IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 23, 2021, accepted August 2, 2021, date of publication August 9, 2021, date of current version August 18, 2021.

*Digital Object Identifier 10.1109/ACCESS.2021.3103241*

# The Implementation of Border Gateway Protocol Using Software-Defined Networks: A Systematic Literature Review

**XI ZHAO[1], SHAHAB S. BAND[2], SAID ELNAFFAR[3,4], MEHDI SOOKHAK[5], (Senior Member, IEEE), AMIR MOSAVI[6,7], AND ELY SALWANA[8]**

[1]School of Information and Communication Engineering, Communication University of China, Beijing 100024, China
[2]Future Technology Research Center, College of Future, National Yunlin University of Science and Technology, Douliou, Yunlin 64002, Taiwan
[3]Faculty of Engineering, Applied Science and Technology, Canadian University Dubai, Dubai, United Arab Emirates
[4]College of Computer Information Technology, American University in the Emirates, Dubai, United Arab Emirates
[5]School of Information Technology, Illinois State University, Normal, IL 61761, USA
[6]Faculty of Civil Engineering, Technische Universität Dresden, 01069 Dresden, Germany
[7]John von Neumann Faculty of Informatics, Óbuda University, 1034 Budapest, Hungary
[8]Institute of IR4.0, Universiti Kebangsaan Malaysia, Bangi, Selangor 43600, Malaysia

Corresponding authors: Xi Zhao (zhaoxi54321@cuc.edu.cn), Shahab S. Band (shamshirbands@yuntech.edu.tw), and Amir Mosavi (amir.mosavi@mailbox.tu-dresden.de)

The open access funding by the publication fund of the TU Dresden.

**ABSTRACT** As a global community, the Internet is comprised of thousands of administrative entities that operate and interact with each other. Transferring data among these entities is possible due to the process of routing, which is challenging due to the lack of centrality. Consequently, the Border Gateway Protocol (BGP) can play a vital role in the routing process as a central hub for disseminating routing information to the various autonomous systems. Yet, the BGP poses security vulnerability due to the difficulty of validation and authentication. Recent studies argue that it would be beneficial to apply the Software-Defined Networking (SDN) approach to address some of the BGP problems. The SDN can help handle BGP-based networks at a low cost and with minimal complexity. However, there are still many scientific and operational problems in this field of study. The main objective of this paper is to identify the challenges that the BGP facing with respect to the adoption of the SDN. The findings revealed that most researchers focused on improving convergence time, while other essential features such as scalability and privacy were overlooked.

**INDEX TERMS** Border gateway protocol, software defined networks, routing, autonomous systems, review.

## I. INTRODUCTION

The Internet is made up of numerous smaller interconnected networks, including end systems like hosts and intermediate systems like routers [1], [2]. Information can also travel on a single path through a network determined by a routine procedure. An Autonomous System (AS) is a network that is managed by a single organization. Each AS employs two routing protocols: intra-AS routing and inter-AS routing protocols [3]. Intra-AS routing is based on Interior Gateway Protocols (IGPs), such as Intermediate System to Intermediate System routing (IS-IS). This topology information is distributed within the AS, and all routers will receive it. As a result, this mechanism cannot be accessed outside of the AS [4]. As a single administrator manages the whole routers, the local administrator decides the AS's methodologies. Inter-AS routing is used among the ASes and is distinct [5]. The Border Gateway Protocol (BGP) routing protocol enables routers to share routing information on a regular basis. BGP may transmit information and data among various host gateways via the Internet or ASes. It is a Path Vector Protocol (PVP) that provides routes to multiple hosts, networks, and gateway routers to determine routing [6].

Since the early days of basic file sharing and hosting of distributed applications on servers, the types of network problems have changed dramatically [7]. Recently, organizations are increasingly employing advanced computing systems to satisfy their requirements, including cloud-based systems, virtualized resources, servers, and remote storage that need extra computing resources, work, and

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

arrangement [8], [9]. However, despite their pervasive adoption, traditional IP-based networks are complex and challenging to manage. *Software-Defined Networking* (SDN) has been recently advertised as a game changer for the future Internet [10], [11]. The SDN implements novel network management options and configuration approaches [12] by separating the data plane from the control plane and pushing the scalable and effective management capabilities to software applications [13], [14] that adopt the concept of the SDN. Generally, the SDN can supply higher performance, effective configuration, and more flexibility [8], [15], [16].

Intra-domain BGP protocol provides high scalability and can be universally adopted. However, it suffers from: potential correctness failures, shortage of route diversity, and Internal BGP (IBGP) messaging duplication [17]. The high workload of backbone routers and its effect on the scale of services is the main reason for the emergence of the SDN by removing routing hardware and transferring the complexity to software [17], [18]. This paper examines the existing limitations of the BGP by a systematic literature review (SLR) and surveys the SDN approaches used to overcome shortcomings. The primary contributions of the present investigation are:

- Reviewing BGP architecture, studying the current approaches in BGP protocol, and expressing its limitations;
- Explaining the implementation of SLR in BGP and SDN;
- Addressing the major BGP problems;
- Reviewing SDN architecture and studying the current approaches of SDN protocols;
- Describing the main advantages of the BGP protocol;
- Supplying an accurate assessment of the processes addressed using certain metrics.

Our literature review methodology is explained in Section 2. A review of existing studies is described in Section 3. The comparison methods are discussed in Section 4. Open issues are given in Section 5, and we conclude this work in Section 6.

## II. METHODOLOGY

Our work is based on the SLR (Systematic Literature Review) method has been used. It is a notion for detecting, evaluating, and inferring the present works associated with a specific research question/subject [19]–[22]. Scholars have tested the research, chosen the assessment devices, and extracted them [23]–[25]. They have also extracted the elements and pointers, integrated them, and proposed them in an outline to assess the BGP and SDN mechanism. Firstly, the theoretical and experimental basics in previous works have been applied for data gathering. Then, by answering the following study concerns, this section seeks to summarize the most important problems and challenges in the BGP:

*Research Question 1:* What is the importance of SDN strategies in the BGP?

This question is answered in Section 3.

*Research Question 2:* How much SDN strategies satisfy the basic BGP metrics?

This question is answered in Section 4.

*Research Question 3:* What problems are determined regarding BGP in the future?

This question is responded to in Section 6.

## III. OVERVIEW OF EXISTING METHODS

The BGP contains several restrictions associated with its completely distributed nature, policy implementation abilities, scalability, security, and complexity [26]. BGP is a key cyberspace mechanism that binds several autonomous systems. An autonomous system (AS) is the collection of networks with the same routing policies [27]. The infrastructures can be integrated with various applications, and the centralized control protocols can be developed using the SDN. One of the advantages of the SDN adoption is the integration with cloud computing where applications can be accessed on-demand [28], [29]. This integration will create dynamic networks and reduces infrastructure costs [12], [30], [31]. In addition, it improves packet transport times, and therefore the network performance, by segregating the packet switching layer from the control layer [32]. We categorize the papers we reviewed into three categories (see Fig 1).

