Improving Load Balancing and Scalability by Implementing Path Selection on BGP Using Multi SD-WAN

Nysret Demaku and Artan Dermaku
Universiteti Kadri Zeka University, Gjilan, Kosovo
Email: Nysret.demaku@uni-gjilan.net; prof.artan.dermaku@uni-gjilan.net

Abstract—This research paper introduces three key problems relevant to data movement across the multi-domains. They are (1) delays in data transmission because of the failures of the links, (2) high throughput data transfer over large networks due to the worst path selection using the BGP, and (3) the efficient distribution of data (Load balancing and scalability). All three problems introduce scalability, load balancing and fail-over concerns with respect to the network architecture. The recent steps taken by SDN due to the introduction and popularity of OpenFlow provide a new way to approach these problems. This research paper proposes and demonstrates solutions to the aforementioned problems using scalable approaches introduced in SDN Controller. This research paper details the elements that influence BGP decisions on path selection using SDN infrastructure. Based on the features, a testbed using NS3 has been designed and implemented which explores ideas related to the domain-to-domain data transmission using SDN. The implementation of the Mesh topology of wires Domains was completed using NS3. This paper discusses also OpenFlow Service and the SDN involvement on BGP improvement over long-distance networks and the end users who wish to obtain the data in a timely manner with minimal effort.

Index Terms—SDN[1], SD-WAN, border gateway protocol, autonomous system, ID3[2] algorithm, OpenFlow

I. Introduction

This research investigates the ways to improve the Scalability, Load Balancing, and failover on inter-domain communication in the SDN AS environment. Software Define Network (SDN) is a new technology that has evolved in the last decade. SDN is a way of separating the network control plane from the data plane. In SDN controller manages and distributes the rules to the network devices to handle the flows that have been initiate by the user.

The intelligence of the router and the switches is implemented and managed in the controller. The switches have an interface that is based on Open Flow protocol and manages and forward the network flow. Despite the fact that SDN is fairly new, SDN networks have many advantages over traditional networks, like the ease of network management and enforcement of security policies. However, SDN is typically not fully implemented by many companies due to several reasons.

One major reason is the limited budget for new network infrastructure. Organizations are often reluctant to invest large budgets on installing a new network infrastructure from scratch. Another reason is the fear of downtime during the transition to SDN. One solution is to set up a limited number of SDN devices for a start.

II. Relatet Works

Pavlos Sermpezis and Xenofontas Dimitropoulos [1] conducted research on BGP convergence and proposed a methodology for performance analysis of inter-domain routing centralization. Here they developed a model. In this section, I compare other models with our model. Here the comparison takes place in many aspects like topology, algorithms used and outcomes, etc. Both models have the below-mentioned similarities and variations. The model proposed in the literature uses the Inter-domain Software Define Networking approach. But I use the Mesh topology of independent domains. Both techniques have their own pros and cons.

In the literature there are two techniques are stated, and they are topology independent SDN cluster and topology related SDN cluster. Here this model is developed mainly for testing the performance of the Inter-domain Routing domain centralization. But our work differs from the model proposed in the literature by these authors. Because the main intention of our model is to improve the routing effectiveness by improving the path selection process. But the main similarity between the two models is its functional areas. Both models deal with the BGP performance improving or reduce the complexities present in the BGP. BGP has many advantages with some major limitations. Lack of flexibility, limited path diversity, limited information, and vulnerability to attacks, are the most common and big issues that arise in the use of BGP. Here both models try to improve the effectiveness of the BGP by reducing or limiting the various limitations present in the current system. In the model proposed in the literature, they used the probabilistic approach for analysing the performance of the inter-domain SDN.

Manuscript received October 20, 2021; revised March 18, 2022.

[1] Software Define Network

[2] Iterative Dichotomiser Algorithm

doi:10.12720/jcm.17.4.250-259

Here first they identified the time required for establishing the connection by the network system after the routing change. Authors developed the time limits (lower limit and upper limit) for establishing the data-plane connection among the two different ASec. And they derived expressions for finding the potential gain of centralization, the economics of the network system, and inter-domain SDN deployment techniques etc. The developed expression is a function of the common network parameters like SDN node numbers, length of paths, and size of the network.

Among the two models, our model helps to resolve many problems. It provides the details by identifying all the paths of mesh topology, bottleneck, and bandwidth. Also, our model improves the performance by eliminating the congested paths. It positively affects the speed of the process also [1]. The proposed model totally improves the path selection process. The model proposed in the literature helps to reduce the complexities involved in the testing and analysis of BGP. Here it mainly identifies the control plane convergence time.

According to the research, the work carried out by ‘Vasileios Kotronis [2]’ on routing centralization across the domains is done using software-defined networking. Here the framework could be proposed by the author regarding the border gateway protocol. In the proposed model I develop a network that contains independent domains. The Mesh topology and border gateway protocol are established in the network. So border gateway protocol is used to finding the path on mesh topology by sending the packet to all the domains and receiving the parameters and data for each domain.

