共同ホワイトペーパー

Robust Localization Towards Trust-Enhanced Networking

富士通株式会社 データ&セキュリティ研究所,
Cyber Security Research Center @ Ben-Gurion University of the Negev

概要 インターネットジオロケーション技術の目的は、インターネットホスト、ユーザおよびクラウドデータの物理的、地理的な場所を特定することです。そして現在、ターゲットマーケティング、許可された地域に限ったデジタルコンテンツ販売、クレジットカード詐欺対策のセキュリティアプリケーションなど、さまざまな目的が提案され使用されています。しかし、ジオロケーション結果の信憑性、つまり正確さや信頼性に関する疑問が呈されます。私たちは、実世界のアセットに関する物理的属性を検証可能にすることでサイバースペースにトラストをもたらすという Trust-Enhanced Networking(TEN)のコンセプト実現に向けた取り組みとして、そのキーコンポーネントの 1 つである Robust Localization(RL)技術を提案します。本ホワイトペーパーでは、既存技術の調査を踏まえて問題点や技術的課題を明らかにし、それらを解決するための研究の方向性と戦略を概説します。

1.はじめに

インターネットは世界中のホストをつないでいますが、特定のホストまたはデータが地理的にどこにあるかを知ることが肝要な場合があります。非公式ではありますが、インターネットジオロケーション(IP ジオロケーションとも呼ばれます)が、インターネットユーザまたはデバイスの地理的な位置を特定する問題を解決するために使用されています。インターネットジオロケーション技術の発展は、オンライン広告、ゼロトラストセキュリティ、プライバシー規制、位置に基づくサービスなどの多くの実用的な用途によって推進されています。ターゲット広告はこれらのアプリケーションの中で最も収益性の高いものの 1 つです。例えば、Web サーバがアクセスしてきたユーザがシアトルにいると判断できる場合、Web サーバは、その提供ページにシアトルの顧客をターゲットとした広告を埋め込むことができます。また、広告に限らず、地理的な位置に基づいてコンテンツを調整することもよくあります。インターネットジオロケーションの他の応用としては、ユーザにより近いサーバへの自動リダイレクトや、ウェブ分析(つまり、Web ページのアクセスログを分析してマーケティングデータを抽出するなどの活用)もあります。また、サイバースペースを起点とするビジネス活動においては、地理的な観点からなりすまし行為を検知し、

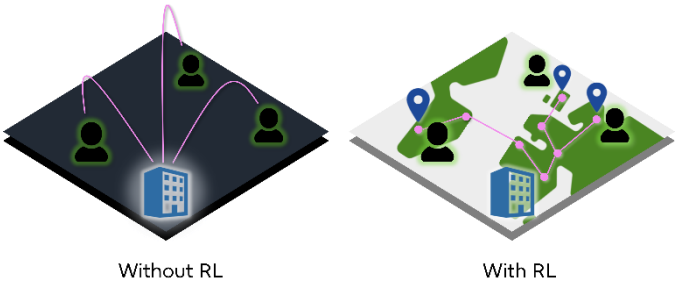

図 1: RL は地理的位置を検証可能にすることで信頼性の高いコミュニケーションを実現します

パートナー企業の真偽を検証するために、相手の所在を確認することが特に重要であると考えています。

富士通が以前発行したホワイトペーパー[1]では、新しいネットワーキングパラダイムである Trust-Enhanced Networking(TEN)のコンセプトを提案しました。TEN は、ネットワークエンティティに関する地理情報を使用して、実世界のエンティティの物理的な属性に関する信頼性の高い情報を提供し、ネットワーク全体におけるユーザのトラストを向上させます。この目的のために、TEN は物理空間からサイバー空間へ段階を追ったマッピングを行います。つまり、地理的な位置が検証されたネットワークエンティティのマップを更に、トラストアウェアなネットワークマップに変換し、ネットワーク制御への活用を図ります。また、トラストを測定するという観点から、

