

AS グラフ構造に基づく経路情報耐性と協調防御の有効性に関する解析

明石 修^{1,a)}

概要：インターネットは自律システム (AS) の集合で構成される巨大分散システムである。各 AS は BGP により経路情報交換を行い接続性を維持するが、その構造は BGP の経路広報接続関係をエッジとする AS のグラフとして捉えられ、経路情報の拡散や、障害時の振舞を解析するための重要な指針となる。本報告では、経路ハイジャック等の経路障害時の挙動に注目し、AS グラフ構造の視点からその振舞を解析し、各 AS が隣接 AS と協調動作した場合の協調戦略の有効性も含めて経路情報の耐性に関して議論する。

Analysis of Cooperative Management Strategies against Route-Hijacking

Abstract:

The Internet is a huge distributed system which consists of Autonomous Systems (ASes). This structure is characterized as the AS graph structure where ASes are connected by BGP peer relations. This structure is important to analyze the behavior of route information distribution, especially when anomalous routing state occurs. This paper focuses on route hijacking which is still one of major routing issues, and analyzes the behavior when some cooperative strategies are applied against hijacked-route distribution.

1. はじめに

インターネットは、7 万を超える自律システム (AS: Autonomous System) が他の複数 AS と接続する巨大分散システムであり、60 万もの IP prefix 情報が AS 間で BGP[1] により交換される。各 AS はそれぞれ個別の組織によって運用されており、近傍 AS 間においてはより密な協調が可能であるが、グローバルな視点での中央集権的な手法は適用が難しい。そのため、さまざまな事象が複数 AS をまたがって発生 [2] する。

経路情報の妥当性の検証は、そのような問題のうちの一つであり、さまざまなレベルでの接続性維持に影響する。BGP では自身の保持する IP prefix 情報を、BGP peer と呼ばれる BGP 上の隣接 AS に広報するが、これは AS 毎にホップしながら伝わっていき、全インターネットに拡散する。広報元では、自身が広報した prefix 情報に関して、全インターネット中の AS での妥当性を検証できないため、

広報元 AS に対する接続性に影響が出る状態になったとしても原因解析は難しい。

対策の一つとして、単一 AS の中だけでなく、複数 AS をまたがった分散観測・統合解析を行い、その結果に応じて近傍 AS 間での協調を通じて問題を解決する方法があげられる。しかしながら、現在の運用や障害対応は、AS 毎のオペレータ間でのアドホックな対応手法が大半であり、ネットワーク運用の安定した自律化に向けて、各 AS の環境に応じた協調動作が可能となるように、基本特性を解析し、新たなフレームワークを構築することが望まれている。経路情報障害ではないが、障害事象に対する経路情報操作の視点では、DDoS パケットフィルタリングに関し、BGP Flowspec[3] を用いたサービスも展開されているが、AS 内に閉じたケースであり、適用範囲の拡大、その構築フレームワーク、効果の指標に関しては議論が必要である。

ネットワーク環境の安定した運用自律化に向けて、AS 間での問題解決に注目し、動的に変化する状況を考慮しながら近傍 AS と協調問題解決する機構を提案し、その有効性を定量評価することが本研究の最終的な目的である。

今回の報告では、まず実際のネットワーク運用上、重要

¹ 国立情報学研究所
National Institute of Informatics
^{a)} akashi@nii.ac.jp

な問題の一つである AS 間経路障害を対象に、特に自己の経路情報が他の組織に意図的、あるいは設定ミスで広報される経路ハイジャックの対策に注目する。本症例においては、自己組織宛のパケットが攻撃者等の組織に転送されてしまい、自組織の通信が不能になるという深刻な障害が今日のインターネットにおいても発生している。

ハイジャック経路情報の遮断の難しさとしては、経路情報は、一つの AS で遮断しても自動的に迂回して他の AS 経由で拡散する性質に由来する。そのため、不正なハイジャック経路を遮断するためには複数 AS でのトポロジを考慮した協調フィルタが必要となる。BGP のベストパス選択ルールでは、特に `local_pref` 値等のポリシー制御を行わない場合、AS パス長で決定されるため [1], 短い AS ホップ数で拡散する不正経路のパスを遮断して無効化を行う手段も用いられるが、同様な協調フィルタが必要となる。

インターネットトポロジの接続数の分布は、power-law で特徴付けされ [4], [5], 少数のハブ AS が多くの AS と接続を持つ形である。従って、ハブ AS は BGP ベストパスの分散に重要な役割を果たす。同時に、ハイジャックを検知する能力を持つ AS の存在箇所としても重要となる。従って、AS グラフの構造から、経路情報の分散、ハイジャック経路の分散、そしてハイジャック検知 AS の存在箇所やその配置方法の有効性を解析することは重要となる。

インターネット全体での AS 経路トポロジの作成や隣接関係の発見、そのグラフ理論的な解析に関しては多くの先行研究があるが、そのグラフ構造を経路情報拡散、経路ハイジャック、隣接協調防御有効性の解析に用いた例は会議報告 [6] の範囲と思われる。[6] では総 AS 数 30,000 程度に対し、AS 経路トポロジの構造を経路ハイジャック障害と連携させ、経路ハイジャック時の経路拡散の振舞等の定量的な統計的解析を行った。しかしながら、隣接協調による防御の有効性解析は不明確な部分も存在し、また現在では 70,000 を超える AS が観測されている。本報告では、同様に CAIDA の AS relationships data [7] から AS のトポロジ構造を作成し、BGP の経路情報拡散をシミュレーションすることで解析する。その上で、経路ハイジャック検知機能を持つ AS を、分散協調防御の視点も含めて配置し、その有効性を解析する。

