匿名通信システム Tor における悪用ユーザ特定手法の検討

川端　良樹 a)・宗　裕文 b)・横山　絵美里 b)・岡崎　直宣 c)

An Examination on the Abusing User Identification Method of the Tor Anonymity System

Yoshiki KAWABATA, Hirofumi SOU, Emiri YOKOYAMA, Naonobu OKAZAKI

Abstract

The Onion Routing (Tor) is the most famous anonymity system supporting the anonymous transport of TCP stream over the Internet. Tor provides the foundation for applications to communicate over public network without compromising their privacy. However, in some cases, it is used by abusing users, for the antisocial purpose. This has prevented the increase of "good" user of the Tor system. In this article, we propose a method for identification of the abusing user of the Tor anonymity system. In the proposed method, Tor system cooperate with Web sites that simulate sites dealing with illegal information, and uses the fingerprint information of the Web sites to identify the users accessing the sites.

Keywords: Anonymous Comunication, Abuse Suppression, The Onion Routing

1. はじめに

現在、インターネットは私たちの生活に欠かせないものになっている。しかしながら、インターネットを利用する上で、パケットのヘッダ情報を盗聴し利用者がアクセスした Web サイトが特定されてしまうことが問題になっている。この対策として匿名通信システムが注目されている。匿名通信システムには Mix-Net や Crowds などあるがその中で最も普及しているのが The Onion Routing(Tor)[1]である。Tor は健康相談や電子投票等の、誰がどこに送信したか、ということを知られたくない場合の情報交換に利用されることを本来の目的としている。しかし、Tor は違法行為を匿名で行う目的で悪用ユーザに利用されるケースがある。このことが、多くの善良なユーザが本来の目的で Tor を利用することを妨げることにつながっていると考えられる。

本稿では、おとりとなる Web サイトを導入し、その Web サイトと協調動作をすることで、悪用ユーザを特定する手法を提案する。そして、実験により、従来の不特定のサイトの指紋情報を用いる手法と比較し、提案手法の効果を検証する。

a)情報システム工学専攻大学院生
b)情報システム工学科学部生
c)情報システム工学科教授

2. The Onion Router(Tor)

2.1 概要

Tor とは、元々アメリカ海軍調査研究所（USNRL）により開発された、低遅延の匿名化通信技術である。Tor の一日あたりの利用者数は、2012 年 8 月から 2013 年 8 月の間およそ 50 万人程度で推移しており、現在最も利用されている匿名化技術である。Tor は複数のプロキシを経由させるオニオンルーティングと呼ばれる仮想回線接続により匿名性をもつ通信を実現している。

ここで Tor の仕組みを図 1 に示す。Tor は図 1 のように Tor ネットワークから無作為に選ばれた三つのプロキシ（以下、OR）を経由し Web サイトへアクセスする多段プロキシ・システムである。Tor では、経由する OR は常に切り替えられ、経由した OR を特定することは難しい。また OR 間の通信は暗号化されているため、盗聴を防ぎ安全な通信を可能としている。

2.2 Tor のユーザ

現在 Tor は軍、ジャーナリスト、警察官、人権活動家などの人々によって様々な目的のために利用されている。例えば、ジャーナリストは、より安全に不正の告発者や反体制派の人らと接触する為に Tor を利用している。

ところが、上記の本来の用途以外に、海外では Tor が違法薬物の取引サイトへのアクセスに使われたり、また日本国内においては、殺人予告、パソコンの遠隔操作に Tor が利用されたりしている。本稿ではこれらの違法行為を匿名

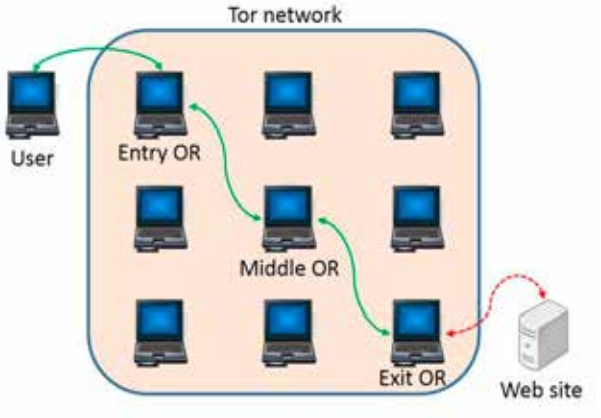

図 1. Tor の仕組み.