表 1:文献レビュー

Domain	*Ref.*	*Year*	*Method*
Delay-based geolocation & accuracy enhancements (landmarks, PoP)	[2]	2021	multilayered common routers
	[3]	2019	nearest common router
	[4]	2021	sorting nodes by their subnets
	[5]	2021	using IP webcams as landmark database
	[6]	2019	statistical learning to study localized delay and hop distance correlation
	[7]	2019	boundary nodes
	[8]	2018	closest common router
	[9]	2015	mining Internet forums
	[10]	2019	PoP partition algorithm
	[11]	2018	low-high-low delay distribution
	[12]	2016	IP city-level geolocation
Analysis methods (data mining & machine learning)	[13]	2016	neural networks with only a few landmarks
	[14]	2022	graph neural network combining IP host knowledge and neighborhood relationships
	[15]	2021	using neural networks to cluster landmarks
	[16]	2018	reverse DNS
	[17]	2017	reverse DNS
	[18]	2016	utilizing users' search queries
	[19]	2010	utilizing Facebook friendships
Cloud (data geolocation)	[20]	2020	"weak" and "strong" proofs
	[21]	2020	atomic proof method, which divides the proof into several minimum computation units
	[22]	2015	constraint-based cloud data geolocation using unclonable and tamper-proof device
	[23]	2013	querying an agent that is installed with the data
Geolocation and Proxy/VPN	[24]	2022	measuring and comparing the TCP handshake and TLS handshake
	[25]	2018	verification of the location information of 7 proxy services
Attack	[26]	2022	a system that allows verification of the claimed geolocations of network nodes in a fully decentralized manner
	[27]	2017	methods of hiding a host's real location
	[28]	2014	route hijacking
	[29]	2010	attacks on delay-based IP geolocation techniques
	[30]	2004	hiding IP geolocation using onion routers
RFC	[31]	2013	authorization policy language for controlling access to location information
	[32]	2020	format used by network operators to publish geolocation feeds

富士通は Quality of Service(QoS)と Quality of Experience(QoE)の発展形として Quality of Trust(QoT)の概念を提案しました。QoT は、ネットワークエンティティの検証された地理的位置から得られる情報を使用して計算されます。

このホワイトペーパーでは、TEN の重要課題の一つである Internet geolocation に関する技術的な課題について概説します。インターネットの文脈における位置は、通常、IP アドレスを意味します。ただし、地理的な位置の粒度が重要になる場合もあります。それはターゲットのアイデンティティを確認する、あるいはデータを盗難から保護する能力に影響します。一方、全地球測位システム(GPS)が地理的位置を追跡する方法としてよく知られていますが、GPS 情報はなりすましに対して脆弱という問題があります。ネットワークを介したリアルタイムな測定に基づいてターゲットの位置を推定するための多くのアプローチもあり、アクティブジオロケーションと呼ばれています。TEN のキー技術でもある Robust Localization(RL)は、そのソ

リューションの一つとして有望です。図１の左側に示すように、サイバー空間で活動を行う際には、物理的な属性が曖昧になることが多いですが、RL では、サイバー空間でのコミュニケーションに関わるエンティティの物理的な属性を明らかにします。RL は、アクティブジオロケーション技術の一つであり、悪意のある攻撃者や脅威に対処する際に、より高信頼な結果を提供する可能性のあるネットワーク測定を利用します。富士通と Ben-Gurion University of the Negev(以下、ベングリオン大学)は、2022 年 9 月以来、インターネット上で信頼できる通信のための技術開発を目標に、高信頼な位置推定技術を探求すべく共同研究を行っております。

2. 技術調査と洞察

本章では、ジオロケーション技術に関する調査結果を示します。ターゲットノードの位置推定精度を向上させるための様々なアプローチがあります。表 1 に既存研究を示します通り、ターゲットインターネットジオロケーションの問題は広範な研究の対象となっています。しかし、「トラスト」や「ロバスト」の側面はまだ十分に検討されていません。さらに、提案されているソリューションの多くは、セキュリティ攻撃に対する脆弱性が懸念されます。巧妙な攻撃者は遅延測定に対して細工を加えることができます。また、機械学習に基づく方式は正常な挙動を示す攻撃者によって騙される可能性があります。さらに強大な攻撃者を想定すると、経路のハイジャックや、ネットワーク負荷のバランスを操作する恐れもあります。

