An Adaptive MT-BGP Traffic Engineering Based on Virtual Routing Topologies

Dr.V. Palanisamy [#1], K. Gowri [*2]

Head of the Department
#Department of Computer Science and Engineering, Alagappa University
Karaikudi, Tamil Nadu, India

Abstract:

Internet is not a single network. The Internet is a collection of networks, each controlled by different administrations. Traffic engineering is an important mechanism for Internet network providers seeking to optimize network performance and traffic delivery. Routing optimization plays a key role in traffic engineering, finding efficient routes so as to achieve the desired network performance. BGP is the de facto protocol used for inter-autonomous system routing in the Internet. BGP has been proven to be secure, efficient, scalable, and robust. In proposed introduced AMPLE – an efficient traffic engineering and management system that performs adaptive traffic control by using multiple virtualized routing topologies in MT-BGP. The proposed system contains three complementary components: offline link weight optimization that takes as input the physical network topology and tries to produce maximum routing path diversity across multiple virtual routing topologies for long term operation through the optimized setting of link weights in BGP (Border Gateway Protocol) with admission traffic control algorithm. In our proposal, AMPLE (Adaptive Multi-toPoLogy traffic Engineering), a holistic system based on virtualized BGP routing topologies for dynamic traffic engineering. This paper also concentrates creates new path with help of ADC algorithm. This scheme allows a network to operate in the region of low delay, no packet loss and high throughput.

Keywords: Admission control algorithm, ATC, BGP, OLWO,

I. INTRODUCTION

Inter-domain Traffic Engineering (TE) based on BGP (Border Gateway Protocol). The BGP is an inter-autonomous system (AS) routing protocol. An autonomous system is an administrative domain. That is, it is a network or group of networks under a common administration and with common routing policies. BGP is used to exchange routing information in the Internet and is the protocol used by default to communicate between Internet service providers (ISP). Customer networks, such as universities and corporations, usually employ protocols known as Interior Gateway Protocol (IGP) to exchange routing information within their networks. Examples of IGPs are Routing Information Protocol (RIP) and Open shortest Path Protocol (OSPF). Customers connect to ISPs, and ISPs use BGP to exchange customer and ISP routes. A network under the administrative control of a single organization is called an autonomous system (AS) [1]. There are two types of routing, intra-domain routing which is the process of routing within an AS, and inter-domain routing which is the process of routing among different ASs. BGP is the dominant inter-domain routing protocol on the Internet (BGP) [2]. BGP has been deployed since the commercialization of the Internet, and version 4 of the protocol has been in wide use for over a decade. There are two variations of BGP: Interior BGP (IBGP), which is used by ISPs to exchange routing information within an AS; and External BGP (EBGP), which is used to exchange routes among autonomous systems. Figure 1 illustrates the difference IBGP and EBGP [6]. BGP is a simple protocol and it generally works well in practice. Thus, it has played a fundamental role within the global Internet [3], despite providing no performance or security guarantees.
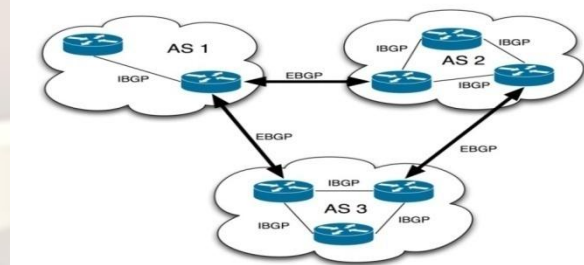

Fig 1: EBGP and IBGP

An autonomous system is also sometimes referred to as a routing domain. An autonomous system is assigned a globally unique number, sometimes called an Autonomous System Number (ASN). Networks within an autonomous system communicate routing information to each other using an Interior Gateway Protocol (IGP). An autonomous system shares routing information with other autonomous systems using the Border Gateway

Protocol (BGP). Previously, the Exterior Gateway Protocol (EGP) was used. In the future, the BGP is expected to be replaced with the OSI Inter-Domain Routing Protocol (IDRP). BGP is a very robust and scalable routing protocol.

