

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号

特許第7187692号

(P7187692)

(45)発行日 令和4年12月12日(2022.12.12)

(24)登録日 令和4年12月2日(2022.12.2)

(51)国際特許分類

F I

H 0 4 L 45/44 (2022.01)

H 0 4 L 45/44

請求項の数 27 (全22頁)

(21)出願番号	特願2021-523608(P2021-523608)	(73)特許権者	503433420
(86)(22)出願日	令和1年11月2日(2019.11.2)		華為技術有限公司
(65)公表番号	特表2022-511665(P2022-511665 A)		HUAWEI TECHNOLOGIES CO., LTD.
(43)公表日	令和4年2月1日(2022.2.1)		中華人民共和国 518129 広東省深
(86)国際出願番号	PCT/CN2019/115174		▲チェン▼市龍崗区坂田 華為総部▲ベ
(87)国際公開番号	WO2020/088684		ン▼公棟
(87)国際公開日	令和2年5月7日(2020.5.7)		Huawei Administration Building, Bantian, Longgang District, Shenzhen, Guangdong 518129, P.R. China
審査請求日	令和3年6月22日(2021.6.22)		
(31)優先権主張番号	201811302078.3	(74)代理人	100110364
(32)優先日	平成30年11月2日(2018.11.2)		弁理士 実広 信哉
(33)優先権主張国・地域又は機関	中国(CN)		最終頁に続く

(54)【発明の名称】 ルート処理方法およびネットワークデバイス

(57)【特許請求の範囲】

【請求項1】

第1の自律システム内のネットワークデバイスに適用される、ルート処理方法であって、ルートプレフィックスと、取得された前記ルートプレフィックスに関連付けられた自律システム情報とを取得するステップであって、前記自律システム情報は、検証されるべき自律システム情報を含み、前記自律システム情報は、前記ネットワークデバイスにおいて構成されたアウトバウンドルートポリシーの実行後に取得される、ステップと、

ルート起点情報ベース内に一致項目があるかどうかを検証するステップであって、前記一致項目は、前記取得されたルートプレフィックスと、前記検証されるべき自律システム情報とを含む、ステップと、

検証結果に基づいて、前記取得されたルートプレフィックスおよび前記自律システム情報を送信するかどうかを決定するステップとを含む方法。

【請求項2】

前記ルート起点情報ベースのエントリは、ルートプレフィックスとソース自律システムとの間の対応を記録し、前記検証されるべき自律システム情報は、前記自律システム情報内のソース自律システム情報であり、または

前記ルート起点情報ベースのエントリは、ルートプレフィックスと自律システムペアとの間の対応を記録し、前記検証されるべき自律システム情報は、前記自律システム情報内の自律システムパス情報である、請求項1に記載の方法。

【請求項 3】

前記自律システム情報は、前記ネットワークデバイスにおいて構成されたアウトバウンドルートポリシーに従う修正後の自律システム情報である、請求項1または2に記載の方法。

【請求項 4】

ルート起点情報ベース内に一致項目があるかどうかを検証する前記ステップは、

前記ルート起点情報ベース内に前記取得されたルートプレフィックスと一致するエントリがあり、かつ前記エントリ内の自律システム情報が前記検証されるべき自律システム情報と異なるとき、前記ルート起点情報ベース内に一致項目がないことを検証するステップを含み、

10

検証結果に基づいて、前記取得されたルートプレフィックスおよび前記自律システム情報を送信するかどうかを決定する前記ステップは、

前記取得されたルートプレフィックスおよび前記自律システム情報を送信しないことを決定するステップを含む、請求項1から3のいずれか一項に記載の方法。

【請求項 5】

前記ルート起点情報ベース内に一致項目がないことを検証する前記ステップの後に、前記方法は、

アラーム情報を出力するステップをさらに含む、請求項4に記載の方法。

【請求項 6】

ルート起点情報ベース内に一致項目があるかどうかを検証する前記ステップは、

20

前記ルート起点情報ベース内に前記取得されたルートプレフィックスと一致するエントリがないとき、前記ルート起点情報ベース内に一致項目がないことを検証するステップを含み、

検証結果に基づいて、前記取得されたルートプレフィックスおよび前記自律システム情報を送信するかどうかを決定する前記ステップは、

あらかじめ構成されたポリシーに従って、前記取得されたルートプレフィックスおよび前記自律システム情報を送信するかどうかを決定するステップを含む、請求項1から3のいずれか一項に記載の方法。

【請求項 7】

ルート起点情報ベース内に一致項目があるかどうかを検証する前記ステップは、

30

前記ルート起点情報ベース内に前記取得されたルートプレフィックスと一致するエントリがあり、かつ前記エントリ内の自律システム情報が前記検証されるべき自律システム情報と同じであるとき、前記ルート起点情報ベース内に前記一致項目があることを検証するステップを含み、

検証結果に基づいて、前記取得されたルートプレフィックスおよび前記自律システム情報を送信するかどうかを決定する前記ステップは、

前記取得されたルートプレフィックスおよび前記自律システム情報を送信することを決定するステップを含み、

前記方法は、

前記取得されたルートプレフィックスおよび前記自律システム情報を搬送するルート情報を送信するステップをさらに含む、請求項1から3のいずれか一項に記載の方法。

40

【請求項 8】

前記ルート起点情報ベースは、リソース公開鍵インフラストラクチャサーバから取得される、請求項1から7のいずれか一項に記載の方法。

【請求項 9】

ルートプレフィックスを取得することは、

第2の自律システムから前記取得されたルートプレフィックスを受信することを含み、または

ルートプレフィックスを取得することは、

前記取得されたルートプレフィックスを生成することを含む、請求項1から8のいずれか

50

一項に記載の方法。

【請求項 10】

前記ネットワークデバイスは、前記第1の自律システムにおける境界ノードである、請求項1から5のいずれか一項に記載の方法。

【請求項 11】

ルートプレフィックスと、取得された前記ルートプレフィックスに関連付けられた自律システム情報とを取得する前記ステップは、

前記ルートプレフィックスと、受信された前記ルートプレフィックスに関連付けられた起点自律システム情報とを受信するステップであって、前記起点自律システム情報は、ソース自律システム情報を含む、ステップと、

ルート起点情報ベース内に一致項目があるかどうかを検証するステップであって、前記一致項目は、前記受信されたルートプレフィックスと、前記ソース自律システム情報とを含む、ステップと、

前記ルートプレフィックスと、前記ネットワークデバイスにおいて構成された前記アウトバウンドルートポリシーの実行後の前記自律システム情報とを取得するステップとを含む、請求項1に記載の方法。

【請求項 12】

前記ルートプレフィックスと、前記ネットワークデバイスにおいて構成された前記アウトバウンドルートポリシーの実行後の前記自律システム情報とを取得する前記ステップは、

前記アウトバウンドルートポリシーに従って前記起点自律システム情報を修正して、前記自律システム情報を取得するステップを含む、請求項11に記載の方法。

【請求項 13】

ネットワークデバイスであって、前記ネットワークデバイスは、第1の自律システム内のネットワークデバイスであり、

取得モジュールであって、前記取得モジュールは、ルートプレフィックス取得サブモジュールおよび自律システム情報取得サブモジュールを含み、前記ルートプレフィックス取得サブモジュールは、ルートプレフィックスを取得するように構成され、前記自律システム情報取得サブモジュールは、前記取得されたルートプレフィックスに関連付けられた自律システム情報を取得するように構成され、前記自律システム情報は、検証されるべき自律システム情報を含み、前記自律システム情報は、前記ネットワークデバイスにおいて構成されたアウトバウンドルートポリシーの実行後に取得される、取得モジュールと、

ルート起点情報ベース内に一致項目があるかどうかを検証するように構成された検証モジュールであって、前記一致項目は、前記取得されたルートプレフィックスと、前記検証されるべき自律システム情報とを含む、検証モジュールと、

検証結果に基づいて、前記取得されたルートプレフィックスおよび前記自律システム情報を送信するかどうかを決定するように構成された決定モジュールとを含むネットワークデバイス。

【請求項 14】

前記ルート起点情報ベースのエントリは、ルートプレフィックスとソース自律システムとの間の対応を記録し、前記検証されるべき自律システム情報は、前記自律システム情報内のソース自律システム情報であり、または

前記ルート起点情報ベースのエントリは、ルートプレフィックスと自律システムペアとの間の対応を記録し、前記検証されるべき自律システム情報は、前記自律システム情報内の自律システムパス情報である、請求項13に記載のネットワークデバイス。

【請求項 15】

前記自律システム情報取得サブモジュールによって取得された前記自律システム情報は、前記ネットワークデバイスにおいて構成されたアウトバウンドルートポリシーに従う修正後の自律システム情報である、請求項13または14に記載のネットワークデバイス。