また、既存技術の大部分は遅延測定に基づく方式ですが、遅延の誤差に関する欠点により高精度のジオロケーションを実現することは難しいです。結果として、遅延測定に基づく技術だけでは地区レベル(district-level)の精度しか達成できません。機械学習やデータマイニングを応用した方式は、ストリートレベルの精度を達成し得ることが示されていますが、訓練や分析のために追加情報を必要とします。

一般に、パッシブな位置推定方式はカバレッジと信頼性{reliability}に問題があります。対象の IP アドレスを事前にインデックス化されていますが、その正確な位置のレコードがデータベースに存在するという保証がないためです。対象の情報が取得可能であっても、記録が古くなっていたり、情報が誤っていたり、位置が検証されていなかったりするために、情報が不正確になることがあります。一方、アクティブな位置推定方式は、ストリートレベルの精度を達成しますが、小さいカバレッジと信頼性の問題があります。例えば、ランドマークや Point of Presence(PoP)を使用すると、ラウンドトリップタイム(RTT)といった遅延測定の精度が向上します。ただし、高信頼なランドマークおよび PoP を識別する必要があります。

近年では、クラウドストレージサービスの利用が浸透しておりますが、データの位置情報に関する技術はまだ初期段階にあります。このトピックはまだ完全には探究されていないため、既存のソリューションは主に、広く研究されている既存のインターネットジオロケーションに依存しています。クラウドサービスの利用者が自身のデータが安全であるとは信じることができ、位置情報やプライバシーに関する規制へ対応できるようなソリューションを開発するための研究が必要です。

もう 1 つの広く使用されているサービスはプロキシと仮想プライベートネットワーク(VPN)です。ユーザはこれを使用して自身のアイデンティティや位置情報を隠すことができます。これにより、ユーザは自分の身元を偽って、地理的位置の制約のために通常は利用できないようなサービスを利用することが可能です。ジオロケーション技術は、こうしたトラストの問題の多くに対処するものと考えています。

最後に、対ジオロケーションの攻撃についての研究も行われています。敵対的なシナリオを扱うことで、ジオロケーション結果のトラストが高まると考えています。IP とクラウドの位置情報に関する既存のソリューションのほとんどは、敵対的な攻撃を受けやすいですが、敵対的なシナリオに対する取り組みは非常に少ないです。したがって、経路ハイジャック、IP 偽装、通信経路の匿名化などの攻撃が、位置情報やトラスト全般に及ぼす影響を理解することを目的とした研究が必要です。

また、2 つの重要な Request for Comments(RFC)に関しても言及する価値があります。RFC 8805[32]で定義される形式では、ネットワークオペレータが IP アドレスプレフィックスの大まかな位置情報を含む位置情報フィード(geolocation feed)を発行することができます。もし粒度が十分に高ければ、権威あるエンティティが公開するフィードは、信頼できるランドマークとして使える可能性があります。RFC 6772[31] は、位置情報へのアクセスを制御するための認可ポリシー言語を定義していま

す。具体的には、ターゲットの現在位置に基づいてデータへのアクセスを制限するために、位置情報に固有の条件要素を定義しています。

3.要件

インターネット上のトラストの重要な構成要素には、通信エンティティの信頼性とデータの信頼性が含まれます。原則として、コミュニケーションを行う際の最初のステップの 1 つは、コミュニケーションを行っているエンティティを識別することです。そして、それを信頼することでトラストなコミュニケーションが始まります。しかし、悪意のないエンティティになりすまして情報を盗んだり、許可なくサービスを使用したりする悪意のあるエンティティの存在はこの原則を脅かします。