II. AMPLE Related Work

AMPLE includes two distinct tasks, first one offline network dimensioning through link weight optimization for achieving maximum intra-domain path diversity across multiple MT-IGP routing topologies; second one adaptive traffic splitting ratio adjustment across these routing topologies for achieving dynamic load balancing in case of unexpected traffic dynamics. In *AMPLE*, the MT-IGP configuration produced in the offline phase provides an opportunity to use multiple diverse IGP paths for carrying traffic with arbitrary splitting across multiple routing topologies. More specifically, each source node can adjust the splitting ratio of its local traffic (through remarking the Multi-Topology ID field of the IP packets) according to the monitored traffic and network conditions in order to achieve sustainable optimized network performance (e.g. minimize the Maximum Link Utilization, MLU). It is worth mentioning that the computing of new traffic splitting ratios at each source PoP node is performed by a central traffic engineering manager. This TE manager has the knowledge about the entire network topology and periodically gathers the overall network status such as the current utilization of each link and traffic matrices based on which the new traffic splitting ratio is computed and thereafter enforced at individual source nodes [8].

III. EXISTING WORK

In Existing System, IGP-based TE mechanisms are only confined to offline operation and hence cannot cope efficiently with significant traffic dynamics. There are well known reasons for this limitation: IGP-based TE only allows for static traffic delivery through native IGP paths, without flexible traffic splitting for dynamic load balancing. In addition, changing IGP link weights in reaction to emerging network congestion may cause routing re-convergence problems that potentially disrupt ongoing traffic sessions. In effect, it has been recently argued that dynamic/online route re-computation is to be considered harmful even in the case of network failures, let alone for dealing with traffic dynamics [7]. In the existing system does not achieve good performance in minimizing the MLU. Even if multiple traffic matrices with different pattern characteristics are considered in link weight optimization, unexpected traffic spikes may still introduce poor TE performance. *AMPLE* encompasses two distinct tasks, namely (1) offline

network dimensioning through link weight optimization for achieving maximum intra-domain path diversity across multiple MT-IGP routing topologies; and (2) adaptive traffic splitting ratio adjustment across these routing topologies for achieving dynamic load balancing in case of unexpected traffic dynamics [8] but these everything done only in MT-IGP.

A) OSPF (Open Shortest Path First) :

In existing method using OSPF in IGP. Based on the network model, some fundamentals of traffic engineering (TE) will be introduced, which include the commonly used cost and objective functions for quantitatively evaluating and comparing different TE methods [9]. Open Shortest Path First (OSPF) is the most commonly used intra-domain internet routing protocol. Traffic flow is routed along shortest paths, splitting flow at nodes where several outgoing links are on shortest paths to the destination. The weights of the links, and thereby the shortest path routes, can be changed by the network operator. The weights could be set proportional to their physical distances, but often the main goal is to avoid congestion, i.e. overloading of links, and the standard heuristic recommended by Cisco is to make the weight of a link inversely proportional to its capacity [10]. The IS-IS protocol is specified in ISO 10589. Each Intermediate System (IS) (router) advertises one or more IS-IS Link State Protocol Data Units (LSPs) with routing information. The Intermediate System to Intermediate System (IS-IS) protocol to support Traffic Engineering (TE) [11].

IV. PROPOSED WORK

In proposed system using BGP protocol. System consists of three complementary components: **offline link weight optimization** that takes as input the physical network topology and tries to produce maximum routing path diversity across multiple virtual routing topologies for long term operation through the optimized setting of link weights. Based on these diverse paths, **adaptive traffic control** performs intelligent traffic splitting across individual routing topologies in reaction to the monitored network dynamics at short timescale. **Admission control algorithm** using dynamically creates a new path with help of virtual routing topologies. According to our evaluation with real network topologies and traffic traces, the proposed system is able to cope almost optimally with unpredicted traffic dynamics and, as such, it constitutes a new proposal for achieving better quality of service and overall network performance in IP networks using BGP. In proposed system, AMPLE has a high chance of achieving inter network performance with large number of routing topologies, although this is yet to

be further verified with traffic traces data from other operational networks when available. Offline network dimensioning through link weight optimization for achieving maximum inter-domain path diversity across multiple MT-BGP routing topologies; and adaptive traffic splits ratio adjustment across these routing topologies for achieving dynamic load balancing in case of unexpected traffic dynamics.