【請求項 16】

前記検証モジュールは、前記ルート起点情報ベース内に前記取得されたルートプレフィ

10

20

30

40

50

ックスと一致するエントリがあり、かつ前記エントリ内の自律システム情報が前記検証されるべき自律システム情報と異なると決定したとき、前記ルート起点情報ベース内に一致項目がないことを検証するように構成され、

それに対応して、前記決定モジュールは、前記取得されたルートプレフィックスおよび前記自律システム情報を送信しないことを決定する、請求項13から15のいずれか一項に記載のネットワークデバイス。

【請求項17】

前記検証モジュールが、前記ルート起点情報ベース内に一致項目がないことを検証した後に、アラーム情報を出力するように構成されたアラームモジュールをさらに含む、請求項16に記載のネットワークデバイス。

【請求項18】

前記ネットワークデバイスは、送信モジュールをさらに含む、

前記検証モジュールは、前記ルート起点情報ベース内に前記取得されたルートプレフィックスと一致するエントリがあり、かつ前記エントリ内の自律システム情報が前記検証されるべき自律システム情報と同じであると決定したとき、前記ルート起点情報ベース内に前記一致項目があることを検証するように構成され、

それに対応して、前記決定モジュールは、前記取得されたルートプレフィックスおよび前記自律システム情報を送信することを決定し、前記送信モジュールは、前記取得されたルートプレフィックスおよび前記自律システム情報を搬送するルート情報を送信する、請求項13から15のいずれか一項に記載のネットワークデバイス。

【請求項19】

前記検証モジュールは、前記ルート起点情報ベース内に前記取得されたルートプレフィックスと一致するエントリがないと決定したとき、前記ルート起点情報ベース内に一致項目がないと決定するように構成され、

それに対応して、前記決定モジュールは、あらかじめ構成されたポリシーに従って、前記取得されたルートプレフィックスおよび前記自律システム情報を送信するかどうかを決定する、請求項13から15のいずれか一項に記載のネットワークデバイス。

【請求項20】

リソース公開鍵インフラストラクチャサーバから前記ルート起点情報ベースを取得するように構成されたルート起点情報ベース取得モジュールをさらに含む、請求項13から19のいずれか一項に記載のネットワークデバイス。

【請求項21】

前記ルートプレフィックス取得サブモジュールは、第2の自律システムから前記取得されたルートプレフィックスを受信するか、または前記取得されたルートプレフィックスを生成するように構成された、請求項13から20のいずれか一項に記載のネットワークデバイス。

【請求項22】

前記ネットワークデバイスは、前記第1の自律システム内の境界ノードである、請求項13から21のいずれか一項に記載のネットワークデバイス。

【請求項23】

前記取得モジュールは、

前記ルートプレフィックスと、受信された前記ルートプレフィックスに関連付けられた起点自律システム情報とを受信することであって、前記起点自律システム情報は、ソース自律システム情報を含む、ことと、

ルート起点情報ベース内に一致項目があるかどうかを検証することであって、前記一致項目は、前記受信されたルートプレフィックスと、前記ソース自律システム情報とを含む、ことと、

前記ルートプレフィックスと、前記ネットワークデバイスにおいて構成された前記アウトバウンドルートポリシーの実行後の前記自律システム情報とを取得することと

を行うように構成される、請求項13に記載のネットワークデバイス。

10

20

30

40

50

【請求項 2 4】

前記取得モジュールは、前記アウトバウンドルートポリシーに従って前記起点自律システム情報を修正して、前記自律システム情報を取得するように構成される、請求項23に記載のネットワークデバイス。

【請求項 2 5】

ネットワークデバイスであって、前記ネットワークデバイスは、第1の自律システム内のネットワークデバイスであり、プロセッサ、メモリ、および通信インターフェースを含み、前記プロセッサ、前記メモリ、および前記通信インターフェースは、互いに接続され、前記メモリは、コンピュータプログラムを記憶するように構成され、前記コンピュータプログラムは、プログラム命令を含み、前記プロセッサは、前記プログラム命令を呼び出して、請求項1から12のいずれか一項に記載の方法を前記ネットワークデバイスに実行させるように構成された、ネットワークデバイス。

10

【請求項 2 6】

コンピュータ可読記憶媒体であって、前記コンピュータ可読記憶媒体は、プログラムを記憶し、前記プログラムがコンピュータにおいて実行されるとき、前記コンピュータは、請求項1から12のいずれか一項に記載の方法を実行することが可能にされる、コンピュータ可読記憶媒体。

【請求項 2 7】

ルート処理装置であって、プログラム命令に関連するハードウェアを含み、前記ハードウェアは、請求項1から12のいずれか一項に記載の方法を実行するように構成された、ルート処理装置。

20

【発明の詳細な説明】

【技術分野】

【0 0 0 1】

この出願は、2018年11月2日に中国国家知識産権局に出願された、発明の名称を「ルート処理方法およびネットワークデバイス」とする中国特許出願第201811302078.3号の優先権を主張し、その全体が参照によりここに組み込まれる。

【0 0 0 2】

本発明は、通信分野、特に、ルート処理方法およびネットワークデバイスに関する。

【背景技術】

30

【0 0 0 3】

境界ゲートウェイプロトコル(Border Gateway Protocol, BGP)ルート起点情報が正しいかどうかを検証するために、リソース公開鍵インフラストラクチャ(resource public key infrastructure, RPKI)ソリューションが使用される。分散RPKIサーバは、各自律システム(autonomous system, AS)によって開始されたBGPルートに対応するソースAS番号、およびBGPルートのルートプレフィックスなどの情報を収集し、ルートプレフィックスはマスクを含む。ルータは、RPKIサーバとの接続を確立し、ルート起点許可(route origin authorization, ROA)データをローカルに記憶する。データは、ルートプレフィックスと、ルートプレフィックスを生成するソース自律システムとの間の関係を含む。ルータは、隣接ノードから、ルートプレフィックスを含むルート情報を受信した後、ローカルに記憶されたROAデータに基づいて、隣接ノードから受信されたルートプレフィックスに対応するソースASが正しいかどうかを検証する。RPKIに関する詳細については、標準組織、インターネット・エンジニアリング・タスクフォース(internet engineering task force, IETF)のリクエスト・フォー・コメント、RFC6810およびRFC6811を参照されたい。

40

【0 0 0 4】

しかしながら、ネットワーク内のすべてのルータが、ROAデータに基づいて、受信されたルートプレフィックスに関連付けられたソースAS情報を検証するわけではない。この場合、受信されたルートプレフィックスに関連付けられたソースAS情報が誤って修正されたならば、受信機ルータによるルート計算が影響される。結果として、自律システム間のデータトラフィックは、計画されたパスに沿って伝送されない。ASのためのネットワーク管

50

理者は、通常、ルータのアウトバウンドルートポリシーを構成する。アウトバウンドルートポリシーが、送信されるべきルートプレフィックスに関連付けられたASパス情報を修正することを含むならば、ルータは、ルートプレフィックスを送信する前に、アウトバウンドルートポリシーに従ってルートプレフィックスに関連付けられたASパス情報を修正する。したがって、誤った手動構成により、上記の問題が生じ得る。

【発明の概要】

【課題を解決するための手段】

【0005】

この出願は、ルートプレフィックスが送信される前に、送信されるべきルートプレフィックスに関連付けられた自律システム情報を検証し、ネットワークデバイスが誤った自律システム情報を含むルート情報を送信する可能性を低減し、異常なネットワークフロー方向を引き起こす可能性を低減するために、ルート処理方法およびネットワークデバイスを提供する。

10

【0006】

第1の態様によれば、本発明の一実施形態は、ルート処理方法を提供する。この方法は、第1の自律システム内のネットワークデバイスに適用され、ルートプレフィックスと、取得されたルートプレフィックスに関連付けられた自律システム情報とを取得するステップであって、関連付けられた自律システム情報は、検証されるべき自律システム情報を含む、ステップと、ネットワークデバイスによって、ルート起点情報ベース内に一致項目があるかどうかを検証するステップであって、一致項目は、取得されたルートプレフィックスと、検証されるべき自律システム情報とを含む、ステップと、検証結果に基づいて、取得されたルートプレフィックスを送信するかどうかを決定するステップとを含む。

20

【0007】

この方法では、ルートプレフィックスを送信する前に、ネットワークデバイスは、まず、ルートプレフィックスに関連付けられた検証されるべき自律システム情報を検証し、検証結果に基づいて、ルートプレフィックスを送信するかどうかを決定する。これは、ネットワークデバイスが、誤った自律システム情報を搬送するルート情報を送信する可能性を低減し、異常なネットワークフロー方向を引き起こす可能性を低減する。

