

Winny ネットワークに対するインデックスポイズニングを用いたファイル流通制御方式

吉田 雅裕^{†1} 大坐 昌 智^{†2}
中尾 彰 宏^{†3} 川島 幸之助^{†1}

P2P ファイル共有ネットワークは世界中で非常に多くのユーザに利用されている。しかし、現在広く普及している P2P ファイル共有ネットワークには、ファイル流通制御機能が実装されていない場合が多く、著作権侵害ファイルやマルウェアなどの流通が問題となっている。これらの問題を解決するために、インデックスポイズニングを用いたファイル流通制御手法が注目されているが、その効果やネットワークへの影響はこれまでにあまり明らかにされていない。そこで本論文では、10 万台以上のアクティブなピアによって構成される実際の Winny ネットワークに対して、ファイル流通制御のためにインデックスポイズニングを適用し評価を行った。提案手法では、Winny ネットワークの本質であるファイル流通技術としての側面を否定することなく、なおかつ、著作権侵害ファイルの流通などの反社会的な利用のみを技術的に制限することを目標とする。キーと呼ばれる、ファイルのメタデータを利用する Winny のファイル流通プロトコルに着目し、ファイルのダウンロードに必要な特定のキーを、インデックスポイズニングを用いてネットワーク上から消去することによりファイル流通制御を実現した。評価実験の結果、提案手法を Winny ネットワークに適用した場合は、Winny ピアが特定のファイルのキーを入手できる確率が、適用しない場合の 0.005%まで低下することを確認した。また、提案手法を用いた制御は、1,000 個のファイルを同時に制御した場合であっても Winny ネットワークへの負荷が少ないことを示した。

An Index Poisoning Method for Controlling File Distribution in Winny Network

MASAHIRO YOSHIDA,^{†1} SATOSHI OHZAHATA,^{†2}
AKIHIRO NAKAO^{†3} and KONOSUKE KAWASHIMA^{†1}

Peer-to-Peer (P2P) file sharing networks have been widely used by millions of users all over the world. However, these networks do not have management

mechanisms for distributing files in general. Consequently, copyright infringements in P2P file sharing networks have become prevalent. In order to prevent illegal file distribution, an index poisoning has attracted much attention recently. Although index poisoning aims to obfuscate uses by diffusing a lot of dummy metadata in P2P networks, its effects have not been well studied yet. In this paper, we apply an index poisoning method to Winny network, one of the most popular P2P file sharing networks in Japan, to control the file distribution. Our evaluation includes index poisoning in live Winny network composed of over 100,000 active peers. In our method, the file distribution technology of the Winny network is not denied. Moreover, our method solves only antisocial behavior, such as a copyright infringement problem. The result shows that our proposed method can decrease the number of query hits to less than 0.005% compared to the case without our control. The result also shows that our proposed method does not exert a bad influence on Winny network, even when 1,000 files are under our control simultaneously.

1. はじめに

P2P ネットワークにより構成されるファイル共有サービスは、今日のインターネット環境を代表するサービスの 1 つとなっている。たとえば、Gnutella, BitTorrent, FastTrack, Overnet などは、世界中で 1 日あたり数百万人規模のユーザに利用されている^{1)–4)}。日本国内においても同様に、Winny, Share などのファイル共有ネットワークを数十万人のユーザが利用している⁵⁾。また、これらのネットワークによって生み出される P2P トラフィックは、今日のインターネットトラフィックの大きな部分を占めている^{6)–8)}。しかし、これまでの P2P ファイル共有ネットワークは、ファイル検索・転送の効率化や、スケーラビリティの向上に重点が置かれて設計されており、ファイル流通制御機能が実装されていない場合が多い。そのため、P2P ファイル共有ネットワークのユーザによる、著作権侵害ファイルの流通や個人情報ファイルの流出などが社会問題となっている⁹⁾。P2P ネットワークのファイル共有技術は、著作権侵害ファイルの流通などから反社会的にとらえられる場合があるが、通信技術として優れた点は多い。そのため、P2P ファイル共有ネットワークの反社会的な

†1 東京農工大学
Tokyo University of Agriculture and Technology

†2 電気通信大学
The University of Electro-Communications

†3 情報通信研究機構/東京大学
NICT/The University of Tokyo

利用を技術的に制限し、社会的な利用を目指した基盤技術として整備していく必要がある。このような背景を受け、近年ではポリューション^{10),11)} やインデックスポイズニング^{12)–14)} と呼ばれる手法を用いることにより、ファイル流通制御機能を持たない P2P ファイル共有ネットワークに対する、ファイル流通制御が試みられている。

ポリューションとは、大量の偽ファイルを P2P ファイル共有ネットワークに拡散することによって、本物のファイルを入手できる確率を下げる手法である¹⁰⁾。偽ファイルは、ファイル名やファイルサイズが本物のファイルとほぼ同じであるが、ファイルのデータは本物のファイルと異なっている。ユーザはダウンロードが完了するまでの間は、ダウンロード中のファイルのデータを確認することができないため、本物のファイルを入手するまでに大量の偽ファイルを入手することになる。しかしながら、ポリューションを用いた制御は大量の偽ファイルがネットワーク上を流通することになるため、結果として P2P トラフィックが増加してしまうという問題点がある¹¹⁾。

一方、インデックスポイズニングでは、偽ファイルの代わりに偽ファイルのメタデータをネットワークに拡散する¹²⁾。ファイルのメタデータには、そのファイルのファイル名やファイルサイズ、ファイルの位置情報 (IP アドレスとポート番号) などが記載され、ファイルをダウンロードする際にその位置を特定するためのポインタとして機能している。インデックスポイズニングで拡散する偽ファイルのメタデータは、本物のファイルとほぼ同じファイル名やファイルサイズが記載されているが、ファイルの位置情報が偽装してあるため、ポインタとしての機能が正常に働かない。そのため、本物のファイルの所持者を特定できなくなる。メタデータのサイズはファイル本体と比べて非常に小さいため、インデックスポイズニングでは制御にあまり多くのトラフィックを必要としない。また、ネットワーク上を実際のファイルが流通するわけではないため、ポリューションのように P2P トラフィックの増加が問題になることもない。以上の理由から、近年ではインデックスポイズニングを用いたファイル流通制御手法が注目され、実際の P2P ファイル共有ネットワークに適用されてきている¹³⁾。しかし、インデックスポイズニングを用いたファイル流通制御が、制御対象ファイル以外のファイルの流通にも悪影響を及ぼした例が報告されている¹⁴⁾。このように、インデックスポイズニングを P2P ファイル共有ネットワークに適用する場合は、ファイル流通制御の効果だけでなく、制御が P2P ファイル共有ネットワークへ及ぼす影響を十分に考慮しなければならない。しかしながら、インデックスポイズニングを用いたファイル流通制御において、その効果を維持しつつも、P2P ファイル共有ネットワークへの影響を最小限に抑えた手法の提案はこれまでにほとんど行われていない。