で行う目的のユーザを「悪用ユーザ」、それ以外を「正規ユーザ」と呼ぶこととする。米国家安全保障局（以下、NSA）、並びに日本の警察庁は悪用ユーザに対して様々な対策をしている。例えば日本の警察庁は、Tor からのアクセスをブロックするようにサイト管理者に協力を求めている[6]。最近では、上記のように Tor が悪用されているというようなニュースが度々放送されるようになり、一般の人々は Tor に対して良い印象を持っておらず、中には Tor というものは悪いことをする為に使用するものだと思い込んでいる人もいるかもしれない。このままでは Tor の正規ユーザが減り、匿名通信技術自体も衰退していく恐れがある。

そこで、本論文では悪用ユーザの利用を抑制することを目的に悪用ユーザを特定する手法を提案する。これにより Tor に対する印象が改善し、Tor の正規ユーザが増加することが期待できる。本研究では、Tor の匿名性を下げる目的である利用者特定手法を参考に提案手法を考える。次章では Tor における利用者特定手法について説明する。

3. 利用者特定手法

本章では既存の利用者特定手法を紹介する。ここで紹介する手法は元々は Tor の匿名性を低下させようとする者（以下、攻撃者）によって行われる手法であるが、適用方法によっては本研究の目的にも利用できると考えられる。本論文では攻撃者により占拠された OR を汚染 OR と呼ぶこととする。

（1） Web サイトの指紋情報を利用した手法

Web サイトにアクセスした際のトラフィックに含まれるサイト独自の特徴（以下、指紋）に着目しそれを観測することで利用者がアクセスした Web サイトを特定するという手法である。[2]は 54%の確率で利用者がアクセスした Web サイトを特定できることが示されている。Web サイトの指紋情報を利用した手法は汚染入口 OR だけ用意すればよく、実現可能性が高い。しかし、利用者がアクセスした Web サイトを特定する確率が高くない。

（2） 特徴的なトラフィックを利用した手法

汚染入口 OR と汚染出口 OR を用意し汚染出口 OR が特徴的なトラフィックを利用者へ送信し、そのトラフィックを汚染入口 OR が観測することで利用者を特定する手法である。[3]は 65%から 100%の確率で利用者がアクセスした Web サイトを特定できることが示されている。特徴的なトラフィックを利用した手法は利用者がアクセスした Web サイトを特定する確率は高いが汚染 OR を二つ用意しなければならず実現可能性が低い。

既存手法では、OCR 機能を持つボットに対する耐性の低さとユーザビリティの低さが問題であった。

従って提案手法では、画像 CAPTCHA におけるデータベース攻撃に対する耐性と総当たり攻撃に対する耐性に重点をおき、既存の文字列 CAPTCHA と比べて、OCR 機能を持つボットに対する耐性をもち、ユーザビリティに配慮した CAPTCHA を作成することを目的とする。

4. 提案手法

4.1 概要

本提案手法では悪用ユーザがアクセスしそうなおとりとなるWebサイト（以下、おとりWebサイト）を導入し、そのサイトと入口ORが協調動作し、特徴的なトラフィックを悪用ユーザに送信する。このことにより、特徴的なトラフィックを利用した手法の実現可能性が低いというデメリットを解決し、実現可能性が高く、高い確率でおとりWebサイトにアクセスした悪用ユーザを特定することを目指す。