【0008】

第1の態様の可能な設計では、ルート起点情報ベースのエントリは、ルートプレフィックスとソース自律システムとの間の対応を記録し、検証されるべき自律システム情報は、関連付けられた自律システム情報内のソース自律システム情報であり、ルート起点情報ベースのエントリは、ルートプレフィックスと自律システムペアとの間の対応を記録し、検証されるべき自律システム情報は、関連付けられた自律システム情報内の自律システムパス情報であり、または検証されるべき自律システム情報は、関連付けられた自律システム情報内のソース自律システム情報と、関連付けられた自律システム情報内の自律システムパス情報とを含む。この設計では、ソース自律システム情報が検証されてもよく、自律システムパス情報が検証されてもよく、または両方が検証されてもよい。各検証は、送信されたルートプレフィックスに関連付けられた自律システム情報が正しいことを保証することができない。したがって、検証における精度を改善するために複数の検証方式が同時に使用されてもよい。

30

40

【0009】

第1の態様の可能な設計では、ルート起点情報ベースは、リソース公開鍵インフラストラクチャサーバから取得される。たとえば、ルート起点情報ベースは、リソース公開鍵インフラストラクチャサーバからネットワークデバイスによってダウンロードされ、またはリソース公開鍵インフラストラクチャサーバによってネットワークデバイスに能動的に送信され(たとえば、定期的に送信され、または必要に応じて送信され)てもよい。別の可能な設計では、ネットワークデバイスは、ルート起点情報ベースをローカルに記憶しないが、ネットワークデバイスが検証を実行する必要があるとき、検証されるべきコンテンツをリソース公開鍵インフラストラクチャサーバに送信する。この設計では、現在の技術にお

50

けるリソース公開鍵インフラストラクチャサーバを使用されてもよく、追加のプロトコルまたはアーキテクチャを開発する必要がない。

【 0 0 1 0 】

第1の態様の可能な設計では、関連付けられた自律システム情報は、ネットワークデバイスにおいて構成されたアウトバウンドルートポリシーに従う修正後の自律システム情報である。この設計では、アウトバウンドルートポリシーに従う修正後の自律システム情報が正しいかどうかを検証されることが可能であり、アウトバウンドルートポリシーは、通常、手動で構成される。したがって、この設計は、手動構成によって引き起こされるエラーを低減することができる。

【 0 0 1 1 】

第1の態様の可能な設計では、ルートプレフィックスを取得するステップは、第2の自律システムからルートプレフィックスを受信するステップ、ルートプレフィックスを生成するステップ、または第1の自律システム内の別のネットワークデバイスによって生成されたルートプレフィックスを受信するステップを含む。この設計では、検証されるべきルートプレフィックスは、別の自律システムからネットワークデバイスによって受信され、ネットワークデバイスによって生成され、またはネットワークデバイスが属する自律システム内の別のネットワークデバイスによって生成され得る。これは、柔軟な検証を提供する。

【 0 0 1 2 】

第1の態様の可能な設計では、ネットワークデバイスは、第1の自律システム内の境界ノードである。さらに、境界ノードは、ルート送信方向における第1の自律システム内のアウトバウンド境界ノードであってもよい。通常、自律システム情報内の自律システムパスは、自律システム内の内部ノードが互いにルート情報を送信するときに修正されない。したがって、検証機能がアウトバウンド境界ノードにおいて配備されてもよく、第1の自律システム内の内部ノードは、検証を実行することは要求されない。

【 0 0 1 3 】

第1の態様の可能な設計では、ルート起点情報ベース内に取得されたルートプレフィックスと一致するエントリがあり、かつエントリ内の自律システム情報が検証されるべき自律システム情報と異なるとき、ネットワークデバイスは、ルート起点情報ベース内に一致項目がないと決定し、取得されたルートプレフィックスを送信しないことを決定する。一致項目がないと決定したとき、ネットワークデバイスは、ルートプレフィックスを送信しない。これは、誤った自律システム情報に関連付けられたルートプレフィックスを送信する可能性を低減する。

【 0 0 1 4 】

第1の態様の可能な設計では、ネットワークデバイスは、ルート起点情報ベース内に一致項目がないと決定した後に、アラーム情報を出力する。アラーム情報は、タイムリーな方式で出力され、ネットワークデバイス内の自律システム情報において不一致が発生したことをネットワーク管理者に通知する。

【 0 0 1 5 】

第1の態様の可能な設計では、ルート起点情報ベース内に取得されたルートプレフィックスと一致するエントリがあり、かつエントリ内の自律システム情報が検証されるべき自律システム情報と同じであるとき、ネットワークデバイスは、ルート起点情報ベース内に一致項目があると決定し、取得されたルートプレフィックスを送信することを決定し、取得されたルートプレフィックスを搬送するルート情報を送信する。一致項目があると決定したとき、ネットワークデバイスは、ルートプレフィックスを送信する。これは、送信されたルートプレフィックスに関連付けられた自律システム情報の精度を改善する。

【 0 0 1 6 】

第1の態様の可能な設計では、ルート起点情報ベース内に取得されたルートプレフィックスと一致するエントリがないとき、ネットワークデバイスは、ルート起点情報ベース内に一致項目がないと決定する。この場合における検証結果は、「不明」と考えられる。この場合が発生するとき、取得されたルートプレフィックスを送信するかどうかは、あらか

10

20

30

40

50

じめ構成されたポリシーに従って決定される。あらかじめ構成されたポリシーは、取得されたルートプレフィックスを送信すること、または取得されたルートプレフィックスを送信しないことであり得る。このように、検証結果が「不明」であるとき、関連する対策があり得る。

【 0 0 1 7 】

第2の態様によれば、本発明の一実施形態は、ネットワークデバイスを提供する。ネットワークデバイスは、第1の自律システム内のネットワークデバイスである。ネットワークデバイスは、第1の態様または第1の態様の可能な実装のうちのいずれか1つにおける方法を実行するように構成され得る。具体的には、ネットワークデバイスは、第1の態様または第1の態様の可能な実装のうちのいずれか1つにおける方法を実行するように構成されたモジュールを含む。

10

【 0 0 1 8 】

第3の態様によれば、本発明の一実施形態は、ネットワークデバイスを提供する。ネットワークデバイスは、第1の自律システム内のネットワークデバイスであり、取得モジュールと、検証モジュールと、決定モジュールとを含む。取得モジュールは、ルートプレフィックス取得サブモジュールおよび自律システム情報取得サブモジュールを含み、ルートプレフィックス取得サブモジュールは、ルートプレフィックスを取得するように構成され、自律システム情報取得サブモジュールは、取得されたルートプレフィックスに関連付けられた自律システム情報を取得するように構成され、関連付けられた自律システム情報は、検証されるべき自律システム情報を含む。検証モジュールは、ルート起点情報ベース内に一致項目があるかどうかを検証するように構成され、一致項目は、取得されたルートプレフィックスと、検証されるべき自律システム情報とを含む。決定モジュールは、検証結果に基づいて、取得されたルートプレフィックスを送信するかどうかを決定するように構成される。

20

【 0 0 1 9 】

第3の態様の可能な設計では、ルート起点情報ベースのエントリは、ルートプレフィックスとソース自律システムとの間の対応を記録し、検証されるべき自律システム情報は、関連付けられた自律システム情報内のソース自律システム情報であり、ルート起点情報ベースのエントリは、ルートプレフィックスと自律システムペアとの間の対応を記録し、検証されるべき自律システム情報は、関連付けられた自律システム情報内の自律システムパス情報であり、または検証されるべき自律システム情報は、関連付けられた自律システム情報内のソース自律システム情報と、関連付けられた自律システム情報内の自律システムパス情報とを含む。

30

【 0 0 2 0 】

第3の態様の可能な設計では、ネットワークデバイスは、リソース公開鍵インフラストラクチャサーバからルート起点情報ベースを取得するように構成されたルート起点情報ベース取得モジュールをさらに含む。たとえば、ルート起点情報ベースは、リソース公開鍵インフラストラクチャサーバからネットワークデバイスによってダウンロードされ、またはリソース公開鍵インフラストラクチャサーバによってネットワークデバイスに能動的に送信されてもよい。

40

【 0 0 2 1 】

第3の態様の可能な設計では、自律システム情報取得サブモジュールによって取得された関連付けられた自律システム情報は、ネットワークデバイスにおいて構成されたアウトバウンドルートポリシーに従う修正後の自律システム情報である。