2. Methodology

AS の隣接関係を示したデータ [7] から AS トポロジを構築し、そのトポロジ上でシミュレーションを行い、経路の伝搬と隣接協調の定量的評価を行う。本データでは、隣接関係に、`provider`, `customer`, `peer` の推定された役割が付記されている。用いたデータは、20201101.as-rel.txt である。

Date	top ASes	leaf ASes	total # of ASes
2010.01	121 (0.4%)	28525 (85.1%)	33508
2020.11	394(0.6%)	59784(84.7%)	70579

表 1 AS グラフの基本構造

Table 1 Basic structure of AS graph

2.1 シミュレーション環境

[6] と同様に、CAIDA の AS relationships data [7] から AS のトポロジ構造を作成し、BGP の経路情報拡散をシミュレーションするシステムを ACL [8] を用いて作成した。このデータセットでは、BGP peer である一組の AS、および接続関係 (`customer/provider`, `peer`) が記述されている。これらの二項関係から、インターネット全体でのグラフを作成する。すなわち、ノードは AS、エッジは BGP の接続関係を示す。

シミュレーション内部では、AS を表すオブジェクトは AS 番号を持ち、それぞれ IP-prefix を表す prefix 番号を一つ割り当てる。各 AS は自 AS 番号を AS パス情報として付与した後、自 prefix を BGP 接続関係にある隣接 AS に広報する。受信した prefix 情報は、BGP ルールに従い、隣接 AS に再度広報される。このとき、通常の BGP と同じく、受信した AS パス情報に自身の AS 番号をプッシュして AS パス情報を更新し、prefix と共に広報する。BGP の特徴であるポリシールーティングを実現する `local_pref` 属性や `community` 属性は付与しない。従ってベストパスの選択、すなわち複数の隣接 AS から同一宛先の prefix を受信した場合は、通例の BGP 経路選択ルールに基づき、AS パスの長さの短い方を優先し、ベストパスのみを広報する。IGP のメトリックも考慮しないため、複数の候補が同一優先順位であった場合、ランダムに選択する。これらは、通例のポリシー制御のない BGP ルータの挙動をシンプルにモデル化した挙動である。ただし、`provider/customer/peer` の関係は付加されているため、受信した経路の再広報に関しては、実際のインターネットの設定に従う。

この系を仮想時間で駆動し、各仮想時間毎に 1AS ホップの広報を全 AS オブジェクトに関して行い、全ての AS に広報が完了した時点で停止する。なお現実の BGP 経路分散は実時間で、仮想時間を用いるシミュレーションと経路拡散途中での挙動が経路の到着時間により異なるが、最終的な定常状態は AS グラフ構造によって定まるため、結果は同じであり、本解析の目的には十分であると考えられる。

基礎データとして AS グラフの構成を表 1 に、接続数の分布を図 1 に示す。前者の日付は [6] 実験時点の 2010.01 のデータであり、総 AS 数は 33,508 である。後者は今回の実験に用いた 2020.11 のデータ (`as-rel.20201101.txt`) であり、総 AS 数は 70579 である。基本的な構成は同様と思われるが、接続数が 10-1000 の部分で、後者の構成数が若干増加している。

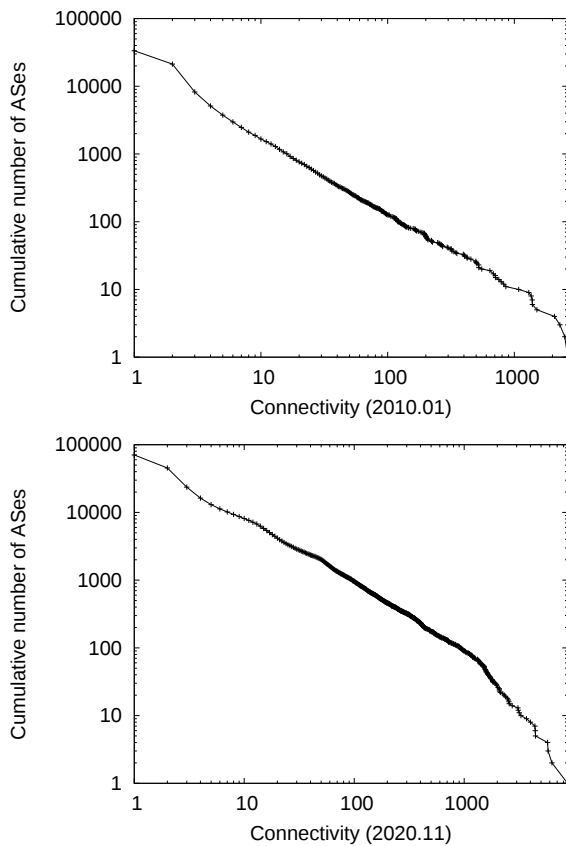


図 1 接続数の分布

Fig. 1 Connectivity distribution

2.2 シミュレーション設定

本データには provider/customer, peer の関係が記述されており、経路を受信し、再広報する場合の挙動が異なる。シミュレーション上は、以下のように再現した。