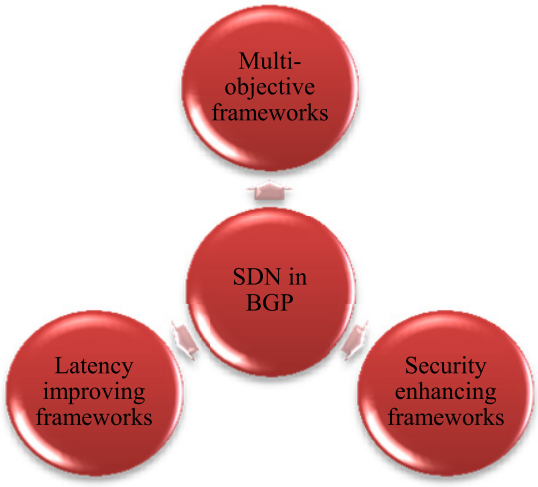


**FIGURE 1.** Classification of the selected articles.

### A. LATENCY IMPROVING FRAMEWORKS

The Internet is made up of AS or contexts, which are networks that belong to various administrative bodies. [33]. Routing between domains/ASes is done in a distributed fashion via BGP. Despite its widespread use, BGP has a number of flaws, such as slow convergence after routing changes, which can cause packet losses and disrupt contact for several minutes. SDN-based inter-domain routing centralization techniques have recently been introduced to accelerate convergence. Initial tests show that these methods can significantly improve control over BGPP efficiency and routing [34]. Furthermore,

Internet latency is primarily determined by the distance that packets travel through WAN networks. This delay may be reduced if the hops between AS are reduced. It is a key feature of the BGP mechanism that all ISPs use by default, but the lack of warning of some network segments allows certain routes to improve [35]. In this section, we review articles on frameworks that have tried to improve latency.

The impact of centralization on routing convergence of a hybrid BGP-SDN platform was assessed by Gämperli, *et al.* [36]. Several applications rely on stable and reliable Internet access, according to the writers' comment. In the proposed network model, they have used an SDN cluster made up of OpenFlow switches. According to this model, for tracking purposes, the whole BGP router peers with a BGP route collector may accumulate routing updates. Besides, they have a BGP speaker within the SDN cluster, called the BGP cluster speaker, transmitting routing information among the SDN controller and external BGP routers. Also, for every BGP peering, there is an association from the cluster BGP to the SDN switch. They have used Python for experimental setups. Low convergence time is a benefit of this model. However, this model does not take security difficulties and other BGP limitations into account, *et al.* [26] proposed a centralized routing model that implements the SDN paradigm. Through contracting routing functions to an external provider, who offers IDR services streamlined by a multi-AS network controller, multi-domain SDN centralization may be understood. They have also claimed that they introduced an emulation platform made on top of Mininet. This work leverages SDN to improve IDR properties while also allowing routing apps to execute through fields. Low convergence time and scalability are the benefits of the suggested model. This paper does not take the privacy issues, accuracy, and connectivity time into account.

The impacts of routing centralization on the IDR performance and the convergence time of BGP were analyzed by Sermpezis and Dimitropoulos [37]. Specifically, for inter-domain networks, they introduced a Markovian model in which a collection of nodes collaborates to centralize their inter-domain routing. They presented the proposed model in 2 main steps, BGP update and inter-domain SDN routing. The high accuracy for the full-mesh and Poisson graph, low convergence time, optimal centralization routing, high time/resource requirements, scalability, and good capability for overall network performance are the advantages of this model. But this model has some shortcomings. This model does not consider the privacy and security issues, whereas they are incompetent for the BGP update times.

Rzym, *et al.* [38] presented a new method for real-time application. In this method, they concentrated on an issue of optimization conceived in a manner that extends to real-time applications. They also investigated the Path Computation Element (PCE) using the 3-layered Traffic Engineering (TE) system consisting of a PCE module equipped with the CPLEX solver and an SDN controller. Moreover, diverse available strategies for applying PCE-based technologies for single and multi-domain networks have been analyzed and compared. In the multi-domain networks, they have presented diverse strategies ending with Label Switched Path (LSP) optimization in multi-domain networks, such as central PCE, standard backward path computation, PCE per domain without cooperation, hierarchical PCE, and standard backward recursive path computation. Finally, an overview of the implementation and application of the SDN framework using the PCE module in the multi-domain Multi-Protocol Label Switching (MPLS) network was provided, assisted by utilizing information obtained by the BGP-LS protocol. They used a virtualized environment for the demonstration of the presented concept. They also checked the effect of the number of requests for computing time and memory use to assess the suggested model. Time optimization and delay optimization with increasing simultaneous requests and memory usage predictable with increasing demands are this model's benefits. In this paper, the security and privacy problems are not considered.

To examine the effect of centralization on the IDR output, Sermpezis and Dimitropoulos [34] suggested a probabilistic paradigm. This paper concentrates on improving the BGP integration. Finally, practical architecture challenges were introduced, such as choosing the nodes to engage in the SDN cluster-based on efficiency requirements or network economics purposes. According to the proposed model, at least one path to other nodes is identified by each node in the network. They considered that a node named the ''source node'' declares a novel IP prefix. SDN cluster nodes obtain route information from the SDN administrator and include an entry to the source node in their RIB for the prefix, even if the path is not constructed. For evaluation of the proposed model, they simulated various scenarios with different network topologies, such as cluster sizes, synthetic graphs, and distributions of BGP update times. The suggested model's benefits are high precision, low convergence time, and low average connectivity time. The impacts of various network parameters, such as topology, network size, number of SDN nodes, or path lengths, are considered within this model on routing performance. Finally, security and scalability issues are not considered in this paper.

A method to optimize the BGP routes using SDN was suggested by Elguea and Martinez-Rios [35]. In this paper, the authors presented two basic BGP protocol issues and then suggested solving these two problems. Two methods are used by the BGP protocol that conducts traffic engineering. The initial one modifies the output provider for putting additional routes. The second approach modifies input routes and involves modifying by applying the AS to the number of hops the neighbors see. Sometimes these two processes decide that the routes are not optimal. Therefore, researchers also recommended a strategy of examining all the routes and primarily checking for the routes started by a neighbor for their directions. The proposed method has two main steps. The first step defines which routes can be optimized. The second step adds the new routes to the router. Analyzing the routes shows

low latency and BGP convergence time as the advantages of the proposed model. Also, in this model, the convergence time does not depend on the router's access paths. Finally, the security issue is not considered.

In order to distinguish irregular behavior of a network and to foresee and avoid BGP route hijacking (DPPBGP) in SDN, Pradeepa and Pushpalatha [39] suggested an intelligent model. With SFlow-integrated OpenFlow, the suggested model's key goal was to decrease the controller workload and the detection time. Integrating SFlow with the OpenFlow controller solves high network management benefits. An efficient and robust intelligent model for route hijack in SDN was the collaboration of CAD with the PSF (Python Software Foundation) prediction model. Their experimental outcomes illustrated a superior performance; the influence of hijack attacks can be identified with 100% accuracy and a false-positive rate of less than 6%. The assessment's overall findings revealed the new DPPBGP method's efficacy by reaching an accuracy level with less detection time.

Finally, Alotaibi, *et al.* [40] explored how to use the SDN model to optimize the multi-domain SDN traffic control and management process. An analysis into a modern multi-state BGP engine that decreases the high convergence time of BGP in multi-domain SDN has been implemented. The multi-state BGP seeks to boost traffic control operation among various independent systems for multi-domain SDN-based gateways. The study found that the field boundary gateways' programmability and flexibility needed to be enhanced to consider improvements in routing details and client traffic requests.