A. Virtual Traffic Allocation

In this Module, the diverse MT-BGP paths according to the link weights computed by OLWO. Monitored network and traffic data such as incoming traffic volume and link utilizations. At each short-time interval, ATC computes a new traffic splitting ratio across individual VRTs for re-assigning traffic in an optimal way to the diverse BGP paths between each S-D pair. This functionality is handled by a centralized TE manager who has complete knowledge of the network topology and periodically gathers the up-to-date monitored traffic conditions of the operating network. These new splitting ratios are then configured by the TE manager to individual source PoP nodes, who use this configuration for remarking the multi-topology identifiers (MTIDs) of their locally originated traffic accordingly.

B. Offline Link Weight Optimization (OLWO)

In this module, to determine the definition of "path diversity" between PoPs for traffic engineering. Let's consider the following two scenarios of MT-BGP link weight configuration. In the first case, highly diverse paths are available for some Pop-level S-D pairs, while for some other pairs individual paths are completely overlapping with each other across all VRTs. In the second case, none of the S-D pairs have disjoint paths, but none of them are completely overlapping either. Obviously, in the first case if any "critical" link that is shared by all paths becomes congested, its load cannot be alleviated through adjusting traffic splitting ratios at the associated sources, as their traffic will inevitably travel through this link no matter which VRT is used. Hence, our strategy targets the second scenario by achieving "balanced" path diversity across all S-D pairs.

Fig 2 gives an overall structure of the proposed AMPLE TE system, with Offline MT-BGP Link Weight Optimization (OLWO) and Adaptive Traffic Control (ATC) and admission control algorithm (ADC) constituting the key components. As previously mentioned, the ultimate objective of OLWO is to provision offline maximum intra-domain path diversity in the routing plane, allowing the ATC component to adjust at short timescale the traffic assignment across individual VRTs in the

forwarding plane. The MT-BGP link weights does not rely on the availability of the traffic matrix a priori, which plagues existing offline TE solutions due to the typical inaccuracy of traffic matrix estimations. Instead, our offline link weight optimization is only based on the characteristics of the network itself, i.e. the physical topology. The computed MT-BGP link weights are configured in individual routers and the corresponding BGP paths within each VRT are populated in their local routing information bases. While OLWO focuses on static routing configuration in a long timescale (e.g. weekly or monthly), the ATC component provides complementary functionality to enable short timescale (e.g. hourly) control in response to the behavior of traffic that cannot be usually anticipated.
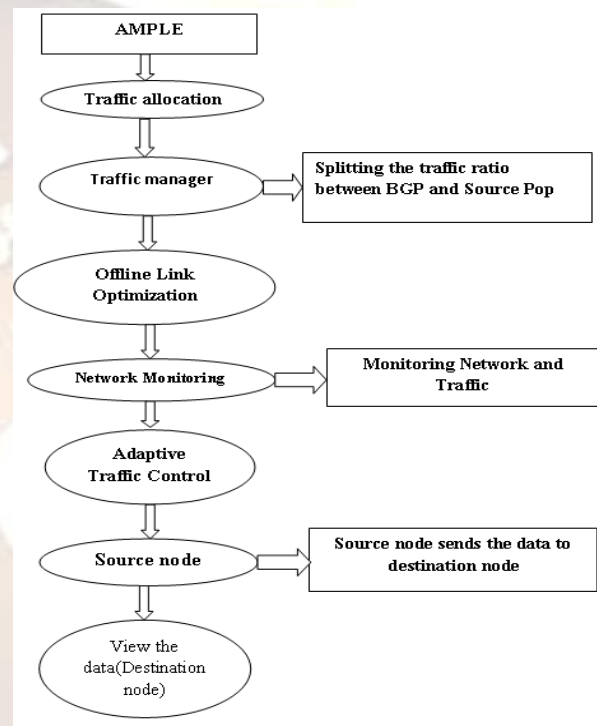