そこで本論文では、日本国内で非常に人気の高い P2P ファイル共有ネットワークである Winny¹⁵⁾ を対象に、インデックスポイズニングを用いたファイル流通制御手法を提案し、実ネットワークにおける評価実験によりその効果を評価する。提案手法では Winny のキー (メタデータ) 上書きルールを利用して、特定のファイルの流通を正確に制御することができ、なおかつ、Winny ネットワークへの影響が少ないファイル流通制御手法を提案する。また、評価実験のために、制御用システムと 2 つの測定用システムを実装し、それらを用いることで提案手法の効果と、制御が Winny ネットワークへ及ぼす影響を明らかにする。

本論文は以下のように構成される。2 章では Winny のファイル流通プロトコルの概要を述べ、3 章で本提案手法について述べる。続いて、4 章で実装したシステムの概要について述べる。次に 5 章で評価環境と評価結果を示す。6 章では、本提案手法の実運用に向けた課題や、他の P2P ファイル共有ネットワークに対する本提案手法の適用について考察する。最後に 7 章でまとめと今後の課題について述べる。

2. Winny のファイル流通プロトコル

Winny は非構造化 P2P ファイル共有ネットワークに該当し、ファイル検索やファイル転送において、中央サーバやスーパーピアなどを必要としない。Winny のファイル流通プロトコルの概要を以下に示す (図 1)。

- (1) ファイル保持ピアが中心となり、隣接ピアに向けて保持ファイルのメタデータが拡散する。Winny では、ファイルのメタデータのことをキーと呼ぶ。キーには保持ファイルのファイル名、ファイルサイズ、ファイル ID (ファイルのデータから求めた MD5 ハッシュ値)、ファイル位置情報 (IP アドレスとポート番号)、キーのネットワーク上での寿命などが記載されている。Winny には、すべての流通ファイルのインデックスを管理するためのサーバが存在せず、代わりに、ネットワークに参加する各ピアがキーをインデックスとして保持することで、流通ファイルの情報を管理している。インデックスは、Winny ネットワークにおける流通ファイルのポインタとして定義され、ユーザがファイルをダウンロードする際に、ファイルの位置を特定するために利用される。各ピアのインデックスは、隣接ピア間で定期的にキーをランダムに交換することによって更新され、キーの寿命が尽きるまでの間保持される。
- (2) Winny ネットワークにおけるファイル検索とは、特定ファイルのキーを検索することと等しい。ファイル検索ピアは検索クエリを用いて、目的とするファイルのキーを入手する。ネットワーク負荷を軽減するために、検索クエリは 1 方向にのみユニキャストで転

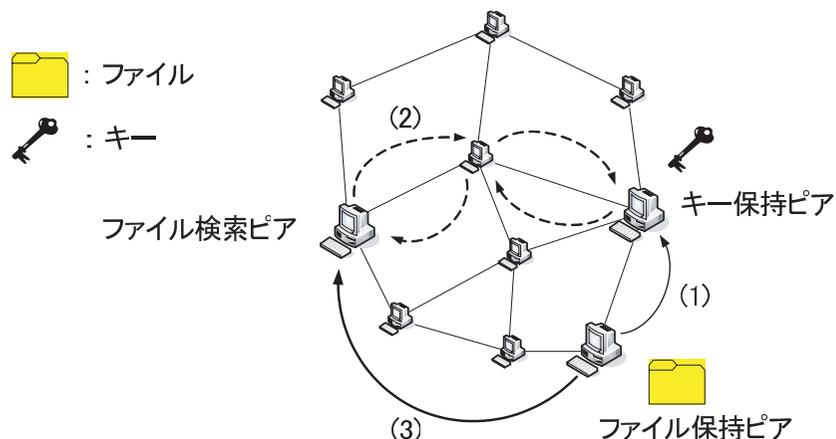


図 1 Winny のファイル流通プロトコル
Fig. 1 File distribution protocol in Winny.

送され、1つの検索クエリは最大で6ホップ先まで転送される。各ピアは同時に7台までのピアと検索リンクを接続しており、そのうち2台は自分よりも回線速度が速いピアであり、残りは同じ回線速度か、自分よりも遅いピアである。検索クエリは、より速い回線速度のピアに向けて転送される。検索クエリにキーがクエリヒットした場合は、検索クエリが転送される過程でクエリの経路上にキーが複製される。

- (3) ファイル検索ピアが目的とするファイルのキーを入手した場合、そのキーにはファイル保持ピアの位置が記載されている。その後、記載されている情報をもとにファイル保持ピアに対してファイルの転送を要求する。

3. Winny ネットワークに対するインデックスポイズニングの適用

インデックスポイズニングを用いたファイル流通制御を行うために、キーに記載される各情報を制御用に調節したダミーキーを、Winny ネットワークに拡散する。Winny ピアはダミーキーの情報をもとにダウンロードを試行しても、目的とするファイルを入手することはできない。

3.1 Winny ネットワークにインデックスポイズニングを適用する際の課題

本論文で提案するファイル流通制御手法は、特定のファイルの流通を制御するだけでなく、Winny ネットワークを不正な目的で利用していないユーザーに対して、Winny ネット

ワークが本来持つ機能を制限しないことを目的とする。これは提案手法が、Winny ネットワークの本質であるファイル共有技術としての側面を否定することなく、なおかつ、著作権侵害ファイルの流通などの反社会的な利用のみを技術的に制限するためである。そこで、Winny ネットワークにインデックスポイズニングを適用する際に、提案手法が解決しなければならない課題を以下に述べる。

- 課題 1: 制御対象ファイル以外のファイルに対する誤った制御

インデックスポイズニングの最も単純な適用方法として、制御対象ファイルと同じファイル名とファイルサイズを持つダミーキーを、ネットワークに大量に拡散する手法がある¹²⁾。この適用方法は、ファイル検索ピアがファイル名をキーワードとして検索クエリを発行する場合に効果的である。なぜならば、検索クエリのキーワードがダミーキーに記載されたファイル名の一部と一致することでクエリヒットが起こり、この結果として大量のダミーキーを入手するからである。しかし、この適用方法は制御対象ファイルでないファイルの検索にも影響を及ぼす場合がある。たとえば、ファイル名に「単語1 単語2」の2つを持つ違法ファイルと「単語2 単語3」の2つを持つ違法でないファイルが流通している場合がある。違法ファイルのみの流通を制御することを目的に、「単語1 単語2」をファイル名として記載したダミーキーを用いて制御した場合に、違法でないファイルを「単語2」をキーワードに検索した際に、その検索クエリに大量のダミーキーがヒットしてしまう。このようなインデックスポイズニングの適用方法では、違法でないファイルの検索結果に大量のダミーキーの情報が表示されるなどの影響を及ぼす可能性があるため、提案手法は、制御対象ファイル以外のファイルには制御の影響を与えないことが必要である。

- 課題 2: ファイル ID を用いたファイル検索への対応

Winny をはじめ、現在普及しているほとんどの P2P ファイル共有ネットワークでは、ネットワーク上でユニークなファイル ID を用いたファイル検索が可能となっている。Winny におけるファイル ID には、ファイルのデータから求める MD5 ハッシュ値が使用されており、データが少しでも異なるファイルから生成されるファイル ID は、それぞれ異なるようになっている。そのため、本物のファイルとファイル名やファイルサイズを似せた偽ファイルを拡散することで制御を行うポリューションや、ファイル名やファイルサイズなどは本物のキーと同じであるが、ファイル ID は異なるダミーキーを拡散することで制御を行うインデックスポイズニングは、ファイル ID 検索を行うユーザーに対しては効果がなくなってしまう。特に近年では、P2P ファイル共有ネットワーク上に大量の偽ファイル