The reviewed papers in the latency improving frameworks category were 8 papers. These papers were analyzed in terms of some aspects, as shown in Table 1. Table 1 summarizes the articles' most essential features. The most important factors that researchers have tried to improve are convergence time, latency, scalability, accuracy, and detection time.

**TABLE 1. Comparison of the critical factors, advantage, and disadvantage of the latency-aware techniques.**

| Paper | Advantages of the proposed method | Disadvantage of the proposed method |
|---|---|---|
| [36] | • Low convergence time<br>• Low latency | • Low security |
| [26] | • Low convergence time<br>• High scalability<br>• Low latency | • Low privacy issues<br>• Low accuracy<br>• High connectivity time |
| [37] | • High accuracy<br>• Low convergence time<br>• Optimal centralization routing<br>• High time/resource requirements<br>• High scalability<br>• Low latency | • Low privacy<br>• Low security |
| [38] | • Delay optimization<br>• Low latency | • Low privacy<br>• Low security |
| [34] | • High accuracy<br>• Low average connectivity time<br>• Low convergence time<br>• Low latency | • Low scalability<br>• Low security |
| [35] | • Low latency<br>• Low BGP convergence time | • Low security |
| [39] | • High accuracy level<br>• Low detection time<br>• Low latency | • Low security |
| [40] | • Reducing the high BGP convergence time<br>• Low latency | • Low flexibility |

### *B. SECURITY ENHANCING FRAMEWORKS*

Communication on the Internet, including a massive number of AS, depends on BGP-based routing. Generally, routers trust the veracity of information in the BGP which renders the entire system exposed to numerous attacks [41]. Hence, security is an essential issue in BGP. Also, using blockchain technology as one of the new approaches to improve the cyber and physical security has grown in importance over the past few years [42], [43]. This section reviews four selected security-based articles and illustrates their advantages and disadvantages.

Kazmi *et al.* [44] presented a new way to dissipate BGP state shift messages from several (ASes). Also, due to IP prefix hijack and Multiple Origin AS (MOAS) attacks, the suggested method tries to minimize the BGP convergence time and alleviate corruption in the routing tables. To optimally automate this operation, they utilized OpenFlow capable routers spread throughout the Internet. This approach is not a clean slate but can be merged into the existing BGP network progressively. In the proposed model, they used Google inter-domain SDN deployment as an instance. Empirical studies showed that the suggested model could dramatically improve (quantify) BGP dissemination and mitigate BGP security problems (quantify). Also, they achieved a 50% reduction in convergence time. Moreover, the suggested system's empirical research found that even unconvergable IP prefixes appear to converge along with accelerating other IP prefixes' convergence time.

Costa and Ramos [45] proposed an SDN-based approach to improve BGP security. They examined the presented approaches in the last works and described the following reasons some weakness for prior methods. First, they have used cryptographic techniques. Second, they have needed some BGP changes due to its widespread adoption and the lack of a centralized authority. Also, the separation of the routing control problem from routers by SDN has been proposed to solve BGP problems. They posited this to be key to addressed BGP security. Also, they have used BGPSecX for improved the BGP security. Their design also contains secure channels between the BGPSecX of different Internet Exchange Points (IXPs) that want to collaborate. BGPSecX has four security defenses against prefix hijacks. First, detection is

via Route Origin Authorization (ROA) verification using a Resource Public Key Infrastructure (RPKI) infrastructure. Second, prefix filtering is another whitelist technique that can be employed to filter false announcements. Third, queries between IXPs are employed for the validation of routing information. Fourth, they are well-known anomaly detection mechanisms. They have believed the proposal to be capable of addressing the three fundamental problems mentioned in the beginning. Consideration of security issues is an advantage of the proposed model. This paper does not consider other BGP challenges.

Employing Microsoft security threat model, Swapna *et al.* [46] analyzed frequently utilized strategies for Software-Defined Wireless Networking (SDWN) to underlay cloud or data center environment. This study proposes a framework for minimizing the void in SDWN protocols for on-demand security research. Their analysis revealed that for security specifications, BGP needs a third-party implementation environment. Also, to download and update the whole configuration from the data store within a single session, they addressed NETCONF. Albeit, NETCONF is exposed to different attacks. So, many threats can be prevented by utilizing Transport Layer Security (TLS) as a security technique. This paper considers the security issues, but convergence time and scalability are not considered.

The investigated papers in the security-enhancing frameworks group were analyzed in terms of some aspects, as described in Table 2. Table 2 summarizes the articles' most essential features. The most important factors, that researchers have tried to improve, are security and bandwidth.

**TABLE 2. Comparison of the key factors, advantage, and disadvantage of the security-aware techniques.**

| Paper | Advantage | Disadvantage |
|---|---|---|
| [44] | • Increasing BGP propagation<br>• Alleviating BGP security issues | • Their solution is not clear |
| [46] | • High security | • Low convergence time<br>• Low scalability |
| [45] | • High security | • Not considering other BGP challenges |

### C. MULTI-OBJECTIVE FRAMEWORKS

There have been numerous changes in the use of the Internet, contributing to a large rise in Internet routing. With the current networking infrastructure, meeting these criteria is challenging and creates more costs and less efficiency. Since network devices are hardware equipment, their processing requires more energy and resources. If network protocols are developed employing software modules, flexibility can be achieved easily [30]. The SDN is generalized to embrace several heterogeneous technologies as the SDN is popularized in different networks ranging from connectivity to main backbone. Besides, the network needs to be split into several fields to obtain confidentiality and scalability for the operation of various carriers and regions [47]. In this section, multi-purpose articles are reviewed.

Lin *et al.* [48] presented an Internetworking with SDN utilizing available BGP. The proposed model first presented an overview of BGP Transition for SDN Networks (BTSDN). They presented the controller running IBGP, OpenFlow proxy and flow redirection, Address Resolution Protocol (ARP) proxy module, destination Media Access Control (MAC) rewriting module. For evaluation, they have used ten nodes for emulating three ASes. According to this scenario, AS 1 was an OpenFlow AS. AS 2 and AS 3 were legacy IP fields. Three PCs acted as web subscribers and were installed on the Microsoft Windows XP. Then, they evaluated the proposed model in two steps. In the first step, the feasibility of the controller is verified to get routing information. In the second step, the feasibility of the BTSDN solution is verified. Therefore, one of the most important advantages of this article is the controller's feasibility to get routing information and the feasibility of the BTSDN solution. However, the scalability of this method was not considered.

Duan *et al.* [49] proposed OFBGP,[1] a modern scalable and open BGP structure without any centralized component, focused on the distributed layout. The OFBGP software is an SDN controller function. Based on their specifications and criteria, BGP functionalities were separated into BGP protocol and BGP judgment in the architecture of OFBGP. For scalability, utilizing a distributed structure, the BGP application can simply scale to boost performance. Using BGP Non-Stop Routing (NSR) technology, obtaining high availability guarantees the link between BGP neighbors and the routing information's accuracy during fault recovery. Specifically, without any central component, OFBGP is based on a distributed structure. Also, in OFBGP, each computational task's internal state is snapshotted and stores the events leading to adjustments. Furthermore, all OFBGP computing tasks run concurrently. There is no cold backup, making it possible to hold certain hardware resources. Low cost of time, high scalability, high availability, low recovery time, and high performance are advantages of the proposed model. The OFBGP model's challenges that may be pitfalls of the OFBGP model are strengthening the internal routing strategy in OFBGP, how to decrease the contact traffic among tasks, and how to help path aggregation in OFBGP.

