

On the efficiency of BGP-TE extensions for GMPLS multi-domain routing

Fagertun, Anna Manolova; Ruepp, Sarah Renée; Buron, Jakob Due; Dittmann, Lars

Published in:

Proceedings of the 13th Conference on Optical Network Design and Modelling

Publication date:

2009

Document Version

Publisher's PDF, also known as Version of record

[Link back to DTU Orbit](#)

Citation (APA):

Manolova, A. V., Ruepp, S. R., Buron, J. D., & Dittmann, L. (2009). On the efficiency of BGP-TE extensions for GMPLS multi-domain routing. In Proceedings of the 13th Conference on Optical Network Design and Modelling: ONDM 2009 (pp. 1-6). IEEE.

DTU Library

Technical Information Center of Denmark

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

On the Efficiency of BGP-TE Extensions for GMPLS Multi-Domain Routing

Anna Manolova, Sarah Ruepp, Jakob Buron, and Lars Dittmann

E-mail: {avm, sr, jbu, ld}@com.dtu.dk

DTU Fotonik Technical University of Denmark

Ørstedes Pl., 2800 Kgs. Lyngby, Denmark

Abstract—This paper evaluates the efficiency of set of modifications to the Border Gateway Protocol (BGP) which aim at providing flexible Traffic Engineering (TE) across multiple GMPLS domains. A short overview and analysis of existing proposals for BGP-TE extensions is presented. Based on that, three modifications are proposed for support of multi-domain TE: an end-to-end path-specific TE_attribute, a Border_node_attribute and a behavioral modification of the protocol. Via analysis and extensive simulations we show that the proposed enhancements successfully improve the most significant BGP drawbacks and the Label Switched Path (LSP) blocking probability in dynamic multi-domain GMPLS environments.

Index Terms—GMPLS, BGP, multi-domain routing, TE.

I. INTRODUCTION

OPTICAL networks have traditionally been configured in a static manner, where each network operator has manually setup connections within its own domain. However, the need for dynamic services poses severe scalability problems to this static approach, especially if the services must be provisioned across multiple domains. Generalized Multi-Protocol Label Switching (GMPLS) [1] is emerging as a promising framework to dynamically control optical networks. While dynamic LSP setup within a single domain is applied already today, operators still use manual route configuration [2] or centralized path computation per domain [3] for providing LSPs across multiple GMPLS domains. In addition to providing simple end-to-end connections, operators would also like to apply TE and Quality of Service (QoS) metrics to their LSPs, even if they span across multiple domains.

In the global Internet, multi-domain routing is traditionally provided by the BGP protocol [4], and several proposals exist for extending BGP for multi-domain QoS provisioning. However, the requirements for routing in GMPLS multi-domain networks are fundamentally different from those in the global Internet [5]. Providing TE requires additional topological and/or state information. Whereas this poses no security threats in an intra-carrier environment, the case of inter-carrier TE is more complicated. In particular, the passing of TE information across domain boundaries must not violate the strong confidentiality constraints and policies which typically are enforced between carriers.

Several approaches for routing in multi-domain optical networks exist: Path Computation Element (PCE) architecture [6], External - Network-to-Network Interface (E-NNI) specification [7], and Optical Border Gateway Protocol (OBGP) [8].

They all focus on computing the best possible path towards a destination by supporting TE functionalities at the same time. The PCE architecture is designed for multi-domain GMPLS networks, but it lacks reachability dissemination function and is based on a centralized approach within the domains. The E-NNI solution is specified only for intra-carrier routing and relies on a hierarchical routing scheme, whereas the OBGP is applicable only in optical wavelength switched networks and is not compliant with the GMPLS signalling mechanisms.

An alternative for multi-domain routing in GMPLS networks is to use the BGP protocol, modified for operation in such networks. In this paper we focus on the efficiency of TE extensions of the BGP protocol for multi-domain GMPLS environments. In particular, we focus on reducing the LSP blocking probability in a dynamic multi-domain optical network.

The remainder of this paper is organized as follows: Sec. II gives an overview of existing BGP extensions for multi-domain QoS provisioning and traffic engineering. Sec. III details our proposed BGP modifications; in particular it positions BGP within the GMPLS framework, and specifies the details of our proposal. Sec. IV presents the simulation study and the corresponding results. Conclusions are given in Sec. V.

