Workgroup: Network Working Group
Internet-Draft: draft-yuchaozhang-i2bgp-01
Published: 3 December 2022
Intended Status: Informational
Expires: 6 June 2023
Authors: Y. Zhang, Ed.
Beijing University of Posts and Telecommunications
P. Cong
Beijing University of Posts and Telecommunications
H. Jiang
Beijing University of Posts and Telecommunications
L. Wang
Beijing University of Posts and Telecommunications
W. Wang
Beijing University of Posts and Telecommunications

Desensitize Intra-domain Information for Inter-domain Routing

Abstract

Border Gateway Protocol (BGP) is a routing protocol for autonomous systems running on TCP. It is currently the only protocol capable of handling multiple connections between unrelated routing domains, such as the size of the Internet. BGP is built on the experience of EGP.

The main function of BGP system is to exchange network access information with other BGP systems. However, it cannot fully utilize the complete information in the domain to achieve the optimal decision. This document proposes I2BGP, which describes how to obtain desensitization information in the domain to optimize routing decisions.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 6 June 2023.

Table of Contents

1. Introduction

Border Gate way Protocol (BGP) early used to solve the problem of the interconnection between a large number of Internet ASs (autonomous systems). Compared with the traditional dual-IP dual-wire technology, it is more efficient. At present, the BGP protocol is widely deployed on the Internet, and there are many important enhancements to improve BGP performance in terms of refifining scheduling granularity, accelerating convergence time, anomalous behavior detection and so on.

However, current BGP-like protocols follow the basic principle of taking hops - the number of Autonomous Systems (AS) on a path - as

the metric for routing: the less hops, the higher the priority of the path, such as [RFC4271]. Such strategy regards all domains as indiscriminate blackbox and thus can not achieve the optimal inter-domain routing decisions due to the lack of intra-domain information.

This document proposes I2BGP which is developed based on BGP-4. It uses a Desensitized Intra-domain information-aware Tactic (DIT) to assist inter-domain routing decisions, which can be embedded in BGP or applied independently as a control-plane strategy. DIT can make use of intra-domain information while protecting data privacy at the same time, thus solving the contradiction between data sharing and privacy protection.

2. Conventions

DIT: The frame that the document proposed, which makes near-optimal inter-domain routing decisions with desensitized intra-domain information.

AS/ASes:Autonomous Systems in the internet.

I2BGP: The improved protocol which is based on BGP and has the ability of extracting intra-domain information to make optimal routing decisions.

DRT: It represents uppercase mathematical symbol of delta.

drt: It represents lower mathematical symbols of delta.

o: The article uses it for the same OR operation, mainly in the formula of encryption and decryption.

o+: The article uses it for the XOR operation, mainly in the formula of encryption and decryption.

RIB: Routing Information Base.

3. Requirements and Use Case Scenario

This section describes some essential requirements for I2GBP and the scenario about the problem hidden in BGP.

3.1. Requirements

3.1.1. Specification of Requirements

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3.1.2. Supporting Information Export

Data within a domain could be exported, mainly referring to the link performance status, e.g., delay, bandwidth, packet loss rate, hops, etc. The performance of an inter-domain transmission is jointly determined by the link performance of all passed domains, then, for different attributes, which can be summarized as bottleneck type (bandwidth) and cumulative type (delay, packet loss rate, hops), the calculation of combination will be different. In this document, I2BGP takes the number of hops as a typical example that ought to be calculated by addition.

3.1.3. Protecting Data Privacy

Private information of domains should not be deduced from the exported information, because information like hops may involve intra-domain topology, which requires that the information cannot be directly disclosed to other ASes.

3.2. Use Case Scenario

BGP cannot use the information in the domain to make routing decisions, which often makes the final routing decision not optimal. Take the forwarding hops as an example, Figure 1 shows two paths between server s and client c: Path A has 4 AS-hops (s -> a1 -> a2 -> a3 -> c) and Path B has 2 AS-hops(s -> b -> c). For client c, Path B will be selected as the actually routing path according the principle of [RFC4271], and Path A will be discarded. But in fact, there are additional hops in each domain, shown as the numbers in Figure 1, which makes path A the real better path.

