicable.

**Conflicts of Interest:** The authors declare no conflicts of interest to report regarding the present study.

## References

1. Husin NA, Zolkepli MB, Manshor N, Al-Hchaimi AAJ, Albahri AS. Routing techniques in network-on-chip based multiprocessor-system-on-chip for IoT: a systematic review. Iraqi J Comput Sci Math. 2024;5:181–204.
2. Wang H, Halak B. TampML: tampering attack detection and malicious nodes localization in NoC-based MPSoC. IEEE Trans Emerg Top Comput. 2024;2:1–12. doi:10.1109/TETC.2024.3434663.
3. Andreu P, Alcaide S, Lopez P, Abella J, Hernandez C. Expanding SafeSU capabilities by leveraging security frameworks for contention monitoring in complex SoCs. Futur Gener Comput Syst. 2025;163(5):107518. doi:10.1016/j.future.2024.107518.
4. Muhsen YR, Husin NA, Zolkepli MB, Manshor N, Al-Hchaimi AAJ, Ridha HM. Enhancing NoC-based MPSoC performance: a predictive approach with ANN and guaranteed convergence arithmetic optimization algorithm. IEEE Access. 2023;11:90143–57. doi:10.1109/ACCESS.2023.3305669.
5. Al-Hchaimi AAJ, Alaidi AHM, Muhsen YR, Alomari MF, Sulaiman NBin, Romdhini MU. Optimizing energy and QoS in VANETs through approximate computation on heterogeneous MPSoC. In: Proceedings of the 2024 4th International Conference on Emerging Smart Technologies and Applications (eSmarTA); 2024; Sana'a, Yemen: IEEE. p. 1–6.
6. Wang H, Ren J, Halak B, Atamli A. GNS: graph-based network-on-chip shield for early defense against malicious nodes in MPSoC. IEEE J Emerg Sel Top Circuits Syst. 2024;14(3):483–94. doi:10.1109/JETCAS.2024.3438435.
7. Nagalaxmi T, Rao ES, ChandraSekhar P. FPGA-based implementation and verification of hybrid security algorithm for NoC architecture. Analog Integr Circuits Signal Process. 2024;121(1–3):1–11. doi:10.1007/s10470-024-02290-z.
8. Chatterjee U. Door Knock: reverse engineering the MPSoC layout through timing attack on NoC. IEEE Embed Syst Lett. 2024;16(4):449–52. doi:10.1109/LES.2024.3371106.
9. Sankar S, Gupta R, Jose J, Nandi S. TROP: TRust-aware OPportunistic Routing in NoC with Hardware Trojans. ACM Trans Des Autom Electron Syst. 2024;29(2):1–25. doi:10.1145/3639821.