II. EXISTING BGP EXTENSIONS FOR MULTI-DOMAIN TE

The existing proposals for BGP TE extensions can be roughly divided in two main groups, depending on the application of the modified BGP. The first group of modifications comes from the Internet community and are directed towards enhancing the BGP protocol for QoS support in the context of the existing global Internet. The second group of proposals comes from the GMPLS community which seek enhancement of the protocol for explicit support within the GMPLS architecture. These two groups have different focus and thus, the suggested TE (or QoS) extensions differ.

Among the first group, are the extensions proposed in [9]–[12], related to the global Internet. The authors of [9] focus on a simple extension for support of diverse path dissemination for load balancing, support of fast convergence and limiting route flapping. The QoS enhancements of BGP suggested in [10] on the other hand focus on explicitly supporting the process of QoS delivery across domain boundaries. The suggested *QoS_NLRI* attribute is used as a primary path

selection criterion, and in order to cope with the one-path-per-destination problem the method proposed in [9] is adopted. The scheme is designed for supporting QoS for IP-based services and is intended to be used in the global Internet, i.e. backward compatibility and graceful migration are of primal importance. The authors of [11] propose an alternative QoS metric which is an abstracted probability interval, providing increased flexibility in dynamic networks and decreased signaling overhead. The authors of [12] bring this idea one step further by introducing a multi-metrical QoS extension using standard QoS metrics.

All cited references focus on extending the BGP with the intention to apply it in the global Internet. This poses serious scalability considerations and none of the suggestions reached a standardization state, showing that applying QoS provisioning on a global scale, involving multiple domains, is far more complicated, than first considered.

Among the second group of suggestions are the works of [13] and [14], focusing on modifying the BGP protocol in the context of the GMPLS framework. The authors of [13] suggest a GMPLS-compliant TE extension with limited application - only for reachability dissemination for Layer 1 Virtual Private Networks. The authors of [14] propose a framework for mapping the specific GMPLS needs into the BGP protocol semantic. Their proposal facilitates the proper interaction between provider networks and between clients and providers. Nevertheless, they do not propose specific extended TE attributes.

Despite the efforts put in the direction of extending BGP for TE support, neither of the proposals gained popularity. It is currently believed that for the case of providing multi-domain QoS in the global Internet a general revision of the BGP protocol is needed. In the case of applicability within the GMPLS framework on the other hand, an alternative solution is being designed - the PCE architecture. Nevertheless, BGP is still considered a viable solution for the GMPLS multi-domain routing due to its widespread applicability today, its maturity and its strong policy-enforcing features.

III. BGP MODIFICATIONS FOR GMPLS MULTI-DOMAIN NETWORKING

In this paper we evaluate the efficiency of BGP-TE extensions under the GMPLS framework. The focus is on facilitating TE (and QoS) provisioning within a group of domains (providers) willing to cooperate, not in the global Internet. We focus on failure-free scenario where protocol re-convergence is caused only during TE information update, which is done by re-advertising the paths with the updated TE metric. First we outline the underlying motivation for modifying the BGP protocol. Then, we provide a general framework of two extended attributes and a behavioral modification of the protocol. At the end, we justify our design choices and illustrate the efficiency of our proposals by simulations.

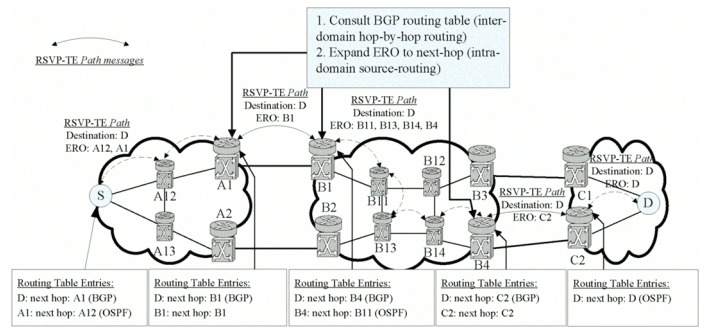


Fig. 1. Connection provisioning under the combined inter-domain BGP hop-by-hop routing and intra-domain OSPF-TE source routing.