And ID3 algorithms is used to avoid the congested path. Next, the failover and load balancing concepts will be implemented on the path. Here in this paper, the SDN paradigm is proposed for inter-domain routing. In this paper, the author proposed a model such as evolving the border gateway protocol for the bird’s eye vision over multiple networks. So by taking this as the reference, path selection can be made using border gateway protocol. Also here the multi-domain centralization is focused by the author to develop the slow convergence of border gateway protocol.

By this study, the BGP for path selection could be easy. Also, the software-defined networking approach is used by the author. Mainly it is used to separate the network control plane from the data plane. Actually, various researches are found regarding border gateway protocol. But the path exploration is the major problem [2]. So this paper is proposed concerning the path exploration using the border gateway protocol. For path selection, the BGP protocol is used.

The convergence problems and their solutions are discussed by the author. Then the proposal is delivered for inter-domain routing with better properties of border gateway protocol. And the hybrid routing method is explored by the author. For that, it has some design goals. They are exploiting centralization, disjoint clusters, and hybrid routing. Here two graphs are explored. They are switch graph and AS graph. The switch graph is represented as the simple directed graph regarding the physical topology. The algorithms are used by the author regarding path exploration. And the path re-computation problem is resolved by the BGP path vector protocol. In the proposed work, the SDN approach is used to develop the properties of inter-domain routing properties when enabling the routing applications across various networks. And it is done by the centralized inter-domain routing controllers and AS clusters. Then the proof-of-concept SDN controller is used to control the AS clusters. Two concepts are implemented such as link-state SDN routing and the interplay between path vectors BGP.

And the new kind of inter-domain protocols is delivered such as HLP which contain link-state routing. A detailed discussion is made about routing centralization. The central NOS is proposed to deliver the rules and procedures of AS clusters. These procedures are used to develop routing stability and mitigate path inflation. The routing control logic is proposed here to make the routing configuration and optimization. And the python-based emulation framework is established here for conducting the experiment such as hybrid BGP-SDN. This framework delivered the mininet emulator and it provides the offer such as OS-level virtualization. This framework is called SIREN. The python code is established for developing the framework. Also, these AS clusters are using a non-SDN mechanism such as router and switch for the internal routing. This framework automatically assigns the IP address and making the configuration regarding the network devices.

This paper explains optimizing the BGP routes using SDN (Software-defined networking) technology for reducing the latency in the networking topology concepts. BGP (border gateway protocol) is a kind of gateway protocol and it is designed for reducing latency. On the internet, the Latency of the packet travel mainly depends on the distance of the packets traveled to the wide-area networks. Normally BGP protocols are there by default in the internet service provider. There are a number of benefits are occurring during the optimization of the BGP routes. The important benefits are identifying the latencies which are caused due to the distance traveled from its source. When optimizing the BGP routes the distances will be reduced and the other better routes will be automatically identified by the BGP.

Hence the mesh topology will be achieved. The mesh topology is connected with the BGP by means of route optimization. During the optimization of the BGP routes, the congested paths will be eliminated by the best path algorithm. This process is also called route elimination [2].

BGP protocol also performs the identification of the shortest routes by collecting the information sent by its neighbor nodes. Hence the link between the nodes will be achieved. But sometimes the routes of the nodes may too far from their neighbor. At that time the latency may higher. Hence the connection may not achieve and it is very difficult to provide the connection in the mesh topology. At that, the routes will be provided by the PRS (public route servers).

TABLE I: SHOWING ALL THE RESEARCH AND THE WORK THAT HAS BEEN DONE TILL NOW

Papers	Short Description	Optimum Path	Path Pruning	Congestion Paths	Improved BGP Delay
Approaches to Reduce BGP Inter-Domain Routing Convergence Delay on the Internet	In this paper, the convergence delay in BGP inter-domain routing is analyses and methods to reduce the convergence delay of BGP is described.	✓			✓
Routing centralization across domains via SDN: A model and emulation framework for BGP evolution	In this paper, the internet routing paradigm is proposed, and it is centralized. The software defined networking paradigm is centralized and it improves the convergence of BGP.	✓	✓		✓
Inter-domain SDN: Analyzing the Effects of Routing Centralization on BGP Convergence Time	The SDN (software defined networking) is proposed. The performance analysis is done on inter-domain routing centralization. The convergence is accelerated using inter-domain routing centralization approaches.	✓			✓
An Improved Quality Path Selection Approach for Border Gateway Protocol.	In this paper, the path selection approaches in BGP are discussed. The router instability causes changes in path selection on the internet. The ISPS approach is proposed here for path selection process.	✓		✓	
A New method to optimize BGP routes using SDN and reducing latency.	In this paper, the BGP routes are optimized using software defined networking approach and reducing latency.	✓			

TABLE II: SHOWING THE RELEVANT RESEARCH AND SHORT DESCRIPTION

Solution	Authors	Short description
To reduce the BGP convergence time	[1] Da Silva, R., & Souza Mota, E.	They used efficient policy configuration, multipath, speeding up updates, centralized control, and limiting path exploration approaches to solve the slow convergence problem.
To improve the general properties of inter-domain routing, such as the convergence behaviour accompanying routing changes	[3]Kotronis, V., Gämperli, A., & Dimitropoulos, X	The SDN centralization, model and emulation framework for BGP is used to solve the BGP convergence problems.
To accelerate convergence of BGP	[4] Sermpezis, P., & Dimitropoulos, X.	The router centralization is proposed which based on SDN is used to solve the slow convergence issue in BGP by accelerating BGP convergence.
To modify the path selection process efficiently	[5] Shukla, S., & Kumar, M.	The ISPS approach is used here to improve the SRS approach. The ISPS continuously monitors the traffic flow for selecting the best path.
To optimize BGP routes	[2] Elguea, L., & Martinez-Rios, F.	Here also, the BGP routes are optimized. The best routes (paths) are selected by using SDN approach and by reducing latency.