- AS_x が provider か peer AS から経路を受信した場合、 AS_x は自身の customer AS に広報する。
- If AS_x が経路を customer AS から受信した場合、 AS_x は自身の provider, peer, 受診元を除く customer AS に広報する
- AS_x が同一経路を provider AS と peer AS から受信した場合、 AS_x は peer AS から受信した経路をベストパスとして選択する。
- AS_x が同一経路を peer AS と customer AS から受信した場合、 AS_x は customer AS から受信した経路をベストパスとして選択する。

実験に際しては、それぞれの接続数を持つ AS からランダムに 5AS を選択し、その結果の平均値を値として用いたが、この値は今後は調整していく必要があると考えられる。

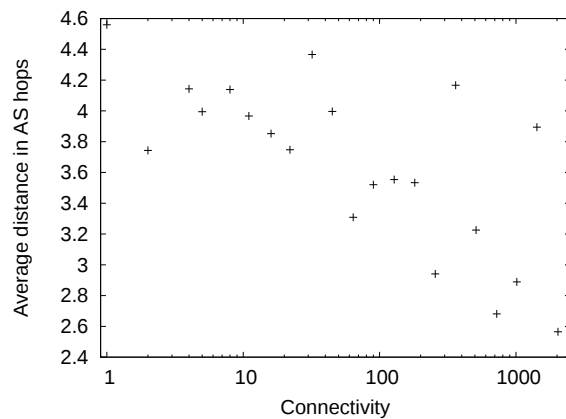


図 2 他の AS への平均 AS パス長

Fig. 2 Average distance to other ASes

3. 実験結果の解析

3.1 ベストパス拡散

図 2 に、接続数 c に関する平均 AS パス長を示す。平均 AS パス長 $D(c)$ は、以下のように定義した。

$$D(c) = \text{average} \left(\sum_{AS_i \in AS_set(c)} \text{distance}(AS_i, AS_{j \neq i}) \right)$$

where:

$$AS_set(c) \equiv \{AS_k | \text{number_of_peers}(AS_k) = c\}$$

$$\text{distance}(AS_i, AS_j) \equiv AS_hops(\text{best_path}(AS_i, AS_j))$$

図 2 では、高い接続数を持つ AS ほど平均 AS ホップ数が少なく他の AS に到達できるベストパスを持つ傾向が、[6] における 2010.01 のデータでの解析と同様に見られる。高い接続数を持つ AS は AS グラフ全体の構造から、より中心に位置する AS であり、経路ハイジャックに対する耐性が強い、また逆にこのような AS から経路ハイジャックが行われてしまうと、他の AS からの正規経路を上書きしてしまうことが予測される。なお 2010.01 のデータでの解析に比べると、本データでは AS 数では倍増の一方、平均 AS パス長では同一の傾向ながら、0.6 ホップ程度の短縮が見られた。

3.2 ハイジャック経路の分散

図 3 に、AS の接続数から見た経路ハイジャックに対する生存割合を示す。本図は本来の prefix 広告元の AS、経路ハイジャックを行う AS の接続数をパラメータとして、ハイジャック経路の広報後の BGP 状態安定後の全 AS 中における平均生存割合を示す。例えば、生存割合 0.5 は、半分の AS でハイジャックされた経路がベストパスとして採用されたことを示す。なお経路広報元 AS、ハイジャッ

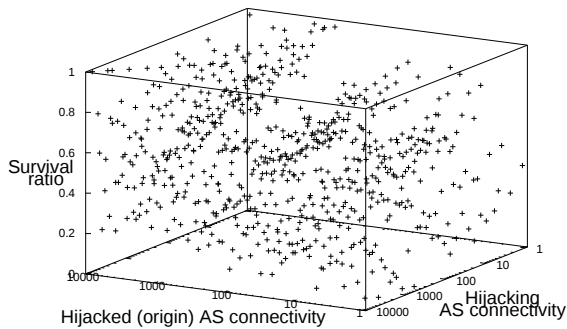


図 3 経路ハイジャックに対する耐性割合.
Fig. 3 Survival ratio against hijacking.

ク AS, それぞれの次数から 5 個の AS をランダムに選択して平均値とした。

図 3 では, 経路ハイジャックをする AS の接続度が大きくなるにつれ, 経路生存の割合が小さくなる傾向を示す。同時に, ハイジャックされる側の接続度が大きくなるにつれ, より大きな生存割合を示す。これは 3.1 節での解析結果とも一致する。

3.3 ハイジャック防御協調戦略の解析

最初の基本となる比較対象の戦略として, ハイジャック検知をする能力がある AS をランダムに配置する戦略 (ST-R) を想定する。ハイジャック検知をした AS は, その受信した経路がハイジャックだと自立的に (他の AS と協調動作や情報交換なしで) 判断可能とし, その経路を廃棄することが可能と仮定する。実験結果を図 4 に示す。

本グラフでは, X 軸をハイジャックする AS の接続数, Y 軸をハイジャック検知可能な AS の数, Z 軸を正規経路の生存割合とする。3 つのグラフはそれぞれハイジャックされる AS の次数の違いであり, 2, 16, 128 を表示した。ハイジャックを検知する AS の数の違いで大きな差異は見られないが, 数が大きくなるに連れ, ゆるやかに生存割合が上がる。また, ハイジャックされる AS の次数でも大きな差異は見られないが, 次数が大きくなるに連れ, 同じくゆるやかに生存割合も上がる。