また、ウェブサービスやクラウドサービスの利用者は、使用しているデータが信頼できるものであること(すなわち、データが改ざんされておらず、安全に保管されていること)を知りたいと考えています。しかし、悪意のある攻撃者によるデータ改ざんまたはクラウドサービスプロバイダ(CSP)による不透明なデータ再配置は、この要件を破り得ます。

インターネット上でのトラスト確保は、サイバー空間に対する深い考察と理解を必要とする問題です。ユーザおよびサービスプロバイダーは、書き換えが施された送信元アドレスをもって作成された IP パケットで IP スプーフィングを実行することにより、簡単に自身のアイデンティティを改ざんできます。また、ユーザはプロキシサーバーや VPN の背後に隠れることもできるため、その場合、ユーザを特定することが非常に難しくなります。遅延測定などで得る物理属性を変更することによって位置情報の操作も簡単に実行され、それを検知することも困難です。さらに、クラウドの内部アーキテクチャが公開されていないため、クラウドに格納されているデータの場所を検証することは複雑な問題です。

ジオロケーションにおけるトラスト

位置情報を確認することはトラストにとって重要な要素です。高信頼なジオロケーションはトラストなサイバー活動を支えます。例えば、組織 A がインターネットリソース B の位置を検証できた場合、A は B の位置が正しく報告されていると信頼します。さらに、A を信頼する顧客 C も、B の位置が正しく報告されていることを信頼することができます。

3.1.課題ステートメント

メタバースにおけるコミュニケーションおよびサービスは、地理的位置に基づいている場合があります。たとえば、日本国外からの日本のテレビ放送の視聴を制限したり、また、ハッカーによる偽装した位置からの偵察や銀行口座へのアクセスを制限します。したがって、ユーザおよびサービスプロバイダーは、相手の申告位置に対して確証を得る必要があります。ほとんどの場合、位置検証はユーザ間の通信遅延測定に基づいて行われます。その精度に関しては、都市レベルの精度を有しており、機械学習やデータマイニングのような他の方式の導入により更に高精度化が期待されます。一方で、それらの位置検証方式において、新しくトラストに関する疑問もオープンに議論されるべきだと考えます。

このホワイトペーパーでは、ターゲットホストの位置を検証するための既存方式の概要を示し、TEN コンセプトの一部であるネットワーク通信のトラストを高めるための新しいアイデアを提案します。

また、データの位置情報を検証する際の主な問題点についても議論します。クラウドサービスの利用拡大に伴い、データの位置情報の確認が重要な課題となっています。ただし、これは未だ十分には開拓されていな研究領域であり、サービスのトラストへの影響に対する業界の認識は非常に限られているのが現状です。

3.2.脅威モデル

私たちは、ユーザ、攻撃者、およびインターネットの三者を含むジオロケーションの問題をモデル化しました。ジオロケーションのユーザは、攻撃者の被害者になる可能性もありますが、ターゲットに関する真の情報とネットワークの測定値に基づく位置情報アルゴリズムを利用して、ターゲットの位置を正確に決定することを目指します。その上で、(1)ユーザは RTT とネットワーク経路の測定データを得るために世界中に分散した多数のランドマークマシンにアクセスでき、(2)ユーザはランドマークにより報告された測定結果を信頼すると仮定します。

攻撃者は、ターゲットが攻撃者の選択した偽造された場所にあるとユーザを誤解させたいと考えています。同様に、CSP は、意図せずに誤ったデータ位置を報告する可能性があります。ユーザがプロキシサーバーや VPN の背後に隠れることによるなりすましや位置情報に基づく攻撃の可能性はさらに厄介です。また、大規模な資源を持つ攻撃者であれば、ジオロケーションのアルゴリズムを操作することや、インターネットの経路をハイジャックすることもでき得ます。

測定値に基づく位置検証のシステムは、自身の位置や測定結果について虚偽報告する悪意のある攻撃者、または、特定のタイミングでプローブへの返答を遅らせるなどにより測定を作為的に操作する悪意のあるターゲットに対して必ずしもロバストではありません。