が流通するようになったため、掲示板や SNS (Social Networking Service) などにおいて本物のファイルのファイル ID が公開され、ファイル ID 検索に利用されるようになっている。そのため提案手法は、制御対象ファイルのファイル ID が公開された場合でも制御が可能でなければならない。

● 課題 3 : ダミーキーによるインデックスの汚染

ファイル流通制御のために、Winny ネットワーク上に拡散したダミーキーがネットワーク上に長時間残る場合には、Winny ネットワークのインデックスをダミーキーが汚染する可能性がある。ここで述べたインデックスの汚染とは、P2P ファイル共有ネットワークのインデックスの大部分を制御用のダミーキーが占めることにより、制御対象でないファイルの流通が阻害されることを指す。特に Winny ネットワークにおいては、各ピア 1 台あたりがインデックスとして保持できるキーの数には限りがある (最大 35,000 個)。大量のダミーキーが長時間 Winny ネットワークに残っていると、他のファイルの流通に使用可能なインデックスの領域がダミーキーによって圧迫されるため、他のファイルの流通を長時間阻害してしまう可能性がある¹⁶⁾。Winny プロトコルはインデックスが汚染されていないことを前提に設計されているため、ダミーキーにより汚染された Winny ネットワークでは、制御対象でないファイルの検索効率などが低下してしまう。

● 課題 4 : DDoS 攻撃の誘発

Winny プロトコルにはキーの認証機構が存在しないため、ファイル検索ピアがキーを入手した場合に、そのキーがダミーキーなのか本物のキーなのかを確認することができない。ダミーキーを入手したファイル検索ピアは、ダミーキーに記載されたファイル位置のピアに対してファイル転送を要求することになる。非常に人気のあるファイルを制御している場合は、ダミーキーに記載されたファイル位置のピアに対して多数のピアからのファイル転送要求が来るため、そのピアの通信回線や PC に大きな負荷がかかってしまう。近年、このようなインデックスポイズニングが DDoS (Distributed Denial of Service) 攻撃を引き起こすという危険性が、複数の P2P ファイル共有ネットワークにおいて指摘されている¹⁷⁾⁻²⁰⁾。

3.2 提案手法

そこで本論文では、Winny ネットワークに対してインデックスポイズニングを適用する際に、3.1 節の課題を解決した適用方法を提案する。

3.2.1 提案手法の概要

提案手法では、制御対象ファイルの流通に必要な本物のキーを、Winny ネットワーク上

から完全に「消去」する。本物のキーが Winny ネットワーク上から完全に消去された場合は、ファイル検索ピアが発行する検索クエリに本物のキーがまったくクエリヒットしなくなる。また、提案手法で拡散するダミーキーが、Winny ネットワークに与える影響を最小限にとどめるために、制御に用いたダミーキーを Winny ネットワーク上からすぐに消去する。一方、従来手法は、ネットワーク上に大量のダミーキーを拡散させ、ファイル検索ピアにダミーキーばかりをクエリヒットさせ、本物のキーをほとんどクエリヒットさせないことで制御している。従来手法は制御中に、本物のキーとダミーキーが両方ともネットワーク上に残り続けるが、提案手法では制御中に、本物のキーとダミーキーが両方ともネットワーク上に残らないという点で異なる。

3.2.2 提案手法で利用した Winny プロトコルの特性

提案手法では Winny プロトコルの以下の 3 つの特性を利用し、ファイル流通制御を実現する。

(1) キーに記載された情報を検証しない：

Winny ネットワークでは、ネットワークに参加する Winny ピアから得られるキーに記載された情報は、すべて正しい情報であるという前提が成り立っている。そのため、Winny ピアがキーを受け取った場合に、キーに記載された情報の整合性が合えば (ファイル名の長さが表現可能範囲を超えていない、ファイルサイズが 2 GB を超えていない、など)、無条件でそのキーをファイルのインデックスとして追加するようになっている。このように Winny プロトコルでは、キーを受け取ったピアがそのキーに記載された情報を中央サーバに問い合わせるなどの方法で検証しない。そのため、ダミーキーに記載する情報を制御のために自由に調節することができ、ファイル流通制御に利用することができる。

(2) 同じファイル ID を持つキーの上書き：

Winny ネットワークではデータがまったく同じファイルを、複数のピアが同時に保持していることがある。その場合は、ファイル ID は同じであるがファイル位置情報が異なる複数のキーが、Winny ネットワーク上に拡散することになる。しかし、1 つのキーには、ファイル位置情報として 1 台のピアのアドレスのみが記載できる。そのため、あるピアがすでにキーをインデックスとして保持している場合に、そのキーと同じファイル ID のキーを再度受け取った場合は、新しく受け取ったキーによって以前のキーが上書きされるという特徴がある (キー上書きルール)。同じファイル ID を持つキーは追加でなく上書きされるという、この特徴的な Winny のキー上書きルールを提案手法で利用することで、本物のキーを制御用のダミーキーで上書きする。

(3) キーの寿命が設定可能:

キーには、Winny ネットワーク上での生存時間(キーの寿命)を設定可能である。Winny のキーの寿命は通常は初期値に 1,500 秒が設定され、その値が尽きるまでネットワーク上に残る。ファイル本体を保持するピアを中心にキーの寿命が尽きるまでの間、隣接ピア間でのキーの交換により、Winny ネットワーク全体にキーが拡散していく。提案手法で制御に利用するダミーキーの寿命を、非常に小さな値(0 秒)にすることにより、Winny ネットワーク上に長時間ダミーキーを残さずに、提案手法を Winny ネットワークに適用することができる。

3.2.3 提案手法の動作

以下に、提案手法を Winny ネットワークに適用した際の、提案手法の一連の動作について述べる。

- (1) Winny ネットワーク全体に、表 1 のような本物のキーが拡散しているとする。
- (2) 表 2 の内容が記載されたダミーキーを、すべてのアクティブピアに対して拡散させる。本論文では Winny のアクティブピアを「過去 30 分以内に 1 度でも観測されたピア」として定義する。ダミーキーには本物のキーと同じファイル ID が記載されているが、ファイル位置情報はおとりピアに変更されている。おとりピアは、Winny ピアとの接続認証のためにハンドシェイク通信のみを行い、Winny ピアからのファイルの転送要求は無視する。ダミーキーの寿命は 0 秒に設定してあるため、ネットワークに拡散された後に瞬時に消滅する。
- (3) すでに本物のキーを保持しているピアに対してダミーキーを拡散させると、Winny のキー上書きルールに従い、本物のキーの内容がダミーキーの内容で更新される。ダミーキーは瞬時にネットワークから消滅するため、本物のキーをダミーキーで上書きすることは、本物のキーをネットワークから消去することと等しい。この上書きルールは、キー保持ピアだけでなくファイル保持ピアに対しても有効である。提案手法では、ファイル保持ピアの保持するファイルそのものは消去されない。しかし、ファイル保持ピアが保持している本物のキーを消去したあとは、ファイル保持ピアからキーの寿命が 1,500 秒に新しくセットされた本物のキーの拡散が止まるため、Winny ネットワーク上のすべてのファイル保持ピアにダミーキーを拡散すれば、以降は Winny ネットワークに本物のキーが拡散されなくなる(この効果はファイル保持ピアが Winny アプリケーションを再起動するまで有効である)。
- (4) Winny ネットワーク上から本物のキーが完全に消去された後は、ファイル検索ピア

表 1 本物のキーの内容

Table 1 Contents of a genuine key.

