ISSN (e): 2250 – 3005 || Volume, 05 || Issue, 05 || May – 2015 ||
International Journal of Computational Engineering Research (IJCER)

Resolution of Some Cases of Bgp Inter-Domain Oscillations with the Spvpoc Algorithm.

Alphonse Binele Abana[1,] Emmanuel Tonye[2]
[1&2](Department of Electrical and Telecommunication Engineering, Polytechnic National Advanced School of Engineering, University of Yaoundé 1, Cameroon)

Abstract:
BGP was introduced in order to allow autonomous systems to exchange information across the Internet. An autonomous system is a set of routers under a single network administration. Each AS decide its internal routing protocol (RIP, OSPF, ...) and its external routing policy. The BGP routing protocol is used to interconnect the various Internet operators together and is designed for the following two purposes: to best meet the requirements imposed by the routing policies of an operator and respect the principle of confidentiality of these policies. The inconsistencies of these policies cause path oscillations. In this paper, after modeling the operation of the bgp protocol, we present the algorithm SPVPOC and we show how it resolves bgp oscillations in some cases

Keywords: *Internet, bgp, Autonomous Systems, path, inter-domain oscillations*

I. Introduction

A theoretical model is the representation of a complex system following a theoretical analysis; the construction of a theoretical model formalizes a process according to the theory. Internet is a set of autonomous systems or AS (set of routers under a single network administration) interconnected each other and applying their own external routing policy. Thus, Internet can be seen as a set of nodes, each with its particular properties to elapse traffic. Each AS decide its internal routing protocol (RIP, OSPF …) and its external routing policy. The BGP (Border Gateway Protocol) routing protocol [01] is used to interconnect the various Internet operators. It is thus possible to model web as a graph where each autonomous system is represented by a node and the edges model the communication links (physical) between the AS. Consequently, any operation on BGP protocol directly influences the Internet. BGP has been designed for two purposes: to best meet the requirements imposed by routing policies of operators and respect the principle of confidentiality of such policies. Inconsistencies of these policies are responsible of path oscillations phenomenon (unstable routes to a destination at an AS). In this article, we study how to avoid this phenomenon. In other to fulfill this task, we have to first understand the operation of the BGP protocol and then understand the conflict detection method proposed by Griffin [09] before seeing how the SPVPOC algorithm proposed by Binele and Tonye [03] resolves inter-domain oscillations in some cases.

II. General View

2.1 Modeling of an AS

As described in [19], Each AS does not necessarily contain a single BGP router. All these routers apply the same external routing policy defined by the AS. From the outside, all BGP routers in the AS will be seen as a single router. Thus, a network of ASes is modeled by a graph where the vertices and edges respectively represent the ASes and BGP links. Rather, it is a multi-graph since there may be multiple BGP connections between two vertices. Figure.1 represents the network and Figure 2 shows the modeling.

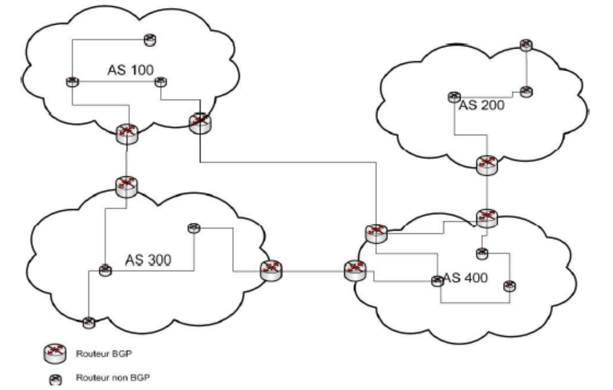

Figure 1-a : example of a Network of ASes

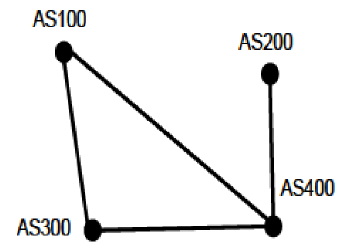

Figure 1-b : Modeling of the network of ASes of figure 1-a

2.2 BGP route attributes

Each router learns from its neighbors a path to a destination. A path P received by a router R on an AS v contains the following attributes [01] :