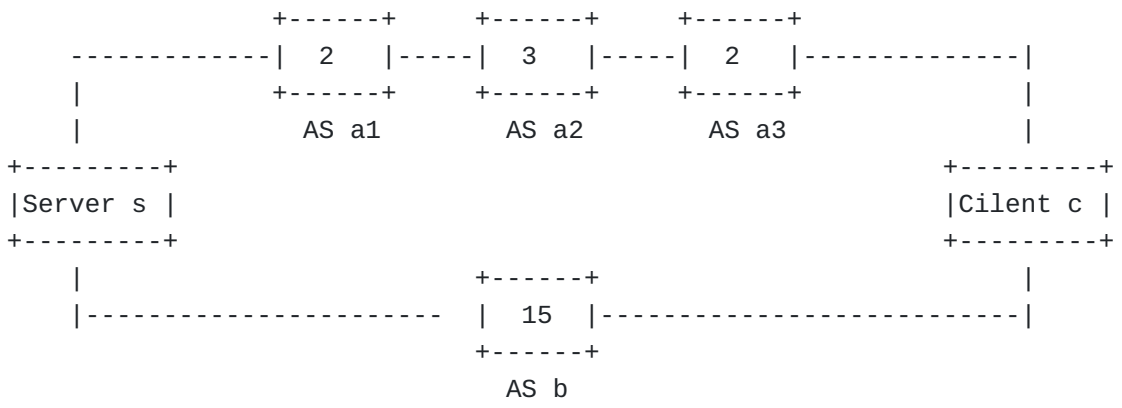


Figure 1: Example of BGP-based inter-domain routing

4. Overview of I2BGP

This section describes the model of I2BGP and how it exports the information from intra-domain without revealing data and finally

makes the route decision. The principles of traditional BGP path selection do not include the consideration of intra-domain performance. This document introduces an additional attribute, Attr, for BGP to accomplish data carrying and spreading.

According to the description of [RFC4271], each domain is a confidential system with complete independence and autonomy. BGP runs at border routers of each domain and specifies the next hop when forwarding across. In order to fetch messages from each domain, I2BGP proposes the DIT technique. It masks the intra-domain topology and abstracts each domain into a characteristic topology graph with its border routers exclusively. Because there are direct and indirect connections among all border routers (nodes) with in the same AS we abstract these connections as edges between nodes.

After taking the information out of the domain, in order to prevent the information in the domain from being leaked, DIT proposes a random obfuscation technology to ensure data security, which can ensure that information in the domain can be obtained while imitating information security issues. Finally, we spread the retrieved information to other domains through the new field Attr, and obtain the optimal route by comparing the final value.

4.1. Homomorphic Encryption

This document introduces homomorphic cryptography to export information without revealing data, and to ensure the validity of the final calculation results. Homomorphic Cryptography provide a potential solution to the contradiction of information exportation and privacy, it is a kind of cryptographic technique that performs arithmetic operations on the encrypted data and yields a result equivalent to the cyphertext result of some computation on the unencrypted original data. Its principle can be explained as follow:

De(En(a) o En(b)) = a o+ b,

where En() is the encryption operation, De() is the decryption operation, o and o+are correspond to the operations on the plaintext and cyphertext domains, respectively. When o+ represents addition, this encryption is an additive homomorphic encryption, and when o+ represents multiplication, this encryption is a multiplicative homomorphic encryption. The encryption function that satisfies both additive homomorphism and multiplicative homomorphism properties is called fully homomorphic encryption, and it alse can perform any times of additive and multiplicative operations

Homomorphic encryption algorithms usually have high computational complexity. I2BGP select a algorithm which encrypt simple numbers and satisfy homomorphic additivity to avoid this problem.

4.2. DIT Overview

In order to achieve the target, this document uses an abstract method to mask the intra-domain topology and reuses the exsiting fields of BGP header.

