

RESEARCH ARTICLE

CITE-PSO: Cross-ISP Traffic Engineering Enhanced by Particle Swarm Optimization in Blockchain Enabled SDNs

EVFRIM GULER 

Department of Computer Engineering, Bartın University, 74100 Bartın, Turkey

e-mail: evrimguler@bartin.edu.tr

This work is supported by the Scientific & Technological Research Council of Türkiye (TUBITAK) under Grant No. 120E448.


ABSTRACT The immense potential of optical networks provides a highly favorable option for addressing rapidly increasing bandwidth needs. Elastic Optical Networks (EONs) exhibit considerable potential in enhancing availability, failure resilience, load balancing, and efficient resource allocations, rendering them a viable option for forthcoming high-speed networks. The integration of Software-Defined Networking (SDN) architecture with EONs, which separates the data and control planes, results in a dynamic and cooperative combination known as Software-Defined Optical Networking (SDON). However, the effective allocation of spectrum poses operational difficulties in this context. The proposed study introduces a framework called Cross-ISP (Internet Service Provider) Traffic Engineering enhanced by Particle Swarm Optimization (CITE-PSO) that is designed to facilitate Quality of Service (QoS)-focused cross-ISP spectrum assignment in SDONs through the integration of blockchain technology. The proposed framework aims to eliminate the need for centralized mediators while ensuring effective coordination of inter-ISP traffic based on QoS considerations. The research presents a novel application of blockchain technology that increases network efficiency and minimizes QoS signaling overhead during inter-ISP routing in SDONs. The proposed framework is evaluated under Hop-by-Hop Wavelength Switching (HWS) and Border-Node-Only Wavelength Switching (BWS) to assess its performance. The simulation results demonstrate that the *CITE-PSO* framework is proficient in managing the inter-ISP routing with QoS capabilities in the SDON architecture. This proficiency is measured by the various metrics across HWS and BWS scenarios.

INDEX TERMS Particle swarm optimization, SDON, blockchain, cross-ISP, QoS, wavelength switching.

I. INTRODUCTION

Communication networks serve as the backbone of modern societies, facilitating seamless data exchange and supporting a vast array of applications and services in today's hyper-connected world. The exponential growth of data and information in the global landscape has been unprecedented, with the total volume of created, captured, copied, and consumed data reaching a staggering 64.2 Zettabytes (ZB) in 2020. As depicted in Fig. 1, the forecasts indicate that this immense analysis is projected to triple, reaching an estimated 181 ZB by 2025 [1]. This remarkable surge can be attributed to the rapid proliferation of hyper-connected

devices and users, whose demands emanate from various sectors, including businesses, connected-homes, and smart environments. The driving force behind this escalating demand is the need for new and enhanced services, such as high-definition video, video-conferencing, Voice-over-IP (VoIP), and online gaming, which have become integral aspects of modern-day communication and interaction paradigms. Traditional networking architectures face numerous challenges when adapting to modern applications and services' dynamic and diverse needs [2]. Inter-network routing plays a pivotal role in ensuring efficient and reliable communication between disparate network domains. One critical aspect of inter-network routing is Traffic Engineering (TE), which involves the optimization of traffic flow to maximize network performance, resource utilization, and

The associate editor coordinating the review of this manuscript and approving it for publication was Tiago Cruz .

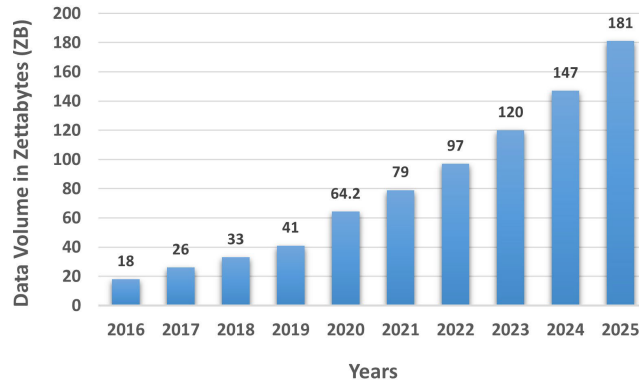


FIGURE 1. Amount of data created, consumed, and stored with forecasts to 2025 [1].

Quality of Service (QoS). Effectively managing the diverse and dynamic nature of traffic patterns while meeting the stringent QoS requirements of various applications remains a complex challenge.

Blockchain (BC) technology, characterized by its decentralized and distributed ledger system, offers a crucial option for Internet Service Providers (ISPs) who aim to achieve safe and transparent information exchange while focusing on QoS and resource utilization [3]. The decentralized nature of blockchain reduces the chance of a single point of failure, increasing overall network resilience and reliability, which is crucial for sustaining constant QoS. BC's cryptographic links and consensus procedures make possible records that cannot be changed. This protects the integrity of transactions that involve using resources and QoS metrics. The BC's transparency encourages confidence among ISPs and gives a common perspective on resource usage, enabling collaborative efforts for efficient resource utilization. Blockchain provides a safe, transparent, and efficient framework for secure communication and collaboration while meeting QoS and resource utilization needs [4].

In the context of Cross-ISP Traffic Engineering (CITE) with a focus on QoS-based routing, the integration of BC technology emerges as a crucial necessity. The pivotal role of BC nodes in the overarching framework illustrates a strategic approach to address the intricacies of secure data exchange in a multi-ISP scenario. Leveraging BC for secure data exchange becomes foundational, ensuring the robustness and reliability required in the complex landscape of cross-ISP interactions. As the network controllers of each optical ISP become BC nodes, they assume responsibility for managing their BC instantiation, including the essential cryptographic keys. The process of establishing secure connections between ISP controllers, facilitated by the exchange of public keys and ISP Numbers (ISPN), adds an extra layer of trust and confidentiality. The optical networking data, a linchpin in cross-ISP QoS-based routing, is fortified through cryptographic signatures. The need for BC in QoS-based cross-ISP routing framework becomes evident as it ensures decentralization, tamper-resistance, and heightened security, addressing the nuanced challenges of secure data exchange

while fostering an environment of trust and reliability in the intricate domain of cross-ISP interactions [5].

To address the intricacies of CITE, this paper proposes a novel approach leveraging Particle Swarm Optimization (PSO) within the context of Software-Defined Optical Networking (SDON) enabled by BC technology. SDON, an extension of Software Defined Networking (SDN) into the optical domain, provides centralized control and programmability, offering unprecedented flexibility in managing optical networks. Meanwhile, the decentralized and immutable nature of BC technology enhances data sharing and fosters transparency and trust among network entities. By harnessing the power of PSO in a BC-enabled SDON environment, this study seeks to optimize traffic engineering decisions, thereby improving QoS, enhancing network resource efficiency, and ensuring seamless communication between interconnected networks.

A. MOTIVATION

In high-speed and high-capacity environments, flexible/elastic optical networks require efficient resource allocation to meet diverse QoS requirements [6]. The adoption of QoS-based routing becomes crucial for managing traffic flow intelligently, prioritizing data types, and delivering differentiated services, especially for real-time applications. Simultaneously, effective spectrum assignment is vital to optimize the utilization of finite and costly spectral resources, mitigating interference and signal degradation [7].

Despite the significance of QoS-based Routing and Spectrum Assignment (RSA), challenges arise due to the dynamic nature of network traffic, diverse QoS requirements, and scalability concerns. The proposed solution involves leveraging SDON, which applies SDN principles to provide a flexible and programmable network infrastructure. SDON's decoupling of the control plane from the data plane allows centralized network management and programmability. This dynamic control enhances the efficiency of QoS-based routing decisions, ensuring that traffic is directed along paths that meet diverse application QoS requirements. Additionally, SDON seamlessly integrates with QoS-based RSA techniques, optimizing spectrum allocation dynamically based on traffic demands and QoS objectives, thus maintaining consistent service quality amid changing traffic conditions [8].

In the realm of multi-ISP networks under the consideration of End-to-End (E2E) routing, BC technology emerges as a valuable tool. BC's unique features, including data sharing, immutability, transparency, and decentralization, can significantly enhance QoS-based inter-network RSA. BC facilitates secure and reliable data sharing among network nodes, enabling real-time exchange of traffic information, congestion levels, and QoS requirements [3], [9]. The immutability of data on the BC ensures the integrity and accuracy of shared information, preventing tampering and enhancing trustworthiness. BC's transparency allows

participants to verify and validate QoS metrics in routing decisions, promoting openness and accountability [10], [11]. In the spectrum assignment context, BC's decentralization facilitates a democratic and fair spectrum allocation process, enabling nodes to negotiate and bid for spectrum resources based on QoS requirements and preferences [12]. BC's transparent and auditable nature ensures that all spectrum assignment decisions are recorded and accessible, fostering trust and cooperation among network operators. Leveraging BC technology in multi-ISP E2E routing can achieve greater efficiency, fairness, and trust, contributing to the resource optimization of flexible networks.

B. CONTRIBUTION AND ORGANIZATION

The study introduces the use of PSO, a nature-inspired optimization technique, in Blockchain-enabled SDN to improve Cross-ISP Traffic Engineering (CITE) decision-making. This approach allows the network to dynamically adjust routing policies and QoS parameters, ensuring high service quality. The adoption of BC technology in SDN ensures secure, transparent data-sharing among network entities, enhancing trust and cooperation between ISPs. The decentralized nature of blockchain allows for fair spectrum assignment, optimizing resource utilization, and mitigating biases in the process. The contributions of this research can be given as follows:

- This paper experiences the Cross-ISP Traffic Engineering enhanced by Particle Swarm Optimization (*CITE-PSO*) framework under Hop-by-Hop Wavelength Switching (HWS) and Border-Node-Only Wavelength Switching (BWS) scenarios to analyze its performance. The *CITE-PSO* employs a feasible path selection strategy to assign an E2E path for service requests while providing the highest value on the respective QoS parameter specified in the priority field of the request.
- The performance of the proposed *CITE-PSO* framework is evaluated and compared against three QoS-based routing strategies in SDN networks: SpectrumChain (*SC*) [5], Hierarchical Routing Approach (*HRA*) [13], and Distributed Routing Approach (*DRA*).
- In this study, NSFNET, US Backbone, Random-14, and Random-24 topologies are used to set up the networks at the inter-network level for network connectivity as an overlay network.
- The research uses Path Setup Time (PST), Network Message Overhead (NMO), Service Acceptance Ratio (SAR), Network Resource Consumption (NRC), Average Path Length (APL), and Network Path Length (NPL) metrics to conduct a comprehensive analysis on the performance of the proposed *CITE-PSO* framework.

This paper's organization is as follows: Section II presents state-of-the-art regarding routing/QoS in SDN and BC. Section III defines the system model of network infrastructure, and Tables 2 – 3 show the terminology and notation tables, respectively. Section IV presents the *CITE-PSO* framework along with basic terms, processes, functionalities,

and concepts related to both networking and BC. Section V provides the experimental results. Section VI discusses open problems and future research directions emanating from our vision before the concluding remarks in Section VII.

II. RELATED WORK

Many applications have harnessed BC technology, encompassing diverse fields such as the Internet of Things (IoT), cloud computing, supply chains, and healthcare systems. Several research studies [14], [15], [16], [17], [18], [19] have extensively explored BC-based routing frameworks within single domains in the literature. However, a notable research gap persists, as none of these studies have delved into QoS-based E2E path setup frameworks tailored for multi-network scenarios within SDN ISPs.

A blockchain-based architecture is put up by [20] to improve the security and privacy of communication between unmanned aerial vehicles and wireless base stations. The work presents a revised Particle Swarm Optimization (PSO) technique for selecting the most efficient path, specifically targeting path deviation attacks and path loss problems. The authors in [21] specifically examine the incorporation of Internet of Things (IoT) devices into the blockchain. The authors suggest a more advanced combination of structures and a sophisticated algorithm called Advanced Time-variant Multi-Objective PSO (AT-MOPSO) to enhance cloud storage and energy efficiency optimization. The suggested approach surpasses existing techniques in terms of both cloud storage cost and energy efficiency. In [22], the authors investigate the advantages of sharding in blockchain networks in terms of scalability. The study showcases a decrease in orphan blocks and presents an on-chain governance mechanism that utilizes PSO to address risks associated with forks. The study conducted by [23] focuses on optimizing energy consumption and ensuring high-quality service in software-defined data centers. The authors suggest utilizing a heuristic optimization method incorporating particle swarm intelligence to select features. The simulation results demonstrate the effectiveness of the suggested approach. The authors in [24] utilize blockchain and Improved PSO (IPSO) to enhance the efficiency and security of work scheduling in cloud computing. The suggested algorithm exhibits superior performance in terms of makespan, execution time, and efficiency compared to existing scheduling methods.

Pertinent literature sheds light on several notable contributions in the context of multi-network E2E path setup within SDN. The authors in [34] propose an innovative SDN-enabled networking architecture, integrating BC technology, security, and autonomy management layers to advance multi-layer communication within SDN networks. The authors of [50] put forth a framework named TRAQR, which focuses on establishing trust and verifying QoS compliance for E2E routing across multi-domain SDNs. In [39], the authors contribute to the realm of multi-domain networks by implementing trusted relationships among SDN controllers through a cross-domain routing framework.

TABLE 1. Summary of the related research regarding their use of technologies and target services.

Research	Blockchain	SDN/SDON	Routing/Path Selection	Multi-Domain/Multi-ISP	Resource Optimization	PSO
[25]	✗	✓	✗	✗	✗	✓
[23]	✗	✓	✗	✗	✓	✓
[26]	✗	✓	✓	✓	✓	✗
[22]	✓	✗	✗	✗	✗	✓
[21], [24]	✓	✗	✗	✗	✓	✓
[27]	✓	✗	✗	✓	✗	✗
[17], [28]–[30]	✓	✗	✓	✗	✗	✗
[20]	✓	✗	✓	✗	✗	✓
[14]–[16], [31]	✓	✗	✓	✗	✓	✗
[32]	✓	✗	✓	✗	✓	✓
[33]	✓	✗	✓	✓	✗	✗
[12]	✓	✗	✓	✓	✓	✗
[34], [35]	✓	✓	✓	✗	✗	✗
[18], [19], [36]–[38]	✓	✓	✓	✗	✓	✗
[5], [39]–[49]	✓	✓	✓	✓	✗	✗
[50]–[52]	✓	✓	✓	✓	✓	✗
[53]	✓	✓	✓	✓	✓	✗
CITE-PSO	✓	✓	✓	✓	✓	✓

Moreover, the study conducted by [40] explores the utilization of BC to store and maintain periodically measured and advertised latency measurements among SDN-based ISPs. The proposed infrastructure by the authors of [36] aims to facilitate the transmission of correlated flows across social network users. The infrastructure focuses on minimizing link overlapping within a set of paths by utilizing topology manager modules, flow association, and path setup modules implemented over SDN controllers. While the aforementioned research utilizes BC technology, none of them specifically addresses the establishment of paths across multi-ISP optical networks.