- LOCAL_PREF: preference value indicating the classification of the choice of the path P in the local routing policy of the AS v
- AS path: AS sequence along the path to reach the destination d of the current AS v
- MED: to discriminate links when two ASes are interconnected with multiple links by associating a degree of preference to each link. A small value of MED indicates a greater preference of the link. This attribute is the cause of internal oscillations of BGP [04] [05].
- Next_hop: The IP address of the border router "next hop" along the path P. If the traffic of R along the path P traverses other routers before leaving AS v, then next_hop is the IP address of the border router that is the exit point of the AS v. If the traffic of R along the path P goes directly from R to a neighboring router in another AS, then next_hop is the IP address of the neighboring router.

For each host AS, a router receives a path (potentially empty) to reach the destination. From this set of paths, the router must choose the best path and adopt it as its own way. The best path is selected according to the algorithm implemented. If a router adopts a new path, if the best path is not the path chosen before, the router informs all of his peers on the newly chosen path.

2.3 Unstable network detection tool: directed conflict graph

In this section we will present the approach of T.G. Griffin [09] who has done an important work in the study of oscillations between AS.

Griffin calculates a conflict graph of path assignments [09] [18] as follows:

Each node of the conflict graph shows a possible path in the network.

Let Q be a path allowed at node v and P a path admitted at node u with v as the first node crossed (P = (u, v) P [v, 0]); It exists two types of arcs between different paths:

- Transmission arcs (dashed line)
- Conflict arcs (solid line)

There is a transmission arc from vP to (u, v)P if u and v are neighbors. In other words, if at node u we have the path 130 and the path 30 at node v, then we put a transmission arc from 30 to 130.

There is a conflict arc from Q to P if the node v may increase the rank of its best path by abandoning P[v,0] in favor of Q which has the effect of forcing u to abandon P. In other words, there is a conflict if a path at node v can force the abandonment of a path at a neighboring node u.

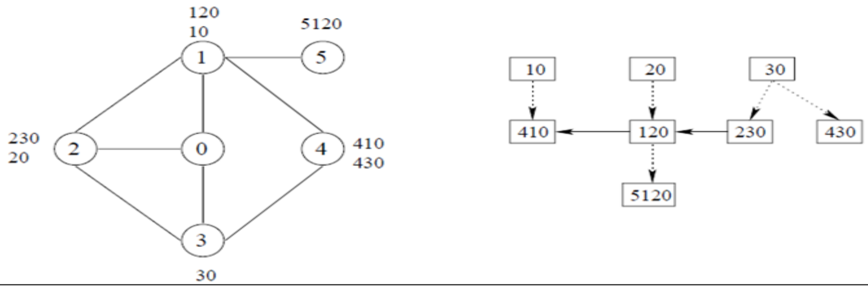

Figure 2: Example of a network with its conflict graph

The main property of this graph is that if there is no cycle in the conflict graph, then the network is stable.

2.4 The SPVPOC algorithm (Stable Path Vector Path Occurrences)

The SPVPOC algorithm gives a solution to solve the SPP (Stable Path Problem) of BGP which was introduced by Griffin in [06]. Let's resume the SPVPOC algorithm that Binele and Tonye proposed in [03] as follows:

Let G = (V, E) be a graph, such as the elements V and E respectively represent ASes and BGP links. Each AS determines a list of paths ordered by order of preference. ASes will try to achieve and maintain the path having a preference value as high as possible. An AS can choose a path only if all the ASes it traverses have chosen the corresponding sub-path. Each AS thus defines a set "choice" containing all possible paths to a destination. The function "Max" will return the route with the highest preference possible at node u while the function "best" will return the route with the highest preference possible at node u if it appearance number is less than the threshold value:

$$best(u) = check\{Hist_{path_{occurence[\max(\text{choice}(u))]}}\} \times \max(choice(u)) \qquad (1)$$

