

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第6920294号
(P6920294)

(45) 発行日 令和3年8月18日 (2021.8.18)

(24) 登録日 令和3年7月28日 (2021.7.28)

(51) Int. Cl.	F I
HO 4 L 12/24 (2006.01)	HO 4 L 12/24
HO 4 L 12/725 (2013.01)	HO 4 L 12/725
HO 4 L 12/721 (2013.01)	HO 4 L 12/721 Z

請求項の数 13 (全 47 頁)

(21) 出願番号	特願2018-523369 (P2018-523369)	(73) 特許権者	518024699
(86) (22) 出願日	平成28年7月21日 (2016.7.21)		ダイナミック・ネットワーク・サービス・インコーポレイテッド
(65) 公表番号	特表2018-521610 (P2018-521610A)		DYNAMIC NETWORK SERVICES, INC.
(43) 公表日	平成30年8月2日 (2018.8.2)		アメリカ合衆国、03101 ニュー・ハンプシャー州、マンチェスター、ダウ・ストリート、150、タワー・トゥー
(86) 国際出願番号	PCT/US2016/043328	(74) 代理人	110001195
(87) 国際公開番号	W02017/015454		特許業務法人深見特許事務所
(87) 国際公開日	平成29年1月26日 (2017.1.26)	(72) 発明者	ジミエウスキ、アール・エドワード
審査請求日	令和1年6月7日 (2019.6.7)		アメリカ合衆国、03784 ニュー・ハンプシャー州、ウェスト・レバノン、ジルソン・ロード、2
(31) 優先権主張番号	62/195,488		
(32) 優先日	平成27年7月22日 (2015.7.22)		
(33) 優先権主張国・地域又は機関	米国 (US)		

最終頁に続く

(54) 【発明の名称】 ルート追跡を用いて地理位置を特定するための方法、システムおよび装置

(57) 【特許請求の範囲】

【請求項 1】

インターネットに動作可能に接続され、インターネットプロトコル (IP) アドレスを有する装置の位置を特定するための方法であって、

特定の実体によって運営されているジオロケーションサーバが前記特定の実体によって運営されていない第三者サービスから、前記装置の第三者推定地理位置を取得するステップを含み、前記第三者推定地理位置は、前記装置の前記 IP アドレスに基づき、

インターネットに動作可能に接続された複数のセンサの各々と前記装置の前記 IP アドレスとの間の送信に関連する遅延を計算することにより、前記複数のセンサにそれぞれ対応する複数の遅延を取得するステップを含み、前記複数のセンサの各々は、異なる地理位置に配置されており、

前記複数の遅延から、最も短い遅延を選択するステップと、

前記複数のセンサの中から、前記選択された最も短い遅延に対応する特定のセンサを特定するステップと、

前記特定のセンサに対応する前記選択された最も短い遅延に少なくとも部分的に基づいて、前記特定のセンサと前記装置との間の最大可能な地理距離を推定するステップと、

前記装置の前記第三者推定地理位置が前記特定のセンサの地理位置から前記最大可能な地理距離内に位置するか否かを判定するステップと、

前記装置の前記第三者推定地理位置が前記特定のセンサの地理位置から前記最大可能な地理距離内に位置していない場合、前記第三者推定地理位置を破棄するステップと、

10

20

前記装置の前記第三者推定地理位置が前記特定のセンサの地理位置から前記最大可能な地理距離内に位置していない場合、前記装置の新たな推定地理位置を決定するステップとを含み、前記新たな推定地理位置は、前記特定のセンサの地理位置から前記最大可能な地理距離内に位置し、

前記新たな推定地理位置に少なくとも部分的に基づいて、前記装置へのパケットの送信および／または前記装置からのパケットの送信に関連する遅延を予測するステップと、

パケット遅延を減少させるおよび／またはパケット量を増加させるために、予測された前記遅延に基づいて、前記装置におよび／または前記装置からパケットをルーティングするステップとをさらに含む、方法。

【請求項 2】

10

前記装置の前記第三者推定地理位置を取得するステップは、サーバから、前記第三者推定地理位置のデジタル表現をダウンロードすることを含む、請求項 1 に記載の方法。

【請求項 3】

前記遅延を計算することは、

前記複数のセンサの各々から、前記装置との間のパケットの送信に関連する往復時間 (R T T) の複数の測定値を取得することと、

前記 R T T の複数の測定値に対応する R T T 分布を決定することと、

前記 R T T 分布に少なくとも部分的に基づいて、前記複数のセンサの各々についての遅延を推定することとを含む、請求項 1 または 2 に記載の方法。

【請求項 4】

20

前記 R T T 分布を決定することは、マルチプロトコルラベルスイッチング (M P L S) ホップに関連する R T T 測定値を排除することを含む、請求項 3 に記載の方法。

【請求項 5】

遅延を推定することは、前記 R T T 分布に基づいて、信頼区間に入る前記遅延を推定することを含む、請求項 3 に記載の方法。

【請求項 6】

前記最大可能な地理距離を推定するステップは、前記選択された最も短い遅延に関連する前記信頼区間に入る前記最大可能な地理距離を推定することを含む、請求項 5 に記載の方法。

【請求項 7】

30

前記特定のセンサは、遅延を測定するために使用される少なくとも 2 0 0 個のセンサのうち 1 つである、請求項 1 ~ 6 のいずれか 1 項に記載の方法。

【請求項 8】

前記遅延を計算することは、

前記複数の遅延のうち、少なくとも 1 つの遅延の少なくとも 1 つの誤差源を特定することと、

前記少なくとも 1 つの誤差源を補償するように、前記複数の遅延のうち、前記少なくとも 1 つの遅延を調整することとを含む、請求項 1 ~ 7 のいずれか 1 項に記載の方法。

【請求項 9】

40

前記複数の遅延から、少なくとも 3 つの遅延を選択するステップと、

前記少なくとも 3 つの遅延を測定した少なくとも 3 つのセンサを特定するステップと、

前記少なくとも 3 つのセンサの三角測量を行うステップとをさらに含む、請求項 1 ~ 8 のいずれか 1 項に記載の方法。

【請求項 10】

前記少なくとも 3 つのセンサの各々の遅延および地理位置に基づいて、前記 I P アドレスをユニキャスト I P アドレスとして特定するステップをさらに含む、請求項 9 に記載の方法。

【請求項 11】

前記新たな推定地理位置に少なくとも部分的に基づいて、特定の地理区域の周りにまたは特定の地理区域からパケットをルーティングするステップをさらに含む、請求項 1 ~ 1

50

0 のいずれか 1 項に記載の方法。

【請求項 1 2】

前記新たな推定地理位置に基づいて、インターネットサービスプロバイダ (ISP) を選択するステップをさらに含む、請求項 1 ~ 1 1 のいずれか 1 項に記載の方法。

【請求項 1 3】

前記新たな推定地理位置に基づいて、ドメインネームシステム (DNS) クエリを解析するステップをさらに含む、請求項 1 ~ 1 2 のいずれか 1 項に記載の方法。

【発明の詳細な説明】

【技術分野】

【0001】

関連出願の相互参照

本願は、米国特許法第 1 1 9 条 (e) に基づき、2015 年 7 月 22 日に出願され且つ「ルート追跡を用いて地理位置を特定するための方法、システムおよび装置」と題された米国特許出願第 62 / 195488 号の優先権を主張する。当該出願の全体は、参照により本明細書に組み込まれる。

【背景技術】

【0002】

背景

インターネットプロトコル (IP) 地理位置 (geographic location) または IP ジオロケーション (geolocation) は、特定の IP アドレスに関連する装置の物理位置を推測または推定することである。換言すると、IP ジオロケーションは、所望レベルの特異度で、IP アドレスを地球上のある位置に特定することである。特定の IP アドレスの地理位置を推測または推定するための技術は、(1) インターネットホストまたはローカルネットワークノードに対応するドメインネームサーバ (DNS) 名、(2) IP アドレスと、既知の地理位置に配置された一群の装置との間の遅延測定値、および (3) IP - 位置の部分マッピング情報と境界ゲートウェイプロトコル (border gateway protocol、BGP) プレフィックス情報との組み合わせから、地理位置を推定する。これらの技術の詳細については、例えば、参照によりその全体が本明細書に組み込まれた米国特許第 7711846 号を参照する。

【発明の概要】

【0003】

残念なことに、IP ジオロケーション推定値は、ケーブル、ルータ、サーバおよびアクセス装置などの物理関係ではなく、IP アドレス、ルーティングプロトコルおよびアプリケーションの論理関係の観測に基づいて推定されたため、不正確であり、場合によって非常に不正確である。論理関係は、しばしば物理関係に関連されるが、必ずしも連携するとは限らない。例えば、インターネット空間では互いに隣接する IP アドレスは、必ずしも互いに地理的に隣接するとは限らず、その逆も同様である。例えば、ブラジルとペルーとは、互いに地理的に隣接するが、インターネット空間では互いに隣接していない。また、装置の物理位置の変化は、必ずしも装置のインターネット空間位置の変化に対応するとは限らず、その逆も同様である。特定の BGP プレフィックスを公告したルータを検討する。プレフィックスを公告することによって、ルータは、物理空間において移動されても、論理的な観点から固定である 1 つ以上の論理的なインターネット関係を確立する。

【0004】

また、プレフィックスを 1 つの場所に配置する必要がない。エンドユーザ (end user) ネットワークは、しばしば単一の地理範囲を有するが、例えば、(ルータ、スイッチおよびファイアウォールを含む) 広域ネットワークに使用されたインフラストラクチャ IP アドレスは、グローバル範囲であり得るプロバイダの運用領域の全体に分散されることがある。したがって、連続のインフラストラクチャ IP アドレスは、単一のプレフィックスとしてインターネットの他の部分に接続されても、物理的に離れた場所に配置されることがある。

10

20

30

40

50

【 0 0 0 5 】

さらに、ジオロケーションの推測または推定に使用されたネットワーク情報は、不正確、不完全、またはその両方である可能性がある。プレフィックスの登録は、しばしば、エンドユーザの自己報告によって行われ、地域インターネット登録官がその有効性をチェックしない。したがって、DNS情報が間違った可能性がある。例えば、特定の区域（例えば、英国）に関連するドメインは、必ずしもその区域にホストされるとは限らない。インターネットサービスプロバイダは、しばしば、都市の略語をルータのインターフェイス名に使用するが、命名規則は、プロバイダによって異なり、必ずしも最新のものととは限らない。例えば、ルータインターフェイスは、光ファイバの遠端に接続されているある都市の名前で命名されてもよい。同様に、BGP情報、特に広範囲の地理区域（例えば、大陸）をカバーするプレフィックスを公告する地域プロバイダのBGP情報は、不確定である可能性がある。

10

【 0 0 0 6 】

また、人為的な遅延によって時間測定値が長くなり、その結果、インターネットノード間の距離推定値を増加することによって、遅延測定値は、しばしば不正確である。これらの遅延は、パケットを符号化するための時間としての直列遅延と、ルータのキュー遅延と、総伝播距離と伝播速度（光ファイバの場合、約200000km/秒）との積に等しい伝播遅延とを含むがこれらに限定されない。通信媒体（通常、光ファイバ）が2点の間に直線ではなく蛇行して配置された場合、伝播遅延がより大きくなる。実際に、多くの光ファイバは、既存の送電線用地に沿って蛇行して配置される。他の場合、光ファイバは、地理的な制約（例えば、丘および川）、経済的な制約（例えば、不動産所有者とインターネットサービスプロバイダとの間のビジネス関係の欠如）、またはその両方の制約によって、蛇行して配置される。一般的には、遅延が長くなれば、伝播経路が遠回りになる可能性が高くなり、エンドポイント間の距離推定値の人為的な増加をもたらす可能性も高くなる。

20

【 0 0 0 7 】

不完全または不正確なネットワーク情報および不正確な遅延測定値によって、IPアドレスの物理位置の推定に関連する不確実性レベルは、ジオロケーション推定値の特異度レベルと共に大きくなる。例えば、非常に高い信頼度で、特定のIPアドレスの惑星（地球）を推測することができる。IPアドレスの大陸を特定する場合、信頼度が低下する傾向がある。また、IPアドレスの国を特定する場合、部分的な理由として各国の大きさおよび国境が変動するため、不確実性がさらに増加する傾向がある。さらに、首都圏/都市レベルでIPジオロケーションを推定する場合の信頼度は、都市の位置および他の都市との近接度に部分的に依存して、さらに低下する傾向がある。

30

【 発明が解決しようとする課題 】

【 0 0 0 8 】

概要

発明者らは、不正確な登録および/またはDNS情報および遅延測定値における遅延によって、利用可能なIPジオロケーションデータが不正確になる傾向があることを認識した。また、プレフィックスが複雑な方法で重なり、相関することがあるため、正確なIPジオロケーション問題を複雑化する。また、本発明者らは、不正確なIPジオロケーションデータがインターネットトラフィックの管理およびトラブルシューティングに悪影響を及ぼすことを認識した。より具体的には、不正確なIPジオロケーション推定は、高いDNS遅延および不正確なDNSベースド負荷分散を引き起こす可能性がある。例えば、トラフィックが実際に米国から来た場合、負荷をヨーロッパのリソースに分散してしまう。さらに、不正確なIPジオロケーション推定は、ネットワーク問題が発生した場所および原因に関する不正確な結論をもたらす、その結果、不適切または非効率的もしくは無駄なトラブルシューティングをもたらす可能性がある。

40

【 課題を解決するための手段 】

【 0 0 0 9 】

50

本技術の実施形態は、他のＩＰジオロケーション技術よりもより正確に実行できるＩＰジオロケーションの方法およびシステムを含む。１つの例は、インターネットに動作可能に接続され、ＩＰアドレスを有する少なくとも１つの装置を特定するための方法を含む。この方法は、第三者から、装置のＩＰアドレスに基づいた装置の第１推定地理位置を自動的に取得するステップを含む。また、方法は、インターネットに動作可能に接続された複数のセンサの各センサから装置のＩＰアドレスへの送信に関連する各々の遅延分布を測定することを含む。複数のセンサの各センサは、異なるジオロケーションに配置される。プロセッサは、測定された遅延分布から少なくとも１つの遅延を選択し、選択された遅延を測定したセンサを特定する。プロセッサは、遅延に基づいて、センサと装置との間の最大可能な地理距離を推定し、それを装置の第１推定地理位置とセンサの地理位置との間の距離と比較する。装置の第１推定地理位置が、センサの地理位置から推定された最大可能な地理距離内に位置していない場合、プロセッサは、最大可能な地理距離および地理位置に基づいて装置の第２推定地理位置を決定する。

10

【 0 0 1 0 】

他の実施形態は、インターネットに動作可能に接続され、ＩＰアドレスを有する少なくとも１つの装置の地理位置を推定するための別の方法を含む。この方法は、第一者から、装置のＩＰアドレスに基づいた装置の第１推定地理位置を自動的に取得するステップと、第二者から、装置のＩＰアドレスに基づいた装置の第２推定地理位置を自動的に取得するステップとを含む。プロセッサは、第１推定地理位置と第２推定地理位置との間の距離を決定する。その距離が所定の閾値を超える場合、プロセッサは、インターネットに動作可能に接続された複数のセンサの各センサから装置のＩＰアドレスへの送信に関連する各々の遅延を測定する。複数のセンサの各センサは、異なる地理位置に配置される。プロセッサは、各々の遅延から少なくとも１つの遅延を選択し、選択された遅延を測定したセンサを特定し、選択された遅延に少なくとも部分的に基づいて、センサと装置との間の最大可能な地理距離を推定する。その後、プロセッサは、センサの地理位置から推定された最大可能な地理距離に基づいて、装置の第３推定地理位置を決定する。

20

【 0 0 1 1 】

更新された新たなジオロケーション推定値を用いて、装置におよび／または装置からパケットをルーティングすることによって、パケット遅延を減少させるおよび／またはパケット量を増加させることができる。また、更新された新たなジオロケーション推定値を用いて、例えば、データセキュリティに関する規則または法律に従って、特定の地理区域の周りに、特定の地理区域を回避して、または特定の地理区域を通して、パケットをルーティングすることができる。ジオロケーション推定値を使用して、インターネットサービスプロバイダ（ＩＳＰ）を選択することができ、ドメインネームシステム（ＤＮＳ）クエリを解析することもできる。

30

【 0 0 1 2 】

また、本技術の実施形態は、インターネットプロトコル（ＩＰ）アドレス内の指定のネットワークプレフィックスのジオロケーションを推定するための方法および装置を含む。指定のネットワークプレフィックスの地理位置を推定するために、プロセッサまたは他のコンピュータ装置は、指定のネットワークプレフィックスのトランシット木を割り出す。トランシット木は、指定のネットワークプレフィックスの自律システム（ＡＳ）経路を表し、第１ＡＳと第２ＡＳとの間の少なくとも１つのエッジを示す。プロセッサは、第１ＡＳの地理位置および第２ＡＳの地理位置に基づいて、指定のネットワークプレフィックスの第１推定地理位置を推定する。場合によって、プロセッサは、第１推定地理位置と、第三者から得られた指定のネットワークプレフィックスの第２推定地理位置とを比較することができる。第１推定地理位置と第２推定地理位置とが一致しない場合、プロセッサは、指定のネットワークプレフィックスとの間の送信遅延測定値を用いて、第１推定地理位置を検証することができる。

40

【 0 0 1 3 】

本技術のさらに別の実施形態は、第１のＩＰアドレスを有する装置のジオロケーション

50

を推定するための方法および装置を含む。この場合、コンピュータネットワーク（例えば、インターネット）に接続された収集装置または他の装置は、パケットを第1のIPアドレスに送信する。パケットに応答して、収集装置は、第1のIPアドレスとは異なる第2のIPアドレスから、ポート到達不能なメッセージを受信する。収集装置または収集装置に結合された別の処理装置は、ポート到達不能なメッセージに응答して、第2のIPアドレスが第1のIPアドレスのエイリアスであると判定する。したがって、収集装置または他の処理装置は、第1のIPアドレスおよび第2のIPアドレスの共通地理位置を推定する。

【0014】

前述した発想および以下でより詳細に説明する追加の発想（これらの発想が相互に矛盾しない前提で）の全ての組み合わせは、本明細書に開示された発明の主題の一部であると理解すべきである。特に、本開示の最後の特許請求の範囲の全ての組み合わせは、本明細書に開示された発明の主題の一部であると考えられる。また、本明細書に明示的に使用された用語および参照により他の開示に援用された用語は、本明細書に開示された特定の概念と最も一致する意味で解釈されるべきであることを理解すべきである。

【0015】

当業者であれば、図面は、主に説明の目的のものであり、本明細書に記載された発明の主題の範囲を限定するものではないことを理解するであろう。図面は、必ずしも一定の縮尺描かれていない。いくつかの例において、本明細書に開示された発明の主題の様々な態様は、異なる特徴を容易に理解させるために、図面においてこれらの特徴を拡大または縮小することがある。図面において、同様の参照符号は、一般的に、同様の特徴（例えば、機能的におよび/または構造的に類似する要素）を指す。