During the route convergence process, cumulative calculations (e.g., addition, min() or max()) over multiple domains can inherently protect the privacy of all upstream domains data, i.e., mathematically speaking, on the basis of c = a + b, it could not infer the values of a and b when only c is known. This is one of the foundations for the privacy protection in DIT. However, the inherent data privacy protection brought by cumulative calculations is effective only after at least one such operation has already been conducted. In other words, the cumulative calculations can only achieve non-destination domain data protection. For example, as shown in the Figure 2, for AS 3, the value of AS 1 or AS 2 cannot be inferred from the cumulative summation sent from AS 2. However, AS 2 is directly connected to the destination domain of the route (AS 1), the value of AS 1 is directly exposed to AS 2 due to the lack of protection from cumulative calculation. That is, for the destination domain of each route, information leakage risk still exists, which is caused by directly connected neighbor domains, we name it the Direct Connection issue.

To solve Direct Connection issue, we propose a basic method named Random Number Confusion. In the path selection process, it is only necessary to select the optimal path by basic comparisons. Just like giving random offsets to all nodes in the coordinate system will not change the relative positions. Therefore, for target domain, DIT adds a random number to the intra-domain data when initially spreading the data to the adjacent domain. After arriving the traget damain, the intra-domain data will be taken out and will not affect the comparison of the final results.

After fetching the data, to carry the above intra-domain data, we add a new filed, Attr, to the BGP packet header, although which is not strictly required because we can also reuse existing fields, provided the re-definition of the field function is approved. And the quantified value of the destination-based cumulative path performance is embedded into this field and diffused to neighbor domains with the route update message.

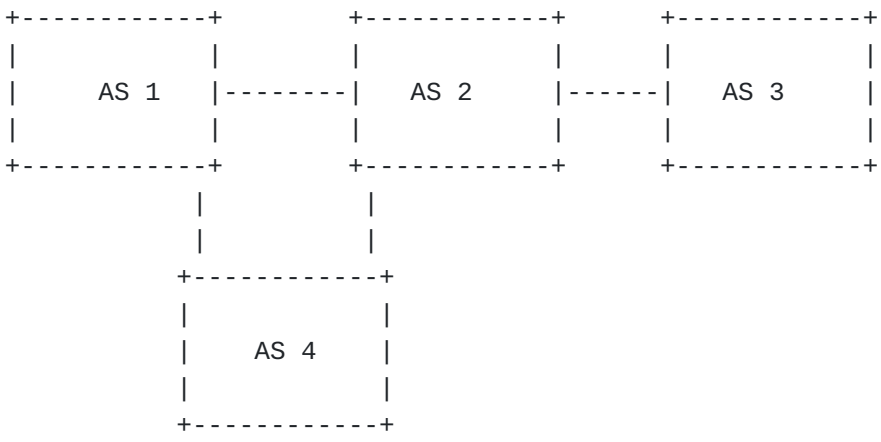
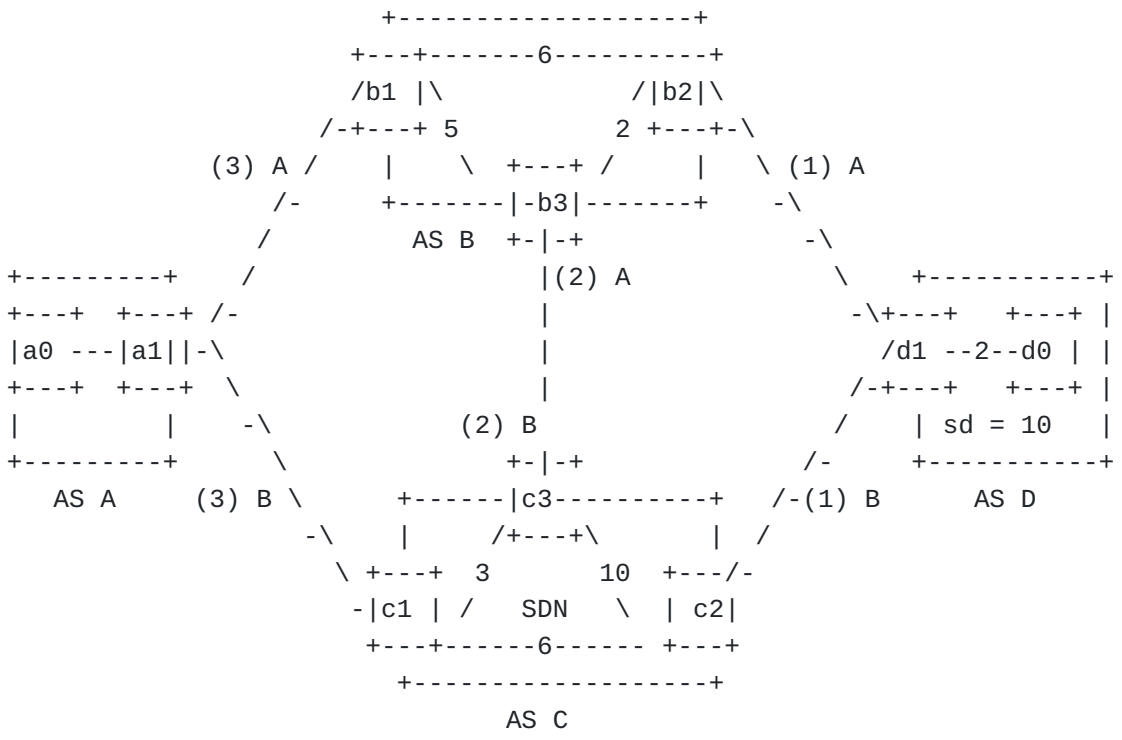