次の協調防御戦略として, ハイジャック検知をする能力がある AS を, 接続度が高い AS から選択する戦略 (ST-L) を想定する。結果を図 5 に示す。図 3 の結果から直感的に, あるいは [6] で定量的にも示したように, 本戦略は有効であり, 20201101.as-rel.txt のデータでも同様の効果を示す結果となる。ST-R と比べて, ハイジャックを検知する AS の数の違いで緩やかな一様ではなく, 数が大きくなるに連れ明確に生存割合が上がる。また, ハイジャックされる AS の次数が大きくなるに連れ, 全体的に生存割合も上がる傾向が見られる。

次に, 経路ハイジャックを検知する AS として, 隣接す

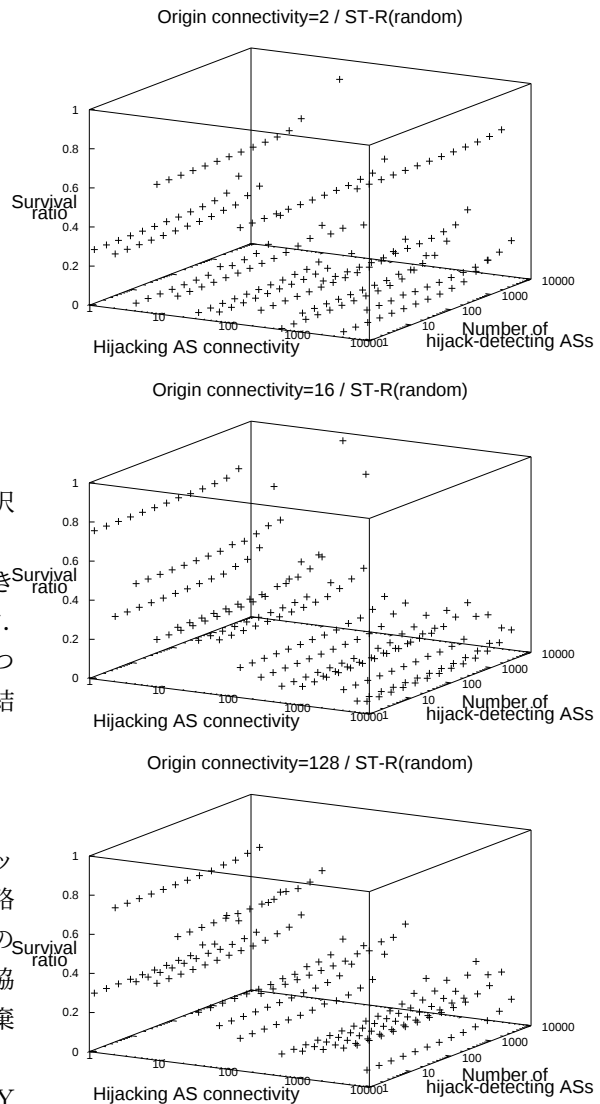


図 4 本来経路の生存割合 (ST-R)
Fig. 4 Ratio of correct routes: Effectiveness of validity-check ASes against route hijacking. (ST-R)

る AS を協調 AS として選択する戦略を想定する (ST-C2)。最初の検知する AS の選択はランダムであるが, その次の AS は隣接する AS とする。なお協調する隣接 AS 数はクラスタ毎で 2 と設定する。協調動作をする隣接 AS の選択として, provider, peer, customer の順番のプレファレンスで行うとする。図 6 に結果を示す。なお, Y 軸のハイジャック検知可能な AS の数は, 協調動作する AS を含めた総数とする。ST-L ほど顕著ではないが, 同様にハイジャックを検知する AS の数の違いで, 緩やかな一様ではなく, 次数が大きくなるに連れ明確に生存割合が上がる。また, ハイジャックされる AS の次数でも, 数が大きくなるに連れ, 全体的に生存割合も上がる傾向が見られる。

ここで, ST-L, ST-R, ST-C2 に関して, ハイジャックを検知する AS の数を X 軸に, その他の部分を平均化してプロットした図を図 7 に示す。ST-L は, ハイジャックを検

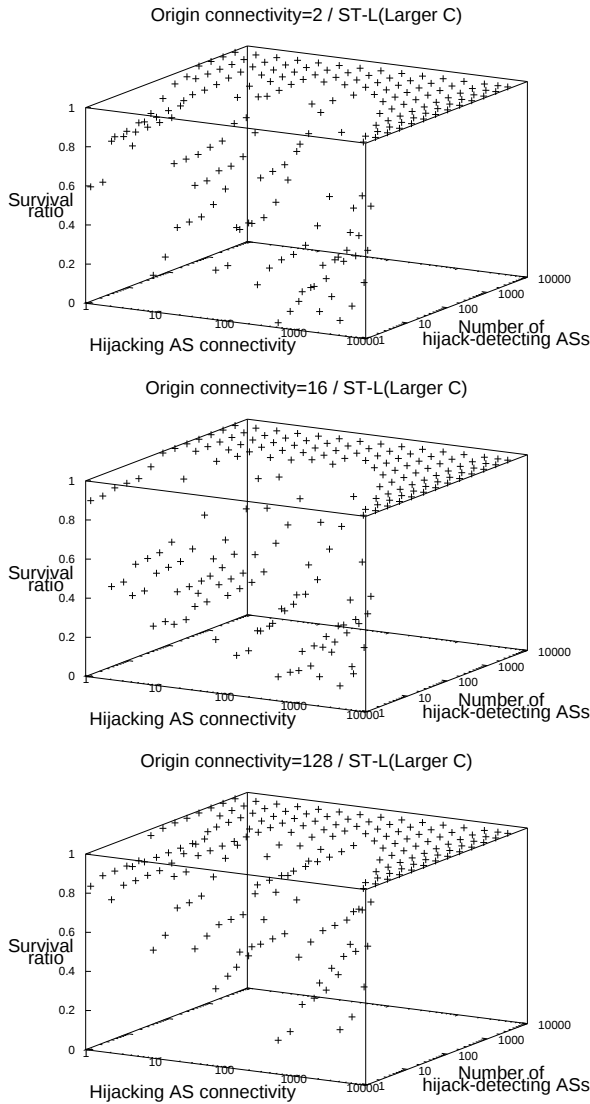


図 5 本来経路の生存割合 (ST-L)