【0016】

本発明の特徴および利点は、図面と併せて以下の詳細な説明からより明らかになるであろう。

【図面の簡単な説明】

【0017】

【図1A】特定のIPアドレスに関連する少なくとも1つの装置のジオロケーションを推定するためのプロセスを示す図である。

【図1B】特定のIPアドレスに関連する少なくとも1つの装置のジオロケーションを推定するための別のプロセスを示す図である。

【図1C】図1Aおよび1Bに示されたプロセスを用いて得られたIPアドレスのジオロケーション推定値に対する訂正を示すマップである。

【図2A】図1Aおよび1Bに示すIPジオロケーションプロセスの実行に適したジオロケーションシステムの一例を示す図である。

【図2B】物理的および仮想的なルート追跡データ収集装置および/またはネットワークセンサを含むルート追跡データ収集装置の位置を示す図である。

【図2C】グローバルに配置されたルート追跡データ収集装置および/またはネットワークセンサによってカバーされた地理的な区域を示す図である。

【図2D】グローバルに配置されたルート追跡データ収集装置および/またはネットワークセンサによってカバーされた地理的な区域を示す図である。

【図3A】ジオロケーションサーバの一例を示す図である。

【図3B】ルート追跡収集データ装置の一例を示す図である。

【図4】TTLを増分することによって、（図2Aに黒い矢印で示された）特定の追跡ルートを決定するためのプロセスを示す図である。

【図5】3つのルート追跡データ収集装置によってカバーされた区域の交差を示す図である。

【図6A】マルチプロトコルラベルスイッチング（MultiProtocol Label Switching、MPLS）トンネルを経由したルーティングを示す図である。

【図6B】MPLSトンネルに関連するIPアドレスのジオロケーションを推定するため

10

20

30

40

50

のプロセスを示す図である。

【図 7 A】IP アドレスのエイリアス除去およびジオロケーションの推定を行うためのプロセスを示す図である。

【図 7 B】図 7 A のプロセスを用いて、特定および測位されたエイリアス化 IP アドレスを示すグラフである。

【図 8 A】ジオロケーションサーバによって生成された、インターネットの起源からコアまで遷移したネットワークプレフィックスの集合を示すトランシット木である。

【図 8 B】図 8 A に示すトランシット木を用いて、指定のネットワークプレフィックスのジオロケーションを推定するためのプロセスを示す図である。

【図 9】単一区域に配置されたネットワークプレフィックス群の境界ゲートウェイプロトコル (BGP) 対時間のルーティング安定性を示す図である。

10

【発明を実施するための形態】

【0018】

詳細な説明

以下、追跡ルートおよび他の情報を用いて、地理位置 (geographic location) を特定するための本発明のシステム、方法および装置に関連する様々な発想および実施形態をより詳細に説明する。上記で説明されおよび以下により詳細に検討される様々な発想は、特定の実施方法に限定されず、多くの方法のいずれかで実施され得ることを理解すべきである。特定の実現例および応用例は、主に説明の目的で提供される。

【0019】

20

理論的には、全てのインターネット性能データを知っていれば、インターネットトラフィックを正確にルーティングすることができる。しかしながら、実際には、全てのインターネット性能データが知られていないため、利用可能なインターネット性能データおよび地理位置情報を用いて、インターネットトラフィックを調整する。例えば、南米の IP アドレスからのデータリクエストは、その IP アドレスと南米のデータセンタとの地理的な近接度に基づいて、南米のデータセンタにルーティングされる可能性がある。しかしながら、南米の IP アドレスの相互接続には制限がある。例えば、アマゾン熱帯雨林およびアンデス山脈は、接続に大きな物理的な障壁を与えている。その代わりに、多くの場合、南米のインターネットトラフィックは、マイアミを経由してルーティングされる。したがって、ブラジルの IP アドレスからデータをリクエストした場合、コロンビアデータセンタがブラジルの IP アドレスに地理的に近いにも関わらず、実際には、コロンビアのデータセンタではなく、そのデータリクエストをマイアミのデータサーバにルーティングした方がより効率的である。同様に、特定の IP アドレスの地理位置に関する情報が不正確の場合、不必要の遅延および混雑などを増やすルーティングをもたらしてしまう。

30

【0020】

IP アドレスの地理位置 (ジオロケーション: geolocation) に関するより正確な推定値を用いて、インターネット上のトラフィックをより効率的に案内することができる。例えば、IP アドレスの地理位置を用いて、IP アドレスにまたは IP アドレスからパケットを送信するための理論上の遅延制限値を予測することができる。理論上の遅延制限値になるべき近づくようにルーティングを決定するために、ジオロケーションデータをグローバル遅延マップに関連付ける必要がある。ジオロケーションデータを用いて、インテリジェントなルーティングの判断に十分な情報を提供することができ且つ発信元および宛先の位置のある程度の匿名性を提供することができる程度の精度で、トラフィックの発信元および宛先の物理位置を特定することができる。例えば、輸出規制を遵守するためまたは盗聴の危険性を減らすため、ジオロケーション情報を用いて、特定の国を経由してまたは特定の国を避けて、機密なデータをルーティングすることができる。また、ジオロケーション情報を用いて、ネットワーク問題の解決およびネットワークの拡張計画を行うことができる。

40

【0021】

遅延測定値、DNS 名、ルーティング情報、または様々な公開または私用ソース (例え

50

ば、データセンタの公開位置、掲示板、店舗位置)から、IPアドレスのジオロケーションを推定することができる。しかしながら、光ファイバが直線に配置されず、地理的に離れたポイントが十分ではなく、測定ポイントの位置精度が十分ではなく且つ均一的に/理想的に分布されておらず、光の速度が速すぎて(光ファイバの1ミリ秒=100キロ)短い測定ができないなどの理由で、多くの既知ポイントからの遅延測定値を使用した三角測量は、概ねの場所しか推定できない。IPアドレスに関連する都市名または空港コードをしばしば含むDNS情報を用いて、ISPのインフラストラクチャの異なるIPアドレスから復元された名前をアルゴリズム的に解析することができるが、ISPの間に命名規則が異なる、矛盾するまたは間違える可能性がある。また、装置を移動することができるため、装置の位置の確認が困難である。特定のサービスプロバイダのサービス地域に基づくルーティング情報から、地理位置を推定することができるが、地域の有力企業のマクロレベルしかできない。

10

【0022】

本明細書に開示された技術は、遅延測定値、DNS情報およびルーティング情報に基づくIPジオロケーションに関する。多くの他の技術とは異なり、本発明の例示的な技術を用いて、市販のジオロケーション情報を含む第三者からのジオロケーションデータの矛盾または誤差を検出し、訂正することができる。これらのジオロケーションデータは、エンドユーザにとって正しいが、インフラストラクチャにとって正しくないため、インターネットトラフィックのルーティングおよび解析における有用性が制限されている。

【0023】

20

第三者のIPジオロケーション推定値における誤差の特定および訂正

図1Aは、第三者のIPジオロケーションデータから、特定のIPアドレスに関連する装置のジオロケーション推定値を精密化するためのプロセス101を示す図である。この例において、プロセスは、1つ以上のIPアドレスの経緯度推定値を含み得るジオロケーションデータを取得すること(ブロック111)から開始する。このデータは、第三者から、例えば、商用位置情報源(例えば、Neustar、MaxMind、Digital Envoyなど)、プレフィックス登録データ、または他の公開または私用ソースから、定期的にまたはユーザの要求に応じて、自動的に入手可能またはユーザの介入によって入手可能である。

【0024】

ブロック112において、プロセッサまたは他の適切な装置は、地球上の多くの箇所から得られた遅延測定値から、ジオロケーションを推定する。例えば、図2A~2Dに示すジオロケーションシステムを用いて、これらの遅延測定値を取得することができる。プロセッサは、これらの遅延測定値を用いて、ジオロケーション推定値の妥当性を検査する(ブロック113)。遅延測定値によって、特定のジオロケーション推定値が妥当でないことを示す場合(例えば、遅延測定値によって、実際の位置がジオロケーション推定値よりも特定の測定位置に近いことを示す場合)、プロセッサは、このジオロケーション推定値を破棄する(ブロック114)。

30

【0025】

また、以下でより詳細に説明するように、プロセッサは、1つ以上の適切な誤差検出技術を用いて、ジオロケーション推定値および/または遅延測定値内の異常値を特定することができる(ブロック115)。上述したように、プロセッサは、遅延、DNS名、公開または私用ソースのデータマイニングおよび/またはルーティング情報を用いて、異常値をさらに解析することができる(ブロック116)。ブロック117において、プロセッサは、遅延、DNS名、公開または私用ソースおよび/またはルーティング情報に基づいて、矛盾するIPアドレスの実際のジオロケーションの確率的な推定値を提供する。

40

【0026】

必要に応じて、プロセッサは、機械学習技術を適用することによって、矛盾特定の信頼性を向上させることができる(ブロック118)。換言すれば、プロセッサは、連続測定からの情報を用いて、信頼区間を縮小することができる。一般的に、遅延測定値が多いほど、より高い信頼性のIPジオロケーション推定値が得られる。また、プロセッサは、初

50

期のジオロケーション推定値、訂正後のジオロケーション推定値および／または訂正值自身を示すマップまたは他の表現を生成することができる（ブロック 119）。

【 0 0 2 7 】

以下の例は、図 1 A に示すプロセスを用いて、エンドユーザプレフィックス 195 . 160 . 236 . 0 / 22 の市販の IP ジオロケーション推定値を評価および訂正する方法を示している。米国ニューハンプシャー（NH）州 Hanover 市に設置された収集装置から、エンドユーザプレフィックス 195 . 160 . 236 . 0 / 22 の IP アドレス 195 . 160 . 236 . 1 までのルート追跡データは、以下の通りである。

【 0 0 2 8 】

【表 1】

ホップ	プローブ1 遅延	プローブ2 遅延	プローブ3 遅延	DNS名（存在する場合） およびホップ IP アドレス
1	1 ms	1 ms	1 ms	DSL ルータ [1.254.254.1]
2	29 ms	26 ms	27 ms	10.20.10.1
3	28 ms	25 ms	25 ms	64.222.166.66
4	31 ms	28 ms	28 ms	POS3-0-0.GW3.BOS4.ALTER.NET [208.192.176.133]
5	38 ms	29 ms	28 ms	0.so-0-1- 1.XL4.BOS4.ALTER.NET [152.63.22.174]
6	39 ms	38 ms	36 ms	0.so-7-0- 0.XL4.NYC4.ALTER.NET [152.63.17.97]
7	42 ms	35 ms	36 ms	0.xe-5-1- 0.BR2.NYC4.ALTER.NET [152.63.18.9]
8	39 ms	36 ms	36 ms	nyc-brdr-02.inet.qwest.net [63.146.27.209]
9	45 ms	49 ms	42 ms	bst-edge-04.inet.qwest.net [67.14.30.26]
10	60 ms	54 ms	59 ms	63.239.36.122
11	56 ms	52 ms	53 ms	vor-b2.worldpath.net [64.140.193.24]
12	59 ms	54 ms	54 ms	195.160.236.1

【 0 0 2 9 】

エンドユーザプレフィックス 195 . 160 . 236 . 0 / 22 は、少なくとも 2 つのサーバ IP アドレス（すなわち、195 . 160 . 236 . 9 および 195 . 160 . 237 . 24）を含み、欧州地域インターネットレジストリ機関である欧州 IP ネットワーク（RIPE）を介して登録されているが、英国に位置すると自己報告している。2 つの商用情報源がこの IP プレフィックスを英国に位置付け、4 つの商用情報源がこの IP プレフィックスをイングランドのマンチェスター市に位置付け、もう 1 つの商用情報源がこの IP プレフィックスを米国ニューハンプシャー州ラコニア市（Laconia）に位置付ける。

【 0 0 3 0 】

エンドユーザプレフィックス 195 . 160 . 236 . 0 / 22 は、Terrenap 社（AS 23148）によって公告される。Terrenap 社は、マイアミに登録されており、大手イン

10

20

30

40

50

ターネットサービスプロバイダとしてのVerizon、Hurricane ElectricおよびXOを含む。A S 2 3 1 4 8は、起源として1 4 0個のプレフィックスを有し、そのうち1 1 3個が米国に位置し、残りがアルゼンチン、ベルギー、ドミニカ共和国、スペインおよびオランダに位置すると思われる。しかしながら、より具体的なプレフィックス1 9 5 . 1 6 0 . 2 3 6 . 0 / 2 4のルートは、異なっている。プレフィックス1 9 5 . 1 6 0 . 2 3 6 . 0 / 2 4は、WorldPath社（A S 3 7 7 0）によって公告される。WorldPath社は、米国ニューハンプシャー州Portsmouth市に登録されており、大手インターネットサービスプロバイダとしてのAT&T、CogentおよびCentury Linkを含む。A S 3 7 7 0は、起源として4 6個の別のプレフィックスを有し、これらの全てが米国の国内に位置する。このことは、このプレフィックスが実際に2つの異なる地理位置に所在しており、少なくとも1つが米国に所在するが、いずれも英国に所在しないことを示唆している。

10

【 0 0 3 1 】

エンドユーザプレフィックス1 9 5 . 1 6 0 . 2 3 6 . 0 / 2 2に関連するD N S情報は、物理位置に関するいくつかの追加的なヒントを与えるが、プレフィックスのジオロケーションを決定的に判断することができない。ルート追跡測定値は、このプレフィックスに関連するルータのD N S名を提供する。通常、D N S名は、最も近い空港を示す3桁の空港コードまたは都市を示す都市略称を含む。上記例の場合、ルータのD N S名は、以下のコード（および空港コードの説明）、すなわち、B O S（米国のボストン（Boston））、N Y C（米国のニューヨーク市（New York City））、B S T（アフガニスタンのボスト（Bost））、およびV O R（未定義）を含む。したがって、D N S情報を用いて、地理位置を特定するための他の証拠を確認することができるが、D N S情報だけでは必ずしも

20

【 0 0 3 2 】

遅延測定値は、I Pプレフィックスと1つ以上の測定位置との間の距離の上限を提供することができる。上記例の場合、（D N S情報から得られたN Y C名が正しく、且つ遅延を測定するために使用されたパケットと目標I Pアドレスとの間の往復経路が対称的であると仮定する場合）遅延測定値は、目標I P（1 9 5 . 1 6 0 . 2 3 6 . 1）がニューハンプシャー州Hanover市から5 3 0 0 k m以内であり、ニューヨーク市から1 8 0 0 k m以内であることを示している。これらの測定値によって、英国は、目標I Pアドレスの可能な場所から除外される。

30

【 0 0 3 3 】

しかしながら、遅延測定値には誤差が存在するため、単純に遅延測定値を減算することによって、目標I Pアドレスの地理位置を正確に推定できないことがある。誤差の原因は、（上記の背景で説明した）遅延、目標I Pアドレスまでの往復経路の非対称性（すなわち、測定パケットは、1つの経路に沿って測定装置から目標I Pアドレスに送信され、異なる経路に沿って目標I Pアドレスから測定装置に返送される）、および以下でより詳細に説明するマルチプロトコルラベルスイッチング（Multiprotocol Label Switching、M P L S）を含む。しかしながら、単一の遅延測定値を用いて、不正確なI Pジオロケーション推定値を破棄することができる。

【 0 0 3 4 】

幸いにも、系統的な測定誤差がない限り、多くの遅延測定値を統合することによって、I Pジオロケーション推定値の不確実性を低減することができる。例えば、一対のノード間で多くの遅延測定を行うことによって、遅延分布を得ることができる。最短遅延は、ノード間の距離のより正確な測定値を与えることができる。目標I Pと多くの異なる測定位置との間に遅延測定およびルート追跡を行うことによって、推定値をより精確にすることができる。

40

【 0 0 3 5 】

この場合、エンドユーザプレフィックス1 9 5 . 1 6 0 . 2 3 6 . 0 / 2 2に位置する2つのサーバまでのルート追跡測定をより多く行うことによって、位置範囲をさらに狭くすることができる。

50

【 0 0 3 6 】

・ 米国ニューハンプシャー州ポーツマス市から 1 9 5 . 1 6 0 . 2 3 6 . 9 までの追跡ルートは、1 つのホップである。

【 0 0 3 7 】

・ 1 gw-vip. ep.psml.renesys.com (195.160.236.9) 0.235 ms 0.236 ms 0.236 ms
・ 米国フロリダ州マイアミ市から 1 9 5 . 1 6 0 . 2 3 7 . 2 4 までの追跡ルートも 1 つのホップである。

【 0 0 3 8 】

・ 1 master.ep.mial.renesys.com (195.160.237.24) 0.269 ms 0.309 ms 0.310 ms
このプレフィックスは、ダイナミックネットワークサービス社のデータセンタに所有される。1 9 5 . 1 6 0 . 2 3 6 . 0 / 2 4 は、ニューハンプシャー州ポーツマス市に所在していると公告され、1 9 5 . 1 6 0 . 2 3 6 . 0 / 2 2 は、フロリダ州マイアミ市に所在していると公告される。/ 2 4 プレフィックスが使用可能である限り、1 9 5 . 1 6 0 . 2 3 6 . 9 は、ポーツマスに所在し、1 9 5 . 1 6 0 . 2 3 7 . 2 4 は、フロリダ州マイアミ市に所在する。/ 2 4 プレフィックスが使用不可になると、両方のプレフィックス（したがって、両方の IP アドレス）は、マイアミ市に所在する。

【 0 0 3 9 】

図 1 B は、コンピュータ、ルータおよび他の装置の IP アドレスに基づいて、それらのジオロケーションを推定するための別のプロセス 1 0 2 を示す図である。ステップ 1 3 0 において、ジオロケーションサーバまたは他のプロセッサは、1 つ以上の第三者サービスから、1 つ以上のコンピュータおよびルータなどのジオロケーション推定値を自動的に取得する。場合によって、ジオロケーションサーバは、第三者が運営するサーバから、これらの推定値を自動的にダウンロードまたは受信することができる。複数の情報源から所定の IP アドレスに関するジオロケーション推定値を受信した場合、ジオロケーションサーバは、これらのジオロケーション推定値を互いに比較することができる（ステップ 1 3 2）。推定値が一致しない場合（例えば、推定値が離れ過ぎる（例えば、1 0 0 キロ以上に離れる）、また 1 つの推定値が一般名称（例えば、「北アメリカ」）であって、他の推定値が特定名称（例えば、「ニューヨーク、NY」）である場合）、ジオロケーションサーバは、IP アドレスと収集装置またはセンサとの間の送信遅延分布を取得することができる（ステップ 1 3 4）。

【 0 0 4 0 】

例えば、以下で詳細に説明するように、ジオロケーションサーバは、IP アドレスと 2 0 0 個以上の収集装置との間のパケット送信に関連する往復時間（round-trip time、RTT）から、遅延分布を得ることができる。ジオロケーションサーバ（または収集装置）は、各収集装置の RTT 測定値に基づいて RTT 分布を決定し、その後、RTT 分布に基づいて、RTT 測定値に関連する信頼区間に入る遅延を推定することができる。場合によって、ジオロケーションサーバは、マルチプロトコルラベルスイッチング（MultiProtocol Label Switching、MPLS）ホップに関連する RTT 測定値、または（IP アドレスと収集装置との間の不可能な物理距離を示す）短すぎる RTT 測定値または長すぎる RTT 測定値を排除する。ジオロケーションサーバは、遅延の誤差源を特定し、これらの誤差源による遅延を調整することもできる。

【 0 0 4 1 】

ジオロケーションサーバは、ステップ 1 3 6 において、位置が特定されている各 IP アドレスの遅延分布から 1 つ以上の遅延を選択し、ステップ 1 3 8 において、対応する収集装置を特定する。その後、ジオロケーションサーバは、選択した遅延を用いて、IP アドレスと収集装置との間の距離を推定する。より具体的には、ジオロケーションサーバは、遅延測定値および光ファイバの速度を用いて、IP アドレスと対応する収集装置との間の最大距離を推定することができる。ジオロケーションサーバは、IP アドレスを囲む収集装置から 3 つ以上の短い遅延を選択した場合、図 5 に示すような三角測量技術を用いて、IP アドレスの地理位置をより精確に推定することができる。収集装置からの範囲が一部