4.2 前提条件

入口ORはWebサイトの指紋情報を利用した手法における汚染ORと同様の役割を持ち、情報を抽出できるものとする。また、おとりWebサイトは公開鍵暗号基盤で認証されておらず、悪用ユーザを対象としている。故に、おとりWebサイトへ正規ユーザはアクセスしないものとする。

4.3 提案手法の流れ

以下で図2を用いて本提案手法の流れを説明する。ここで管理者ORとは悪用ユーザを抑制したい立場のTorの管理者が入口ORに位置したORである。

（1） おとりWebサイトは悪用ユーザからアクセス要求がきたことを確認する。

（2） おとりWebサイトはパケットキャプチャを開始する。

（3） 管理者ORにパケットキャプチャを開始するように指示する。

（4） 管理者ORはパケットキャプチャを開始する。

（5） 悪用ユーザへ応答を返す。

（6） おとりWebサイト側のキャプチャデータと管理者OR側のキャプチャデータを比較して悪用ユーザを特定する。

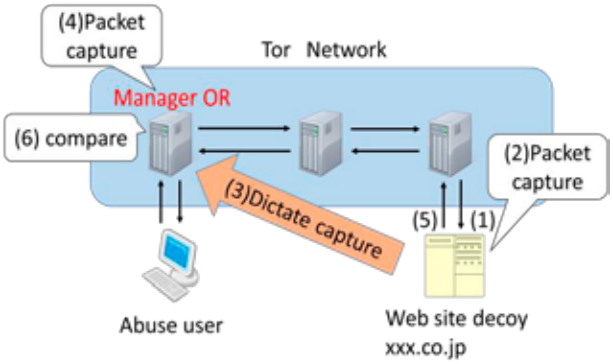

図 2. 提案手法の概略図.

4.4 動作手順

提案手法の動作手順はおとりWebサイトを作成するおとりWebサイト作成フェーズ、図2の(3)、(4)の処理に当たる協調動作フェーズ、図2の(6)の処理に当たる悪用ユーザ決定フェーズの三つに分けられる。

以下でそれぞれのフェーズについて詳しく説明する。

I. おとりWebサイト作成フェーズ

おとりWebサイトには現実のWebサイトと区別をつけるために特定の信号を含ませる。管理者ORでこの信号を受け取ることで悪用ユーザが対応するおとりWebサイトを利用したことを判断する。ここで、信号は本来のHTML及び依存コンテンツを送信した後に、特定の間隔で遅延させたダミーコンテンツを複数回付加して送信することで実現する（図3）。付加するダミーコンテンツの量とその遅延時間については以下のように定める。

まず、ダミーコンテンツの数Numとそれぞれのサイズ$Size_i$を定義する。次に、それぞれのダミーコンテンツを送信する待ち時間$Time_i$（秒）を設定する。そして、おとりWebサイト本来のコンテンツを送信した後、それぞれのダミーコンテンツを$Time_i$だけ待って送信する。図3はNum=3、$Size_1$=$Size_2$=$Size_3$=300(KB)、$Time_1$=30、$Time_2$=40。$Time_3$=50と設定した場合の信号である。

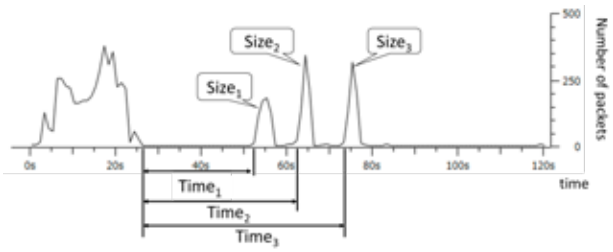

図 3. おとり Web サイトの通信トラフィック.