Fig. 5 Ratio of correct routes: Effectiveness of validity-check ASes against route hijacking. (ST-L)

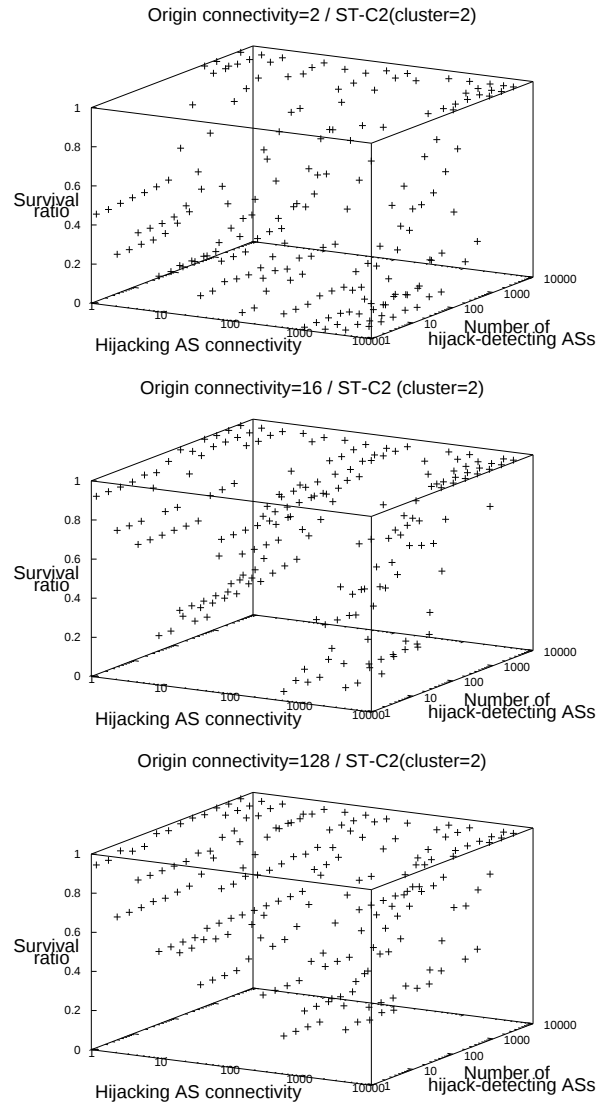


図 6 本来経路の生存割合 (ST-C2:cluster=2)

Fig. 6 Ratio of correct routes: Effectiveness of validity-check ASes against route hijacking. (ST-C2:cluster=2)

知する AS の数全てにおいてランダム選択である ST-R, 大きさ 2 のクラスタを構成する協調動作戦略 ST-C2 を生存率において上回るが, ST-C2 も効果を示す. ST-R は, 明らかにハイジャックを検知する AS の数の変化において, その生存割合を変化しない.

ランダム選択である ST-R は, 割合の多い接続数の少ない AS(図 1) を選択する確率が高いため, ST-L に対して生存割合が低いと考えられる. また, customer AS を持たない leaf AS も 85% 程存在し (表 1), その選択確率が高いためであると思われる. 一方, ランダム選択を基本とする ST-C2 であるが, 隣接 AS を provider あるいは peer AS から選択するため, 選択された側のハイジャック検知機能により, 生存割合が上がると考えらる.

隣接 AS 協調動作の有効性を解析するため, 隣接 AS 選択部分を変更した戦略を用いた実験結果を示す. 比較のため,

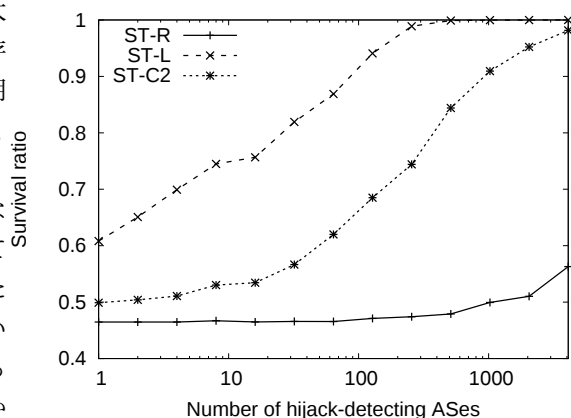


図 7 本来経路の平均生存率 (ST-R, ST-L, ST-C2)

Fig. 7 Ratio of average correct routes: Effectiveness of cooperative validity-check ASes (ST-R, ST-L, ST-C2)