A. BGP within the GMPLS framework

GMPLS networks provide QoS to users and support TE for providers based on explicit resource reservations and flexible traffic control mechanisms. This implies that source routing is a fundamental part of the framework. Source routing within a domain is supported by OSPF-TE [15], which provides the needed path towards a destination, but for multi-domain routing this is not possible due to security and privacy considerations between domains, meaning that no topological and/or state information is allowed to be disseminated beyond domain boundaries [16]. This creates the biggest challenge for BGP. BGP supports a hop-by-hop routing paradigm and is a path-vector protocol, whereas GMPLS needs source routing and typically employs a link-state routing protocol. Nevertheless, it is possible to use BGP for GMPLS multi-domain routing. Combining the hop-by-hop BGP routing with the OSPF-TE source routing for multi-domain GMPLS provisioning can be seen on Fig. 1. The *Path* message of the RSVP-TE [17] protocol, used to signal the connection, specifies an Explicit Route Object (ERO) which is incomplete - it is specified only up to the egress router from the own domain. This egress router is provided by the BGP next_hop attribute. Within a domain, each ingress router consults its routing table to identify the next_hop to the destination and expands the ERO object using the OSPF-TE intra-domain routing. Another option is specifying a loose hop ERO of AS identifiers (again, provided by the BGP AS_path attribute).

B. Motivation for BGP modifications

As it was shown, BGP can be used within the GMPLS framework, but it suffers several drawbacks, caused by the underlying design considerations of the protocol, which make it an unattractive solution.

The first drawback of BGP is the lack of adequate TE (or QoS) information dissemination. As outlined in Sec. II, several options for TE enhancements are available, but the proposals within the GMPLS framework seem incomplete. Thus, new suggestions applicable in general mesh GMPLS networks are needed. The second problem with BGP, which is encountered in the global Internet, is the slow protocol convergence, caused by path exploration and chattiness among the BGP routers. A direct implication for GMPLS networks is a worsened

survivability. The third drawback can be seen in the one-path-per-destination policy of the protocol. BGP supports the Internet's best-effort routing paradigm and disseminates only one path towards each destination - the best path. This makes the protocol very scalable but hinders diverse path computation needed for survivability in GMPLS networks. Ensuring link-disjoint paths in multi-domain case is very complex. This problem can be approached (but not completely solved) by providing AS-disjoint paths to a destination - a feature BGP cannot support. In this case, only the link-disjointness in the destination and the source domains remains to be solved. The last challenge for BGP can be found in the path dependency phenomenon. BGP speakers advertise only this route which they use for traffic forwarding as well. This results in overloading multi-domain links and low utilization of available resources if there are multiple links between domains.

Summarizing the drawbacks of the BGP protocol it can be seen that the traditional BGP implementation hinders TE (both with respect to LSP provisioning and to survivability support), it lacks flexibility and is inadequate in highly dynamic multi-domain environments where the LSP requests arrive randomly and the connection duration is generally unknown. Despite the outlined problems though, it still holds one very strong advantage which makes it attractive: policy enforcing. When inter-carrier scenarios are considered this feature is fundamental.

C. BGP enhancements for multi-domain GMPLS TE

As noted, the existing proposals for BGP extensions within the GMPLS framework are inadequate for meeting the outlined BGP drawbacks. Thus, we suggest to utilize some of the concepts proposed for QoS-enhanced BGP in the global Internet for GMPLS networks. In particular, we adopt the idea of disseminating path-related (not domain-related) QoS metric per destination within an extended *TE_attribute*. This might seem to harm the scalability of the protocol but as we focus on applying the BGP for TE support within a group of GMPLS domains not in the whole Internet, this is not a concern. The proposed path-related *TE_attribute* is representative for the overall path from a certain node to the destination. Since this metric is accumulative, no domain-specific information leaks out of the domain. Several different TE-related metrics can be disseminated such as wavelength availability, delay, SLRG, physical impairments. This can be used for multi-constraint path computation and for survivability support. The proposed format of the extension is a Type-Length-Value (TLV) format, where each *TE_attribute* carries a group of TLV fields, specifying the value of the corresponding TE metric.

Unlike the existing proposals for QoS-enhanced BGP [10], [11], we do not consider the disseminated QoS metric as a first decision step in the path selection process under the BGP operation, due to implications posed by the standard BGP operation, which are illustrated in the Results section (Sec. IV). Instead, we suggest an alternative BGP operation, motivated and detailed below.