脅威モデルの第三者は、インターネット自体です。インターネットは攻撃者とユーザの両方に対して公平であるが、待ち行列遅延や迂回経路の結果として通信遅延にノイズが加算されます。この特性は、ジオロケーションのアルゴリズムが活用する測定結果に、潜在的な不正確性と予測不能性を生じさせます。一般的に、攻撃者によるネットワーク特性の悪意のある改ざん(遅延の追加など)が微小に行われた場合、インターネット自体の特性に起因するノイズと区別することは困難です。

4.技術的な課題

前述のように、ロバストなジオロケーションを求める TEN の要件では、複数の技術的な課題に対処する必要があります。TEN にはネットワークのトラストを幅広く、そして深く理解する必要があることは明らかですが、ロケーションベースのサービスの脆弱性を理解する必要もあります。すなわち、ネットワークのセキュリティとトラストの弱点を同定し、ロケーションベースサービスのロバスト性を強化するための技術を提案する必要があります。さらに、トラストを高めるためには、クラウドなどの新しいテクノロジーや環境の技術的要件をより深く理解する必要があります。

トラストの観念

トラストの観念を既存のジオロケーション技術に統合するには、認証とトラスト伝搬のメカニズムを統合する必要があります。例えば、アクティブジオロケーションに一般的に使用される ICMP Echo Reply および Time Exceeded メッセージには、認証機能がありません。アクティブジオロケーションのトラストレベルを高めために、認証のような機能を追加することは、プロトコルの改訂を必要とするためチャレンジングな課題です。

この状況は、権威あるソースからの信頼できるジオロケーションフィードによって若干緩和されます。ただし、ジオロケーションフィードの粒度はほとんどのユースケースで不十分なため、ジオロケーションサービスは十分に信頼できない追加の情報ソースも使用する必要があります。したがって、ここでの課題は 2 つあります。(1)権威あるジオロケーションフィードとしてジオロケーションデータのソースを識別すること、および(2)オポチュニスティックなソースに対するトラストの低減度合を定量化することです。

プライバシーとセキュリティ

プライバシーの問題に関しては、自己主権的なメカニズムを検討すべきです。理想的には、ユーザが位置情報の所有権と管理権を持ち、自分の地理的位置を他の組織や相手に自由に提示できるようにすべきです。位置情報のプライバシー設定を制御するために設計されたメカニズムもありますが[31]、そのようなメカニズムはアプリケーションレベルの位置情報交換のために設計されています。アクティブプロービングまたは他の位置推定技術に対して同様の制御を提供することは、主要な課題の一つです。

インターネットユーザが位置情報を隠すために使用する最も一般的な技術には、VPN や Web Proxy があります。より高度でプライバシーに関心のあるユーザは、Tor ネットワークなどのオニオンルーティングインフラストラクチャを使用します。インターネット標準は、実際の位置情報を公開したくないユーザのプライバシーを尊重する必要がありますが、同時に、そのようなユーザによって報告された位置は信頼し難くなります。したがって、位置情報を隠すようなプライバシー強化技術を効果的に検出することは、ビデオオンデマンドのような商用アプリケーションおよびゼロトラストのようなサイバーセキュリティアプリケーションの両方が直面する技術課題です。さらに、RL 技術は、位置情報に対するあらゆる種類の攻撃に対応できる必要があります(表 1 を参照)。

パフォーマンスとインフラストラクチャのリソース

ジオロケーションのパフォーマンスとロバスト性に影響する要因は多くあります。例えば、アクティブジオロケーションには、世界中に配置された広範囲のプローブネットワークが必要です。ターゲットホストの位置情報を取得する前に、プローブはそのホストに ping を実行し、結果を中央サーバに報告し、そのサーバが位置情報を推測する必要があります。タイムリーなアクティブジオロケーションへの障壁は、ゼロトラスト認証などのリアルタイムな応答を必要とするユースケースでの有用性を制限します。

