BGPsecの評価に向けた 実験用エミュレーションプラットフォームSQUABの改良

梅田 直希[1,a)] 矢内 直人[1] 竹村 達也[1] 岡田 雅之[2] 岡村 真吾[3]

概要：BGPsec はインターネットの屋台骨として知られる Border Gateway Protocol (BGP) に, 電子署名を導入することでインターネット経路情報の正当性を確保するプロトコルである. BGPsec の実験評価は十分に進んでいないことから, 著者らは近年に汎用的な BGP 拡張プロトコルの評価用プラットフォームとして SQUAB (Scalable QUagga-based Automated configuration on Bgp, AINA 2021) を提案した. しかし, SQUAB の既存機能ではネットワークトポロジの記述及び経路収束の確認をユーザが手動で行わなければならないことから, 大規模なネットワークの実験には不向きであった. 本稿では, SQUAB に RIPE RIS で公開されている AS トポロジ情報から該当ネットワークを定義するファイルを自動で生成する機能を新たに導入する. また, ルータ間の通信データを取得する機能もあわせて導入する. BGP ルータのみのネットワークと BGPsec 混在ネットワークの比較実験においては, 経路選択に違いが見られた一方で, 収束時間には有意な差が見られないことが明らかになった.

1. はじめに

1.1 背景

Border Gateway Protocol (BGP) [23] は自律システム (AS) と呼ばれる単位でインターネット経路を交換する事業者間プロトコルとして知られているいるが, その経路情報に関する正当性は保証されていない. このため, 経路ハイジャックと呼ばれる, 誤った経路情報が広告されることで AS 単位（すなわち事業者単位）でネットワークを遮断する攻撃が可能である. これまでの実態調査によると, 平均して一日 4.7 件程度の経路ハイジャックが発生している [35]. このような背景を受けて, BGP に電子署名を導入することで経路情報の正当性を保証する BGPsec [15] が登場している.

BGPsec の機能のうち, 経路の広告元を保証する Route Origin Validation (ROV) は普及しつつある. また, 各事業者と一意に管理される AS 番号の紐づけを保証する RPKI も広く浸透している [5]. すなわち, 既にインフラそのものは整いつつある状況といえる. 一方で, AS 間で交換される経路情報の正当性を保証する機能である Path Validation は, 著者らが認識している限りでは普及が進んでいない. これには, BGPsec の中でも Path Validation に関する評価データが不足している点が大きいといえる.

1.2 本研究の学術的問いと技術的課題

本研究では, BGPsec の Path Validation の評価として, 以下の問いを明らかにする: **BGPsec Path Validation と BGP の経路収束に違いがあるのか？** BGP の拡張は経路の収束時間を増加させる可能性が知られており [24], BGPsec においても同様に経路収束が遅くなることが予想される. BGP と BGPsec が混在する環境では経路情報のセキュリティが改善されないことが既存の結果 [16] として知られている. このため, BGPsec Path Validation の経路収束が長引く仮説が事実であるならば, BGP と BGPsec が混在する過渡期においては, むしろ攻撃しやすい AS が発生する可能性も予想される. このため, 上述した問いは明らかにされるべきといえる.

上述した BGPsec の評価に向けて, 著者はこれまでに BGP 用実験プラットフォーム SQUAB [34] を開発している. 大まかには, SQUAB は BGPsec と BGP が混在する環境での実験評価を実現している. 一方, SQUAB の既存機能では入力となる経路情報を手作業で設定する必要があった. これは現実世界における経路収束を評価できるような大規模なネットワークに相当する実験環境の構築が, 容易ではないことを意味する. 加えて, SQUAB は経路の収束を判定する機能がないため, 各 AS のルーティングテーブルを目視で確認する方法しかなかった. AS の数が増えた

[1] 大阪大学
[2] 長崎県立大学
[3] 奈良工業高等専門学校
[a)] n-umeda@ist.osaka-u.ac.jp

場合, この確認作業も手間となり, 現実的には収束確認をすることができない. 以上のことから, SQUAB の従来機能では, 大規模なネットワークにおける評価が容易ではない.

一方, 既存の BGP 実験用プラットホーム [25] もあるが, これらは単一の AS を通じて実際のトラフィックを収集解析 [25] することが主な機能である. このためネットワーク全体を俯瞰的に眺めることができず, 実験を通じて得られた結果ではネットワーク全体における収束を評価することができない.

1.3 貢献

本研究では実験用プラットフォーム SQUAB の拡張を通じて, BGP ルータのみのネットワークと BGPsec が混在するネットワークにおける経路収束の違いを議論する. 具体的に, まず経路収束を自動的に確認できる機能と BGP 経路情報の公開データベースである RIPE RIS と連携する機能を SQUAB に導入した. これにより, 将来的には大規模なネットワークにおける実験も期待できるようになった. 詳細は 4 に記載する.

拡張した SQUAB を用いて評価をした結果, BGPsec が混在するネットワークにおいては, 収束した経路情報内に BGPsec 対応ルータが属する AS の出現率が減少する一方で, ネットワーク全体での経路の収束時間に有意な差は見られなかった. 著者らが知る限り, BGP と BGPsec が混在する環境において経路収束の違いの検討は, 本研究が初めてである. 詳細は 5 に記載する.

2. 前提知識

本節では本研究における前提知識として, BGP と BGPsec, および関連研究について紹介する.