10

20

30

40

50

しか重ならない場合、ジオロケーションサーバは、以下でより詳細に説明するように、そのIPアドレスをエニーキャスト（anycast）IPアドレスとして特定することができる。

【0042】

ステップ142において、ジオロケーションサーバは、第三者のジオロケーション推定値がステップ140で推定された距離によって描かれた円周（または交差区域）内に位置するか否かを判断する。肯定の場合、ジオロケーションサーバは、第三者のジオロケーション推定値が一定の距離範囲内で精確である。否定の場合、ジオロケーションサーバは、収集装置の位置および計算距離に基づいて、IPアドレスの新たな地理位置を生成する。この新たな推定値は、RTT測定分布によって決められ、距離測定の不確実性に影響を与える信頼区間に入る可能性がある。場合によって、距離測定の変化は、非常に大きい。例えば、図1Cは、一対のIPアドレスに対応する新しいジオロケーションおよび古いジオロケーションを用いて生成されたマップを示している。図示のように、1つのIPアドレスの位置は、米国のニューヨーク市からセネガルのダカルに訂正され、もう1つのIPアドレスの位置は、フランスのパリからオーストラリアのパースに訂正された。

10

【0043】

新たなジオロケーション推定値は、様々な形で使用することができる。例えば、プロセッサは、新たなジオロケーション推定値を用いて、ルーティングテーブルの更新の一部として、IPアドレスとの間のパケット送信に関連する遅延を予測することができる。更新された遅延およびルーティングテーブルを用いて、ネットワーク内のホップの数の代わりに、実際の距離に基づいて、トラフィックをより効率的にルーティングすることができる（ステップ146）。また、更新された遅延およびルーティングテーブルを用いて、追加ルータの設置時間および場所を計画することができる（例えば、南米に追加ルータを設置することによって、マイアミのルータを経由してトラフィックを送信する必要性を排除または削減することができる）。これによって、ネットワークの特定部分の全体的な遅延を短縮することができる、および/またはパケット量を増加することができる。

20

【0044】

また、新たなジオロケーション推定値を用いて、特定の地理区域を優先するまたは回避することができる。例えば、ユーザは、セキュリティリスクを引き起こす可能性がある国または地域またはその周辺を回避して、機密情報をルーティングしたいことがある。この場合、ユーザは、トラフィックを直接にルーティングすることができないが、インターネットサービスプロバイダ（ISP）のルータのジオロケーションに基づいて、トラフィックを搬送するISPを選択することができる（ステップ148）。また、ユーザは、機密情報の送信に関する法律、規則またはポリシーに準拠するように、ISPルータのジオロケーションに基づいてISPを選択することによって、特定の国を通してトラフィックをルーティングすることができる。

30

【0045】

さらに、新たなジオロケーション推定値を用いて、ホップ数および遅延に加えてまたはその代わりに、ジオロケーションに基づいて、ドメインネームシステム（DNS）クエリを解析することができる（ステップ150）。ユーザのジオロケーションを精確に知ることによって、ユーザが照会したドメインを、リクエストされたデータをホストしている最も適切なデータセンタに変換することができる。これによって、地理的に近いデータセンタを選択することができ、遅延または上述した問題のいずれかを低減することができる。

40

【0046】

例示的なジオロケーションシステム

図2Aは、例えば図1Aに示すプロセス101に従って、第三者のジオロケーションデータの誤差を特定および訂正するために使用できるルート追跡データの収集に適したジオロケーションシステム200の一例を示す。必要に応じて、収集されたルート追跡データは、インターネットサービスプロバイダ（例えば、Sprint社およびAT&T社）から得られたDNSデータおよびルーティングデータに組み入れることができる。

50

【 0 0 4 7 】

図 2 A に示されたジオロケーションシステム 2 0 0 は、ジオロケーションサーバ 2 1 0 を含む。ジオロケーションサーバ 2 1 0 は、ジオロケーションデータベース 2 1 2、1 つ以上のクライアント 2 1 4、およびルート追跡データ収集装置 2 2 0 のネットワークに接続される。明瞭化のため、図 2 A が 1 つのみのジオロケーションサーバ 2 1 0 および 1 つのみのデータベース 2 1 2 を示しているが、システム 2 0 0 は、同期された複数のジオロケーションサーバ 2 1 0 および複数のデータベース 2 1 2 を含むおよび / または使用することができる。複数のジオロケーションサーバ 2 1 0 を使用する場合、ジオロケーションサーバ 2 1 0 を同期することによって、複数のデータベース 2 1 2 に分散され得るデータを処理することができる。したがって、有線および / または無線の通信プロトコルおよび / または技術を用いて、データベース 2 1 2 を同期することができ、通信を行うことができる。

10

【 0 0 4 8 】

ルート追跡データ収集装置 2 2 0 は、各々のプロバイダのデータセンタ内に存在する実在マシンまたは仮想マシンである。これらの実在マシンまたは仮想マシンの各々は、自律システム (A S) 2 3 0 またはルーティングドメインに属する。動作時、ルート追跡データ収集装置 2 2 0 は、自身の A S 2 3 0 および他の A S 2 3 0 内のルータ 2 4 0、標的コンピューティング装置 2 5 0、および境界ゲートウェイプロトコル (B G P) ルータ 2 6 0 (境界ルータ 2 6 0 とも知られている) までの経路に関連する遅延を測定する。

20

【 0 0 4 9 】

A S 2 3 0 は、コンピューティング装置 2 5 0 の郵便番号として考えられてもよい。すなわち、各々の A S 2 3 0 は、I S P に基づいたインターネットの近隣としてみなすことができ、必ずしも地理的な近隣とは限らない。各 A S 2 3 0 は、境界ゲートウェイプロトコル (B G P) ルータ 2 6 0 (境界ルータ 2 6 0 とも知られている) および A S 2 3 0 のルーティングポリシーを実装し、隣接する A S 2 3 0 に位置する B G P ルータ 2 6 0 との接続を維持する他のルータ 2 4 0 を含む。出願の時点では、グローバルインターネット上の A S の数は、5 4 0 0 0 を超えている。

【 0 0 5 0 】

より正式には、A S 2 3 0 は、単一の管理実体 (例えば、大学、企業、事業部) を代表する共通ネットワーク管理者 (または管理者グループ) によって管理されている単一且つ明確に定義されたルーティングポリシーに従って、接続された I P ネットワークグループである。A S 2 3 0 内の所定の I P ネットワークにおけるノードは、同様のネットワークプレフィックスを共有し、そのプレフィックスに含まれる個々の I P アドレスを利用してインターネットに接続する。殆どの自律システム 2 3 0 は、複数のネットワークプレフィックスを有する。A S 2 3 0 は、T C P / I P ネットワークにおいてドメイン間のルーティングを行うために使用される外部ゲートウェイプロトコル (exterior gateway protocol、E G P) である B G P を用いて、境界ルータ 2 6 0 の間でルーティングメッセージを交換することによって、他の A S 2 3 0 とルーティング情報を共有することができる。

30

【 0 0 5 1 】

B G P の更新を交換するために、境界ルータ 2 6 0 とその B G P ピアのうち 1 つとの間の接続を確立することによって、ルーティング情報を A S 2 3 0 内にまたは A S 2 3 0 間で共有することができる。当業者なら理解するように、境界ルータ 2 6 0 間でデータを交換するプロセスは、「ピアリング」と呼ばれる。ピアリングセッションにおいて、2 つのネットワークは、直接に接続され、データを直接に交換する。内部 B G P ピアリングセッションでは、単一の A S 2 3 0 内の境界ルータ 2 6 0 と内部ルータ 2 4 0 とは、直接に接続される。外部 B G P ピアリングセッションでは、隣接する A S 2 3 0 内の境界ルータ 2 6 0 は、互いに直接に接続される。

40

【 0 0 5 2 】

図 2 A および 4 は、ルート追跡データ収集装置 2 2 0 a から標的コンピュータ 2 5 0 a までのルート追跡測定を示す。ルート追跡データ収集装置 2 2 0 a は、インターネット制

50

御メッセージプロトコル (Internet Control Message Protocol、I C M P) を用いて、第 1 パケットを標的コンピュータ 2 5 0 a に送信する。また、ルート追跡データ収集装置 2 2 0 a は、「生存時間」(time to live、T T L) として知られ、「1」に等しいホップ制限値を第 1 パケットに指定する。第 1 ルータ 2 4 0 a は、第 1 パケットを受信すると、T T L を (1 から 0 に) 減らす。T T L = 0 を有するパケットを受信すると、第 1 ルータ 2 4 0 a は、標的コンピュータ 2 5 0 a への経路に沿って第 1 パケットを次のルータに送信する代わりに、「時間超過」メッセージ 4 0 1 a をルート追跡データ収集装置 2 2 0 a に返す。これによって、ルート追跡データ収集装置 2 2 0 a は、標的コンピュータ 2 5 0 a への経路に位置する第 1 ルータ 2 4 0 a までのホップに関連する遅延を決定することができる。次いで、ルート追跡データ収集装置 2 2 0 a は、T T L = 2 を有する第 2 パケットを標的コンピュータ 2 5 0 a に送信する。第 2 ルータ 2 6 0 a は、別の時間超過メッセージを返す。このように、その後の (T T L = 3 ~ T T L = 6 を有する) パケットは、ルータ 2 6 0 b、2 6 0 c、2 4 0 b、2 6 0 d および 2 6 0 e から時間超過メッセージを誘発する。標的コンピュータ 2 5 0 a は、T T L = 7 を有する最終パケットを受信すると、「エコー応答」メッセージ 4 0 2 をルート追跡データ収集装置 2 2 0 a に返す。これによって、ルート追跡データ収集装置 2 2 0 a は、最終ホップの遅延を測定することができる。

【 0 0 5 3 】

各ジオロケーションデータベース 2 1 2 は、ルート追跡データ収集装置 2 2 0 によって取得されたルート追跡データに加えて、B G P 更新メッセージデータ、ルーティング登録データ、ドメインネームサーバ (D N S) データ、インターネットワークデータ、公開および私用ソースのデータマイニング、および / またはこれらのデータソースのいずれかまたは全てに関連するデータまたはこれらから得られるデータを含むがこれらに限定されない他のデータを含む。上記で説明したおよび下記で説明するように、これらのデータは、I S P および / または他のソースから収集することができ、ジオロケーション推定値の精度を向上させるために使用することができる。

【 0 0 5 4 】

ルート追跡データ収集装置のグローバル配置およびカバー範囲

図 2 B は、図 2 A のグローバルに配置されたルート追跡データ収集システムにおけるルート追跡データ収集装置の位置を示す。システムは、地理的なアクセス可能性、人口密度および I P アドレス密度などに基づいて配置された数十個 ~ 数百個 (例えば、3 0 0 以上) または数千個の収集装置を含むことができる。図 2 B のマップ上の各ドットは、異なる物理的または仮想的なルート追跡データ収集装置を表す。

【 0 0 5 5 】

図 2 C および 2 D は、図 2 A および 2 B に示されたものと類似するグローバルに配置されたルート追跡データ収集システムの地理的なカバー範囲を示す。図 2 C および 2 D の陰影は、インターネットプロトコル (I P) アドレスのセルまたはグループのメジアン遅延 (median latency) を示す。より具体的には、図 2 C および 2 D の経緯度の 1 / 4 の各セルは、現在最も近いルート追跡データ収集装置からそのセル内の全ての I P のメジアン遅延に従って、陰影を付ける。図 2 C および 2 D のセル 2 0 1 が黒くなれば、ルート追跡データ収集装置がセル内の全ての I P に近くなり、ジオロケーション推定値の精度が高くなる。図 2 C および 2 D のセル 2 0 1 が白くなれば、ルート追跡データ収集装置がセル内の全ての I P に遠くなり、ジオロケーション推定値の精度が低くなると考えられる。黒は、0 m s の遅延を示し、白は、少なくとも 1 0 0 m s の遅延を示し、灰色は、中間遅延 (例えば、2 5 m s) を示す。

【 0 0 5 6 】

図 2 C および 2 D の陰影は、追加の収集装置を配置すること、およびルート追跡データ収集装置によって各セルから収集されたデータに重みを付けることを支援することができる。最適なシナリオとしては、全てのセルが完全に黒くなることである。この最適なシナリオの場合、1 0 0 % の信頼性または精度でジオロケーションを推定することができる。

10

20

30

40

50

【 0 0 5 7 】

ジオロケーションサーバおよびルート追跡データ収集装置

図 3 A は、ジオロケーションサーバ 1 1 0 を示すブロック図である。ジオロケーションサーバ 1 1 0 は、ユーザインターフェイス 3 1 2 に接続されたプロセッサ 3 1 8 と、通信インターフェイス 3 1 9 と、実行可能な命令 3 1 6 を格納するメモリ 3 1 4 とを含む。これらの実行可能な命令 3 1 6 は、ジオロケーションサーバプロセス 3 1 7 を実行させる命令を含む。これらの実行可能な命令は、プロセッサ 3 1 8 によって実行されると、プロセッサ 3 1 8 に指示して、ルート追跡データおよびネットワークプレフィックス情報などに基づいて IP アドレスのジオロケーションを解析し、推定する。

【 0 0 5 8 】

プロセッサ 3 1 8 は、ユーザからのリクエストおよび / またはシステムによって生成されたリクエストを処理するためのプログラム要素を動作させる 1 つ以上の高速データ処理ユニットを含むことができる。多くの場合、これらの高速データ処理ユニットは、一体化したシステム (バス) コントローラ、メモリ管理制御ユニット、浮動小数点ユニット、グラフィックス処理ユニットのような専用処理サブユニット、およびデジタル信号処理ユニットなどを含むがこれらに限定されない様々な専用処理ユニットを含むことができる。また、プロセッサ 3 1 8 は、高速アクセス可能な内部メモリを含むことができ、プロセッサ自体以外のメモリをマッピングし、アドレス指定することができる。内部メモリは、高速レジスタ、様々なレベル (例えば、レベル 1、2、3) のキャッシュメモリ、RAM、ROM などを含むがこれらに限定されない。プロセッサ 3 1 8 は、命令アドレスを介してアクセス可能なメモリアドレス空間を使用することによって、メモリ 3 1 4 および実行可能な命令 3 1 6 にアクセスすることができる。プロセッサ 3 1 8 は、命令アドレスを構築および復号することによって、メモリ状態および / または実行可能な命令を有する特定のメモリアドレス空間までの回路経路にアクセスすることができる。

【 0 0 5 9 】

通信インターフェイス 3 1 9 は、多くのインターフェイスアダプタを受け入れる、それらに接続するおよび / またはそれらと通信することができる。これらのインターフェイスアダプタは、一般的にアダプタカードの形を有するが、必ずしもアダプタカードの形を有する必要はない。これらのインターフェイスアダプタは、入力出力 (I / O) インターフェイス、記憶インターフェイスおよびネットワークインターフェイスなどを含むがこれらに限定されない。例えば、通信インターフェイス 3 1 9 に含まれたネットワークインターフェイスを用いて、図 2 A のルート追跡データ収集装置 3 2 0 に情報を送信することができ、当該収集装置から情報を受信することもできる。

【 0 0 6 0 】

ユーザインターフェイスディスプレイ 3 1 2 は、ビデオインターフェイスからの信号を受信するインターフェイス (例えば、DVI 回路およびケーブル) を備えた陰極線管 (CRT) または液晶ディスプレイ (LCD) 系モニタを含むことができる。代替的に、ユーザインターフェイスディスプレイ 3 1 2 は、タッチスクリーンおよび / または他の情報表示装置を含むことができる。ビデオインターフェイスは、メモリ 3 1 4 に記憶され且つプロセッサ 3 1 8 によって実行される実行可能な命令 3 1 6 によって生成された情報を合成する。実行可能な命令 3 1 6 は、ジオロケーションサーバプロセス 3 1 7 を含み、ジオロケーションサーバプロセス 3 1 7 は、1 つ以上のルート追跡データ収集装置 2 2 0 から得られたデータを処理および解析するための命令セットを備える。ユーザインターフェイスディスプレイ 3 1 2 は、Apple (登録商標) OS、Windows (登録商標) OS、Linux (登録商標)、Unix (登録商標) などのオペレーティングシステムおよび / またはオペレーティング環境によって提供された従来のグラフィックユーザインターフェイスを含むことができる。ユーザインターフェイスディスプレイ 3 1 2 は、テキスト機能および / またはグラフィック機能を介して、プログラム要素および / またはシステム設備の表示、実行、対話、操作および / または作動を可能にすることができる。ユーザインターフェイスディスプレイ 3 1 2 は、コンピュータシステムに作用、対話および / または作動することができる機

10

20

30

40

50

能をユーザに提供する。ユーザインターフェイスディスプレイ 312 は、それ自体および / または同様のものを含む要素集合内の他の構成要素と通信することができる。ユーザインターフェイスディスプレイ 312 は、プログラム要素、システム、ユーザ、データ通信、リクエスト、および / または応答を包含、通信、生成、取得および / または提供することができる。

【0061】

図 3 B は、例示的なルート追跡データ収集装置 220 を示すブロック図である。ルート追跡データ収集装置 220 は、サーバ 110 内の通信インターフェイス 319 およびプロセッサ 318 と各々類似する通信インターフェイス 332 およびプロセッサ 324 を含む。また、ルート追跡データ収集装置 220 は、1 つ以上の標的コンピューティング装置 (10
例えば、図 2 A のルータ 240 および標的コンピューティング装置 250) からのルート追跡データを収集するための命令 329 を含む実行可能な命令 328 を記憶するメモリ 326 を含む。

【0062】

ルート追跡データおよびルート追跡データの収集

図 1 および 4 は、ルート追跡データシステムの動作原理を示す。ルート追跡を行うために、ルート追跡データ収集装置 220 a は、インターネット制御メッセージプロトコル (Internet Control Message Protocol、I C M P) を用いて、第 1 パケットを標的コンピュータ 250 a に送信する。また、ルート追跡データ収集装置 220 a は、「生存時間」 (time to live、T T L) として知られ、「1」に等しいホップ制限値を第 1 パケットに 20
指定する。第 1 ルータ 240 a は、第 1 パケットを受信すると、T T L を (1 から 0 に) 減らす。T T L = 0 を有するパケットを処理すると、第 1 ルータ 240 a は、標的コンピュータ 250 a までの経路に沿って第 1 パケットを次のルータに送信する代わりに、「時間超過」メッセージ 401 a をルート追跡データ収集装置 220 a に返す。これによって、ルート追跡データ収集装置 220 a は、標的コンピュータ 250 a までの経路上に位置する第 1 ルータ 240 a までのホップに関連する遅延を決定することができる。次いで、ルート追跡データ収集装置 220 a は、T T L = 2 を有する第 2 パケットを標的コンピュータ 250 a に送信する。第 2 ルータ 260 a は、別の時間超過メッセージを返す。このように、その後の (T T L = 3 ~ T T L = 7 を有する) パケットは、ルータ 260 b、260 c、240 b、260 d および 260 e から時間超過メッセージを引き出す。標的コンピュータ 250 a は、T T L = 8 を有する最終パケットを受信すると、「エコー応答」 30
メッセージ 402 をルート追跡データ収集装置 220 a に返す。これによって、ルート追跡データ収集装置 220 a は、最終ホップの遅延を測定することができる。