更に、文献で研究されている側面は、ジオロケーションの粒度と精度です。これらは、インターネットにおけるジッターと経路のばらつきによってチャンレンジングな課題になります。既存のインターネット技術をもってしても、クライアントデバイスのレポートを信頼することなくロバストかつ効率的な方法で、ジオロケーションの粒度をオフィスや建物のレベルまで高めることは難しい課題です。

データのジオロケーション

クラウドベースのサービスによって保管されるデータの位置情報は、新たなニーズであり、大きな課題です。データの位置推定の難しさは、CSP 自身のアーキテクチャ(すなわち、フロントエンドとデータストレージの分離)、世界中に分散されたマルチレベルのキャッシュサーバなどから生じます。CSP が顧客のデータの場所を証明できるスキームは提案されていますが、実際にはほとんど使われていません。データが特定のデータセンターに配置されているかどうかをユーザが検証できるようにする技術の開発は大きな課題です。

5.まとめと今後の取り組み

TEN のコンセプトを紹介した前回のホワイトペーパー[1]に続いて、本ホワイトペーパーでは、TEN についてさらに詳しく説明し、TEN のユースケースの実現可能性を支える重要なコンポーネントである RL 技術にフォーカスして説明しました。インターネットにおける位置情報は、ターゲットマーケティングのようなサービス向上から耐フィッシング攻撃のようなセキュリティ強化に至るまで多くの現実的かつ重要なアプリケーションを持っており、本ホワイトペーパーで議論した技術領域の進歩は広範囲に及ぶ影響を持っています。

技術調査の結果、インターネットジオロケーションの分野では多くの先行研究がある一方で、脅威や攻撃者を想定してそれを緩和する技術に関する取り組みは数少ないことが分かりました。したがって、ジオロケーションにおける敵対的要素へのセキュリティ施策は未解決の研究課題であると考えます。文献レビューから得た洞察に基づいて RL の研究方向を示すために、私たちは、特に脅威・攻撃の緩和と精度向上に焦点を当てて、課題ステートメントと脅威モデルを記述しました。また、Web プロキシや VPN が介在する場合の地理位置情報、データ自体の地理位置情報に関する技術的課題を示し議論しました。

TEN 構想の実現を推進するためには、まず達成すべき目標を立て、それを達成するための戦略が重要です。

私たちの包括的な目標は、(1)TEN の必要性に関する認知を促進すること、(2)その必要性に対処する新技術の開発を推進すること、(3)TEN パラダイム実現に向けた新技術を他組織が利用・採用できるように準備すること、の 3 つです。

私たちは TEN の必要性についての議論を奨励し、認知を促進するために、IETF Meeting のようなイベントを通して学術界および産業界の両方に対して働きかけを実施しており、いくつかのステークホルダーやワーキンググループと議論をし始めております。今後も IETF との取り組みを継続しつつ、他の関連団体やコミュニティ、イベントなどへの参画も検討していきます。

新技術の開発を進めるために、学術界や産業界のパートナーと協力して、文献レビューから洞察された未解決の課題に取り組む予定です。富士通とベングリオン大学はすでに、TEN の重要な要素である RL の分野で共同研究を開始しています。そして、得られた研究結果や知見を、国際会議、論文誌などの場で発表することで、TEN の認知向上や活用促進を図ります。

私たちは TEN 技術の導入を促進するため、それに繋がるテスト API などオープンソースツールの作成も検討しています。また、開発したソリューションについて、標準化へ向けた取り組みや、ステークホルダーとの PoC を通して、TEN 技術の価値と実行可能性を実証します。

メタバースや Web3 が登場し、このテクノロジーの進化が目覚ましい時代と相まって、社会やビジネスの活動がサイバー空間

に移行しつつあります。ステークホルダー間のトラストを促進する上で、TEN の思想はますます重要になると考えています。私たちは、本ホワイトペーパーで概説した RL の技術領域を皮切りに、TEN のパラダイム実現に向けた研究開発を推進して参ります。

参考文献

[1] Fujitsu, "サイバー上の信頼性をリアルのフィジカル情報による裏付けで強化する「Trust-Enhanced Networking」のコンセプトに関するホワイトペーパーを公開," https://www.fujitsu.com/jp/about/research/article/202212-trust-enhanced-networking.html, 2022.