【 0 0 2 2 】

第3の態様の可能な設計では、ルートプレフィックス取得サブモジュールは、第2の自律システムから取得されたルートプレフィックスを受信するか、または取得されたルートプレフィックスを生成するように構成される。

【 0 0 2 3 】

第3の態様の可能な設計では、ネットワークデバイスは、第1の自律システム内の境界ノ

50

ードである。

【 0 0 2 4 】

第3の態様の可能な設計では、検証モジュールは、ルート起点情報ベース内に取得されたルートプレフィックスと一致するエントリがあり、かつエントリ内の自律システム情報が検証されるべき自律システム情報と異なるとき、ルート起点情報ベース内に一致項目がないと決定するように構成され、それに対応して、決定モジュールは、取得されたルートプレフィックスを送信しないことを決定する。

【 0 0 2 5 】

第3の態様の可能な設計では、アラームモジュールがさらに含まれ、検証モジュールが、ルート起点情報ベース内に一致項目がないと決定した後に、アラーム情報を出力するように構成される。

10

【 0 0 2 6 】

第3の態様の可能な設計では、ネットワークデバイスは、送信モジュールをさらに含み、検証モジュールは、ルート起点情報ベース内に取得されたルートプレフィックスと一致するエントリがあり、かつエントリ内の自律システム情報が検証されるべき自律システム情報と同じであるとき、ルート起点情報ベース内に一致項目があると決定するように構成され、それに対応して、決定モジュールは、取得されたルートプレフィックスを送信することを決定し、送信モジュールは、取得されたルートプレフィックスを搬送するルート情報を送信する。

【 0 0 2 7 】

20

第4の態様によれば、本発明の一実施形態は、ネットワークデバイスを提供する。ネットワークデバイスは、第1の自律システム内のネットワークデバイスである。ネットワークデバイスは、プロセッサ、メモリ、および通信インターフェースを含む。プロセッサ、メモリ、および通信インターフェースは、互いに接続される。メモリは、コンピュータプログラムを記憶するように構成される。コンピュータプログラムは、プログラム命令を含む。プロセッサは、プログラム命令を呼び出して、第1の態様または第1の態様の可能な実装のうちのいずれか1つにおける方法を実行するように構成される。

【 0 0 2 8 】

第5の態様によれば、本発明の一実施形態は、ネットワークデバイスを提供する。ネットワークデバイスは、第1の自律システム内のネットワークデバイスである。ネットワークデバイスは、プロセッサ、メモリ、および通信インターフェースを含む。プロセッサ、メモリ、および通信インターフェースは、互いに接続される。メモリは、コンピュータプログラムを記憶するように構成される。コンピュータプログラムは、プログラム命令を含む。プロセッサは、プログラム命令を呼び出して、第3の態様または第3の態様の可能な設計における、自律システム情報取得サブモジュール、検証モジュール、および決定モジュールの機能と、第3の態様の可能な設計における、ルートプレフィックス取得サブモジュールによって取得されたルートプレフィックスを生成する機能とを実現するように構成される。通信インターフェースは、第3の態様の可能な設計における、ルート起点情報ベース取得モジュール、アラームモジュール、および送信モジュールの機能を実現するように構成される。

30

40

【 0 0 2 9 】

第6の態様によれば、本発明の一実施形態は、ネットワークデバイスを提供する。ネットワークデバイスは、第1の自律システム内のネットワークデバイスである。ネットワークデバイスは、プロセッサ、メモリ、および通信インターフェースを含む。プロセッサ、メモリ、および通信インターフェースは、互いに接続される。メモリは、コンピュータプログラムを記憶するように構成される。コンピュータプログラムは、プログラム命令を含む。プロセッサは、プログラム命令を呼び出して、第3の態様または第3の態様の可能な設計における検証モジュールおよび決定モジュールの機能を実現するように構成される。通信インターフェースは、第3の態様の可能な設計における、ルートプレフィックス取得サブモジュールによって第2の自律システムから取得されたルートプレフィックスを受信す

50

る機能と、ルート起点情報ベース取得モジュール、アラームモジュール、および送信モジュールの機能とを実現するように構成される。通信インターフェースおよびプロセッサは、協働して、第3の態様または第3の態様の可能な設計における、自律システム情報取得サブモジュールの機能を実現する。その代わりに、通信インターフェースは、第3の態様における自律システム情報取得サブモジュールの機能を独立に実現する。

【0030】

上記の態様において提供されたネットワークデバイスの有益な効果については、第1の態様および第1の態様の可能な設計における有益な効果の記載を参照されたい。詳細は、ここで再度記載されない。

【0031】

第7の態様によれば、本発明の一実施形態は、コンピュータ可読記憶媒体を提供する。コンピュータ可読記憶媒体は、プログラムを記憶する。プログラムがコンピュータにおいて実行されるとき、コンピュータは、第1の態様または第1の態様の可能な設計のいずれか1つにおける方法を実行することが可能にされる。

【0032】

第8の態様によれば、本発明の一実施形態は、プログラム命令に関連するハードウェアを含むルート処理装置を提供する。ハードウェアは、第1の態様または第1の態様の可能な設計のいずれか1つにおける方法を実行するように構成される。

【0033】

本発明の技術的解決策をより明確に記載するために、以下は、実施形態において使用される添付の図面を簡単に記載する。明らかに、以下の記載における添付の図面は、本発明の単にいくつかの実施形態を表し、この技術分野の当業者は、創作的な努力なしにこれらの添付の図面から他の技術的解決策および添付の図面を依然として導き出し得る。

【図面の簡単な説明】

【0034】

【図1】本発明の一実施形態による適用シナリオの概略図である。

【図2】本発明の一実施形態による方法の概略フローチャートである。

【図3】本発明の一実施形態による方法の概略フローチャートである。

【図4】本発明の一実施形態による方法の概略フローチャートである。

【図5】本発明の一実施形態によるネットワークデバイスの構造の概略図である。

【図6】本発明の一実施形態によるネットワークデバイスの構造の概略図である。

【発明を実施するための形態】

【0035】

図1は、本発明の一実施形態による適用シナリオの概略図である。図1は、自律システムAS1、AS2、AS3、AS4、およびAS5を含む。AS1は、AS1内に境界ノードR11およびR12を含む。AS2は、AS2内に境界ノードR21およびR22を含む。AS3は、AS3内に境界ノードR31およびR33を含み、AS3内に内部ノードR32も含む。AS4は、AS4内に境界ノードR41およびR42を含む。AS5は、AS5内に境界ノードR51およびR52を含む。各境界ノードは、ルート機能を有するネットワークデバイスであってもよい。たとえば、境界ノードは、ルータ、またはルート機能を有するスイッチである。

【0036】

以下は、現在の技術における異常なネットワークフロー方向の場合を記載する。AS1がルートプレフィックス10.1.0.0/16を生成し、AS2およびAS3を通じてAS4に10.1.0.0/16を送信する。加えて、AS1はまた、10.1.0.0/16を、別のASパス、すなわちAS5を通じてAS4に送信する。R41は、R33およびR52からルートプレフィックス10.1.0.0/16を含むルート情報を別々に受信する。R33から受信されたルート情報は、10.1.0.0/16と、10.1.0.0/16に対応するASパス(AS3, AS2, AS1)とを含む。マーキングモード「(AS3, AS2, AS1)」は、10.1.0.0/16に対応するソースASがAS1であり、10.1.0.0/16がAS1、AS2、およびAS3を順に通過することを示す。R52から受信されたルート情報は、10.1.0.0/16と、10.1.0.0/16に対応するASパス(AS5, AS1)とを含む。マーキングモード「(AS5, A

10

20

30

40

50

S1)」は、10.1.0.0/16に対応するソースASがAS1であり、10.1.0.0/16がAS1およびAS5を順に通過することを示す。10.1.0.0/16までのルートを計算するとき、R41は、より短いASパスを選択するルールに従って、R52をネクストホップとして選択する。言い換えれば、R41は、10.1.0.0/16への宛先を有するデータパケットを、R33の代わりにR52に送信する。上記の記載は、ネットワーク計画における通常のフロー方向に基づくことが仮定される。しかしながら、AS3のための管理者は、R33におけるアウトバウンドルートポリシーを構成し得る。アウトバウンドルートポリシーは、R33によって外部に送信されるルート情報内のASパス情報に影響する。たとえば、R33におけるアウトバウンドルートポリシーが誤って構成されたならば、10.1.0.0/16をR33によって外部に送信するための通常のASパス(AS3, AS2, AS1)が(AS3)に変更される。結果として、R41は、10.1.0.0/16への宛先を有するデータパケットをR33に送信し、異常なネットワークフロー方向が引き起こされる。