Where u is an AS, "$Hist_{path_{occurence}}$" is an historic of all the possible paths to a destination at an AS with their appearance numbers (occurrences), $Hist_{path_{occurence[\max(\text{choice}(u))]}}$ is the appearance number of the route (path) with the highest preference "$\max(\text{choice}(u))$" at AS u; the function check returns 1 if the this number is lower than the threshold value "Max_path_occurence" and 0 if not. Thus,

$$\text{check}\{\text{ Hist\_path\_occurence}[\max(\text{choice(u)})]\} = \begin{cases} 1 \text{ if } \text{Hist}_{\text{path}_{\text{occurence}[\max(\text{choice(u)})]}} < threshold\ value \\ 0 \text{ if } \text{Hist}_{\text{path}_{\text{occurence}[\max(\text{choice(u)})]}} \geq \text{threshold value} \end{cases}$$

(2)

From (1) and (2) we have:

$$\text{best(u)} = \begin{cases} \max(\text{choice(u)}) \text{ if } \text{Hist}_{\text{path}_{\text{occurence}[\max(\text{choice(u)})]}} < threshold\ value \\ \varepsilon \text{ if } \text{Hist}_{\text{path}_{\text{occurence}[\max(\text{choice(u)})]}} \geq \text{threshold value} \end{cases} \qquad (3)$$

if best(u)= ε, the AS will not change it best path thus, it will retain its current best path at that step.

Let's take the example of the Bad Gadget with 5 ASes of figure 3. The table 1 shows the historic "Hist_path_occurence" which gives the appearance number of all the paths for all ASes at each step. For example for AS2 at step 6, we have the historic [(210,1);(20,1)]: thus, Max(choice(AS2))=20 and Hist_path_occurence(20)=1. If the threshold value of appeareance number is fixed to 2, check[Hist_path_occurence(20)]=check(1)=1. So best(AS2)=20.

III. Application To Some Cases

3.1 Bad Gadget with 5 ASes

Let be the Bad Gadget with 5 ASes below

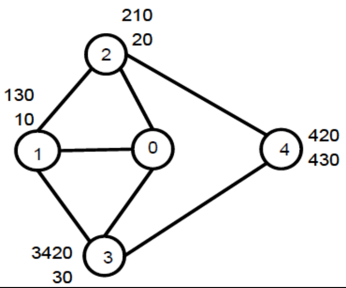

Figure 3: Bad Gadget with 5 ASes

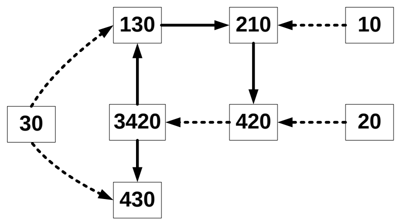

Figure 4: Conflict graph of the Bad Gadget with 5 ASes

Considering the figure 4 above, we can see that there is a conflict on this network as explained on the section 2.3. We will apply the SPVPOC protocol to this network to solve this conflict. Each AS only retains the state changes of its path (change of the number of occurrences of its paths). In this way, we obtain a local management of the path states. In Table 1, at the transition from step 8 to step 9, if we consider that the Max_path_occurrence value is 2, AS 2 detects an oscillation on the path 210 as its number of occurrences is 2; therefore it is considered as a bad path.

Etape	AS1			AS2			AS3			AS4		
	130	10	rib-in	210	20	rib-in	3420	30	rib-in	420	430	rib-in
0	*	*	10	*	*	20	*	*	3420	*	*	420
1	*	*	10	1	*	210	*	*	3420	*	*	420
2	*	*	10	1	*	210	*	*	3420	*	*	Ø
3	*	*	10	1	*	210	*	1	30	*	*	Ø
4	1	*	130	1	*	210	*	1	30	*	1	430
5	1	*	130	1	1	20	*	1	30	*	1	430
6	1	*	130	1	1	20	*	1	30	1	1	420
7	1	*	130	1	1	20	1	1	3420	1	1	420
8	1	1	10	1	1	20	1	1	3420	1	1	420
9	1	1	10	2	1	210	1	1	3420	1	1	420

Table 1: example of path occurrences counting in the Bad Gadget with 5 ASes.

AS 2 will retain its best path 20 to the destination 0 obtained in step 8 and the system will then converge.