In [28], the study introduces a novel encryption and trust assessment framework that utilizes BC technology to store the identities of Aggregator Nodes (ANs) and Sensor Nodes (SNs). The authors in [31] represent a BC-based multi-path QoS routing security method by enhancing the conventional Ad hoc On-Demand Distance Vector (AODV) protocol, namely AODV-MQS. They create a network chain with intermediary nodes used to store the statuses of all nodes in the chain. The authors of [27] introduce the “BlockJack” system that utilizes a distributed and tamper-proof consortium BC to prevent IP prefix hijacking in the Border Gateway Protocol (BGP). BlockJack facilitates the synchronization between the BC and BGP networks by means of interfaces that guarantee operational autonomy. Limited computing, memory, energy, and encryption algorithm complexity are concerns for encrypting data in IoT wireless sensors. In [29], nodes can authenticate and link to numerous networks or clusters using the proposed BC security IoT protocol by storing the appropriate keys for networks or groups at the sensor level. In [30], the authors use BC to reward potentially self-serving nodes for helping to route packets as brokers. For self-organizing, non-cooperative adhoc networks, the authors want to develop a multi-hop routing protocol called Data Broker within the BC framework. The BlockQoS framework is proposed in [51] to utilize BCs to achieve equitable monetization of on-demand QoS. The BlockQoS platform enables clients to efficiently manage their QoS

needs using a BC-based system that operates via a smart contract. The authors of [41] represent a novel framework, named BC-based BGP4 Orchestration (BBO), to enhance the transparency of BGP4 transactions. The proposed framework leverages an Internet number resource authority and a trustworthy management entity to achieve its objectives. The research in [42] indicates a decentralized framework with low complexity that utilizes deep learning and BC technologies to provide security against BGP attacks. The proposed model in the research is designed to enhance the management, flexibility, and scalability of BGP environments through the use of SDN. The authors in [43] propose an architecture that utilizes BC technology to establish secure routing in SDN-enabled IoT networks [4] across multiple domains. SDN controllers are universally outfitted with BCs and utilize smart contracts [54] to upload abstract topologies to the BC. The study in [44] introduces a framework inspired by BC aimed at ensuring secure routing across multiple domains of unmanned aerial vehicle-IoT applications. Through the utilization of smart contracts, abstract typologies are posted to the BC by all SDN controllers. Moreover, it ensures routing reliability and oversees worldwide credibility within the blockchain. The authors of [52] suggest a simple BC-based authentication method that stores the credentials of regular sensors. To provide lightweight authentication, minimal credentials are saved on the BC because IoT nodes have a short lifespan owing to battery depletion. Additionally, a genetic algorithm-enabled SDN controller, which is also utilized for on-demand routing to reduce the energy consumption of the nodes in the IoT network, performs the route computation. A route accuracy technique is also suggested to ensure no malicious nodes are in the route that was computed.

Regarding the incorporation of BC technology in optical networks, scholars have made notable contributions to various research endeavors. For instance, in [45], the proposed study indicates a peer-to-peer optical network enhanced by BC infrastructure that facilitates the efficient management and sharing of network resources across multiple domains,

dispensing with the need for a central authority. Similarly, the authors in [35] employ BC to ensure secure leasing transactions for optical network slicing, thereby establishing a robust and high-quality communication network for IoT applications. In another study [37], the authors delve into secure spectrum trading within EONs, leveraging a BC-based framework to embed virtual optical networks. The utilization of a BC-assisted ledger, cooperatively maintained by all virtual optical networks, ensures tamper-proof transactions in spectrum trading, thereby enhancing the integrity and trustworthiness of the network. In a related investigation, the authors of [46] propose a supportive mechanism to promote vendor diversity and interoperability in distributed optical networks. This approach enables the efficient allocation of responsibility and the establishment of trusted accountability for network events and activities, hence promoting a dependable and transparent distributed control architecture. Lastly, the study in [38] puts forth a distributed control architecture for optical networks, incorporating a blockchain model to enhance network management and control, ultimately contributing to the advancement of the field.

The BC-based SDON is defined by the authors as a system that facilitates fault tolerance in a highly efficient manner, taking into account measures such as processing rate and recovery latency. The BC consensus protocol defined by the authors in [53] establishes dynamic leaders responsible for writing blocks into the BC system, with the ultimate goal of establishing trusted optical communication networks. In [33], the authors propose the establishment of optical and wireless networks based on BC technology to enhance the security of authentication methods and mitigate potential intrusion scenarios in multi-domain networks within the context of 6G cellular networks. In [47], a comprehensive overview is presented on the application of bit error rate and optical signal-to-noise ratio in the context of multi-domain optical networks to assess and validate the quality of transmission. An alternative methodology shown in [48] suggests the implementation of a peer-to-peer network consisting of network-slicing administrators. This network would facilitate the coordination of optical network resource sharing in a multi-domain environment, employing BC technology. The integration of holding-time-aware routing and multi-path routing traffic pampering with adaptive modulation is combined to formulate an integer linear programming model while reducing spectrum resource use in SDN consolidated with EONs without including BC technology discussed in [26].

None of the aforementioned studies explore the topic of RSA for QoS-based E2E path establishment in inter-ISP SDONs. This research introduces a novel approach that integrates Particle Swarm Optimization (PSO), a nature-inspired optimization technique, into the context of BC-enabled SDON. The primary objective is to propose a QoS-enabled inter-ISP RSA framework enhanced by BC technology within SDONs. To the best of our knowledge, apart from our prior works [5] and [49], no other studies have explored

the utilization of blockchain for spectrum management and routing efficacy in SDONs. Leveraging the efficiency of PSO in exploring solution spaces and converging towards optimal solutions, the proposed approach significantly enhances the decision-making process in cross-ISP traffic engineering. The integration of PSO with SDON further empowers the network to dynamically and adaptively adjust routing policies and QoS parameters, effectively catering to real-time traffic demands and ensuring a consistently high level of service quality.

III. SYSTEM MODEL

This section describes a network architecture incorporating the suggested efficient framework for spectrum management within the context of BC-empowered adaptive Software-Defined Optical Networks (SDONs). Fig. 2 illustrates the network configuration of four Internet Service Providers (ISPs) based on the SDON concept. To ensure consistent synchronization among state-related transactions as well as blocks inside the blockchain network, every SDON ISP engages in intercommunication with one another. This study investigates two distinct scenarios pertaining to the capability of network devices in terms of wavelength conversion:

- 1) The Hop-by-Hop Wavelength Switching (HWS) method allows network devices to alter the wavelengths utilized for data relaying. This is illustrated with inner nodes, denoted by hexagonal red-blue objects, which have exclusively intra-connected links, and border/edge nodes, represented by cylinder-shaped dark-blue objects, which have inter-connected links across multiple ISPs.
- 2) The Border-Node-Only Wavelength Switching (BWS) refers to the practice of equipping just the network equipment at the periphery with wavelength converters. This facilitates the transfer of information between a pair of ISPs through the utilization of separate and continuous spectrums, also known as subcarriers.

In Fig. 2, the controller of SDON used in the cross-ISP system is based on modules and network applications that are analogous to those used in BC [3].

The Blockchain Manager (BM), Spectrum Monitoring Manager (SMM), Global Routing Agent (GRA), and Blockchain Application (BA) are novel controller modules that exhibit distinct characteristics compared to conventional controller modules. The BM module is responsible for managing many duties connected to BC technology. These functions are performed by its sub-components, which include the Hashing Agent, Validator Agent, Consensus Protocol Handler, Mining Agent, and Transaction/Block Agent. To verify the legitimacy of blocks sent by other controllers, the validator agent applies block verification criteria within the BC system. Another component of the BM system is the hashing agent, which is responsible for executing hashing operations on transactions and blocks inside the BC network. In contrast, the transaction/block agent is responsible for generating transactions or blocks

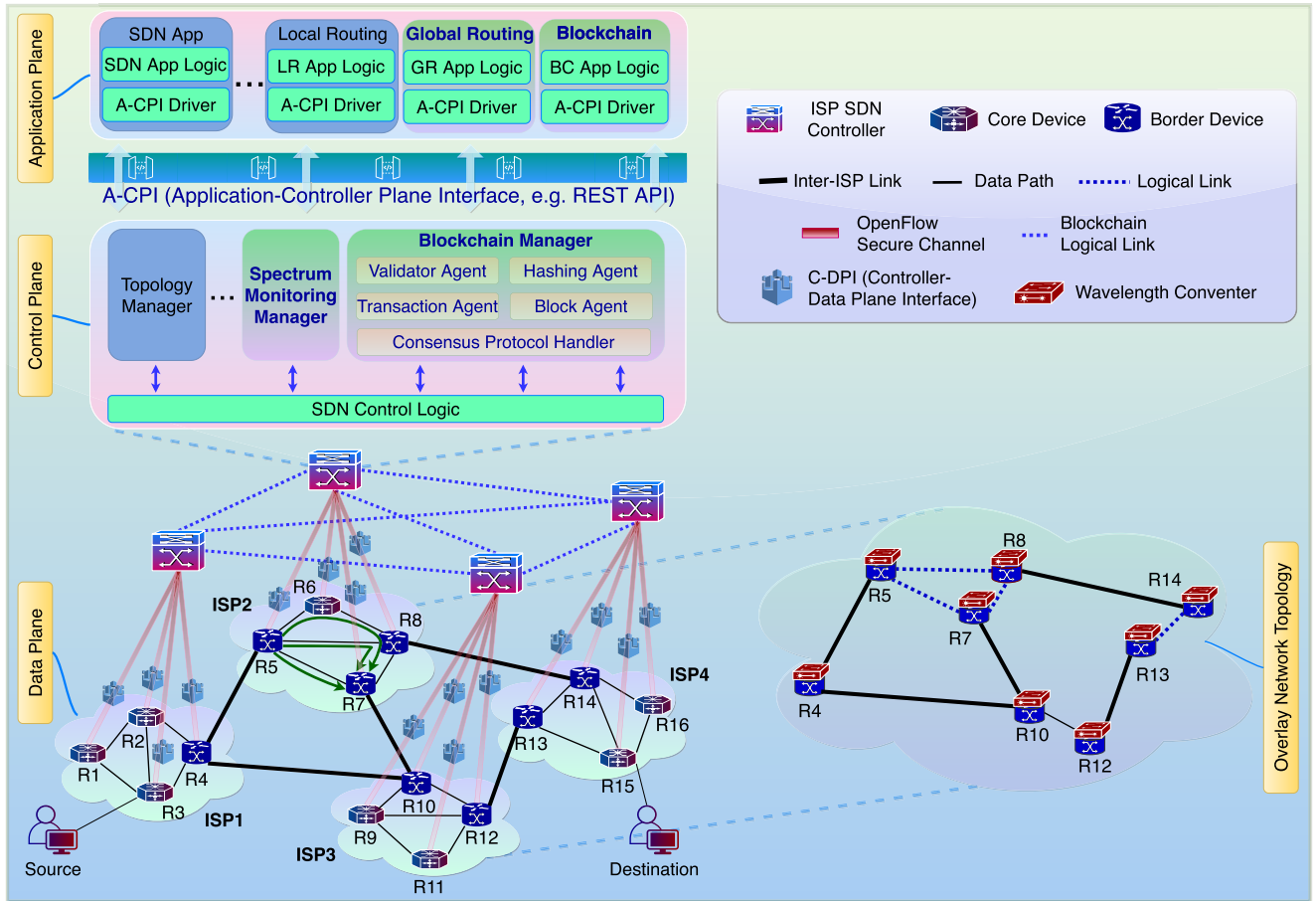


FIGURE 2. An illustration of SDON ISP networks model and its abstracted overlay network.

to ensure the continuous operation of the BC network. The determination of the consensus mechanism to be employed in the BC network is carried out by the consensus protocol handler. Subsequently, the mining agent performs mining tasks in the controller, taking into account the specific use cases of the blockchain and the consensus protocol that has been established [3].

Integrating the SDON controller’s specific module, namely SMM, into the cross-ISP architecture is a crucial design decision. The SMM module performs continuous monitoring of network resources to assess the viability of contiguous and uninterrupted subcarriers within intra-ISP optical fiber lines. When ISPs modify their subcarrier allocations, the SMM sends notifications to the BM component. The BM component then proceeds to update or generate the required transaction(s) inside the BC network.

When a service request between ISPs is received by the controller, the routing module, called GRA, utilizes the border/edge nodes of cross-ISPs as well as transactions with their specific QoS metrics in the blocks to identify an inter-ISP-aware E2E fiber path or link(s). The other application module, namely BA, oversees the transmission and reception of blocks to and from the BC network while also handling the management of request messages.

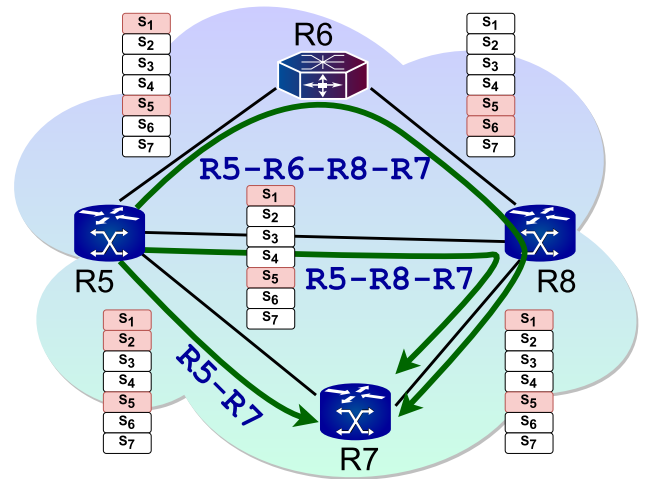


FIGURE 3. The ISP2 network exhibits various link spectrum availability examples between network devices R5 and R7, which can be referred to as partial optical paths or pathlets. These pathlets include R5-R7, R5-R8-R7, and R5-R6-R8-R7. The red and white spectrums (or subcarrier) serve as visual representations of the occupied and accessible spectrums, respectively, over an optical fiber network.

A. PARTIAL OPTICAL PATH (PATHLET)

A fragmented optical route, also known as a pathlet, refers to a distinct pathway connecting two distinct border nodes of ISPs. The termini of a path segment are referred to as ingress

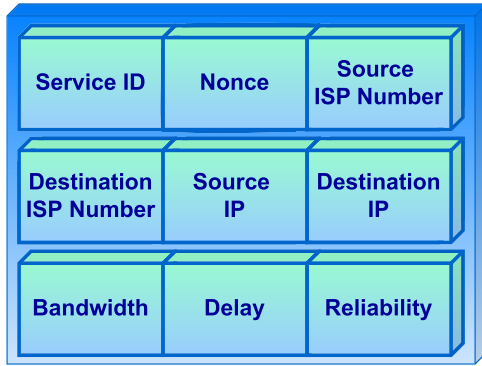


FIGURE 4. Data structure of service request (SR).

and egress nodes, which denote the devices responsible for the entry or exit of data to or from an ISP. The provided diagram, Fig. 3, demonstrates the existence of three optical fiber paths connecting border network nodes R5 and R7 within ISP2. These paths are denoted as R5-R7, R5-R8-R7, and R5-R6-R8-R7, with the assumption that the links are bidirectional.

B. SERVICE REQUEST

According to the routing framework, a *Service Request (SR)* is a request for the provisioning of connectivity between users (i.e., computers) on the same or different networks using specific QoS parameters, such as bandwidth and delay. Theoretically, users may ask for any rate of service (bandwidth and/or delay), and a continuous-rate network must be able to support arbitrary service requests. The SR data structures in the framework are shown in Fig. 4. A SR message contains the following information:

- **Service ID:** The persistent service identifier for a service.
- **Nonce:** Randomly generated distinct *Service Request ID*.
- **Source and Destination ISP Number:** ISP numbers of the source/destination ISPs, respectively.
- **Source and Destination IP:** The source and destination computers' IP addresses, respectively.
- **Bandwidth:** The bandwidth demand of a service request over the E2E path.
- **Delay:** The acceptable delay for a service request over the E2E path.
- **Reliability:** The tolerable reliability of a service request over the E2E path.