項目	内容
ファイル名	testfile.txt
ファイル ID	1369164e5dad2ca85db3408316c3ff33
ファイルサイズ	1,024 Byte
ファイル位置情報	ファイル保持ピア
キーの寿命	1,500 秒

表 2 ダミーキーの内容

Table 2 Contents of a dummy key.

項目	内容
ファイル名	testfile.txt
ファイル ID	1369164e5dad2ca85db3408316c3ff33
ファイルサイズ	1 Byte
ファイル位置情報	おとりピア
キーの寿命	0 秒

が発行する検索クエリに本物のキーがクエリヒットしなくなるため、本物のファイルを保持するピアの位置を特定することができなくなる。

3.2.4 提案手法の特徴

従来手法によるファイル流通制御では、制御中であっても本物のキーはネットワーク上から完全に消滅しない。そのため、3.1 節で示した課題 2 が生じる。また、従来手法では、制御に用いた大量のダミーキーを、制御している間はずねにネットワーク上に残さなければならないため、3.1 節で示した課題 1, 3, 4 が生じる。一方、提案手法ではこれらの課題をすべて解決している。

- 制御対象ファイルのみに有効な制御(課題 1 の解決):
ダミーキーは Winny ネットワーク上から瞬時に消去されるため、制御対象でないファイルを検索するために発行される検索クエリに、ダミーキーがクエリヒットしない。結果的に、提案手法は制御対象ファイルのみに有効となる。
- ファイル ID 検索への対応(課題 2 の解決):
提案手法はダミーキーで本物のキーを上書きし、ネットワーク上から本物のキーを完全に消去する。そのため、ファイル名検索、および、ファイル ID 検索のどちらで検索を行っても、検索クエリに本物のキーがクエリヒットしなくなる。結果としてファイル ID 検索に対しても有効な手法となる。

● インデックスを汚染しない (課題 3 の解決):

提案手法で用いるダミーキーは、Winny ネットワーク上に長時間残らない。そのため、ダミーキーが Winny ピアのインデックスに追加されることはなく、他のファイルの流通に使用可能なインデックスの領域をダミーキーが圧迫しない。

● DDoS 攻撃を誘発しない (課題 4 の解決):

ダミーキーはネットワーク上から瞬時に消去されるため、Winny ピアはダミーキーの情報をもとにダウンロードを試行することができない。よって、非常に人気のあるファイルを制御している場合であっても、ダミーキーに記載されたファイル位置情報の Winny ピアに対して、ファイル転送要求が集中することがない。

4. 実装システムの概要

提案手法を実 Winny ネットワークに適用し、その有効性と Winny ネットワークへの影響を評価するために、システムの実装を行った。開発は Visual Studio 2005 環境で C# を用いて行い、実装したシステムは Windows XP SP2 で動作する。実装したシステムは、提案手法を Winny ネットワークに適用する Winny ポイズニングシステムと、提案手法を評価するための Winny クローリングシステム、Winny パケットパーサの合計 3 つからなる。

4.1 Winny ポイズニングシステム

Winny ポイズニングシステムを用いてネットワーク上にダミーキーを拡散し、制御対象ファイルの流通制御を行う。Winny ポイズニングシステムは、5 台の Winny ポイズニングピアと 1 台のシステム管理サーバによって構成される。Winny ポイズニングピアには、

- Winny ネットワーク上のアクティブピアのアドレスを収集する機能
- アクティブピアに対してダミーキーを拡散する機能

の 2 つの機能を実装している。Winny ポイズニングピアはマルチスレッドプログラムで構築され、5 台のスレッド数の合計は 3,000 スレッドとなる。Winny ポイズニングシステムは、Winny ネットワークを構成する 10 万台以上のすべてのアクティブピアに対して、15 分以内に接続を試行することができる。システム管理サーバは Winny ポイズニングピアが収集したユニークなアクティブピアのアドレスを管理し、それらを重複がないように 5 台の Winny ポイズニングピアに割り当てることで、システム全体が分散協調動作するように管理する。

4.2 Winny クローリングシステム

提案手法の評価を行うために、Winny ネットワーク上に拡散している大量のキーを、Winny

表 3 0 ホップ検索クエリに対する応答
Table 3 Response of 0 hop search query.

クエリに応答したピア	ファイル位置情報	キーの寿命
ファイル保持ピア	ファイル保持ピア	1,500 秒以上
キー保持ピア	ファイル保持ピア	1,500 秒以下

ポイズニングシステムとは独立して収集する必要がある。そこで、Winny ネットワークに対してクローリング手法を用いてアクティブ測定を行う Winny クローリングシステムを実装した。クローリング手法とは、あるピアが保持する他ピアの情報を取得するという動作を、得られた他ピアに対して繰り返すことで、ネットワーク全体を測定する手法である。

提案手法の評価を行うために、

- (1) ファイル名をキーワードとした 6 ホップ検索クエリ
- (2) ファイル ID をキーワードとした 6 ホップ検索クエリ
- (3) ファイル ID をキーワードとした 0 ホップ検索クエリ

の 3 種類のクエリを使用して、Winny ネットワークからアクティブピアの情報とキー情報を収集する。

実際の Winny ピアは、ファイル名、あるいはファイル ID をキーワードとした 6 ホップする検索クエリを使用して、特定のキーの検索を行う。Winny クローリングシステムが、実際の Winny ピアと同じ検索クエリを用いて特定のキーを検索することで、実際の Winny ピアが本物のキーを入手できる確率が、提案手法を用いた制御でどの程度変化するかを測定する。

また、ファイルとキーの移動を確認するために、0 ホップ検索クエリを用いて測定を行う。通常の検索クエリは 6 ホップするが、検索クエリの経路情報に 5 ホップ分の架空の経路をあらかじめ書き込んでおくことで、他のピアに転送されない 0 ホップ検索クエリを実現できる。0 ホップ検索クエリで測定を行うと表 3 に示すように、そのファイルのキーのみを保持するピアと、そのファイルを実際に保持しているピアとの間で得られるキーの情報に違いが見られる。ファイル保持ピアから得られるキーは、キーの寿命が初期値の約 1,500 秒になっており、0 ホップ検索クエリに回答したピアのアドレスと、そのクエリによって得られたキーに記載されているファイル位置情報のアドレスが等しくなる。キー保持ピアから得られるキーは、キーの寿命が 1,500 秒よりも小さな値となり、クエリに回答したピアと、得られたキーに記載されているファイル位置情報のアドレスも異なる。0 ホップ検索クエリに対する応答の違いから、Winny ネットワーク上のキー保持ピアとファイル保持ピアの数

