Computer Security Symposium 2020
26 - 29 October 2020

BGPsec の展開可能性に向けたBGP との同時運用の検討

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 は電子署名の利用を通じて BGP にセキュリティを導入したプロトコルである。しかしながら、BGPsec の普及は進んでいない。これは BGPsec の社会実装のしやすさ、すなわち展開可能性が不透明であることに起因する。本稿では BGPsec の展開可能性の改善に向けて、BGPsec と BGP の同時運用を検討する。とくに BGPsec と BGP の同時運用において、ルーティングの異常が発生しないか明らかにする。まず、上述した観点の測定に向けて、同時運用を行うためのソフトウェアルータ・プラットフォーム SQUAB を設計した。次に、RIPE RIS の経路データベースを参考に実際のネットワークを再現した環境において実験と評価を行った。実験結果として、経路情報の異常は確認されなかったが、BGPsec 非対応ルータが含まれる経路が選択される傾向があることが明らかになった。

キーワード：BGP, BGPsec, 同時運用, 展開可能性,

A Study on Deployability of BGPsec with BGP

Naoki Umeda[1,a)]　Naoto Yanai[1]　Tatsuya Takemura[1]　Masayuki Okada[2]　Shingo Okamura[3]

Abstract: BGPsec is a protocol for introducing the security into the border gateway protocol (BGP) by the use of digital signatures. Nevertheless, since social implementation of BGPsec, i.e., deployability, is unclear, deployment of BGPsec is still an ongoing work. In this paper, we discuss the inter-operation of BGPsec and BGP towards improvement of the deployability for BGPsec. More specifically, we discuss the deployability from the standpoint whereby an error of the routing is caused or not. To do this, we first present a software platform named SQUAB to conduct the inter-operation. Next, we experimentally evaluate the aforementioned standpoints based on an actual network environment by utilizing the RIPE RIS database for routing information. As a result, we confirm that an error of the routing is not caused, and routers tend to choice that the path includes BGPsec incompatible router.

Keywords: BGP, BGPsec, Inter-Operation, Deployability

1. はじめに

1.1 背景

Border Gateway Protocol (BGP) [1] は、各インターネット事業者ごとに構成している *Autonomous Systems (ASes)* と呼ばれる単位で経路情報の交換を行うプロトコルであり、各 AS には一意の番号が割り当てられている。BGP はインターネットの屋台骨として利用がなされている一方、交換されている経路情報の正当性を保証する機能が備わっていない。このため、攻撃者が不正な経路情報を送り出しても、ASes は受け取った情報を常に正しいものとして受理してしまう。この脆弱性を利用した経路ハイジャックの事例として、2008 年のパキスタンテレコムによる YouTube アクセス不能事件 [2]、2018 年の仮想通貨イーサリアムの窃盗事件 [3] などが挙げられる。2015 年の調査 [4] によると、このような事件は被害規模が大きい一方、一日平均 4 件 と多発している。これらの理由から、経路情報の正当性保証の導入は重要かつ緊急な課題となっている。

[1] 大阪大学. Osaka University
[2] 長崎県立大学. University of Nagasaki
[3] 奈良工業高等専門学校. National Institute of Technology, Nara College
[a)] n-umeda@ist.osaka-u.ac.jp

この問題に対し、電子署名を用いて BGP の安全性を保証する技術 [5] が注目されている。具体的には、経路の発信元である AS とその IP prefix の legitimate pair を保証する route origin validation と、AS がつながった path 上の members を保証する path validation がある。このうち、前者については RPKI [6] や ROA [7] [8] など関連する技術の実用化により解決されつつある。一方、後者を実現する技術として BGPsec [9] が知られているものの、実用化のめどがたっていない。また、BGPsec の標準化は 2011 年にその検討が開始したものの、標準化に向けた実装実験などは十分に行われておらず、実際にどの程度の効果があるかも不明である。

BGPsec の普及が進んでいないことは、BGP がインターネット基盤を支えるプロトコルとしてすでに広く普及しており、その拡張版の標準化や導入が困難であることに起因する [10]。一般に、インターネットのような広く定着しているインフラストラクチャにおいて、BGPsec のような新しいプロトコルの導入は難しい。直観的には社会実装のしやすさ、すなわち**展開可能性 (Deployability)** が低い。すべての環境でプロトコルを同時に入れ替えることは運用の観点から難しいため、BGPsec と BGP の同時運用を考える必要があるが、このときどのような事象が生じるかも不透明なままである。