A relevant application on a user computer generates the SR message, which is then transmitted to the relevant (source) network controller. An SR is a communication that expresses a request for traffic with particular QoS attributes, namely a continuous and uninterrupted subcarrier demand, between end-users (or entities) who may be located inside the same or different ISPs.

The *CITE-PSO* architecture, which is built on BC technology, utilizes a range of message types in its operational processes. The components encompassed in this category

TABLE 2. Table of terminologies.

Terminology	Description
SDON	Software-Defined Optical Networking
EON	Elastic Optical Network
ISP	Internet Service Provider
E2E	End-to-End
RSA	Routing and Spectrum Assignment
IN-ScP	Inter-ISP Spectrum-Constraint Path Problem
LSL	Link Spectrum Length
PaL	Pathlet Length
LSM	Link Spectrum Matrix
PSM	Pathlet Spectrum Matrix
ISP Number	Internet Service Provider Number
CCD	Continuity, Contiguity, and Discreteness

are a service request communication, which incorporates a distinct service identity number, source, and destination IP addresses, as well as the desired subcarrier(s) demand along the entirety of the optical fiber channel. In addition, a pathlet request message is included, which consists of a distinct identity number for the pathlet request, the ingress and egress nodes of the pathlet within an ISP, the IP addresses of the source and destination hosts, and the desired quantity of subcarriers for the pathlet. Furthermore, the utilization of a pathlet response message is observed, comprising a pathlet response identifier number and the decision made by the ISP controller in relation to the provision of the requested pathlet, either accepting or rejecting it. Finally, a service response message is utilized with a distinct service identifier number and the determination made by the source-ISP controller regarding the provision of the requested service following an assessment of the incoming pathlet response message.

C. CROSS-ISP QOS-BASED OPTICAL ROUTING

Assuming that there are n optical networks, illustrated in Fig. 2 as graphs $N_i(V_i, E_i)$, with $1 \leq i \leq n$, let V and E represent the groups of all nodes and links from those networks, respectively.

$$V = \{V_1, V_2, \dots, V_n\}, \quad \forall V_i \in N_i, \quad 1 \leq i \leq n$$

$$E = \{E_1, E_2, \dots, E_n\}, \quad \forall E_i \in N_i, \quad 1 \leq i \leq n$$

$$V_i = \{v_{i,1}, v_{i,2}, \dots, v_{i,v}\}, \quad \forall v_{i,t} \in V_i, \quad 1 \leq t \leq v, \quad t \in \mathbb{Z}^+$$

$$E_i = \{1e_i, 2e_i, \dots, me_i\}, \quad \forall 1e_i \in E_i, \quad 1 \leq l \leq m, \quad l \in \mathbb{Z}^+$$

Consider the sets V_i and E_i , where *V_i is subset of V_i . These are the sets of all the nodes, links, and border nodes in the network N_i . In N_i , $P_i = \{P_i^1, P_i^2, \dots, P_i^j\}$ is the set of all the different pathlets. P_i^j is made up of a series of links from E_i and is shown as $P_i^j = \{1e_i^j, 2e_i^j, \dots, me_i^j\}$.

$$1e_i^j = \{1s_i^j, 2s_i^j, \dots, ks_i^j\}, \quad \forall 1e_i^j \in E_i, \quad 1 \leq l \leq n, \quad j \in \mathbb{Z}^+$$

$$1s_i^j = \{1s_i^j, 2s_i^j, \dots, ks_i^j\}, \quad \forall 1e_i^j \in E_i, \quad 1 \leq l \leq n, \quad j \in \mathbb{Z}^+$$

In a given network i , the link l over pathlet j , denoted as $1e_i^j$, possesses k spectrums. This set of spectrums, represented

TABLE 3. Table of notations.

Notation	Description
N_i	Graph model of physical networks $(N_i(V_i, E_i))$, $1 \leq i \leq n$, n is the number of ISPs
V	$V = \{V_1, V_2, \dots, V_n\}$ is the set of physical nodes for all ISPs, $\forall V_i \in N_i$, $1 \leq i \leq n$, $n = V $
E	$E = \{E_1, E_2, \dots, E_n\}$ is the set of physical links for all ISPs, $\forall E_i \in N_i$, $1 \leq i \leq n$, $n = E $
V_i	$V_i = \{v_{i,1}, v_{i,2}, \dots, v_{i,v}\}$ is the set of nodes in ISP i , $\forall v_{i,t} \in V_i$, $1 \leq t \leq v$, $t \in \mathbb{Z}^+$
E_i	$E_i = \{e_{i,1}, e_{i,2}, \dots, e_{i,m}\}$ is the set of links in ISP i , $\forall e_{i,l} \in E_i$, $1 \leq l \leq m$, $l \in \mathbb{Z}^+$
P_i	$P_i = \{P_i^1, P_i^2, \dots, P_i^j\}$ is the set of all different pathlets in ISP i , $1 \leq i \leq n$, $i \in \mathbb{Z}^+$
P_i^j	$P_i^j = \{1e_i^j, 2e_i^j, \dots, me_i^j\}$ is the set of used physical links in E_i for the pathlet j , $1 \leq i \leq n$, $i \in \mathbb{Z}^+$
le_i^j	$le_i^j = \{1s_i^j, 2s_i^j, \dots, ks_i^j\}$ specifies the k spectrums in the link l over pathlet j , $k \in \mathbb{Z}^+$
ls_i^j	$ls_i^j = \{1s_i^j, 2s_i^j, \dots, ks_i^j\}$ specifies the available spectrums on link l for pathlet j in ISP i
G^O	$G^O = N(*V, *E)$ is the abstraction of entire ISP networks

by le_i^j , is equivalent to the set of all spectrums on link l over pathlet j in network i , denoted as le_i^j . Let ls_i^j represent the collection of spectrums that are available on link l for pathlet j in network i . The overlay network topology, denoted as $G^O = N(*V, *E)$, is an abstraction of the networks N_i . In this abstraction, $*V = \bigcup_{i=1}^n *V_i$ represents the set of all border nodes in the networks, while $*E$ represents the set of logical linkages connecting these border nodes.

Assumption 1: Let $m_e \in E$ and $n_e \in E$ be two links. We have $|mS| = |nS|$, where mS and nS represent the sets of spectrums on links m_e and n_e , respectively. The notation $|\cdot|$ denotes the cardinality of a set.

Definition 1 (Spectrum Contiguity): If there are two spectrums, denoted as x_m^j and y_m^j , on a link m over a pathlet j in a network i , where $1 \leq x, y \leq k$, and if the difference between x and y is equal to 1, then x_m^j and y_m^j can be classified as contiguous spectrums.

Definition 2 (Contiguous Spectrum Set): In the context of a network, let us consider a link denoted as m and a pathlet denoted as j . For this specific link and pathlet, we have a set of spectrums denoted as $mS_i^j = \{1m_s^j, 2m_s^j, \dots, am_s^j\}$, where $1 \leq a \leq k$. If all the spectrums in this set are adjacent to each other, then we can classify mS_i^j as a set of consecutive spectrums.

Definition 3 (Spectrum Continuity): The continuity property is stated to be held by two spectrums, denoted as x_m^j and y_n^j , which are located on adjacent links m and n along the pathlet j in a network i . For the continuity property to hold, it is required that x is equal to y , while m and n are not equal.

This is assumed that each link within a network possesses a total of k spectrums, which can either be available for use or already allocated to service requests at any given moment. In the context of an optical network, the allocation of spectrums to accommodate a service demand of m spectrums, where m is less than or equal to k , necessitates adherence to a set of three criteria known as CCD (spectrum Continuity, spectrum Contiguity, and spectrum Discreteness, denoting non-overlapping). Spectrum discreteness in gridless flexible optical networks involves strategically allocating spectrum segments to connections, ensuring that the start frequency of

a new segment precisely aligns with the end frequency of an existing one to prevent fragmentation. This process, termed ‘‘spectrum discretization,’’ optimizes spectral efficiency and promotes effective utilization of the continuous spectrum in such networks. The problem of inter-ISP spectrum-constrained path (IN-ScP) can be defined as a route problem involving multiple constraints.

Definition 4 (Inter-ISP Spectrum-Constrained Path Problem (IN-ScP)): Let us consider a network $N(*V, *E)$ that is an abstraction of networks $N_i(V_i, E_i)$. Each link e in the set E is characterized by the number of spectrums it has accessible or assigned at any given moment, denoted by k . The problem at hand involves finding a path from a source node s to a destination node d , subject to CCD constraints, a specified bandwidth requirement, and a delay threshold. Here, s belongs to the set of nodes denoted as $*V_i$, d belongs to the set of nodes denoted as $*V_j$, and it is important to note that $*V_i$ and $*V_j$ are not equal. The objective is to allocate spectrums for the service demand, which requires m spectrums (with m less than or equal to k), on all links along the chosen path while ensuring minimum reliability and the allocated spectrums exhibit continuity, contiguity, and discreteness.

A path that meets the CCD constraints is commonly known as a (spectrum-constrained) feasible path [55]. There exist numerous pathways inside the network $N(*V, *E)$ that adhere to the given restrictions. According to Definition 4, it may be stated that each of these pathways represents a possible solution to the IN-ScP issue.

Definition 5 (Link Spectrum Length (LSL)): The Link Spectrum Length for a connection across a pathlet j in a network i , denoted as le_i^j , refers to the count of spectrums present on the link. It may be calculated using the following formula:

$$L(le_i^j) = \sum_{\forall k_m s_i^j \in le_i^j} 1$$

Definition 6 (Pathlet Length (PaL)): The Pathlet Length for a particular pathlet P_i^j in a network i is defined as the

number of links along the pathlet, denoted as $L(P_i^j)$:

$$L(P_i^j) = \sum_{\forall m e_i^j \in P_i^j} 1$$

Definition 7 (Link Spectrum Matrix (LSM)): The Link Spectrum Matrix for a given link across a pathlet j in a network i , denoted as $m e_i^j$, is a matrix of size $1 \times k$. It is expressed as follows:

$$m e_i^j M = [1 m s_i^j \ 2 m s_i^j \ \dots \ k m s_i^j]$$

where

$$k m s_i^j = \begin{cases} 1, & \text{if } m s_i^j \text{ is available} \\ 0, & \text{if } m s_i^j \text{ is occupied} \end{cases}$$

Definition 8 (Pathlet Spectrum Matrix (PSM)): Given a pathlet in a network i represented as P_i^j , the Pathlet Spectrum Matrix for P_i^j is a $m \times k$ matrix and represented as following: The Pathlet Spectrum Matrix for a given pathlet in a network i , denoted as P_i^j , is a matrix of size $m \times k$. It is expressed as follows:

$$M^{P_i^j} = \begin{bmatrix} 1 e_i^j M \\ 2 e_i^j M \\ \vdots \\ m e_i^j M \end{bmatrix} = \begin{bmatrix} 1 s_i^j & 2 s_i^j & \dots & k s_i^j \\ 1 s_i^j & 2 s_i^j & \dots & k s_i^j \\ \vdots & \vdots & \vdots & \vdots \\ 1 s_i^j & 2 s_i^j & \dots & k s_i^j \end{bmatrix}$$

where each row in $M^{P_i^j}$ is $m e_i^j M$ for a link $m e_i^j$ over the pathlet j in a network i .

IV. BLOCKCHAIN-ENABLED CROSS-ISP TRAFFIC ENGINEERING FRAMEWORK

This section provides an in-depth look at the architecture of the Cross-ISP (Internet Service Provider) Traffic Engineering enhanced by Particle Swarm Optimization (CITE-PSO) framework, shedding light on its foundational concepts, procedures, and features pertaining to the execution of both Blockchain (BC) and optical networking activities.

Secure Data Exchange in a Multi-ISP Scenario. In scenarios involving numerous ISPs, each ISP may fall under the governance of a distinct operator or organization. However, the exchange of personal information across these ISPs poses challenges [56]. It not only escalates the overall cost of message transmission due to the extensive network involved but also heightens the risk of security breaches, given the potential exploitation of operational privacy across multiple domains [57].

Leveraging Blockchain for Secure Data Exchange. The primary objective of this study is to harness the inherent advantages of blockchain technology to facilitate the secure exchange of encrypted data using both public and private key transactions. Blockchain’s decentralized and immutable nature provides a robust solution to the challenges associated with secure data exchange in a multi-ISP environment.

Role of Blockchain Nodes in CITE-PSO Architecture. Within the CITE-PSO architecture, each optical ISP network

controller relies on a dedicated BC node to effectively manage its own blockchain instantiation. The ISP controller, serving as a BC node, assumes the responsibility of maintaining the requisite set of public and private keys essential for cryptographic operations.

Establishing Secure Connections with ISP Numbers (ISPN). In the CITE-PSO, the ISP controllers initiate connections with their counterparts through the exchange of their respective public keys. These unique BC node identities, referred to as ISP Numbers, play a crucial role in facilitating secure communication within the inter-ISP network.

Cryptographically Signed Optical Networking Data. To ensure the integrity and security of communication, the optical networking data within the CITE-PSO framework is cryptographically signed. This signed data includes essential information such as the ISPN and a comprehensive listing of border devices.

The Need for Blockchain in the Framework. Blockchain technology is integral to the CITE-PSO framework for several reasons: (i) its decentralized and tamper-resistant nature ensures the security and immutability of exchanged data, preventing unauthorized access and manipulation; (ii) the cryptographic capabilities of blockchain enhance the authenticity and integrity of optical networking data, thereby establishing a trustworthy environment for inter-ISP communication. The utilization of blockchain addresses the challenges of secure data exchange, providing a resilient foundation for the framework’s operations within a complex, multi-ISP landscape.

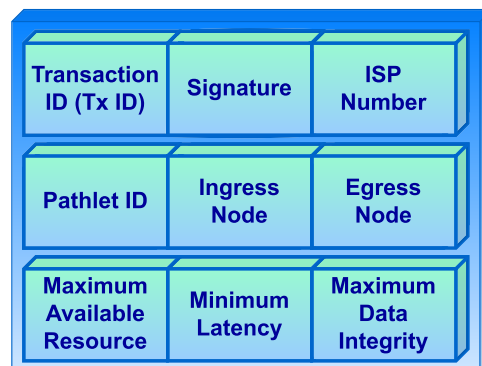


FIGURE 5. Transaction data structure in CITE-PSO.

The CITE-PSO is responsible for generating transactions that consist of various data, depending on their specific use cases. These transactions are derived from optical pathlets, which carry QoS measurements. The generation process is facilitated by the involvement of ISP controllers. Therefore, ISP controllers establish and designate distinct pathlets within their own intra-ISP networks for various border node pairs. These pathlets are subsequently recorded as independent transactions on the BC ledger [3]. The diagram in Fig. 5 illustrates the structure of a transaction within the BC. The components encompassed in this context are the Transaction Identifier (Tx ID), the digital signature (Signature), the Internet Service Provider Number (ISPN),

the *Pathlet Identifier (Pathlet ID)*, the *Ingress and Egress Nodes*, the *Maximum Available Resource* (i.e., subcarriers), *Minimum Latency*, and *Maximum Data Integrity*. These elements serve to specify the distinct identification of a transaction, the cryptographic digital signature generated by the ISP controller, the unique number assigned to an ISP, the specific identifier of a pathlet, the initial and final nodes of an optical pathlet within an ISP, the maximum number of contiguous and continuous subcarriers available in an optical pathlet, the latency of E2E data communication over inter-ISP networks, and reliable data transfer through SDONs, respectively.