Moreover, Rzym *et al.* [50] analyzed the deployment of Path Computation Element (PCE) notion on the SDN structure in the multi-domain network utilizing Path Computation Element Protocol (PCEP) and BGP Link-State (BGP-LS) strategies. Suggested formulations of the models were used for determining the flow of traffic between the links open. In this research, they used the PCE-based path computation employing a 3-layer TE system. These layers consist of an IBM Cplex LP solver-equipped PCE module, an SDN controller responsible for transmitting path setup demands, and virtual routers to handle traffic effectively through a single

[1] OFBGP is a new scalable and available BGP architecture for SDN

field network. The PCE module uses accessible network status knowledge intelligently and executes dedicated optimization algorithms. They also introduced the PCE architecture, which is the collection of PCE server, PCE client (PCC), and reliable PCE Protocol (PCEP). The Cisco IOS XRv 5.3.0 was utilized in the test-bed implementation. Also, they have utilized the OpenDaylight in the Lithium as a controller. Furthermore, they used graphs as a network model in which links are edges and routers are vertices. Links within the ASes are standard FastEthernet, and their proposed model described the issue of the total cost reduction of flows implemented within the network. For evaluation, the optimization time, memory usage, and RAM usage were used. This paper does not consider the privacy and security issues as well as scalability.

Lin *et al.* [51] proposed an easy and experimental BGP-based transition solution called BTSDN. Using the latest BGP protocol to link the OpenFlow network to the Internet, BTSDN discusses its functionality. In BTSDN, to substitute the existing Internet worldwide, SDN networks can be implemented incrementally on the Internet. Then they proposed BTSDN architecture, according to this architecture. OpenFlow switches directly linked to a border router to act as OpenFlow protocol proxy for the border routers. Since conventional BGP routers do not support OpenFlow, the border routers' actions cannot be controlled by the controller. However, on the OpenFlow proxy, the controller can install those directions into the flowtable and monitor the border router. So, the controller can also monitor the actions of the whole intra-domain network on BTSDN. Also, they classified the traffic. They listed all the traffic and the transfer port from which the traffic comes due to the destination IP address's next hop. In two steps, they completed the full trial. Step 1; verification of the controller's viability to gain knowledge about global routing; in this step, they have used the static flow pusher Application Programming Interface (API) in Floodlight to install the BGP path. In the second step, BTSDN feasibility is verified. This step aims to confirm if each PC in passive and proactive models interacted with other PCs in other non-OpenFlow fields, respectively. They used WinFTP in this step. For evaluation, intra-domain packet delivery, availability, Quagga responsibilities, and traffic classifier were used. Therefore, confirmation of controllability and feasibility is one of the most important results of this study.

Furthermore, Godán *et al.* [52] examined an approach for IBGP information dissemination using SDN. The prior goal is achieved by substituting per-ASBR (AS Border Router) for path reflection, while the latter is guaranteed by delegating complexity to SDN for multicast tree maintenance. The authors also discussed the IBGP challenges, such as the shortage of route diversity and potential correctness failures at the data and control plane. Moreover, any important features of multicast communication have been checked. Their proposal was based on an IBGP full-mesh. IBGP full-mesh is necessary to ensure complete visibility and accuracy of the path. Consequently, any AS internal router gets complete external accessibility information in full-mesh BGP, thus ensuring its attributes. They also focused on the hybrid router design that combines both the OpenFlow protocol and legacy distributed routing protocols like OSPF (Open Shortest Path First) and BGPP. Ultimately, they used the Ryu controller in their proposed model. Therefore, each ASBR advertises itself to the controller, which adjusts the ASBR with the multicast addresses specified, and distributes this information to the remainder of the AS routers. Whenever a novel router is detected in the network, it is transmitted to the current multicast groups by the controller to join each one. They used an emulated environment based on Mininet, hybrid routers, and Ryu controller for evaluation. In the evaluation phase, some tests were applied to the proposed model. Scalability, amount of memory consumed, amount of control traffic has been considered. The SDN controller's availability, multicast reliability, and privacy and security issues were not considered.

The BGP-based Path Vector (BGP-PV) method was suggested by. Hassan *et al.* [53] to pick a path from the vector shown by the PV and channel the traffic accordingly. First, the authors expressed some of the reasons for utilizing path vector as a protocol. The Path Vector Protocol (PVP) is utilized as a protocol for network routing in the proposed model, which preserves dynamically modified path information. It is possible to deny changes that looped across the network and returned to the same node. Compared to distance vector routing in convergence and more efficient in route selection, the path vector is an extension of the distance vector algorithm. A PVP is based on the IDR protocol, which manages dynamically modified path data. A node preserves different paths in a routing table according to the suggested model. The whole of these paths is saved in the vector forms. The path is built on the route switches that are chosen. The controller passes a withdrawal message among all nodes on the path if the active route is not available. In this article, the simulation environment was used. The suggested model's benefits are decreasing the average end-to-end latency, raising the overall network throughput, and lowering the routing rate.

Gomez *et al.* [54] proposed Effective Tunnel-based Multi-Path BGP (ETMP-BGP) to get the entire control of multi-path BGP routing. This method was proposed based on SDN and is used to manage the destination-based routing problem. On AS-level routes, this technique can identify congestions and modify those routes on a per-source basis. Furthermore, the global multi-path AS-level routing was constructed into a linear programming model. According to the suggested model, tunnels are assigned to redirect part of the traffic to the destination while the source AS collects congestion input from the goal AS. To construct tunnels, they used MPLS. A greedy algorithm was also suggested to continuously record congestion input from destinations and continually allocate capacity-based traffic. The proposed method can mitigate the AS-level congestions and conduct better than available BGP layouts due to the performed simulation. Also, load-balancing and good performance when links were

tighter and low average packet loss rate are the advantages of the proposed model. In this method, scalability and privacy issue were not considered.

Elguea and Martinez-Rios [55] examined metrics to change SDN-based BGP routes. They found limited opportunities for modular management and improved traffic engineering in a router that executes BGP due to network equipment operating systems' constraints. These devices were developed and dimensioned solely for this purpose. With SDN, it is feasible to get all the router's details about the BGP configurations in a PC. It allows handling the routes in more detail, and in general, all the data that enable better routes to be inferred than otherwise. Tools like this, written in Java to implement BGP, allows any policy to be defined and implemented to create new routes. It is almost challenging to test routes with too many specifics in the router beforehand. However, the opportunities and versatility are far higher in a PC. You can also decide the geographical position of each AS, locate the country to which it belongs or stop crossing and returning to other continents. Doing real-time route handling enables the Internet to be more complex, stable, and fast. While additional latency mitigation methods, like the cache, exist, it is more effective to choose shorter paths.