Fig 2: AMPLE structure

C. Network Monitoring

Network monitoring is responsible for collecting up-to-date traffic conditions in real-time and plays an important role for supporting the ATC operations. AMPLE adopts a hop-by-hop based monitoring mechanism that is similar to the proposal [10]. The network monitoring agent deployed at every PoP node is responsible for monitoring: The volume of the traffic originated by the customers PoPs. The utilization of inter-PoP links. The central TE manager polls individual monitoring agent within each PoP and collects their locally monitored traffic volume and link utilizations. These samples are then used by the central TE manager for updating its maintained traffic engineering information base and computing traffic splitting ratios for the next interval.

Such a hop-by hop based exemplar works efficiently in a TE system with a central manager. The main reason is that, new traffic splitting ratios are computed by the TE manager who is able to have the global view on the network, enabling it to achieve a global optimum in traffic control.

A. Adaptive Traffic Control (ATC)

In this Module, Measure the incoming traffic volume and the network load for the current interval as compute new traffic splitting ratios at individual PoP source nodes based on the splitting ratio configuration in the previous interval, according to the newly measured traffic demand and the network load for dynamic load balancing. An efficient algorithm for adaptive adjustment of traffic splitting ratio at individual PoP source nodes.

ATC Parameters:
- $t(u,v)$ – traffic between PoP node u and v.
- $\emptyset u,v(r)$ – traffic splitting ratio of $t(u,v)$ at u on routing topology r, $0.0 \leq \emptyset u,v(r) \leq 1.0$.

These parameters are used in the ATC algorithm.
The algorithm consists of the below steps. We define an iteration counter x which is set to zero initially.

Step-1: Identify the most utilized link l_{max} in the network. This can be used for updated in the traffic engineering information base.
Step-2: For the set of PoP S-D pairs traffic flows that are routed through l_{max} in *at least one but not all* the routing topologies (Full Degree of Involvement is equal to zero) consider each at a time and compute its new traffic splitting ratio among the routing topologies until the first feasible one is identified. A feasible traffic flow means that, with the new splitting ratios, the utilization of l_{max} can be reduced without introducing new hot spots with utilization higher than the original value.
Step-3: If such a feasible traffic flow is found, accept the corresponding new splitting ratio adjustment. Increment the counter k by one and go to Step-1 if the maximum X iterations have not been reached (i.e. $x \leq X$). If no feasible traffic flow exists or $x = X$, the algorithm stops and final result values for the computed traffic splitting ratios.

V. ADMISSION CONTROL ALGORITHM

In order for the Bandwidth Broker to decide whether an incoming resource reservation request will be accepted or not it has to perform some sort of admission control. This function can be performed using straightforward algorithms or using more sophisticated architectures [16]. Our admission control algorithm is the set of criteria controlling whether to admit a new flow; these are based on an approximate model of traffic flows and use measured

quantities as inputs [17]. In proposed system using admission control algorithm at border gateway protocol. Here admission control algorithm mainly used for to seek the less traffic path. After found the less traffic flow, but if there is no path, then ADC immediately inform to virtual routing topologies. Suddenly if possible means it's creates own path.
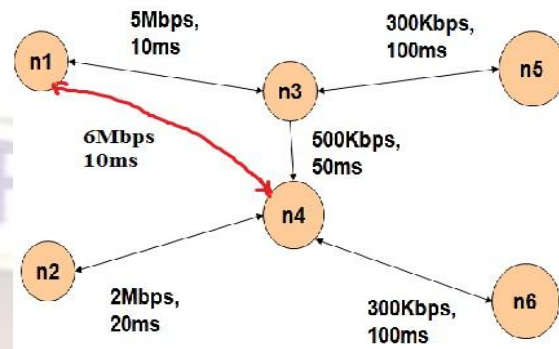

Fig 3: Creates new path with help of ADC

In figure 3, packets send from node 1 to node 2 (system). Its have various path between node 1 and node 2. But the paths all are high traffic may be packets will send delay or packets will loss rather than virtual routing topologies creates new path between 1 and 2 (mentioned in red color line) because high bandwidth with low traffic, its identified with help of admission control algorithm.