10. Faccenda RF, Comarú G, Caimi LL, Moraes FG. A comprehensive framework for systemic security management in NoC-based many-cores. IEEE Access. 2023;11:131836–47. doi:10.1109/ACCESS.2023.3336565.
11. Liu S, Chauhan S, Karanth A. SNAC: mitigation of snoop-based attacks with multi-tier security in NoC architectures. In: Proceedings of the Great Lakes Symposium on VLSI 2024; 2024; Clearwater, FL, USA. p. 560–3.
12. Alqaysi ME, Albahri AS, Hamid RA. Hybrid diagnosis models for autism patients based on medical and sociodemographic features using machine learning and multicriteria decision-making (MCDM) techniques: an evaluation and benchmarking framework. Comput Math Methods Med. 2022;2022:1–19. doi:10.1155/2022/9410222.
13. Albahri OS, Zaidan AA, Albahri AS, Alsattar HA, Mohammed R, Aickelin U, et al. Novel dynamic fuzzy Decision-Making framework for COVID-19 vaccine dose recipients. J Adv Res. 2022;37(7821):147–68. doi:10.1016/j.jare.2021.08.009.
14. Alamoodi AH, Albahri OS, Zaidan AA, AlSattar HA, Ahmed MA, Pamucar D, et al. New extension of fuzzy-weighted zero-inconsistency and fuzzy decision by opinion score method based on cubic pythagorean fuzzy environment: a benchmarking case study of sign language recognition systems. Int J Fuzzy Syst. 2022;24:1–18.
15. Pamučar D, Stević Ž, Sremac S. A new model for determining weight coefficients of criteria in MCDM models: full consistency method (FUCOM). Symmetry. 2018;10(9):393. doi:10.3390/sym10090393.
16. Žižović M, Pamucar D. New model for determining criteria weights: level based weight assessment (LBWA) model. Decis Mak Appl Manag Eng. 2019;2(2):126–37. doi:10.31181/dmame1902102z.
17. Pamucar D, Deveci M, Gokasar I, Işık M, Zizovic M. Circular economy concepts in urban mobility alternatives using integrated DIBR method and fuzzy Dombi CoCoSo model. J Clean Prod. 2021;323(1):129096. doi:10.1016/j.jclepro.2021.129096.
18. Salih MM, Zaidan BB, Zaidan AA. Fuzzy decision by opinion score method. Appl Soft Comput J. 2020;96(1):106595. doi:10.1016/j.asoc.2020.106595.
19. Smarandache F. Neutrosophic set—a generalization of the intuitionistic fuzzy set. Int J Pure Appl Math. 2005;24:287.
20. Borah G, Dutta P. Fuzzy risk analysis in crop selection using information measures on quadripartitioned single-valued neutrosophic sets. Expert Syst Appl. 2024;255(1):124750. doi:10.1016/j.eswa.2024.124750.
21. Wang J, Zhang X. Two types of single valued neutrosophic covering rough sets and an application to decision making. Symmetry. 2018;10(12):710. doi:10.3390/sym10120710.
22. Luo X, Wang Z, Yang L, Lu L, Hu S. Sustainable supplier selection based on VIKOR with single-valued neutrosophic sets. PLoS One. 2023;18(9):e0290093. doi:10.1371/journal.pone.0290093.
23. Chai JS, Selvachandran G, Smarandache F, Gerogiannis VC, Son LH, Bui Q-T, et al. New similarity measures for single-valued neutrosophic sets with applications in pattern recognition and medical diagnosis problems. Complex Intell Syst. 2021;7(2):703–23. doi:10.1007/s40747-020-00220-w.
24. Zhao Y, Wang X, Jiang Y, Wang L, Yang M, Singh AK, et al. On hardware-trojan-assisted power budgeting system attack targeting many core systems. J Syst Archit. 2020;109(2):101757. doi:10.1016/j.sysarc.2020.101757.
25. Reinbrecht C, Aljuffri A, Hamdioui S, Taouil M, Forlin B, Sepulveda J. Guard-NoC: a protection against side-channel attacks for MPSoCs. In: Proceedings of the 2020 IEEE Computer Society Annual Symposium on VLSI (ISVLSI); 2020; Limassol, Cyprus: IEEE. p. 536–41.
26. Fernandes R, Marcon C, Cataldo R, Sepulveda J. Using smart routing for secure and dependable NoC-based MPSoCs. IEEE/ACM Trans Netw. 2020;28(3):1158–71. doi:10.1109/TNET.2020.2979372.
27. Nuiaa RR, Alsaidi SAAA, Mohammed BK, Alsaeedi AH, Alyasseri ZAA, Manickam S, et al. Enhanced PSO algorithm for detecting DRDoS attacks on LDAP servers. Int J Intell Eng Syst. 2023;16(5):728–36. doi:10.22266/ijies2023.1031.61.
28. Shahrani AMAl, Rizwan A, Algarni A, Alissa KA, Shabaz M, Singh BK, et al. A deep learning network-on-chip (NoC)-based switch-router to enhance information security in resource-constrained devices. J Circuits Syst Comput. 2024;33(4):2450064. doi:10.1142/S0218126624500646.
29. Wang H, Halak B. Hardware trojan detection and high-precision localization in NoC-based MPSoC using machine learning. In: Proceedings of the 28th Asia and South Pacific Design Automation Conference; 2023; Tokyo, Japan. p. 516–21.