Eight important papers were analyzed in the multi-objective frameworks section in terms of some aspects. Table 3 summarizes the advantages and disadvantages of the articles. The most critical factors that researchers have tried to improve are the cost of time, availability, recovery time, and optimization time.

**TABLE 3. Comparison of the key factors, pros, and cons of the multi-objective techniques.**

| Paper | Advantage | Disadvantage |
|---|---|---|
| [48] | • The feasibility of the controller<br>• Feasibility of BTSDN solution | • Low scalability |
| [49] | • Low cost of time<br>• High scalability<br>• High availability<br>• Low recovery time | • High communication traffic<br>• Low internal routing policy |
| [50] | • Low cost<br>• Appropriate for real-time systems | • Low privacy<br>• Low security<br>• Low scalability |
| [51] | • High availability<br>• The feasibility of the controller | • Low scalability |
| [52] | • High scalability<br>• Low amount of memory consumed | • Low availability<br>• Low multicast reliability<br>• Low privacy<br>• Low security |
| [53] | • Reducing the average end-to-end delay<br>• Increasing the network throughput<br>• Minimizing the routing cost | • Low scalability |
| [54] | • Load-balancing and good performance<br>• Low average packet loss rate | • Low scalability<br>• Low privacy |
| [55] | • High flexibility<br>• Appropriate for real-time systems<br>• High dynamicity | • High latency |

## IV. DISCUSSION

In this paper, 19 papers about the BGP protocol and SDN approaches for solving the BGP limitations have been reviewed. The BGP is a significant aspect of the Internet routing infrastructure utilized among ASes to transmit routing information. The goal of BGP is to share its info with other BGP network systems and interchange network compatibility and accessibility info for AS routes. This method enables all systems on both sides of the BGP to create topology graphs of the entire network. One of the important benefits of BGP is that corporate users can set up flexible connections between their corporate network and multiple ISPs. Two significant features distinguish BGP from other routing protocols, (1) It aggregates and disseminate Network Layer Reachability Information (NLRI) across routers, (2) It uses path attributes for implementing routing policies. Dissimilar to other routing protocols, BGP problems may result in important and widespread damage. Current research on BGP emphasizes resolving some issues related to operations and security. Operational worries of BGP, such as scalability, convergence delay, routing stability, and performance, have been addressed widely.

On the other hand, most of the security investigations focused on issues such as confidentiality, authentication, authorization, integrity, and validation of the BGP messages. For example, Karakus and Durresi [56] presented a picture of Quality of Service (QoS)-motivated literature in open flow-enabled SDN networks investigating related studies. They suggested that some new apps, like video conferencing, distance learning, etc., have been popular in networking lately. These apps still contain some problems with QoS or QoE demands from their subscribers/clients, considering the benefits of these QoS-dependent apps for subscribers. Also, Mitseva *et al.* [57] undertook a study of the fundamental challenges to BGP and proposed a framework for analyzing current proposals for BGP security. According to this fact, they introduced a complete and up-to-date query of suggested proposals to secure BGP. Finally, Sahay *et al.* [58] provided a review on SDN's employment for improving the network's security because of the growing and abrupt progress of SDN. In particular, the latest analysis techniques focusing on SDN use for network security have been investigated, including threat prevention and prevalence, smart grid security, traffic control, service chaining, configuration and policy management, and implementation of middle-boxes. They also highlighted the key advantages and flaws in network security, including prevention and avoidance of threats, traffic control, and architecture, as well as configuration and policy compliance.

According to the BGP shortcomings, security and privacy limitation are the most important limitations in the BGP. Furthermore, BGP is vulnerable to attacks and misconfigurations. These limitations affected the performance of this protocol and network. The most important BGP attacks are listed below, (1) Data falsification attacks, such as prefix hijack, sub-prefix hijack, AS path forgery, interception attack, replay/suppression attack, and collusion attack. (2) Protocol manipulation attacks, such as MED modification, Exploit RFD/MRAI timer, denial of service (DoS), and route leak.

Because of the limited scale of the SDN network supported by a single controller, many researchers suggested logically centralized but physically distributed SDN solutions to make it broadly commercial. The scalability and availability become more emphasized in the architecture design of SDN controllers and network applications. Since SDN allows the networks to scale out flexibility, the control plane's scalability is particularly important. Meanwhile, designing a more robust and high availability solution to evade losses caused by the failure of control plane components is essential. Also, SDN can enhance the networks routing functionality. Recently, several studies applied its principles in the Internet's inter-domain routing as well. SDN provides high control of a network through programming with its decoupling of the control plane from the data plane. This feature can bring potential aids of improved configuration, enhanced performance, and encouraged innovation. For instance, the SDN control may have packet forwarding at a switching level and link tuning at a data link level, breaking the layering barrier. Furthermore, with the ability to obtain instantaneous network status, SDN lets a real-time centralized control of a network based on immediate network status and user-defined policies. Enhancing configuration, improving performance, and encouraging innovation are the main benefits of SDN. Still, in the SDN, some challenges are raised that the network designer has focused on them. (1) It needs changing a whole network infrastructure to implement SDN protocol and controller. Henceforth, it requires wide-ranging network reconfiguration and increases cost because of reconfiguration. (2) New management tools need to be procured, and everybody should be trained to use them. (3) Security is a big issue of SDN. (4) SDN controllers are the single points of failure. Finally, we summarized the results of the analyzed articles in Fig. 2. As can be seen, researchers in previous studies have focused more on improving latency and convergence time. Therefore, we conclude that latency and convergence time are the most common issues related to BGP and SDN.

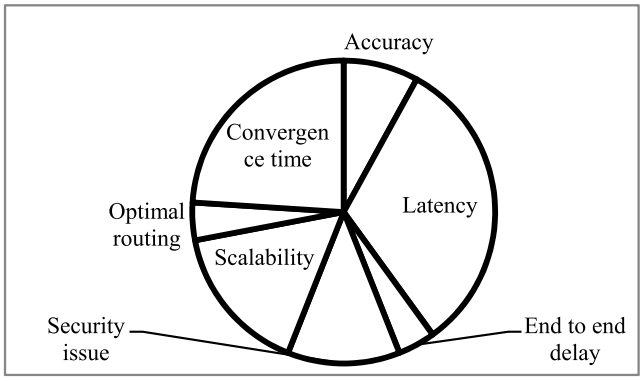


**FIGURE 2.** The most important factors studied in the literature.

## V. OPEN ISSUES AND FUTURE WORK

BGP was designed nearly three decades ago and had many limitations due to its fully distributed nature, policy implementation capabilities, scalability, security, and complexity. Furthermore, SDN provides a forum for innovative networking strategies; however, the transition from traditional to SDN networking may be difficult. Popular concerns include SDN interoperability with legacy network equipment, unified control efficiency and privacy concerns, and the absence of technical support specialists. Some models took into account network scalability, security concerns, and optimal routing, while others took into account communication traffic, average packet loss rate, and routing cost. In contrast, the simulation was used. In the field of computer defense, which involves risks, attacks, and risk management, having improved protections to avoid attacks and following the appropriate protocol are both very motivational issues.