10

【0037】

本発明の実施形態は、ルート処理方法および対応するネットワークデバイスを提供する。この方法およびこのネットワークデバイスは、同じ発明概念に基づき、この方法およびこのネットワークデバイスは、問題を解決するための類似の原理を有する。したがって、ネットワークデバイスの実施形態と方法の実施形態との間で相互参照が行われることが可能であり、繰り返される記載は提供されない。

【0038】

本発明の実施形態では、図1に表された適用シナリオにおいて、ルート起点情報ベースサーバ、たとえば、RPKIサーバが配置される。R33は、RPKIサーバからルート起点検証データを取得して、ルート起点情報ベースを形成し得る。ルート起点検証データは、ROAデータ、または自律システムパス許可(autonomous system path authorization, ASPA)データであり得る。ROAデータは、ルートプレフィックスとソース自律システムとの間の対応を記載し、ルートプレフィックスに対応するソースASが正しいかどうかを検証するために使用される。ASPAデータは、ルートプレフィックスと自律システムペアとの間の対応を記載し、ルートプレフィックスに対応するASパス情報が正しいかどうかを検証するために使用される。確かに、ROAデータベースおよびASPAデータベースは、ソースAS検証情報およびASパス検証情報を提供するために、1つのデータベースとして実現され得る。このようにして、R33が、10.1.0.0/16を搬送するルート情報をAS4内のR41に送信する前に、R33は、まず、ルート起点を検証し、たとえば、ソースASが正しいかどうかを検証し、ASパスが正しいかどうかを検証し、またはソースASおよびASパスが正しいかどうかを検証し得る。検証が成功したならば、R33は、10.1.0.0/16を搬送するルート情報を送信する。これは、異常なネットワークフロー方向を引き起こす可能性を低減する。

20

30

【0039】

上記は、R33がAS1から発信された10.1.0.0/16をAS2から受信する場合を記載する。別の場合には、10.1.0.0/16がAS3によって生成される、たとえば、R31、R32、またはR33によって生成されるならば、AS3内のルートデバイスが10.1.0.0/16を送信するとき、ルート情報の受信機が受信されたルート情報に対応するルート起点のみを検証することをIETF RFC 6810およびIETF RFC 6811が指定するので、10.1.0.0/16に対応するルート起点が正しいかどうかを検証するための現在の技術における解決策はない。本発明の実施形態では、R33は、AS3によって生成されたルートプレフィックスを検証し、次いでルートプレフィックスを送信し得る。これは、R33によって外部に送信されるルートプレフィックスに対応するAS起点情報の精度を改善し、異常なネットワークフロー方向を引き起こす可能性が低減する。

40

【0040】

本発明の実施形態において記載されたネットワークデバイスは、ルート機能を有するデバイスであってもよい。たとえば、ネットワークデバイスは、ルータ、またはルート機能を有するスイッチである。

【0041】

50

図2は、本発明の一実施形態による方法の概略フローチャートである。図1を参照すると、実行主体として図1におけるR33が使用され、一例としてルートプレフィックス10.1.0.0/16が使用される。

【0042】

S201:R33は、ROAデータをRPKIサーバからダウンロードし、それによってR33は、ROAデータをローカルに記憶し、ROAデータは、ROAベースとも呼ばれる。ROAベース内のエントリは、ルートプレフィックスとソースASとの間の対応を記録し、ルートプレフィックスに対応するソースASが正しいかどうかを検証するために使用される。

【0043】

たとえば、ネットワーク計画段階において、AS1のための管理者が、RPKIサーバに対応する国際機関に、10.1.0.0/16に対応するソースASとしてAS1を登録するならば、R33によってダウンロードされるROAデータは、10.1.0.0/16とソースAS1との間の対応を含み、言い換えれば、R33によってダウンロードされるROAデータは、10.1.0.0/16を含み、10.1.0.0/16に対応するソースASは、AS1である。

10

【0044】

図2における実施形態において表される方法が実行される毎にROAデータがダウンロードされる必要はないことが理解され得る。

【0045】

S202:R33は、AS1から発信されたルート情報をAS2から受信し、ルート情報は、ルートプレフィックス10.1.0.0/16を搬送し、対応するASパス情報は(AS2, AS1)であり、10.1.0.0/16がAS1から発信され、AS2を通過することを示す。たとえば、R33は、R32からルート情報を受信する。

20

【0046】

S203:R33が10.1.0.0/16をAS4に転送する前に、R33は、10.1.0.0/16に対応するASパス情報内に、R33が配置されるASに関する情報を挿入する。R33は、AS3に関する情報をASパス情報内に挿入して、新しいASパス(AS3, AS2, AS1)を形成し、10.1.0.0/16がAS1から発信され、AS2およびAS3を順に通過することを示す。

【0047】

S204:R33が10.1.0.0/16をAS4に転送する前に、R33は、R33において構成されたアウトバウンドルートポリシーに従ってAS情報を修正する。修正後のAS情報は、検証されるべきソースAS情報を含む。

30

【0048】

図2における実施形態では、検証が実行される前に使用されるAS情報は、ルートプレフィックスに関連付けられた自律システム情報と呼ばれ、ルートプレフィックスに関連付けられた自律システム情報は、検証されるべきソースAS情報を含む。たとえば、ステップS204における修正後のASパスが(AS3)であると仮定すると、ASパス(AS3)は、10.1.0.0/16に関連付けられたAS情報と呼ばれる。ステップS203およびS204は、オプションのステップである。ステップS203は実行されるが、ステップS204は実行されないとき、ステップS203におけるASパス(AS3, AS2, AS1)は、10.1.0.0/16に関連付けられたAS情報と呼ばれる。ステップS203もステップS204も実行されないとき、ステップS202におけるASパス(AS2, AS1)は、10.1.0.0/16に関連付けられたAS情報と呼ばれる。

40

【0049】

S205:R33は、ROAデータ内に一致項目があるかどうかを検証し、一致項目は、ステップS204における修正後のAS情報内に10.1.0.0/16および検証されるべきソースAS情報を含む。

【0050】

以下は、3つのケースを記載する。

【0051】

ケース1

ROAベース内に10.1.0.0/16に一致するエントリがあり、かつエントリ内のソースAS

50

がAS1であることが仮定される。ステップS204が実行されない、またはステップS204における修正後のASパスが(AS9, AS2, AS1)に変更されたならば、検証されるべきソースAS情報は、AS1である。10.1.0.0/16について、検証されるべきソースASは、ROAベース内のソースASと同じであり、両方ともAS1である。R33は、ROAデータが一致項目を含むと決定し、ステップS207を実行する。

【0052】

ケース2

ROAベースは、10.1.0.0/16に一致するエントリを含み、エントリ内のソースASはAS1であり、かつステップS204における修正後のASパスは(AS3, AS2, AS9)であることが仮定される。この場合、検証されるべきソースAS情報は、AS9である。AS1は、AS9とは異なる。したがって、R33は、ROAデータ内に一致項目がないと決定し、ステップS206を実行する。

10

【0053】

ケース3

ROAベース内に10.1.0.0/16に一致するエントリがないならば、R33は、ROAデータ内に一致項目がないと決定し、ステップS208を実行する。ケース3は、R33が、10.1.0.0/16に対応する検証されるべきソースASが正しいかどうか分からないとも理解され得る。言い換えれば、検証結果は「不明」である。

【0054】

3つのケースは、単に、ROAデータ内に一致項目があるかどうかを示すための例として使用されることが理解されるべきである。しかしながら、3つのケースのみがあると考えられるべきでない。

20

【0055】

S206:10.1.0.0/16を送信しないことを決定する。ステップS206の後に、ステップS209がさらに実行されてもよい。

【0056】

S207:AS4内のR41に10.1.0.0/16を送信することを決定する。次いで、ステップS210が実行される。

【0057】

S208:あらかじめ構成されたポリシーに従って、10.1.0.0/16を送信するかどうかを決定する。あらかじめ構成されたポリシーは、10.1.0.0/16を送信すること、または10.1.0.0/16を送信しないことであってもよい。

30

【0058】

S209:アラーム情報を送信する。たとえば、アラーム情報は、ネットワーク管理ワークステーションに送信されてもよい。アラーム情報は、検証結果が不一致であるルートプレフィックスを搬送し、ルートプレフィックスに関する情報、たとえば、ASパス情報を搬送し得る。

【0059】

S210:10.1.0.0/16および修正後のASパスを搬送するルート情報をAS4内のR41に送信する。たとえば、ステップS204においてASパスが(AS9, AS2, AS1)に修正されたならば、送信されたルート情報内のルートプレフィックスは10.1.0.0/16であり、送信されたルート情報内のASパスは、(AS9, AS2, AS1)である。ケース1において、ステップS204が実行されないならば、ステップS210において送信された10.1.0.0/16に対応するASパスは(AS3, AS2, AS1)であることが理解されるべきである。