In the context of the BC-based *CITE-PSO* framework, ISP controllers perform transaction verification by applying a predefined set of criteria. These criteria encompass the following conditions: (i) the transaction must possess a digital signature; (ii) the maximum available subcarrier must have a positive value; (iii) a valid ISPN must be assigned; and (iv) the ingress and egress endpoints specified in the transaction must be under the ownership of the ISP responsible for creating the transaction. To explain the transactions made by the ISP2 controller for optical pathlets between border nodes R5 and R7 in ISP2, Table 4 is shown. This information is depicted in Fig. 3. The ISP2 controller initiates the generation of transactions for distinct optical pathlets by utilizing their respective identification numbers and the maximum count of consecutive subcarriers, as demonstrated in [49].

A. CROSS-ISP TRAFFIC ENGINEERING ENHANCED BY PARTICLE SWARM OPTIMIZATION

The Particle Swarm Optimization (PSO) algorithm employs a swarm mode that allows it to simultaneously explore an extensive region within the solution space of the optimized objective function [58]. The movement of a collection of potential solutions, which are referred to as “particles,” is regulated throughout the search area in order to accomplish this goal. The PSO algorithm exploits the principles [59]:

- 1) *Proximity*: The swarm must possess the capability to do basic calculations involving spatial and temporal dimensions.
- 2) *Sensing Capability*: The swarm should possess the ability to detect and respond to changes in environmental quality.
- 3) *Diverse response*: the swarm should not restrict its means of acquiring resources to a limited scope.
- 4) *Stability*: The swarm must exhibit consistent behavior regardless of environmental fluctuations.
- 5) *Adaptability*: The swarm should modify its behavioral style when it is deemed advantageous.

The five principles encompass the fundamental attributes of the PSO system and serve as guiding principles for the establishment of the swarm artificial life system. Within the structure of PSO, particles have the ability to adjust their positions and velocities in response to changes in the environment, specifically when certain criteria related to proximity and quality are met. Furthermore, the swarm

in PSO exhibits unrestricted movement as it persistently explores the optimal solution within the feasible solution space. Particles in PSO exhibit consistent movement within the search space but can adjust their movement strategy to accommodate changes in the environment [60]. The particles’ locations and velocities, as outlined in Eqs. 1 and 2, respectively, dictate their trajectory throughout the optimization process. Eq. 1 provides the position vector of the particle, where X^i represents the chosen nodes and can take on values of either 0 or 1. Eq. 2 indicates the velocity vector of the particle, with the velocity vector values belonging to the set of real numbers, denoted as \mathbb{R} . The positions that are most widely recognized inside the search-space undergo updates whenever superior locations are detected by other particles. These positions serve as guidance for directing the movement of each individual particle. It is anticipated that the swarm will be guided toward optimal solutions.

$$X^i = [x_1^i, x_2^i, \dots, x_p^i], \quad \forall x^i \in X^i : x^i \in \{0, 1\} \quad (1)$$

$$V^i = [v_1^i, v_2^i, \dots, v_p^i], \quad \forall v^i \in V^i : v^i \in \mathbb{R} \\ i \in [1, swarmSize] \quad (2)$$

In Algorithm 1, the inputs are G^O , SR , $BlockChain$, the number of iterations (*iterations*), and *swarmSize*, which represents the population size used to construct the search space. In line 4, the *CITE-PSO* algorithm generates random starting particles for the SR and stores them in the *Population* (i.e., *Swarm*) data structure along with their corresponding fitness values, which are set to ∞ .

Algorithm 1 CITE-PSO

```

1: procedure CITE-PSO( $G^O$ ,  $SR$ ,  $BlockChain$ , iteration, swarmSize)
2:   initialize counter with 0
3:   initialize  $Swarm$ ,  $Best_G$  as  $\emptyset$ 
4:   create all particles with  $G^O$  and hold them in  $Swarm$ 
5:   while counter < iteration do
6:      $SR$ 
7:       calculate fitness with Algorithm 2 using  $Swarm$ ,  $G^O$ ,  $SR$ ,
          $BlockChain$ 
8:       Update each element of the particle’s  $Best_p$ 
9:       Update  $Best_G$  using all  $Best_p$ 
10:      Update each element of the particle’s velocity and location
         using Eq. 3 and 4
11:      counter ++
12:   return  $Best_G$ 

```

The generated particles $P = \{p_1, p_2, \dots, p_{swarmSize}\}$ are included in the *Population* in line 4. For each individual p_i , there are attributes X_i , V_i , F_i , RP , and $Best_p^i$, together with their respective fitness values. The set of fitness values, denoted as $F = \{f_1, f_2, \dots, f_{swarmSize}\}$, is obtained by the utilization of the `findPath()` technique in Algorithm 2, together with the personal best values. RP indicates the real path of p_i , ($\forall \in [1, swarmSize]$). The set of personal best positions, denoted as $Best_p$, is defined as $\{best_p^1, best_p^2, \dots, best_p^{swarmSize}\}$, where *swarmSize* represents the size of the population. In line 6, the method returns the count of genuine nodes in the 0 – 1 discrete route (X).

TABLE 4. Transactions created by ISP2 controller for pathlets between R5 and R7 border devices as illustrated in Fig. 3.

Tx ID	Signature	ISP2	Pathlet ID	Ingress Node	Egress Node	Max Available Resource	Min Latency	Max Data Integrity
ISP2_1	0000asx34...	ISP2	R5_R7_1	R5	R7	3	10	0.992
ISP2_2	0000kbf4g...	ISP2	R5_R7_2	R5	R7	3	9	0.994
ISP2_3	0000erfg4...	ISP2	R5_R7_3	R5	R7	2	9	0.994
ISP2_4	0000ytx6j...	ISP2	R5_R7_2	R5	R7	1	10	0.992
ISP2_5	0000fdx4...	ISP2	R5_R7_3	R5	R7	2	7	0.996
ISP2_6	0000uprth...	ISP2	R5_R4_1	R5	R7	2	13	0.991
...

In line 7, the algorithm calculates the fitness value for each particle in the population in order to identify the particle with the lowest fitness value, which is considered the best. The CITE-PSO algorithm utilizes the comparison of the $Best_P$ and $Best_G$ values with the fitness values of individual particles to ascertain the most optimum outcome. The values undergo updates in the event that a superior value is discovered (lines 8 – 9). In line 10, the velocity and position of a particle are changed using Eqs. 3 and 4, correspondingly. Eqs. 3 and 4 specify the actions in the following manner.

$$V^{i+1} = V^i + c_1 \times r_1 \times (Best_P^i - X^i) + c_2 \times r_2 \times (Best_G - X^i) \quad (3)$$

$$X^{i+1} = X^i + V^{i+1} \quad (4)$$

In Eq. 3, r_1 and r_2 are random numbers while updating the velocity with a new position as in Eq. 4. $U(a, b)$ is a symbol for a uniformly distributed random number between 0 and 1 as shown in Eq. 5. In Eq. 6, $sig(V^{i+1})$ is a sigmoid limiting transformation.

$$X^{i+1} = \begin{cases} 1 & \text{if } U(0, 1) < sig(V^{i+1}) \\ 0 & \text{otherwise} \end{cases} \quad (5)$$

$$sig(V^{i+1}) = \frac{1}{1 + \exp(-V^{i+1})} \quad (6)$$

The constituents of all particles are comprised only of the binary values 0 and 1. The particles are initially at rest, with starting velocities of 0. The initial location of the particle denotes the point of origin, whereas the final position denotes the point of destination. In line 6 of Algorithm 1, the binary representation of each particle’s route is transformed into a sequence of real node numbers. When constructing the actual pathways, the particle assigns a value of 1 to the nodes that are included in the path. As an illustration, consider the particle’s trajectory from the source node 1 to the destination node 6, denoted as 1 – 0 – 1 – 1 – 0 – 1. Subsequently, the genuine trajectory corresponding to this particle is determined to be 1 – 3 – 4 – 6 in accordance with the illustration presented in Fig. 6.

The discovered path may not always constitute a viable path according to the QoS measurements. In the event that a genuine path is absent, the computation of the fitness value in the $findPath()$ function on line 7 incorporates an error term for the particle in question. The $findPath()$ attempts to determine a route originating from the actual particle. It is not guaranteed that all nodes included by the 0-1 particle will constitute a valid route. An error measurement

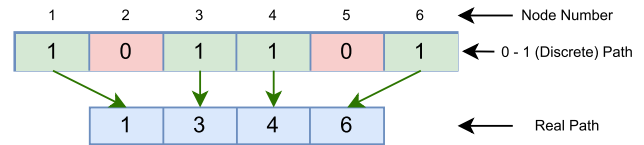


FIGURE 6. Converting a discrete path to a real path.

Algorithm 2 FitnessPSO(): Calculate Particle’s Fitness Value

```

1: procedure FitnessPSO(Swarm, GO, SR, BC)
2:   for each particle in Swarm do
3:     fitness ← 0
4:     realPath ← getRealPathList(particle)
5:     path ← findPath(Population, GO, SR, BC, realPath)
6:     similarity ← similarityCheck(realPath, path)
7:     if path == ∅ then
8:       fitness ← ∞
9:       break
10:    fitness ← δ × ∑v(i,i+1)∈path w(i, i + 1)
11:    if similarity > 0 then
12:      fitness ← fitness + similarityPenalty    ▷ Use Eq. 7
13:    if realPath.size() > path.size() then
14:      fitness ← fitness + sizePenalty        ▷ Use Eq. 8
15:  return Population
    
```

is established to mitigate this issue and identify alternative pathways that are more appropriate. The error assessment is utilized to establish a path consisting of nodes within the actual particle. The length of this path is then assigned to the error measurement associated with this path. In the event that a path is identified without the utilization of all the nodes of the actual particle, an error value is appended in direct correlation to the number of unused nodes as a means to signify the presence of superfluous nodes inside the path. The fitness value of each particle is determined by the estimated error assessment value. In the event where the genuine path lacks a trajectory, the fitness value is optimized to signify that this particle is an inadequate answer and to diminish its influence.

The computation of the personal best and global best values of the particles occurs in lines 8 and 9 of Algorithm 1. In line10, the objective is to modify the velocity and position data of the chosen swarm. In the process of determining the updated velocity, the initial value is subjected to a mathematical operation known as the sigmoid function, which serves to standardize the value within the interval of 0 to 1, as seen in Eq. 6. Next, utilizing this assigned value, a series of random integers within the range of $U(a, b)$

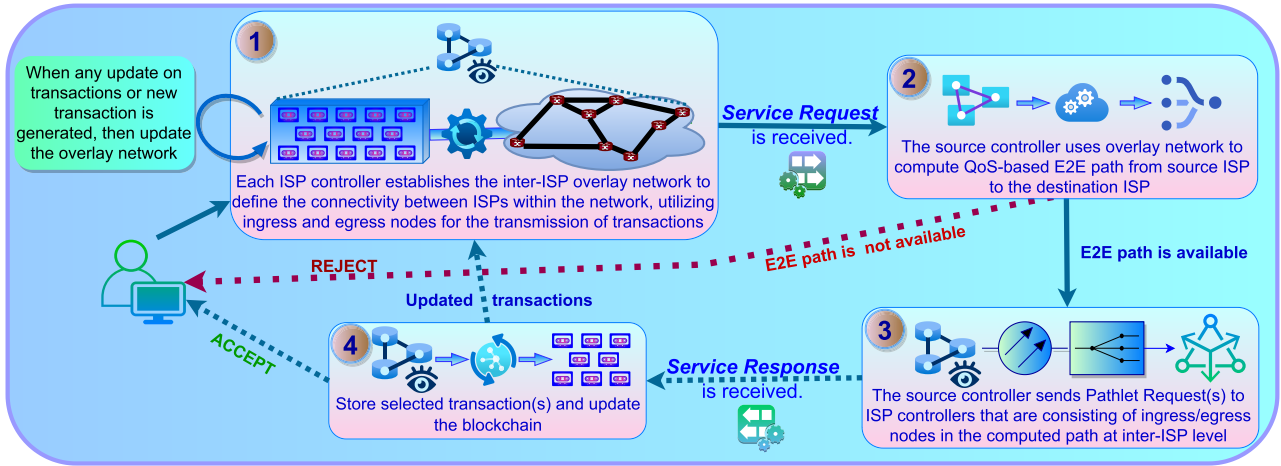


FIGURE 7. Workflow of inter-ISP routing for a service request.

and $0 - 1$ are created to revise the current position data, as described in Eq. 5. The counter is incremented by a value of 1 in line 11, and this iterative procedure persists until the hysteresis condition is met. This iterative process is then repeated at each subsequent step.

The *FitnessPSO* method, as described in Algorithm 2, is designed to determine the fitness values by tracing the trajectories of the particles inside the swarm. The nodes of the particle, which are composed of binary digits (0s and 1s), are derived in line 4. In line 5, the objective is to identify a path using the *realPath* that has been acquired. In line 6, an evaluation is conducted to see if there are disparities between the used approach and the path obtained by the *getRealPathList()* function. As an illustration, the *realPath* may consist of the nodes 1 – 2 – 4 – 5 – 6, whereas the identified route may consist of the nodes 1 – 2 – 4 – 6. It is evident from the given information that node 5 is not utilized in the current context. However, the particle retains this value. To signify the inaccuracy of this value, a penalty value derived from the aforementioned value is incorporated into the fitness value computation conducted in line 12. The penalty value is computed based on the equation represented as Eq. 7, where δ is the subcarrier(s) demand in *SR*.

$$similarityPenalty \leftarrow \delta \times similarity \quad (7)$$

In line 14, the presence of a penalty value is warranted if there exists a difference in length between the particle’s actual trajectory and the computed route. This implies that other pathways of lesser length may exist, but the particle lacks the capability to discover them. To serve this objective, the penalty term in Eq. 8 incorporates the disparity in magnitude across different pathways. As the penalty value increases, the corresponding effect becomes more pronounced, hence promoting a tendency towards shorter courses.

$$sizePenalty \leftarrow \delta \times (realPath.size() - path.size()) \quad (8)$$

The objective of the technique is to determine the shortest path information of the herd while considering the global best value.

1) PATH FINDING PROCESS OF CITE-PSO FRAMEWORK

Illustrating the intricacies of service request management within a Software-Defined Optical Networking (SDON) environment, Fig. 7 provides a detailed sequence diagram outlining the End-to-End (E2E) optical path-finding process within the *CITE-PSO* framework. This orchestrated procedure unfolds in a series of well-defined steps, ensuring the efficient establishment of Quality of Service (QoS)-optimized paths for service demands. Initially, each Internet Service Provider (ISP) controller takes the initiative to establish the inter-ISP overlay network, meticulously defining connectivity between ISPs. The overlay network serves as a crucial conduit for transaction transmission, utilizing dedicated ingress and egress nodes. The overlay network undergoes real-time updates upon transactional changes, ensuring constant synchronization. Subsequently, a user or client initiates a service demand, prompting the ISP controller to compute an E2E optical fiber route. This route comprises smaller segments known as pathlets, extending from an edge/border device within the source ISP’s network to a border node of the destination ISP. The controllers of the source-ISP and destination-ISP are responsible for overseeing the management of the partial optical routes. These routes are established through the utilization of intra-domain routing protocols, policies, rules, and service-level agreements. The purpose of these routes is to facilitate the transmission of data from the user/source-host to the source-ISP border node of the E2E optical link, as well as from the destination-ISP border node to the destination-host. The computation, rooted in the ISP’s Blockchain (BC) ledger, incorporates QoS specifications and preferences provided in the service demand. The originating ISP controller finalizes the E2E optical path, leveraging the latest transactions of the pathlets stored in the BC ledger as shown in Table 4. When QoS conditions in E2E routing computation are met, the source ISP controller dispatches Pathlet Request(s) to relevant ISP controllers within the inter-ISP path. Each ISP controller promptly responds, striving to meet the specified QoS requirements. The outcome conveyed

through a service response message is determined based on pertinent QoS factors and is characterized by either acceptance (Accept) or rejection (Reject). Throughout this intricate process, the *CITE-PSO* framework seamlessly stores selected transactions and diligently updates the BC, fortifying the security and immutability of the exchanged data. This structured workflow, enriched with robust components and dynamic interactions, encapsulates the effectiveness and reliability of the *CITE-PSO* framework in the domain of multi-ISP networks.