It is essential to define the correct abstractions provided to the services operating on the network. Therefore, layered control channel architectures are good choices that use network programming languages and compilers. Another fragment of the puzzle is the virtualization/slicing abstraction. Collaborative protection against novel DDoS attacks is one possible service that would be useful to run on a cross-domain basis utilizing the suggested platforms. SDN-based traffic engineering for mutual monitoring and mitigation could benefit from this service.

Also, reliability plays a significant role in any software development. If any problem occurs in a system, the solution must perform automatically. An SDN controller can support a minimum of 100 switches, mitigate the broadcasting overhead, and curb the proliferation of the entries in the flow table [59]. Open interfaces of the SDN network may bring a new kind of attack that may decrease the performance of the SDN. So, the solutions must be in the SDN framework for integrity, remote access management, authentication, and user authorization [60].

The future analysis involves quantifying the multi-AS cluster SDN controller scalability, resiliency, and centralization trade-offs. For instance, a fascinating area to explore is the effective positioning of controllers in a multi-domain environment to cope with latency and delivery trade-offs. Another feature of extensions, along with policy connections among inter-domain services operating on top of the controller, is policy support. For arbitrary topologies and several laws, effective algorithms for computing shortest paths may be core components of the ongoing work.

Also, exploring redundant methods for fast re-routing on the IP layer can be investigated in the future. Moreover,

SDN and OpenStack are considerably new technologies to advance these technologies' security aspects. Minimizing the convergence time of the BGP is another open research opportunity that can lead to increasing the reliability of networks. Researchers can also look for cross-vendor compatibility and security constraints when the cloud is integrated with SDN.

## VI. CONCLUSION

The current distributed environment does not allow for sufficient customization of routing protocol usage. As a result, it is possible to do so by separating the control and data planes using SDN. SDN, abstractions, simplicity, and programmability revolutionize network service, configuration, and management through unified control. Domains are associated with the use of BGP in multi-domain SDN to share routing and route information between domains or different ASes. This study provided a systematic review of the limitations of BGP strategies. An in-depth analysis of 19 studies from our search query revealed various limitations on the BGP as well as the SDN approaches, as well as many open issues. In addition, the advantages and disadvantages of numerous articles have been illustrated. In this paper, we investigated a variety of methods and compared them based on criteria such as accuracy, optimal routing, and reliability, as well as scalability and convergence time. This study referred to some of these approaches' main drawbacks in order for more well-organized BGP methods to be developed in the future. The findings revealed that while the majority of the investigated papers improve convergence time, scalability, optimal routing, and privacy issues are not addressed.

This review aimed to provide a comprehensive overview of SDN and BGP studies in order to identify research gaps and potential future research directions. However, limitations such as the absence of non-English studies can be viewed as a drawback of this study. As a result, the SDN and BGP should be investigated in order to comprehend both the opportunities and the significant challenges of the twenty-first century. This paper will be useful in encouraging further research to find more solutions that are low in cost, time, and security.

## REFERENCES

[1] B. R. Smith and J. J. Garcia-Luna-Aceves, "Securing the border gateway routing protocol," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Nov. 1996, pp. 81–85.
[2] J. Honig, D. Katz, M. Mathis, Y. Rekhter, and J. Yu, *Application of the Border Gateway Protocol in the Internet*, document RFC-1164, Jun. 1990.
[3] M. O. Nicholes and B. Mukherjee, "A survey of security techniques for the border gateway protocol (BGP)," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 1, pp. 52–65, 1st Quart., 2009.
[4] V. Pandey and A. S. Baghel, "Providing end-to-end secure communication in wireless network using BGP routing technique," in *Innovations in Computer Science and Engineering*. Singapore: Springer, 2019, pp. 77–86.
[5] M. Singh, "Routing protocol for WMNs," in *Node-to-Node Approaching Wireless Mesh Connectivity*. Spain: Springer, 2019, pp. 15–20.
[6] P.-C. Chen, M. E. Stalzer, and A. H. Redmon, "Border gateway protocol routing configuration," Google Patents 9 935 816, Apr. 3, 2018.
[7] D. Kreutz, F. Ramos, P. E. Veríssimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: A comprehensive survey," *Proc. IEEE*, vol. 103, no. 1, pp. 14–76, Jan. 2015.
[8] N. McKeown, "Software-defined networking," *INFOCOM Keynote Talk*, vol. 17, no. 2, pp. 30–32, 2009.
[9] Z. Wu, S. Shen, C. Lu, H. Li, and X. Su, "How to protect reader lending privacy under a cloud environment: A technical method," *Library Hi Tech*, vol. 7, pp. 112–132, Dec. 2020.
[10] A. A. Neghabi, N. J. Navimipour, M. Hosseinzadeh, and A. Rezaee, "Nature-inspired meta-heuristic algorithms for solving the load balancing problem in the software-defined network," *Int. J. Commun. Syst.*, vol. 32, no. 4, p. e3875, Mar. 2019.
[11] N. Cardona, E. Coronado, S. Latré, R. Riggio, and J. M. Marquez-Barja, "Software-defined vehicular networking: Opportunities and challenges," *IEEE Access*, vol. 8, pp. 219971–219995, 2020.
[12] A. A. Neghabi, N. J. Navimipour, M. Hosseinzadeh, and A. Rezaee, "Load balancing mechanisms in the software defined networks: A systematic and comprehensive review of the literature," *IEEE Access*, vol. 6, pp. 14159–14178, 2018.
[13] S. D. A. Shah, M. A. Gregory, S. Li, and R. D. R. Fontes, "SDN enhanced multi-access edge computing (MEC) for E2E mobility and QoS management," *IEEE Access*, vol. 8, pp. 77459–77469, 2020.
[14] R. Mohammadi, R. Javidan, M. Keshtgari, and N. Rikhtegar, "SMOTE: An intelligent SDN-based multi-objective traffic engineering technique for telesurgery," *IETE J. Res.*, pp. 1–11, Mar. 2021.
[15] W. Xia, Y. Wen, C. H. Foh, D. Niyato, and H. Xie, "A survey on software-defined networking," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 1, pp. 27–51, 1st Quart., 2015.
[16] K. Kirkpatrick, "Software-defined networking," *Commun. ACM*, vol. 56, no. 9, pp. 16–19, Sep. 2013.
[17] F. Godán, S. Colman, and E. Grampín, "Multicast BGP with SDN control plane," in *Proc. 7th Int. Conf. Netw. Future (NOF)*, Nov. 2016, pp. 1–5.
[18] S. Scott-Hayward, G. O'Callaghan, and S. Sezer, "SDN security: A survey," in *Proc. IEEE SDN Future Netw. Services (SDN FNS)*, Nov. 2013, pp. 1–7.
[19] Q. Al-Tashi, S. J. Abdulkadir, H. M. Rais, S. Mirjalili, and H. Alhussian, "Approaches to multi-objective feature selection: A systematic literature review," *IEEE Access*, vol. 8, pp. 125076–125096, 2020.
[20] K. Elibal and E. Özceylan, "A systematic literature review for industry 4.0 maturity modeling: State-of-the-art and future challenges," *Kybernetes*, vol. 4, pp. 192–210, Dec. 2020.
[21] Z. Yu, L. Song, L. Jiang, and O. K. Sharafi, "Systematic literature review on the security challenges of blockchain in IoT-based smart cities," *Kybernetes*, vol. 11, pp. 136–144, Mar. 2021.
[22] T. Mostafaie, F. M. Khiyabani, and N. J. Navimipour, "A systematic study on meta-heuristic approaches for solving the graph coloring problem," *Comput. Oper. Res.*, vol. 120, Aug. 2020, Art. no. 104850.
[23] C. R. M. Hay, F. Nissen, and S. W. Pipe, "Mortality in congenital hemophilia A—A systematic literature review," *J. Thrombosis Haemostasis*, vol. 19, no. S1, pp. 6–20, Jan. 2021.
[24] K. Çakar and Ş. Aykol, "Case study as a research method in hospitality and tourism research: A systematic literature review (1974–2020)," *Cornell Hospitality Quart.*, vol. 62, Feb. 2021, Art. no. 1938965520971281.
[25] P. M. Alamdari, N. J. Navimipour, M. Hosseinzadeh, A. A. Safaei, and A. Darwesh, "A systematic study on the recommender systems in the E-commerce," *IEEE Access*, vol. 8, pp. 115694–115716, 2020.
[26] V. Kotronis, A. Gämperli, and X. Dimitropoulos, "Routing centralization across domains via SDN: A model and emulation framework for BGP evolution," *Comput. Netw.*, vol. 92, pp. 227–239, Dec. 2015.
[27] N. Hadipratama, D. Desmulyati, and A. Taufik, "External border gateway protocol (EBGP) routing design in router core," *Jurnal Mantik*, vol. 4, no. 3, pp. 1728–1733, 2020.
[28] A. Keshavarzi, A. T. Haghighat, and M. Bohlouli, "Online QoS prediction in the cloud environments using hybrid time-series data mining approach," *Iranian J. Sci. Technol., Trans. Electr. Eng.*, vol. 45, no. 2, pp. 461–478, Jun. 2021.
[29] P. Goudarzi, M. Hosseinpour, and M. R. Ahmadi, "Joint customer/provider evolutionary multi-objective utility maximization in cloud data center networks," *Iranian J. Sci. Technol., Trans. Electr. Eng.*, vol. 45, no. 2, pp. 1–14, 2020.
[30] R. B. R. Gonuguntla and L. Hash, "A technology case study on integrating open stack with SDN for internet connectivity using BGP," Ph.D. dissertation, Dept. Comput. Sci., Texas Univ., Austin, TX, USA, 2016.
[31] C.-F. Lai, H.-X. Zhong, P.-S. Chiu, and Y.-H. Pu, "Development and evaluation of a cloud bookcase system for mobile library," *Library Hi Tech*, vol. 9, pp. 326–344, Jun. 2020.