【0063】

ルート追跡データ収集装置 220 a は、T T L を増やすたびに、パケットを送信し、トランシットルータからの「T T L 超過」応答 401 a、401 b、401 c . . . を監視することによって、標的コンピュータ 250 a までの経路上に位置する連続ホップおよび標的コンピュータ 250 a までの往復時間の両方を見出す。ルート追跡データ収集装置 220 a は、収集された「T T L 超過」応答を使用して、I C M P パケットがターゲット装置 250 a に到達し且つ I C M P エコー応答 402 を返すまでに通過したルータのリスト 40
を構築する。

【0064】

収集されたルート追跡データは、対応するルート追跡データ収集装置 220 の識別子および / または I P アドレスを含む追跡ルート内の各装置の識別子を含む。含まれた I P アドレスは、グローバルまたはローカルコンピュータネットワークの一部であるルータを表すことができる。また、ルート追跡データは、ルート追跡データ収集装置 220 がルータから応答を受信するために要した時間と、ルート追跡データ収集装置 220 が標的コンピューティング装置から I C M P エコー応答を受信するために要した時間とを含む。

【0065】

必要に応じて、ジオロケーションサーバ 110 は、ルート追跡データ収集装置 220 に 50

よって取得されたルート追跡データを受信し、処理することによって、以下に示すようなデータ構造で、人間可読中間フォーマットを生成することができる。

【 0 0 6 6 】

【 数 1 】

```
tr_base_fields = [('dcv',str), # data version
                  ('ts',int), # timestamp of start of trace
                  ('protocol',str), # [I]CMP,[U]DP,[T]CP
                  ('port',int),
                  ('collector_ip', str),
                  ('collector_external_ip', str),
                  ('collector_name', str),
                  ('target_ip', str),
                  ('halt_reason', str),#
[S]uccess,[L]oop,[U]nreachable, [G]ap
                  ('halt_data', int),# additional information for
failed trace
                  ('hoprecords', T5HopList)]
```

10

【 0 0 6 7 】

20

以下には、tr_base_fieldsデータフォーマットのルート追跡データの一例を示す。ジオロケーションサーバプロセスの説明を簡略化するために、各フィールドは、単独の行に列挙される。

【 0 0 6 8 】

【 数 2 】

```
1: T5
2: 1431005462
3: I
4: O
5: 192.170.146.138
6: 192.170.146.138
7: vps01.nycl
8: 88.203.215.250
9: S
10: 11
11: q,0,1,0
12: 63.251.26.29,0.363,2,254
13: 74.217.167.75,1.297,3,252
14: 129.250.205.81,1.171,4,252
15: 129.250.4.148,1.614,5,250,576241
16: 129.250.3.181,87.140,6,250,519266
17: 129.250.4.54,112.258,7,247,16013
18: 129.250.3.25,114.446,8,248
19: 83.217.227.22,123.002,9,245
20: 212.39.70.174,125.613,10,245
21: 88.203.215.250,124.967,11,51
```

30

40

【 0 0 6 9 】

50

ジオロケーションに使用されるフィールドは、次のもの、すなわち、2：タイムスタンプ（1970年1月1日以降の秒数、すなわち、UNIXエポック）、7：収集装置名（各収集装置の特有の識別子、例示の収集装置は、ニューヨーク市にある）、8：ルート追跡の目標IPアドレス、11～21：ルート追跡ホップ（ネットワークトポロジーに従って変動する可変数）を含む。

【0070】

各ホップは、コンマで区切られ、ホップIP（応答を受信しなかった場合、q）、ミリ秒の往復時間（RTT）、TTL、リバースTTL、および0以上のMPLSラベルからなるサブリストを含む。

【0071】

いくつかの実現例において、ジオロケーションサーバプロセスは、各ホップから得られたRTT値であるルート追跡データ収集装置の遅延に基づいている。上記の例で示すように、1回のルート追跡で複数の応答ホップを生成し、各ホップは、収集装置（この場合、ニューヨーク市に位置する収集装置）のIPおよび往復時間（RTT）を有する。ジオロケーションサーバプロセスは、各ルート追跡を個々のタプル（収集装置の所在都市、IP、RTT）または収集装置のエッジ遅延に分解する。

【0072】

この例の収集されたルート追跡データにおける第12行：63.251.26.29, 0.363, 2, 254を検討する。IPアドレス63.251.26.29は、収集装置からの往復時間が0.363ms（RTT）である。いくつかの実現例において、ジオロケーションサーバプロセスは、ホップの第3フィールドまたは第4フィールド（TTLおよびリバースTTL）を考慮しない場合がある。特定の整数識別子を用いて、各都市を表すことができる。例えば、ニューヨーク市のジオネームIDは、5128581である。ニューヨーク市に所在するルート追跡データ収集装置からのホップは、（5128581, 63.251.26.29, 0.363）というタプルとして表すことができる。

【0073】

光ファイバの速度制約によって、1msのRTTは、大きな円周または往復経路に沿って約100キロを移動した可能な最大距離に対応する。すなわち、このホップの場合、0.363msのRTTでは、ニューヨーク市に位置するルート追跡データ収集装置から、IPアドレス63.251.26.29を有する装置までの最大距離は、36.3キロ（22.6マイル）である。場合によって、データセンタを離れる時に初期遅延があるため、このIPは、同一のデータセンタに配置されている可能性が高い。この証拠の他に、他のルート追跡からの追加測定値による支持によって、ジオロケーションサーバプロセスは、ルート追跡データ収集装置が配置されている都市の緯度および経度、並びにこの収集装置によってカバーされる半径に基づいて、IPジオロケーションをより精確にすることができる。ジオロケーションサーバプロセス分析は、光速度の考慮に基づいて、ジオロケーションサーバから引き出される推論を確証する。

【0074】

マルチプロトコルラベルスイッチング（MPLS）およびジオロケーション

場合によって、ルート追跡ホップは、行末にマルチプロトコルラベルスイッチング（MPLS）ラベルを含むことがある。上記の行15、16および17に示すように、各々のルート追跡ホップは、MPLSラベル576241、519266および16013でそれぞれ終わる。これらのMPLSホップのRTTは、しばしば、MPLSトンネル送出ホップのRTTに対応し、以下で図6Aを参照してより詳細に説明するようにより大きい妥当半径をもたらすため、遅延の測定および比較のために、これらのMPLSホップを破棄することができる。複数の測定値を検討する場合、MPLSホップを削除することによって、より厳密な妥当性エンベロープを提供することができる。したがって、いくつかの実現例において、MPLSホップをフィルタリングすることによって、統計的に妥当な半径を減少させ、測定値を改善することができる。

【0075】

10

20

30

40

50

例示のルート追跡データからMPLSラベルを破棄すると、以下のように、ジオロケーションを行うためのタブルのリストを生成することができる。各タブルにおいて、第1要素は、ニューヨーク市に位置する収集装置のジオネームID(5128581)およびルート追跡の起点に対応する。

(5128581, 63.251.26.29, 0.363)

(5128581, 74.217.167.75, 1.297)

(5128581, 129.250.205.81, 1.171)

(5128581, 129.250.3.25, 114.446)

(5128581, 83.217.227.22, 123.002)

(5128581, 212.39.70.174, 125.613)

(5128581, 88.203.215.250, 124.967)

なお、最後のホップ内のIPアドレスは、88.203.215.250であり、目標IPアドレス(フィールド8)と同様である。これは、ルート追跡内の最終標的装置が、ルート追跡データ収集装置によって行われたプロービングに応答または反応したことを意味する。

【0076】

エッジ遅延の重なりを用いたジオロケーション

いくつかの実現例において、ルート追跡データ収集装置のエッジ遅延は、図2Bに示すグローバルに配置されたルート追跡データ収集装置によって行われたルート追跡に依存することができる。場合によって、総数300以上の収集装置は、一日に5百万を超える測定を行うことができる。ジオロケーションサーバは、各エッジの複数の測定値に基づいて、統計的な推測を生成することができる。各々のルート追跡データ収集装置に埋め込まれたタイマは、各収集装置からIPアドレスまでの妥当半径を定義するために利用されるRTTの測定値に、ノイズを追加することができる。測定値の欠陥またはノイズを考慮するために、ジオロケーションサーバは、異常値を特定するための改良トンプソンTauテスト(Modified Thompson Tau test)を用いて、(潜在的または人為的に)低いRTTを有する異常値を排除することができる。計算上の便宜として、各収集装置エッジの遅延の25%値を使用すると、改良トンプソンTauテストの代わりに、異常値を合理的に排除することができる。以下、25%値を使用する。しかしながら、このことは、本技術の態様を定義するものではなく、異常値を排除できる多くの方法のうち、1つとして見なすべきである。異常値を減らすまたは排除するための他の可能性として、5%値、10%値、15%値、中央値、モード、または他の適切な技術の使用を含むがこれらに限定されない。

【0077】

図5は、3つのルート追跡データ収集装置によってカバーされた区域の交差を示す。いくつかの実現例において、ジオロケーションサーバプロセスは、各収集装置、例えばルート追跡データ収集装置501a、503aおよび505aから、標的コンピュータ装置に対応するIPアドレスまでの妥当半径を生成することができる。所定のIPアドレス、ネットワークプレフィックスおよび/または標的装置に対して、各収集装置によってカバーされる半径によって画定された円周509、511および513の交差部分は、IPが存在する可能性がある区域507aを画定する。当該区域内の都市は、そのIPのジオロケーション候補である。例えば、ルート追跡データ収集装置501b、503bおよび505bによって収集されたルート追跡データに基づいて、収集装置501b、503bおよび505bの中間の都市507bは、候補都市である可能性がある。

【0078】

場合によって、これらの円周は、交差しなくてもよい。この場合、遅延は、IPが2つ以上の収集装置の設置都市に近い、すなわち、一対の収集装置の中間点よりも収集装置の設置都市に近いことを示している。このような状況は、同一のIPを有する装置が2つ以上の場所に位置していることを示すため、ジオ不一致(geo-inconsistency)に分類される。これは、エニーキャストネットワークの特徴である。ジオロケーションサーバプロセスは、ジオ不一致インスタンスを特定し、対応するIPをエニーキャストとして標記する

10

20

30

40

50

。

【 0 0 7 9 】

インターネットプロバイダが特定のIPの位置を変更できるため、収集されたルート追跡データを定期的にプローブすることによって、標的のジオロケーションが定常である時に、目標IPアドレスまでの測定値を測定したことを確認することができる。

【 0 0 8 0 】

以下、実質的にハイパーテキストプリプロセッサコード（PHP）の形式で、目標装置のプロービング、目標装置が所在する都市の特定、およびエニーキャストIPアドレスの特定を含むジオロケーションサーバプロセスのいくつかの機能の擬似コード表現の一例を提供する。

【 0 0 8 1 】

【数 3 - 1】

```

# For each IP found in traceroutes, construct a sorted list
# of (25th percentile RTT, collector-city)
func ip_to_collector_latencies(traceroutes):
    # Construct RTT array for each unique (collector_city, IP) pair
    rtt_dictionary = new dict
    for all recent traceroutes:
        for each hop in traceroute:
            if not MPLS(hop):
                rtt_dictionary[(collector_city, IP)].append(RTT)

    # Construct list of 25th percentile RTTs, collector city pairs for
    each IP
    collector_latencies = new dict
    for each IP:
        for every pair-wise combination of collector cities:
            if collector1-IP-latency + collector2-IP-latency <
                minimum possible latency between collectors:
                mark IP as anycast
                break
    if IP is not anycast:
        rtt_collector_list = new list
        for each collector_city:
            rtt_array = rtt_dictionary[(collector_city, IP)]
            rtt25 = compute_25th_percentile_latency(rtt_array)
            rtt_collector_list.append((rtt25, collector_city))
        rtt_collector_list.sort()
        collector_latencies[IP] = rtt_collector_list
    return collector_latencies

```

【 0 0 8 2 】

【数 3 - 2】

```

# When correcting a third-party geolocation of an IP,
# we can compute the minimum possible RTT to each collector city,
# and compare against the observed latency
func is_geolocation_plausible(IP, city):
    rtt_collector_list = collector_latencies[IP]
    for (rtt, collector_city) in rtt_collector_list:
        minpossrtt = minimum_rtt[(city, collector_city)]
        if rtt < minpossrtt:
            return False # IP is misgeolocated
    return True # IP geolocation is plausible

# We can also create a list of all plausible cities for
# self-determining an IP geolocation
func geolocate_ip(IP):
    plausible_cities = create_list_of_all_cities()
    rtt_collector_list = collector_latencies[IP]
    for (rtt25, collector_city) in rtt_collector_list:
        for city in plausible_cities:
            minpossrtt = minimum_rtt[(city, collector_city)]
            if rtt25 < minpossrtt:
                # IP cannot be in this city based on speed-of-light in
                fiber consideration
                plausible_cities.remove(city)
    return plausible_cities

```

【0083】

いくつかの実現例において、ジオロケーションサーバは、遅延が大きすぎて選択を単一の都市または大都市に減縮することができない場合に、IPアドレスをより広い地理範囲に割り当てる。例えば、妥当な都市の最終リストが全て同じ州または地方に位置する場合、ジオロケーションサーバプロセスは、ジオロケーションを州範囲または地方範囲に割り当てることができる。ジオロケーションサーバプロセスのさらなる実装は、IPを割り当てることができる全ての可能なグリッドセルを決定する。

【0084】

ジオ遅延 (geolateness) 決定の例示

本社が南アフリカに位置するインターネットプロバイダMTN (AS 6637) から起源するIPアドレス41.181.245.81を検討する。

【 0 0 8 5 】

以下は、ジオロケーションサーバプロセスからの出力情報である。

【 0 0 8 6 】

【 数 4 】

TLATSUMG2 1429865014 1430956773 41.181.245.81 0 0 0 -- 50

39 2265 342.4 London,GB 0.7 1478 2643743

(0.7,1478,2643743) (6.2,3,2641170) (10.4,51,2925533)

(20.3,46,2657896) (22.9,1,3173435) (24.4,28,2867714)

(32.0,2,3196359) (32.9,55,3067696) (38.9,1,756135)

(41.0,1,3099434) (46.5,1,649360) (61.3,56,250441)

(68.9,100,5101798) (69.0,3,5128581) (73.6,1,4930956)

(74.6,105,4744870) (75.5,2,4781530) (90.2,4,4887398)

(91.3,2,4180439) (97.2,1,108410) (98.3,113,4164138)

(103.3,2,4684888) (108.5,1,524901) (127.2,1,3598132)

(134.8,1,1277333) (136.1,46,5380748) (136.8,1,1174872)

(138.8,3,5391959) (139.2,1,5780993) (139.7,117,5809844)

(140.4,4,5368361) (149.2,10,3397277) (149.9,2,3369157)

(156.3,1,5392171) (194.2,1,3448439) (204.5,16,3435910)

(264.4,1,1835848) (340.3,1,2028462) (342.4,2,1581130)

【 0 0 8 7 】

上記の出力情報において、下線付きフィールドは、最も近い収集装置の位置、目標IPまでの遅延、測定値の数、および収集装置が位置する都市のジオネームIDである。この場合、最も近い収集装置は、ロンドンに位置し、ロンドンに位置する収集装置から目標IPまでの遅延は、0.7msである。

【 0 0 8 8 】

下線付きフィールドの下方のデータは、各収集装置からの遅延の25%値を有するタブルである。各タブルは、コンマで区切られた3つの項目、すなわち、RTT(25%値)、測定値の数、ジオネームIDを含む。

【 0 0 8 9 】

下線付きフィールドの直後の第1タブルが最小遅延を有するように、遅延に従ってこれらのタブルを並べる。

【 0 0 9 0 】

タブル(0.7,1478,2643743)は、1478個の測定値に基づいて、ロンドン(2643743)に位置する収集装置から0.7msという1番目短い測定値を有する。このタブルは、便宜上、前述した3つのフィールドの情報を繰り返している。

【 0 0 9 1 】

タブル(6.2,3,2641170)は、ノッティンガム(2641170)収集装置からの6.2msという2番目に短い測定値を有する。合計で39個の収集装置都市がそのIPに測定値を返した。

【 0 0 9 2 】

ロンドンとケープタウンとの間のファイバの可能な最小RTT遅延は、95.7msである。ロンドンのルート追跡データ収集装置からIPアドレス41.181.245.81までの遅延がわずか0.7msであるため、ジオロケーションサーバプロセスは、光速制約に基づいて、そのIPがインターネットプロバイダの識別情報によって示唆されたように、南アフリカに位置していないことを確実に判断することができる。また、ジオロケ

10

20

30

40

50

ーションサーバプロセスは、ロンドン収集装置からの遅延が短いため、そのIPの位置をロンドンに割り当てることができる。この訂正を行うために、ジオロケーションサーバプロセスは、まず、他のルート追跡データ収集装置もロンドンがそのIPの可能な位置であることを裏付けることを判断する。

【0093】

例えば、以下は、ロンドンの収集装置からのIPアドレス41.181.245.81までの単一のルート追跡データである。このIPアドレスがロンドンに位置することを明確に宣言する前に、多くの場所からの多くのルート追跡を用いて、更なる裏付けを提供することができる。

【0094】

10

【数5】

```
tracert to 41.181.245.81 (41.181.245.81), 30 hops max, 60 byte
packets 1 20.ae1.edge-01-lon.as33517.net (80.231.219.189) 0.319
ms 0.282 ms 0.361 ms 20.ae0.edge-02-lon.as33517.net
(185.38.96.27) 0.365 ms 0.338 ms 0.307 ms 3 xe-10-3-
3.edge3.London15.Level3.net (212.187.193.189) 0.358 ms 0.285 ms
0.338 ms 4 MTN-GROUP.edge3.London15.Level3.net (212.187.195.162)
1.791 ms 1.830 ms 1.872 ms 5 41.181.190.190 (41.181.190.190)
2.034 ms 2.083 ms 2.060 ms 6 41.181.245.81 (41.181.245.81)
0.820 ms 0.784 ms 0.914 ms
```

20

【0095】

ドメインネームシステム(DNS)逆引き

いくつかの実現例において、ジオロケーションサーバプロセスは、可能な場合、IPのDNS逆引き(rDNS)を用いて、推論をさらに補足することができる。プロバイダは、定義した命名規則に従って、ジオロケーション情報をルータ名にエンコードすることがよくある。上記のルート追跡例において、下線付きの80.231.219.189は、同様に下線付きのrDNS、すなわち、20.ae1.edge-01-lon.as33517.netを有する。ラベルの一部「lon」は、そのIPアドレスがロンドンに位置することを示している。ジオロケーションサーバプロセスには、手動で得られたルールに基づくエンジンを有する。このエンジンは、必要に応じて、これらのラベルからジオロケーション情報を抽出する。これらのラベルは、物理的な遅延とは異なり、人間によって入力され、正しく管理されていない場合、間違ったことがある。しかしながら、rDNSからのジオロケーションを遅延からのジオロケーションに組み合わせることによって、より正確なIPジオロケーションを得ることができる。69.252.112.58(se02.woburn.ma.boston.comcast.net)を例示として検討する。