Admission control algorithm performs the following steps

The Admission Control Algorithm steps:

New Predictive Flow.

If an incoming flow α requests service at predictive class k, the admission control algorithm:
Step1: Denies the request if the sum of the flows requested r_k^α rate and current usage would exceed the targeted link utilization level:

$$v\mu > r_k^\alpha + \widehat{\nu}_G + \sum_{i=1}^{N} \widehat{\nu}_i,$$

Step2: Denies the request if admitting the new flow could violate the delay bound, D_k, of the same priority level:

$$D_k > \widehat{D}_k + \frac{b_k^\alpha}{\mu - \widehat{\nu}_G - \sum_{i=1}^{k-1} \widehat{\nu}_i},$$

or could cause violation of lower priority classes'delay bound D_j.

$$D_j > \hat{D}_j \frac{\mu - \hat{v}_G - \sum_{i=1}^{j-1} \hat{v}_i}{\mu - \hat{v}_G - \sum_{i=1}^{j-1} \hat{v}_i - r_k^\alpha} + \frac{b_k^\alpha}{\mu - \hat{v}_G - \sum_{i=1}^{j-1} \hat{v}_i - r_k^\alpha}, \quad k < j \le K (7)$$

New Guaranteed Flow

If an incoming flow α requests guaranteed service, the admission control algorithm:

Step 1: Denies the request if either the bandwidth check in Equation fails or if the reserved bandwidth of all guaranteed flows exceeds the targeted link utilization level:

$$v\mu > r_G^\alpha + v_G.$$

Step 2: Denies the request if the delay bounds of predictive classes can be violated when the bandwidth available for predictive service is decreased by the new request:

$$D_j > \hat{D}_j \frac{\mu - \hat{v}_G - \sum_{i=1}^{j-1} \hat{v}_i}{\mu - \hat{v}_G - \sum_{i=1}^{j-1} \hat{v}_i - r_G^\alpha}, \quad 1 \le j \le l$$

If the request satisfies all of these inequalities, the new flow is admitted.

Effect of a new predictive flow on traffic

When a new flow α is added at the same priority level

$$D_k^{*'} = \frac{\sum_{i=1}^{k-1} b_i}{\mu - v_G - \sum_{i=1}^{k-1} v_i} + \frac{b_k + b_k^\alpha}{\mu - v_G - \sum_{i=1}^{k-1} v_i}$$

$$= D_k^* + \frac{b_k^\alpha}{\mu - v_G - \sum_{i=1}^{k-1} v_i}. \quad (2$$

When a new flow α is added at a lower priority level:

$$D_j^{*'} = \frac{\sum_{i=1}^{k-1} b_i + b_k + b_k^\alpha + \sum_{i=k+1}^{j} b_i}{\mu - v_G - \sum_{i=1}^{k-1} v_i - v_k - r_k^\alpha - \sum_{i=k+1}^{j-1} v_i}$$

$$= D_j^* \frac{\mu - v_G - \sum_{i=1}^{j-1} v_i}{\mu - v_G - \sum_{i=1}^{j-1} v_i - r_k^\alpha} + \frac{b_k^\alpha}{\mu - v_G - \sum_{i=1}^{j-1} v_i - r_k^\alpha}, \quad k < j \le K (3)$$

Effect of new guaranteed flow on predictive traffic:

$$D_j^{*'} = \frac{\sum_{i=1}^{j} b_i}{\mu - v_G - \sum_{i=1}^{j-1} v_i - r_G^\alpha}$$

$$= D_j^* \frac{\mu - v_G - \sum_{i=1}^{j-1} v_i}{\mu - v_G - \sum_{i=1}^{j-1} v_i - r_G^\alpha}, \quad 1 \le j \le l (4)$$

In this paper, An adaptive MT-BGP traffic engineering based on virtual routing topologies. *AMPLE* includes three distinct tasks, namely (1) offline network dimensioning through link weight optimization for achieving maximum inter-domain path diversity across multiple MT-BGP routing topologies; and (2) adaptive traffic splitting ratio adjustment across these routing topologies for achieving dynamic load balancing in case of unexpected traffic dynamics. (3) Admission control algorithm used in proposed system. Virtual routing topologies creates new path with help of ADC algorithm. These objectives are low delay, no packet loss and high throughput. *AMPLE* (Adaptive Multi-toPoLogy traffic Engineering a current BGP), TE approach that is capable of adaptively handling traffic dynamics in operational IP networks. Instead of re-assigning BGP link weights in response to traffic fluctuations, we adopt multi-topology BGPs (MT-BGPs) *AMPLE* system based on virtualized BGP routing topologies for dynamic traffic engineering.