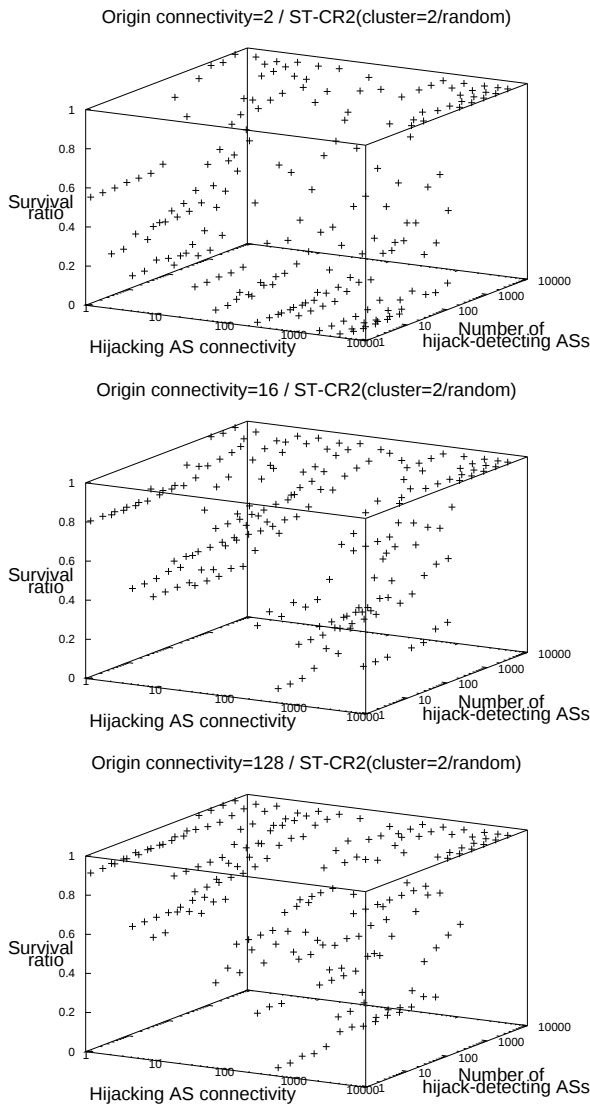


図 8 本来経路の生存割合 (ST-CR2: cluster=2,random)

Fig. 8 Ratio of correct routes: Effectiveness of validity-check ASes against route hijacking. (ST-CR2: cluster=2,random)

隣接する AS からランダムに選択したケース (ST2-CR2) (図 8) と, provider AS より先に peer AS を最初に選択する preference に変更したケース (ST2-CP2) を試した. なお, 隣接 AS の最大数は 2 のままとした. また, ST-C2, ST-CR2, ST-CP2 に関して, ハイジャックを検知する AS の数を X 軸に, その他の部分を平均化してプロットした図を図 9 に示す.

協調戦略間の有効性に関して, [6] では差異が不明確であったが, 本実験では生存割合として, ST-CP2, ST-C2, ST2-CR2 の順番で効果が見られる. Peer 第一選択が provider 第一選択より有効そうである理由としては, peer 戦略が階層構造の他の木構造部分を直接防御できるのに対し, 直上の provider は, 配下に持つ木構造が統計的に大きくなかった, という解釈が可能であるが, leaf AS が高確

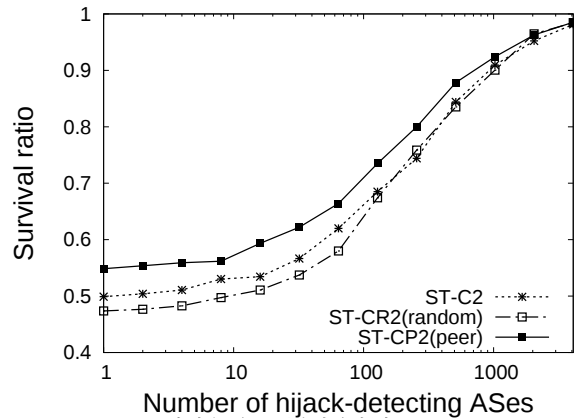


図 9 本来経路の平均生存割合 (ST-C2, ST-CR2, ST-CP2)

Fig. 9 Ratio of average correct routes: Effectiveness of cooperative validity-check ASes. (ST-C2, ST-CR2, ST-CP2)

率で選択されるサンプリングの影響を排除し, その階層構造に基づくより詳細な解析が必要と思われる.

次に, 協調動作する隣接 AS の数の違いに注視する. すなわち最初のランダム AS 選択からハイジャック検知 AS が, provider, peer AS の preference で隣接 AS から協調動作する AS を選択する ST2 をベースに, 協調動作する AS を隣接 AS から選択肢, その数を 3(ST-C3), 4(ST-C4) と変化させ, 実験を行った. ST2-C3 は図 10 に, ST2-C4 は図 11 に示す.

またこれらの比較のため, 同様にハイジャックを検知する AS の数を x 軸に, その他の部分を平均化してプロットした図を図 12 に示す.

本部分も [6] では差異が不明確であったが, この図では, ST-C4 がより高い生存割合を示し, ST2-C3 が次点となる. ST-C3 は, ハイジャック検知を行う AS 数が 1000 を超える辺りで, ST-C2 の効果が逆転する. ハイジャック検知 AS 数が増えることでの効果に関しては, より詳細な解析が必要と思われる.

