VPNを用いたユーザ間のIPアドレス交換による検閲とユーザトラッキングの防止の提案

李 驍睿[1]　新城 靖[1]　知念 慧弥[1]

1. 序論

近年、オンラインサービス提供者によるユーザプライバシーの侵害事例が増加している。サービス提供者は、精密な広告ターゲティングやマーケティングを行うため、さらには第三者へユーザデータを販売するために、ユーザの行動をトラッキングしている。

ユーザの識別方法としては、主にIPアドレスやCookieが用いられる。X（旧 Twitter）やInstagramなどの多くのオンラインサービスを利用する際、広告の内容がユーザの関心に強く関連していることが見受けられる。Cookieによるトラッキングは、ブラウザのプライベートモードを利用したり、不要なCookieを削除することで容易に拒否できるが、IPアドレスによるトラッキングを避けることはできない。IPアドレスは、トラッキングだけでなく検閲にも利用されている。検閲を回避するために、Tor [1] を用いてIPアドレスを変更することも行われている。

我々は、ユーザのプライバシーを保護するために、ユーザ間でIPアドレスを交換する手法を提案する。この手法では、ユーザがVPNを介してIPアドレスを交換することで、サービス提供者によるトラッキングを困難にする。本研究では、Richard Stallmanが提唱した「Charlieカード交換パーティ」の手法を用いる。Charlieカードとは、ボストン市の地下鉄に導入されたSuicaのような交通カードである。これは、当局がユーザの行き先をトラッキングできるものであった。これを嫌ったStallmanは、チャージが0になったカードをパーティに持ち寄りランダムに交換することで、ユーザへのトラッキングを防止することを考案した。本研究ではこの手法を用いて、インターネットに分散したユーザが互いのIPアドレスを交換できるようにする。

しかし、単純にこの手法を実装すると、Sybil Attackに対する脆弱性を持つことになる。また、各ユーザは交換すべきパブリックIPアドレスを持っていないことがある。本研究ではこれらの課題を解決し、ユーザビリティを向上させる。

[1] 筑波大学
University of Tsukuba

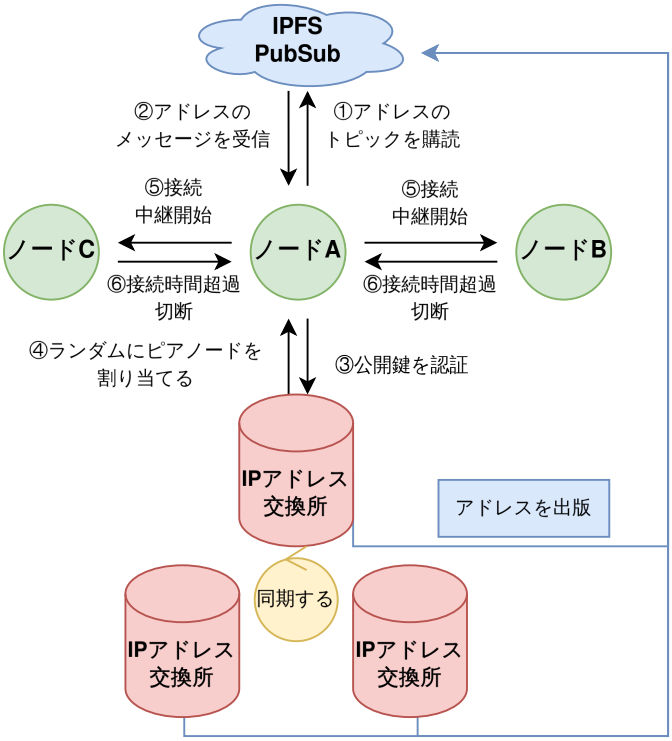

図 1　VPNによるIPアドレス交換の実装

2. 提案手法

2.1 概要

本研究は、図1で示したようにユーザのノードをVPNで接続してIPアドレスを交換する。各ユーザは、**IPアドレス交換所**（以下、**交換所**と略す）と呼ぶノードに接続し、交換相手となるユーザを得る。この論文では、この交換相手を**ピア**と呼ぶ。交換所については次の節で詳しく述べる。次に、各ユーザはVPNプログラムを実行し、ピアに接続する。この時公開鍵暗号方式で相互に認証してから、VPNトンネルを確立する。各ノードは互いにVPNを経由してオンラインサービスにアクセスする。その結果、そのノードとピアはオンラインサービスに対して実質的に互いにIPアドレスを交換したことになり、本来のIPアドレスは、隠蔽される。ある時間が経過すると、各ノードは別のピアを探し、IPアドレスを再交換する。