[2] Shichang Ding, Fan Zhao and Xiangyang Luo, "A street-level IP geolocation method based on delay-distance correlation and multilayered common routers," *Security and Communication Networks 2021*, 2021.

[3] Fan Zhao, Xiangyang Luo, Yong Gan, Shuodi Zu, Qingfeng Cheng and Fenlin Liu, "IP geolocation based on identification routers and local delay distribution similarity," *Concurrency and Computation: Practice and Experience*, 2019.

[4] Shuodi Zu, Xiangyang Luo and Fan Zhang, "IP-geolocater: a more reliable IP geolocation algorithm based on router error training," *Frontiers of Computer Science*, 2021.

[5] Qiang Li, Zhihao Wang, Dawei Tan, Jinke Song, Haining Wang, Limin Sun and Jiqiang Liu, "Geocam: An IP-based geolocation service through fine-grained and stable webcam landmarks," *IEEE/ACM Transactions on Networking*, 2021.

[6] Zhihao Wang, Hong Li, Qiang Li, Wei Li, Hongsong Zhu and Limin Sun, "Towards IP geolocation with intermediate routers based on topology discovery," *Cybersecurity*, 2019.

[7] Fan Zhao, Rui Xu, Ruixiang Li, Ma Zhu and Xiangyang Luo, "Street-level geolocation based on router multilevel partitioning," *IEEE Access*, 2019.

[8] Jing-ning Chen, Fen-lin Liu, Ya-feng Shi and Xiangyang Luo, "Towards IP location estimation using the nearest common router," *Journal of Internet Technology*, 2018.

[9] Guang Zhu, Xiangyang Luo, Fenlin Liu and Jingning Chen, "An algorithm of city-level landmark mining based on Internet forum," in *Proceedings of 2015 18th International Conference on Network-Based Information Systems, IEEE*, 2015.

[10] Fuxiang Yuan, Fenlin Liu, Donghua Huang, Yan Liu and Xiangyang Luo, "A high completeness PoP partition algorithm for IP geolocation," *IEEE Access*, 2019.

[11] Shuodi Zu, Xiangyang Luo, Siqi Liu, Yan Liu and Fenlin Liu, "City-level IP geolocation algorithm based on PoP network topology," *IEEE Access*, 2018.

[12] Siqi Liu, Fenlin Liu, Fan Zhao, Lixiang Chai and Xiangyang Luo, "IP city-level geolocation based on the pop-level network topology analysis," in *Proceedings of 2016 6th International Conference on Information Communication and Management (ICICM), IEEE*, 2016.

[13] Hao Jiang, Yaoqing Liu and Jeanna N Matthews, "IP geolocation estimation using neural networks with stable landmarks," in *Proceedings of 2016 IEEE Conference on Computer CommunicationsWorkshops (INFOCOM WKSHPS), IEEE*, 2016.

[14] Zhiyuan Wang, Fan Zhou, Wenxuan Zeng, Goce Trajcevski, Chunjing Xiao, Yong Wang and Kai Chen, "Connecting the hosts: Street-level IP geolocation with graph neural networks," in *Proceedings of the 28th ACM SIGKDD Conference on Knowledge Discovery and Data Mining*, 2022.

[15] Fan Zhang, Fenlin Liu, Rui Xu, Xiangyang Luo, Shichang Ding and Hechan Tian, "Street-level IP geolocation algorithm based on landmarks clustering," *CMCCOMPUTERS MATERIALS & CONTINUA*, 2021.