展開可能性の向上に向けた一つのやり方は、（もしあるならば）BGP と BGPsec 両方に対応しているネットワークを介して運用すること [11] [12] であるが、文献 [10] によると、これも大きな問題がある。他にも、BGPsec に対応していないネットワークに対し、AS_PATH 属性を隠すなどの機能を実装して BGPsec に対応していないルータへ送信する方法が考えられるが、BGPsec に対応しているネットワーク事業者の観点からは運用コストが大幅に増加してしまうことになり、対応によりむしろ不利益が生じかねない。

直観として、BGPsec の運用は BGP 単体の運用と比べて負荷が大きく、実装・導入が進んでいない。その結果として、展開可能性が十分に評価されず、更なる導入が喚起されることもないという悪循環が生じている。

1.2 貢献

本稿では BGPsec の展開可能性を向上させるべく、BGP との同時運用を見据えた検討を行う。具体的には、BGP との同時運用時においてルーティングの異常が発生しないか、実験的手法により明らかにする。これらを明らかにすることで、BGPsec 導入時においても BGP の機能に対し本質的な影響がないか評価することができる。

本稿における技術的貢献は二点である。まず、BGPsec と BGP の同時運用を行える評価用プラットフォームとして *Scalable QUagga-based Automated configuration on Bgp (SQUAB)* を新たに考案したことである。現在公開されている BGPsec の参照実装 [13] [14] は BGP との同時運用自体は考慮しているものの、大規模なトポロジを構築する際は実験環境の構築をテストベッド上で行う、あるいは手作業で行う必要があるなど、実験に至るまでの作業負荷が大きい。本稿で設計する SQUAB は、あらかじめ手元で設定を記述し、ツールに読み込ませることで、その設定に従った BGP ルータおよびネットワークトポロジを自動生成する。これにより、一般的な計算能力の端末においても地域単位など広範囲な評価が行えるようになった。

つぎに、RIPE RIS データセットを参考に、SQUAB 上でネットワークを仮想的に構成することで、経路情報の測定を行った。その結果、経路のループの発生は確認されなかったこと、同一ホップ数で異なる経路が選択される可能性があること、更に選択される経路については BGPsec 非対応のルータが含まれるものが選択される傾向があることが明らかになった。

2. 関連研究

本節では関連研究として BGP セキュリティの運用問題と BGP セキュリティの現状について紹介する。

2.1 BGP セキュリティの運用問題

BGP セキュリティの運用研究としては、BGP と任意の BGP 拡張機能の実験・導入を支援するプラットフォーム D-BGP [10] が開発されている。また、同時運用の脅威検討としては、Lychev ら [15] が BGP セキュリティを部分的に導入してもセキュリティが改善されないことを示している。本稿はこれらの知見を踏まえたうえで、BGPsec に特化したプラットフォームの設計と運用実験を行う点が新しい。

BGPsec の導入実装の現状としては、BGP 専用の公開鍵管理基盤 (PKI) としてリソース PKI (RPKI) [6] の標準化が完了しており、すでに普及とその有効性も確認されつつある [16]。また、BGPsec の評価ツールとしては、AS_PATH 検証用 [13], [14] と ORIGIN AS 検証用 [17], [18] それぞれの参照実装が開発されている。本稿では Quagga ベースの BGP-SRx [13] をもとに実装を行った。

2.2 BGP セキュリティの現状

BGP への更なる攻撃 [19], [20], [21], [22] も発見されている一方、近年では暗号通貨を盗むことを目的にした BGP 経路ハイジャックの応用 [23], [24], [25], [26] や匿名通信の無力化 [27] も報告されている。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 [28], [29]。これらの攻撃含めた実世界の BGP の運用は、BGPsec の導入が実現すれば完全に制御可能になる [30]。

そのような次第ではあるが、現在もっとも研究が進んでいる BGP セキュリティの研究領域は、経路情報の受け取り先を限定するフィルタリング [31], [32], [33] である。フィルタリングだけで高い精度かつ高速に経路ハイジャックを防げることが示されている [32], [33]。しかしながら、これらのアプローチでは他の事業者の観点から経路ハイジャックの事実を検知することが難しく、先述したブラックホールサービスへの適用が難しい可能性がある。また、BGP の安全性を確実に保証するという観点から、やはり BGPsec の導入は必要といえる。