V. EVALUATION

This section represents a comparative analysis of the performance of the Cross-ISP Traffic Engineering Enhanced by Particle Swarm Optimization (*CITE-PSO*) framework with that of the SpectrumChain (*SC*) framework [5], the Hierarchical Routing Approach (*HRA*) [13], and the Distributed Routing Approach (*DRA*) that represents the current operational mode and utilizes the shortest path selection based on the border gateway protocol [3]. To evaluate the performance of wavelength conversion in the Hop-by-Hop Wavelength Switching (*HWS*) and Border-Node-Only Wavelength Switching (*BWS*) scenarios discussed earlier, we take into account multiple metrics: End-to-End (E2E) Path Setup Time (*PST*), Network Message Overhead (*NMO*), Services Acceptance Ratio (*SAR*), Network Resource Consumption (*NRC*), Average Path Length (*APL*), and Network Path Length (*ANL*).

TABLE 5. Abbreviations and meanings used in the performance evaluation.

Abbreviation	Meaning
<i>HWS</i>	Hop-by-Hop Wavelength Switching scenario
<i>BWS</i>	Border-Node-Only Wavelength Switching scenario
<i>CITE-PSO</i>	Cross-ISP Traffic Engineering enhanced by PSO
<i>CITE-PSO_HWS</i>	<i>CITE-PSO</i> in <i>HWS</i>
<i>CITE-PSO_BWS</i>	<i>CITE-PSO</i> in <i>BWS</i>
<i>SC_HWS</i>	<i>SpectrumChain (SC)</i> in <i>HWS</i>
<i>SC_BWS</i>	<i>SpectrumChain (SC)</i> in <i>BWS</i>
<i>HRA_HWS</i>	<i>HRA</i> (Hierarchical Routing Approach) in <i>HWS</i>
<i>HRA_BWS</i>	<i>HRA</i> (Hierarchical Routing Approach) in <i>BWS</i>
<i>DRA_HWS</i>	<i>DRA</i> (Distributed Routing Approach) in <i>HWS</i>
<i>DRA_BWS</i>	<i>DRA</i> (Distributed Routing Approach) in <i>BWS</i>

Simulation Setup: In this study, we employ an Erdos-Renyi random network topology characterized by a connectivity degree of 0.7. The network is configured to emulate Software-Defined Optical Networks (SDONs) at the ISP level. The number of nodes in the SDONs is systematically increased within the range of 5 to 10. This experimentation is conducted using four distinct network topologies [5]: NSFNET, US Backbone, Random-14 node, and Random-24 node. The primary objective is to evaluate the sensitivity of the proposed algorithms (*CITE-PSO*, *SC*, *HRA*, and *DRA*) in diverse scenarios, specifically those involving wavelength switching. We denote these scenarios as *CITE-PSO_HWS*, *CITE-PSO_BWS*, *SC_HWS*, *SC_BWS*, *HRA_HWS*, *HRA_BWS*, *DRA_HWS*, and *DRA_BWS* to distinguish between various algorithmic configurations.

The experiments focus on investigating service requests between Internet Service Providers (ISPs) utilizing two subcarriers. Each service request involves a source node and a destination node located in separate ISP networks. The chosen delay and reliability thresholds for feasible paths are set at over 100 *ms* and 0.8, respectively. The optical fiber link assessment aims to identify service rejection instances attributable to network resource constraints. To simulate realistic conditions, the availability of subcarriers is taken into account. Intra-ISP links provide 100 randomly available subcarriers, while interconnecting links offer 200 subcarriers. These choices are made to represent typical operational conditions and resource availability within SDONs [61].

The experimental design utilizes identical random topologies within the intra-ISP networks of Random, NSFNET, and US Backbone. This approach ensures a comprehensive evaluation across various network configurations, allowing for a robust analysis of algorithm performance in different settings. In order to examine the impact of varying switch numbers, we manipulate the number of switches within each intra-ISP network topology, namely NSFNET, US Backbone, Random-14, and Random-24 node inter-ISP networks, during the simulations. A set of 200 service requests is established in all performance scenarios, each consisting of distinct source and destination nodes originating from various ISPs. Table 5 presents a comprehensive compilation of the abbreviations and their corresponding meanings employed in the performance evaluation.

A. PATH SETUP TIME (PST)

The E2E Path Setup Time (PST) is a significant metric in multi-ISP routing scenarios, specifically within the context of cross-ISP traffic engineering [3]. This metric quantifies the duration required to establish the necessary flow rule entry, enabling the provision of a service or flow over an E2E optical fiber path. In the realm of multi-ISP routing, where diverse and interconnected networks are involved, PST serves as a critical indicator of the efficiency and responsiveness of the framework. Networking and topological delays, such as round-trip times between controllers and switches, transmission times of messages/packets between controllers, and processing times for packets/messages, all affect the PST. In the complex environment of multi-ISP routing, these delays can substantially impact the overall performance and scalability of the SDON. Therefore, the PST metric is valuable for evaluating and examining the system's scalability, shedding light on the flow setup latency and the efficiency of incorporating, removing, or modifying flow rules within switch flow tables. In summary, PST provides insights into the responsiveness and effectiveness of the SDON in managing services and flows across multiple ISPs, making it a crucial parameter for assessing the performance of multi-ISP routing frameworks.

In Table 6, a comprehensive evaluation of the E2E PST values across different frameworks under the two wavelength

TABLE 6. Path setup time (PST) in *CITE-PSO*, *SC*, *HRA*, and *DRA* with respect to *HWS* and *BWS* scenarios.

Cases	Number of Switches per ISP					
	5	6	7	8	9	10
<i>CITE-PSO_HWS</i>	90	92	92	96	97	99
<i>CITE-PSO_BWS</i>	93	95	100	102	106	107
<i>SC_HWS</i>	83	85	90	92	92	95
<i>SC_BWS</i>	86	90	95	95	98	99
<i>HRA_HWS</i>	172	188	193	219	238	254
<i>HRA_BWS</i>	184	196	200	255	287	294
<i>DRA_HWS</i>	95	119	127	152	167	182
<i>DRA_BWS</i>	134	149	151	166	180	212

(a) NSFNET (14-ISP)

Cases	Number of Switches per ISP					
	5	6	7	8	9	10
<i>CITE-PSO_HWS</i>	87	92	95	97	100	107
<i>CITE-PSO_BWS</i>	85	95	98	102	104	107
<i>SC_HWS</i>	83	86	90	93	97	98
<i>SC_BWS</i>	83	90	93	96	101	103
<i>HRA_HWS</i>	169	191	195	223	245	260
<i>HRA_BWS</i>	177	200	205	246	281	306
<i>DRA_HWS</i>	94	119	130	150	170	190
<i>DRA_BWS</i>	132	153	152	173	187	228

(c) Random (14-ISP)

Cases	Number of Switches per ISP					
	5	6	7	8	9	10
<i>CITE-PSO_HWS</i>	94	94	103	114	115	126
<i>CITE-PSO_BWS</i>	97	102	110	111	115	134
<i>SC_HWS</i>	88	92	100	104	107	118
<i>SC_BWS</i>	93	97	108	108	111	122
<i>HRA_HWS</i>	183	183	208	242	254	293
<i>HRA_BWS</i>	196	198	218	277	317	454
<i>DRA_HWS</i>	166	171	186	204	206	248
<i>DRA_BWS</i>	174	177	200	226	237	292

(b) US Backbone (24-ISP)

Cases	Number of Switches per ISP					
	5	6	7	8	9	10
<i>CITE-PSO_HWS</i>	93	93	100	105	111	136
<i>CITE-PSO_BWS</i>	100	102	107	112	112	139
<i>SC_HWS</i>	88	92	97	99	107	124
<i>SC_BWS</i>	92	96	100	102	108	128
<i>HRA_HWS</i>	187	188	213	232	252	310
<i>HRA_BWS</i>	195	198	219	243	307	441
<i>DRA_HWS</i>	162	166	188	191	204	267
<i>DRA_BWS</i>	164	179	196	207	228	301

(d) Random (24-ISP)

conversion scenarios (i.e., *HWS* and *BWS*), including *CITE-PSO*, *SC*, *HRA*, and *DRA*, reveals noteworthy insights into the impact of the *CITE-PSO* framework on network efficiency and QoS when compared to the *DRA* and *HRA* approaches. Specifically, the PST value of the *CITE-PSO* framework is as low as 40% and 50% of PST value for the *DRA* and *HRA* approaches, respectively. When the quantity of ISP networks exceeds 7, the disparity between *CITE-PSO* and the other two (i.e., *DRA* and *HRA*) is more accentuated. It’s interesting to note that the *SC* framework outperforms the suggested *CITE-PSO* algorithm in finding the outcomes by computing the E2E path faster. The reason for this is that the *CITE-PSO* approach requires additional time to identify globally optimal outcomes within a specified number of populations, a characteristic that is well-documented within the PSO framework.

The performance disparity described earlier is also evident in Tables 6a – 6d, which pertain to the NSFNET, US Backbone, Random-14, and Random-24 topologies when increasing the number of switches per ISP from 5 to 10. In Tables 6a – 6d, the *CITE-PSO* and *SC* frameworks under consideration leverage the utilization of existing transactions within the blockchain to select a QoS-oriented E2E path that exhibits lower PST compared to the *DRA* and *HRA* methodologies across various wavelength scenarios. The *CITE-PSO* algorithm demonstrates the capability to effectively perform path selection, similar to the random technique employed by the *SC* method, by considering all operations within a specified number of populations. The *CITE-PSO* algorithm achieves results that closely align with the outcomes of the *SC* approach. Due to the increasing intensity of the inter-ISP networks in Tables 6b and 6d, the PST values of the *CITE-PSO* and *SC* framework exhibit a

minor rise when the number of switches per network reaches 7, as observed in the *BWS* and *HWS* wavelength scenarios. Furthermore, the *CITE-PSO* framework has at least two times better PST value than *DRA* and *HRA* methodologies.

B. NETWORK MESSAGE OVERHEAD (NMO)

Network Message Overhead (NMO) plays a crucial role in assessing the scalability performance of a multi-ISP routing framework as the network scales and includes a larger number of nodes. In the context of establishing E2E optical fiber connections over inter-ISP networks, the controllers are responsible for handling a substantial volume of flow request-related message exchanges [13]. NMO becomes a vital metric as it quantifies the number of messages transmitted and processed during the establishment of an E2E path for a flow. As the network expands, the computational resources at controllers, including CPUs and memory, may become constrained, potentially leading to bottlenecks. Thus, this metric becomes especially relevant in a multi-ISP routing environment where the complexity of managing diverse flows and connections across interconnected networks requires careful consideration of message overhead to ensure optimal performance and resource utilization.

In a manner consistent with the aforementioned PST studies, Fig. 8 displays the NMO values for the *CITE-PSO*, *SC*, *HRA*, and *DRA* frameworks, encompassing all wavelength switching scenarios. Notably, the NMO value of *DRA* decreases when the number of switches surpasses 8. This is due to the *DRA* leveraging the Border Gateway Protocol (BGP)-based shortest paths that are already calculated at an inter-ISP level as a routine part of BGP’s operation. Therefore, this reduces superfluous

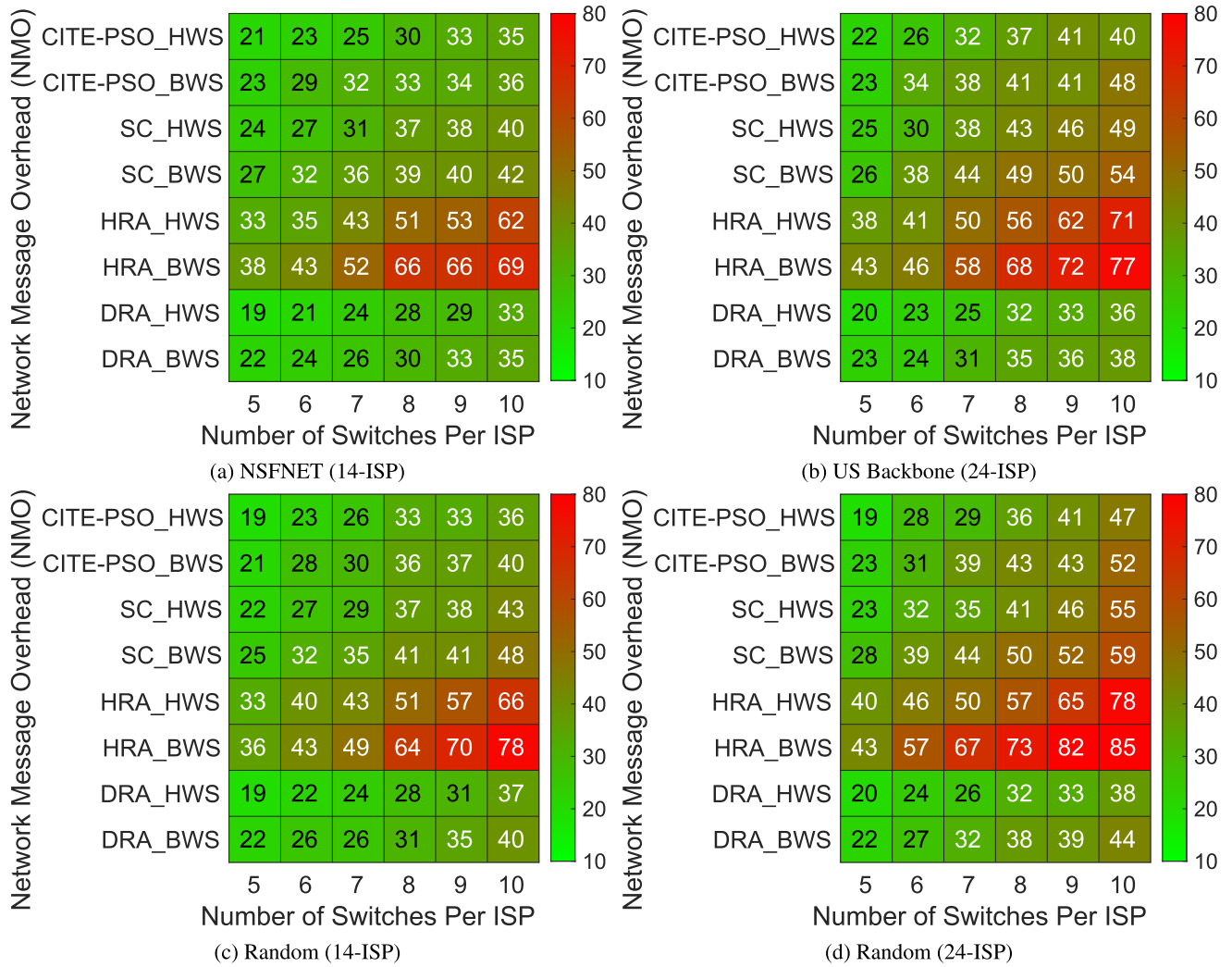


FIGURE 8. Network message overhead (NMO) in CITE-PSO, SC, HRA and DRA with respect to HWS and BWS scenarios.

communications with downstream ISPs, and DRA exhibits slightly better performance compared to the CITE-PSO framework when considering the varying number of switches per ISP, as depicted in Figs. 8a – 8d. Figs. 8c demonstrates that the CITE-PSO framework achieves a reduced NMO value for the establishment of a QoS-based E2E optical fiber path, specifically when the number of switches in ISP networks reaches 8. In contrast to traditional approaches, the CITE-PSO framework demonstrates notable efficiency in managing NMO, surpassing the performance of SC and HRA methodologies while slightly trailing DRA. The lower NMO observed in CITE-PSO is attributed to its adeptness in identifying shorter E2E paths within multi-ISP environments. By leveraging PSO within a blockchain-enabled SDON, CITE-PSO reduces message exchanges when computing optical fiber connections over cross-ISP networks. Moreover, the evaluation across wavelength switching scenarios underscores the advantage of HWS over BWS, with HWS providing a broader spectrum of path selection options. This aligns with the overarching observation that HWS, by offering more efficient outcomes, effectively reduces routing

costs, further highlighting the efficacy of the CITE-PSO framework in enhancing network performance in multi-ISP scenarios.