3.2 Bad Gadget with 4 ASes

Let be the Bad Gadget with 4 ASes below

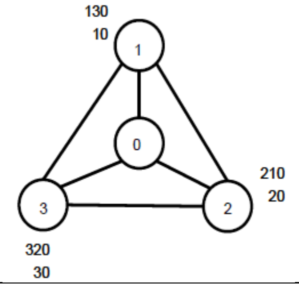

Figure 5: Bad Gadget with 4 ASes

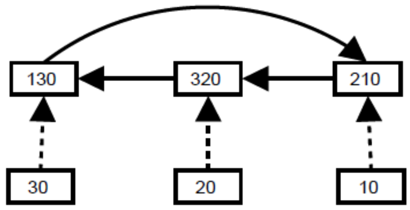

Figure 6: Conflict graph of the Bad Gadget with 4 ASes

As seen in the previous section we can see that there is a conflict in the network (cycle in the conflict graph), each AS only retains the state changes of its paths (change of the number of occurrences of its paths). In Table 2, at the transition from step 6 to step 7, if we consider that the Max_path_occurrence value is 2, AS 2 detects an oscillation on the path 210 as its number of occurrences is 2; therefore it is considered as a bad path.

Etape	AS1			AS2			AS3		
	130	10	rib-in	210	20	rib-in	320	30	rib-in
0	*	*	10	*	*	20	*	*	320
1	*	*	10	1	*	210	*	*	320
2	*	*	10	1	*	210	*	1	30
3	1	*	130	1	*	210	*	1	30
4	1	*	130	1	1	20	*	1	30
5	1	*	130	1	1	20	1	1	320
6	1	1	10	1	1	20	1	1	30
7	1	1	130	**2**	1	210	1	1	30

Table 2: example of path occurrences counting in the Bad Gadget with 4 ASes.

Thus, AS 2 will retain its best path 20 to the destination 0 obtained in step 6 and the system will then converge.

3.3 Bad Backup

Let be the Bad Backup with 5 ASes below

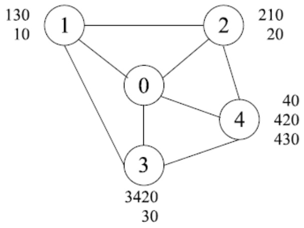

Figure 7: Bad Backup with 5 ASes

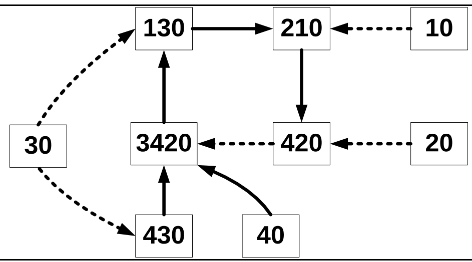

Figure 8:Conflict graph of the Bad Backup with 5 ASes

As seen in the previous section we can observe a cycle on the conflict graph. By applying the SPVPOC algorithm, each AS only retains the state changes of its paths (change of the number of occurrences of its paths). In Table 3, at the transition from step 9 to step 10, if we consider that the threshold (Max_path_occurrence) value is 2, AS 2 detects an oscillation on the path 210 as its number of occurrences is 2; therefore it is considered as a bad path.

Etape	AS1			AS2			AS3			AS4			
	130	10	rib-in	210	20	rib-in	3420	30	rib-in	420	430	40	rib-in
0	*	*	10	*	*	20	*	*	3420	*	*	*	420
1	*	*	10	1	*	210	*	*	3420	*	*	*	420
2	*	*	10	1	*	210	*	*	3420	*	*	1	40
3	*	*	10	1	*	210	*	1	30	*	*	1	40
4	1	*	130	1	*	210	*	1	30	*	*	1	40
5	1	*	130	1	*	210	*	1	30	*	1	1	430
6	1	*	130	1	1	20	*	1	30	*	1	1	430
7	1	*	130	1	1	20	*	1	30	1	1	1	420
8	1	*	130	1	1	20	1	1	3420	1	1	1	420
9	1	1	10	1	1	20	1	1	3420	1	1	1	420
10	1	1	10	2	1	210	1	1	3420	1	1	1	420

Table 3: Bad Backup with 5 ASes

Thus, AS 2 will retain its best path 20 to the destination 0 obtained in step 9 and the system will then converge.