一方、近年の研究では BGP を管理機能の分散化 [34], [35]、あるいは中央化 [36], [37] など、プラットフォームの変化も進んでいる。本研究で設計する SQUAB を応用することで、これらのアーキテクチャにおけるセキュリティ上の影響について実証的に検証することも期待できる。

3. BGPsec の展開可能性

本節では、本稿における問題設定を述べる。まず BGP と BGPsec の機能を述べ、その後にこれらの同時運用と本稿で主に取り上げる問題について述べる。

3.1 BGP

BGP [1] は、インターネット全体での宛先問題を自律システム (AS) と呼ばれる、ルータおよび IP アドレスの集合単位で解決するプロトコルである。一般に AS にはインターネットサービスプロバイダや大学など独立したネットワークが該当し、各 AS にはそれぞれ一意な AS 番号が割り当てられている。BGP では、この AS 番号で各ネットワークを区別し、その AS が保有する IP プレフィックスと各宛先への経路を他の AS と交換することで、AS 間で経路を構成する。この交換処理を広告と呼び、一般には TCP 方式で行われる。広告は、利用可能な経路情報を定義する `Network Layer Reachability Information (NLRI)` とその宛先に向けた `AS_PATH` を含むアップデートメッセージの送受信により実現される。なお、`AS_PATH` は `path segment type`, `path segment`, `length`, `path segment value` の組を各 AS ごとに羅列したものである。

3.2 BGPsec

BGPsec [9] 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、 `AS_PATH` 属性の代わりに、 `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 [9]。`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。Algorithm Suite Identifier の値によって指定される署名アルゴリズムに応じて

、署名長が可変する。なお、IP プレフィックスは RPKI [6] により保証される。

3.3 本稿で取り上げる問題: 同時運用

全ての AS を瞬間的に BGPsec 対応に変更するのは不可能であるため、同時運用は必ず考える必要がある。

BGP では BGPsec とパケットの構成が異なるため、`BGPsec_PATH`、すなわち `Secure_PATH` と `Signature_Block` が解釈できない。BGPsec のパケットを BGP 側で解釈するためには上述した `Secure_PATH` から AS 番号リストのみを取り出し、従来の `AS_PATH` として広告する必要がある [9]。このとき、1 節でも述べたとおり、BGPsec に対応している AS 側から見ると `AS_PATH` への変換という余分な処理が生じる。

本稿では上述した設定において、ルーティングが正常に機能する**安定性 (Stability)** を議論する。Sambasivan ら [10] によると、部分的に BGPsec の導入が進んだ場合、互いに隣接し、かつ BGPsec に対応している AS 群である island AS と、その間に存在する「溝 (gulf) AS」が発生し、island AS の外や gulf AS の外に対し、例えばネットワークのループ検知が共有されないことや、経路が収束しないことなどが起こりえるとされている。安定したインターネットを維持するためには、同時運用時においてもこのようなルーティングの安定性が満たされているか明らかにする必要がある。

4. 今回の計測手法

本稿では以下に述べる手法で、性能を評価する。まず方針について述べたのち、BGP と BGPsec の同時運用を可能とするプラットフォーム SQUAB を紹介し、最後に実験に用いるデータセットについて述べる。

4.1 方針

本稿では BGP と BGPsec を運用できるルータを用いて実際のネットワークを構築し、同時に動かすことで、どのような問題が起きるかを評価する。

この実験に際して、BGPsec 用のプラットフォームである BGP-SRx を仮想コンテナ用プラットフォームの Docker [*1] 上に展開したのち、それらのネットワークを構築し、さらに設定を一部自動で行う評価用プラットフォーム SQUAB (Scalable QUagga-based Automated configuration on Bgp) を考案している。大まかには、SQUAB は BGP-SRx が展開された Docker コンテナと接続に必要な

[*1] Docker: `https://www.docker.com/`

Docker network を作成したのち、コンテナ上で BGP-SRx を実行するのに必要な Config ファイルの生成とプロセスの起動を行う。

上述した手法によって作成したネットワークを著者らの研究室内に設けることで実験を行う。具体的には、RIPE RIS データセット[*2]を参考に、BGP-SRx が稼働するコンテナを用いてネットワークを構築する。SQUAB に対し設定を与えることで、実世界に存在するトポロジを再現できる。これにより、実際の運用を考慮した評価が行える。