2.1 BGP と BGPsec

2.1.1 Border Gateway Protocol

BGP は, 構成単位となる各 AS が到達可能性情報, すなわち IP プレフィックスと AS 間のつながりを表す `AS_PATH` を隣接する AS に Update Message として広告する. 各 AS は受け取った情報と予めオペレータに定義された静的ポリシに基づいて各 IP プレフィックスへの最適経路を一つだけ決定し, 自身の AS 番号を `AS_PATH` の先頭に付加して隣接 AS に広告することによって, 宛先となる IP プレフィックスに到達するまで `AS_PATH` を模索する.

このとき, 宛先となる IP プレフィックスに対する到達可能経路が複数あったとしても, 選択される最適経路は基本的に 1 つだけとなる. オペレータは設定として, 物理的に隣接している AS の情報, AS 間での経路情報の送受信に関するポリシなど様々な設定が求められる. しかしながら, BGP の設定は複雑であるため, 専門家でも BGP のミスコンフィグレーションが起こりえる [25]. 一方, 各 AS のオペレータは自身の AS だけ設定するため, インターネット全体を俯瞰的に管理するような機構は持たない. つまり, ミスコンフィグレーションや経路ハイジャックなどが発生しても, 従来の BGP では検知できない.

2.1.2 Border Gateway Protocol Security Extension

BGPsec [15] は経路情報に電子署名を付加することで, `AS_PATH` の正当性を確認できるプロトコルである. より正確には, 電子署名と `BGPsec_PATH` 属性が新たに定義されており, この正当性を確認する. `BGPsec_PATH` 属性は, `Secure_PATH` と `Signature_Block` によって構成される. `Secure_PATH` は経路情報が通過してきた各 AS の AS 番号をリスト化したものであり, 従来の `AS_PATH` と同等である. 一方, `Signature_Block` は `Secure_PATH` の中の各 AS が付加した電子署名を格納するところである. なお, IP プレフィックスは RPKI [14] により保証される.

2.2 関連研究

本節では, BGP に関する実験用ツール・ネットワーク実験用テストベッド開発の観点での関連研究, および BGP のセキュリティと運用上の問題に関わる既存研究を紹介する.

2.2.1 BGP に関する実験用ツール

BGP に関する実験用ツール [4], [18], [22], [31] は多数存在するが, これらは実在する AS 群など現実世界におけるエコシステムとの相互的作用をなすことは難しい. つまり, 実際の AS における現在の方針との接続性を含めた評価が制限されることを意味している. 一方で, PEERING [25] は現実世界のエコシステムまで考慮した初のツールである. しかしながら, PEERING は BGP の単一の AS の境界を通じたエコシステムのみにおける実験に特化しており, インターネット全体を俯瞰的に捉えたような各 AS の接続性を測定する実験には不向きである.

2.2.2 ネットワーク実験用テストベットの開発

CloudLab[*1], XSEDE [*2], Emulab[*3]など多くのテストベッド環境は計算資源としてハードウェアを提供している. 特に, Emulab はネットワーク実験に特化したテストベッド環境であり, EPIC [27] や DETER [28] の様に Emulab をベースとして各用途に合わせて拡張したツールも多く存在している. Emulab は計算リソースだけではなくネットワーク遅延を表現したネットワークの接続性も実験環境として提供する. しかしながら, Emulab の使用は大学教授など研究プロジェクトの責任を持つことができる人などユーザが制限されており, その承認手続きに時間を消費する場合がある. また, PlanetLab[*4] や WIDE[*5] では参加者が計

[*1] https://www.cloudlab.us/
[*2] https://www.xsede.org/
[*3] https://www.emulab.net/portal/frontpage.php
[*4] https://planetlab.cs.princeton.edu/
[*5] https://www.wide.ad.jp/

算機資源を持ち寄ってネットワークを構成することによって実験環境を共有している．しかしながら，参加者はグローバル IP アドレスが割り当てられて Linux が動作している計算機を二台提供するなど，いくつかの条件を満たす必要がある．上述したテストベッドと比較して，SQUAB は計算コストが軽量なコンテナをベースとしているため，第三者のリソースなしでも一般的なノートパソコン一台のみで実験を行うことができる．それゆえに，誰でも SQUAB を利用して実験を素早く開始することが可能である．SQUAB に最も類似したツールは DOCKEMU [32] であり，Docker を利用して実験用ネットワーク環境を構築する．しかしながら，DOCKEMU はネットワークシミュレータ NS-3[*6] に基づいている一方，SQUAB は Docker の利点を生かしてネットワークのエミュレーションを提供している．

2.2.3 BGP のセキュリティと運用上の問題

BGP セキュリティの研究は文献 [12] に始まり，これは経路生成元が作成する証明書と経路を受け取った各 AS が作成する証明書を利用して経路情報の不正を明らかにする方法であるが，計算負荷などの問題で普及しなかった．BGP の安全性と計算負荷などのトレードオフを考慮し，Secure Origin BGP（soBGP） [37] や Pretty Secure BGP（psBGP） [36] が提案された．しかしながら，従来の BGP との相互作用によって新たな脆弱性が引き起こされることにより，安全性が低下するといった課題が生じた [11]．

近年では BGP への更なる攻撃の調査 [2], [3], [10], [19] も発展が著しく，BGP の攻撃を介して暗号通貨を盗む攻撃 [1], [7], [33] も確認された．また，近年では DoS 攻撃などサイバー攻撃を緩和させるために，あえて BGP の経路ハイジャックを行うブラックホールサービスの普及も進んでいる [8], [13], [21], [30]．これらの攻撃含め実世界の BGP の運用は，BGPsec の導入が実現すれば制御が可能である [29]．一方で，Lychev ら [16] や Morillo ら [20] は BGPsec が完全に展開しない限り BGP のセキュリティは改善されないと述べている．BGP のセキュリティの運用面での研究として，従来の BGP とその任意の拡張機能の間の相互運用を支えるために D-BGP [24] と呼ばれれる用途の広いプロトコルが提案された．