Figure 2: Inter-domain information security scenarios

DIT does not constrain the intra-domain switching policy implemented by each domain. Figure 3 shows a typical process of inter-domain routing message diffusion, AS B runs a traditional routing protocol and AS C uses a central controller similar to an SDN controller. This document takes the number of hops as example. Suppose AS D updates the route of d0, then based on the intra-domain topology information, d1 sends this update message to AS B (b2) and AS C (c2), where the Attr value is 12 = s_d + 2. The router compares the Attr to decide whether to update the local RIB. When the received Attr is smaller than the local, the route entry will be updated, otherwise it will not change. In the intra-domain, AS B or AS C exchange update messages using the intra-domain protocol. AS C (c3) sends this update to AS B (b3), where the Attr value is the number of hops of the optimal path from c3 to c2 (c3 -> c1 -> c2) plus the Attr value received by c2 (21 = 3 + 6 + 12). For AS B (b3), the received Attr is greater than the local, so the local RIB is not updated. Similarly, the Attr sent to AS C is 14 = 2 + 12, which is smaller than local value, then updates the corresponding route entry. AS B (b1) and AS C (c1) send update message to AS A (a1). Then, AS A updates the optimal path for reaching d0 in AS D based on the two messages received from AS B and AS C, in which Attr is 19 and 17, respectively. Take the example from a1 to d0, for a1, it will choose c1 as next hop because the corresponding path has a smaller Attr value.



Update Message						RIB					
(1)A	AS D(d1) -> AS B(b2)					b2	New Attr = Attr:maint				
Des	Next-hop	AS-path	Attr	Des-AS		Des	Next-hop	AS-path	Attr	De	
d0	d1	1	12	D		d0	d1	1	12		
(1)B	AS D(d1) -> AS C(c2)					c2	New Attr = Attr:maint				
Des	Next-hop	AS-path	Attr	Des-AS		Des	Next-hop	AS-path	Attr	De	
d0	d1	1	12	D		d0	d1	1	12		
(2)A	AS B(b3) -> AS C(c3)					c3	New Attr > Attr:updat				
Des	Next-hop	AS-path	Attr	Des-AS		Des	Next-hop	AS-path	Attr	De	
d0	b2	3	14	D		d0	c2->b3	2->3	22->17		
(2)B	AS C(c3) -> AS B(b3)					b3	New Attr > Attr:mainta				
Des	Next-hop	AS-path	Attr	Des-AS		Des	Next-hop	AS-path	Attr	De	
d0	c1	2	21	D		d0	b2	2	14		