以下に、評価対象となる安定性について述べる。本稿では、安定性を「収束した経路がループを持たないこと」「収束した経路が正解と比較して同じ結果をいつでも得られること」と定義する。実験においては、十分な時間が経過した際に、それぞれの事象が発生しているか実際のルーティングテーブルから確認することで評価する。即ち、ルーティングテーブルにおいて自身の AS 番号を含む PATH が含まれていないこと、また後述する正解データとどの程度一致しているかということを確認することで安定性を評価していく。

4.2 要素技術：BGP-SRx

BGP-SRx はルーティングソフトウェアである Quagga[*3]に対し、BGPsec の機能を実装することで設計された BGPsec 用プラットフォームである。大まかには端末にインストールすることで、その端末自体を仮想 BGPsec ルータとして動作させることができ、また、設定ファイルの編集により IP プレフィックスやネットワークトポロジなどの設定が可能である。同様の機能を提供するプラットフォームには BIRD BGPsec[*4]もあるが、著者らが認識している範囲では BGP-SRx が最も開発・更新が進んでいる。また、基になっている Quagga 自体も幅広く応用研究 [36] [37] がされている。本稿では AS の境界ルータは BGP-SRx を元に実装した。

BGP-SRx のモジュールは大きく 3 つである。ルータそのものとして動作する `quagga-srx`, 鍵および電子署名を生成する `srx-crypto-api`, 署名に関する validation を確認する機能を提供する `srx-server` である `quagga-srx` は署名を扱う機能はなく、`srx-crypto-api` と `srx-server` が提供している。このとき、`quagga-srx` は各モジュールとの接続を提供している。

なお、BGP ルータとしての設定は `quagga-srx` にある `zebra.conf` と `bgpd.conf` によって制御されており、また `srx-server` の設定は `srx_server.conf` で行える。後述するプラットフォームにおいては、これらの設定を変更するスクリプトを作成している。

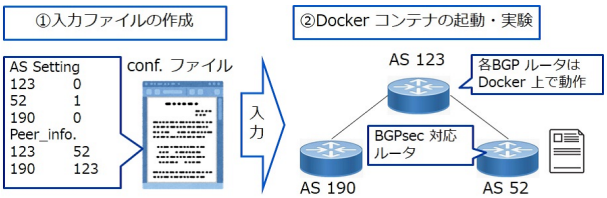

図 1 SQUAB のワークフロー

4.3 SQUAB の設計

SQUAB は、BGP-SRx を通じて自動的に仮想ネットワークを構築することで、経路情報更新を実機で評価するプラットフォームである。

前述した通り SQUAB は Docker 上で BGP-SRx ルータとして起動している。従来であれば、Docker 上で仮想的にネットワークを構築する際、コンテナ同士のネットワーク接続や、各コンテナごとに異なる内容の設定ファイルを作成する必要があった。これに対し、SQUAB では仮想ルータとそれらのネットワーク全体を一個のプロジェクトとして管理できる。

SQUAB のワークフローを図 1 に示す。ユーザの観点からは図 1 左側に記載した設定ファイルを編集するだけで、図 1 右側にあるような該当する設定の BGP ルータの立ち上げ、接続及び通信実験の開始までを行うことが可能となっている。

より詳細には SQUAB で提供する機能は (1) IP プレフィックスが重複しないようなネットワークの構成、(2) 各コンテナをプロジェクト単位で一括起動・削除、および (3) 各コンテナからのルーティング情報の収集である。(1) は `zebra.conf` と `bgpd.conf` にネットワークアドレスを順次割り当てることで、また、(2) は Docker のコンテナ名および Docker ネットワーク名を生成規則に従って命名することで実現する。最後に (3) については、ルーティングテーブルの内容を出力させるスクリプトを実行して、ホスト側の端末に送信するように設計している。なお、BGP-SRx ではネットワーク内に `srx-server` を設ける必要があるが、これは (1) の処理の際に `srx_server.conf` の IP アドレスを設定することで併せて行う。上述した SQUAB の設定ファイルには、ルータに割り当てる AS 番号、それぞれが BGPsec 対応であるか否か、AS 同士の接続情報を記述する。