30

【0096】

ウォバーン(Woburn)は、ボストンの北約15kmに位置している。ジオロケーションサーバプロセスをこのIPアドレスに適用すると、次の結果が得られる。

40

【0097】

【数 6】

TLATSUMG2 1430698623 1431022690 69.252.112.58 0 0 0 -- 186 116 1042
 307.5 Boston,MA,US 8.5 6 4930956 8.5,6,4930956 9.2,11,5128581
 9.4,7,5101798 10.2,6,5102076 12.8,5,5087168 14.4,16,4744870
 15.1,6,4140963 15.7,5,4781530 16.4,5,5083221 16.7,5,5091383
 24.9,14,6167865 29.1,12,4887398 35.8,13,4180439 36.8,16,4852832
 51.4,3,5419384 52.5,14,4164138 54.4,19,4684888 63.4,6,4699066
 66.9,6,5780993 76.3,18,5809844 77.6,5,6173331 77.8,13,5380748 10
 77.8,70,2643743 78.6,20,5392171 79.2,9,5391959 80.2,4,3598132
 80.9,26,5368361 81.9,2,5746545 83.8,7,2960316 84.6,11,2787416
 84.8,5,2641170 85.3,6,3991164 87.5,12,2988507 88.8,3,2964574
 90.7,6,4005539 94.3,35,2759794 95.1,34,2925533 98.55,4,3674962
 98.6,5,2867714 100.05,12,2657896 100.2,6,2660646 101.3,14,756135
 101.4,8,3173435 101.6,5,3621849 104.7,5,3117735 107.3,6,3067696
 108.5,6,2761369 109.0,6,2673730 111.8,6,2520600 113.9,6,792680
 113.9,6,2735943 114.45,4,3196359 116.1,5,3099434 116.9,10,3060972 20
 119.0,6,683506 120.0,6,3054643 120.9,5,2267057 123.2,5,649360
 123.9,7,2523920 126.8,5,625144 128.6,6,5856195 129.0,6,498817
 132.2,5,3397277 132.3,14,745044 133.0,6,727011 135.6,5,250441
 135.6,11,524901 135.9,6,726050 135.9,11,703448 138.7,6,293397
 139.2,6,593116 143.25,4,323786 145.5,5,360630 148.3,6,3871336
 149.9,5,587084 150.5,10,3448439 161.9,5,2548885 162.4,7,3451190
 165.3,6,108410 165.8,3,616052 171.0,3,3461655 173.6,28,1850147
 174.8,9,3435910 183.7,5,1526384 184.9,5,1528675 187.1,6,1853909 30
 195.9,11,292223 196.1,15,1668399 198.6,12,1275339 204.9,5,1835848
 207.25,8,1668341 216.4,4,1174872 217.45,4,1277333 219.9,9,1273294
 220.9,21,2147714 222.3,4,160263 224.15,4,184745 224.7,6,3369157
 224.7,30,1819729 225.0,10,1264527 230.55,4,1808926 234.8,6,285787
 240.4,5,1176615 243.0,6,1701668 252.2,31,1880252 253.35,4,1816670
 266.2,5,1784658 268.9,6,6930887 275.05,4,1797929 276.5,5,1821306
 276.9,4,1609350 281.3,3,1581130 281.4,4,2063523 286.5,5,2028462
 300.9,5,2158177 307.5,4,1735161 40

【0 0 9 8】

ボストンは、IPアドレス(69.252.112.58)から8.5msの最も近い
 ルート追跡データ収集装置である。しかしながら、rDNSは、IPアドレスがマサチュ
 セッツ州ウォバーン(Woburn)に位置するという情報を提供している。ジオロケーショ
 ンサーバプロセスは、ウォバーンがこの収集装置の遅延分布範囲内の可能な都市であるか
 否かを検証する。これによって、ジオロケーションサーバプロセスは、ジオロケーショ
 ンをボストンではなくウォバーンにより正確に割り当てることができ、IPジオロケーショ
 ン推定値の精度を向上させる。

【0 0 9 9】

また、いくつかの実現例において、ジオロケーションサーバは、類似のrDNS名を見 50

出し、遅延を用いて検証した後、自然言語処理を介してジオロケーションを割り当てることによって、ルールを自動的に発見しようとする。ジオロケーションサーバは、発見した全てのrDNS名のデータベースを管理することによって、ルールを発見する。IPv4の場合、アドレス空間全体の逆解析を行うことによって、現時点では12.2億を超えるrDNSエントリを生成する。IPv6の場合、スペースの巨大さを考慮して、グローバルオープンDNSの帰納およびルート追跡されているIPv6スペースのrDNSの選択的な解析から得られたパッシブDNSから、rDNSエントリを収集する。サービスに指示して、受信したクエリおよび提供した応答の両方(リクエストのタイムスタンプ、リクエストしたドメインおよびレコードの種類、提供した応答、および任意のDNSクエリおよび応答を分類する他の属性を含むがこれらに限定されない)を記録することによって、オープンDNSの帰納からrDNSを収集する。

10

【0100】

単純な例として、ジオロケーションサーバは、(既存のルールを検査することによって、または遅延を検討することによって)rDNS内の「nyc」を含む文字列が、関連するIPアドレスがニューヨーク市に位置することを強く示すことを発見することができる。現在、IPv4には260万件を超えるrDNSエントリがあるが、その多くは、現在では商用プロバイダによってニューヨーク市に割り当てられていない。

【0101】

67.17.81.197(loop0.csl.NYC2.NYC.gblx.net)を検討する。現時点では、3つの異なる商用プロバイダは、このIPアドレスを米国テキサス州ダラス市、エクアドル(都市なし)、または米国(都市なし)に各々割り当てている。このIPアドレスは、NYCに位置する場合、遅延上一致するが、テキサス州またはエクアドルに位置する場合、完全に不可能である。現在のところ、全てのIPv4空間には100個を超える.nyc.gblx.netのrDNSレコードがあって、全ての遅延は、IPアドレスがニューヨーク市に位置する場合と一致している。また、「nyc」を含む多数のrDNSルールも、ニューヨーク市に関連している。したがって、ジオロケーションサーバは、rDNS内の文字列「nyc.gblx.net」が、ニューヨーク市に割り当てられた関連するIPアドレスを強く示すことを発見することができ、それによって、対応するルールを自動的に作成し、作成したルールをルールに基づくrDNS処理エンジンに追加することができる。

20

【0102】

公開データソースおよび私用データソース

いくつかの実現例において、ジオロケーションサーバは、本明細書に記載の技術を用いて更なる検証を行うために、公開ソース、私用ソースおよび準私用ソースから、可能な物理アドレスを特定する。これらのソースは、他の方法で公開されていない特定の物理アドレスを見つけるためのデータセンタの掲示板または企業のキャリアページ、プルダウンメニューでルータ位置を提供するルートルッキングメガネ、複数の場所に位置する大手チェーン店のような、IPアドレスに結び付けることができる店舗位置、および数十個のグローバルおよびローカルインターネットルーティングレジストリ(IRR)からのプレフィックス登録データを含むが、これに限定されない。

30

【0103】

上述した技術の一例として、119カ国に位置しており、3万6千軒を超えるマクドナルド(登録商標)レストランを検討する。これらの店舗の多くには番号が付けられており、数千軒が上記のrDNSデータに見付けられる。以下の2つのIPアドレスおよびそのrDNSエントリを検討する。

40

- ・ip=206.59.233.82 fqdn=nmd.mcd18734.mia.wayport.net
- ・ip=206.59.233.83 fqdn=eth1-l.nmd.mcd18734.mia.wayport.net

これらの2つのIPアドレスは、明らかにマクドナルドの店舗番号18734を参照している。公開ウェブサイトを参照することによって、この店舗は、マイアミの中心部から約12マイル離れ、1930 palocka Blvd, Opa-Locka (Dade County)、FL、33054に位置する。このように見付けた可能なジオロケーションは、本明細書に記載された他の方法でさ

50

らに検証することができる。

【 0 1 0 4 】

エニークキャスト例

別の例として、標的装置がエニークキャストIPを有する場合、ジオロケーションサーバプロセスから異なる結果を得ることができる。以下に示すIPアドレス199.27.135.101の結果を検討する。

【 0 1 0 5 】

【 数 7 】

TLATSUMG2 1429747203 1430956517 199.27.135.101 <u>7191</u> 181.069922721	10
0.648613384403	
1850147=3448439,1850147=3448439,1835848=3448439,1835848=3448439,1880	
252=3674962,1880252=3674962,2147714=2520600,2147714=2520600,1853909=	
3448439,1853909=3448439,1850147=3461655,1850147=3461655,1819729=3448	
439,1819729=3448439,1835848=3461655,1835848=3461655,2147714=3117735,	
...,683506=1668399 187 116 3833 201.0 Chicago,IL,US 0.4 48 4887398	
0.4,48,4887398 0.4,50,4164138 0.4,60,4744870 0.4,66,5809844	
0.4,73,2147714 0.5,22, 3067696 0.5,97,5368361 0.6,23,2520600	20
0.6,49,4180439 0.6,73,5392171 0.7,21,2673730 0.7,24,4781530 0.7,71,	
4684888 0.7,124,2925533 0.7,126,2759794 0.7,232,2643743	
0.8,19,3117735 0.8,47,2988507 0.9,44,5128581 1.0,52, 5380748	
1.0,52,6167865 1.1,113,1850147 1.2,69, 3448439 1.3,24,2761369	
1.3,27,3173435 1.3,36,756135 1.4,25,4140963 1.4,27,5101798	
1.5,20,1835848 1.6,111, 1880252 1.8,118,1819729 1.9,23,5102076	
1.9,37, 5391959 4.6,19,6173331 5.2,35,3060972 5.3,23,4699066 5	
.4,13,3461655 5.6,14,3099434 5.6,21,4930956 5.8,36, 2787416	
6.0,18,2641170 6.0,26,2960316 6.9,20,2867714 7.0,17,3196359	30
7.1,9,5746545 8.2,19,5083221 8.3,23,1853909 8.7,21,5091383	
10.5,56,4852832 10.6,9,2964574 10.6,16, 3674962 11.0,15,649360	
11.9,24,2660646 12.7,20,498817 13.5,22,593116 13.9,43,2657896	
14.6,18,2158177 16.15, 20,3369157 17.7,21,3054643 19.0,29,1668341	
19.9,24,792680 20.9,20,5780993 21.9,44,524901 22.0,21,3991164 22.4,	
40,703448 23.0,19,5419384 23.6,27,2523920 24.2,20,2735943	
24.4,19,2267057 26.1,19,5087168 29.5,15,3598132 29.8, 16,1609350	
35.1,36,1264527 37.1,21,6930887 39.0,18,625144 39.4,57,1668399	40
41.2,20,727011 43.2,14,1277333 44.7, 21,683506 44.8,16,1735161	
45.2,24,726050 45.9,20,4005539 46.9,19,1821306 47.4,15,745044	
47.8,16,323786 49.8,22, 5856195 50.1,14,2063523 50.2,18,3397277	
51.6,18,3621849 59.8,23,1701668 61.0,18,250441 61.0,23,293397	
68.0,44, 1275339 71.2,18,2548885 73.2,12,616052 74.9,21,587084	
75.8,15,1528675 80.4,11,1581130 83.4,22,108410 84.9, 37,1273294	
93.0,18,1526384 105.6,47,292223 113.4,25, 3451190 126.1,17,160263	
132.3,15,1174872 141.7,15,360630	50

【 0 1 0 6 】

上記の例に示されている第 1 行の下線付き値 7 1 9 1 は、地理上一致していない収集装置の都市ペアの数を表している。上記の IP アドレスは、4 8 8 7 3 9 8 (シカゴ) から 0 . 4 m s でありながら、4 1 6 4 1 3 8 (マイアミ)、4 7 4 4 8 7 0 (アシュバーン)、5 8 0 9 8 4 4 (シアトル)、および 2 1 4 7 7 1 4 (シドニー) の各々からも 0 . 4 m s である。上記の IP アドレスを有する単一の装置がこれらの各都市 (および結果内のいくつかの他の都市) と同様に近くなることが物理的に不可能であるため、上記の IP アドレスがエニーキャストアドレスであることを推定することができ、「地球」というジオロケーションに割り当てることができる。

【 0 1 0 7 】

ジオロケーションサンドイッチの決定

追跡ルートを、収集装置の IP アドレスから目標 IP アドレスまでの IP アドレスのシーケンスとして見なす。本明細書に記載された 1 つ以上の技術および他の技術を用いて、各 IP アドレスをジオロケーションに割り当てることができる。IP アドレスのシーケンスをサブシーケンスまたはホップフラグメントにさらに細分することができる。いくつかの実現例において、フラグメントの最初のホップおよび最後のホップが同一の国に位置するが、1 つ以上の中間ホップが他の国に位置する場合、ジオロケーションサーバは、サンドイッチアプローチを用いて、追跡ルートの一部または全てのフラグメントを検討する。

【 0 1 0 8 】

サンドイッチアプローチの基礎は、追跡ルートがある国を離れて別の国に進入する可能性が殆どなく、元の国に戻るだけということである。そのようなフラグメントが見つかった場合、フラグメント内の 1 つ以上の IP アドレスの位置が間違っていて特定された可能性がある。フラグメント内の各 IP アドレスは、本明細書に記載の技術を用いて、さらに分析することができる。いくつかの実現例において、ジオロケーションサーバプロセスは、このアプローチの一般論を用いて、フラグメント内の最初のホップおよび最後のホップが一見では距離上近いが、フラグメントのホップ間の距離の合計が大きいであるルート追跡シーケンスを探す。すなわち、最初のホップから最後のホップまでの正味距離は、ホップ間の距離の合計よりも小さい。このような U 字形シーケンスは、例えば、2 つのローカルプロバイダが、ビジネス上の理由または他の理由で、全てのマーケットにおいて物理的に接続しておらず、離れた場所でトラフィックを交換する場合に、合理的である。潜在的に間違ったジオロケーションと同様に、このような一見では異常なジオロケーションは、本明細書に記載された他の手法で検証する必要がある。

【 0 1 0 9 】

サンドイッチジオロケーションの例

以下、ニューヨーク市の収集装置からオーストラリアの IP アドレスまでの追跡ルートを検討する。IP シーケンス 1 1 4 . 3 1 . 1 9 9 . 2 4 2、1 1 4 . 3 1 . 1 9 9 . 5 9 および 1 1 4 . 3 1 . 1 9 9 . 5 8 のホップ (ホップ 1 3、1 4 および 1 5) が各々米国、ニュージーランドおよび米国に位置するため、この IP シーケンスをサンドイッチとして特定する。この場合、シーケンス内の各ホップが MPLS トンネル (4 列目の MPLS ラベルで示されている) に位置し、RTT が個々の IP のものではなく、トンネルの最後の RTT を反映するため、RTT は、役に立たない。

【 0 1 1 0 】

10

20

30

40

【数 8】

From vps01.nycl to 203.209.210.16 at UTC 1434920785 (2015-06-21-21:06:25)

TTL	IP	RTT	MPLS	ASN	CC	City	
0	192.170.146.138	0.0	--	29791	US	New York	
2	63.251.26.29	0.338	--	13789	US	New York	
3	216.52.95.70	0.794	--	13789	US	New York	
4	38.88.194.85	0.897	--	174	US	New York	
5	154.54.47.17	1.347	--	174	US	New York	10
6	154.54.27.157	13.565	--	174	US	Cleveland	
7	154.54.44.85	20.738	--	174	US	Chicago	
8	154.54.6.85	32.995	--	174	US	Kansas City	
9	154.54.30.53	70.842	--	174	US	San Francisco	
10	154.54.28.34	71.549	--	174	US	San Jose	
11	154.54.1.162	72.421	--	174	US	San Jose	
12	38.122.92.2	75.331	--	174	US	San Jose	
13	114.31.199.242	241.947	16521	4826	US	San Jose	
14	114.31.199.59	237.467	289900	4826	NZ	--	20
15	114.31.199.58	237.879	16721,16946	4826	US	San Jose	
16	114.31.199.28	241.783	16946	4826	AU	Sydney	
17	175.45.72.119	237.379	16955	4826	AU	Sydney	
18	114.31.196.163	237.158	16741	4826	AU	Melbourne	
19	114.31.196.38	237.027	--	4826	AU	Melbourne	
20	175.45.117.218	252.021	--	4826	AU	Melbourne	
21	203.209.196.49	249.522	--	23681	AU	Melbourne	
22	203.209.196.61	252.346	3154	23681	AU	Melbourne	
23	203.209.210.16	269.123	--	23681	AU	Melbourne	30

【 0 1 1 1 】

しかしながら、サンドイッチ内のIPアドレスの逆引きDNS（以下に示されている名前中の「sjc」および「ca」）のジオロケーションヒントは、全ての3つのIPアドレスのジオロケーションがカリフォルニア州サンノゼ（San Jose）であることを示唆している。

【 0 1 1 2 】

【数 9】

114.31.199.242	bundle-101.cor01.sjc01.ca.VOCUS.net	
114.31.199.59	bundle-100.cor02.sjc01.ca.VOCUS.net	40
114.31.199.58	bundle-100.cor01.sjc01.ca.VOCUS.net	

【 0 1 1 3 】

サンノゼ（San Jose）のある場所からの更なる検査によって、114.31.199.59は、サンノゼから2.157msである。光ファイバの速度制約によって、サンノゼからニュージーランドのWellingtonまでの可能な最小RTTが107msであるため、ニュージーランド（NZ）は、妥当なジオロケーションではない。

【 0 1 1 4 】

【数 1 0】

```

Traceroute to 114.31.199.59 from San Jose, CA:
traceroute to 114.31.199.59 (114.31.199.59), 30 hops max, 60 byte
packets
 1  vl99.mag01.sjc01.atlas.cogentco.com (66.250.250.113)  0.338 ms
0.347 ms
 2  te0-4-0-1.ccr22.sjc01.atlas.cogentco.com (154.54.84.153)  0.698
ms te0-4-0-1.ccr21.sjc01.atlas.cogentco.com (66.28.4.157)  0.628 ms
 3  be2095.rcr21.b001848-1.sjc01.atlas.cogentco.com (154.54.3.138)
1.242 ms  1.252 ms
 4  38.122.92.2 (38.122.92.2)  1.128 ms 38.122.93.2 (38.122.93.2)
1.120 ms
 5  bundle-101.cor01.sjc01.ca.VOCUS.net (114.31.199.242)  1.348 ms
1.166 ms
 6  bundle-100.cor02.sjc01.ca.VOCUS.net (114.31.199.59)  2.157 ms *

```

10

【 0 1 1 5】

ジオロケーションサーバは、114.31.199.59がサンノゼから2.157msであると断定する。すなわち、真のジオロケーションは、サンノゼの収集装置から215キロ以内である。したがって、ニュージーランドは、妥当なジオロケーションではない。また、ジオロケーションサーバは、このIPアドレスのrDNSに埋め込まれたサンノゼ(San Jose)の空港コード「sjc」を検出することによって、サンノゼが実際のジオロケーションであることをさらに裏付け、このIPアドレスのジオロケーションをカリフォルニア州サンノゼ(San Jose)に訂正する。

20

【 0 1 1 6】

エッジ遅延ジオロケーション

いくつかの実現例において、ジオロケーションサーバは、エッジ遅延アルゴリズムを用いて、隣接するホップのジオロケーションを推測する。この方法は、追跡ルート内の最後から2番目のホップのジオロケーションが最終標的のジオロケーションを示しているか否かを調べる場合、特に最終標的が(ネットワークエンジニアによってしばしばアイボールネットワークとして呼ばれる)エンドユーザネットワークであって、逆引きDNSにジオロケーションヒントが存在しない場合に、特に有用である。この場合、最後から2番目のホップは、インフラストラクチャ、例えば、データセンタの場所をrDNSに埋め込んだデータセンタルータのIPアドレスである。