BGP セキュリティにおいて最も進んでいる研究領域は，経路情報の受け取り先を限定するフィルタリング [9] であり，高い確率で経路ハイジャックを防げることが示されている [17], [26]．しかしながら，これらのアプローチでは他の事業者が経路ハイジャックの事実を観測することが難しい．また，前項で述べたようなブラックホールサービスへの適用が難しいという指摘 [29] もある．直観的には，フィルタリングなどは計算コストがかからないものの確実に安全性を保証することはできない．

*6 https://www.nsnam.org/

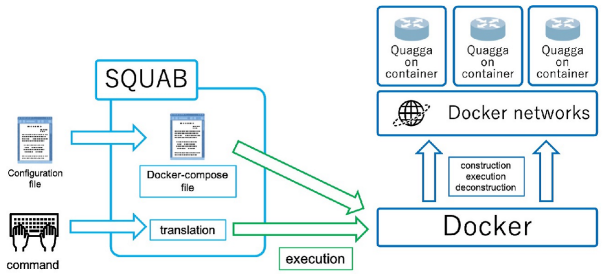

図 1 SQUAB のアーキテクチャ

BGPsec の社会実装としては，BGPsec で利用する公開鍵を管理するリソース公開鍵基盤 (RPKI) [14] が挙げられる．こちらは完全に標準化されており，展開と有効性は既に確認されている [5]．さらに，BGPsec の参照実装として BGP-SRx[*7], The BGPsec enabled Bird Routing Daemon[*8], FRRouting[*9], GoBGP[*10]がいくつか公開されており，本稿では Quagga ベースのソフトウェアルータである BGP-SRx を利用して SQUAB を開発した．

3. SQUAB

SQAUB [34] は，仮想環境上に BGPsec 対応ルータと BGPsec 非対応ルータ（すなわち BGP 対応ルータ）で構成されるネットワークを簡単に構築できる実験用プラットフォームである．本節では SQUAB の機能概要と従来機能の問題点を述べる．

3.1 概要

SQUAB は BGP ソフトウェアルータ Quagga[*11] 及び BGPsec ソフトウェアルータ BGP-SRx を仮想コンテナに搭載することで，BGP ネットワークの設定を自動化できる．主な機能としては，ユーザが AS，BGP ルータの機能，及び AS 間の接続をインターフェースを通じて設定することで，その設定情報に従い BGP あるいは BGPsec 対応ルータを搭載した仮想コンテナ群からなるネットワークを自動生成する．設定が完了した段階で，各ルータは相互に接続され，実験が開始できるようになっている．

SQUAB では仮想コンテナを要素技術として用いることで，実験環境が軽量に動作する利点を持つ．従来の実験環境が仮想マシンを軸にハードウェアから仮想化することに対し，仮想コンテナはアプリケーションレベルで仮想化する．このため，仮想化する機能を大幅に削減することで，軽量な実験が可能となる．なお，仮想コンテナには Docker[*12] コンテナを用いている．SQUAB の全体像を図 1 に示す．

*7 https://www.nist.gov/services-resources/software/bgp-secure-routing-extension-bgp-srx-prototype
*8 http://www.securerouting.net/tools/bird/
*9 https://github.com/FRRouting/frr
*10 https://osrg.github.io/gobgp/
*11 https://www.quagga.net/
*12 https://www.docker.com/

3.2 既存の問題点

SQUAB の現状の問題点は大きく二つある．(1) 経路収束の確認方法があいまいなこと, また, (2) 大規模なネットワークの環境構築が手作業で行わなければならないことである．これらの問題を解決した機能の導入が, 大規模なネットワークの経路収束の評価には必要となる．以下にそれぞれの問題点の詳細を述べる．

まず前者について, SQUAB では経路収束を自動的に判定する機能がなく, ユーザが目視で確認しなければならない．BGP において, 経路情報の収束を確実に判断する方法は, ネットワーク全体で新たな経路の広告を表す Update Message のやりとりがなくなったことを確認することである．しかし, SQUAB の既存の機能では, やりとりされるデータを観測する方法が提供されておらず, 各 AS ルータが持つルーティングテーブルを目視で判断せざるを得なかった．大規模なネットワークにおいては全てのルータのルーティングテーブルを目視で確認した上で, 収束したと判断することは容易ではない．

次に後者について, SQUAB は実験対象とするネットワークのトポロジを所定の形式で記述しなければならない．より現実に即した実験を行うためには, インターネット上に実際に流れている経路情報を元にした現実のトポロジを扱う必要がある．このとき, 扱うべきトポロジのデータは様々公開[*13]されてはいるものの, それを目視で SQUAB が扱える形にすべて変換することは現実的ではない．

4. SQUAB の拡張

本節では本稿における SQUAB の拡張機能について述べる．本稿で導入する SQUAB の拡張機能は大きく二点である．まず, 経路収束の確認機能である．構築されたネットワーク上を流れる Update Message の状態をツール側で抽出することで, 経路が収束しているか自動的に確認できるようになった．次に, 既存のトポロジ公開データベースである RIPE RIS との連携機能である．大まかには SQUAB に対して実在するネットワークトポロジを自動的に取得・入力することで, ネットワークの構築が効率的に行えるようになる．

4.1 経路収束の確認機能

経路収束の確認機能として, 観測データの直近のデータを確認し, そこに Update Message が含まれているかどうかを確認する機能を導入した．これにより, ネットワーク全体での収束を評価する．