5. 実験

本節では BGP と BGPsec の同時運用に関する実験について述べる。まず実験目的を述べたのち、それを具体化する実験環境と設定を述べる。その後に、結果について示す。

*2 RIPE Raw Data: `https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris/ris-raw-data`
*3 Quagga: `https://www.quagga.net/`.
*4 `http://www.securerouting.net/tools/bird/BGPsec`

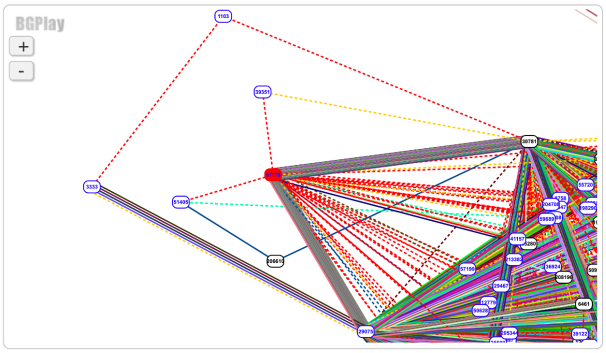

図 2　NAITWAYS-AS を含むトポロジ

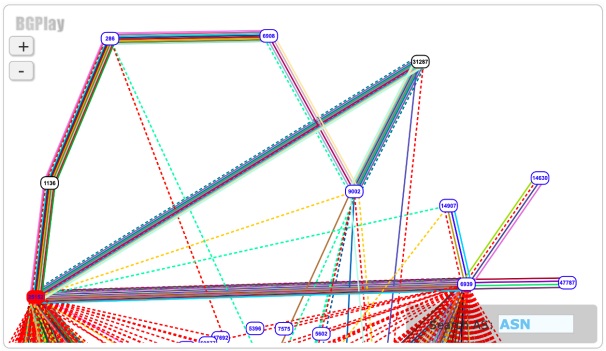

図 3　K-ROOT-SERVER を含むトポロジ

5.1　実験目的

本実験では BGP と BGPsec の同時運用において、経路を更新する際に十分な時間がたてば経路情報が正しく収束するか、また収束した経路がループを持たないかの二点を調査する。本実験においては、RIPE RIS データセットを参考に現存するトポロジを選び、SQUAB に入力し実行することで、上述した内容を確認する。文献 [38] によると、通常の BGP では 200 秒程度で経路が収束することから、200 秒経過後のルーティングテーブルを比較することで確認を行う。

本実験では RPKI による署名の検証鍵、AS 番号および IP プレフィックスの紐づけを含めないこととする。本実験の主目的は BGP と BGPsec が同時に運用できるか明らかにすることである。このとき、BGPsec ルータと RPKI 間の連携が機能しない場合、BGP との同時運用以前に、BGPsec 自体が機能しないことが考えられる。すなわち、同時運用に関する議論がむしろ困難になることが予想される。

5.2　実験環境と設定

本実験ではプラットフォームとして SQUAB を利用する。これに、RIPE RIS を参考にして構成したトポロジを入力して調査を行う。

実行する計算機の環境は表 1 に示す。

今回は、SQUAB に NAITWAYS-AS(AS57119) を含むトポロジ (図 2) と K-ROOT-SERVER(AS25152) を含むトポロジ (図 3) を構築するような入力を与え、調査を行う。なお、NAITWAYS-AS を含む方は AS29075 と AS30781 より左上の部分のみ、K-ROOT-SERVER を含む方は AS25152 と AS6939 より上の部分のみを入力として与えている。入力の際に、どの AS が BGPsec 対応であり、どれがそうでないかも同時に与えることで、特定の割合で BGPsec 対応ルータが存在しているネットワークを構築する。どのルータを BGPsec 対応として設定するかはランダムに設定する。

表 1　実験環境

OS	macOS 10.15.6
CPU	2.3 GHz デュアルコア Intel Core i5
メモリ	8GB
Docker ver.	2.3.0.4

表 2　正解データと異なる経路の数

BGPsec ルータの割合	100%	75%	50%	25%	(全経路数)
NAITWAYS-AS	10	5	4	4	56
K-ROOT-SERVER	2	0	0	1	90

経路情報の収束については、ネットワーク構築後 200 秒間経過した時点で収束しているとみなし、その時のルーティングテーブルの内容を比較する。同一トポロジの BGP ルータのみで構成されるネットワークで得られたルーティングテーブルの内容を正解データとして用い、ある割合で BGPsec 対応ルータが含まれるネットワークの結果と比較する。