を確認することが可能であり、提案手法を用いた制御でファイルとキーの広がり方がどのように変化するかを測定できる。

Winny クローリングシステムは 8 台の Winny クローリングピアと 1 台のシステム管理サーバ、そして、1 台のデータベースサーバによって構成される。Winny クローリングピアはマルチスレッドプログラムで構築され、8 台のスレッド数の合計は 8,000 スレッドとなる。Winny クローリングシステムは、Winny ネットワークを構成する 10 万台以上のすべてのピアに対して、5 分以内に接続を試行することが可能である。8,000 スレッドのうち 2,000 スレッドをファイル名、および、ファイル ID をキーワードとした 6 ホップ検索クエリによるクローリングのために割り当て、残りの 6,000 スレッドを 0 ホップ検索クエリによるクローリングのために割り当てる。システム管理サーバはユニークなアクティブピアの情報を管理し、Winny クローリングピアに重複がないようにそれらを割り当てる。また、Winny クローリングピアは、収集した情報を定期的にデータベースサーバに送信し保存する。

4.3 Winny パケットパーサ

Winny クローリングシステムを用いてアクティブ測定を行うことで、提案手法を Winny ネットワークに適用した際の、Winny ネットワーク全体の挙動を測定することが可能となる。しかし、提案手法を Winny ネットワークに適用することで、Winny ピア 1 台あたりの挙動がどのように変化するかということに関しては、1 台の Winny ピアの通信を集中的に調査するパッシブ測定が必要である。そこで、最も一般的に使用されている Winny アプリケーション (Winny2β7.1)^{*1} を起動したピアをネットワークに参加させ、パケットキャプチャソフトの WinDump²¹⁾ を用いて全入出力パケットを記録した。Winny のすべてのパケットは暗号化されているため、Winny パケットパーサを用いて記録した全入出力パケットの復号、および、解析を行った。

5. 評価

10 万台以上のアクティブピアによって構成される実 Winny ネットワーク上で、提案手法の評価実験を行う。

*1 Winny2β7.1 を使用している場合は、他の Winny ピアのためにファイルの中継を行うことがある。中継動作はファイルの複製をとまなうため、結果として違法ファイルの複製を助長してしまう可能性がある。しかし、Winny2β7.1 ではキャッシュフォルダの容量が不足すると中継動作が行われなくなる。本論文の評価実験では、Winny2β7.1 のキャッシュフォルダを容量の小さいディスクドライブ上に作成することで、中継動作を発生させないようにしている。

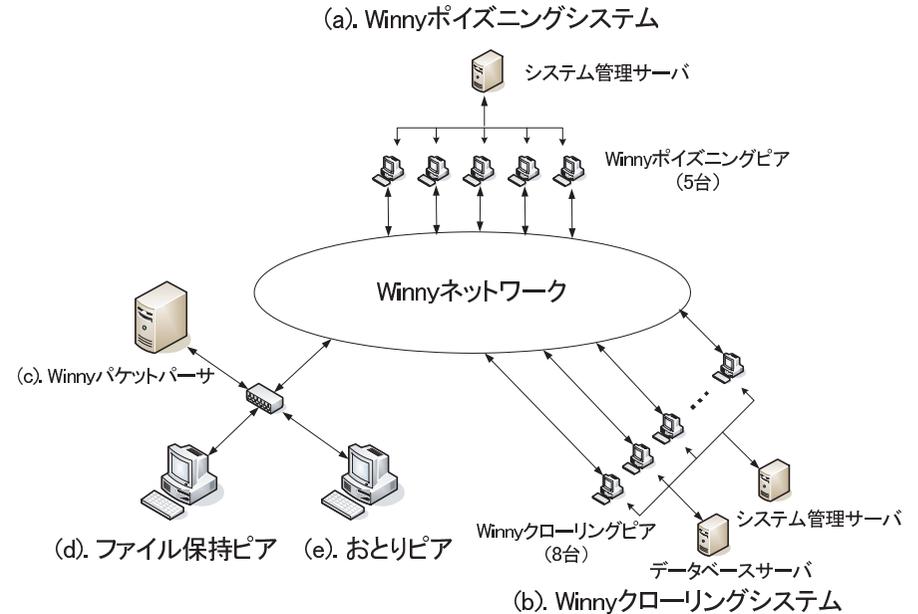


図 2 評価環境

Fig. 2 Evaluation environment.

5.1 評価環境

評価環境の概要を図 2 に示す。評価の際には、制御対象ファイルを保持するピア (図 2 (d)) と、ファイル転送に貢献しないおとりピア (図 2 (e)) をそれぞれ 1 台ずつ Winny ネットワークに参加させる。ファイル保持ピアとおとりピアの通信内容は、Winny パケットパーサ (図 2 (c)) を用いて解析する。Winny ポイズニングシステム (図 2 (a)) を用いて制御対象ファイルの流通制御を行い、Winny クローリングシステム (図 2 (b)) を用いてその効果を評価する。

5.2 評価条件

- ファイル保持ピアが保持するファイル：

ファイル保持ピアには、ファイル名やファイルサイズは同じであるが、ファイル ID のみが異なる 2 つのファイルを保持させた。これらのファイルは、iTunes ランキング²²⁾ の上位 100 位までの曲の中から選択した「アーティスト名 + 曲名」をファイル名に持つ、

拡張子が「mp3」のファイルとし、ファイルサイズは7MByteとした。ただし、そのファイルの中身はランダムなバイト列によって構成されており、mp3 ファイルとして再生することができない壊れたファイルである。提案手法を用いた制御の有無によって、ファイル流通状況がどのように変化するかを比較するために、2つのファイルのうち一方のファイルは提案手法による制御を行い、もう一方のファイルは制御せずに通常の Winny プロトコルにより自由に流通させた。

ファイル保持ピアが保持する2つのファイルは、ユーザにとって無益な偽ファイルであるため、評価実験中にそれらのファイルIDが掲示板やSNSで共有される可能性は低い。よって、ファイル検索は主にファイル名検索クエリを用いて行われる可能性が高い。ファイル名検索クエリがファイル保持ピアに到達した場合、これらの2つのファイルは同じファイル名を持つため、どちらもクエリヒットする。つまり、これらの2つのファイルはどちらもほぼ同じ条件で検索、および、クエリヒットすることが考えられる。また、ユーザはファイルIDからファイルのデータを推測することはほぼ不可能である。そのため、これらの2つのファイルはどちらもほぼ同じ条件でダウンロードされると考えられる。

- 測定期間と制御期間：

評価実験は、2008年10月29日の午後4時から10月31日の午前10時までの合計42時間行った。測定開始から3時間は提案手法によるファイル流通制御を行わない。測定開始から3時間経過後、ファイル保持ピアが保持する2つのファイルのうち一方のファイルを24時間制御する。制御終了から3時間経過後、ファイル保持ピアの Winny アプリケーションを再起動した。

5.3 評価目的と評価方法

評価目的と評価方法を以下の評価項目に示す。

- 評価項目1：ファイル保持ピア数とキー保持ピア数の変化

提案手法を用いたファイル流通制御により、制御対象ファイルとそのキーの拡散をどの程度制御できるかを評価する。制御対象ファイルを保持するピアと、そのファイルのキーを保持するピアの Winny ネットワーク上での台数の変化を、Winny クローリングシステムが発行する0ホップ検索クエリを用いて測定する。