C. SERVICES ACCEPTANCE RATIO (SAR)

To assess and analyze the overall impact of all path selection approaches with respect to the different wavelength switching scenarios, Fig. 9 presents the acceptance ratio of requested services for CITE-PSO, SC, HRA, and DRA approaches by means of their averages while increasing number of switches per ISP at NSFNET, US Backbone, Random-14, and Random-24 node network topologies at the inter-ISP level in Figs. 9a – 9d. The Service Acceptance Ratio (SAR) results provide valuable insights into the performance of different SDON topologies, taking into account varying numbers of switches (ranging from 5 to 10) in each network.

The comprehensive evaluation of SAR in both HWS and BWS scenarios underscores the superior performance of CITE-PSO and SC compared to DRA and HRA approaches. The CITE-PSO in both wavelength switching scenarios consistently exhibit slightly higher SAR values than their

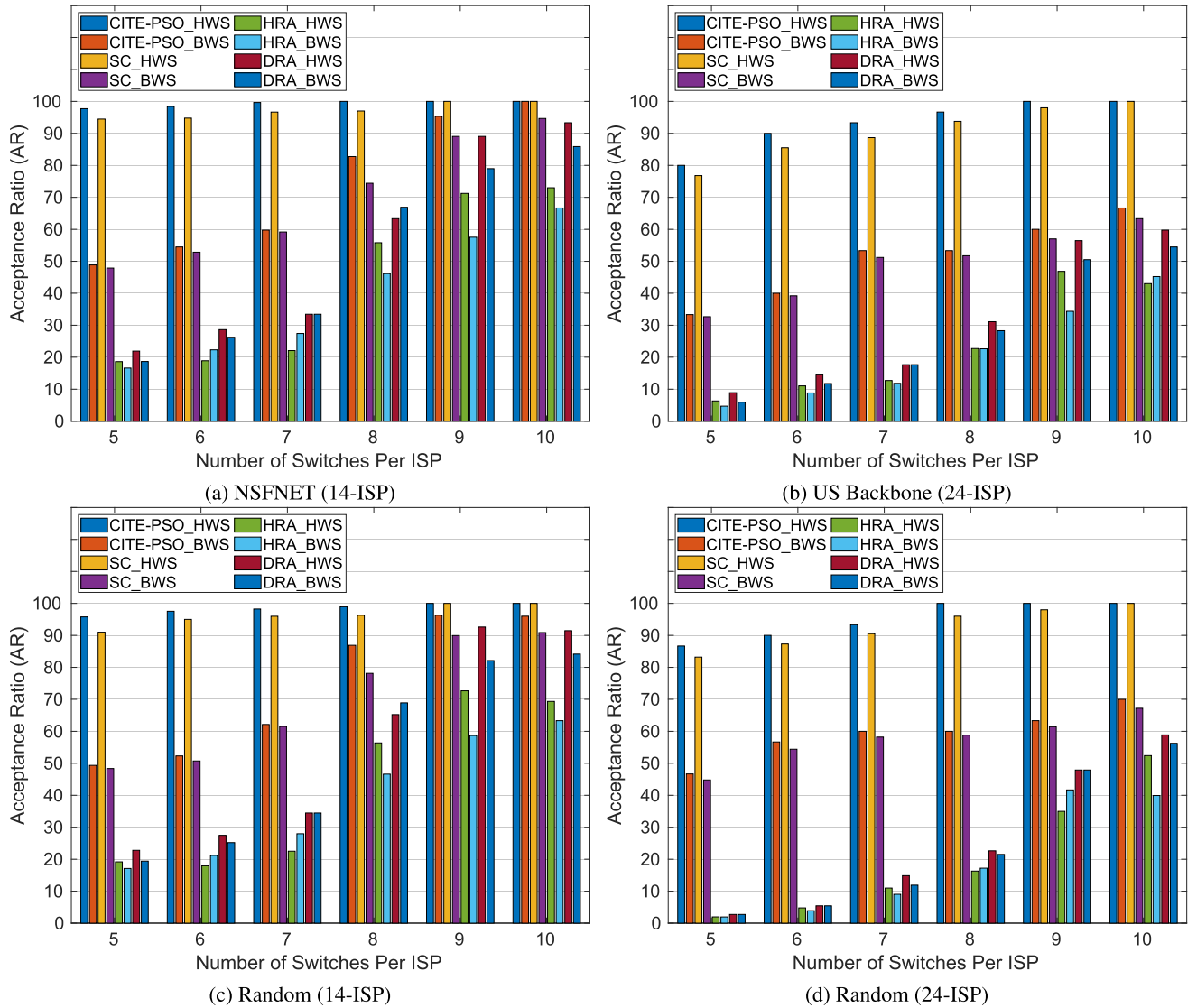


FIGURE 9. Acceptance ratio (AR) in CITE-PSO, SC, HRA and DRA with respect to HWS and BWS scenarios.

SC counterparts. This marginal difference can be attributed to the advanced optimization capabilities of the PSO algorithms employed in *CITE-PSO*, optimizing network traffic management and thereby enhancing QoS to achieve superior service acceptance. On the contrary, *SC_HWS* and *SC_BWS*, relying on random pathlet selection from transactions in the BC for E2E routing, tend to yield lower SAR values. This discrepancy highlights the potential challenges associated with random pathlet selection in BC-based routing, emphasizing the effectiveness of the PSO-based approach adopted by *CITE-PSO*. Furthermore, *CITE-PSO* consistently performs better than *SC* across a range of topologies, including NSFNET and Random-14, as shown in Figs. 9a and 9c. This shows that the CITE-PSO framework can handle more services by quickly exploring the solution space and locating the best and most available E2E paths.

D. NETWORK RESOURCE CONSUMPTION

Network Resource Consumption (NRC) stands as a pivotal metric in the context of cross-ISP networks, offering valuable insights into the utilization and efficiency of available network resources. In the realm of inter-ISP communication, the judicious allocation and management of network resources are paramount to ensure QoS for diverse services and applications. NRC provides a condensed approximation of the bandwidth-hop count product, offering a comprehensive view of how efficiently network resources are utilized in the process of setting up, managing, and maintaining QoS-based E2E path requests. In a cross-ISP network, where visibility is often limited due to the diverse and independently managed domains of different ISPs, monitoring network flow, or bandwidth, becomes a critical strategy. Therefore, to analyze path selection strategies, NRC is another crucial

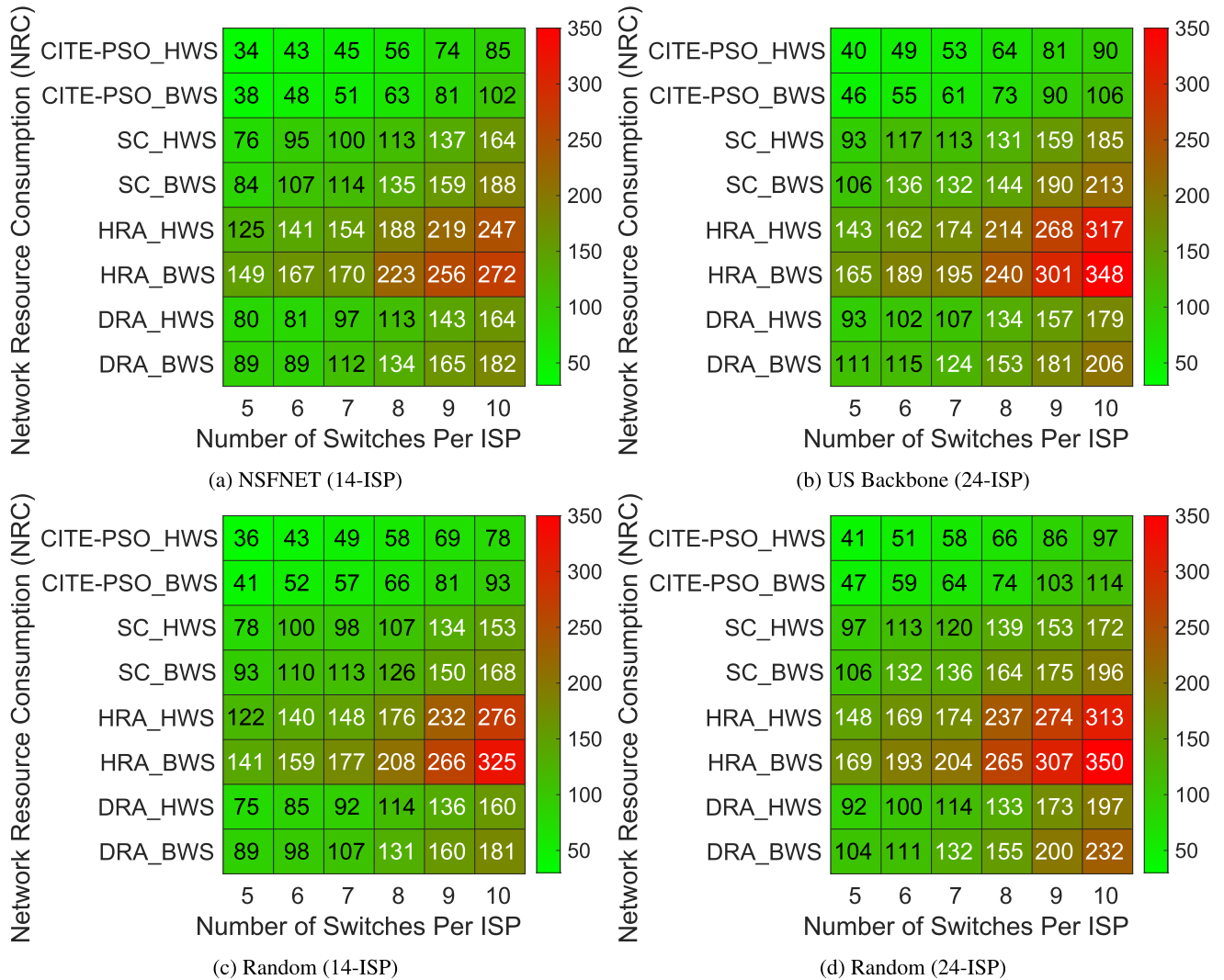


FIGURE 10. Network resource consumption (NRC) in CITE-PSO, SC, HRA and DRA with respect to HWS and BWS scenarios.

performance metric through a condensed approximation of the bandwidth-hop count product, as shown in Fig. 10.

Figs. 10a – 10d represent the total network resource consumption while varying the bandwidth demand of a service request (i.e., average 2-subcarrier per service) and number of switches per network with NSFNET, US Backbone, Random-14, and Random-24 inter-ISP network topologies, respectively. In Figs. 10a – 10d, the CITE-PSO approach outperforms the other approaches as much as by twice other approaches when the number of switches per network is up to 8. When the number of switches in ISP networks is higher than 8, the CITE-PSO framework still has better resource usage as much as by 50% and three times than SC, DRA, and HRA, respectively. This is because, as previously stated, the CITE-PSO seeks all available transactions for the lowest hop count when selecting a path for a service request, whereas the other approaches pick the first available or randomly appropriate transaction for faster path setup. Moreover, the CITE-PSO and SC frameworks are seen to use similar BC-based path selection in inter-ISPs, whereas the

CITE-PSO considers picking an E2E path with less number of hops for the entire network by using all available transactions in the BC. This occurs because CITE-PSO leverages the capability to choose the most suitable particle, exploring an extensive solution space to identify optimal outcomes with a minimal number of hops along the E2E path over inter-ISPs.

E. AVERAGE PATH LENGTH (APL)

The Average Path Length (APL) is a metric to gauge the average distance or number of hops between nodes (or switches) within operational networks. A lower APL signifies improved efficiency and accelerated communication between network components. APL is of considerable significance in network design and optimization, directly impacting bandwidth utilization, latency, and the overall effectiveness of the network.

In a similar environmental setup as in PST, NMO, etc., the values of APL exhibit substantial variation depending on the

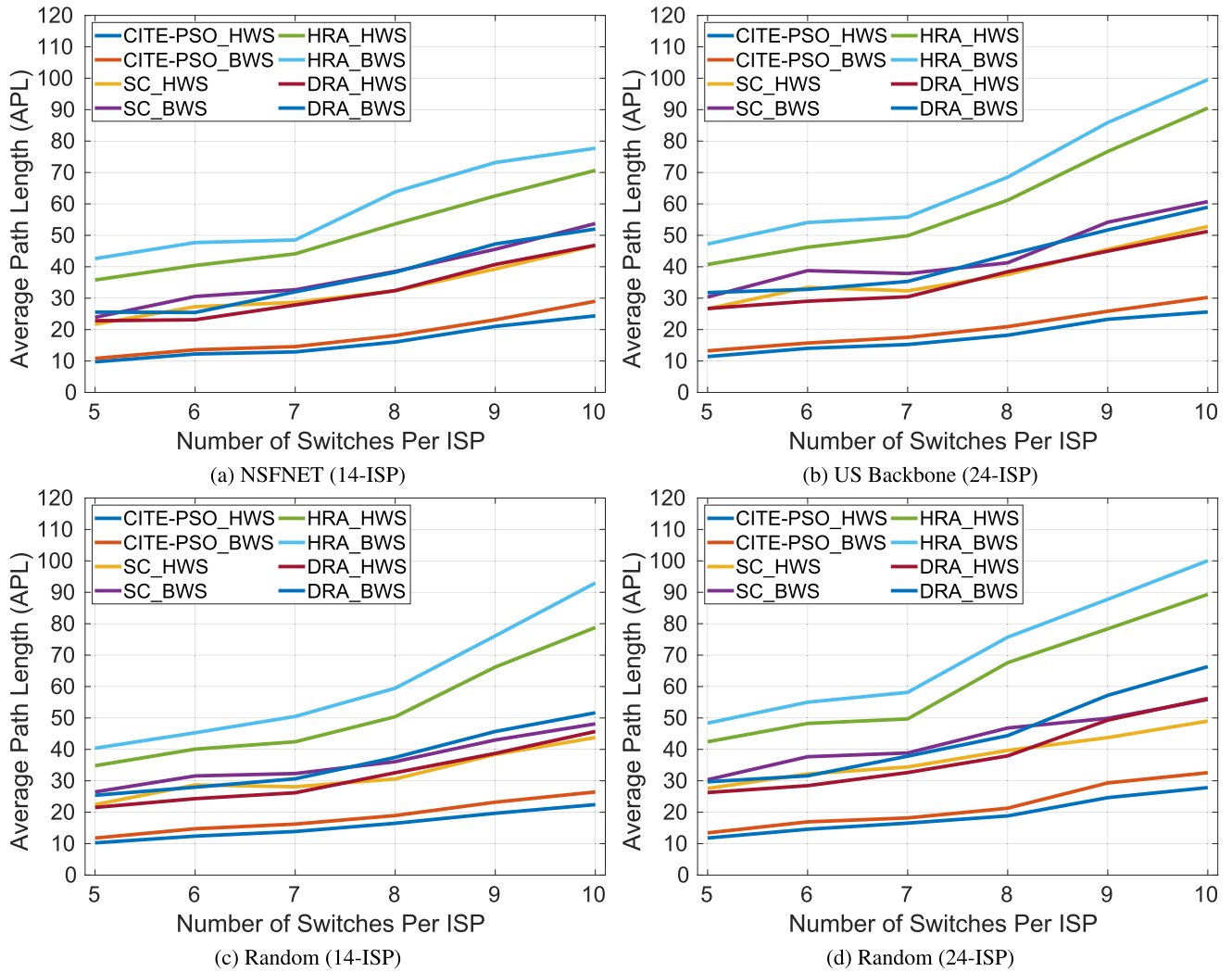


FIGURE 11. Average Path Length (APL) in CITE-PSO, SC, HRA and DRA with respect to HWS and BWS scenarios.

specific characteristics of the network topology, as shown in Fig. 11.