各ルータは BGP か BGPsec のいずれか自らが従うプロトコルの仕様 [1] [9] に従い、アップデートメッセージを広告するものとする。なお、広告する経路は IPv4 に従うもののみとする。なお、署名の検証に利用する公開鍵は BGPsec ルータ自身に予めインストールしているものとする。

経路がループを持たないかは、ルーティングテーブル上に自身の AS 番号を含む経路を保持していないかを調べることで確認する。また、正解データとの比較は、全ての AS が持つ各ネットワークに向けた最適経路を比較したときに、一致しなかった経路の数を数えることで評価する。

5.3　結果

BGP のみのネットワークで収束する経路情報と比較して、異なる最適経路として収束していた経路の数を表 2 に示す。なお、経路のループについてはいずれの実験パターンにおいても確認されなかった。

AS 数が多く、全経路数も多い K-ROOT-SERVER を含む方は正解データとほとんど違いのない収束結果が得られたのに対して、AS 数と全経路数が共に比較的少ない NAITWAYS-AS を含む方が正解データと異なる収束結果が多く生まれる結果となった。

6. 考察

6.1 実験結果をふまえて

正解データと異なる経路はいずれにおいても、ASのホップ数は同じで、経由するASが異なるものであった。

NAITWAYS-ASを含むトポロジのBGPsecルータの割合が75%の実験パターンでは、AS206610とAS29075がBGPsec非対応ルータとして設定した。このとき、同じホップ数で到達でき、かつ複数経路が存在し、片方の経路上にのみBGPsec非対応ルータが含まれる場合は、そのBGPsec非対応ルータを含む方の経路が採用されていることが確認できた。

今回採用したトポロジではNAITWAYS-ASを含む方が、あるASから目的のASに向けて同一ホップ数で複数の経路が選択可能であるパターンが多かったために、正解データと異なる経路が多く発生したと考えられる。一方、K-ROOT-SERVERを含む方では、そのようなパターンが少なかったため、収束結果が比較的安定していたと考えられる。

あるASから目的のASに対して同一ホップ数で複数の経路が存在する場合、BGPsec非対応ルータを含む方が選ばれることは、処理速度の観点から自然なことであると考えられる。経路広告を受け取ったルータは、よりホップ数が少ない経路の経路広告を受け取らない限り、それを書き換えることはない。BGPsec非対応ルータは署名の生成や検証を行う必要がない分、より早く経路広告を行うことが可能であり、他のASに対して情報を伝える速度はBGPsec対応ルータよりも速い傾向にあると考えられる。よって、経路広告を受け取る側から見ると、BGPsec対応ルータよりも非対応ルータを含む経路の経路情報が先に到達する可能性が高く、その経路がルーティングテーブルに保持されることになる。

6.2 制約

本稿の実験ではBGP-SRxの機能の制約上、ルータ上で署名の作成や検証を行う部分でどの程度の時間を要するかが調査できていない。BGPでは、AS間である経路情報の広告を送信してから次のものを送信するまでに待機する時間MRAI(Minimal Route Advertisement Interval)を設定することが可能だが、現状のインターネットでは多くのASの境界で最長の30秒に設定されている。経路広告を行う前の準備に要する時間を測定し、それが30秒以内であるか確認することは、BGPsecに時間的なオーバーヘッドが存在するか評価する上で非常に有用である。これを考える時は、RPKIに対する公開鍵証明書の問い合わせも考慮する必要があるが、それも別で実装が必要である。

また、SQUABで自動生成可能なトポロジは二つのAS同士の接続のみで構成されるようなものになっている。このため、三つ以上のASが相互接続されているようなトポロジにおいてどのような挙動が発生するかを評価することはできていない。

7. まとめ

本稿ではBGPsecの展開可能性として、BGPsecとBGPの同時運用を検討した。その際、BGP-SRxに向けた実験用プラットフォームとしてSQUABを新たに設計することで、評価を行った。実験の結果、経路情報においてループの発生はなかったこと、ホップ数は同一であるが、異なるPATHが採用される可能性があることが分かった。また、採用されるPATHについては特にBGPsec非対応ルータを含むものが採用されやすいことも明らかになった。

謝辞 本研究の一部はJSPS科研費18K18049およびセコム財団挑戦的研究助成の助成を受けたものです。

参考文献

[1] Rekhter, Y., Hares, S. and Li, T.: *A Border Gateway Protocol 4 (BGP-4)* (2006). Published: RFC 4271.