30

【 0 1 1 7】

このアプローチは、MPLSトンネル内部の追跡ルートおよびMPLSトンネル外部の隣接IPアドレス間の遅延差の分布を構築することによって機能する。全てのペアのRTTの間のメジアン遅延差を計算する。ペア内の一方のIPアドレスのジオロケーションが正しいと仮定して、計算した遅延差を用いて、ペア内の他方のIPアドレスのジオロケーションを推定する。ジオロケーションサーバは、次に、計算したメジアン値を各対の隣接するIPアドレスの推定ジオロケーションの可能な最小RTTと比較する。前者のメジアン値が後者の最小RTTよりも小さい場合、IPアドレスの片方または両方のジオロケーションが正しくない可能性がある。また、いくつかの実現例において、ペア内の一方のIPアドレスのジオロケーションを確認した場合、ジオロケーションサーバプロセスは、他方のIPアドレスのジオロケーションが、隣接するIPアドレスから、RTTのメジアン値および光ファイバの速度によって画定された半径の範囲内に位置すると推定する。

40

【 0 1 1 8】

最後から2番目のホップの例

マイクロソフト(登録商標)は、ワイオミング州のシャイアン(Cheyenne)近くのララミー郡(Laramie County)にデータセンタを有する。以下に示すように、シャイアンの東

50

部にあるニューハンプシャー州ポーツマスに位置する収集装置からの追跡ルート、およびシャイアの西部にあるワシントン州シアトルに収集装置からの追跡ルートを検討する。

【 0 1 1 9 】

【 数 1 1 】

Portsmouth to 191.234.85.3 [mpr=27.69ms]:

traceroute to 191.234.85.3 (191.234.85.3), 30 hops max, 60 byte packets

```

 1 rtr01.psm1.renesys.com (10.200.0.7)  0.193 ms  0.189 ms  0.188 ms
 2 hsrp2.psm1.renesys.com (195.160.236.3)  2.381 ms  2.395 ms  2.397 ms
 3 ray-b2.worldpath.net (64.140.193.25)  0.470 ms  0.516 ms  0.516 ms
 4 bst-edge-05.inet.qwest.net (63.239.32.25)  6.178 ms  6.188 ms  6.188 ms
 5 nyc-edge-04.inet.qwest.net (205.171.30.62)  8.228 ms  8.238 ms  8.238 ms
 6 63.151.150.98 (63.151.150.98)  8.462 ms  8.129 ms  8.120 ms
 7 ae0-0.nyc-96cbe-1b.ntwk.msn.net (207.46.38.113)  8.038 ms  8.104 ms  8.257 ms
 8 ae6-0.was02-96cbe-1c.ntwk.msn.net (191.234.84.142)  14.889 ms  14.797 ms *
 9 * * *
10 * * *
11 * * *
12 * * *
13 * * *
14 ae7-0.den01-96cbe-1a.ntwk.msn.net (191.234.84.222)  52.028 ms  52.041 ms  52.044 ms
15 ae8-0.cys01-96cbe-1a.ntwk.msn.net (191.234.80.191)  56.479 ms  56.490 ms  54.767 ms
16 191.234.85.3 (191.234.85.3)  54.487 ms  54.500 ms  57.758 ms

```

10

20

Seattle to 191.234.85.3 [mpr=15.45ms]:

traceroute to 191.234.85.3 (191.234.85.3), 30 hops max, 60 byte packets

```

 1 173.208.32.170.rdns.pingpipe.com (173.208.32.170)  0.125 ms  0.058 ms  0.055 ms
 2 v3508.er01.sea.ubiquity.io (23.105.64.1)  6.931 ms  7.117 ms  7.069 ms
 3 38.88.0.25 (38.88.0.25)  0.976 ms  1.161 ms  1.111 ms
 4 154.24.19.33 (154.24.19.33)  1.560 ms  1.510 ms  1.689 ms
 5 154.24.42.225 (154.24.42.225)  1.653 ms  1.580 ms  1.753 ms
 6 te0-1-0-7.ccr22.sea01.atlas.cogentco.com (154.54.41.145)  1.567 ms  1.325 ms  1.459 ms
 7 be2084.ccr21.sea02.atlas.cogentco.com (154.54.0.254)  1.740 ms  1.946 ms  2.126 ms
 8 38.104.126.78 (38.104.126.78)  1.177 ms  1.134 ms  1.076 ms
 9 * * *
10 * * *
11 ae15-0.cys01-96cbe-1a.ntwk.msn.net (191.234.84.11)  55.000 ms  55.482 ms  55.377 ms
12 191.234.85.3 (191.234.85.3)  55.327 ms  55.269 ms  55.436 ms

```

30

40

【 0 1 2 0 】

両方の追跡ルートの最後から2番目のホップは、埋め込み r D N S を含む。各々のホップの r D N S は、Cys01を含み、C Y S は、シャイアン (Cheyenne) の I A T A 空港コー

50

ドである。最終標的の遅延が最後から2番目のホップの1ms以内にあるため、最後から2番目のIPアドレスと目標IPアドレスとが同一のデータセンタにあることを強く示唆している。ジオロケーションサーバは、最後から2番目のホップと目標IPアドレスとの間の遅延および最後から2番目のホップのrDNSを考慮して、この目標IPアドレスを最後から2番目のホップと同様の位置、すなわち、ワイオミング州シャイアンに割り当てる。

【0121】

IPエイリアスおよびMPLSラベルを使用したジオロケーション

ネットワーク接続装置（例えば、ルータ、ファイアウォールおよびスイッチ）は、通常、多くの異なるネットワークインターフェイスを有する。これらのインターフェイスの各々は、特有のIPアドレスを持つことができ、（多くの場合、銅線または光ファイバを介して）他の装置と物理的に接続することができる。例えば、1つのコンピュータ装置は、コンピュータ装置の（潜在的に多くの）インターフェイスに割り当てられた全てのIPアドレスと同様に、1つの地理位置に位置する。1つの装置に属する全てのIPアドレスを見出すプロセスは、エイリアス除去（de-aliasing）と呼ばれる。

【0122】

いくつかの実現例において、上記のジオロケーションサーバは、MPLSラベルに基づく技術に加えて、1つ以上のエイリアス除去技術（例えば、メルカトル技術）を用いて、エイリアス化されたIPアドレスを見出すことができる。ジオロケーションサーバは、これらの技術を用いて、IPのエイリアスセットを特定し、各セットの共通ジオロケーションを推定することができる。これらのエイリアスセットは、通常、インターネット上の1つのルータに設けたインターフェイスを表す。その結果、ジオロケーションサーバは、全てのセットのジオロケーションをより正確に判定し、観測された多くの追跡ルートのジオロケーションを訂正し、追跡されている装置に隣接するホップの可能なジオロケーションを1人以上のユーザに通知または警告することができる。

【0123】

メルカトル（Mercator）技術は、選択されたIPアドレスの任意のポートに任意のパケットを送信し、特定のルート追跡データ収集装置の目標ではないIPアドレスから、ポート到達不能なメッセージの返送時間を監視することを含むことができる。ルート追跡データ収集装置の目標ではないIPアドレスから適切なメッセージを受信すると、このIPアドレスが1つ以上のIPエイリアスを有することを推測することができる。このように、世界中に配置されたルート追跡データ収集装置は、グローバルルート追跡で観測された全てのIPアドレスを目標にすることができ、妥当なIPエイリアスのペアを収集することができる。また、この手法によって新たに発見されたIPアドレスをIPアドレスのリストに追加して、反復的にプローブすることによって、より多くのIPエイリアスを発見することができる。観察された矛盾のないペアは、推移閉包プロセスを介して共通セットに集めることができる。

【0124】

代替的な実現例は、ジオロケーションサーバに送信された世界範囲のルート追跡データ内のMPLSラベルの共通シーケンスを観察することを含む。特定のシーケンスに対して、異なる追跡が異なるルータインターフェイスを通過する時に、ラベルが変化しないが、そのIPアドレスが変化する可能性がある。ジオロケーションサーバは、MPLSラベルを用いて、異なるIPアドレスを同一の装置に関連付けることができる。

【0125】

MPLSラベルを用いて、異なるIPアドレスを同一の装置に関連付けることを理解するために、図6Aに示されたMPLSトンネル600を検討する。MPLSトンネル600は、エッジLSRとも呼ばれる入来ラベルエッジルータ（Label Edge Router、LER）602と送出LER606との間に接続されているいくつかのラベルスイッチルータ（label switch router、LSR）604a～604c（まとめてLSR604という）を含む。LER602は、パケットを受信すると、パケットの転送等価クラス（Forwarding

10

20

30

40

50

Equivalence Class、FEC) およびパケットのラベルスイッチング経路 (Label Switching Path、LSP) を決定し、パケットのMPLSヘッダを作成し、MPLSトンネル600の第1のLSR604aにパケットを転送する前に、適切なラベルをMPLSヘッダに挿入する。MPLSヘッダ内のラベルは、入来LERと送出LERとの間のMPLSトンネル600内のノード (この例では、LSR604) を特定する。

【0126】

パケットを受信すると、第1のLSR604aは、パケットのMPLSヘッダ内のラベルを検査することによって、パケットの宛先を判断する。しかしながら、他のルータとは異なり、第1のLSR604aは、必ずしもIPルーティング情報を持っているとは限らない。代わりに、第1のLSR604aは、単にパケットのMPLSヘッダ内のラベルを検査することによって、MPLSトンネル600におけるパケットの次の宛先 (この場合、第2のLSR604b) を決定する。第1のLSR604aは、MPLSヘッダを更新してから、パケットをLSR604bに転送する。同様の動作を繰り返すことによって、パケットが送出LER606に到達する。この送出LER606は、完全なIPルーティングテーブルを有し、パケットを適切にルーティングする。

【0127】

LSR604は、完全なIPルーティングテーブルではなく、特定のMPLSラベル情報を使用して動作するため、トラフィックを比較的迅速にルーティングすることができる。しかしながら、LSR604は、IPルーティング情報ではなくMPLSラベルに依存するため、必ずしもトラフィックをMPLSトンネル600の外側の宛先にルーティングできるとは限らない。具体的に、第1のLSR604aは、入来LER602から、TTL=1のパケットを受信する場合、「時間超過」メッセージを入来LER602に返せず、パケットを第2のLSR604bに転送する。第2のLSR604bは、パケットを第3のLSR604cに転送し、第3のLSR604cは、パケットを送出LER606に転送し、送出LER606は、「時間超過」メッセージを入来LER602に返す。入来LER602がTTL=2のパケットおよびTTL=3のパケットを第2のLSR604bおよび第3のLSR604cに各々転送する場合、同様のことが起こる。すなわち、パケットは、送出LER606に転送され、送出LER606は、「時間超過」メッセージを入来LER602に返す。また、送出LER606は、TTL=4のパケットを受信することに対応して、(正確に)「時間超過」メッセージを返す。TTL=4にならないと、実際のエンドポイントが見えないが、結果として報告された中間ホップに到達した時間は、実際にLER606に関するものである。インターネット上のMPLSトンネルの普及を考えると、MPLSトンネルを見つけて、MPLSトンネルの中間ホップ遅延を無視することによって、遅延を用いて、ジオロケーションを容易に特定することができる。

【0128】

図6Bは、ルート追跡データ内のMPLSラベルを用いて、特定のルータの地理位置を推定するためのプロセス600を示す。既知のMPLSドメインを通った追跡ルートの場合、ジオロケーションサーバは、LSPを選択するために入来LERに使用されたFECを決定する (ステップ602)。追跡ルート内の各MPLSホップに対して、ジオロケーションサーバは、MPLSホップのIPアドレスを追跡ルート上のある点のMPLSラベルシーケンスにマッピングする (ステップ604)。ジオロケーションサーバは、選択した時間枠に亘って、MPLSドメインを通った全ての追跡ルートに対して、IPアドレスのマッピングを繰り返す (ステップ606)。ジオロケーションサーバは、各々の特有の着信MPLSラベルシーケンスに対応する全てのIPアドレスを集約し (ステップ608)、遅延時間、rDNS情報またはその両方を用いて、集約したIPアドレスのジオロケーションを推定する (ステップ610)。

【0129】

例として、以下の3つの追跡シーケンスを検討する。以下の表は、遭遇したIPアドレスとMPLSラベルを列挙する。MPLSラベルシーケンスは、全ての3つのケースにおいて同様である。下線付きのIPアドレスは、同一のルータに属し、ラベルシーケンス (

10

20

30

40

50

1314, 1496, 1793)によって特定される。斜体のIPアドレスは、別の共通ルータに属し、ラベルシーケンス(1314, 1496, 1793, 1807, 1609)によって特定される。ジオロケーションサーバは、共通のラベルシーケンスを共有する同一のMPLSドメインを通った複数の追跡シーケンスから見付けたMPLSのIPアドレスを同一のルータに属するものとして特定することができる。MPLSのIPアドレスは、同一のルータに属するため、同様の地理位置を有する。

【0130】

【表2】

追跡フラグメント#1		追跡フラグメント#2		追跡フラグメント#3	
IPアドレス	MPLS ラベル	IPアドレス	MPLS ラベル	IPアドレス	MPLS ラベル
4.69.143.238	1314	4.69.143.238	1314	4.69.143.238	1314
4.69.161.114	1496	4.69.161.114	1496	4.69.161.114	1496
<u>4.69.137.58</u>	1793	<u>4.69.137.50</u>	1793	<u>4.69.137.54</u>	1793
4.69.134.154	1807	4.69.134.154	1807	4.69.134.154	1807
4.69.134.129	1609	4.69.134.137	1609	4.69.134.141	1609

【0131】

上記の技術を用いて、ジオロケーションサーバは、1つの機器に属し、したがって1つのジオロケーションに位置する可能性が高い組のIPアドレスを収集する。次いで、ジオロケーションサーバは、遅延および/またはDNS情報を用いて、各組のIPアドレスを共通のロケーションまたはロケーションセットに設定しようとする。

【0132】

メルカトルサブプロセスを用いて見出したIPエイリアスセットの場合、IPアドレス自体は、一般的に直接プローブ可能である。ジオロケーションサーバは、複数の場所から特定のメンバセットにPINGすることによって、最も近い収集装置を検出し、遅延測定値に基づいて、一組の妥当な地理位置を割り出す。

【0133】

いくつかの実現例において、ジオロケーションサーバは、三角測量技術を使用して、最も近い収集装置を決定する。ジオロケーションサーバは、各セット内の全てのIPを逆解析することによって、空港コード、都市名または他の地理的な略称を探す。DNS情報からの場所セットと遅延測定値からの場所セットとの交差は、より小さい潜在的な場所セットを形成する。この場所セットが空の場合、ジオロケーションサーバは、(人間が入力したものであり、誤差がある)DNS情報を無視する。各セットのIPエイリアスの最終結果は、観測された全ての遅延測定値と一致し、可能な場合、DNSラベルから得られた地理的なヒントと一致する妥当な場所セットである。

【0134】

MPLSラベルを用いて見出したIPエイリアスセットの場合、IPアドレス自体は、必ずしも直接的にプローブ可能ではなく、ルート追跡を介して、他の宛先に送信することによって観測可能である。また、このようなルート追跡測定で観察された遅延情報は、そ

のタイミングがトンネルの終端に関連する可能性があるため、MPLSトンネルの中間ホップを得るために使用できない。したがって、上述したように、ジオロケーションサーバは、一般的にMPLSラベルを用いて、ルート追跡から得られた遅延測定値を特定できるMPLSトンネル内の中間ホップの遅延を廃棄することができる。遅延情報の直接的なプロービングまたは正確な遅延情報の間接的な取得が不可能の場合、ジオロケーションサーバは、DNSラベル逆引きを行うことによって、MPLSトンネルに属するIPエイリアスの位置を特定することができる。

【0135】

図7Aおよび7Bは、ジオロケーションサーバプロセスに利用されたIPエイリアス除去技術の一例を示す。以下、ジオロケーションサーバに利用され、共通ルータ上のIPアドレスを特定し、セット全体のジオロケーション推定値を改善するためのメルカトル技術の一例を示す。以下の12個のIPアドレスは、IPエイリアスの関連セットとして特定された。

【0136】

【数12】

68.86.83.46, 68.86.83.42, 68.86.83.38, 68.86.83.34, 68.86.82.94,
50.242.148.85, 68.86.82.82, 68.86.85.218, 68.86.82.86, 68.86.82.90,
23.30.206.41, 23.30.206.153

【0137】

ジオロケーションサーバは、図7Aに示すプロセス700を用いて、グラフ内の接続された要素を見つけることによって、上記のセットを特定する。すなわち、IPアドレスAのメルカトルプローブがIPアドレスBを返す場合、IPアドレスAおよびBが関連することができる。このような関連付けは、理論的にグラフ上で、有向エッジで、AおよびBを各々表す2つのノードを連結したものであるとして描くことができる。AがBのエイリアスであり且つBがCのエイリアスである場合、A、BおよびCは、互いのエイリアスである。

【0138】

換言すれば、プロセス700は、センサからの任意のパケット（例えば、TCP（Transmission Control Protocol）パケットまたはUDP（User Datagram Protocol）パケット）を、選択したIPアドレスを表すルータインターフェースの任意のポートに送信することを含む。センサは、往復遅延を測定し、ポート到達不能なメッセージを監視する（ステップ704）。センサがポート到達不能なメッセージを受信すると、センサまたはジオロケーションサーバは、ポート到達不能なメッセージが任意のパケットの宛先とは異なるIPアドレスから返されたものであるかを判断する（ステップ706）。肯定の場合、ジオロケーションサーバは、ポート到達不能なメッセージを返したIPアドレスを含む宛先のIPアドレスが1つ以上のIPエイリアスを有すると判定する（ステップ708）。次に、ジオロケーションサーバは、全てのIPエイリアスが同一のジオロケーションに位置すると判断し（ステップ710）、上述した技術を用いてジオロケーションを推定する。

【0139】

上記の12個のIPアドレスおよび得られた関連性は、図7Bに示す接続グラフによって表すことができる。図7Bは、全てのIPアドレスが関連していることを示す。図7Bにおいて、12個のIPアドレスのうち7個が強く接続されたサブグラフを形成するため、各IPアドレスは、両方向から「可視」である。すなわち、Aをプローブする場合、コンポーネントの少なくとも1つのメンバを返し、コンポーネントの1つ以上のメンバをプローブする場合、Aを返す。接続されたコンポーネントしか必要としないが、強く接続されたコンポーネントは、エイリアスの非常に強い証拠を提供する。

【0140】

上記の接続性に基づいて、ジオロケーションサーバは、同一装置に属するIPアドレスを推測することができ、これらのIPアドレスを同一の地理位置に割り当てることができる。遅延測定値は、これらのIPアドレスが全てカリフォルニア州サンノゼ（San Jose）

10

20

30

40

50

に近いことを示している。これらのIPアドレスの全てのDNS情報は、サンノゼのグレートオークス (Great Oaks) 地区を示している。例えば、図7の68.86.83.46ノード705をbe-17-pe02.1lgreatoaks.ca.ibone.comcast.netに変換することができる。ジオロケーションサーバによる自動分析に基づいて、12個のIPアドレスは、全て米国のカリフォルニア州サンノゼのグレートオークスに位置する。

【0141】

現時点では、3つの商用IPジオロケーションプロバイダは、これらの12のIPアドレスに対して、以下のジオロケーション推定値を与えた。

【0142】

プロバイダ1：米国、特定の都市なし

プロバイダ2：バージニア州アッシュバーン (Virginia, Ashburn)、ジョージア州マリエッタ (Georgia, Marietta)、コロラド州デンバー (Colorado, Denver)、カリフォルニア州ロサンゼルス (California, Los Angeles) を含むいくつかの米国都市

プロバイダ3：ワシントン州シアトル (Washington, Seattle)、コロラド州デンバー (Colorado, Denver)、テキサス州ダラス (Texas, Dallas)、ジョージア州マリエッタ (Georgia, Marietta) を含むいくつかの米国都市