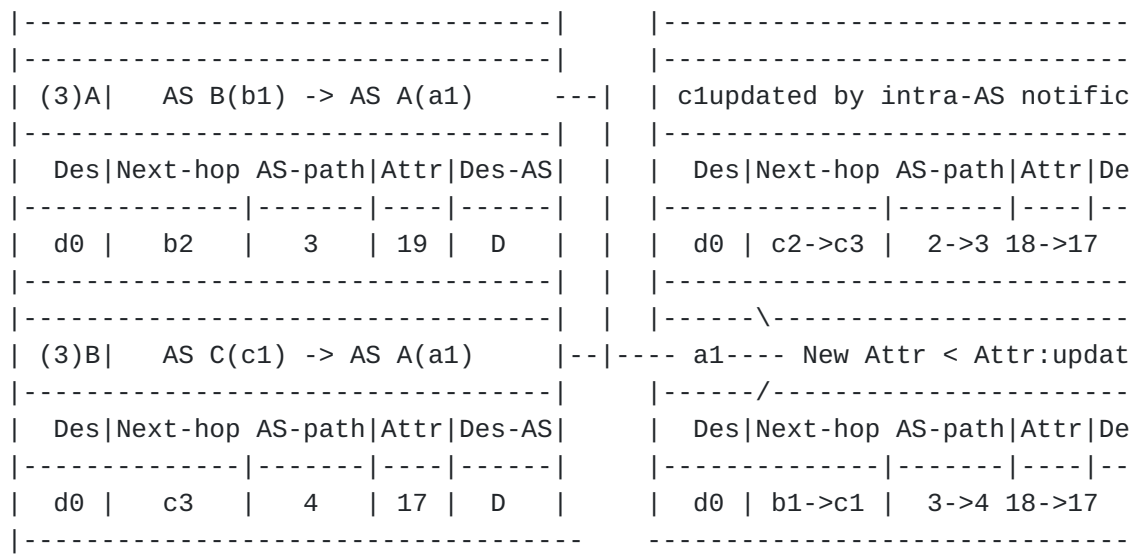

(3)A| AS B(b1) -> AS A(a1)
Des|Next-hop AS-path|Attr|Des-AS|
d0 | b2 | 3 | 19 | D |
(3)B| AS C(c1) -> AS A(a1)
Des|Next-hop AS-path|Attr|Des-AS|
d0 | c3 | 4 | 17 | D |
c1updated by intra-AS notific
Des|Next-hop AS-path|Attr|De
d0 | c2->c3 | 2->3 18->17
a1---- New Attr < Attr:updat
Des|Next-hop AS-path|Attr|De
d0 | b1->c1 | 3->4 18->17

Figure 3: Diffusion example: diffusion of DIT update messages and RIB updates triggered by a new route

4.3. Delta Trap

While Random Number Confusion solves the destination direct connection issue, there is still a trap of information leakage. It can be drawed from a mathematical perspective. Suppose it is known that x1 + x2 = y1 and x1 + x2 + x3 = y2. Even if x1 and x2 are unknown, x3 can also be calculated by using the difference value(DRT) between y1 and y2, i.e., x3 = y2 - y1. As shown in the Figure 2, the value of AS 3 can be obtained using the aforementioned difference value(DRT) method by A 4. To solve the problem, the document proposed Enhanced DIT.

4.4. Enhanced DIT

Delta Trap (DRT) is triggered by one path which has one more hop (itself) than the other of same destination. From the perspective of connection topology, triangular structure is at risk of data leakage. Based on this, the document design a private number comparison algorithm leveraged by homomorphic encryption, which is capable of comparing paths in a triangle topology under guarantee of data security. The comparison result could guide the logical removal of non-shortest paths. It includes classic homomorphic encryption algorithm Paillier and a private number comparison algorithm.

Paillier algorithm randomly selecting two large prime to generate key. Then it can process the corresponding value by encrypting and decrypting. Based on Paillier, the private number comparison which is used as an independent module of DIT to patch the leakage caused by Delta Trap(DRT).