Adopting a per-path QoS metric solves only one of the outlined BGP problems - the lack of TE information dis-

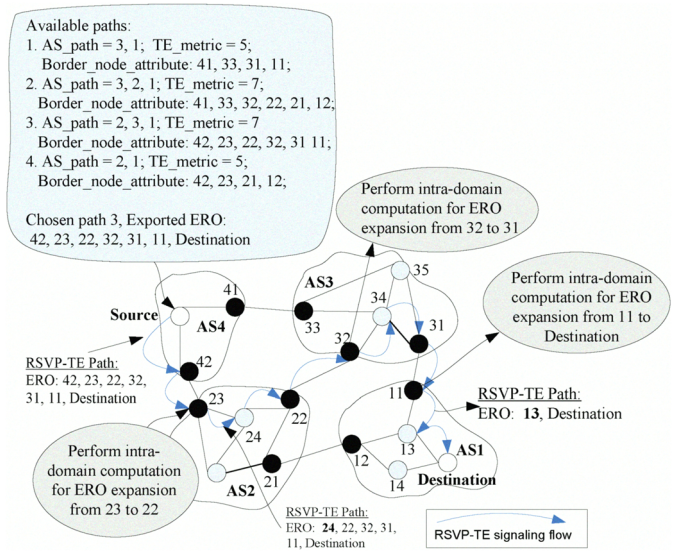


Fig. 2. LSP establishment under the proposed modified BGP operation. Source node chooses among all available paths based on TE metric. Loose ERO provided by the *Border_node_attribute*.

semination. In fact, disseminating QoS metric only supports QoS provisioning but not Traffic Engineering as such. Within the BGP scope neither diverse path selection for survivability support is possible, nor dynamic rearrangement of existing connections. Even load balancing is performed on a local basis using careful configuration of local preferences and policies. This is mainly due to the one-path-per-destination policy and the hop-by-hop nature of the protocol. In order to provide multiple paths per destination and to map the hop-by-hop BGP into the source-routing requirements of GMPLS we propose two additional modifications: a *Border_node_attribute* and a behavioral modification of the protocol. The behavioral modification consists of using the BGP only as a dissemination protocol, not as a path selection one. In this way, every BGP speaker has multiple paths per destination and each head-end router has the option of choosing independently among the available paths. This solves the path dependency problem and the lack of path diversity. In order for this modification to be effective, we also need to introduce the *Border_node_attribute* which logs the identifiers of all border nodes along a path. This attribute uniquely identifies each path and gives the head-end router bigger control over the end-to-end connection. An illustrative example of the proposed enhancements is shown on Fig. 2, where the hop-by-hop BGP routing is substituted by a loose explicit route routing. The *Border_node_attribute* is fed into the RSVP-TE ERO object and used as loose hop routing for the request. Head-end routers in AS 2 and AS 3 can choose independent paths to the destination node, not following the segments of the shown one.

Disseminating all possible paths to a destination can harm the scalability of the routing protocol even if only few GMPLS domains participate. In order to avoid this, we suggest the application of certain export policies which make intelligent

decision regarding which paths to be disseminated further. In particular, we focus on two main observations: longer paths with the needed TE metric can increase the connection blocking probability due to unnecessary high usage of resources; and for survivability support (or load balancing) one needs at least two disjoint paths. The second aspect we focus on becomes a real challenge due to the lack of coordination between the border routers and if only two disjoint paths are disseminated further, a node may end up with receiving non-disjoint paths from two independent neighbors. Taking this into account, we suggest that long paths are only accepted if they provide strict AS-disjointness.

The described modifications also avoid the path exploration during TE information update. In fact, after all policy-compliant paths have been disseminated, only their TE state is updated (either periodically or at certain triggering events). This considerably reduces the signaling overhead during re-convergence of the protocol.

Under the proposed BGP enhancements the routing is split into two levels: an inter-domain level, specifying a border-node path provided by BGP, and an intra-domain level, specifying the full path between neighboring border nodes by employing traditional OSPF-TE routing. This operational mode is closer to the traditional source routing operation employed in intra-domain GMPLS networks, where head-end routers have full control over the overall path. In our case, the head end router has increased control over the end-to-end path, compared to the traditional hop-by-hop BGP operation, but still preserves the individual domains' right to control the traffic within their own borders.