III. SOFTWARE DEFINED NETWORKING (SDN) OVERVIEW

SDN is a new technology that has begun in the last decade that physically separates the network control plane from the forwarding plane, and where a control plane controls domain devices, which provides simplicity in router management within AS and provides faster inter-domain routing (see Fig. 1). Network management can centrally enforce changes, update routing policies through the NOS global view, and deploy them. The SDN control layer is usually referred to as the Network Operating System (NOS) because it supports the network control logic and provides the application layer with an abstracted view of the global network, which contains enough information to specify policies while hiding all implementation details.

The Open Networking Foundation (ONF) describes SDN as a networking model that separates the intelligence of the network control plane from the forwarding plane, and logically centralizes the control in the controller [3].

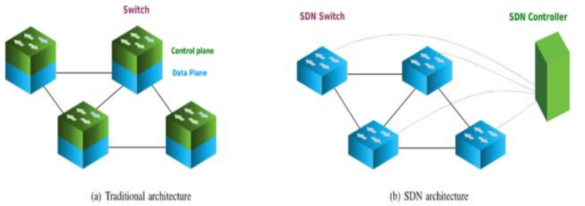

Fig. 1. Traditional network verses software define network

The essential part of SDN is the SDN controller. A controller is an application which is responsible for making the logical decisions in an SDN network. The controller manages all the southbound devices in an SDN network and installs the flow entries in the SDN devices. Some of these flow entries are generated after going through a logical decision making process. Such entries are called reactive flow entries.

Other type of flow entries are the proactive flow entries, which are flow table entries that are installed predicting or determining the conditions of the network. For example, a flow entry to change the network topology if the bandwidth utilization exceeds a threshold value would be a proactive flow entry. Controller, is consider to be the brain of the SDN (See Fig. 2).

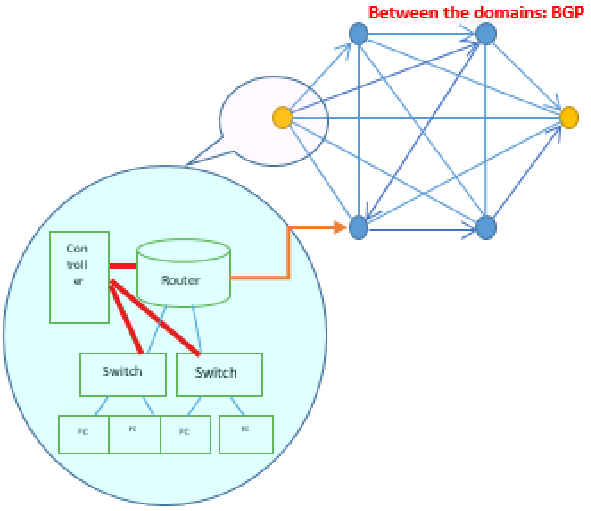

Fig. 2. Inside the AS and the SDN RESOURCES

Because of the software based functions and Open Flow protocol which allows the data flow to and from the switch is very easy to be implemented this can help improve the old way of router complexity. SDN can help build simpler control planes by centralizing instead of replicating complexity in all the switches and routers inside the AS.

IV. SDN Protocol – OpenFlow

OpenFlow is an open standard being developed by Open Networking Foundation. It is the first standard interface for communications between controller and forwarding layers of SDN. The purpose of OpenFlow is to give the controller direct access to forwarding planes of network equipment. Despite the fact that SDN is not directly connected to the OpenFlow protocol, it is de facto standard for communications between controllers and devices. OpenDayLight controller website states that “while OpenFlow is a useful protocol in many scenarios, SDN is not limited to OpenFlow or any single protocol”. There are few technologies that can perform similar capabilities such as I2RS, VxLAN, and PCEP.

V. Challenges of SDN

Designing a controller requires major effort if the controller is to provide flexible interfaces for network services and applications and a verified OpenFlow interface. It involves more than just designing and implementing the interfaces [4]. Selected challenges are described below:

Scalability. One of the issues when offloading control from the switching hardware is the scalability and performance of the network controllers. SDN’s centralized control scalability issues. The controller is the main important part in SDN, and a single may result in a single point of failure and not good performance (bottleneck) when considering wide-area SDN. The entire network will not function if there is a problem with the controller as it is centralized management. These switches will experience latency. A single controller solution is not very suitable for wide-area SDN. Other concerns on the scalability of SDN in vast networks are the aggregating and disseminating of a massive amount of information, both from and throughout the network. Those processes need to be carried out in real-time, which makes things worse [4], [5].