Private Number Comparison firstly detects the triangle structures from the network topology. Then it will compare paths, comparison and path selection would be accomplished by communicating with each other. As shown in Figure 4, suppose A, B and C, each of which is responsible for local values, N_A, N_B, N_C , respectively. First, A sends encrypted N_A, $En^A(N_A)$, to B and C. After receiving the message from A, B sends $En^A(N_A)$ o $En^A(N_B)$ to C, where o represents homomorphic addition calculation, which means En(x) o En(y) = En(x+y). After receiving the message from A and B, C sends $En^A(N_A + N_B)$ o $En^A(drt_C)$ and $En^A(N_A)$ o $En^A(N_C + drt_C)$ to A in the specified order. After receiving the message from C, A decrypts and subtracts the two values, De^A $(En^A(N_A + N_B + drt_C))$ - $De^A(En^A(N_A + N_C + drt_C))$, and get the signed delta value DRT_C, which will be sent back to C. Finally, according to the value of DRT_C, C and A can determine the priority of the two paths, $Path_{(C->A)}$ and $Path_{(C->B->A)}$.

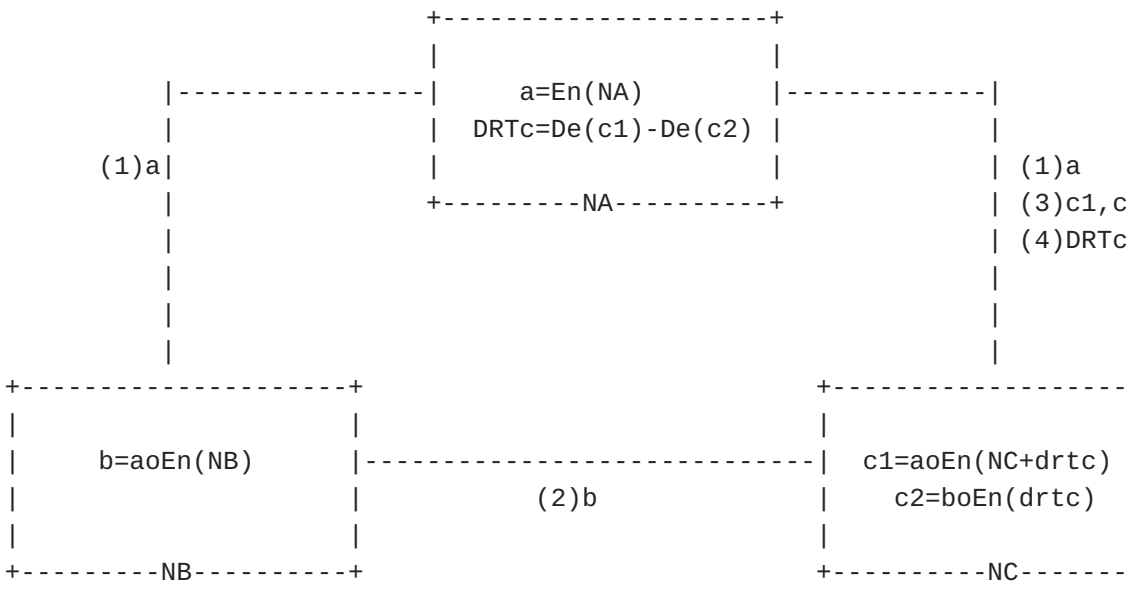


Figure 4: Comparison example: communication and computation process of homomorphic encryption-based private number comparison

The specific process of diffusing is showed in Figure 5. The received BGP message will trigger an UPDATE operation, after which A can then specify the downstream of subsequent transmission. For cases that the direct connection is the optimal path, as shown in the left figure, A directly diffuses the message and uses an identifier to notify the downstream C. For the cases that the direct connection, for example A to C, is not optimal. As shown in the right figure, then A will notify this update to the directly connected downstream node B instead of C, and then B will forward this update to C. Then for C, the path notified by B would be accepted as the optimal one.