IV. SIMULATION RESULTS

This section presents the results obtained from simulating the proposed BGP modifications in the event-driven simulator OPNET Modeler [18]. The used network topology consists of 8 transparent Wavelength Division Multiplexed (WDM) domains interconnected in a general mesh. Traffic is uniformly distributed between 56 source-destination pairs. There are 20 bidirectional multi-domain links and 20 wavelengths per link. Wavelength continuity is assumed. At the time of connection setup, performed via the RSVP-TE protocol, the wavelength is chosen randomly among all available at the destination node. The connection duration is exponentially distributed number with mean value 2 hours. Only uni-directional connections are assumed. Traffic load is calculated per source node and is normalized to the link capacity (see eq. 1).

$$\text{Normalized Load} = \frac{\text{Mean Connection Duration}}{\text{Mean Interarrival Time} * W} \quad (1)$$

where W is the amount of wavelengths per link. Since in our used topology all source nodes have 2 outgoing links, the Load per node cannot exceed 2 Erlang. The simulations' duration is 30 days. The considered TE metric is Wavelength Availability (WA), which is a bottleneck type of metric and is calculated according to $WA_{path_i} = \min\{WA_{rec}, WA_l : l \in L\}$, where WA_{rec} is the received metric and L is the set of links

along the segment between the current node and the indicated next_hop. Within each domain, local TE is performed per request by choosing the best possible path at the time of the request. When our proposed modifications are used, the path with the best TE metric is chosen at the time of the connection request in between all available paths to the destination.

The performance of the following different schemes for conveying TE information between domains is investigated:

- *BGP-TE case 1* - employs end-to-end TE metric used as a first decision criterion [10] in the BGP path selection process¹;
- *BGP-TE case 2* - employs end-to-end TE metric used as a first tie-breaking criterion in the BGP path selection process (see footnote 1 for clarification);
- *BGP-TE case 3* - employs local TE by using the Multi-Exit-Discriminator between domains with the "Always Compare" policy [4];
- *Enhanced BGP* - employs our suggested modifications, i.e. an end-to-end TE metric together with the *Border_node_attribute* and the behavioral modification of the protocol.

A. Blocking probability

Fig. 3 presents the results for the blocking probability versus the Normalized Load in the network for all tested schemes. A remarkable result is that using the TE metric as a primary path selection (*BGP-TE case 1*) yields the worst result. The reason is that when the TE state of a path is updated (the update direction is from the destination to all sources) all BGP speakers choose the best possible current path which contains the unutilized multi-domain links. Thus, most of the domains converge towards using the same multi-domain links (links, which have not been used before the last TE information update). This causes congestion on these links and increased blocking probability.

We consider the main reason for the result from Fig. 3 to be the path dependency problem inherent to the normal BGP operation and the greediness of the applied TE method. Since the TE metric is of primal importance in GMPLS networks, this motivated us to design our solution as described in Sec. III, where the TE metric is used as the only path selection criteria. As it can be seen, our proposal (*Enhanced BGP*) provides significantly lower blocking probability compared to all other tested cases. This is due to the fact that the head-end routers have higher control over which path is used and can intelligently balance the traffic by using multiple paths.

Another interesting result is that the difference between *BGP-TE case 2* and *BGP-TE case 3* is minimal. This is likely due to the fact that in the used topology most of the connections do not traverse more than 3 domains in total. Thus the advantage of having an end-to-end TE metric per path compared to having knowledge of only the TE metric of the neighboring domain, as in *BGP-TE case 3* [4], is reduced.

¹The BGP path selection process consists of comparing the path attributes of the candidate paths in a certain order [4].