まずネットワーク全体で, BGP の経路が収束しているか確認する最も確実な方法は, 経路の追加・削除を表す Update Message が送信されていないことを確認することである．ネットワーク上に流れるデータを観測するには, `tcpdump` を用いることが一般的であり, 各コンテナの全ネットワークインターフェースカード (NIC) を `tcpdump` で観測することで, ネットワーク全体の通信のデータを収集することが可能である．SQUAB では, BGP 通信のみを観測すればよいため, BGP で利用する TCP/179 ポートを観測する機能を実装している．観測したデータはコンテナ内に蓄積される．併せて, 全てのコンテナから観測データを一括して取り出す機能も実装した．

4.2 RIPE RIS との連携機能

RIPE RIS との連携機能として, RIPE RIS のデータ形式を SQUAB の入力ファイルに変換するスクリプトを実装することで, スクリプトに引数を与えるだけで, 実存するトポロジを記述した Config ファイルを生成できるようにした．

より具体的には, インターネットスケールの制御情報に関する公開データセットである RIPE RIS に対し, AS PATH 経路情報を可視化・収集できる BGPlay [6] の API が公開されている．BGPlay は, 対象となる AS を指定することで, その AS が含まれる全ての AS PATH 経路情報を入手できる．この BGPlay から得られるデータを SQUAB Config ファイルに変換するスクリプトを実装している．これにより, Config ファイルを自動生成できるようになったことで, ネットワークの構築が容易になった．

5. 実験

本節では拡張版 SQUAB を用いた実験について述べる．とくに BGPsec 対応ルータを導入した際の経路収束への影響を議論する．

5.1 実験目的

BGP と BGPsec が混在した環境で, 経路収束に際してどのような影響の違いがあるか評価する．具体的には, (1) 経路選択に違いがあるか, また, (2) 経路の収束時間に違いがあるのかを明らかにする．

この確認にあたり, 以下の実験を行う．まず (1) について, ネットワーク全体で経路が収束した際に, 各ルータのルーティングテーブルに含まれるターゲットとする AS の数を数える．ターゲットとする AS とは, ある実験パターンでは BGPsec 非対応ルータを導入し, また別の実験パターンでは BGPsec 対応ルータを導入する AS のことである．もし同じトポロジのネットワークに対して新たに BGPsec 対応ルータを導入した際に, 導入前の同一トポロジと比べて経路が異なっているようであれば, 経路の選択方法が BGPsec 導入により変化しているといえる．

次に (2) について, 各 AS ルータが経路広告を開始して

[*13] RIPE RIS Raw Data: `https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris/ris-raw-data`

からネットワーク全体で経路が収束するまでの時間を計測する. (1) と同様, 同じトポロジのネットワークに対して新たに BGPsec 対応ルータを導入した際に, 導入前のネットワークと比べて収束時間がどれくらい異なっているか確認する. とくに, 既存のルータが BGPsec 対応ルータに置き換わった割合に対して, どの程度の収束時間の増加が引き起こされるかを明らかにする.

5.2 実験設定

上述した二つの実験における設定をそれぞれ以下に述べる.

5.2.1 経路選択の違いの評価

あるトポロジにおいて, BGP ルータが BGPsec 対応ルータに置き換わった時に, 経路の選択に違いが生まれるか評価する. とくに, 一部の AS の境界に設置されているルータを BGPsec に変更することで, 各 AS が持つ経路情報に変化が生まれるかを調べる.

具体的に, 全 AS の識別子集合を N とし, あるルータを BGPsec 非対応あるいは BGPsec 対応にしたときに, 以下の計算を経路収束時における評価方法として用いる:

$$\frac{\sum_{i \in Route} \sum_{j \in T} |\{AS_{i,j}\}|}{\sum_{i \in Route} \sum_{j \in N} |\{AS_{i,j}\}|} \quad (1)$$

ここで, 任意の i, j において, $AS_{i,j}$ は T あるいは N, かつ, $Route$ 両方の集合に含まれる単一 AS, $T \subseteq N$ は BGPsec 対応ルータへ置き換える対象となったルータが属する AS の識別子集合, $Route$ は N に属する全てのルータが持つ最適経路の識別集合とする. すなわち, ある $AS_i \in N$ が持つ最適経路を R_i としたときに, $Route = \bigcup_{i \in N} R_i$ となる. なお, {} は集合を定義する演算子, || は集合の要素を数える演算子をそれぞれ意味する.

つまり, (1) 式は T あるいは N, かつ, $Route$ 両方の集合に属する単一の AS から定義される要素数 1 の集合をそれぞれ定義し, かつ, その総数を数えている. これにより, T に属するルータが BGPsec 対応ルータに置き換えられたとき, (1) 式の値が増減するかで, 経路選択の違いを評価している. 直観的には, 置き換えの前後における数値の変化が小さいほど, 影響が小さいといえる.

なお, この実験をするにあたって, 図 2 で示すトポロジを利用した. また, 経路収束の確認には, 新たに導入した経路収束の確認機能を利用している.

また, 全ルータが BGPsec 非対応ルータのネットワーク, かつ, T に 3 個の AS（全体の 10%に相当する）が属するとき, T に属する AS を BGPsec 非対応ルータとした実験を実験パターン A, T に属する AS を BGPsec 対応ルータに置き換えた実験を実験パターン B とする. 同様に, 全ルータが BGPsec 非対応ルータのネットワーク, かつ, T に 12 個の AS （全体の 40%に相当する）が属するとき, T に属する AS を BGPsec 非対応ルータとした実験を実験パターン C, T に属する AS を BGPsec 対応ルータに置き換えた実験を実験パターン D とする.