- 評価項目2：クエリヒット回数

制御対象ファイルを検索する Winny ピアの視点に立った場合に、提案手法を適用することで制御対象ファイルの入手がどの程度困難になるかを評価する。実際の Winny ピアはファイル名、あるいは、ファイルIDをキーワードとした6ホップ検索クエリを用いて

特定のキーを検索する。Winny クローリングシステムに、この2種類の検索クエリにそれぞれ1,000スレッドずつを割り当て、制御対象ファイルの検索を行う。これは、1,000台の Winny ピアが約30秒に1回、異なる Winny ピアに対して検索クエリを発行することとほぼ等しい。提案手法を用いたファイル流通制御により、6ホップ検索クエリに制御対象ファイルのキーがクエリヒットする回数が、どの程度変化するかを測定する。

- 評価項目3：ファイル転送要求回数

提案手法を用いたファイル流通制御により、ファイル保持ピアに対するファイル転送要求回数をどの程度減らすことができるかを評価する。Winny パケットパーサを用いてファイル保持ピアの通信内容を解析する。同様に、制御中のおとりピアに対するファイル転送要求回数についても測定し、提案手法がおとりピアに対するDDoS攻撃としないことを確認する。

- 評価項目4：インデックス汚染率

制御のために拡散するダミーキーが、Winny ピアのインデックスにどの程度影響を与えているかを評価する。Winny ピアは最大で35,000個のキーをインデックスとして保持できるが、インデックスのほとんどを制御用のダミーキーが占めていると、他のファイルの流通に使用可能なインデックスの帯域が圧迫されるため、Winny ネットワーク上で他のファイルが正常に流通しなくなる可能性がある。そこで、Winny ピアのインデックスに占める制御用ダミーキーの割合をインデックス汚染率として定義し、同時に制御するファイル数を変えながら、Winny ピアのインデックス汚染率の変化を測定する。インデックス汚染率を測定するために、Winny の拡散クエリ¹⁵⁾を使用した。拡散クエリはホップしないクエリであり、拡散クエリを受け取った Winny ピアは、自分のインデックスの中からランダムに選択したキーを返答する。Winny クローリングシステムが拡散クエリを用いて Winny ピアからランダムにキーを収集することで、Winny ピアのインデックスの何%をダミーキーが占めているかを推測する。拡散クエリを用いて20分間キーを収集し、得られたキーに占めるダミーキーの割合をインデックス汚染率として算出する。また、制御用のダミーキーを長時間ネットワークに残した場合（従来手法）と、制御用のダミーキーをすぐにネットワークから消去した場合（提案手法）で、インデックス汚染率にどの程度違いがあるかを評価する。Winny プロトコルでは、キーに寿命として最大9,999秒までの値が記載できるため、そのような値を持つダミーキー¹⁶⁾は Winny ネットワーク上に長時間残ることになる。

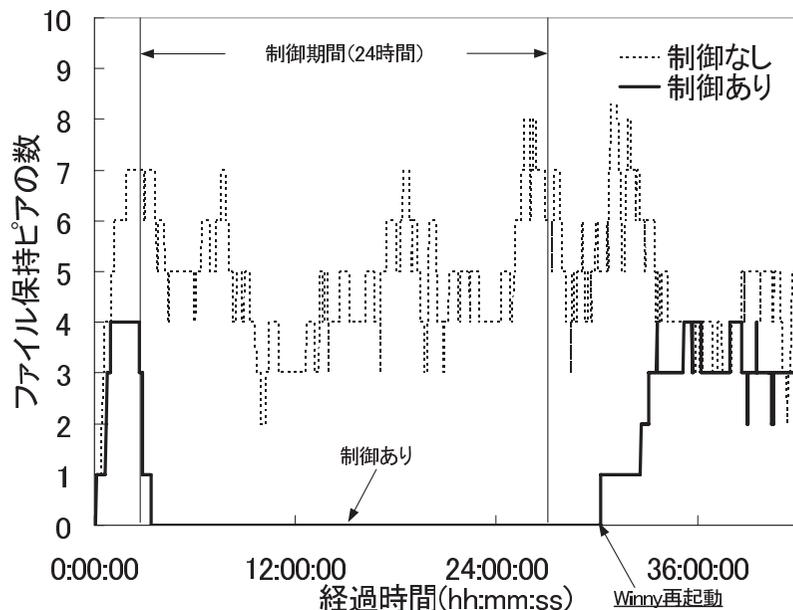


図 3 1 分間あたりのアクティブなファイル保持ピアの数
Fig. 3 Number of file holding peers per 1 minute.

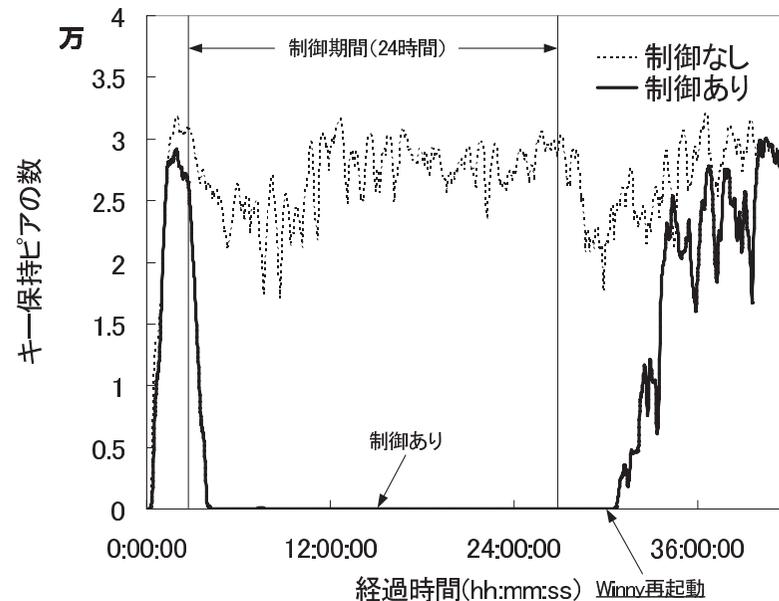


図 4 1 分間あたりのアクティブなキー保持ピアの数
Fig. 4 Number of key holding peers per 1 minute.