II. 協調動作フェーズ

協調動作フェーズでは4。3の『提案手法の流れ』における(1)から(3)までの動作を行う。

III. 悪用ユーザ決定フェーズ

協調動作フェーズで収集した悪用ユーザと管理者OR間のキャプチャデータと出口ORとおとりWebサイト間のキャプチャデータからグラフを作成する。そして、このふたつのグラフを比較し類似していれば悪用ユーザはおとりWebサイトへアクセスしたのが分る。この二つのグラフを比較する指標として相関係数を用いる。相関係数とは二つのデータ間の類似性の度合いを示す指標である。相関係数が1に近いほど正の相関があり、ゼロに近ければ無相関であり、-1に近ければ負の相関がある。相関係数rの算出方法を数式(1)に示す。ここで、$f_1(t)$、$f_2(t)$はそれぞれ管理者OR側で収集したデータを用いて作成したグラフ、おとりWebサイト側で収集したデータを用いて作成したグラフを表している。そして、$f_1(t)$、$f_2(t)$の平均値をそれぞれavg_1、avg_2と表す。また、Nは観測したデータのサンプリング数である。相関係数rについて表2のように判定基準を定める[7]。

$$r = \frac{\frac{1}{N}\sum_{t=1}^{N}(f_1(t)-avg_1)(f_2(t)-avg_2)}{\sqrt{\frac{1}{N}\sum_{t=1}^{N}(f_1(t)-avg_1)^2}\sqrt{\frac{1}{N}\sum_{t=1}^{N}(f_2(t)-avg_2)^2}} \quad (1)$$

表 1. 相関係数の基準.

$\|0.7\| < r \leqq \|1\|$	かなり強い相関がある
$\|0.4\| < r \leqq \|0.7\|$	やや相関あり
$\|0.2\| < r \leqq \|0.4\|$	弱い相関あり
$\|0\| < r \leqq \|0.2\|$	ほとんど相関なし

5. 評価実験

本章では、利用者特定手法の中でも幅広く研究がされている Web サイトの指紋情報を利用した手法と提案手法の有効性を示すために評価実験を行う。

5.1 評価指標と評価対象

本論文ではWebサイトにアクセスした悪用ユーザを特定することが目的であるため、全体特定率とWebサイト特定率で評価を行う。本実験では全体特定率をEsr、Webサイト特定率をWsrとし、それぞれの算出方法を数式(2)に示す。ここで、$Success_i$、WebSite、Accessはそれぞれ、各Webサイトの特定成功数、アクセスするWebサイトの数、アクセス回数である。

$$Esr = \frac{\sum_{i=1}^{WebSite} Success_i}{WebSite \cdot Access}, \quad Wsr = \frac{Success_i}{Access} \quad (2)$$

これらの特定率が高いほどユーザがどこにアクセスしたのか容易に分かることを示す。それぞれの特定率を求め、それらの値で評価する。

本実験では、以下の二つの手法を評価対象とする。

- Webサイトの指紋情報を利用した手法
- 提案手法

ここで、想定するWebサイトの指紋情報を利用した手法について述べる。この手法では、Torネットワークの攻撃者の入口OR（以下、攻撃者OR）を用いて利用者宛てに流れるトラフィックを収集できることを前提としている。また、あらかじめ攻撃者が事前に指紋情報のデータベース（以下、攻撃者データベース）を作成し、その攻撃者データベースを定期的に更新していくものとする。そして、利用者がアクセスした際に攻撃者ORで収集される指紋情報を攻撃者データベースで比較し指紋情報が最も近いものを利用者がアクセスしたWebサイトとする。

指紋情報は通信トラフィック総量、通信パケット数、通信トラフィック平均、通信トラフィック分散、通信チャンク平均、通信チャンク分散とする。ここで通信チャンクとは、パケットの向きが変わる度に、前回向きが変わった点から向きが変わる直前までのパケットを足し合わせたパケットのまとまりのことである。

5.2 実験環境

実験に用いるWebサイトは、Webサイトのアクセスランキング付けを行っているAlexa[4]の上位から国ドメインだけが違うだけで同じサイトなどの重複をさけて100サイト選択した。また、著作権上の問題を回避するため現実のサイトを用いることができない。そこで、現実のサイトのHTML及びその他コンテンツサイズ、コンテンツ数を元にダミーデータからなるWebサイトを作成した。また、パケットキャプチャにはwireshark[5]を用いた。