40

【0060】

図2における実施形態では、ステップS201、S203、204、およびS209はオプションである。加えて、ステップの順序は単に一例であり、ステップは、また、別の適切な順序で実行されてもよい。たとえば、ステップS201は、ステップS205の前に実行されてもよい。

【0061】

50

図2に表された実施形態では、ルートプレフィックスを送信する前に、R33は、まず、ルートプレフィックスに対応するソースAS情報を検証し、検証結果に基づいて、ルートプレフィックスを送信するかどうかを決定する。これは、送信されたルート情報内のソースAS情報の精度を改善し、異常なネットワークフロー方向を引き起こす可能性が低減する。さらに、R33は、アウトバウンドルートポリシーに従って修正後のソースAS情報を検証する。これは、誤った手動構成によって引き起こされるソースAS情報エラーを低減する。加えて、ROAベース内に一致するルートプレフィックスがないならば、あらかじめ構成されたポリシーに従って処理が柔軟に実行される。加えて、ROAデータにおいて一致結果が不一致であるならば、R33内のソースAS情報において不一致が発生したことをネットワーク管理者に通知するためにアラームが送信される。

10

【0062】

図3は、本発明の一実施形態による方法の概略フローチャートである。図1を参照すると、実行主体として図1におけるR33が使用され、一例としてルートプレフィックス10.1.0.0/16が使用される。図3における実施形態は、ルートプレフィックスに対応するASパスに関する情報を検証するために使用される。

【0063】

S301:R33は、ASPAデータをRPKIサーバからダウンロードし、それによってR33は、ASPAデータをローカルに記憶し、ASPAデータは、ASPAベースとも呼ばれる。ASPAベース内のエントリは、ルートプレフィックスと自律システムペアとの間の対応を記録し、ルートプレフィックスに対応するASパスが正しいかどうかを検証するために使用される。

20

【0064】

たとえば、ネットワーク計画段階では、AS1のための管理者は、RPKIサーバに対応する国際機関に、AS1がAS2に10.1.0.0/16を送信することを計画していることを登録する。AS2のための管理者は、RPKIサーバに対応する国際機関に、AS2がAS3に10.1.0.0/16を送信することを計画していることを登録する。AS3のための管理者は、RPKIサーバに対応する国際機関に、AS3がAS4に10.1.0.0/16を送信することを計画していることを登録する。したがって、R33によってダウンロードされるASPAデータは、10.1.0.0/16を含み、10.1.0.0/16に対応するASペアは、[AS1, AS2]、[AS2, AS3]、および[AS3, AS4]である。マーク「[AS1, AS2]」は、AS1が10.1.0.0/16をAS2に送信することを示す。

【0065】

30

図3における実施形態において表された方法が実行されるとき毎にASPAデータがダウンロードされる必要はないことが理解され得る。

【0066】

ステップS302およびS303については、それぞれステップS202およびS203を参照されたい。

【0067】

S304:R33は、R33において構成されたアウトバウンドルートポリシーに従ってAS情報を修正する。修正後のAS情報は、検証されるべきASパス情報を含む。

【0068】

図3における実施形態では、検証前のAS情報は、ルートプレフィックスに関連付けられた自律システム情報と呼ばれ、関連付けられたAS情報は、検証されるべきASパス情報を含む。たとえば、ステップS304における修正後のASパスが(AS3, AS5, AS1)であると仮定すると、ASパス(AS3, AS5, AS1)は、10.1.0.0/16に関連付けられたASに関する情報と呼ばれ、検証されるべきASパス情報は(AS3, AS5, AS1)である。

40

【0069】

S305:R33は、ASPAベース内に一致項目がないことを検証する。

【0070】

R33は、ASPAベース内に10.1.0.0/16に一致するASペアを有するエントリを見つけるが、エントリ内のASペアおよび検証されるべきASパス情報(AS3, AS5, AS1)は一致しない(すなわち、両方が同じではない)。これは、検証されるべきASパス情報が、10.1.0.0/

50

16に関連付けられたソースASがAS1であることを示すためである。AS1は、10.1.0.0/16をAS5に送信し、AS5は、10.1.0.0/16をAS3に送信する。したがって、R33は、ASPAベース内に一致項目がないことを検証する。次いで、ステップS306が実行される。

【0071】

S306:R33は、10.1.0.0/16を送信しないことを決定する。次いで、ステップS307が実行される。

【0072】

S307:R33がアラーム情報を送信する。ステップS307は、オプションのステップである。

【0073】

以下は、図3における実施形態に基づく例を使用することによって、いくつかの他の可能な実装を記載する。実装は、これらの可能な実装に限定されないことが理解されるべきである。

【0074】

可能な場合、ASPAベースは10.1.0.0/16を含み、10.1.0.0/16に対応するASペアは、[AS1, AS2]、[AS2, AS3]、および[AS3, AS4]である。ステップS304は実行されない。検証されるべきASパスは(AS3, AS2, AS1)である。R33は、ASPAベース内に一致項目があると決定し、10.1.0.0/16を送信することを決定し、10.1.0.0およびASパス(AS3, AS2, AS1)を搬送するルート情報を送信する。

【0075】

可能な場合には、ASPAベース内に10.1.0.0/16に一致するエントリがないならば、R33は、ASPAベース内に一致項目がないと決定し、あらかじめ構成されたポリシーに従って、10.1.0.0/16を送信するかどうかを決定する。あらかじめ構成されたポリシーは、10.1.0.0/16を送信すること、または10.1.0.0/16を送信しないことであってもよい。この場合は、また、R33が、10.1.0.0/16に対応する検証されるべきASパス情報が正しいかどうかかわからないとも理解され得る。言い換えれば、検証結果は「不明」である。

【0076】

可能な場合、ASPAベースは10.1.0.0/16を含み、10.1.0.0/16に対応するASペアは、[AS1, AS2]、[AS2, AS3]、および[AS3, AS4]である。ステップS303もステップS304も実行されない。検証されるべきASパスは(AS2, AS1)である。検証されるべきASパスがASペア[AS1, AS2]と一致するので、R33は、ASPAベース内に一致項目があると決定し、10.1.0.0/16を送信することを決定し、10.1.0.0およびASパス(AS2, AS1)を搬送するルート情報を送信する。

【0077】

可能な場合、ASPAベースは10.1.0.0/16を含み、10.1.0.0/16に対応するASペアは、[AS1, AS2]、[AS2, AS3]、および[AS3, AS4]である。ステップS303が実行された後に、ASパスは(AS3, AS2, AS1)である。ステップS304における修正後のASパスは(AS2, AS1)である。R33は、ASPAベース内に一致項目があると決定し、10.1.0.0/16を送信することを決定し、10.1.0.0およびASパス(AS2, AS1)を搬送するルート情報を送信する。

【0078】

図3に表された実施形態では、送信されたルート情報のASパス情報の精度を改善し、異常なネットワークフロー方向を引き起こす可能性が低減するために、ルートプレフィックスを送信する前に、R33は、まず、ルートプレフィックスに関連付けられたASパス情報を検証し、検証結果に基づいて、ルートプレフィックスを送信するかどうかを決定する。さらに、誤った手動構成によって引き起こされるASパス情報エラーを低減するために、R33は、アウトバウンドルートポリシーに従う修正後のASパス情報を検証する。加えて、ASPAベース内に一致するルートプレフィックスがないならば、あらかじめ構成されたポリシーに従って処理が柔軟に実行される。加えて、ASPAデータにおいて一致結果が不一致であるならば、R33内のASパス情報において不一致が発生したことをネットワーク管理者に通知するためにアラームが送信される。

10

20

30

40

50

【 0 0 7 9 】

図4は、本発明の一実施形態による方法の概略フローチャートである。図1を参照すると、実行主体として図1におけるR33が使用され、一例としてルートプレフィックス10.1.0.0/16が使用される。図4において、10.1.0.0/16は、AS3によって、たとえば、R33によって生成される。

【 0 0 8 0 】

S401:R33は、ROAデータをRPKIサーバからダウンロードし、それによってR33は、ROAベースとも呼ばれるROAデータをローカルに記憶する。ROAベース内のエントリは、ルートプレフィックスとソースASとの間の対応を記録し、ルートプレフィックスに関連付けられたソースASが正しいかどうかを検証するために使用される。

10

【 0 0 8 1 】

たとえば、ネットワーク計画段階では、AS3のための管理者が、RPKIサーバに対応する国際機関に、10.1.0.0/16に関連付けられたソースASをAS3として登録する場合。R33によってダウンロードされたROAデータは、10.1.0.0/16とソースAS3との間の対応を含む。言い換えれば、R33によってダウンロードされたROAデータは、10.1.0.0/16を含み、10.1.0.0/16に対応するソースASは、AS3である。