IV. Conclusion

BGP is an inter-AS routing protocol and presents many oscillation problems which must be resolved quickly because the operation of the Internet depends on it. In this paper, we have studied and characterized cases of oscillations caused by the overall inconsistency of policies adopted by the ASes. Then we presented the new SPVPOC algorithm proposed by Binele and Tonye [03]. This solution inherits all the properties of the current BGP and is more stable. Finally, we applied this algorithm to few cases of inter-domain oscillations like the Bad Gadget with 4, 5 ASes and the Bad Backup with 5 ASes. A perspective would be to study the behavior of the protocol for intra-domain oscillations (iBGP).

References

[1]. REKHTER,Y.,LI,T.,AND HARES, S. A Border Gateway Protocol 4 (BGP-4). Internet Draft draft-ietf-idr-bgp4-25.txt, September 2004.

[2]. Timothy G. Griffin, F. Bruce Sherpherd, and Gordon Wilfong. Policy disputes in pathvector protocols. Proc. 7th Int. Conf. Network Protocols (ICNP'99), pages pp. 21–30,1999.

[3]. Alphonse BINELE and Emmanuel TONYE, "A new approach to fight against the inter –domain BGP oscillations", in OSR Journal of Electronics and Communication Engineering (IOSR-JECE) e-ISSN: 2278-2834,p-ISSN: 2278-8735.Volume 10, Issue 1, Ver. II (Jan -Feb. 2015), PP 66-74

[4]. Timothy G. Griffin and Gordon Wilfong. Analysis of the med oscillation problem in bgp. in Proc. of the 10th IEEE Int. Conf. on Network Protocols, pages pp. 90–99, 2002.

[5]. Ken Schummacher. Stabilité dans bgp. December 2004.

[6]. Timothy G. Griffin and Gordon Wilfong. A safe path vector protocol. Proc. IEEE INFOCOM, vol.2 :pp. 490–499, 2000.

[7]. Kannan Varadhan,Ramesh Govindan and Deborah Estrin. Persistent route oscillations in inter-domain routing. Elsevier Science B.V., 2000.

[8]. Jerome BARBOU, Alpha Amadou DIALLO, Greg´ ori FABRE, Damien FONTAINE, Intissar GALL -Universite Paris VI - M2-Rout - Routage Interdomaines

[9]. T. G. Griffin, F, B. Shepherd, and G. Wilfong, "The stable paths problem and interdomain routing,"IEEE/ACM Trans. Networking, vol. 10 no. 2,pp. 232-243,2002

[10]. R. Musunuri Texas Univ., Dallas, TX, USA, "An overview of solutions to avoid persistent BGP divergence", in IEEE Network: The Magazine of Global Internetworking vol 19, 2005,pp28-34

[11]. T. G. Griffin, F, B. Shepherd, and G. Wilfong, "Policy disputes in path vector protocols,"in Proc. of IEEE ICNP conference, 1999, pp. 21-30.

[12]. T. G. Griffin, F, B. Shepherd, and G. Wilfong, "An analysis of BGP convergence properties,"in Proc. of INFOCOM conference,, 1999, pp. 277-288.

[13]. IEEE, "A method to eliminate BGP divergence based on AS relationships", in Circuits,Communications and System (PACCS), Second Pacific-Asia Conference on vol 1, 2010, pp 31-34.

[14]. L. Gao and J. Rexford, "Stable Internet routing without global coordination," IEEE/ACM Trans. Networking, vol. 9, no. 6, pp681-692,2001

[15]. T.G. Griffin, F.B. Shepherd, and G.Wilfong, "A safe path vector protocol," in Proc. of INFOCOM conference,2000,pp. 490-499

[16]. J.A Cobb, M.G. Gouda, and R. Musunuri, "A stabilizing solution to the stable paths problem," in Proc. of Symp. on self-stabilizing systems, Springer-Verlag Lecture Notes in Computer Science, vol. 2704, 2003, pp169-183

[17]. J.A. Cobb and R. Musunuri, "Convergence of inter-domain routing," in Proc. of IEEE GLOBECOM conference, 2004, pp1353-1358

[18]. G. Wilfong T. G. Griffin, F. B. Shepherd. The stable paths problem as a model of bgp routing. Septembre 2000.

[19]. Ken Schumacher, thesis on the Stability of BGP. University of Montpelier 2. 2004, page.10.