30. Sudusinghe C, Charles S, Mishra P. Denial-of-service attack detection using machine learning in network-on-chip architectures. In: Proceedings of the 15th IEEE/ACM International Symposium on Networks-on-Chip; 2021; Clearwater, FL, USA. p. 35–40.
31. Hu S, Wang H, Halak B. Cascaded machine learning model based DoS attacks detection and classification in NoC. In: Proceedings of the 2023 IEEE International Symposium on Circuits and Systems (ISCAS); 2023; Monterey, CA, USA: IEEE. p. 1–5.
32. Sudusinghe C, Charles S, Ahangama S, Mishra P. Eavesdropping attack detection using machine learning in network-on-chip architectures. In: Proceedings of the 16th IEEE International Symposium on Networks-on-Chip (NOCS); 2022. p. 21–8.
33. Sinha M, Gupta S, Rout SS, Deb S. Sniffer: a machine learning approach for DoS attack localization in NoC-based SoCs. IEEE J Emerg Sel Top Circuits Syst. 2021;11(2):278–91. doi:10.1109/JETCAS.2021.3083289.
34. Vashist A, Keats A, Dinakarrao SMP, Ganguly A. Securing a wireless network-on-chip against jamming-based denial-of-service and eavesdropping attacks. IEEE Trans Very Large Scale Integr Syst. 2019;27(12):2781–91. doi:10.1109/TVLSI.2019.2928960.
35. Chaves CG, Sepúlveda J, Hollstein T. Lightweight monitoring scheme for flooding DoS attack detection in multi-tenant MPSoCs. In: Proceedings of the 2021 IEEE International Symposium on Circuits and Systems (ISCAS); 2021; Daegu, Republic of Korea: IEEE. p. 1–5.
36. Sepúlveda J. Secure cryptography integration: NoC-based microarchitectural attacks and countermeasures. In: Network-on-chip security and privacy. USA: Springer; 2021. p. 153–79.
37. Al-Samarraay MS, Salih MM, Ahmed MA, Zaidan AA, Albahri OS, Pamucar D, et al. A new extension of FDOSM based on Pythagorean fuzzy environment for evaluating and benchmarking sign language recognition systems. Neural Comput Appl. 2022;34(6):4937–55. doi:10.1007/s00521-021-06683-3.
38. Al-Hchaimi AAJ, Sulaiman NB, Mustafa MAB, Mohtar MNB, Mohd Hassan SLB, Muhsen YR. A comprehensive evaluation approach for efficient countermeasure techniques against timing side-channel attack on MPSoC-based IoT using multi-criteria decision-making methods. Egypt Informatics J. 2023;24(2):351–64. doi:10.1016/j.eij.2023.05.005.
39. Al-Hchaimi AAJ, Sulaiman NB, Mustafa MAB, Mohtar MNB, Mohd SLB, Muhsen YR. Evaluation approach for efficient countermeasure techniques against denial-of-service attack on mpsoc-based iot using multi-criteria decision-making. IEEE Access. 2022;11:89–106.
40. Talal M, Tan MLP, Pamucar D, Delen D, Pedrycz W, Simic V. Evaluation and benchmarking of research-based microgrid systems using FWZIC-VIKOR approach for sustainable energy management. Appl Soft Comput. 2024;166(2):112132. doi:10.1016/j.asoc.2024.112132.
41. Zaidan AA, AlSattar HA, Qahtan S, Deveci M, Pamucar D, Gupta BB. Secure decision approach for internet of healthcare things smart systems-based blockchain. IEEE Internet Things J. 2023;10(24):21647–55. doi:10.1109/JIOT.2023.3308953.
42. Sakthivel AD, Augustin F. Fuzzy APPSS: a novel method for quantifying COVID-19 impact in India under triangular spherical fuzzy environment. Sci Rep. 2024;14(1):30961. doi:10.1038/s41598-024-82046-x.
43. Puška A, Štilić A, Pamucar D, Simic V, Petrović N. Optimal selection of healthcare waste treatment devices using fuzzy-rough approach. Environ Sci Pollut Res. 2024;2(4):1–20. doi:10.1007/s11356-024-32630-5.
44. Mohammed RT, Zaidan AA, Yaakob R, Sharef NM, Abdullah RH, Zaidan BB, et al. Determining importance of many-objective optimisation competitive algorithms evaluation criteria based on a novel fuzzy-weighted zero-inconsistency method. Int J Inf Technol Decis Mak. 2022;21(1):195–241. doi:10.1142/S0219622021500140.
45. Alamoodi AH, Mohammed RT, Albahri OS, Qahtan S, Zaidan AA, Alsattar HA, et al. Based on neutrosophic fuzzy environment: a new development of FWZIC and FDOSM for benchmarking smart e-tourism applications. Complex Intell Syst. 2022;8(4):3479–503. doi:10.1007/s40747-022-00689-7.
46. Qahtan S, Alsattar HA, Zaidan AA, Deveci M, Pamucar D, Delen D, et al. Evaluation of agriculture-food 4.0 supply chain approaches using Fermatean probabilistic hesitant-fuzzy sets based decision making model. Appl Soft Comput. 2023;138:110170. doi:10.1016/j.asoc.2023.110170.

47. Mei Y, Yang J, Chen B. Multi-criteria group decision-making method based on an improved single-valued neutrosophic hamacher weighted average operator and grey relational analysis. J Comput Commun. 2023;11(3):167–88. doi:10.4236/jcc.2023.113013.
48. Haq RSU, Saeed M, Mateen N, Siddiqui F, Naqvi M, Yi JB, et al. Sustainable material selection with crisp and ambiguous data using single-valued neutrosophic-MEREC-MARCOS framework. Appl Soft Comput. 2022;128(22858):109546. doi:10.1016/j.asoc.2022.109546.
49. Zeng S, Luo D, Zhang C, Li X. A correlation-based TOPSIS method for multiple attribute decision making with single-valued neutrosophic information. Int J Inf Technol Decis Mak. 2020;19(1):343–58. doi:10.1142/S0219622019500512.
50. Zaidan AA, Alsattar HA, Qahtan S, Deveci M, Pamucar D, Hajiaghaei-Keshteli M. Uncertainty decision modeling approach for control engineering tools to support industrial cyber-physical metaverse smart manufacturing systems. IEEE Syst J. 2023;17(4):5303–14. doi:10.1109/JSYST.2023.3266842.