【 0 0 8 2 】

図4における実施形態において表された方法が実行されるとき毎にROAデータがダウンロードされる必要はなくてもよいことが理解され得る。

【 0 0 8 3 】

S402:R33は、ルートプレフィックス10.1.0.0/16を生成する。

20

【 0 0 8 4 】

S403:R33は、10.1.0.0/16をソースAS3に関連付ける。R33が10.1.0.0/16を搬送するルート情報をAS4に送信するとき、R33は、10.1.0.0/16に対応するASパスに、R33が配置されるAS(すなわち、AS3)に関する情報を挿入する。この場合、AS3は、10.1.0.0/16に関連付けられたソースASである。

【 0 0 8 5 】

S404:R33が10.1.0.0/16をAS4に送信する前に、R33は、R33において構成されたアウトバウンドルートポリシーに従ってAS情報を修正する。図4における実施形態では、検証前のAS情報は、ルートプレフィックスに関連付けられたAS情報と呼ばれ、関連付けられたAS情報は、検証されるべきAS情報を含む。修正後のASパスが(AS1)であり、10.1.0.0/16に関連付けられたAS情報が(AS1)であり、検証されるべきAS情報がソースAS情報、すなわちAS1であることが仮定される。

30

【 0 0 8 6 】

S405:R33は、ROAデータ内に一致項目がないことを検証する。検証されるべきソースAS情報はAS1であるが、ROAベース内の10.1.0.0/16に対応するソースASはAS3である。AS1は、AS3とは異なる。したがって、R33は、ROAデータ内に一致項目がないと決定する。ステップS406が実行される。

【 0 0 8 7 】

S406:R33は、10.1.0.0/16を送信しないことを決定する。次いで、ステップS407が実行され得る。

40

【 0 0 8 8 】

以下は、図4における実施形態に基づく例を使用することによって、いくつかの他の可能な実装を記載する。実装は、これらの可能な実装に限定されないことが理解されるべきである。

【 0 0 8 9 】

可能な場合には、ステップS404が実行されない、またはステップS404は実行されるが、ステップS404における修正後のASパスに対応するソースASが依然としてAS3である(たとえば、ステップS404における修正後のASパスは(AS2, AS3)である)図2における実施形態におけるケース1を参照すると、R33は、ROAデータ内に一致項目があると決定する。

50

図2における実施形態におけるケース1を参照されたい。

【0090】

可能な場合、ROAデータベース内に10.1.0.0/16に一致するエントリがないならば、R33は、ROAデータ内に一致項目がないと決定する。図2における実施形態におけるケース3を参照されたい。

【0091】

図4における実施形態では、ステップS401、S404、およびS407はオプションである。加えて、ステップの順序は単に一例であり、ステップは、また、別の適切な順序で実行されてもよい。たとえば、ステップS401は、ステップS405の前に実行されてもよい。

【0092】

上記の例では、R33は、10.1.0.0/16を生成する。したがって、10.1.0.0/16に関連付けられたソースASはAS3である。10.1.0.0/16はまた、R31またはR32によって生成され、R33に送信されてもよいことが理解されるべきである。この場合、10.1.0.0/16に関連付けられたソースASは、依然としてAS3である。実行方法については、図4における実施形態を参照されたい。詳細は再度記載されない。

【0093】

図4に表された実施形態では、送信されたルート情報内のソースAS情報の精度を改善し、異常なネットワークフロー方向を引き起こす可能性を低減するために、ソースASがAS3であるルートプレフィックスを送信する前に、AS3内のネットワークデバイスは、まず、ルートプレフィックスに関連付けられたソースAS情報を検証し、検証結果に基づいて、ルートプレフィックスを送信するかどうかを決定する。他の有益な効果については、図2における実施形態における有益な効果の記載を参照されたい。

【0094】

図2から図4における実施形態は、R33が実行主体である場合を記載する。別の実装では、AS3内のR31またはR32は、また、RPKIサーバとの接続を確立してもよく、ROAデータまたはASPAデータをダウンロードし、10.1.0.0/16を送信する前に10.1.0.0/16に対応するAS情報を検証する。具体的な方法については、図2から図4における実施形態におけるR33によって実行されるステップを参照されたい。詳細は、ここで再度記載されない。

【0095】

図2から図4における実施形態では、R33は、ROAデータまたはASPAデータをRPKIサーバからダウンロードする。別の可能な設計では、RPKIサーバは、ROAデータまたはASPAデータをR33に能動的にプッシュする。

【0096】

図5は、方法の実施形態におけるネットワークデバイスの可能な構造の概略図である。ネットワークデバイス500は、図1におけるR31、R32、またはR33であり得る。ネットワークデバイス500が図1におけるR33であるならば、ネットワークデバイス500は、図2、図3、または図4に表された実施形態におけるR33の機能を実現する。図5を参照すると、ネットワークデバイス500は、取得モジュール501、検証モジュール502、および決定モジュール503を含む。これらのモジュールは、方法の実施形態におけるネットワークデバイスの対応する機能を実行し得る。取得モジュールは、図2におけるステップS202からS205、図3におけるステップS302からS305、または図4におけるステップS402からS404を実行する際にネットワークデバイス500をサポートするように構成されたルートプレフィックス取得サブモジュールおよび自律システム情報取得サブモジュールを含み得る。検証モジュール502は、図2におけるステップS205、図3におけるステップS305、または図4におけるステップS405を実行する際にネットワークデバイス500をサポートするように構成される。決定モジュール503は、図2におけるステップS206からS208、図3におけるステップS306、または図4におけるステップS406を実行する際にネットワークデバイス500をサポートするように構成される。ネットワークデバイス500は、ルート起点情報ベース取得モジュール504および送信モジュール506をさらに含む。ルート起点情報ベース取得モジュール504は、図2におけるステップS201、図3におけるステップS301、また

10

20

30

40

50

は図4におけるステップS401を実行する際にネットワークデバイス500をサポートするように構成される。送信モジュール506は、図2におけるステップS210を実行する際にネットワークデバイス500をサポートするように構成される。任意選択で、ネットワークデバイス500は、図2におけるステップS209、図3におけるステップS307、または図4におけるステップS407を実行する際にネットワークデバイス500をサポートするように構成されたアラームモジュール505をさらに含む。

【0097】

具体的な実行プロセスについては、図2、図3、または図4に表された実施形態における対応するステップの詳細な記載を参照されたい。詳細は、ここで再度記載されない。

【0098】

統合モジュールが使用されるとき、図5における実施形態におけるモジュールが統合されてもよい。たとえば、図5における実施形態における検証モジュール502および決定モジュール503は、1つのモジュールに組み合わされてもよい。

【0099】

図6は、方法の実施形態におけるネットワークデバイスの可能な構造の概略図である。ネットワークデバイス600は、図1におけるR31、R32、またはR33であり得る。ネットワークデバイス600が図1におけるR33であるならば、ネットワークデバイス600は、図2、図3、または図4に表された実施形態におけるR33の機能を実現する。ネットワークデバイス600は、プロセッサ601、メモリ602、通信インターフェース603、およびバス604を含む。プロセッサ601、通信インターフェース603、およびメモリ602は、バス604を通じて互いに接続される。バス604は、周辺構成要素相互接続(peripheral component interconnect、略してPCI)バス、拡張業界標準アーキテクチャ(extended industry standard architecture、略してEISA)バス、または同様のものであり得る。バスは、アドレスバス、データバス、制御バス、および同様のものに分類されてもよい。表現の容易さのために、図6においてバスを表現するために1つの太線のみが使用されるが、これは、1つのバスのみまたは1種類のバスのみがあることを意味しない。プロセッサ601は、コンピュータプログラムを記憶するように構成される。コンピュータプログラムは、プログラム命令を含む。プロセッサ601は、プログラム命令を呼び出して、図2、図3、または図4におけるステップを実行するように構成される。

【0100】

可能な設計では、通信インターフェース603は、図2におけるステップS201、S202、S209、およびS210、図3におけるステップS301、S302、およびS307、または図4におけるステップS401およびS407を実行する。プロセッサ601は、プログラム命令を呼び出して、図2におけるステップS203からS208、図3におけるステップS303からS306、または図4におけるステップS402からS406を実行するように構成される。

【0101】

本発明の一実施形態は、コンピュータ記憶媒体をさらに提供する。コンピュータ可読記憶媒体は、プログラムを記憶する。プログラムが実行されるとき、コンピュータは、方法の実施形態における方法を実現することが可能にされる。