次の戦略では, 協調する AS が直列化するように選択する. すなわち, ランダム選択したハイジャック検知 AS が, provider, peer AS の preference で隣接 AS から協調動作する AS を選択し, さらにその協調動作 AS が次の協調動作する隣接 AS を同様の preference で選択する. 協調動作する AS 数を 2(ST-S2), 3(ST-S3), 4(ST-S4) と変化させ, 実験を行った. 図 13 に結果を示す. 定義より, 隣接 AS 数が 2 の場合, ST-S2 は ST-C2 と同じとなる.

この実験では, ST-S4 がより高い生存割合を示し, ST-S3 が次点となる. ST-S2 は, ハイジャック検知を行う AS 数が 10 以下で, ST-S3 の効果が逆転するが, 数が小さい部分に関しては, 配置箇所数とクラスタ効果のトレードオフ誤差が出やすいため, 解釈には注意が必要と思われる.

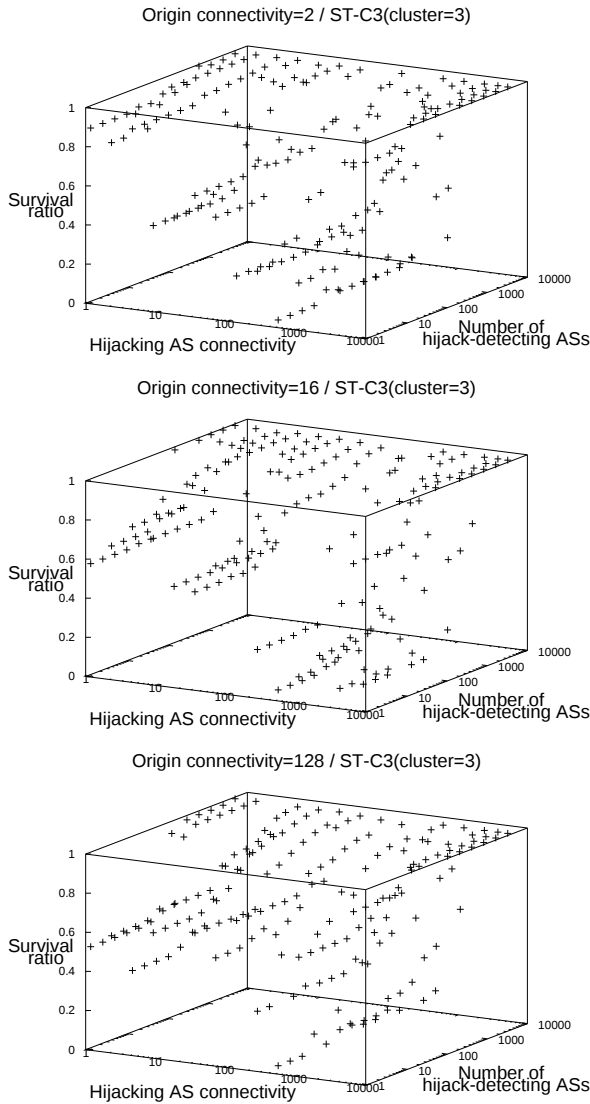


図 10 本来経路の生存割合 (ST-C3:cluster=3)

Fig. 10 Ratio of correct routes: Effectiveness of validity-check ASes against route hijacking. (ST-C3:cluster=3)

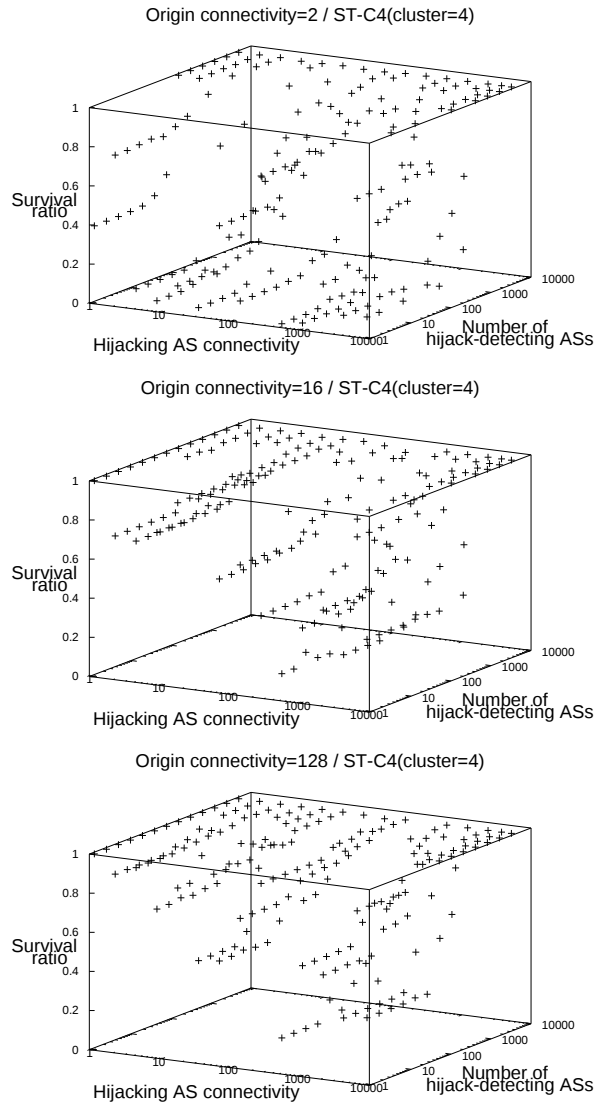


図 11 本来経路の生存割合 (ST-C4:cluster=4)

Fig. 11 Ratio of correct routes: Effectiveness of validity-check ASes against route hijacking. (ST-C4:cluster=4)