[2] : YouTube Hijacking: A RIPE NCC RIS case study, (online), available from ⟨https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study⟩ (2008).

[3] Siddiqui, A.: What Happened? The Amazon Route 53 BGP Hijack to Take Over Ethereum Cryptocurrency Wallets. `https://www.internetsociety.org/blog/2018/04/amazons-route-53-bgp-hijack/`.

[4] Vervier, P., Thonnard, O. and Dacier, M.: Mind Your Blocks: On the Stealthiness of Malicious BGP Hijacks, *Proc. of NDSS 2015*, Internet Society (2015).

[5] Kent, S., Lynn, C. and Seo, K.: Secure border gateway protocol (S-BGP), *IEEE Journal on Selected areas in Communications*, Vol. 18, No. 4, pp. 582–592 (2000).

[6] Lepinski, M. and Kent, S.: *An Infrastructure to Support Secure Internet Routing* (2012). Published: RFC 6480.

[7] Huston, G. and Michaelson, G. G.: *Validation of Route Origination Using the Resource Certificate Public Key Infrastructure (PKI) and Route Origin Authorizations (ROAs)* (2012). Published: RFC 6483.

[8] Lepinski, M., Kong, D. and Kent, S.: *A Profile for Route Origin Authorizations (ROAs)* (2012). Published: RFC 6482.

[9] Lepinski, M. and Sriram, K.: *BGPsec Protocol Specification* (2017). Published: RFC 8205.

[10] Sambasivan, R. R., Tran-Lam, D., Akella, A. and Steenkiste, P.: Bootstrapping Evolvability for Inter-Domain Routing with D-BGP, *Proc. of SIGCOMM 2017*, ACM, p. 474–487 (2017).

[11] Xu, W. and Rexford, J.: MIRO: Multi-Path Interdomain Routing, *SIGCOMM Comput. Commun. Rev.*, Vol. 36, No. 4, p. 171–182 (2006).

[12] Peter, S., Javed, U., Zhang, Q., Woos, D., Anderson, T. and Krishnamurthy, A.: One Tunnel is (Often) Enough, *Proc. of SIGCOMM 2014*, ACM, p. 99–110 (2014).

[13] : NIST BGP Secure Routing Extension (BGP / SRx) Prototype. `https://www.`

nist.gov/services-resources/software/bgp-secure-routing-extension-bgp-srx-prototype.

[14] : BIRD BGPsec. http://www.securerouting.net/tools/bird/.

[15] Lychev, R., Goldberg, S. and Schapira, M.: BGP Security in Partial Deployment: Is the Juice Worth the Squeeze?, *SIGCOMM Computer Communication Review*, Vol. 43, No. 4, p. 171–182 (2013).

[16] Chung, T., Aben, E., Bruijnzeels, T., Chandrasekaran, B., Choffnes, D., Levin, D., Maggs, B. M., Mislove, A., Rijswijk-Deij, R. v., Rula, J. and Sullivan, N.: RPKI is Coming of Age: A Longitudinal Study of RPKI Deployment and Invalid Route Origins, *Proc. of IMC 2019*, ACM, p. 406–419 (2019).

[17] : FRRouting. https://github.com/FRRouting/frr.

[18] : GO-BGP. https://osrg.github.io/gobgp/.

[19] Ballani, H., Francis, P. and Zhang, X.: A Study of Prefix Hijacking and Interception in the Internet, *Proc. of SIGCOMM 2007*, ACM, p. 265–276 (2007).

[20] Birge-Lee, H., Wang, L., Rexford, J. and Mittal, P.: SICO: Surgical Interception Attacks by Manipulating BGP Communities, *Proc. of CCS 2019*, ACM, p. 431–448 (2019).

[21] Goldberg, S., Schapira, M., Hummon, P. and Rexford, J.: How Secure Are Secure Interdomain Routing Protocols, *Proc. of SIGCOMM 2010*, ACM, p. 87–98 (2010).

[22] Miller, L. and Pelsser, C.: A Taxonomy of Attacks Using BGP Blackholing, *Proc. of ESORICS 2019*, LNCS, Vol. 11735, Springer, pp. 107–127 (2019).