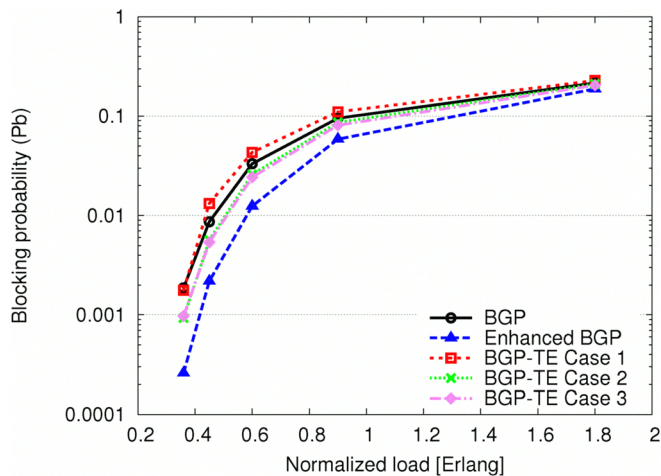


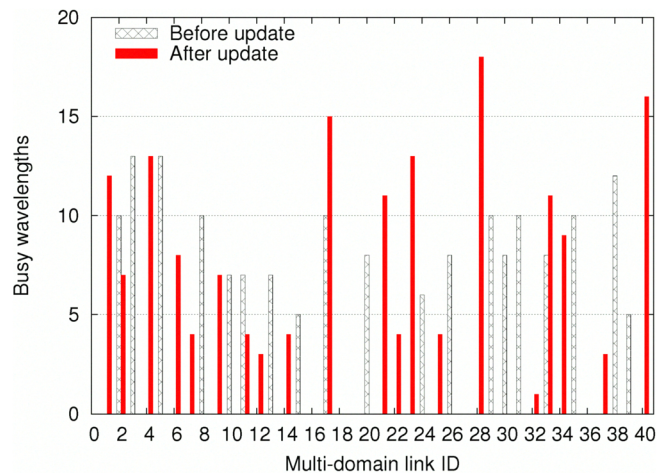
Fig. 3. Blocking probability vs. Normalized load. "BGP" indicates standard BGP without any TE information dissemination.

B. Path dependency and multi-domain link utilization

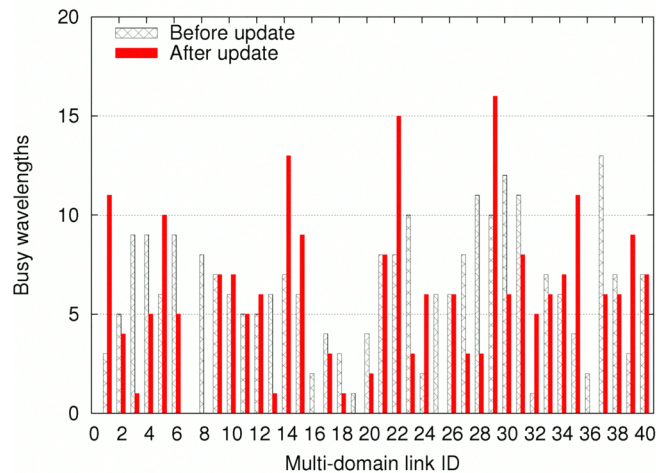
In order to illustrate how our proposal copes with the outlined problems inherent to the traditional BGP protocol (see Sec. III-B) we investigate the multi-domain link usage before and after re-convergence of the protocol (updating the TE state of the paths) for two of the mechanisms - *BGP-TE case 1* and *Enhanced BGP*. The goal is to illustrate the main reasons for the bad performance of the *BGP-TE case 1* scheme and to show how *Enhanced BGP* introduces improvement. For the used setup the achieved blocking probabilities for the schemes are 0.048 for *BGP-TE case 1* and 0.014 for *Enhanced BGP*. Fig. 4 presents snapshots of the multi-domain link usage before and after updating the TE state of the paths for the considered schemes. As it can be seen, most of the inter-domain links are not used before or after re-convergence under the *BGP-TE case 1* scheme (Fig. 4(a)). This is due to the one-path-per-destination policy and the path dependency inherent to the operation of the standard BGP protocol. Furthermore, it can be seen how most of the traffic is merely shifted from one set of links to another - only 4 out of 40 links are used both before and after the re-convergence. This also illustrates the poor utilization of the multi-domain link resources. The *Enhanced BGP* scheme on the other hand (Fig. 4(b)) achieves efficient resource utilization and load balancing - only one multi-domain link is not used at all, and five are not used after updating the TE state of the paths. Moreover, most of the links are relatively evenly loaded. This is due to the fact that the *Enhanced BGP* scheme provides multiple paths per destination and the path dependency is eliminated, which allows for better utilization of the multi-domain resources.