5.3 実験方法

本実験では各比較対象の全体特定率及びWebサイト特定率で比較する。提案手法では動画、検索、ショッピング、企業HP、ニュースサイトの5種類から選択しておとりWebサイトを作成する。Webサイトの指紋情報を利用した手法と比較するために、Webサイトの指紋情報を利用した手法においても上記の5種類のWebサイトを選択する。

（1） Webサイトの指紋情報を利用した手法

指定したURLをブラウザに入力すると、Torプロキシ経由で接続される。この時の通信トラフィックを利用者側でパケットキャプチャすることで指紋情報とする。本実験では*WebSite=100*、*Access=10*とし1000データで攻撃者データベースを作成する。また、同様に利用者の指紋情報を1000データ用意する。この利用者の指紋情報にそれぞれ最も類似した指紋情報を攻撃者データベースから求める。そして、対応するWebサイトが本当に利用者のアクセスしたWebサイトかどうか判断する。これを1000データ全てで行い、全体特定率及びWebサイト特定率を求める。本実験では、簡単化のため利用者がWebサイトにアクセスする際に閲覧するページはトップページのみとする。閲覧時間についてはTorを利用してWebサイトを閲覧する際、接続に時間がかかることや経路によって帯域が異なることを考慮した時間を設定する。上記の理由から本実験では閲覧時間を2分間に設定する。

（2） 提案手法

(1)と同様に、指定したURLをブラウザに入力すると、Torプロキシ経由で接続される。この時の通信トラフィックを利用者の入出力に加え、Webサイトの入出力でもパケットキャプチャを行う。本実験では、各ダミーコンテンツサイズが300KBである5つのおとりWebサイトを作成した。各おとりWebサイトにおけるダミーコンテンツ毎の遅延を表2に示す。そして、5つのおとりWebサイト及び95サイトのそれぞれに10回ずつアクセスした1000個のパケットキャプチャデータを用いる。そして、提案手法では全てのおとりWebサイトのキャプチャデータから相関係数r求め、*r*が0。7以上のWebサイトが対応するおとりWebサイトかどうか判断する。そして、全体特定率及びWebサイト特定率を求める。相関係数の算出にはR言語のcor関数[7]を用いた。

表 2. 各おとり Web サイトの遅延(sec).

おとりWebサイト	T1	T2	T3
A（動画）	30	40	50
B（検索）	20	30	40
C（ショッピング）	10	20	30
D（企業HP）	30	40	50
E（ニュース）	20	30	40

5.4 実験結果

表3は提案手法とWebサイトの指紋情報を利用した手法の全体特定率を表している。また、図4のProposal methodは提案手法の各おとりWebサイトごとのWebサイト特定率を表している。また、Exsisting methodはWebサイトの指紋情報を利用した手法の結果から各おとりWebサイトと同じ種類のWebサイトをそれぞれ一つずつ選択したときのWebサイト特定率を表している。図4のA、B、C、D、Eはそれぞれ動画、検索、ショッピング、企業HP、ニュースサイトの5種類から選択したWebサイトである。

6. 考察

表3よりWebサイトの指紋情報を利用した手法では52%、提案手法では100%の全体特定率を示した。このことから、提案手法は非常に高い全体特定率を持ち、本研究の目的である悪用ユーザの特定に有効であることが分かる。

図4において、どの種類のWebサイト特定率をみてもWebサイトの指紋情報を利用した手法より提案手法の方

表 3. Web サイトの指紋情報を利用した手法と提案手法の全体特定率.