【0102】

本発明の一実施形態は、プログラム命令に関連するハードウェアを含むルート処理装置をさらに提供する。ハードウェアは、方法の実施形態における方法において使用される。

【0103】

本発明の実施形態において言及される「第1の」は、単に名称識別子として使用され、順序における1番目を表現しない。この規則は、「第2の」にも適用可能である。

【0104】

本発明の実施形態において開示された内容において記載された方法のステップは、ハードウェア、またはソフトウェア命令を実行することによってプロセッサによって実現され得る。ソフトウェア命令は、対応するソフトウェアモジュールによって形成されてもよく、ソフトウェアモジュールは、ランダムアクセスメモリ(random access memory, RAM

10

20

30

40

50

)、フラッシュメモリ、リードオンリメモリ(read only memory, ROM)、消去可能プログラム可能リードオンリメモリ(erasable programmable ROM, EPROM)、電氣的消去可能プログラム可能リードオンリメモリ(electrically EPROM, EEPROM)、ハードディスク、リムーバブルハードディスク、光ディスク、またはこの技術分野においてよく知られた任意の他の形式の記憶媒体に記憶されてもよい。たとえば、記憶媒体は、プロセッサに結合され、それによってプロセッサが記憶媒体から情報を読み取り、記憶媒体に情報を書き込むことができる。確かに、記憶媒体は、その代わりに、プロセッサの構成要素であってもよい。プロセッサおよび記憶媒体は、ASIC内に配置されてもよい。

【0105】

上記の1つまたは複数の例において、本発明において記載された機能は、ハードウェア、ソフトウェア、ファームウェア、またはそれらの任意の組み合わせによって実現され得ることをこの技術分野の当業者は認識すべきである。本発明がソフトウェアによって実現されるとき、上記の機能は、コンピュータ可読媒体に記憶され、またはコンピュータ可読媒体内の1つまたは複数の命令またはコードとして伝送されてもよい。コンピュータ可読媒体は、コンピュータ記憶媒体および通信媒体を含む。通信媒体は、コンピュータプログラムが1つの場所から別の場所に伝送されることを可能にする任意の媒体を含む。記憶媒体は、汎用または専用のコンピュータにアクセス可能な任意の利用可能な媒体であってもよい。

10

【0106】

本発明の目的、技術的解決策、および有益な効果は、上記の具体的な実施形態においてさらに詳細に記載されている。上記の記載は、単に本発明の具体的な実装であるが、本発明の保護範囲を限定するために意図されないことが理解されるべきである。本発明の技術的解決策に基づいて、行われる任意の修正、等価な置換、および改善は、本発明の保護範囲内にあるものである。

20

【符号の説明】

【0107】

- 500 ネットワークデバイス
- 501 取得モジュール
- 502 検証モジュール
- 503 決定モジュール
- 504 ルート起点情報ベース取得モジュール
- 505 アラームモジュール
- 506 送信モジュール
- 600 ネットワークデバイス
- 601 プロセッサ
- 602 メモリ
- 603 通信インターフェース
- 604 バス

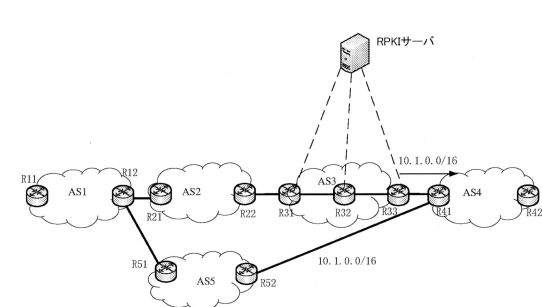
30

40

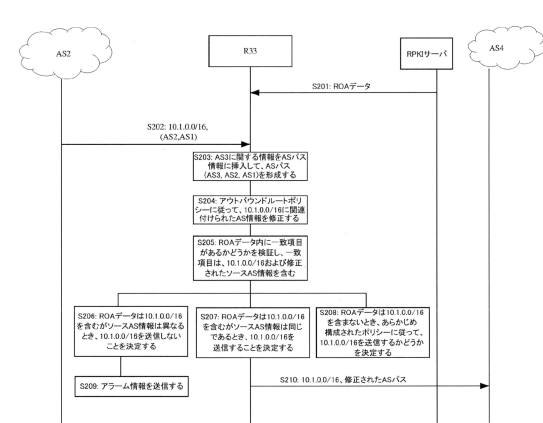
50

【図面】

【図 1】

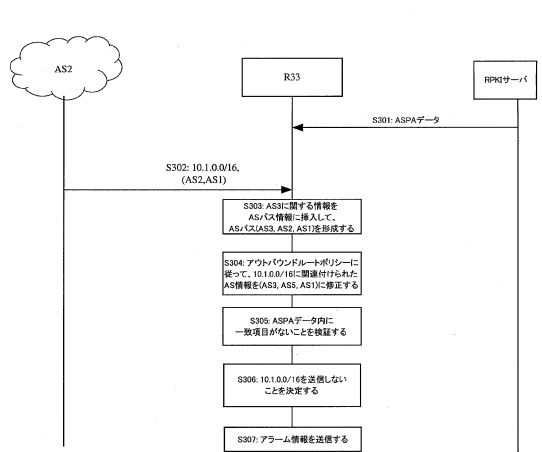


【図 2】

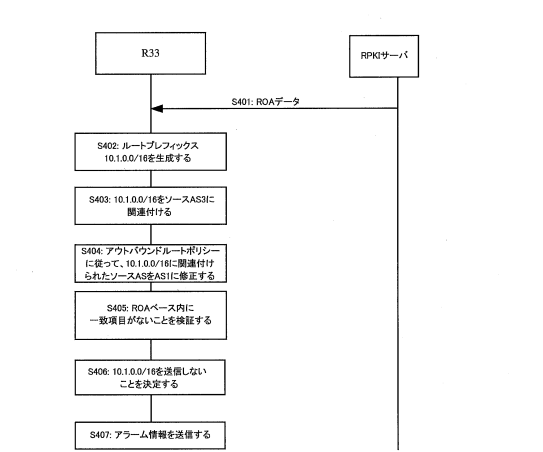


10

【図 3】



【図 4】



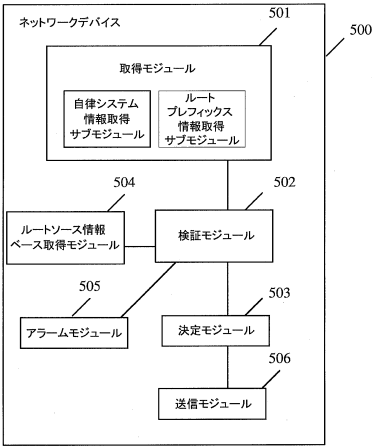
20

30

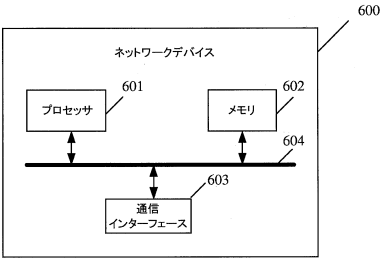
40

50

【図 5】



【図 6】



10

20

30

40

50

フロントページの続き

- (74)代理人 100133569
弁理士 野村 進
- (72)発明者 王 ▲海▼波
中華人民共和国 5 1 8 1 2 9 広東省深▲チェン▼市龍岗区坂田 華為総部▲ベン▼公楼
- (72)発明者 庄 ▲順▼万
中華人民共和国 5 1 8 1 2 9 広東省深▲チェン▼市龍岗区坂田 華為総部▲ベン▼公楼
- 審査官 宮島 郁美
- (56)参考文献 特開 2 0 1 1 - 0 8 7 3 0 2 (J P , A)
米国特許出願公開第 2 0 1 1 / 0 0 9 3 6 1 2 (U S , A 1)
特開 2 0 0 9 - 1 6 4 9 1 7 (J P , A)
中国特許出願公開第 1 0 6 0 6 0 0 1 4 (C N , A)
Validation of Route Origination using the Resource Certificate PKI and ROAs draft-ietf-sidr-roa-validation-10.txt, インターネットホームページ, 米国, 2010年11月11日, <https://data.ietf.org/doc/html/draft-ietf-sidr-roa-validation>
I R R を用いた次世代 B G P 経路制御アーキテクチャーの提案, 電子情報通信学会技術研究報告, V o l . 1 0 6 N o . 4 6 2 , 2007年01月11日
- (58)調査した分野 (Int.Cl. , D B 名)
H 0 4 L 1 2 / 0 0 - 1 3 / 1 8 , 4 1 / 0 0 - 6 9 / 4 0