C. TE information update

Here we evaluate the impact of the Updating Interval (UI) of the TE information on the connection blocking probability since the efficiency of using TE for path selection depends on it. Fig. 5 illustrates the improvement in blocking proba-



(a) BGP-TE case 1



(b) Enhanced BGP

Fig. 4. Multi-domain link usage before and after updating the TE state of the paths for *BGP-TE case 1* and *Enhanced BGP* schemes.

bility achieved by increasing the update frequency for *BGP-TE case 1*, *BGP-TE case 2* and the *Enhanced BGP* schemes.

An interesting result is that the smaller UI for the *BGP-TE case 1* yields the worst result. Furthermore, the difference between the achieved blocking probabilities for that scheme is negligible. Both *BGP-TE case 2* and *Enhanced BGP* schemes behave as expected - the smaller the period between updates the lower the blocking probability. The reason for the bad results achieved by *BGP-TE case 1* is that the difference between the used UIs is negligible. Further investigation revealed that *BGP-TE case 1* has better performance only when the UI is comparable to the connection duration. In this case the source node practically performs load balancing by using different paths, provided by the re-converged BGP protocol, more often. A drawback in this case is the required Update overhead which is considerably higher. Fig. 6 compares the best performing results we have achieved for the *BGP-TE case 1* scheme (UI = 7200 sec.) and the *BGP-TE case 2* scheme (UI = 100 000 sec.), and the result for

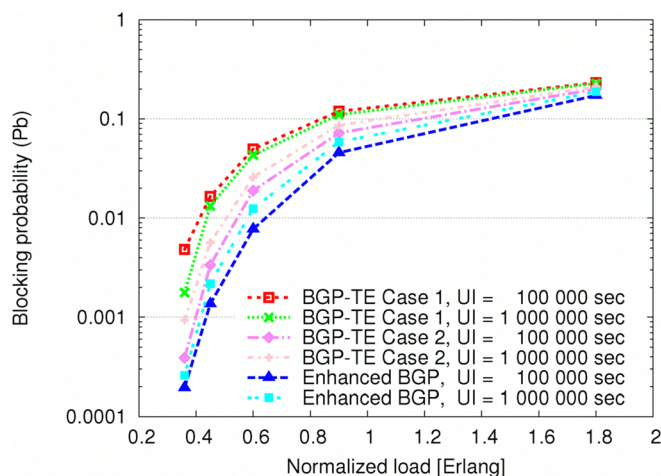


Fig. 5. Blocking probability vs. Normalized load for different UIs.

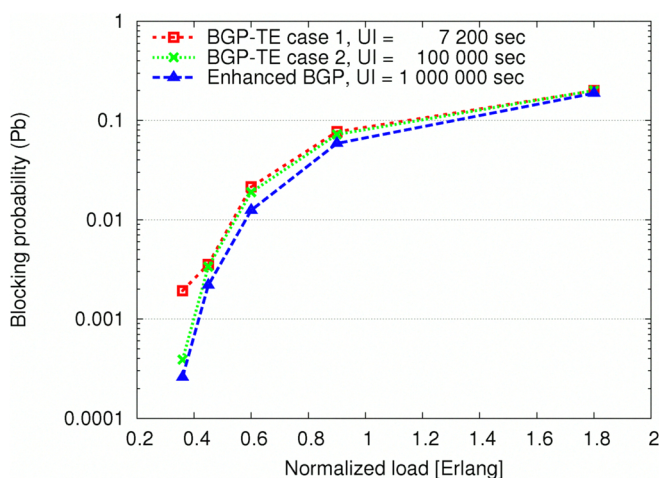


Fig. 6. Performance comparison for three different UI.

the *Enhanced BGP* with the longest UI (1 000 000 sec.). The comparison shows that our suggestion outperforms the other schemes in terms of blocking probability even with using the longest tested UI. For the specific test case the *Enhanced BGP* scheme performs between 8% (for high loads) and 35% (for middle loads) better than the *BGP-TE case 2* scenario by using a 10 times longer UI.

V. CONCLUSION

In this paper we investigate the efficiency of different mechanisms for conveying and using TE information via the BGP protocol in GMPLS multi-domain networks. We address the drawbacks of earlier suggestions and the specific requirements for multi-domain TE in GMPLS environments and design a solution for QoS provisioning via BGP protocol extensions. Our proposal has three main aspects which are designed to solve four specific BGP-inherent problems: lack of TE information dissemination, lack of path diversity, path dependency (i.e. low control over the end-to-end path) and slow convergence time. Apart from adopting suggestions for

TE dissemination via the BGP protocol, proposed for the global Internet, we propose to use BGP as a dissemination protocol, not as a path selection one, and introduce a new path attribute - the *Border_node_attribute*.