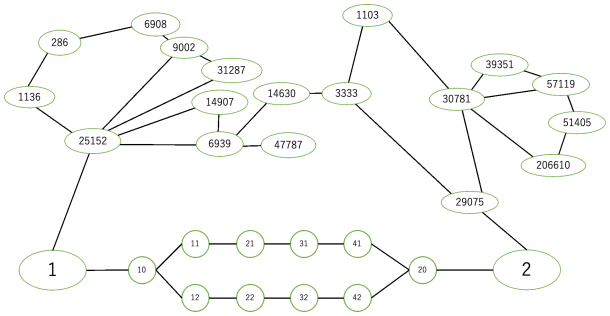

図 2 実験で利用したトポロジ

5.2.2 収束時間の違いの評価

BGPsec 対応ルータの台数が増加するごとに, ネットワーク全体で経路収束に至るまでの時間がどのように変化するか計測する.

具体的に, 前節の実験同様, 全ルータの集合を N とし, あるルータを BGPsec 非対応あるいは BGPsec 対応にしたとして, その置き換える対象となったルータが属する AS の集合を T とする. このとき, ルータの台数を増やすこと, すなわち, $|T|$ を大きくした際の経路の収束時間をそれぞれ計測する. 計測方法としては, ネットワーク全体で最初にキャプチャされたパケットの時刻と, 最後の Update Message の時刻を評価する. 直観的には $|T|$ を大きくしても収束時間が変わらないならば, 影響が小さいといえる.

この実験でも経路選択の違いの評価同様に, 図 2 で示すトポロジを利用した. また, 経路収束の確認には, 新たに導入した経路収束の確認機能を利用している.

実験パターンについても同様に, 全ルータの集合 N が BGPsec 非対応ルータのネットワーク, かつ, T に 3 個の AS が属するとき, T に属する AS を BGPsec 非対応ルータとした実験を実験パターン A, T に属する AS を BGPsec 対応ルータに置き換えた実験を実験パターン B とする. また, T に 12 個の AS が属するとき, T に属する AS を BGPsec 対応ルータに置き換えた実験を実験パターン C とする.

5.3 実験結果

5.3.1 経路選択の違いの評価

5.2.1 節に述べた実験パターン A, 実験パターン B, 実験パターン C, 実験パターン D それぞれのネットワークで経路が収束するまで実験を行い, それぞれで (1) 式に基づいた計算を行った. その結果を, 図 3, 4, 及び図 5, 6 に示す. また, その際に BGPsec 対応ルータとして数え上げた絶対数（すなわち (1 式の分子) を表 1, 及び表 2 に示す.

実験パターン A から実験パターン B, 及び, 実験パターン C から実験パターン D 両方の場合において (1) 式の数値が下がっていることから, BGPsec 対応ルータに置き換えられたことにより, 経路選択に明らかな違いがみられて

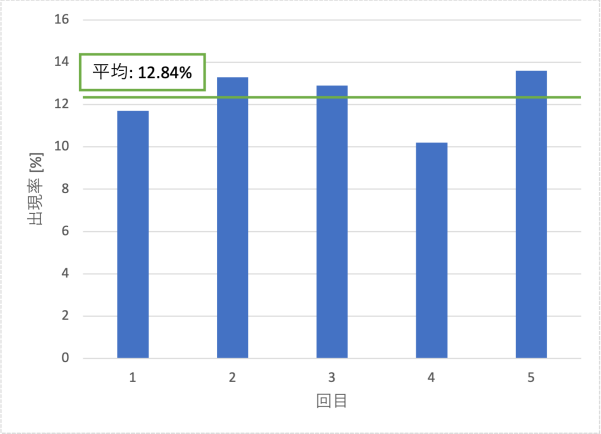

図 3 実験パターン A での出現率

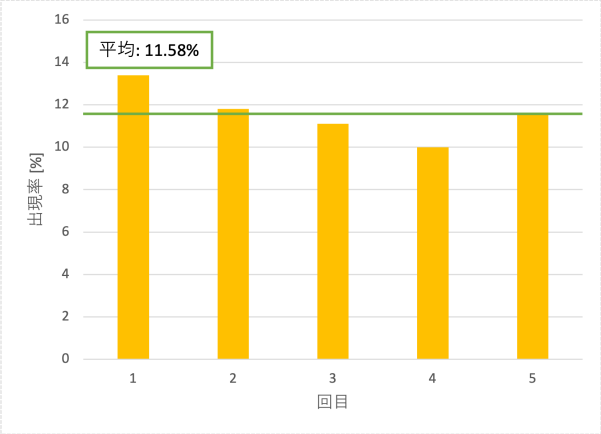

図 4 実験パターン B での出現率

表 1 全体の 10% の AS を置き換え対象の AS 集合 T としたときの絶対数
(全体数はいずれも 3926 個の AS)