4. 議論

現実の BGP で広報される経路は、32 ビットの IP アドレス prefix であり、一つの AS が任意の長さのネットマスクを持つ複数の prefix を広報する。ネットマスクの異なる prefix は別 prefix としてそれぞれ広報・分散され、それぞれの AS の BGP 経路表に存在する。IP パケットの経路のフォワード先検索では、よりネットマスク長の長いロングストマッチ経路が優先されるため、本シミュレーションで用いた 1AS へ 1prefix の割当は、現実の経路分散とパケットフォワードと異なるが、経路ハイジャックとして捉えた場合の振舞の基本挙動は同じと考えられる。

ハイジャック検知 AS のクラスター構成に関しては、今回はあくまで総 AS 数で各戦略の比較を行ったが、観測ポ

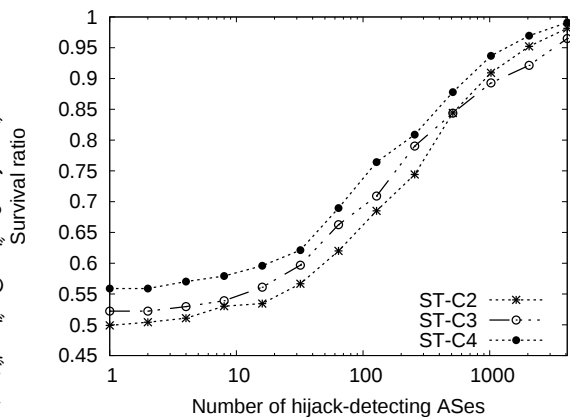


図 12 本来経路の平均生存割合 (ST-C2,3,4)

Fig. 12 Ratio of average correct routes: Effectiveness of cooperative validity-check ASes. (ST-C2,3,4)

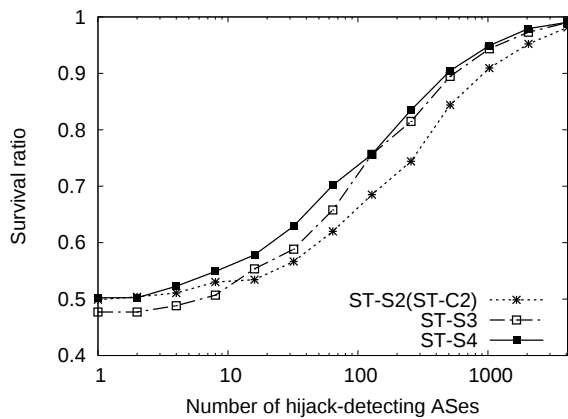


図 13 本来経路の平均生存割合 (ST-S2,3,4)

Fig. 13 Ratio of average correct routes: Effectiveness of cooperative validity-check ASes. (ST-S2,3,4)

イント数で比較する視点もあり、現実を導入した場合に近いシナリオとも言える。また、総 AS 数が少ない場合のバイアスなどが少ないことも想定され、今後はこちらの視点の評価も加えていきたい。

またサンプリングに関しては、時間の制約により、少ない同一接続数の AS の選択 (同一接続数の AS から、今回は 5AS を選択)、接続数の設定もログスケールとしたため、より詳細な実験も行っていく予定である。また、各接続数に属す AS 数の偏りも小さくないため、サンプリングの行い方も調整していく必要があると思われる。

5. 結論

本報告では、インターネットを AS と BGP 接続関係からグラフ構造として捉え、特に経路情報の拡散に関して、その基本解析を行った。解析に関しては、現在においても AS 間経路制御の重要な問題の一つである経路ハイジャックに注目し、その検知防御において、さまざまな AS 間協調動作を設定し、その有効性を解析した。解析にあたっては、AS 間の BGP 接続関係を記述する公開データから、BGP 経路情報をシミュレーションするシステムを作成し、実験を行った。協調する隣接 AS は、BGP 接続数の多い AS、あるいは、provider/peer から選択することで、少数の観測ポイントでも有効性を上げられる可能性を定量的に示した。今後は、戦略の有効性解析の詳細化を進め、新たな隣接 AS 協調戦略に関しても、その有効性解析を進めていく予定である。

謝辞

本研究は JSPS 科研費 19K24358 の助成を受けたものである。

参考文献

- [1] Rekhter, Y., Li, T. and Hares, S.: A Border Gateway Protocol 4 (BGP-4) (2006). RFC4271.
- [2] The North American Network Operators' Group: <https://www.nanog.org>.
- [3] Loibl, C., Hares, S., Raszuk, R., McPherson, D. and Bacher, M.: Dissemination of Flow Specification Rules (2020). RFC8955.
- [4] Faloutsos, M., Faloutsos, P. and Faloutsos, C.: On Power-law Relationships of the Internet Topology, *ACM SIGCOMM Computer Communication Review*, Vol. 29, No. 4, pp. 251–262 (1999).
- [5] Barabási, A.-L. and Albert, R.: Emergence of Scaling in Random Network, *Science*, Vol. 286, pp. 509–512 (1999).
- [6] Akashi, O.: Analysis of Cooperative Management Strategies against Route-Hijacking, *1st IFIP/IEEE Workshop on Managing Federations and Cooperative Management (In conjunction with IM11)* (2011).
- [7] CAIDA: AS Relationships. <https://www.caida.org/data/as-relationships/>.
- [8] Allegro Common Lisp: <https://www.franz.com>.