

4-14 BGP データを用いた AS パスの比較による喪失経路の解析

小林研究室

1915039 篠田 健心

1. はじめに

インターネットは自律ネットワークシステム(AS)の相互接続によって構成されたネットワークであり、BGP(Border Gateway Protocol) [1]という経路制御プロトコルにより BGP ルータ間で経路情報を交換し、経路制御を行う。先行研究 [2]では多地点での UPDATE メッセージを取得し、喪失経路(WITHDRAW)数と更新経路(ANNOUNCE)数から経路障害の程度を表す指標を定め、経路障害の規模を推定した。本研究では、複数の AS から届く UPDATE メッセージが持つ経路変更候補である ASPATH と、経路変更候補と自 AS が持つ経路情報を比較し、最適な経路を選択・保持する RIB(Routing information Base)の ASPATH を比較することで喪失した AS 番号の推定を行う。

2. 解析手法

本研究では、Route Views Project [3]から取得した UPDATE メッセージと 2 時間間隔で出力される経路表である RIB データを使用する。先行研究 [2]は、UPDATE メッセージに記載されている 1 分間の WITHDRAW, ANNOUNCE の prefix 数 x_w , x_a から経路障害の程度を表す指標値を式 (1), (2) のように定めた。

$$I_w = \frac{\log_{10}(x_w) - \mu_w}{\sigma_w} \dots (1) \quad I_a = \frac{\log_{10}(x_a) - \mu_a}{\sigma_a} \dots (2)$$

公開されている経路障害のうち発生及び修正時刻、原因の AS が明確な経路障害である 2017 年 11 月 25 日に発生した経路障害 [4]等の指標値 I_w , I_a の時間変化の共通点を調べ、同様の变化をした時刻を特定する。図 1 に示すように、特定した時刻の UPDATE メッセージとその時刻より前の RIB から prefix と ASPATH を取り出す。

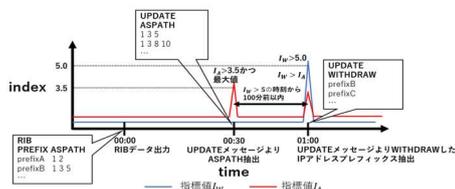


図 1 取り出す指標値の変化と使用する BGP データまた、取り出したデータを図 2 の手順で処理することにより、喪失した AS 番号の推定を行う。



図 2 RIB と UPDATE の ASPATH の比較方法

3. 結果

経路障害が発生した 2017 年 11 月 6 日について、指標値の変化が確認できたデータ取得地点で ASPATH を比較した結果を図 3 に示す。

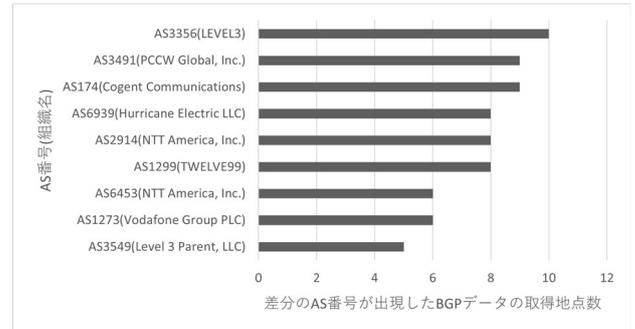


図 3 各データ取得地点から得た共通の差分の AS 番号 図 3 より、経路障害の原因である level3 (AS3356) の出現を 10 地点で確認することができた。また、指標値より得られた時刻である 2019 年 12 月 13 日の RIB から変化が確認できた経路を図 4 に示す。ただし、青線は 08:00 (UTC) の RIB データ、赤線は I_a が最大の時刻での UPDATE メッセージの ASPATH を示している。

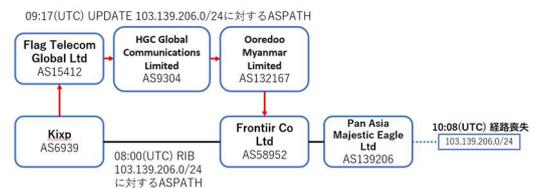


図 4 差分 AS が見られた RIB データの ASPATH の変化 2019 年 12 月 13 日の UPDATE と RIB の差分として得られた共通の AS である AS15412 を通る迂回経路が採用されたことが RIB データから確認でき、AS15412 の喪失により指標値 I_w が増加したと考えられる。

4. まとめ

本研究では 15 地点の BGP データを取得し、路障害発生時の指標値 I_w , I_a の時間変化と同様の变化をした時刻情報のリストから、UPDATE メッセージの ASPATH と RIB データの ASPATH の比較により、喪失した可能性のある AS 番号を推定した。

参考文献

- [1] RFC4271, A Border Gateway Protocol 4(BGP-4), <https://www.rfc-editor.org/rfc/rfc4271>
- [2] 山岸大起, 「BGP データを用いた経路障害規模の解析」 富山県立大学卒業論文 2019 年度
- [3] University of Oregon, Route Views Project, <http://routeviews.org/>
- [4] ThousandEyes, Comcast Suffers Outage Due to Significant Level 3 BGP Route Leak <https://www.thousandeyes.com/blog/comcast-outage-level-3-route-leak>