これらは、商用IPジオロケーションデータの典型的な例である。商用ジオロケーションプロバイダは、全てのエイリアスを同一の位置に割り当てることが殆どないが、(特に国際接続ルータの場合) エイリアスを異なる国に割り当てることが珍しいことではない。

【0143】

トランシット木

いくつかの実施形態において、ジオロケーションサーバは、遅延およびDNS解析を用いて、国レベルで間違ったジオロケーションを特定し、その後、訂正および改良を行うことができる。これを達成するために、ジオロケーションサーバは、複数(例えば、600以上)のピアセッションからのBGPルーティングデータに対する分析を実行する。ジオロケーションサーバは、BGPデータ収集装置から、インターネット上で追跡される各ネットワークプレフィックスまでの自律システム(AS)経路に関する情報を含むBGPデータを受信する。各AS経路は、ルートを交換し、一定のビジネス関係を維持する近隣自律システムを表すAS-ASEッジを含む。

【0144】

図8Aは、ジオロケーションサーバによって生成された、インターネットの起源からコアまで遷移する単一のネットワークプレフィックスを示す。いくつかの実現例において、ジオロケーションサーバは、機械学習分類器を用いて、これらのASEッジをいくつかの異なるカテゴリ(タグ)、例えば、トランシット、ピアリング、クラスタ、交換のうちの1つに分類する。地方または地域のトランシットプロバイダは、限定された地理範囲に経営するため、したがって、所在国に割り当てられたネットワークプレフィックスを遷移すると予想される。生成されたBGPエッジのタグは、ジオロケーションサーバによって利用され、各ネットワークプレフィックスがインターネットの起源からコアまで遷移した状態、例えば、図8Aに示すトランシット木を決定する。

【0145】

図8Bは、同一のトランシットエッジが所有する他のプレフィックスの仮定ジオロケーションに基づいて、検討中のプレフィックスの可能なジオロケーションを決定するためのプロセス800を示している。ステップ802において、ジオロケーションサーバは、生成されたエッジタグに基づいて、検討中のプレフィックスのトランシット木を割り出す。次に、ジオロケーションサーバは、トランシット木内のエッジの全てまたは一部のプレフィックスのジオロケーションを調べる(ステップ804)。プレフィックスが通過すると観察された各エッジに対して、ジオロケーションサーバは、エッジを通過した全てのプレフィックスの地理分布を割り出し、そのエッジを通過した検討中のプレフィックスを観測しているBGPピアの数に基づいて、地理分布に加重値を付ける(ステップ806)。ジオロケーションサーバは、これらの加重地理分布を、検討中のプレフィックスの国家レベ

10

20

30

40

50

ルの（可能な）推奨ジオロケーションに結合する（ステップ808）。ステップ810において、ジオロケーションサーバは、トランシット木から推定地理位置を、1つ以上の第三者によって報告された検討中のプレフィックスのジオロケーションと比較する。上述したように、ジオロケーションサーバは、例えば、報告されたジオロケーションを自動的に取得することができる。推定地理位置が報告されたジオロケーションと一致しない場合、ジオロケーションサーバは、例えば上述した技術を用いて、遅延測定値を有するプレフィックスのジオロケーションを検証する（ステップ812）。

【0146】

図8Aに示されたトランシット木の実用例は、1つの大手商業プロバイダによって米国のオレゴン州ポートランド市に割り当てられたプレフィックス118.150.0.0/20に関するものである。このプレフィックスのトランシット木を調べると、多くのトランシットエッジが、このプロバイダによって台湾に割り当てられたプレフィックスを有し、殆どのBGPピアが、これらのエッジ、特にプレフィックスの起源に最も近いエッジを観察していることは分かる。ジオロケーションサーバによって行われた採点によって、このプレフィックスの最も可能なジオロケーションは、実際に台湾であり、米国ではないことを示している。遅延測定値は、このプレフィックスが台湾に位置する可能性があるが、米国に位置する可能性が全くないことを証明している。

【0147】

時間上相関するルーティングイベント

いくつかの実現例において、ジオロケーションサービスは、BGP故障履歴および不安定性データを用いて、間違っただジオロケーションを特定し、その後、訂正および改良を行うことができる。これを達成するために、ジオロケーションサーバは、複数（例えば、600以上）のピアセッションからのBGPルーティングデータから得られた、インターネット上の追跡プレフィックスの一部または全部に対して、故障および不安定性計算を実行し、同一時間に特定の行動を示すプレフィックスセットを「イベント」として特定する。これらのイベントを時間に相関させることによって、ネットワークインフラストラクチャおよびこれらのプレフィックスのルーティング経路の共通点を見出すことができる。

【0148】

割り出されたこれらのイベントは、しばしば、特定の地理位置における大きなネットワーク故障および復旧を表す。例えば、ジオロケーションサーバは、商業サービスが、121個のプレフィックス（これらのプレフィックスの96%がインドに割り当てられている）が同時に取り下げられたイベントを観測した。同日の15分後、ジオロケーションサーバは、これらのプレフィックスの殆どが戻されたことを観測した。この2つのイベントが99個の共通プレフィックスを含むため、同一の物理インフラストラクチャにおける障害および復旧である可能性がある。これらのプレフィックスの殆どが地理的にインドに割り当てられたという事実は、この解釈を裏付けている。

【0149】

ジオロケーションサーバは、インドに位置していない少数のプレフィックスを解析することによって、潜在的に間違っただジオロケーションの候補セットを生成することができた。同一ネットワークの障害によるものではなく、プレフィックスが同時に取り下げられるおよび復旧される可能性が非常に低い、ゼロではない。したがって、これらのプレフィックスのジオロケーションを検証する必要がある。

【0150】

例えば、米国ウィスコンシン州ラシーンのModine Manufacturing Companyに登録された198.40.150.0/24は、このようなプレフィックスの1つであった。2011年に、全ての利用可能な商業サービスがこのプレフィックスをインドに割り当て、殆どの商業サービスが今でもそうしている。ジオロケーションサーバは、198.40.150.0/24がAS21758（Modine Manufacturing Company）によって公告され、AS18101（Reliance Communications Mumbai）を独占的に通過したことを観測した。AS18101は、インドに独占的に位置し、ムンバイおよびチェンナイに多くのプレフ

10

20

30

40

50

ックスを有する。非常に驚くべきことに、彼らは、Modine社の本拠地であるウィスコンシン州ラシーン地域にもインターネットサービスを提供している。A R I Nからのレジストリは、このプレフィックスがウィスコンシン州のラシーンにあると記録している。これは、間違いなく、間違ったジオロケーションの共通原因である。

【 0 1 5 1 】

遅延データは、このプレフィックスがインドのチェンナイにあることを示唆している。Modine社が2008年12月の記者発表でインドのチェンナイに新しい製造施設を公告したことがあるため、これは、驚くべきことではない。駐在事務所のプレフィックスを本社の物理アドレスに登録することが珍しいことではない。ジオロケーションサーバは、時間的に相関する一群のBGPルーティング故障および復旧から潜在的に間違ったジオロケーションを発見することによって、このプレフィックスをチェンナイに配置し、遅延データを用いて新たなジオロケーションを検証することができる。遅延データだけではこのような間違ったジオロケーションの特定に十分であるが、BGPルーティングイベントは、より小さい地理的な規模で、特に遅延だけでは決定できない近接都市の位置を訂正および改良することができる。

10

【 0 1 5 2 】

図9は、短期間の地域的なインターネット不安定におけるネットワークプレフィックスの集合を示す。x軸は、時間を示し、y軸の各「列」は、各プレフィックスを示す。図中、パターンがはっきりと現れることによって、アルゴリズム的に分類されたプレフィックスの共通の不安定パターンを示すことができる。ジオロケーションサーバは、分類内の地理的な矛盾を検索し、上述した技術を用いて、異常を検証または無効化する。

20

【 0 1 5 3 】

エニーキャストインスタンスからの距離

いくつかの実現例において、ジオロケーションサービスは、グローバルエニーキャストネットワークに問い合わせることによって得られたIPアドレスの地理分布を用いて、不正確なジオロケーションを特定し、その後、訂正および改良を行うことができる。システムは、商用DNSサービスの一部として正式なDNS応答を提供し、世界中の数千万回の再帰に対する回答を与えるために、広く配置されたグローバルエニーキャストネットワークを含む。本明細書に記載の技術を用いて、エニーキャストネットワークの各インスタンスを照会する再帰の地理分布を監視することによって、地理的な異常値を発見し、可能な訂正を調べることができる。また、rDNSと同様に、エニーキャストインスタンスのジオロケーションは、そのインスタンスに対する位置クエリの弱い識別子である。すなわち、うまく設計されたエニーキャストネットワークは、クエリをローカルに保つ傾向がある。

30

【 0 1 5 4 】

パラメトリック経路フィッティング

いくつかの実現例において、ジオロケーションサービスは、追跡ルートエッジの下流で得られたIPアドレスの地理分布を用いて、間違ったジオロケーションを特定し、その後、訂正および改良を行うことができる。各追跡ルートは、ルート追跡データ収集装置から宛先IPアドレスまでの経路に沿って得られた一連の連続IPアドレスから構成される。その経路に沿った連続IPアドレスの各ペアは、グラフの理論的な用語で有向エッジとして見なすことができる。各エッジまたは各連続エッジシーケンスに対して、ジオロケーションサーバは、特定の経路フラグメントを通過した全ての追跡ルートのエッジの下流で得られた一組のIPアドレスを割り出すことによって、遅延およびホップを示すデータモデルを構築する。次に、ジオロケーションサーバは、有向経路フラグメントに各々関連する各下流IPアドレスセット内の地理的な異常値を探す。本明細書に記載の技術を用いて、これらの異常値の可能な訂正をさらに調べることができる。

40

【 0 1 5 5 】

位置特定できないIPアドレス

いくつかの実現例において、ジオロケーションサーバは、（例えば、「地球」または大

50

陸のような非常に広い区域以外の)合理的な特異度で、位置特定できないIPアドレスを特定する。このような特異度の欠如にはいくつかの理由がある。例えば、IPアドレスがモバイル装置に帰属しているため、自由にローミングすることができる。IPアドレスが衛星回線の他方端にある。衛星は、通常、静止軌道にあり(それによって、RTT 500msを超える遅延を有し)、広い地理区域をカバーする広幅ビームを有する。遅延を用いて衛星接続を特定することができるが、IPの実際の位置は、衛星ビームの任意位置にあってもよい。

【0156】

また、IPアドレスは、エニーキャストであり、すなわち、BGPルーティングを介して複数の場所から公表される可能性がある。この場合、これらのIPアドレスは、同時に多くの異なる場所に存在するため、単一のジオロケーションを有していない。しばしば、コンテンツプロバイダは、エニーキャストルーティング技術を用いて、一般的なコンテンツのレプリカストアからエンドユーザまでの遅延を短縮する。上記に説明したように、ジオロケーションサーバは、遅延測定値に基づいて、地理的に矛盾であると特定されたIPアドレスをエニーキャストとして標記する。

【0157】

ジオロケーションプロバイダは、通常、データベースに含まれた各IPアドレスを単一の地理位置に割り当てる。エニーキャストネットワークの場合、この方法は、錯誤を引き起こすことがある。例えば、8.8.8.8に位置するGoogle(登録商標)の一般的な公開DNS再帰リゾルバを検討する。前例に使用された商用プロバイダと同様のプロバイダを用いて、ジオロケーションサーバは、以下のジオロケーションを出力する。

【0158】

プロバイダ1: 米国カリフォルニア州マウンテンビュー(Mountain View, California, USA)

プロバイダ2: 米国カリフォルニア州マウンテンビュー(Mountain View, California, USA)

プロバイダ3: 米国カリフォルニア州マウンテンビュー(Mountain View, California, USA)

ジオロケーションサーバは、Google(登録商標)DNSのIPアドレス8.8.8.8が110個のルート追跡データ収集装置から5ms以内にあり、26704個異なる収集装置ペア間で矛盾があるため、エニーキャスト(すなわち、多くの実際のGoogle位置)である可能性が高いことを示している。しかしながら、ジオロケーションサーバの測定結果は、IPアドレス8.8.8.8を有するGoogleインスタンスのいずれも実際にマウンテンビューに位置していないことを示している。Google自身が公開した情報もこの結果を裏付けている。ジオロケーションサーバは、遅延測定値を用いて、エニーキャストプレフィックスを見つけるだけでなく、各エニーキャストインスタンスの可能な位置を特定することもできる。

【0159】

結論

本明細書は、本発明の様々な実施形態を記載および例示したが、当業者であれば、本明細書に記載の機能を実行するため、および/または結果を得るため、および/または利点を得るために、様々な他の手段および/または構造を想到することができ、これらの変形および/または修正の各々は、本明細書に記載された本発明の実施形態の範囲内に含まれるとみなされる。より概括的に、当業者であれば、本明細書に記載された全てのパラメータ、寸法、材料および構成は、例示的であり、実際のパラメータ、寸法、材料および/または構成は、本発明の教示が使用される特定の応用に依存することを理解するであろう。当業者は、本明細書に記載のパラメータおよび構成が例示的であり、実際のパラメータおよび/または構成が本発明のシステムおよび技術が使用される具体的な用途に依存することを理解すべきである。また、当業者は、通常の実験によって、本発明の具体的な実施形態と同等するものを認識または把握することができるであろう。したがって、本明細書に

記載の実施形態は、例示のみとして提示され、添付の特許請求の範囲および均等の範囲内に含まれることを理解すべきである。本発明は、具体的に説明した以外の方法で実施することができる。本明細書に記載された本発明の実施形態は、本明細書に記載された個々の特徴、システム、物品、材料、キット、および/または方法を対象とする。さらに、これらの特徴、システム、物品、キット、および/または方法の2つ以上の組み合わせが、互いに矛盾しない場合、本発明の範囲に含まれる。

【0160】

上述した本発明の実施形態は、多くの方法のいずれかで実施することができる。例えば、いくつかの実施形態は、ハードウェア、ソフトウェア、またはそれらの組み合わせを用いて実装されてもよい。一実施形態の任意の態様をソフトウェアの少なくとも一部に実装する場合、ソフトウェアコードは、単一のコンピュータによって提供された任意の適切なプロセッサまたはプロセッサ群または複数のコンピュータに分散された任意の適切なプロセッサまたはプロセッサ群に実行され得る。

10

【0161】

この点に関して、本発明の様々な態様は、少なくとも部分的にコンピュータ可読記憶媒体（または複数のコンピュータ可読記憶媒体）（例えば、コンピュータメモリ、1つ以上のフロッピー（登録商標）ディスク、コンパクトディスク、光学ディスク、磁気テープ、フラッシュメモリ、フィールドプログラマブルゲートアレイ（FPGA）、他の半導体装置、または他の有形的なコンピュータ記憶媒体または非一時的な媒体）にエンコードされた1つ以上のプログラムとして具体化することができ、これらのプログラムは、1つ以上のコンピュータまたは他のプロセッサ上で実行されると、上述した技術の様々な実施形態を実現する方法を実行する。コンピュータ可読媒体は、格納しているプログラムを1つ以上の異なるコンピュータまたは他のプロセッサにロードして、上述した本発明の様々な態様を実施することができるように、移動可能である。

20

【0162】

本明細書において、「プログラム」または「ソフトウェア」という用語は、一般的な意味で、コンピュータまたは他のプロセッサに指示して、上述した本発明の様々な態様を実施するようにプログラムすることができる任意の種類のコンピュータコードまたはコンピュータ実行可能な命令セットを指す。また、この実施形態の1つの態様によれば、実行されると本発明の方法を実行する1つ以上のコンピュータプログラムは、単一のコンピュータまたはプロセッサ上に駐在する必要がなく、多くの異なるコンピュータまたはプロセッサにモジュール式で配置されても、本発明の様々な態様を実施することができる。

30

【0163】

コンピュータ実行可能な命令は、多くの形態、例えば、1つ以上のコンピュータまたは他の装置によって実行されるプログラムモジュールであってもよい。一般的には、プログラムモジュールは、特定のタスクを実行するまたは特定の抽象データ型を実装するルーチン、プログラム、オブジェクト、コンポーネント、データ構造などを含む。典型的には、プログラムモジュールの機能は、必要に応じて、様々な実施形態に組み合わられてもよく、分散されてもよい。

【0164】

また、本明細書に記載された技術は、少なくとも1つの例示を与えた方法として具体化されてもよい。方法の一部として行われた動作は、任意の順序を実行してもよい。したがって、例示的な実施形態では連続的な動作として示されているが、例えば、例示の順序と異なる順序で、例えば、いくつかの動作を同時に行うように、実施形態を構成することができる。

40

【0165】

なお、本明細書において定義され、使用された全ての定義は、辞書定義、参照により組み込まれた文書の定義、および/または定義された用語の通常意味よりも優先する。

【0166】

特に明記しない限り、不定冠詞「a」または「an」は、本明細書および特許請求の範

50

囲に使用された場合、「１つ以上」を意味する。

【０１６７】

「および／または」という語句は、本明細書および特許請求の範囲に使用された場合、列挙された要素の「一方または両方」を意味し、すなわち、これらの要素が一部の場合に共に存在し、他の場合に単独に存在することを意味する。同様に、「および／または」で列挙された複数の要素は、列挙された要素のうち「１つ以上」として解釈すべきである。具体的に、「および／または」という語句によって具体的に特定された要素以外に、他の要素が、特定された要素と関連するか否かにかかわらず、必要に応じて存在してもよい。したがって、非限定的な例として、「Ａおよび／またはＢ」は、「含む（comprising）」などの開放型言語と併せて使用された場合、一実施形態において、Ａのみ（必要に応じて、Ｂ以外の要素）を含み、別の実施形態において、Ｂのみ（必要に応じて、Ａ以外の要素）を含み、さらに別の実施形態において、ＡおよびＢの両方（必要に応じて他の要素）を含むことを意味する。

10

【０１６８】

「または」という用語は、本明細書および特許請求の範囲に使用された場合、上記で定義した「および／または」と同様の意味を有すると理解すべきである。例えば、「または」または「および／または」は、リスト中の項目を分ける場合、包括的であり、すなわち、要素の数またはリストの少なくとも１つを含み、必要に応じてリストにない追加の項目を含むとして解釈すべきである。明白に反対の意味を示す用語、例えば、「１つのみ」または「正確に１つのみ」または「からなる」は、特許請求の範囲に使用された場合、要素の数またはリストの１つのみの要素を含むことを意味する。一般的に、本明細書に使用された用語「または」は、前方に「どちらか」、「一方」、「一方のみ」などの排他的な条件があった場合、排他的な意味（すなわち、両方ではなく、一方または他方）を意味するとして理解すべきである。「本質的に～からなる」という用語は、特許請求の範囲に使用された場合、特許法の分野に使用される通常の意味を有するものとする。