When comparing the *CITE-PSO_HWS* and *CITE-PSO_BWS* algorithms with the *SC_HWS* and *SC_BWS* algorithms in Figs. 11a–11d, it becomes apparent that the *CITE-PSO* often provide lower APL values as much as by %50 than *SC*. In situations including wavelength switching at each hop and across borders, the efficiency of APL reduction is demonstrated by *CITE-PSO_HWS* and *CITE-PSO_BWS*. Thanks to the utilization of optimization-powered techniques, particularly the implementation of PSO, *CITE-PSO* demonstrates superior performance compared to *SC*, *DRA*, and *HRA*. Despite *SC* and *CITE-PSO* employing BC-based E2E routing, *SC* relies on randomly available pathlet selection, resulting in higher APL values. This implies that *CITE-PSO* is more efficient than the *SC* framework. The *CITE-PSO* uses a PSO approach to find cost-effective particles from a wide range of solutions, leading to lower resource usage and reduced delays. In summary, the *CITE-PSO_HWS* and *CITE-PSO_BWS*, which utilize optimization techniques, have demonstrated superior

performance compared to other approaches in terms of lowering APL. This underscores the significance of including routing methods in the design and administration of networks.

F. NETWORK PATH LENGTH (NPL)

The Network Path Length (NPL) is another crucial metric for assessing multi-ISP resource optimization in SDONs, directly influencing network performance and efficiency. The NPL measures the mean number of ISP uses or ISP-based distances that data packets traverse within an SDON. A decrease in NPL often signifies shorter routes, leading to reduced network resource usage and improved QoS. The adaptive network layer is a key part of comparing different QoS-based routing systems in different SDON topologies, which is why NPL is an important metric in this case.

The analysis of NPL values reveals notable disparities among the various network topologies, namely NSFNET, US Backbone, Random14, and Random24, as shown in Figs. 12a–12d, similar to the previous metrics. In terms of typical network lengths, NSFNET and Random14 inter-ISP

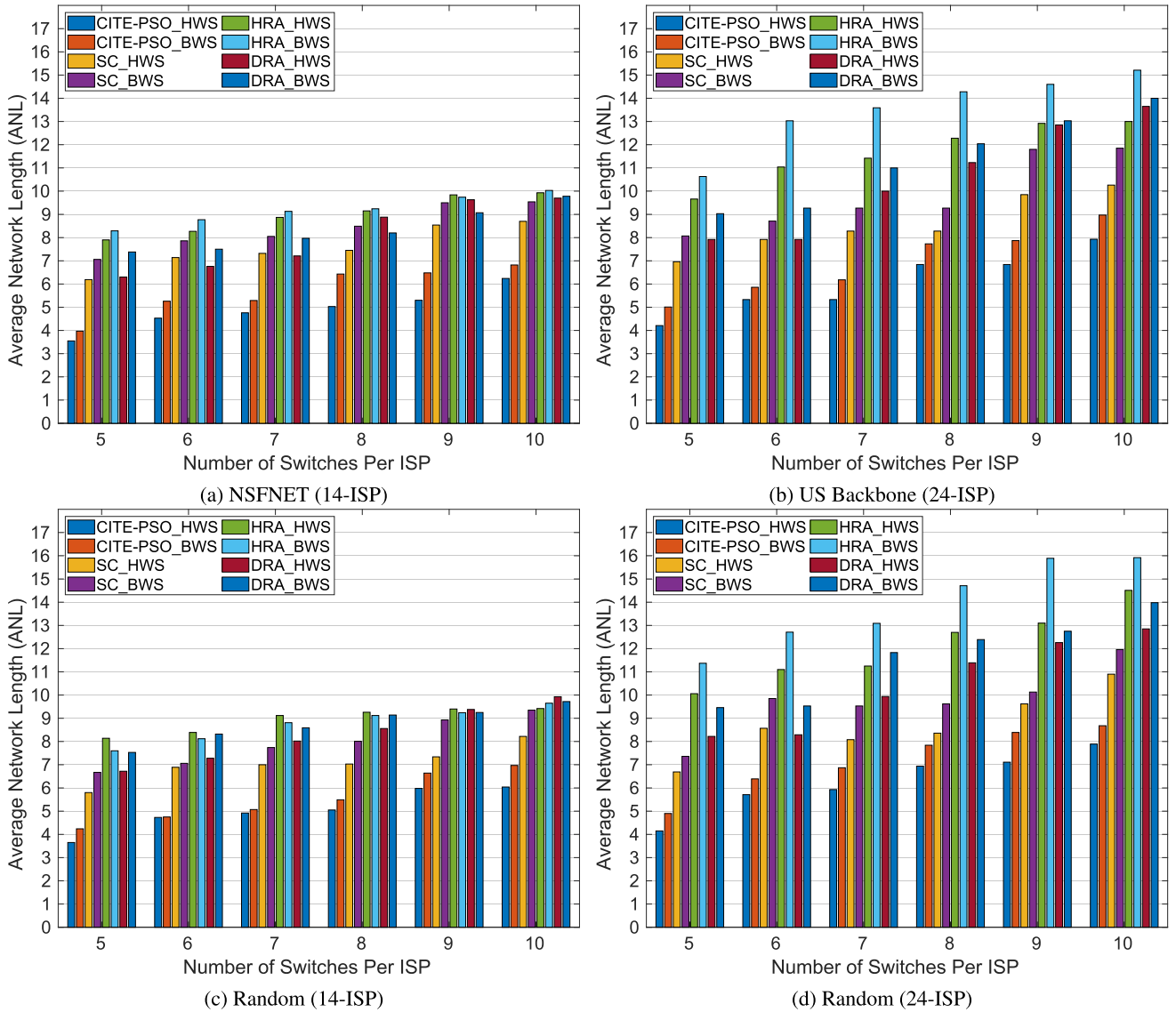


FIGURE 12. Network Path Length (NPL) in CITE-PSO, SC, HRA and DRA with respect to HWS and BWS scenarios.

network topologies demonstrate the shortest distances on average, while US Backbone and Random-24 tend to have slightly higher path lengths. This observation underscores the substantial impact of network layout on the efficiency of routing. As the number of switches inside a network expands, as shown in Figs. 12a–12d, there is a tendency for network resource usage.

The proposed CITE-PSO framework provides superior performance in terms of NPL across all topologies and switch configurations when compared to SC, HRA, and DRA approaches with both wavelength switching scenarios. The results show that using PSO in QoS-aware cross-optical network traffic management frameworks based on BC technology usually leads to shorter NPLs than the other examined frameworks. Reduced resource usage in the networks is typically favored due to their association with enhanced routing efficiency, which can provide notable benefits inside SDON networks. Border-node-only wavelength switching

incurs slightly higher path lengths over the networks than hop-by-hop wavelength switching scenarios as shown in Figs. 12a–12d due to the use of longer paths to support continuity and contiguous subcarrier assignments.

Furthermore, when comparing CITE-PSO_HWS and CITE-PSO_BWS with SC_HWS and SC_BWS, we find that the optimization-driven CITE-PSO framework provides more effective routing with significantly shorter NPLs compared to basic BC-centric solutions. These results improve our understanding of SDON optimization and routing techniques. The CITE-PSO uses particle swarm optimization to find better paths through multiple ISPs using BC-based technology.

VI. DISCUSSION AND CHALLENGES

The current research introduces the CITE-PSO framework, employing Particle Swarm Optimization (PSO) to effectively

manage Cross-ISP Traffic Engineering (CITE) in Blockchain (BC)-enabled Software-Defined Optical Networks (SDON). The primary focus is on ensuring Quality of Service (QoS) throughout the End-to-End (E2E) traffic flow. Despite the promise of this framework, there are areas requiring further refinement and enhancement, prompting the identification of numerous potential avenues for future research and development. This section conducts a thorough analysis of various constraints, problems, and potential directions for future investigation within the proposed *CITE-PSO* framework.

A. BC LEDGER OBSOLESCENCE

Transactions within the *CITE-PSO* framework involve encapsulated pathlets and are susceptible to ongoing modifications due to network dynamics and variations in traffic conditions. These transactions follow a sequential process, starting with the initiation of a transaction following any modification in the state of a pathlet. The process involves transmission to block proposer nodes, waiting for inclusion in the new block, dissemination through the BC network, and eventual recording in the BC ledger.

However, a potential challenge arises in the form of BC Ledger Obsolescence. This issue stems from the fact that the state change of the pathlet in the transaction may not persist until accurately recorded in the BC ledger. Similar to routine updates in conventional networks, there is a risk that certain transactions may not faithfully represent the current and most recent states of pathlets on the BC. In other words, there might be a time gap between the modification in the pathlet's state and its accurate reflection in the BC ledger, potentially leading to discrepancies and obsolescence in the recorded data.

B. BLOCK TIME

Also referred to as the block interval, this period assumes significant importance in enhancing the overall transaction throughput of the model and ensuring timely updates to the BC ledger based on pathlet status updates from ISPs. However, this temporal metric introduces the potential for increased computational demands on network controllers and greater utilization of link resources within networks. Striking a nuanced balance between block generation duration, associated computing burden, and BC ledger obsolescence becomes crucial.

C. BC STORAGE

The *CITE-PSO* framework models transactions within networks as pathlets containing network topology and QoS information. ISPs, with their intricate characteristics encompassing size, topology, services, and user dynamics, frequently undergo modifications during their operational lifespan. These modifications are captured in recent transactions disseminated across interconnected networks.

BC storage challenge pertains to the potential long-term limitations arising from the storage requirements, while

BC Ledger Obsolescence deals with the accuracy and timeliness of recording transactions. As networks evolve, the increasing volume of transactions may lead to a significant amount of data being stored in the BC ledger, impacting storage capacity. The primary difference lies in their focus and implications. BC Ledger Obsolescence addresses the risk of outdated information due to delays in recording, impacting the real-time representation of pathlet states. On the other hand, this storage challenge concerns long-term storage capacity, anticipating challenges associated with an increasing volume of transactions and potential impacts on network overhead managed by controllers. While BC Ledger Obsolescence is more immediate in its consequences, BC storage poses a concern for the sustainable storage and management of historical network data over an extended period.

D. CONSENSUS PROTOCOL OVERHEAD

Consensus protocols are crucial in reducing the workload on network controllers in SDON settings. Future research aims to explore consensus methods that are lightweight, robust, and efficient, considering the associated trade-offs. The suggested *CITE-PSO* framework, where ISP controllers act as BC nodes, raises concerns about imposing computationally intensive tasks on these entities, such as solving cryptographic challenges for block creation. To address this challenge, a lightweight and efficient consensus mechanism could be a remedy to ease the load on controllers. Additionally, thorough investigations into network and controller overhead are considered valuable for addressing the spatial aspect of the identified constraints and issues.

In light of these considerations, BC technology emerges as a widely recognized disruptive innovation with substantial promise. The potential application of BC technology in routing stands out as a notable use case, contingent upon the effective resolution of the identified issues by researchers and professionals across academic and industrial sectors.

VII. CONCLUSION AND FUTURE WORK

The escalating demand for data traffic, marked by its volume and speed, coupled with the persistent dynamic shifts, exerts substantial pressure on Internet Service Providers (ISPs) and their communication networks. Elastic Optical Networks (EONs) present a promising solution, given their distinctive attributes in bandwidth aggregation, segmentation, and provisioning of variable data rates. The synergy of EONs with Software-Defined Optical Networking (SDON) further augments their potential. This study introduces an innovative approach to improving network resource efficiency within the realm of Cross-ISP Traffic Engineering enhanced by Particle Swarm Optimization (CITE-PSO).

In this study, the proposed framework, referred to as *CITE-PSO*, integrates Particle Swarm Optimization (PSO) into a Quality of Service (QoS)-enabled inter-ISP spectrum management and routing framework. This novel combination incorporates a routing model prioritizing QoS with

Blockchain (BC) technology in SDONs, representing the first instance of such integration in the literature. The *CITE-PSO* framework establishes a spectrum management and coordination framework that fosters collaboration among conflicting parties in routing. Leveraging the decentralized nature of BC technology eliminates the need for third-party entities in QoS-supported inter-ISP routing models. Notably, the *CITE-PSO* framework simultaneously addresses privacy and security concerns faced by ISPs during inter-ISP routing collaboration. Simulations incorporate Hop-by-Hop Wavelength Switching (HWS) and Border-Node-Only Wavelength Switching (BWS), providing a comprehensive understanding of system performance under varying operational conditions.

Future works could focus on the integration of different consensus mechanisms such as Practical Byzantine Fault Tolerance, Proof of Stake, Proof of Weight, etc. These mechanisms aim to further enhance the adaptability, efficiency, and overall performance of the *CITE-PSO* framework in dynamic and evolving network environments. Additionally, exploring AI-based optimization techniques, including Federated Learning, Recurrent Neural Networks, Reinforcement Learning, etc., could provide more detailed insights into the framework's capabilities, ensuring robustness and effective decision-making in complex network scenarios.