● 評価項目 5：制御に要したトラヒック

提案手法を用いたファイル流通制御に、どの程度のトラヒックが必要かを評価する。WinDump²¹⁾を用いて、Winny ポイズニングピアに発生した入出力トラヒックを測定した。

5.4 評価結果

5.4.1 評価項目 1

図 3 と図 4 に、アクティブなファイル保持ピアとキー保持ピアの数を 1 分間ごとにプロットした結果を示す。測定開始から 3 時間経過するまでは、ファイル保持ピアが保持する 2 つのファイルは他の Winny ピアによって自由にダウンロードされるため、アクティブなファイル保持ピアが増加していくことが分かる。ファイル保持ピアが増加すると同時に、そのファイルのキーを保持するピアも増加している。提案手法を用いたファイル流通制御を開始すると、ファイル保持ピアのキーがダミーキーで消去されるため、ファイル保持ピ

アからのキーの拡散が停止する。キー保持ピアのキーに対しても、Winny ポイズニングシステムはダミーキーを用いて次々と消去していく。そのため、制御を開始するとファイル保持ピアとキー保持ピアが Winny ネットワーク上でほとんど発見できなくなり、制御期間中は、ほぼ 0 ピアのまま推移していくことが分かる。ファイル保持ピアは制御開始から 30 分以内に Winny ネットワーク上から完全にいなくなり、キー保持ピアも制御開始から 1 時間 30 分以内に完全に観測されなくなった。表 4 に、制御期間中のファイル保持ピアとキー保持ピアのユニーク数の合計を示す。制御期間中に新たに発見されたファイル保持ピア数の合計は、制御ありの場合は 0、制御なしの場合は 47 であった。同様に、キー保持ピア数の合計は、制御ありの場合は 163、制御なしの場合は 104,763 となり、提案手法を用いたファイル流通制御を行うことで、ファイルとキーが Winny ネットワーク上にほとんど拡散しなくなっていることが分かる。

また、制御終了後はファイル保持ピアの Winny アプリケーションを再起動するまでは、

表 4 制御期間中のファイル保持ピアとキー保持ピアのユニーク数の合計

Table 4 Total number of peers that hold a file or a key.

	ファイル保持ピア		キー保持ピア	
制御あり	4	(0)	33,141	(163)
制御なし	47	(47)	108,601	(104,763)

() 内は制御開始から x 時間を除いた合計

(x = ファイル保持ピア : 0.5 時間, キー保持ピア : 1.5 時間)

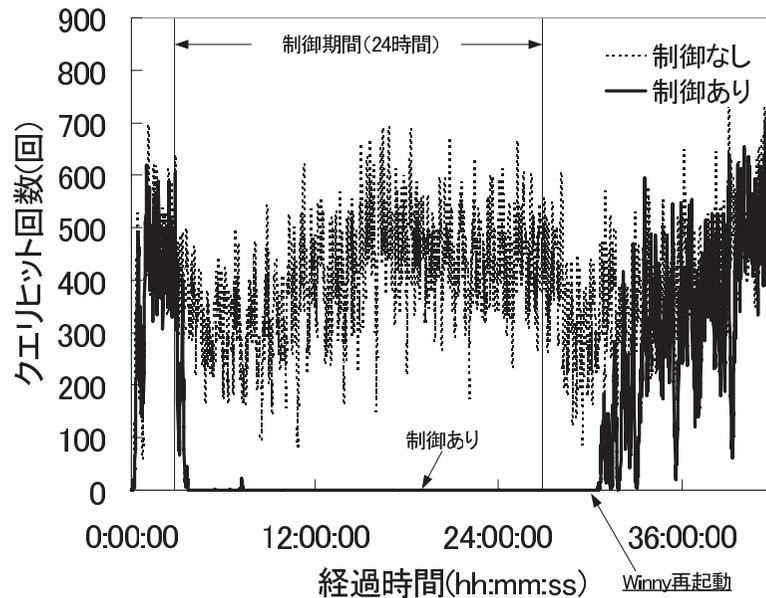


図 5 1 分あたりのクエリヒット回数 (ファイル名検索クエリ)

Fig. 5 Number of query hits per 1 minute (using a file name as keyword for query).

ファイル保持ピアからのキーの拡散が停止している。しかし、ファイル保持ピアの Winny アプリケーションを再起動した後はキーの拡散が再開している。提案手法では、ファイル保持ピアのキーのみを消去しており、保持しているファイルそのものが消去されるわけではない。そのため、ファイル保持ピアの Winny アプリケーションが再起動すると、キーが再構築され拡散が再開する。また、制御前にすでに複数の Winny ピアに制御対象ファイルが拡散していた場合は、オリジナルのファイル保持ピアだけでなく、制御対象ファイルを保持す

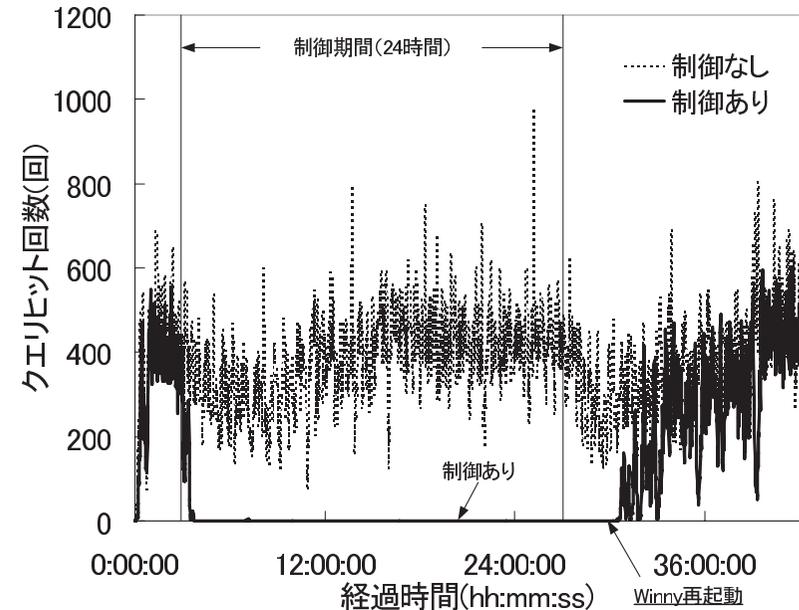


図 6 1 分あたりのクエリヒット回数 (ファイル ID 検索クエリ)

Fig. 6 Number of query hits per 1 minute (using a file identifier as keyword for query).

るすべてのピアの、いずれかのピアが再起動した場合でもキーの拡散が再開する。以上の理由から、提案手法を用いてファイル流通制御を行う場合は、本物のキーが Winny ネットワーク上から完全に消滅した場合でも、制御を継続する必要がある。

5.4.2 評価項目 2

図 5 と図 6 に、ファイル名、および、ファイル ID をキーワードとした 6 ホップ検索クエリに、本物のキーがクエリヒットした回数を 1 分間ごとにプロットした結果を示す。制御開始前までは、ファイル保持ピアが保持する 2 つのファイルのキーが、ファイル名検索クエリとファイル ID 検索クエリにクエリヒットしている。しかし、制御開始後は制御ありのファイルのキーが、どちらの検索クエリにもクエリヒットしなくなり、1 分間あたりのクエリヒット回数はほぼ 0 回で推移している。このように、提案手法を用いた制御は、実際の Winny ピアがファイル名検索クエリとファイル ID 検索クエリのどちらを使用してファイルの検索を行った場合でも有効であり、制御期間中に本物のキーを入手することはほぼ不可能である。

表 5 制御期間中のクエリヒット回数の合計
Table 5 Total number of query hits in control period.

	ファイル名検索クエリ	ファイル ID 検索クエリ
制御あり	5,973 (59)	5,093 (22)
制御なし	566,737 (533,732)	537,261 (488,780)

() 内は制御開始から 1.5 時間の値を除いた合計

表 6 制御期間中のファイル転送要求回数の合計
Table 6 Total number of file transfer requests in control period.