[32] G. Oguya, "Hardening the software defined network [SDN] controller using border gateway protocol [BGP]," Ph.D. dissertation, College Biol. Phys. Sci., Univ. Nairobi, Nairobi, Kenya, 2018.
[33] L. Dewangan and A. R. Vaishnava, "Energy-efficient smart wearable IoT device for the application of collapse motion detection and alert," *IETE J. Res.*, pp. 1–7, Dec. 2020.
[34] P. Sermpezis and X. Dimitropoulos, "Can SDN accelerate BGP convergence?—A performance analysis of inter-domain routing centralization," in *Proc. IFIP Netw. Conf. (IFIP Netw.) Workshops*, Jun. 2017, pp. 1–9.
[35] L. M. Elguea and F. Martinez-Rios, "A new method to optimize BGP routes using SDN and reducing latency," *Procedia Comput. Sci.*, vol. 135, pp. 163–169, Jan. 2018.
[36] A. Gämperli, V. Kotronis, and X. Dimitropoulos, "Evaluating the effect of centralization on routing convergence on a hybrid BGP-SDN emulation framework," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 4, pp. 369–370, Feb. 2015.
[37] P. Sermpezis and X. Dimitropoulos, "Inter-domain SDN: Analysing the effects of routing centralization on BGP convergence time," *ACM SIGMETRICS Perform. Eval. Rev.*, vol. 44, no. 2, pp. 30–32, Sep. 2016.
[38] G. Rzym, K. Wajda, and P. Chołda, "SDN-based WAN optimization: PCE implementation in multi-domain MPLS networks supported by BGP-LS," *Image Process. Commun.*, vol. 22, no. 1, pp. 35–48, Mar. 2017.
[39] R. Pradeepa and M. Pushpalatha, "A hybrid OpenFlow with intelligent detection and prediction models for preventing BGP path hijack on SDN," *Soft Comput.*, pp. 1–10, Nov. 2019.
[40] H. Alotaibi, S. Li, and M. A. Gregory, "Utilising SDN to counter BGP convergence delays," in *Proc. 29th Int. Telecommun. Netw. Appl. Conf. (ITNAC)*, Nov. 2019, pp. 1–6.
[41] L. Mastilak, M. Galinski, P. Helebrandt, I. Kotuliak, and M. Ries, "Enhancing border gateway protocol security using public blockchain," *Sensors*, vol. 20, no. 16, p. 4482, Aug. 2020.
[42] M. Dehghani, M. Ghiasi, T. Niknam, A. Kavousi-Fard, M. Shasadeghi, N. Ghadimi, and F. Taghizadeh-Hesary, "Blockchain-based securing of data exchange in a power transmission system considering congestion management and social welfare," *Sustainability*, vol. 13, no. 1, p. 90, Dec. 2020.
[43] A. Fathurohman, "Implementation of the border gateway protocol (BGP) protocol in the public network of the universitas muhammadiyah semarang," *J. Intell. Comput. Health Inform.*, vol. 2, no. 1, pp. 12–16, 2021.
[44] H. Kazmi, H. Nawaz, M. A. Gulzar, F. Zaffar, and A. Gehani, "BGP is high on SDN: Improving BGP convergence and security using SDN and reassertions," Dept. Comput. Sci., Texas Univ., Austin, TX, USA, Tech. Rep., 2015.
[45] R. Costa and F. M. V. Ramos, "An SDN-based approach to enhance BGP security," 2016, *arXiv:1602.06924*. [Online]. Available: http://arxiv.org/abs/1602.06924
[46] A. I. Swapna, M. R. Huda, and M. K. Aion, "Comparative security analysis of software defined wireless networking (SDWN)-BGP and NETCONF protocols," in *Proc. 19th Int. Conf. Comput. Inf. Technol. (ICCIT)*, Dec. 2016, pp. 282–287.
[47] S. Son, D.-J. Kang, S. P. Huh, W.-Y. Kim, and W. Choi, "Adaptive tradeoff strategy for bargaining-based multi-objective SLA establishment under varying cloud workload," *J. Supercomput.*, vol. 72, no. 4, pp. 1597–1622, Apr. 2016.
[48] P. Lin, J. Bi, and H. Hu, "Internetworking with SDN using existing BGP," in *Proc. 9th Int. Conf. Future Internet Technol. (CFI)*, 2014, pp. 1–2.
[49] W. Duan, L. Xiao, D. Li, Y. Zhou, R. Liu, L. Ruan, Y. Xia, and M. Zhu, "OFBGP: A scalable, highly available BGP architecture for SDN," in *Proc. IEEE 11th Int. Conf. Mobile Ad Hoc Sensor Syst.*, Oct. 2014, pp. 557–562.
[50] G. Rzym, K. Wajda, and K. Rzym, "Analysis of PCE-based path optimization in multi-domain SDN/MPLS/BGP-LS network," in *Proc. 18th Int. Conf. Transparent Opt. Netw. (ICTON)*, Jul. 2016, pp. 1–5.
[51] P. Lin, J. Bi, and H. Hu, "BTSDN: BGP-based transition for the existing networks to SDN," *Wireless Pers. Commun.*, vol. 86, no. 4, pp. 1829–1843, Feb. 2016.
[52] T. Farasat and A. Khan, "Detecting and analyzing border gateway protocol blackholing activity," *Int. J. Netw. Manage.*, vol. 31, no. 4, p. e2143, 2021.
[53] S. Hassan, S. Arlimatti, W. Elbreiki, and A. Habbal, "Border gateway protocol based path vector mechanism for inter-domain routing in software defined network environment," in *Proc. IEEE Conf. Open Syst. (ICOS)*, Oct. 2016, pp. 76–80.
[54] J. L. G. Gomez, R. Wang, M.-H. Chen, and C.-F. Chou, "ETMP-BGP: Effective tunnel-based multi-path BGP routing using software-defined networking," in *Proc. IEEE Int. Conf. Syst., Man, Cybern. (SMC)*, Oct. 2017, pp. 420–425.
[55] L. M. Elguea and F. Martinez-Rios, "New metrics to modify BGP routes based on SDN," *Wireless Netw.*, vol. 26, no. 8, pp. 5623–5630, Nov. 2020.
[56] M. Karakus and A. Durresi, "Quality of service (QoS) in software defined networking (SDN): A survey," *J. Netw. Comput. Appl.*, vol. 80, pp. 200–218, Feb. 2016.
[57] A. Mitseva, A. Panchenko, and T. Engel, "The state of affairs in BGP security: A survey of attacks and defenses," *Comput. Commun.*, vol. 124, pp. 45–60, Jun. 2018.
[58] R. Sahay, W. Meng, and C. D. Jensen, "The application of software defined networking on securing computer networks: A survey," *J. Netw. Comput. Appl.*, vol. 131, pp. 89–108, Apr. 2019.
[59] A. Metzler and A. Metzler, "Ten things to look for in an SDN controller," Dept. Comput. Sci., Texas Univ., Austin, TX, USA, Tech. Rep., May 2013.
[60] D. S. Rana, S. A. Dhondiyal, and S. K. Chamoli, "Software defined networking (SDN) challenges, issues and solution," *Int. J. Comput. Sci. Eng.*, vol. 7, no. 1, pp. 884–889, Jan. 2019.