Via simulations we illustrate the problems some of the earlier suggestions for BGP extensions face when applied in connection-oriented networks. We prove the efficiency of our proposal by illustrating improvement on the connection blocking probability. Furthermore, we investigate the effect of the TE information update interval on the efficiency of several mechanisms and show that our suggestion can achieve the lowest blocking probability by using the least update overhead.

Based on the proposed extensions, the GMPLS multi-domain path selection gets one step closer to the traditional path computation performed in intra-domain GMPLS networks by efficiently integrating a hop-by-hop-based multi-domain routing protocol into a source-routing environment.

ACKNOWLEDGMENT

The work described in this paper was carried out with the support of the BONE-project ("Building the Future Optical Network in Europe"), a Network of Excellence funded by the European Commission through the 7th ICT-Framework Programme.

REFERENCES

- [1] E. Mannie, *Generalized Multi-Protocol Label Switching (GMPLS) Architecture*, RFC 3945, Oct. 2004.
- [2] MUPBED - Multi-Partner European Testbed for Research networkings, <http://www.ist-mupbed.org>
- [3] DRAGON - Dynamic Resource Allocation via GMPLS Optical Networks, <http://dragon.maxgigapop.net>
- [4] Y. Rekhter, *A Border Gateway Protocol 4 (BGP-4)*, RFC 4271, 2006.
- [5] G. Bernstein, B. Rajagopalan, *Optical Inter Domain Routing Considerations*, IETF Draft, draft-bernstein-optical-bgp-01.txt, Exp. May 2001.
- [6] A. Farrel, *A Path Computation Element (PCE) - Based Architecture*, RFC 4655, Aug. 2006.
- [7] The OIF Forum, *External Network-Network Interface (E-NNI) OSPF - based Routing - 1.0 (Intra-Carrier) Implementation Agreement*, Jan. 2007.
- [8] M. Blanchet, F. Parent, B. St-arnaud, *Optical BGP (OBGP): InterAS Lightpath Provisioning*, IETF draft, ietf-draft-parent-obgp-01.txt, 2001.
- [9] D. Bernstein, *Advertisement of Multiple Paths in BGP*, IETF draft, draft-walton-bgp-add-paths-06.txt, Exp. 2009
- [10] G. Cristallo, C. Jacquenet, *Providing Quality of Service Indication by the BGP-4 Protocol: the QoS_NLRI attribute*, IETF draft, draft-jacquenet-qos-nlri-05.txt, Exp. 2003
- [11] L. Xiao, K. Lui, J. Wang, and K. Nahrstedt, *QoS extensions to BGP*, In Proceedings of International Conference on Network Protocols (ICNP) 2002, France, November 2002.
- [12] T. Zhang, Y. Ciu, L. Fu, T. Korkmaz, *Scalable BGP QoS Extension with Multiple Metrics*, In Proceedings of International conference of Networking and Services (ICNS) 2006.
- [13] H. Ould-Brahim, D. Fedyk, *Traffic Engineering Attribute*, IETF draft, draft-fedyk-bgp-te-attribute-03.txt, Exp. March 2009.
- [14] Y. Xu, A. Basu, Y. Xue, *A BGP/GMPLS Solution for Inter-Domain Optical Networking*, IETF draft, draft-xu-bgp-gmpls-02.txt, Exp. Dec. 2002
- [15] K. Kompella, Y. Rekhter, *OSPF Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)*, RFC 4203, Oct. 2005.
- [16] T. Otani, S. Okamoto, *GMPLS Inter-domain Traffic Engineering Requirements*, IETF draft, draft-otani-ccamp-interas-gmpls-te-07.txt, Exp. June 2008.
- [17] L. Berger, *Generalized Multi-Protocol Label Switching (GMPLS) Signaling, Resource Reservation Protocol-Traffic Engineering (RSVP-TE) Extensions*, RFC 3473, Jan. 2003.
- [18] OPNET Modeler, <http://www.opnet.com>