実験パターン	1	2	3	4	5	平均
A	462	526	510	404	534	487.2
B	529	467	439	395	456	457.2

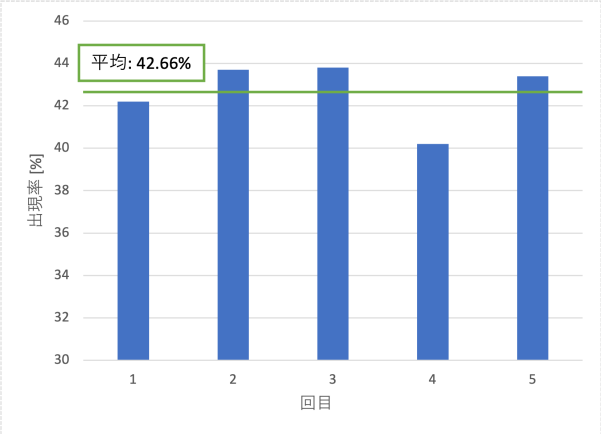

図 5 実験パターン C での出現率

いる. なお, 分母の数値は変化が見られなかったことから, 分子のみが変化している. すなわち, BGPsec 対応 AS の出

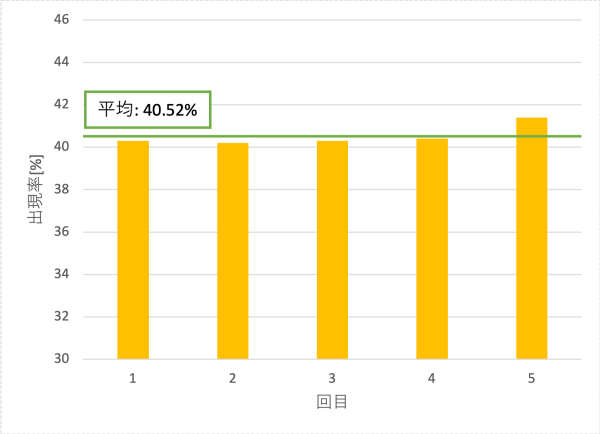

図 6 実験パターン D での出現率

表 2 全体の 40% の AS を置き換え対象の AS 集合 T としたときの絶対数
(全体数はいずれも 3926 個の AS)

実験パターン	1	2	3	4	5	平均
C	1660	1717	1721	1580	1707	1677
D	1585	1580	1583	1589	1626	1592.6

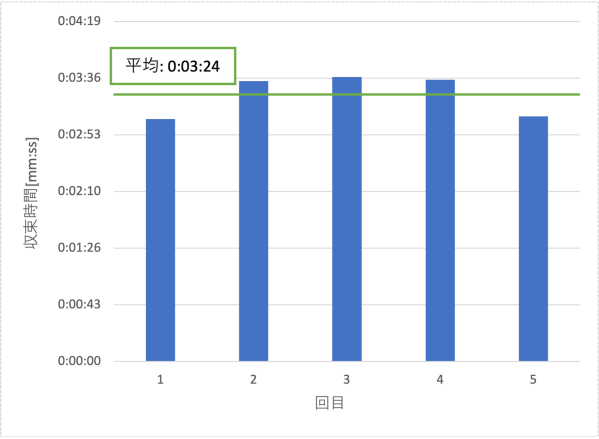

図 7 実験パターン A での収束時間

表 3 経路収束時間

実験パターン	1	2	3	4	5	平均
A	03:05	03:34	03:37	03:35	03:07	03:24
B	03:06	03:34	03:37	03:36	03:08	03:24
C	03:34	03:36	03:35	03:05	03:39	03:30

現割合のみが低下していることがわかる.

5.3.2 収束時間の違いの評価

5.2.2 節で述べた実験パターン A, 実験パターン B, 実験パターン C それぞれのネットワークで経路が収束するまで実験を行い, その結果を図 7, 8, 及び図 5 に示す. また, それぞれの実験で計測した時間の実測値を表 3 に示す.

6. 考察

本節では前節の実験結果を踏まえて, 経路選択の違い, 及び, 収束時間の違いについて, それぞれ考察する.

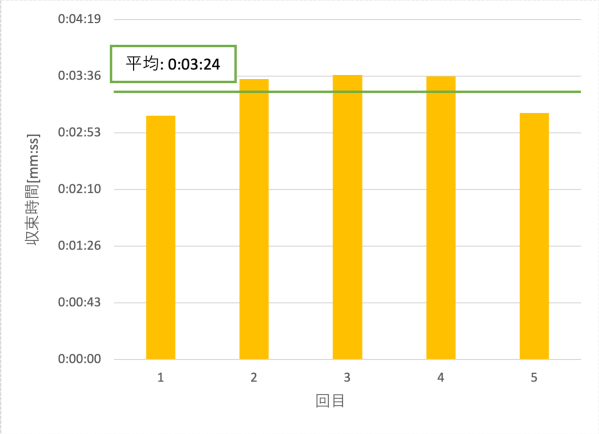

図 8 実験パターン B での収束時間

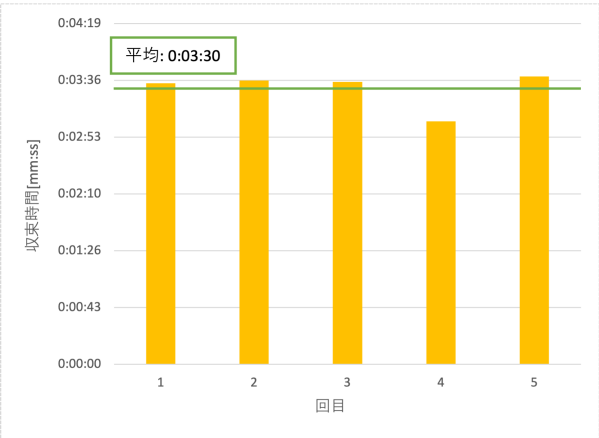

図 9 実験パターン C での収束時間

6.1 経路選択の違いの評価

5.3.1 節に述べたとおり, BGPsec 対応 AS の出現数の減少の傾向が見られた. 一見するとわずかな違いに見えるが, 以下に述べる理由から, 有意な違いと考えられる.