VI. CONCLUSION

In this paper we presented an adaptive MT-BGP traffic engineering based on virtual routing topologies. TE system based on virtualized BGP routing that enables short timescale traffic control against unexpected traffic dynamics using multi-topology BGP based networks. The framework contains three major components, namely Offline Link Weight Optimization (OLWO), Adaptive Traffic Control (ATC) and admission control Algorithm. Admission control algorithm achieved low delay and high throughput Instead of frequently changing BGP link weights then create own path based on virtual routing topologies, we use multi-topology BGP routing protocols that allow adaptively splitting traffic across multiple routing topologies.

REFERENCES

[1]   S. Murphy, *"BGP Security Vulnerabilities analysis", IETF draft, 2002.*
[2]   N. Feamster, J. Winick, and J. Rexford, ."*A model of BGP routing for network*

engineering",. In Proc. ACM SIGMETRICS, June 2004.

[3]   Amit Narayanan   *"A Survey on BGP Issues and Solutions "*.

[4]   J. W. Stewart, *"BGP4: Inter-Domain Routing in the Internet, the Addison-Wesley Networking Basics Series"*.

[5]   Ning wang, Kin hon ho, George pavlou, and Michael howarth, university of surrey *"An overview of routing optimization for internet traffic engineering"*.

[6]   Cisco Systems, *BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS-VPN, 2005.*

[7]   Ning Wang, Kin Hon Ho, George Pavlou, *AMPLE: "An Adaptive Traffic Engineering System Based on Virtual Routing Topologies".   IEEE communications Magazine March 2012*.

[8]   N. Wang, K-H. Ho and G. Pavlou, *"Adaptive Multi-topology IGP Based Traffic Engineering with Near-Optimal Performance ", Proc. IFIP Networking 2008.*

[9]   A. Sridharan, R. Guerin, C. Diot, *"Achieving Near-Optimal Traffic Engineering Solutions for   Current OSPF/IS-IS Networks"*, in: IEEE INFOCOM 2003, San Francisco, CA, 2003.

[10] Bernard Fortz, Mikkel Thorup. *"Internet Traffic Engineering by Optimizing OSPF Weights."* In: Proc. IEEE INFOCOM (2000).

[11] B. Fortz and M. Thorup, *"Optimizing OSPF/IS-IS Weights in a Changing World"*, IEEE Journal on Selected Areas in Communications (JSAC), Vol. 20, No. 4, May 2002, pp. 756-767.

[12] Helena Sandstrom, Ulf Bodin, Olov Schelen *"Adaptive Threshold-Based Admission Control"*, 2005

[13] sugih Jamin, Scott Shenker, Lixia zhang, and David D. Clark " *An admission control algorithm for predictive real-time service*.

[14] T.D. Lagkas, G.I. Papadimitriou*, A.S. Pomportsis *"QAP: A QoS supportive adaptive polling protocol for wireless LANs"* Computer Communications 29 (2006) 618–633

[15] Yuxia Lin, Vincent W.S. Wong, *"An admission control algorithm for multi-hop 802.11e-based   WLANs"*. Computer Communications 31 (2008) 3510–3520

[16] Ch. Bouras K. Stamos *"Evaluating Admission Control Modules for Bandwidth Brokers in DiffServ Networks Using ns-2".*

[17] Sugih Jamin, Peter B. Danzig, Scott J. Shenker, and Lixia Zhang "*A Measurement-based Admission Control Algorithm for Integrated   Services   Packet   Networks (Extended Version)"*, 1997.