20

【０１６９】

１つ以上の要素のリストを参照する「少なくとも１つ」という用語は、本明細書および特許請求の範囲に使用された場合、必ずしもリストに具体的に列挙された全ての要素の少なくとも１つを含まず、リスト内の複数の要素から選択された少なくとも１つの要素を含み、リスト内の要素の組み合わせを除外しないことを意味すると理解すべきである。また、「少なくとも１つの」という用語によって具体的に特定されたリスト内の要素以外に、他の要素が、具体的に特定されたリスト内の要素と関連するか否かにかかわらず、必要に応じて存在してもよい。したがって、非限定的な例として、「ＡおよびＢの少なくとも１つ」（または同等に「ＡまたはＢの少なくとも１つ」、または同等に「Ａおよび／またはＢの少なくとも１つ」）は、一実施形態において、少なくとも１つのＡ、場合によって２つ以上のＡを含み、Ｂを含まない（場合によって、Ｂ以外の要素を含む）ことを意味し、別の実施形態において、少なくとも１つのＢ、場合によって２つ以上のＢを含み、Ａを含まない（場合によって、Ａ以外の要素を含む）ことを意味し、さらに別の実施形態において、少なくとも１つのＡ、場合によって２つ以上のＡ、および少なくとも１つのＢ、場合によって２つ以上のＢ（場合によって、他の要素）を含むことを意味する。

30

40

【０１７０】

特許請求の範囲および上記の明細書において、「備える（comprising）」、「含む（including）」、「もつ（carrying）」、「有する（having）」、「含有する（containing）」、「関与する（involving）」、「保有する（holding）」、「構成される（composed of）」などの全ての接続用語は、開放的な意味、すなわち、限定せず含むという意味で理解すべきである。「～からなる」および「本質的に～からなる」という接続用語のみは、米国特許商標庁の特許審査手続書第 2 1 1 1 . 0 3 項に記載されているように、閉鎖型または半閉鎖型接続用語として理解すべきである。

【図 1 A】

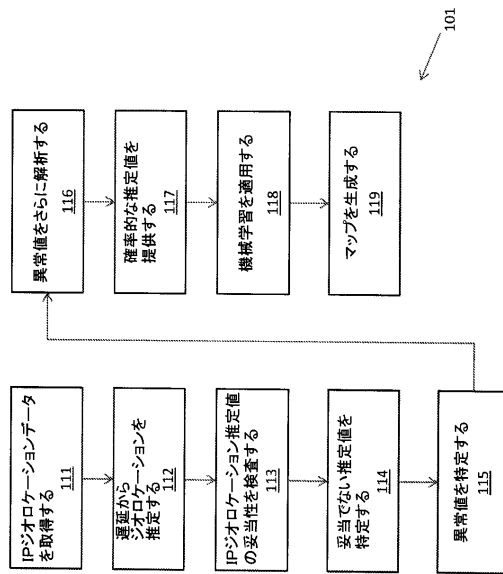


FIG. 1A

【図 1 B】

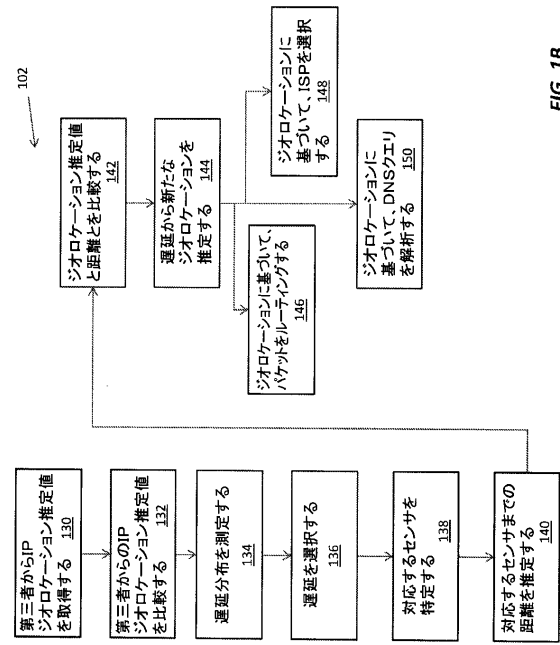


FIG. 1B

【図 1 C】

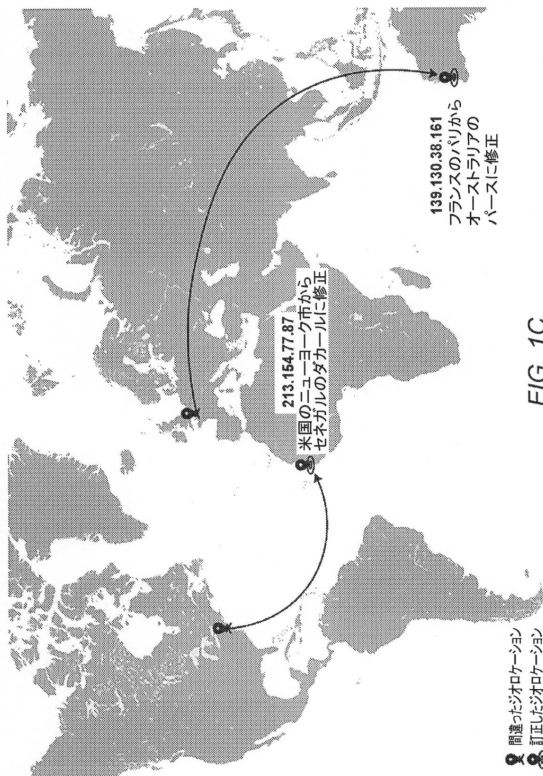


FIG. 1C

【図 2 A】

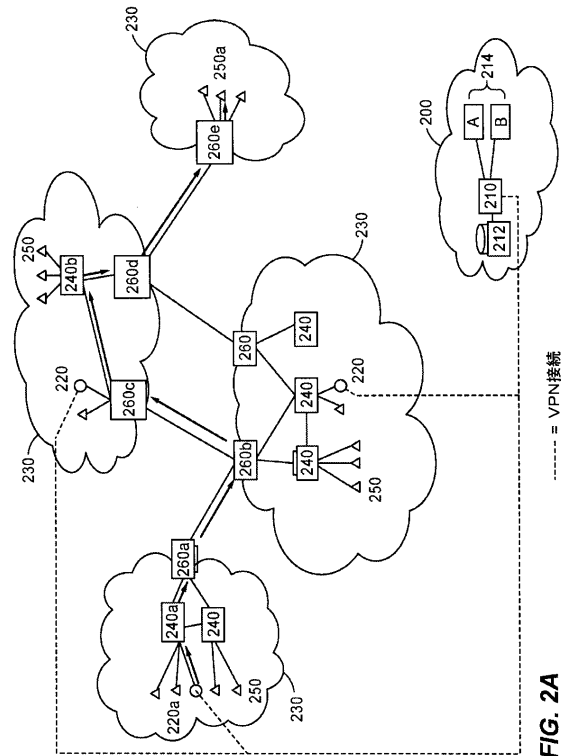


FIG. 2A

【図 2 B】

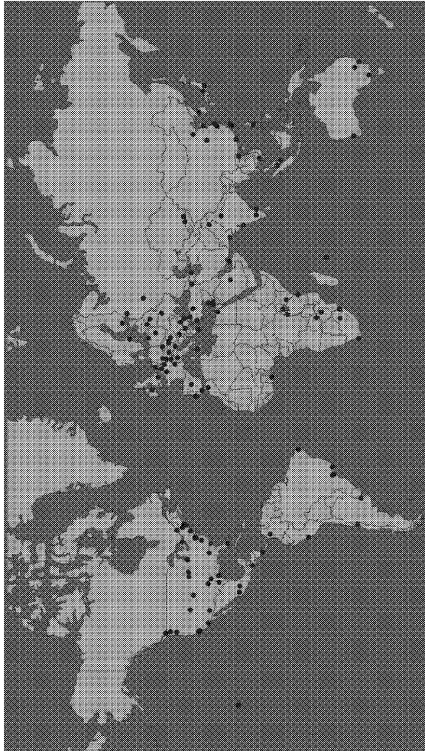


FIG. 2B

【図 2 C】

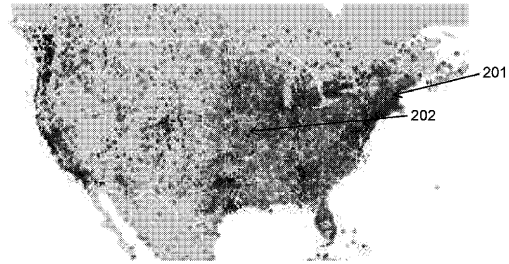


FIG. 2C

【図 2 D】

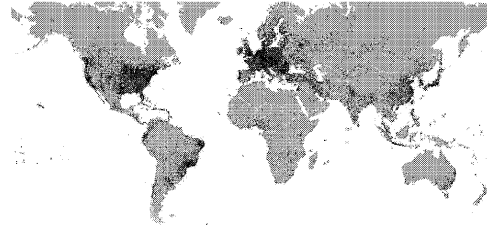


FIG. 2D

【図 3 A】

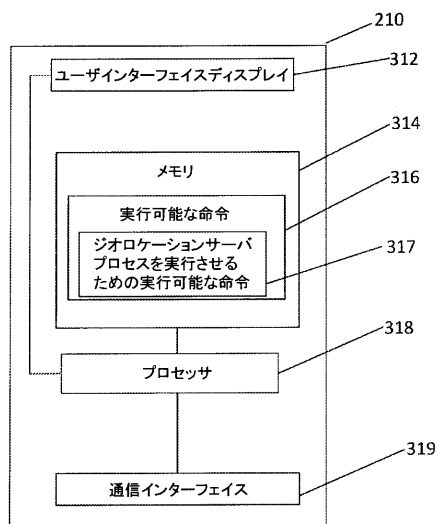


FIG. 3A

【図 3 B】

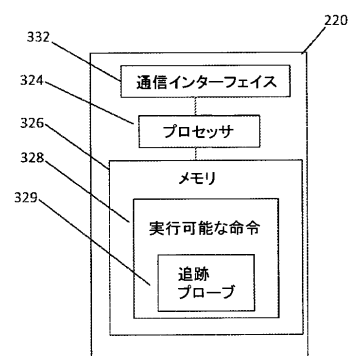
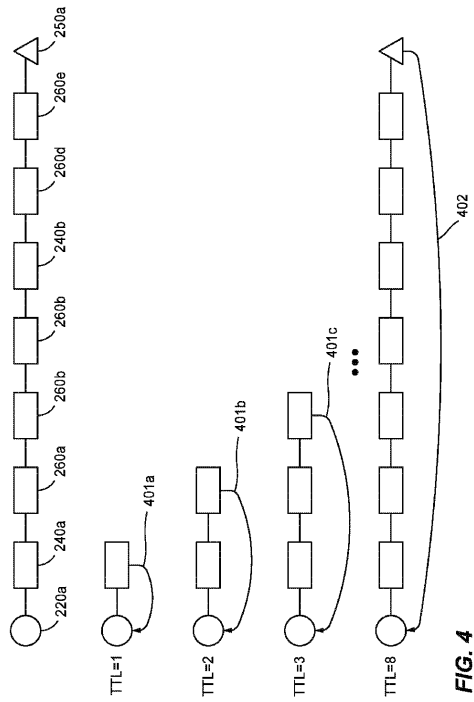


FIG. 3B

【図 4】



【図 5】

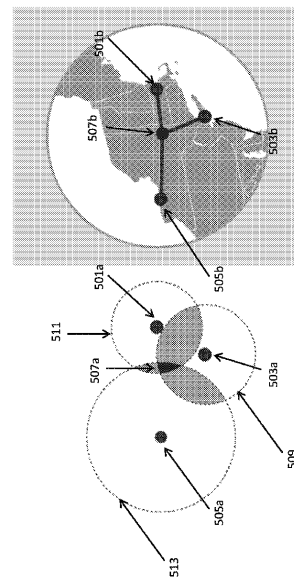


FIG. 5

【図 6 A】

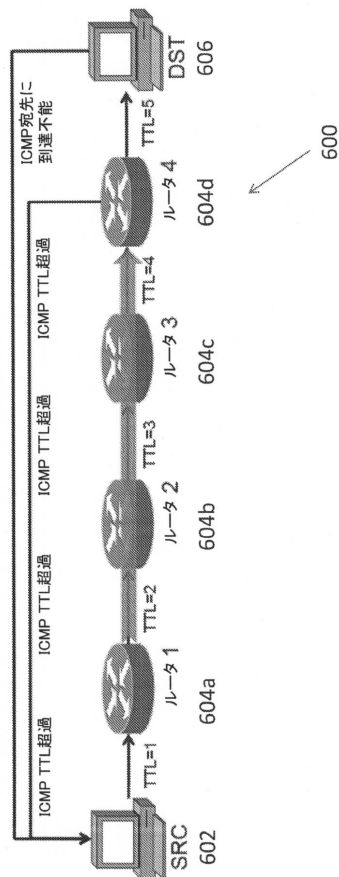


FIG. 6A

【図 6 B】

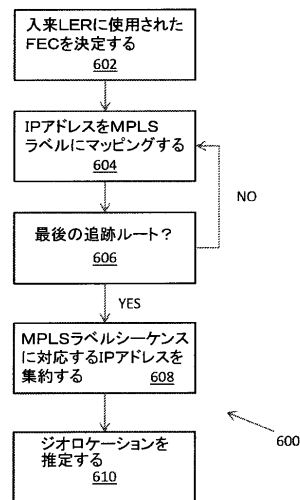


FIG. 6B

【図 7 A】

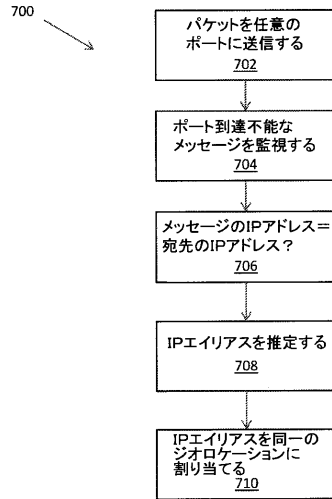


FIG. 7A

【図 7 B】

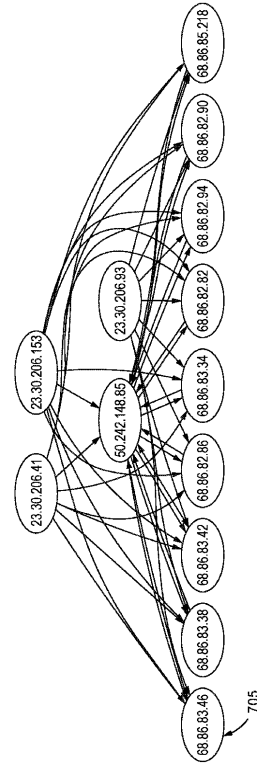


FIG. 7B

【図 8 A】

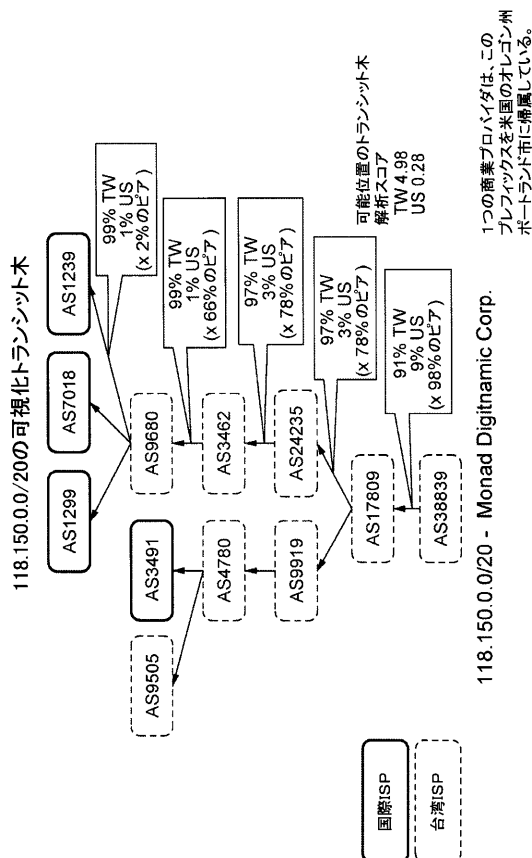


FIG. 8A

【図 8 B】

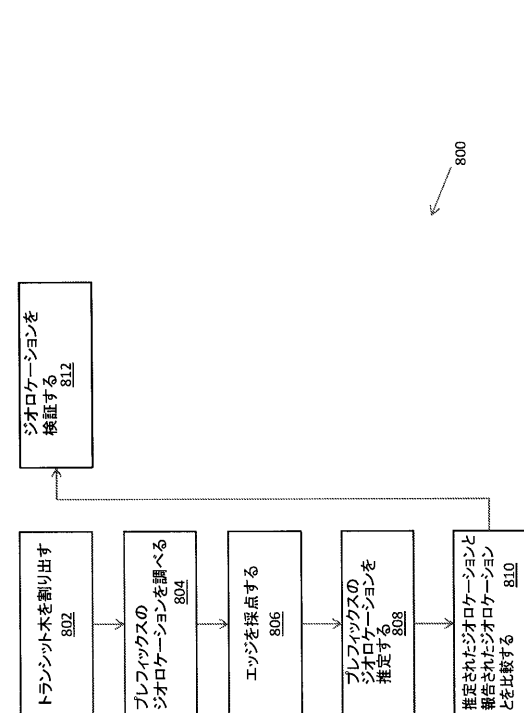
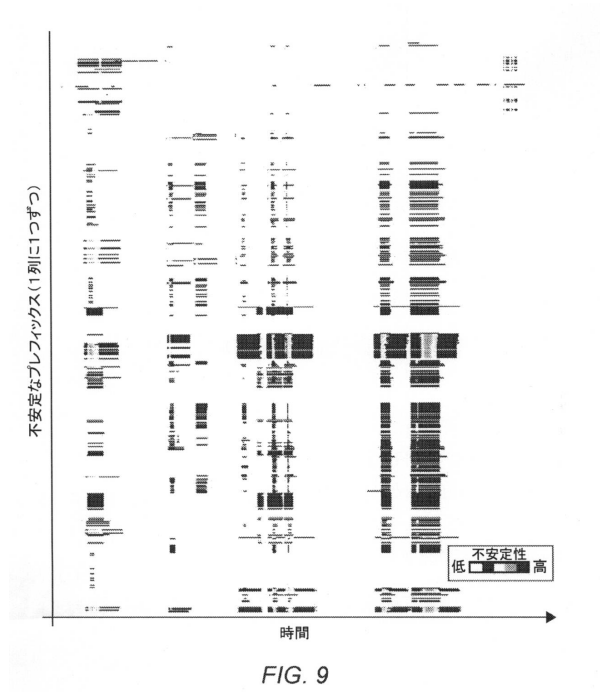


FIG. 8B

【図 9】



フロントページの続き

(72)発明者 タイシンガー, トーマス・リー

アメリカ合衆国、05055 バーモント州、ノーウィッチ、サンドバック・レーン、57

(72)発明者 マドリー, ダグラス・カール

アメリカ合衆国、03766 ニュー・ハンプシャー州、レバノン、レッジ・レーン、18

審査官 羽岡 さやか

(56)参考文献 米国特許出願公開第2011/0282988(US, A1)

特表2004-507917(JP, A)

米国特許第07711846(US, B2)

S.S.Siwpersad et al., Assessing the geographic resolution of exhaustive tabulation for geolocating Internet hosts, International Conference on Passive and Active Network Measurement, 2008年

Bamba Gueye et al., Constraint-Based Geolocation of Internet Hosts, IEEE/ACM TRANSACTIONS ON NETWORKING, VOL.14, NO.6, 2006年12月, P.1219-1232

Danilo Cicalese et al., A Fistful of Pings: Accurate and Lightweight Anycast Enumeration and Geolocation, 2015 IEEE Conference on Computer Communications(INFOCOM), 2015年5月1日, P.2776-2784

Doxa Chatzopoulou et al., IP Geolocation, 2007年1月, P.1-6

(58)調査した分野(Int.Cl., DB名)

H04L 12/00 - 12/955