まず, BGP における最適経路は原則として最小ホップ数によって選択される. このため, 仮に一部のルータの処理速度が遅かったとしても, ある AS からある AS への経路で最適経路が一つしかない場合は, 十分な時間を待つことで, その経路に必ず収束する. 一方で, そうならない状況としては, ある AS からある AS への経路として最小ホップ数となる経路が複数存在する場合がある. このとき, 様々な偶然により, ある経路が最適として選ばれることがあれば, 別の経路が選ばれる場合もある. BGPsec 対応ルータの処理速度の遅さは, このような場合において影響が出てくることとなる. つまり, BGPsec 対応ルータを含む経路の到達が遅れ, 最適経路としてはより選ばれにくくなっていると考えられる.

なお, 本稿の実験では BGPsec 対応ルータが最適経路として選ばれにくい傾向がみられたが, 各 AS の設定において, 特定の AS からの経路の優先や特定の属性を含む経路を優先するなど AS 固有の設定は行なっていない. このため, 実際の運用においては, そのような優先制御を考慮することで, BGPsec 対応 AS を含む経路情報を積極的に取り込んでいくことが重要と考えられる.

6.2 収束時間の違いの評価

実験結果によると, 経路収束時間の分散も大きいことから, 収束時間には有意な違いが発生していないと考えている. また, その原因として, 電子署名の計算時間よりも BGP 自体の通信時間の方が時間がかかっているためと考えられる.

一方で, 本稿の実験環境では, BGPsec 対応ルータは RPKI の通信を含めていない. このため, RPKI との通信を含めると, BGPsec 対応ルータを含むことで収束時間に大きな差が出ると考えられる. これは電子署名の計算よりも通信時間が大きな影響を持つことにも起因している. RPKI をエミュレートする機構をインターネットを挟んだ別の場所に設置し同様の実験を行うことで, BGPsec 対応ルータによる違いが発生するか確認することが今後の課題である.

また, ネットワーク全体で収束時間がほとんど変化がなかった一方で, 経路選択には違いが発生していることから, 経路選択の違いは僅かなタイミングの差で発生している可能性が高いと考えられる.

7. まとめ

本稿では BGPsec と BGP が混在するネットワーク環境の評価に向けて, 実験用プラットホーム SQUAB [34] の拡張機能を設計した. 拡張機能はネットワーク上で経路収束を自動的に判定できる経路収束の確認機能と, ネットワーク設定用の Config ファイルを RIPE RIS データベースのデータから自動生成する RIPE RIS との連携機能である. これらにより, 大規模なネットワークにおける実験も, 容易に環境構築できるようになる.

SQUAB の拡張機能を用いて BGPsec と BGP が混在するネットワークと, BGP ルータのみのネットワークを比較する実験を行ったところ, 最終的な経路の収束結果として経路選択に違いが見られた一方で, 収束時間については有意な差が見られなかった. この結果から, 経路選択の違いは僅かなタイミングの差で発生していることが示唆される.

実際のインターネット上で観測されるネットワークトポロジを反映するような大規模実験の実施は, 今後の課題である.

謝辞: 本研究の一部は JSPS 科研費・若手研究 18K18049, 及び, 文部科学省 Society 5.0 実現化研究拠点支援事業により支援されている.

参考文献

[1] Apostolaki, M., Zohar, A., Vanbever, L.: Hijacking bitcoin: Routing attacks on cryptocurrencies. In: Proc. of