Placement and Reliability. In the wide-area SDN implementation, controller(s) location could have major importance on SDN performance. Whether the SDN consists of single or multiple controllers, the placement of the controller(s) will have an impact on the performance and the cost of the network. The research shows that latency drives the overall behavior of the network, and bandwidth for the control traffic affects the number of flows that the controller can process. Alternative approaches try to solve the controller(s) placement issue, optimize the reliability of the control network and identify several placement algorithms and strategies along with metrics to characterize the reliability of SDN control networks [6].

Availability. SDN in the vast global network could suffer from various failures. The potential failures include controller/switch failure and link failure. SDN controllers can be overloaded due to an enormous number of requests from linked network devices. An SDN-enabled switch could be confronted with a failure if any of its sub-components does not function correctly. Controller failure could cause the traffic routing/forwarding functions of linked network devices to become limited. Network link failure can occur due to the link itself failing or the terminating devices failing. In SDN networks, the design, including placement and selection of network devices such as the SDN-controllers and SDN-switches, should be strong, and this should be tested for a range of scenarios. An approach that improves SDN robustness is to use a runtime system that automates failure recovery by spawning a new controller instance and replaying inputs observed by the old controller. The controller can install static rules on the switches to verify topology connectivity and locate link failures based on those rules. Another approach is to try to improve recovery time by the frequent issuing and receipt of monitoring messages, but this may place a significant load on the control plane. In multi-controller SDN, a load balancing mechanism based on a load informing strategy is proposed to balance the load among controllers dynamically [7], [8].

Security. SDN controllers may suffer from a range of security problems, which can reduce network performance. The attacks might affect performance due to the lack of controller scalability in the event of a denial of service (DoS) attack. The impact could become severe in the extensive network for the single controller or multiple controller scenarios. The attacks can target the forwarding layer, control layer, and application layer. DoS is an attack that might target the forwarding and control layers. DoS could be caused by massive traffic flows that flood the switches which subsequently flood controllers with traffic route requests. The result is a slowing down of the network and possibly device collapse. Another type of attack is the compromised controller attack, which happens when the attacker gains access to the controller and utilizes this access to alter or deny traffic routing. Data leakage and flow rule modification is the impacts of attacks on forwarding layer input buffers, which can be disastrous [9]. Controller hijacking and fraudulent rule insertion attacks are types of malicious attacks. DoS is related to availability-related attacks. Types of DoS attacks include the Controller-Switch Communication Flood that aims to overload the affected switches and controllers. There are possible countermeasures for each of the likely attacks. Attacks targeting the forwarding plane could be avoided by proactive rule caching, rule aggregation, increasing switch buffering capacity, decreasing switch-controller communication delay, and packet type classification based on traffic analysis. Other attacks that target the control and application plane could be mitigated by controller replication, dynamic master controller assignment, efficient controller placement, controller replication with diversity, and resourceful controller assignments [10].

VI. SDN in the WAN

The introduction of SDN in WAN has introduced an improvement in management and control of the network. One of the critical factors for SDN implementation in the WAN is scalability. Issues such as single point of failure and performance bottleneck can appear due to the centralized nature of SDN.

There are two approaches for SDN deployment in the WAN, i.e., using a single controller or multiple controllers. Due to its limitation of becoming a single point of failure and lower performance, and also because of the need to many domain controllers when dealing with BGP the single controller approach are not likely to be suitable for SDN implementation in the WAN for research and testing purposes. In our thesis, we use only one controller per domain. In the multiple controller approach, two architectures are proposed, i.e. the centralized architecture and fully-distributed or multi-domain architecture [11].

VII. Multi-domain SDN Architecture

A multi-domain SDN architecture refers to a network architecture that connects multiple SDN domains. SDN domain refers to the administrative SDN domain, which might be a sub-network in a data center network, or a carrier or an enterprise network, or an Autonomous System (AS). Many distributed control plane architectures with a logically centralized cannot cope with inter-domain flows between SDN domains. There are two main issues for multi-domain SDN: vertical and horizontal, as shown in the vertical approach, the controllers are connected into a hierarchical control plane where the controller functionality is organized vertically. In this deployment model, control tasks are distributed to different controllers depending on selected criteria such as network view and locality requirements. The communication between SDN controllers are performed via RESTful APIs. Local events are handled by the controller that is lower in the hierarchy, and global events are handled at the higher level, which is called the master controller. In the horizontal approach, multiple controllers were organized in a flat control plane where each one governs a subset of the network switches, and the SDN controllers can communicate with each other using a standard inter-domain SDN protocol [12].

VIII. Communication between Domains in SDN

The SDN inter-domain communication protocol can be implemented using the SDN controller East-Westbound interface. Its main functions are to set up a connection between controllers in different domains and exchange control, service, and application information. The East-Westbound interface has not been standardized, which could lead to an interoperability challenge in the deployment of multi-domain SDN. Currently, many SDN controllers have been developed by open-source communities and private companies, complying with the Southbound interface standard, i.e. OpenFlow, but there are no interoperable protocols for the East-Westbound interface.