2.2 IP アドレス交換所

交換所は、複数のノードからの要求を受け付け、ランダムにペアリングを行い、ピアを紹介する。本研究では、検閲耐性を高めるため交換所は時々、自身の IP アドレスを変更し、その IP アドレスをすべてのノードに伝える必要がある。この時、DNS を使えばプロトコルやポート番号が含めらないという問題がある。

また、HTTP サーバを使うと単一障害点のリスクがある。そこで本研究では、IPFS[2] が持っている Publish-Subscribe モデルに基づく通信機能（IPFS PubSub）を用いて交換所の IP アドレスと付随するその他の情報を公開する。各ノードは、交換所の発見を 2 段階で行う。まず、各ノードは IPFS PubSub の特定のトピックを購読し、交換所からのメッセージを待ち受ける。その後、交換所が自身のアドレスをそのトピックに出版すると、ノードはそのメッセージを受信する。交換所は、出版するメッセージを自身の秘密鍵で署名し信頼性を確保する。各ノードは署名を検証後、取得したアドレスで交換所に接続する。

本研究では、単一障害点を無くすために、IP アドレス交換所のノードを複数実行し、相互にバックアップとして機能するようにする。各交換所ノードは、ノードの OAuth Token、公開鍵、ノードの IP アドレス、レーティングなどの情報を同期する。レーティングについては第 3 章で述べる。

3. Sybil Attack への対策

交換所が単純に全てのノードを受け入れると、Sybil Attack に対して脆弱になる。すなわち、検閲やユーザトラッキングを試みる組織が大量の Sybil ノードを生成し、交換所に登録すれば、一般のユーザは、Sybil ノードと IP アドレスを交換してしまう。

本研究では、このような Sybil Attack を防ぐために、電子投票の技術を利用することを検討している。これにより、1 人のユーザは 1 度に 1 つのノードしか利用できないようにする。

Sybil Attack の防止のために、本研究ではレーティングを導入する。各ノードは、接続が切断されるたびに、交換所にピアの接続時間と通信量を報告する。交換所は、各ピアのレーティングのスコアを算出し、レーティングの低いピアとのペアリングの確率を下げるか、接続を拒否する。本研究では、レーティングのスコアを、ピアとの接続時間、通信量、最後のオンライン時刻などを基づき算出する。

4. 実装

本研究では、各ノードの通信機能を libp2p[*1]の Rust 言語実装である rust-libp2p[*2]を使用し実装する。本研究では、libp2p が提供する gossipsub、UPnP および STUN の機能を使用する。また、libp2p-stream を使用し、VPN トンネルのトラフィックを転送する。トラフィックの暗号化には、QUIC でも用いられている TLS 1.3 を使用する。gossipsub は、IPFS PubSub にも使用されており、IPFS PubSub のトピックに参加することが可能である。UPnP と STUN は、パブリック IP アドレスを不要としながら、P2P 通信するために利用でき、ユーザビリティの向上に貢献する。

5. 関連研究

IP アドレスによるユーザトラッキングや検閲を回避する手段としては、Tor が広く使われている [1]。Tor では、中継ノードを提供するボランティアと、それを利用するユーザは別れている。これに対して、本研究では、対等なユーザが互いの IP アドレスを交換する点が異なる。

6. まとめ

本研究では、ユーザ間の IP アドレス交換を利用した検閲とユーザトラッキングを防ぐ手法を提案する。提案手法では、各ユーザは IP アドレス交換所というノードに接続し、IP アドレスを交換する相手を探し、そのノードと VPN 接続を行い、互いに相手の IP アドレスでオンラインサービスを利用する。交換所の発見とアドレス共有に IPFS PubSub を活用し、交換所側の頻繁な IP アドレス変更に対応する。また、Sybil Attack への対策としてレーティングを導入し、信頼性の低いピアとの接続を制限する。また、UPnP や STUN に対応させパブリック IP アドレスを不用にし、ユーザビリティの向上を目指した。

現在、libp2p を利用して提案手法を実装している。今後の課題は、提案手法を実装し、評価することである。

参考文献

[1] Dingledine, R., Mathewson, N. and Syverson, P.: Tor: The Second-Generation Onion Router, *13th USENIX Security Symposium (USENIX Security 04)*, pp. 1–18 (2004).

[2] Benet, J.: IPFS - Content Addressed, Versioned, P2P File System, `https://arxiv.org/abs/1407.3561` (2014).

[*1] `https://docs.libp2p.io/concepts/introduction/overview/`

[*2] `https://github.com/libp2p/rust-libp2p`