手法	全体特定率
Webサイトの指紋情報を利用した手法	52%
提案手法	100%

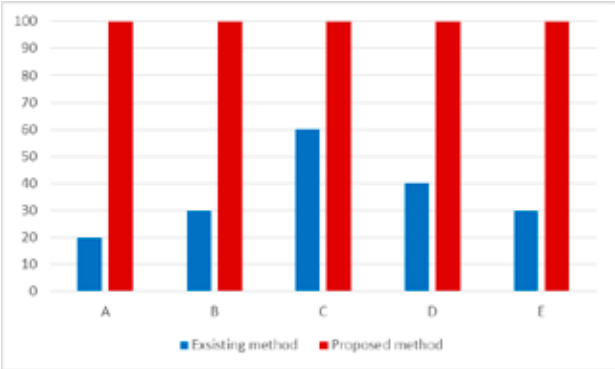

図 2. Web サイトごとの特定率.

が高いことが分かる。ここで、図4のWebサイトの指紋情報を利用した手法ではAの動画サイトが最も低い特定率となっており、Cのショッピングサイトは最も高い特定率を示している。これは、Webサイトの指紋情報を利用した手法では、Aの動画サイトは更新頻度が高いため指紋情報が頻繁に変化し特定率が低く、Cのショッピングサイトは指紋情報となりうるコンテンツが多いため特定率が高いと考えられる。一方、図4の提案手法ではAの動画サイト、Cのショッピングサイトなど種類に依らず高いWebサイト特定率を示している。これは、提案手法では、Webサイトのコンテンツに依らない信号をトラフィックに含め、それによりWebサイトを特定しているためである。このような結果から、Webサイトの指紋情報を利用した手法はWebサイトのコンテンツによって特定率にバラつきが生じるが、提案手法はどのようなWebサイトであっても常に高い特定率を示せることがわかる。

Webサイトの指紋情報を利用した手法は、常に高い特定率を維持することが難しいがどのようなWebサイトにも適用できる。一方、提案手法は悪用ユーザがおとりWebサイトを利用しなければ悪用ユーザを特定できないが、利用した場合は高い確率で特定できる。このように、Webサイトの指紋情報を利用した手法と提案手法はお互いのデメリットを補完するものであるといえる。今後は、提案手法とWebサイトの指紋情報を利用した手法を組み合わせて利用することで、常に高い特定率を維持しつつ、悪用ユーザが特定システムから逃れられないようなシステムを提案していきたい。

7. まとめ

本論文では匿名通信システムTorにおける悪用ユーザ特定手法の提案を行った。本提案手法は、入口ORと、おとりとなるWebサイトが協調動作して悪用ユーザを特定するものである。また、利用者特定技術の中でも幅広く研究されているWebサイトの指紋情報を利用した手法と提案手法の比較評価を行った。その結果、Webサイトの指紋情報を利用した手法はWebサイトのコンテンツによってWebサイト特定率にバラつきが生じるが、提案手法はどのようなWebサイトであっても常に高いWebサイト特定率を示せることが分かった。今後は提案手法とWebサイトの指紋情報を利用した手法を組み合わせ適用範囲を広げる方法についても検討したい。

参考文献

1) R. Dingledine, N. Mathewson, and P. Syverson: Tor: The Second-Generation Onion Router, In In Proceedings of the 13th USENIX Security Symposium, 2004.
2) A. Panchenko, L. Niessen, and A. Zinnen: Website Fingerprinting in Onion Routing Based Anonymization Networks, Proceedings of the 10th annual ACM workshop on Privacy in the electronic society pp.103-114, 2011.
3) Z. Ling, J. Luo, W. Yu, X. Fu, D. Xuan, and W. Jia: A New Cell-Counting-Based Attack Against Tor, Networking,IEEE/ACM Transactions on, Vol.20, Issue.4, pp.1245-1261, 2012.
4) Alexa: Alexa Top 500 Global Site http://www.alexa.com/topsites.
5) Wireshark: Wireshark http://www.wireshark.org.
6) WIRED： 日本の警察庁、匿名化ツール「Tor」のブロックをサイト管理者に促す http://wired.jp/2013/04/22/japan-police-stop-using-tor/
7) 山田 剛史, 杉澤 武俊: 村井 潤一郎: R によるやさしい統計学, pp.62-64, オーム社, 2008.