IX. BGP Overview

BGP is categorized as a path vector protocol, a variant of distance vector protocol. Instead of distributing link cost information, it propagates full path information to avoid cycles. BGP employs TCP as its transport protocol, which ensures transport reliability and eliminates the need for BGP to handle retransmission, acknowledgment, and sequencing. Routers that use BGP are called BGP speakers. Two BGP speakers that participate in a BGP session are called neighbors or peers. Peer routers exchange four types of messages: open, update, notification, and keep-alive. The update message carries routing information while the remaining three messages handle session management [12].

The routers that support BGP usually wait for BGP connections on port 179. A router that wants to establish a peer session will first open a TCP connection to port 179 on the peer router. Once the connection is set up, each side sends an open message to negotiate the session's parameters. In order to constantly monitor the reachability of their neighbors, the BGP routers send regularly keep-alive messages. During the opening exchange, the BGP routers announce a hold time, the maximum interval during which the peer should have to wait between successive messages.

BGP is a protocol used for maintaining routing information between ASes. Each AS is connected to a number of other ASes (called neighbors or peers) and exchanges its routes with them according to AS-specific policies. After receiving information an AS may propagate it to its own neighbors. This lets the information spread like gossip.

X. Routing Policies

BGP itself is a vector protocol in the purest form. When deferent routes for a given prefix are available, the shorter one is considered to be the better one. Although this behavior seems to be reasonable, it is not always desirable for a particular AS operator. For that reason, BGP allows creating a set of rules that determine which route is the best and, what is more important, whether a route is suitable to be forwarded to a neighbor. Such a set of rules are called policies (See Table III).

Table III: Steps Used to Select the Path in BGP

Selection Criteria	
Nr	Criteria
1	Selects the route with the highest local-preference
2	Selects the route with the lower AS-path length
3	Prefers the route with origin IGP over BGP and origin BGP over others
4	Among the routes received from the same AS neighbor, discard those having higher multi-exit-discriminator than the lowest
5	Prefer routes learnt via eBGP to those learned via iBGP
6	Prefer routes with lower IGP metric to the egress point
7	Prefer the route announced by the BGP router with the lowest router-id (i.e., IP address)

XI. Algorithem Selection

The ID3 is one of the decision tree algorithms. The raw data is transformed into a rule-based decision-making tree by decision tree algorithms. The ID3 decision-making algorithm was introduced in the year of 1986. The full form of ID is Iterative Dichotomiser. This algorithm divides the attributes into two groups. These two groups of attributes are dominant attributes. The other attributes are used to construct a tree. Here, the most dominant attribute is found and it is put as a decision node on the tree. After that, the second dominant attribute is found. This process is continued until it reaches a decision for that branch. The decision tree algorithm is used to make the best decision. The algorithm that we are going to use is ID3. It is used in many types of research. By using this decision-making algorithm, the best path for BGP routing protocol can be found. We use ID3 because it eliminates the overloaded paths by taking the parameters that have been collected previously from each domain in a Mesh Topology.

XII. Mathematical Modelling

As a topology for our implementation, we are using Mesh Topology, but as future work will be to implement in other topologies as well. All the domains in mesh (see pictures 2 and 3) topology will have their network set up with routers, switches, and PC-s and will be connected with each other using BGP protocol. Applying route discovery by sending the packet to all the domains in order to find all the paths from the source domain to all domains in a mesh topology and then create all optional paths that lead to the destination. The formula below manages to find all the paths within a mesh topology.

$$fC(r) \sum_{(a,b)\epsilon R} C(a,b)$$

NT (N) = NPT <= Mt

Node time of the node/Throughput = Node processing time <= Maximum through

$$Total\ Delay(S) \sum_{S,D} Ca,b = \sum_{n=1}^{n} \mathrm{T}_{delay}(d)$$

After finding all the paths on the mesh topology and their information dhe next step will be to find Transmission delay is equal with adding together the

Transmission Delay, Queuing Delay and Processing Delay.

T_delay=T_process+T_queue+T_transmit

The probability that a uniformly distributed random variable falls within any interval of fixed length is independent of the location of the interval itself (but it is dependent on the interval size), as long as the interval is contained in the distribution's support.

$$\mathrm{P}(\mathrm{x} \in [\mathrm{x}, \mathrm{x}+\mathrm{d}]) = \int_{x}^{x+d} \frac{dy}{b-a} = \frac{d}{b-a}$$

which is independent of x. This fact motivates the distribution's name.

Applying the ID3 will be the next step in order to eliminate the overloaded paths.

XIII. Multi AS Domains

The advantage of the multi AS Domains is that the topology approach grows as the size of the topology increases. This is done by the controller in each domain that manages to discover the paths to other domains and share the information with everyone. Centralizing the routing control on all domains will help process the delay and find an optimal path faster. Running the algorithm in each domain can be set after any interval time that is convenient.