[23] Apostolaki, M., Zohar, A. and Vanbever, L.: Hijacking Bitcoin: Routing Attacks on Cryptocurrencies, *Proc. of IEEE S&P 2017*, IEEE, pp. 375–392 (2017).

[24] Smith, J. M. and Schuchard, M.: Routing Around Congestion: Defeating DDoS Attacks and Adverse Network Conditions via Reactive BGP Routing, *Proc. of IEEE S&P 2018*, pp. 599–617 (2018).

[25] Ekparinya, P., Gramoli, V. and Jourjon, G.: The Attack of the Clones Against Proof-of-Authority, *Proc. of NDSS 2020*, Internet Society (2020).

[26] Tran, M., Choi, I., Moon, G. J., Vu, A. V. and Kang, M. S.: A Stealthier Partitioning Attack against Bitcoin Peer-to-Peer Network, *Proc. of IEEE S&P 2020*, IEEE, pp. 496–511 (2020).

[27] Sun, Y., Edmundson, A., Vanbever, L., Li, O., Rexford, J., Chiang, M. and Mittal, P.: RAPTOR: Routing Attacks on Privacy in Tor, *Proc. of Usenix Security 2015*, USENIX Association, pp. 271–286 (2015).

[28] Giotsas, V., Smaragdakis, G., Dietzel, C., Richter, P., Feldmann, A. and Berger, A.: Inferring BGP Blackholing Activity in the Internet, *Proc. of IMC 2017*, ACM, p. 1–14 (2017).

[29] Nawrocki, M., Blendin, J., Dietzel, C., Schmidt, T. C. and Wählisch, M.: Down the Black Hole: Dismantling Operational Practices of BGP Blackholing at IXPs, *Proc. of IMC 2019*, ACM, p. 435–448 (2019).

[30] Smith, J. M., Birkeland, K., McDaniel, T. and Schuchard, M.: Withdrawing the BGP Re-Routing Curtain: Understanding the Security Impact of BGP Poisoning through Real-World Measurements, *Proc. of NDSS 2020*, Internet Society (2020).

[31] Goldberg, S.: Why Is It Taking So Long to Secure Internet Routing?, *Queue*, Vol. 12, No. 8, p. 20–33 (2014).

[32] Lychev, R., Schapira, M. and Goldberg, S.: Rethinking Security for Internet Routing, *Communication of the ACM*, Vol. 59, No. 10, p. 48–57 (2016).

[33] Sermpezis, P., Kotronis, V., Gigis, P., Dimitropoulos, X., Cicalese, D., King, A. and Dainotti, A.: ARTEMIS: Neutralizing BGP Hijacking Within a Minute, *IEEE/ACM Transactions on Networking*, Vol. 26, No. 6, pp. 2471–2486 (2018).

[34] Hlavacek, T., Cunha, I., Gilad, Y., Herzberg, A., Katz-Bassett, E., Schapira, M. and Shulman, H.: DISCO: Sidestepping RPKI' s Deployment Barriers, *Proc. of NDSS 2020*, Internet Society (2020).

[35] Saad, M., Anwar, A., Ahmad, A., Alasmary, H., Yuksel, M. and Mohaisen, A.: RouteChain: Towards Blockchain-based Secure and Efficient BGP Routing, *Proc. of ICBC 2019*, IEEE, pp. 210–218 (2019).

[36] Asharov, G., Demmler, D., Schapira, M., Schneider, T., Segev, G., Shenker, S. and Zohner, M.: Privacy-Preserving Interdomain Routing at Internet Scale, *Proceedings on Privacy Enhancing Technologies*, Vol. 2017, No. 3, pp. 147 – 167 (2017).

[37] Pouryousef, S., Gao, L. and Venkataramani, A.: Towards Logically Centralized Interdomain Routing, *Proc. of NSDI 2020*, USENIX Association, pp. 739–757 (2020).

[38] Katz-Bassett, E., Scott, C., Choffnes, D. R., Cunha, I., Valancius, V., Feamster, N., Madhyastha, H. V., Anderson, T. and Krishnamurthy, A.: LIFEGUARD: Practical Repair of Persistent Route Failures, *ACM SIGCOMM Computer Communication Review*, Vol. 42, No. 4, p. 395–406 (2012).