REFERENCES

- [1] A. Holst. (2021). *Total Data Volume Worldwide 2010-2025*. [Online]. Available: <https://www.statista.com/statistics/871513/worldwide-data-created/>
- [2] A. Hakiri, A. Gokhale, P. Berthou, D. C. Schmidt, and T. Gayraud, "Software-defined networking: Challenges and research opportunities for future internet," *Comput. Netw.*, vol. 75, pp. 453–471, Dec. 2014.
- [3] M. Karakus, E. Guler, and S. Uludag, "QoSChain: Provisioning inter-AS QoS in software-defined networks with blockchain," *IEEE Trans. Netw. Service Manag.*, vol. 18, no. 2, pp. 1706–1717, Jun. 2021.
- [4] S. W. Turner, M. Karakus, E. Guler, and S. Uludag, "A promising integration of SDN and blockchain for IoT networks: A survey," *IEEE Access*, vol. 11, pp. 29800–29822, 2023.
- [5] E. Guler, M. Karakus, and S. Uludag, "Blockchain-enhanced cross-ISP spectrum assignment framework in SDONs: SpectrumChain," *Comput. Netw.*, vol. 223, Mar. 2023, Art. no. 109579.
- [6] Y. Wang, X. Cao, and Y. Pan, "A study of the routing and spectrum allocation in spectrum-sliced elastic optical path networks," in *Proc. IEEE INFOCOM*, Feb. 2011, pp. 1503–1511.
- [7] M. Klinkowski and K. Walkowiak, "Routing and spectrum assignment in spectrum sliced elastic optical path network," *IEEE Commun. Lett.*, vol. 15, no. 8, pp. 884–886, Aug. 2011.
- [8] A. S. Thyagaturu, A. Mercian, M. P. McGarry, M. Reisslein, and W. Kellerer, "Software defined optical networks (SDONs): A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 4, pp. 2738–2786, 4th Quart., 2016.
- [9] M. Karakus and E. Guler, "RoutingChain: A proof-of-concept model for a blockchain-enabled QoS-based inter-AS routing in SDN," in *Proc. IEEE Int. Black Sea Conf. Commun. Netw. (BlackSeaCom)*, May 2020, pp. 1–6.
- [10] E. Guler, M. Karakus, and S. Uludag, "Evaluating path selection strategies with blockchain-based routing in multi-domain SDNs," in *Proc. Int. Balkan Conf. Commun. Netw. (BalkanCom)*, Sarajevo, Bosnia and Herzegovina, Aug. 2022, pp. 6–10.
- [11] M. Karakus, "Implementation of blockchain-assisted source routing for traffic management in software-defined networks," *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*, vol. 11, no. 3, pp. 1250–1268, 2023.
- [12] M. Saad, A. Anwar, A. Ahmad, H. Alasmay, M. Yuksel, and A. Mohaisen, "RouteChain: Towards blockchain-based secure and efficient BGP routing," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, Nov. 2019, pp. 210–218.
- [13] M. Karakus and A. Durrresi, "A scalable inter-AS QoS routing architecture in software defined network (SDN)," in *Proc. IEEE 29th Int. Conf. Adv. Inf. Netw. Appl.*, Mar. 2015, pp. 148–154.
- [14] E. Ak and B. Canberk, "BCDN: A proof of concept model for blockchain-aided CDN orchestration and routing," *Comput. Netw.*, vol. 161, pp. 162–171, Oct. 2019.
- [15] J. Yang, S. He, Y. Xu, L. Chen, and J. Ren, "A trusted routing scheme using blockchain and reinforcement learning for wireless sensor networks," *Sensors*, vol. 19, no. 4, p. 970, Feb. 2019.
- [16] G. Ramezan and C. Leung, "A blockchain-based contractual routing protocol for the Internet of Things using smart contracts," *Wireless Commun. Mobile Comput.*, vol. 2018, pp. 1–14, Nov. 2018.
- [17] P. Wang, X. Liu, J. Chen, Y. Zhan, and Z. Jin, "QoS-aware service composition using blockchain-based smart contracts," in *Proc. ICSE*. New York, NY, USA: Association for Computing Machinery, 2018, pp. 296–297.
- [18] P. Kamboj and S. Pal, "QoS in software defined IoT network using blockchain based smart contract: Poster abstract," in *Proc. SenSys*. New York, NY, USA: Association for Computing Machinery, 2019, pp. 430–431.
- [19] Y. E. Oktian, E. N. Witanto, S. Kumi, and S.-G. Lee, "ISP network bandwidth management: Using blockchain and SDN," in *Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Oct. 2019, pp. 1330–1335.
- [20] M. Kayalvizhi and S. Ramamoorthy, "Blockchain-based secure data transmission for UAV swarm using modified particle swarm optimization path planning algorithm," *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 11, pp. 554–563, 2021.
- [21] C. Nartey, E. T. Tchao, J. D. Gadze, B. Yeboah-Akokuah, H. Nunoo-Mensah, D. Welte, and A. Sikora, "Blockchain-IoT peer device storage optimization using an advanced time-variant multi-objective particle swarm optimization algorithm," *EURASIP J. Wireless Commun. Netw.*, vol. 2022, no. 1, pp. 1–27, Dec. 2022.
- [22] R. Nourmohammadi and K. Zhang, "An on-chain governance model based on particle swarm optimization for reducing blockchain forks," *IEEE Access*, vol. 10, pp. 118965–118980, 2022.
- [23] K. H. K. Reddy, A. K. Luhach, V. V. Kumar, S. Pratihari, D. Kumar, and D. S. Roy, "Towards energy efficient smart city services: A software defined resource management scheme for data centers," *Sustain. Comput., Informat. Syst.*, vol. 35, Sep. 2022, Art. no. 100776.
- [24] M. U. Sana, Z. Li, F. Javaid, M. W. Hanif, and I. Ashraf, "Improved particle swarm optimization based on blockchain mechanism for flexible job shop problem," *Cluster Comput.*, vol. 26, no. 5, pp. 2519–2537, Oct. 2023.
- [25] Q. Zhang, H. Li, Y. Liu, S. Ouyang, C. Fang, W. Mu, and H. Gao, "A new quantum particle swarm optimization algorithm for controller placement problem in software-defined networking," *Comput. Electr. Eng.*, vol. 95, Oct. 2021, Art. no. 107456.
- [26] L. Al-Tarawneh and O. A. Saraereh, "An optimal method for resource allocation in SDN optical networks," *Opt. Fiber Technol.*, vol. 74, Dec. 2022, Art. no. 103120.
- [27] I. Wayan Budi Sentana, M. Ikram, and M. Ali Kaafar, "BlockJack: Towards improved prevention of IP prefix hijacking attacks in inter-domain routing via blockchain," 2021, *arXiv:2107.07063*.
- [28] S. Awan, N. Javaid, S. Ullah, A. U. Khan, A. M. Qamar, and J.-G. Choi, "Blockchain based secure routing and trust management in wireless sensor networks," *Sensors*, vol. 22, no. 2, p. 411, Jan. 2022.
- [29] W. Jerbi, O. Cheikhrouhou, A. Guermazi, M. Baz, and H. Trabelsi, "BSI: Blockchain to secure routing protocol in Internet of Things," *Concurrency Comput., Pract. Exper.*, vol. 34, no. 10, p. e6794, May 2022.
- [30] X. Ling, P. Chen, J. Wang, and Z. Ding, "Data broker: Dynamic multi-hop routing protocol in blockchain radio access network," *IEEE Commun. Lett.*, vol. 25, no. 12, pp. 4000–4004, Dec. 2021.
- [31] C. Ran, S. Yan, L. Huang, and L. Zhang, "An improved AODV routing security algorithm based on blockchain technology in ad hoc network," *EURASIP J. Wireless Commun. Netw.*, vol. 2021, no. 1, pp. 1–16, Dec. 2021.
- [32] M. Revanesh and V. Sridhar, "A trusted distributed routing scheme for wireless sensor networks using blockchain and meta-heuristics-based deep learning technique," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 9, p. e4259, Sep. 2021.
- [33] H. Yang, *Optical and Wireless Convergence Network Based on Blockchain*. Cham, Switzerland: Springer, 2022, pp. 131–143.

- [34] P. Fernando and J. Wei, "Blockchain-powered software defined network-enabled networking infrastructure for cloud management," in *Proc. IEEE 17th Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2020, pp. 1–6.
- [35] F. Chen, Z. Li, B. Li, C. Deng, Z. Tian, N. Lin, Y. Wan, and B. Bao, "Blockchain-based optical network slice rental approach for IoT," in *Proc. IEEE Comput., Commun. IoT Appl. (ComComAp)*, Dec. 2020, pp. 1–4.
- [36] W. Hou, Z. Ning, L. Guo, and P. Guo, "SDN-based optimizing solutions for multipath data transmission supporting consortium blockchains," in *Proc. Int. Conf. Comput., Inf. Telecommun. Syst. (CITS)*, Jul. 2018, pp. 1–5.
- [37] S. Ding, G. Shen, K. X. Pan, S. K. Bose, Q. Zhang, and B. Mukherjee, "Blockchain-assisted spectrum trading between elastic virtual optical networks," *IEEE Netw.*, vol. 34, no. 6, pp. 205–211, Nov. 2020.
- [38] H. Yang, Y. Liang, Q. Yao, S. Guo, A. Yu, and J. Zhang, "Blockchain-based secure distributed control for software defined optical networking," *China Commun.*, vol. 16, no. 6, pp. 42–54, Jun. 2019.
- [39] Q. Qiao, X. Li, Y. Wang, B. Luo, Y. Ren, and J. Ma, "Credible routing scheme of SDN-based cloud using blockchain," in *Proc. 5th Int. Conf. Pioneering Comput. Scientists, Eng. Educators (ICPCSEE)*, Guilin, China, Sep. 2019, pp. 189–206.
- [40] A. Arins, "Blockchain based inter-domain latency aware routing proposal in software defined network," in *Proc. IEEE 6th Workshop Adv. Inf., Electron. Electr. Eng. (AIEEE)*, Nov. 2018, pp. 1–2.
- [41] M. Hassan, M. Gregory, and S. Li, "Blockchain enhanced BGP4 security for an SDN based federation," in *Proc. 32nd Int. Telecommun. Netw. Appl. Conf. (ITNAC)*, Nov. 2022, pp. 1–7.
- [42] T. Kayathri, N. Kumaresan, and R. V. Bhasker, "SDBGPChain: A decentralized low complexity framework to detect and prevent the bgpdendrimer tree blockchain attacks using SDN with smart contract based," *Comput. Netw.*, vol. 230, Jul. 2023, Art. no. 109800.
- [43] Z. Zeng, X. Zhang, and Z. Xia, "Intelligent blockchain-based secure routing for multidomain SDN-enabled IoT networks," *Wireless Commun. Mobile Comput.*, vol. 2022, pp. 1–10, Feb. 2022.
- [44] A. Aldaej, M. Atiquzzaman, T. A. Ahanger, and P. K. Shukla, "Multidomain blockchain-based intelligent routing in UAV-IoT networks," *Comput. Commun.*, vol. 205, pp. 158–169, May 2023.
- [45] P. Alemany, R. Vilalta, R. Muñoz, R. Martínez, and R. Casellas, "Managing network slicing resources using blockchain in a multi-domain software defined optical network scenario," in *Proc. Eur. Conf. Opt. Commun. (ECOC)*, Dec. 2020, pp. 1–4.
- [46] S. Fichera, A. Sgambelluri, F. Paolucci, A. Giorgetti, N. Sambo, P. Castoldi, and F. Cugini, "Blockchain-anchored disaggregated optical networks," *J. Lightw. Technol.*, vol. 39, no. 20, pp. 6357–6365, Oct. 2021.
- [47] S. Fichera, N. Sambo, F. Paolucci, F. Cugini, and P. Castoldi, "Leveraging blockchain to ratify QoT performance in multi-domain optical networks," in *Proc. 45th Eur. Conf. Opt. Commun. (ECOC)*, Sep. 2019, pp. 1–4.
- [48] P. Alemany, R. Vilalta, R. Munoz, R. Casellas, and R. Martinez, "Evaluation of the abstraction of optical topology models in blockchain-based data center interconnection," *J. Opt. Commun. Netw.*, vol. 14, no. 4, pp. 211–221, Apr. 2022.
- [49] E. Guler, M. Karakus, and S. Uludag, "SpectrumChain: An efficient spectrum management framework in blockchain-enabled flexible SDNs," in *Proc. IEEE Int. Conf. Commun.*, May 2022, pp. 5744–5749.
- [50] P. Podili and K. Kataoka, "TRAQR: Trust aware end-to-end QoS routing in multi-domain SDN using blockchain," *J. Netw. Comput. Appl.*, vol. 182, May 2021, Art. no. 103055.
- [51] M. M. Shabir, S. M. Danish, and K. Zhang, "BlockQoS: Fair monetization of on-demand quality-of-service using blockchains," *Distrib. Ledger Technol., Res. Pract.*, vol. 2, no. 2, pp. 1–25, 2023.
- [52] S. Abbas, N. Javaid, A. Almogren, S. M. Gulfam, A. Ahmed, and A. Radwan, "Securing genetic algorithm enabled SDN routing for blockchain based Internet of Things," *IEEE Access*, vol. 9, pp. 139739–139754, 2021.
- [53] S. Kou, H. Yang, H. Zheng, W. Bai, J. Zhang, and Y. Wu, "Blockchain mechanism based on enhancing consensus for trusted optical networks," in *Proc. Asia Commun. Photon. Conf. (ACP)*, 2017, pp. 1–3.
- [54] M. Karakus, E. Guler, and S. Uludag, "Smartcontractchain (SC²): Cross-ISP QoS traffic management framework with SDN and blockchain," *Peer-Peer Netw. Appl.*, vol. 16, no. 6, pp. 3003–3020, 2023.
- [55] Y. Liu, N. Hua, X. Zheng, H. Zhang, and B. Zhou, "Discrete spectrum-scan routing based on spectrum discretization in flexible optical networks," in *Proc. OFC/NFOEC*, Mar. 2012, pp. 1–3.
- [56] F. Skopik, G. Settanni, and R. Fiedler, "A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing," *Comput. Secur.*, vol. 60, pp. 154–176, Jul. 2016.
- [57] K. D. Joshi and K. Kataoka, "PRIME-Q: Privacy aware end-to-end QoS framework in multi-domain SDN," in *Proc. IEEE Conf. Netw. Softwarization (NetSoft)*, Jun. 2019, pp. 169–177.
- [58] P. Zhang, Y. Hong, X. Pang, and C. Jiang, "VNE-HPSO: Virtual network embedding algorithm based on hybrid particle swarm optimization," *IEEE Access*, vol. 8, pp. 213389–213400, 2020.
- [59] D. Wang, D. Tan, and L. Liu, "Particle swarm optimization algorithm: An overview," *Soft Comput.*, vol. 22, pp. 387–408, Jan. 2018.
- [60] M.-C. Yuen, S.-C. Ng, and M.-F. Leung, "A competitive mechanism multi-objective particle swarm optimization algorithm and its application to signalized traffic problem," *Cybern. Syst.*, vol. 52, no. 1, pp. 73–104, Jan. 2021.
- [61] W. Fadini, B. C. Chatterjee, and E. Oki, "A subcarrier-slot partition scheme with first-last fit spectrum allocation for elastic optical networks," *Comput. Netw.*, vol. 91, pp. 700–711, Nov. 2015.



EVRYM GULER received the M.Sc. degree in computer science from the University of Michigan-Flint and the Ph.D. degree in computer science from Georgia State University, where his research focused on multicast aware virtual network embedding in software-defined networks. He is currently an Assistant Professor with the Department of Computer Engineering, Bartin University, and a Seasoned Researcher with over a decade of experience in IT, advanced analytics, and optimization techniques. His passion lies in tackling complex problems that demand a blend of mathematics, operational research, and creative solutions. He has published extensively in top-tier journals and conferences, contributing significantly to areas, such as software-defined networks, elastic optical networks, multicast tree embedding, and blockchain technologies. His academic journey has been marked by prestigious scholarships and awards. In addition to his research work, his contributions extend beyond academia, as he has held leadership roles in student associations, demonstrating his commitment to community, and leadership.

...