XIV. Inter-domain Routing

An autonomous system shares routing information with other autonomous systems using the protocol called Border Gateway Protocol (BGP). On each independent Autonomous System an improved way of finding and selecting the paths can be implemented. In each of this AS e new algorithm will be implemented that will process the delay in each path and find the most optimal paths available on the time the algorithm has run. This algorithm that runs inside domain will eliminate (prune) the overloaded paths and will select only the paths that have less Delay and less bottleneck available. For example, we can have 10 paths that are available for the destination from Domain 1 to Domain 6. If we take the paths as we find them then the probability that the delay will happen is much higher than if we manage to rank the paths and provide the best one to the next packet that will be sent. So we apply the ID3 algorithm that prunes the overloaded paths and create the list with only "Good Paths". This will have a big advantage on data transmission.

XV. Network View Generalisation

In the inter-domain context, controlling the flow of data packets between the domains in a global network have the need of each controller to have a relative global network view for the next controller hop.

Hence, Speaking Routers are required to exchange reachability and topology information between inter-domain networks.

The view of networks covers the information like:

Reachability: IP addresses.

- Topology: nodes (e.g. switches, servers, hosts, controllers, firewalls, balancers, others), links, link attributes, port throughput, link connections.
- Network service capabilities, such as SLA (service FlowTables in each switch, and how many flow entries each FlowTable supports.
- Forwarding capability parameters, such as latency, reliability, packet loss rate, availability, maximum throughput, time delay variation, and cost.

The network dynamic information mainly includes the network status, such as FlowTable entries information in each switch, real-time bandwidth utilization in the topology, and all the flow paths in the network [12].

XVI. Network Configuration

Network simulator software NS3 is used in order to simulate the network with independent domains and the domain infrastructure within. We placed two OpenFlow switches on each domain, with 2 PC in each OpenFlow switch connected. Open flow and Controller is installed within the quagga router. We created six domains (The test could be done also in many domains as well as future work) in a mesh topology (the tests and implementation will be done in the future also in other topologies like: Grid Topology, Random graphs Erdos - Renyi, Scale-free graphs - Barabási – Albert model, Small-World Graphs - Newman-Watts – Strogatz). The IP address is allocated dynamically taking into consideration the scalability of the network. The controller that is installed in the router is Learning Controller [13].

XVII. Evaluation of Multi Domain Paths

Regarding AS mesh topology simulation, we initially design the topology with SDN switches, routers Open flow and controllers then we expand to the mesh topology of AS domains. In order to get the information for each domain after the design, we send the packed to all the domains in the mesh topology. The following are the simulation parameters that we have used (See Table IV):

Table IV: Simulating Parameters

Parameter	Value
Network Topology	Mesh network topology
Number of Domain	6
Number of PCs (domain)	4
Number of Switches (domain)	2
Number of Router	1
Routing Protocol	BGP routing protocol

OpenFlow Controller	Learning controller
Mac Protocol	CSMA
Data Rate	5Mbps
Transfer Delay Time	2ms
Transport Layer Protocol	UDP
Simulating Time	100sec

XVIII. Scenarios and Result

Simulation is performed to demonstrate the validity of proposed techniques (Fig. 3).

The simulation is based on the complexity analysis of the algorithm NS path optimization.

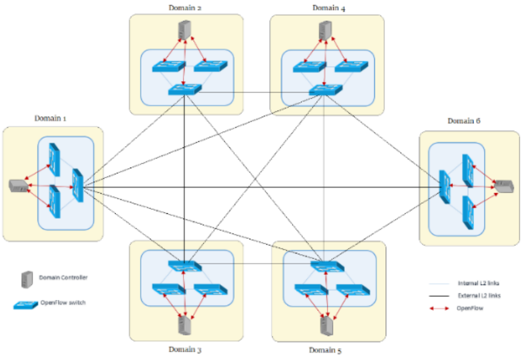

Fig. 4. Diagram showing six AS domain used for implementation

In order to gather e wider results and compare them, we proposed few scenarios. We have considered the following scenarios: Consider the network presented in Fig. 4, in which there are 6 AS Domains, D1 to D6. Each AS chooses its route from source to destination. Now, let us assume that domain D1 is not satisfied with the performance provided by D2 due to les resources or congestion and does not want D2 to carry its traffic to D6 because it will cause delay or even fail to send the traffic to the destination.

In order for the traffic from D1 to go to the D6, without any congestion we firstly need to find all the paths within the topology. Finding all the paths it is not an easy task. For our scenario, we will use Domain 1 to Domain 5.This is the default test with default capacity and for the testing purpose we use only one path of the domain 1 => 4 => 5.

The problem that is raised here is the Processing delay when sending data to domain 5. In the above table, we have some paths that are overloaded and we consider them as a NOT GOOD PATH, because of the delay that can cause on delivering the data from Domain 1 to Domain 5. In order to overcome this problem and improve the load on the links, we need to use an algorithm that can remove the overloaded paths and the failed paths and leave only the good paths as available paths for data transmission(See Table V-VI).