**XI ZHAO** was born in Henan, China, in 1989. She received the B.S. degree in information engineering from Zhengzhou University of Light Industry, Henan, in 2011, and the M.S. degree in electronic and communication engineering from the Communication University of China, Beijing, China, in 2014, where she is currently pursuing the Ph.D. degree with the School of Information and Communication Engineering. From 2014 to 2017, she was a Teaching Assistant with the School of Electronic and Electrical Engineering, Shangqiu Normal University, Henan. She is the author of more than five articles. Her research interests include signal and information processing, data analysis, computer communication, and audio network protocol.

**SHAHAB S. BAND** received the M.Sc. degree in artificial intelligence from Iran and the Ph.D. degree in computer science from the University of Malaya (UM), Malaysia, in 2014. He was an Adjunct Assistant Professor with the Department of Computer Science, Iran University of Science and Technology. He served as a Senior Lecturer with UM and Islamic Azad University, Iran. He participated in many research programs within the Center of Big Data Analysis, IUST and IAU. He has been associated with young researchers and elite club, since 2009. He supervised or co-supervised undergraduate and postgraduate students (master's and Ph.D.) by research and training. He has authored or coauthored articles published in IF journals and attended to high-rank A and B conferences. He is a Professional Member of ACM. He is also an associate editor, a guest editor, and a reviewer of high-quality journals and conferences.

**SAID ELNAFFAR** received the M.Sc. and Ph.D. degrees from Queen's University, ON, Canada. He worked at UAE University, American University of Ras al Khaimah, and American University in the Emirates. He is currently an Associate Professor of computer science with the Canadian University Dubai. He is known by his captivating teaching and training style. He received the IBM Ph.D. Fellowship Award and worked as a Research Associate with the Centre of Advanced Studies (CAS) of IBM Canada. He is also the winner of the Best Teaching Award and Best Research Paper in computing education. His research has been funded by numerous governmental agencies, and industrial firms. His work is published in reputable international journals and IEEE/ACM Conferences. He organized and served on many program committees of pronounced conferences and workshops. He is also an entrepreneur and helped many firms with his industrial consultation and professional training. He has several industrial certifications from IT giants, such as Google and IBM in contemporary fields, such as machine learning, data science, and software engineering and development.

**MEHDI SOOKHAK** (Senior Member, IEEE) received the Ph.D. degree in computer science from the University of Malaya (UM), in 2015, with a focus in information security. He was an Active Researcher with the Center of Mobile Cloud Computing Research (C4MCCR), UM. From 2016 to 2017, he was with Carleton University, Canada, as a Postdoctoral Fellow. He is currently an Assistant Professor of cybersecurity with Illinois State University, Normal, IL, USA. He has authored more than 40 articles in high ranking journals and conferences. His research interests include cloud and mobile cloud computing, fog computing, vehicular cloud computing, the IoT and smart cities, computation outsourcing, access control, network security, wireless sensor and mobile *Ad Hoc* networks, such as architectures, protocols, security, and algorithms, big data security and analytic, distributed systems, and cryptography and information security. He served as the chair of several conferences, such as ICCE 2019-2020. He serves as an Editor of several ISI journals, such as *Vehicular Communications*, IEEE Access, and *Electronics*.

**AMIR MOSAVI** completed his graduate studies with London Kingston University, U.K., and received the Ph.D. degree in applied informatics. He is currently an Alexander von Humboldt Research Fellow for big data, the IoT, and machine learning. He is also a Senior Research Fellow with Oxford Brookes University. He is also a Data Scientist for climate change, sustainability, and hazard prediction. He was a recipient of the Green-Talent Award, the UNESCO Young Scientist Award, the ERCIM Alain Bensoussan Fellowship Award, the Campus France Fellowship Award, the Campus Hungary Fellowship Award, and the Endeavour-Australia Leadership.

**ELY SALWANA** received the M.A. degree in information technology from the University of Technology Malaysia, in 2005, with a focus on management, and the Ph.D. degree in computer science from the University of Malaya, in 2016. She is currently a Research Fellow with the Institute of IR4.0, Universiti Kebangsaan Malaysia (UKM), Bangi, Malaysia. Her primary research interests include information work, data analytics, knowledge organization, and participatory information practices. The contexts of her research ranges from public organization, education, virtual worlds, and corporate. She has 11 years of working experience related to her field of study in university, as a lecturer, a researcher, and a supervisor for undergraduate and postgraduate student. She has involved in many research projects and grants that related to computer sciences especially in her area of interest as the group leader and a researcher, and all the projects are successfully delivered on time and followed project schedule.