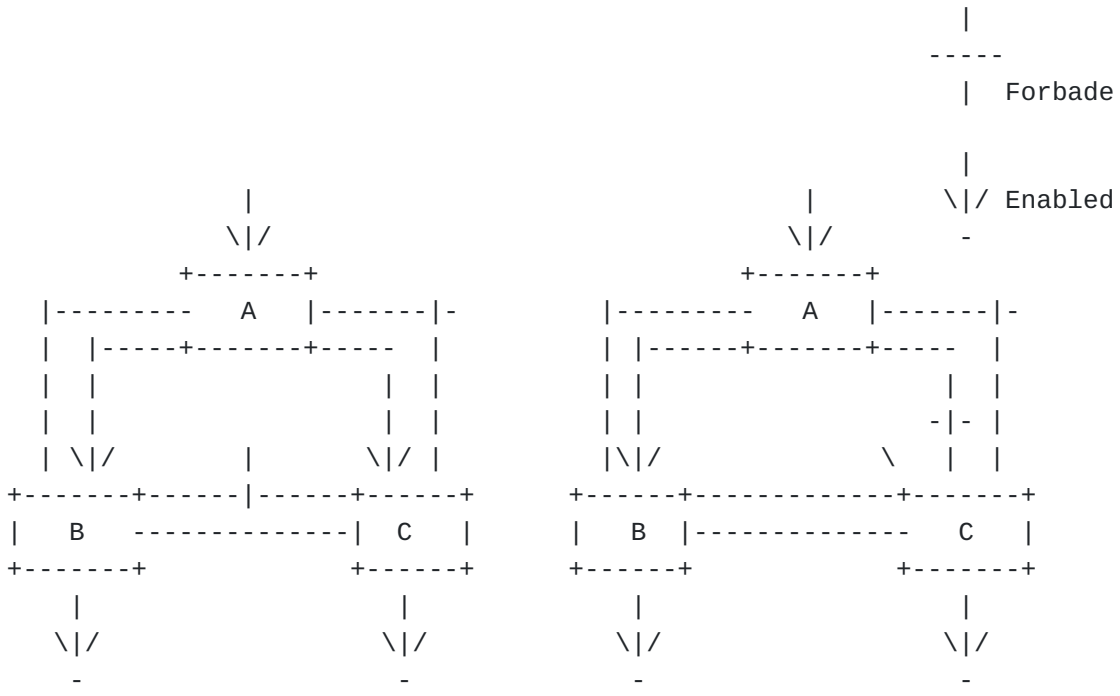


Figure 5: Two types of diffusion constraint

5. Manageability Considerations

I2BGP introduces a new field Attr based on BGP to obtain the message of link in domain. The transmission and use of this field is similar to med and local-pref in the BGP header.

6. IANA Considerations

There are no IANA considerations related to this document.

7. Security Considerations

Owning to I2BGP is based on BGP, I2BGP faces the same security risks like BGP. A BGP implementation MUST support the authentication mechanism specified in [RFC5925]. The authentication provided by this mechanism could be done on a per-peer basis. BGP vulnerabilities analysis is discussed in [RFC4272]. Specific content has been explained in [RFC4271].

8. Normative References

[RFC4271] Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, DOI

10.17487/RFC4271, January 2006, <https://www.rfc-editor.org/info/rfc4271>.

[RFC4272] Murphy, S., "BGP Security Vulnerabilities Analysis", RFC 4272, DOI 10.17487/RFC4272, January 2006, <https://www.rfc-editor.org/info/rfc4272>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC5925] Heffernan, A., "Protection of BGP Sessions via the TCP MD5 Signature Option", RFC 5925, DOI 10.17487/RFC5925, August 1998, <https://www.rfc-editor.org/info/rfc5925>.

[RFC5492] Chandra, R. and J. Scudder, "Capabilities Advertisement with BGP-4", RFC 5492, DOI 10.17487/RFC5492, November 2002, <https://www.rfc-editor.org/info/rfc5492>.

[RFC4760] Bates, T., Chandra, R., Katz, D., and Y. Rekhter, "Multiprotocol Extensions for BGP-4", RFC 4760, DOI 10.17487/RFC4760, January 2007, <https://www.rfc-editor.org/info/rfc4760>.

Authors' Addresses

Yuchao Zhang (editor)
Beijing University of Posts and Telecommunications
China

Email: yczhang@bupt.edu.cn

Peizhuang Cong
Beijing University of Posts and Telecommunications
China

Email: congpeizhuang@bupt.edu.cn

Haiyang Jiang
Beijing University of Posts and Telecommunications
China

Email: jianghaiyang@bupt.edu.cn

Lei Wang
Beijing University of Posts and Telecommunications
China

Email: lwang@bupt.edu.cn

Wendong Wang
Beijing University of Posts and Telecommunications
China

Email: wdwang@bupt.edu.cn