TABLE V: SHOWS ALL THE POSSIBLE PATHS FROM D1 TO D5 BEFORE APPLYING THE ID3 ALGORITHM

Domain-1 ----> Domain-5

Thro.put	T.Delay	P.Delay	Q. Delay	Hop	Bott	Conver	Route Path
781.856	0.00512	0.00905	0.00506	0	0	10.067	1 -> 5
609.012	0.00657	0.01024	0.01679	1	0.25	11.929	1 -> 2 -> 5
781.856	0.00512	0.01058	0.01613	1	0	10.373	1 -> 3 -> 5
609.576	**0.00656**	**0.00921**	**0.01238**	**1**	**0.25**	**11.667**	**1 -> 4 -> 5**
609.638	0.00656	0.01081	0.01185	1	0.25	11.862	1 -> 6 -> 5
657.46	0.00608	0.01081	0.0136	2	0.167	11.436	1 -> 2 -> 3 -> 5
567.94	0.00704	0.00992	0.01078	2	0.333	12.414	1 -> 2 -> 4 -> 5
567.855	0.00704	0.01097	0.01417	2	0.333	12.477	1 -> 2 -> 6 -> 5
658.151	0.00608	0.0101	0.01247	2	0.167	11.27	1 -> 3 -> 4 -> 5
657.704	0.00608	0.01119	0.01621	2	0.167	11.433	1 -> 3 -> 6 -> 5
567.362	0.00705	0.01028	0.01392	2	0.333	12.316	1 -> 4 -> 6 -> 5
609.456	0.00656	0.01039	0.01149	3	0.25	11.843	1 -> 2 -> 3 -> 4 -> 5
609.169	0.00657	0.01121	0.01429	3	0.25	11.965	1 -> 2 -> 3 -> 6 -> 5
548.779	0.00729	0.01055	0.01234	3	0.375	12.714	1 -> 2 -> 4 -> 6 -> 5
609.302	0.00656	0.01068	0.01361	3	0.25	11.856	1 -> 3 -> 4 -> 6 -> 5
583.438	0.00686	0.0108	0.01259	4	0.3	12.197	1 -> 2 -> 3 -> 4 -> 6 -> 5

TABLE VI: SHOWS ALL THE POSSIBLE PATHS FROM D 1 TO D 5 AFTER APPLYING ID3 ALGORITHM

XVIII. Domain-1 ----> Domain-5

Thro.put	T.Delay	P.Delay	Q. Delay	Hop	Bott	Conver	Route Path
781.856	0.00512	0.00575	0.00506	0	0	10.067	1 -> 5
781.856	0.00512	0.00708	0.01613	1	0	10.373	1 -> 3 -> 5
609.576	0.00656	0.00582	0.01238	1	0.25	11.667	1 -> 4 -> 5
609.638	0.00656	0.00745	0.01185	1	0.25	11.862	1 -> 6 -> 5
657.46	0.00608	0.00739	0.0136	2	0.167	11.436	1 -> 2 -> 3 -> 5

XIX. Conclusion

This research paper introduces three key problems relevant to data movement across the multi-domains. They are (1) delays on data transmission because of the failures of the links, (2) high throughput data transfer over large networks due to the worst path selection using the BGP, and (3) the efficient distribution of data (Load balancing and scalability). All three problems introduce scalability, load balancing, and fail-over concerns with respect to the network architecture. The recent steps taken by SDN due to the introduction and popularity of OpenFlow provide a new way to approach these problems. This research paper proposes and demonstrates solutions to the aforementioned problems using scalable approaches introduced in SDN Controller.

This research paper details the elements that influence BGP decisions on path selection using SDN infrastructure. Based on the features, a testbed using NS3 has been designed and implemented which explores ideas related to the domain to domain data transmission. The implementation of the Mesh topology of wires Domains was completed using NS3. This paper discusses also OpenFlow Service and the SDN involvement on BGP improvement over long-distance networks and the end-users who wish to obtain the data in a timely manner with minimal effort.

The result shows that the requirement for improving scalability, load balancing, and failover has been reached. Referring to the result, with this research we have achieved to improve scalability, load balancing, and failover on interdomain communication.

ID3 is an algorithm that uses an entropy-based decision tree learning algorithm which continues to grow a tree until it makes no errors over the set of training data. This fact makes ID3 prone to overfitting [13] In order to reduce overfitting, pruning is used. When we apply the pruning we manage to remove the path that does not fulfill the criteria and we left only with a “GOOD PATHS”. See the picture below:

The future work should be concentrated on further improving load balancing on the BGP paths. Also, another point of focus should be on the virtual resources of routers that stand as border gateway. For many years the BGP protocol as not been improved and challenged, so there is a need to come up with another way that should be more secure, efficient and improve the load balancing between the domains. Implementing a similar scenario in different platforms like GNS3 would be also and contribute towards finding better resources and paths for transmitting the data.

This paper presents three major problems related to the movement of data and data transfer between AS.

They are (1) data transmission delays, (2) failure to transfer data due to node damage. (3) failure to balance data transmission due to poorly selected routes. All three problems represent scalability, load balancing, and failures with respect to network architecture. The latest steps taken by SDN due to the introduction and popularity of OpenFlow offer a new opportunity to approach these problems. This paper proposes and demonstrates solutions to the above problems using the scalable approaches presented in the Controller SDN.