IEEE S&P 2017. pp. 375–392. IEEE (2017)
[2] Ballani, H., Francis, P., Zhang, X.: A study of prefix hijacking and interception in the internet. In: Proc. of SIGCOMM 2007. pp. 265–276. ACM (2007)
[3] Birge-Lee, H., Wang, L., Rexford, J., Mittal, P.: Sico: Surgical interception attacks by manipulating bgp communities. In: Proc. of CCS 2019. pp. 431–448. ACM (2019)
[4] Chen, K., Choffnes, D.R., Potharaju, R., Chen, Y., Bustamante, F.E., Pei, D., Zhao, Y.: Where the sidewalk ends: Extending the internet as graph using traceroutes from p2p users. In: Proc. of CoNEXT 2009. pp. 217–228. ACM (2009)
[5] Chung, T., Aben, E., Bruijnzeels, T., Chandrasekaran, B., Choffnes, D., Levin, D., Maggs, B.M., Mislove, A., Rijswijk-Deij, R.v., Rula, J., Sullivan, N.: RPKI is coming of age: A longitudinal study of rpki deployment and invalid route origins. In: Proc. of IMC 2019. pp. 406–419. ACM (2019)
[6] Di Battista, G., Mariani, F., Patrignani, M., Pizzonia, M.: Bgplay: A system for visualizing the interdomain routing evolution. In: Proc. of GD 2003. LNCS, vol. 2912, pp. 295–306. Springer (2004)
[7] Ekparinya, P., Gramoli, V., Jourjon, G.: The attack of the clones against proof-of-authority. In: Proc. of NDSS 2020. Internet Society (2020)
[8] Giotsas, V., Smaragdakis, G., Dietzel, C., Richter, P., Feldmann, A., Berger, A.: Inferring bgp blackholing activity in the internet. In: Proc. of IMC 2017. pp. 1–14. ACM (2017)
[9] Goldberg, S.: Why is it taking so long to secure internet routing? Queue **12**(8), 20–33 (2014)
[10] Goldberg, S., Schapira, M., Hummon, P., Rexford, J.: How secure are secure interdomain routing protocols. In: Proc. of SIGCOMM 2010. pp. 87–98. ACM (2010)
[11] Huston, G., Rossi, M., Armitage, G.: Securing bgp - a literature survey. IEEE Communications Surveys & Tutorials **13**(2), 199–222 (2011)
[12] Kent, S., Lynn, C., Seo, K.: Secure border gateway protocol (s-bgp). IEEE Journal on Selected areas in Communications **18**(4), 582–592 (2000)
[13] Kumari, W.A., McPherson, D.R.: Remote Triggered Black Hole Filtering with Unicast Reverse Path Forwarding (uRPF). RFC 5635 (Aug 2009). DOI: 10.17487/RFC5635, `https://rfc-editor.org/rfc/rfc5635.txt`
[14] Lepinski, M., Kent, S.: An Infrastructure to Support Secure Internet Routing. RFC 6480 (Feb 2012). DOI: 10.17487/RFC6480, `https://rfc-editor.org/rfc/rfc6480.txt`
[15] Lepinski, M., Sriram, K.: BGPsec Protocol Specification. RFC 8205 (Sep 2017). DOI: 10.17487/RFC8205, `https://rfc-editor.org/rfc/rfc8205.txt`
[16] Lychev, R., Goldberg, S., Schapira, M.: Bgp security in partial deployment: Is the juice worth the squeeze? SIGCOMM Computer Communication Review **43**(4), 171–182 (2013)
[17] Lychev, R., Schapira, M., Goldberg, S.: Rethinking security for internet routing. Communication of the ACM **59**(10), 48–57 (2016)
[18] Mao, Z.M., Rexford, J., Wang, J., Katz, R.H.: Towards an accurate AS-level traceroute tool. In: Proc. of SIGCOMM 2003. pp. 365–378. ACM (2003)
[19] Miller, L., Pelsser, C.: A taxonomy of attacks using bgp blackholing. In: Proc. of ESORICS 2019. LNCS, vol. 11735, pp. 107–127. Springer (2019)
[20] Morillo, R., Furuness, J., Herzberg, A., Morris, C., Wang, B., Breslin, J.: ROV++: Improved deployable defense against bgp hijacking. Internet Society (2021)
[21] Nawrocki, M., Blendin, J., Dietzel, C., Schmidt, T.C., Wählisch, M.: Down the black hole: Dismantling operational practices of bgp blackholing at ixps. In: Proc. of IMC 2019. pp. 435–448. ACM (2019)
[22] Peterson, L., Bavier, A., Fiuczynski, M.E., Muir, S.: Experiences building planetlab. In: Proc. of Usenix Security 2006. pp. 351–366. USENIX Association (2006)
[23] Rekhter, Y., Hares, S., Li, T.: A Border Gateway Protocol 4 (BGP-4). RFC 4271 (Jan 2006). DOI: 10.17487/RFC4271, `https://rfc-editor.org/rfc/rfc4271.txt`
[24] Sambasivan, R.R., Tran-Lam, D., Akella, A., Steenkiste, P.: Bootstrapping evolvability for inter-domain routing with d-bgp. In: Proc. of SIGCOMM 2017. pp. 474–487. ACM (2017)
[25] Schlinker, B., Arnold, T., Cunha, I., Katz-Bassett, E.: Peering: Virtualizing bgp at the edge for research. In: Proc. of CoNEXT 2019. pp. 51–67. ACM (2019)
[26] Sermpezis, P., Kotronis, V., Gigis, P., Dimitropoulos, X., Cicalese, D., King, A., Dainotti, A.: Artemis: Neutralizing bgp hijacking within a minute. IEEE/ACM Transactions on Networking **26**(6), 2471–2486 (2018)
[27] Siaterlis, C., Genge, B., Hohenadel, M.: Epic: a testbed for scientifically rigorous cyber-physical security experimentation. IEEE Transactions on Emerging Topics in Computing **1**(2), 319–330 (2013)
[28] Sklower, K., Joseph, A.D.: Very large scale cooperative experiments in emulab-derived systems. In: Proc. of DETER 2007. pp. 1–7. USENIX Association (2007)
[29] Smith, J.M., Birkeland, K., McDaniel, T., Schuchard, M.: Withdrawing the bgp re-routing curtain: Understanding the security impact of bgp poisoning through real-world measurements. In: Proc. of NDSS 2020. Internet Society (2020)
[30] Smith, J.M., Schuchard, M.: Routing around congestion: Defeating ddos attacks and adverse network conditions via reactive bgp routing. In: Proc. of IEEE S&P 2018. pp. 599–617. IEEE (2018)
[31] Staff, R.N.: Ripe atlas: A global internet measurement network. Internet Protocol Journal **18**(3) (2015)
[32] To, M.A., Cano, M., Biba, P.: Dockemu–a network emulation tool. In: Prc. of WAINA 2015. pp. 593–598. IEEE (2015)
[33] Tran, M., Choi, I., Moon, G.J., Vu, A.V., Kang, M.S.: A stealthier partitioning attack against bitcoin peer-to-peer network. In: Proc. of IEEE S&P 2020. pp. 496–511. IEEE (2020)
[34] Umeda, N., Yanai, N., Takemura, T., Okada, M., Cruz, J.P., Okamura, S.: Squab: A virtualized infrastructure for experiments on bgp and its extensions. In: Proc. of AINA 2021. LNNS, vol. 225, pp. 600–613. Springer (2021)
[35] Vervier, P., Thonnard, O., Dacier, M.: Mind your blocks: On the stealthiness of malicious BGP hijacks. In: Proc. of NDSS 2015. Internet Society (2015)
[36] Wan, T., Kranakis, E., van Oorschot, P.C.: Pretty secure bgp (psbgp). In: Proc. of NDSS 2005. IEEE (2005)
[37] White, R.: Securing bgp through secure origin bgp. The Internet Protocol Journal **6**(3), 47–53 (2003)