[16] Ovidiu Dan, Vaibhav Parikh and Brian D Davison, "Distributed reverse DNS geolocation," in *Proceedings of 2018 IEEE International Conference on Big Data (Big Data), IEEE*, 2018.

[17] Quirin Scheitle, Oliver Gasser, Patrick Sattler and Georg Carle, "Hloc: Hintsbased geolocation leveraging multiple measurement frameworks," in *Proceedings of 2017 Network Traffic Measurement and Analysis Conference (TMA), IEEE*, 2017.

[18] Ovidiu Dan, Vaibhav Parikh and Brian D Davison, "Improving IP geolocation using query logs," in *Proceedings of the Ninth ACM International Conference on Web Search and Data Mining*, 2016.

[19] Lars Backstrom, Eric Sun and Cameron Marlow, "Find me if you can: improving geographical prediction with social and spatial proximity," in *Proceedings of the 19th international conference on World wide web*, 2010.

[20] Yang Zhang, Dongzheng Jia, Shijie Jia, Limin Liu and Jingqiang Lin, "Splitter: an efficient scheme to determine the geolocation of cloud data publicly," in *Proceedings of 2020 29th International Conference on Computer Communications and Networks (ICCCN), IEEE*, 2020.

[21] Dongzheng Jia, Yang Zhang, Shijie Jia, Limin Liu and Jingqiang Lin, "Dpvgeo: Delay-based public verification of cloud data geolocation," in *Proceedings of 2020 IEEE Symposium on Computers and Communications (ISCC), IEEE*, 2020.

[22] Dong Lai Fu, Xin Guang Peng and Yu Li Yang, "Trusted validation for geolocation of cloud data," *The Computer Journal*, 2015.

[23] Mark Gondree and Zachary NJ Peterson, "Geolocation of data in the cloud," in *Proceedings of the third ACM conference on Data and application security and privacy*, 2013.

[24] Elisa Chiapponi, Marc Dacier, Olivier Thonnard, Mohamed Fangar and Vincent Rigal, "Badpass: Bots taking advantage of proxy as a service," in *Proceedings of Information Security Practice and Experience: 17th International Conference, ISPEC 2022, Springer*, 2022.

[25] Zachary Weinberg, Shinyoung Cho, Nicolas Christin, Vyas Sekar and Phillipa Gill, "How to catch when proxies lie: Verifying the physical locations of network proxies with active geolocation," in *Proceedings of the Internet Measurement Conference 2018*, 2018.

[26] Katharina Kohls and Claudia Diaz, "VerLoc: Verifiable localization in decentralized systems," in *Proceedings of 31st USENIX Security Symposium (USENIX Security 22)*, 2022.

[27] Abdelrahman Abdou, Ashraf Matrawy and Paul Oorschot, "Accurate manipulation of delay-based Internet

geolocation," in *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, 2017.

[28] Sharon Goldberg, "Why is it taking so long to secure internet routing? Routing security incidents can still slip past deployed security defenses," *Queue*, 2014.

[29] Phillipa Gill, Yashar Ganjali and Bernard Wong, "Dude, where's that IP? circumventing measurement-based IP geolocation," in *Proceedings of 19th USENIX Security Symposium (USENIX Security 10)*, 2010.

[30] Roger Dingledine, Nick Mathewson and Paul Syverson," Tor: The second-generation onion router," in *Proceedings of 13th USENIX Security Symposium (USENIX Security 04)*, 2004.

[31] H Schulzrinne, H Tschofenig, J Cuellar, J Polk, J Morris and M Thomson, "Geolocation policy: A document format for expressing privacy preferences for location information," *Technical report, RFC 6772 (IETF Stadrads Track)*, 2013.

[32] E Kline, K Duleba, Z Szamonek, S Moser and W Kumari, "A format for selfpublished IP geolocation feeds," *Technical report, RFC 8805 (Informational)*, 2020.

お問い合わせ先

富士通株式会社

データ＆セキュリティ研究所

contact-nwt@cs.jp.fujitsu.com