This paper details the elements that influence BGP's decision to choose the best routes using the SDN infrastructure. Based on the features, a testbed using NS3 has been designed and implemented to explore domain-related ideas to domain data transmission. The implemented Mesh topology of wires domains was completed using a network simulator NS3 in a dedicated infrastructure.

This paper also discusses the OpenFlow Service and the involvement of SDN in improving BGP in long-distance networks (Autonomous Systems) and end-users who wish to receive the data in a timely manner with a minimum of effort. This has been done by implementing the ID3 algorithm which helped to select a group of best paths to be used for data transmission. The best paths are selected by considering the node parameters. The result shows that the requirement for improved scalability, load balancing, and failover has been reached. Referring to the result, with this research we have achieved to improve scalability, load balancing, and failure over interdomain communication. Future work

Future work should focus on further improving load balancing on the BGP paths. Also, another point of focus should be on the virtual resources of routers that stand as a border gateway. For many years the BGP protocol has not been improved and challenged, so we need to come up with another way that should be more secure, efficient and improve the load balancing between domains. Implementing a similar scenario in a different platform like GNS3 would also contribute to finding better resources and paths for transmitting data.

Another future work will be the implementation that can not only be implemented in different testing platforms but can also be tested in different topologies. I have started to implement in different topology but could not manage to complete it so this can be future work.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Nysret’s and Artan’s contribution is equal in this paper. We both did the literature research and completed the paper in equal contribution. Artan’s contribution apart of other equal contribution is in mathematical model. We did implementation and testing together as we work together in the same University and we started and complete the paper together.

ACKNOWLEDGMENT

The authors wish to thank A, B, C. This work was supported in part by a grant from XYZ.

REFERENCES

[1] R. D. Silva and E. S. Mota, “A survey on approaches to reduce BGP interdomain routing convergence delay on the internet,” *IEEE Communications Surveys & Tutorials*, 2017.

[2] K. Shuraia, K. Farookh, O. Hussaina, and K. Hussain, “Guaranteeing end-to-end QoS provisioning in SOA based SDN architecture: A survey and open issues,” *Future Generation Computer Systems*, vol. 119, June 2021.

[3] V. Kotronis, A. Gämperli, and X. Dimitropoulos, «Routing centralization across domains via SDN: A model and emulation framework for BGP evolution,” *Computer Networks*, 2015.

[4] P. Sermpezis and X. Dimitropoulos, “Inter-domain SDN: Analysing the effects of routing centralization on BGP convergence time,” *ACM SIGMETRICS Performance Evaluation Review*, 2017.

[5] S. Shukla and M. Kumar, “An improved quality path selection approach for border gateway protocol,” *International Journal of Intelligent Engineering And Systems*, 2017.

[6] Y. Zhiwei and L. Jong-Hyouk, “BGPChain: Constructing a secure, smart, and agile routing infrastructure based on blockchain,” *ICT Express*, January 2021.

[7] M. Pablo and H. L. Raquel, “JeanCampc, using bursty announcements for detecting BGP routing anomalies,” *Computer Networks*, vol. 188, April 2021,

[8] A thesis Submitted in Fulfilment of the Requirements for the Degree of Doctor of Philosophy, F W, RMIT University, Nov. 2018.

[9] P. Lin, J. Bi, S. Wolff, and Y. Wang. A West-East Bridge Based SDN Inter-Domain Testbed. [Online]. Available: http://netarchlab.tsinghua.edu.cn/~junbi/IEEEComMag-2015.pdf

[10] A. Ishtiaq, A. Ashikur, and K. Rahman, “QoS performance enhancement policy through combining fog and SDN, simulation modelling practice and theory,” *Elsivier*, February 2021.

[11] Prof. Alvarez, Machine Learning, Decision Tree Pruning Based on Confidence Intervals, Accesed 2019

[12] F. Wibowo, M. Gregory, and K. Gomez, Multi-Domain Software Defined Networking: Research Status and Challenges, Melbourne, Australia, Article, 2017

[13] Elizabeth O'Dowd, Benefits of Software-Defined Networking in Healthcare, Hit Infrastrukture. [Online]. Available: https://hitinfrastructure.com/features/benefits-of-software-defined-networking-in-healthcare

Prof. Ass. Dr. Nysret Demaku was born in Prishtina, Kosovo. He received B.S. and MSc degree from Kingston University of London. I have completed my PHD in Computer Science in LSBU and UNIBIT in the research topic “Applying Load Balancing, Scalability and Fail over in inter-domain SDN”. His research interests include SDN with NFV architecture towards 5G, Service orchestration. Control plane optimization for QoS and SDN for mobile and wireless networks

Associate Prof. Dr. Artan Dermaku is the Dean at the Faculty of Computer Science at the UKZ. He received his bachelor, master degree and PhD from TU-Wien. He has worked for two years as Scientific Project –Research Employee at Vienna University in Austria, on the project: “Complementary Approaches to Constraint Satisfaction” - Finding and implementing of the heuristic - approaches in order to solve CSP (Constraint Satisfaction) problems. His research interests include Theory and algorithms. Data and network science, Evolutionary computing and optimization, Machine learning etc.