	ファイル保持ピア	おとりピア
制御あり	0	0
制御なし	62	—

表 5 に、制御期間中のクエリヒット回数の合計を示す。制御開始から 1 時間 30 分の値を除いた 22.5 時間のクエリヒット回数の合計をもとに、制御ありのファイルのキーがクエリヒットする確率を、制御なしと比較する。提案手法を用いたファイル流通制御を行うことで、ファイル名検索クエリに対しては $59/533,732 \approx 0.011\%$ 、ファイル ID 検索に対しては $22/488,780 \approx 0.005\%$ まで、本物のキーがクエリヒットする確率が低下する。この結果からも、提案手法を用いた制御は実際の Winny ピアが本物のキーを入手できる確率を大幅に低下させ、ファイル流通制御としての効果が高いことが分かる。

5.4.3 評価項目 3

表 6 に、制御期間中の 24 時間のファイル転送要求回数の合計を示す。制御なしのファイルは、Winny ピアが自由にダウンロードすることが可能なため、ファイル保持ピアに対して合計 62 回のファイル転送要求があった。一方、制御ありのファイルのキーは、ダミーキーを用いて Winny ネットワーク上から次々と消去されていくため、ファイル保持ピアに対してファイル転送要求がまったく来ていない。これらの結果から、Winny ネットワーク上に実在する、制御対象ファイルの検索、および、ダウンロードを試行するピアに対しても、提案手法を用いた制御が有効に機能していることが分かる。また、ダミーキーのファイル位置情報にはおとりピアが記載されているが、おとりピアに対してファイル転送要求がまったく来ていない。これは、ダミーキーが Winny ネットワーク上に残っている時間が非常に短いため、ファイル検索ピアはダミーキーも入手することができないからである。そのため、提案手法を用いた制御を行ったとしても、ダミーキーに記載されたファイル位置情報のピアに対して、多数の Winny ピアからのアクセスが集中することがないため、提案手法を用いた

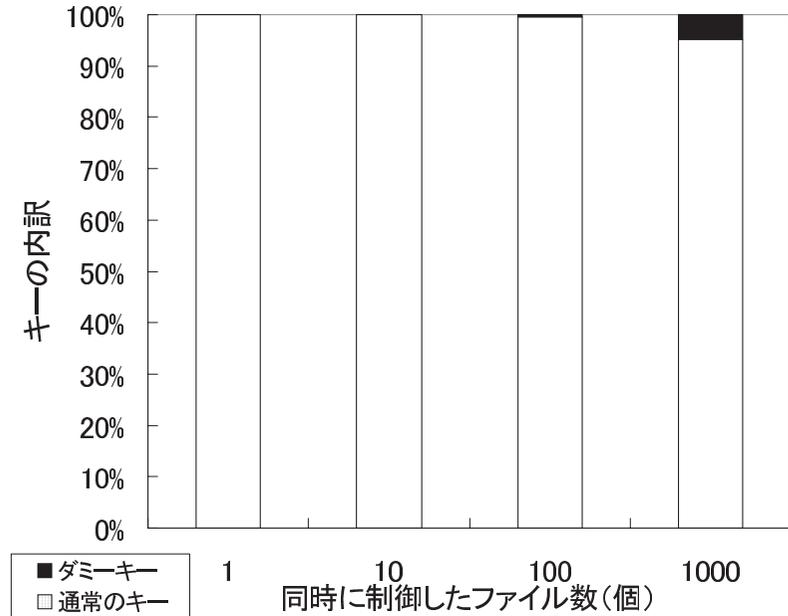


図 7 インデックス汚染率 (ダミーキーの寿命: 9,999 秒)
Fig. 7 Ratio of dummy keys (key lifetime: 9,999 sec).

制御が特定のピアへ負荷をかけることもない。

5.4.4 評価項目 4

ダミーキーが Winny ピアのインデックスに与える影響について評価した結果を示す。Winny クローリングシステムは拡散クエリを用いて 20 分間で合計 8,000 万個以上のキーを収集した。

図 7 に、ダミーキーの寿命を 9,999 秒として制御を行った場合 (従来手法) のインデックス汚染率を示す。同時に制御するファイル数が少ない場合は、Winny ピアのインデックスにもほとんど影響を与えていない。しかし、1,000 個のファイルを同時に制御した場合は、インデックス汚染率が 5% を超えている。Winny ポイズニングシステムを用いてダミーキーをネットワーク全体に拡散させると、ほぼすべてのアクティブな Winny ピアにダミーキーが広がることになる。もし仮に、寿命が 9,999 秒となっているダミーキーを用いて 35,000 個のファイルを同時に制御すると、各ピアのインデックスのすべてをダミーキーが占めてし

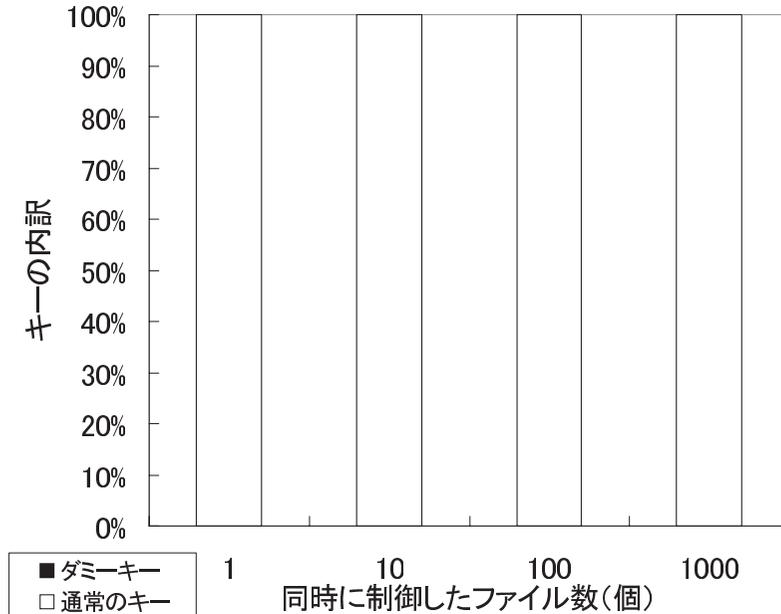


図 8 インデックス汚染率 (ダミーキーの寿命: 0 秒)
Fig. 8 Ratio of dummy keys (key lifetime: 0 sec).

まい、他のファイルがまったく流通しなくなる可能性がある。

図 8 に、ダミーキーの寿命を 0 秒として制御を行った場合 (提案手法) のインデックス汚染率を示す。提案手法では、同時に 1,000 個のファイルを制御した場合であってもインデックス汚染率をほぼ 0% に保つことができ、各ピアのインデックスにほとんど影響を与えていない。提案手法は、制御用のダミーキーを Winny ネットワーク上からすぐに消滅させることで、各ピアのインデックスを汚染しないようにしているため、実際の Winny ネットワークに対して十分に適用可能な制御方式となっている。

5.4.5 評価項目 5

制御期間中に 1 台の Winny ポイズニングピアが生成した平均入出力トラフィックは 5.29 Mbps であった。Winny ポイズニングピアは、アクティブピアのアドレスを収集する機能と、アクティブピアにダミーキーを拡散する機能がある。Winny ポイズニングピアが生成した 5.29 Mbps のトラフィックのうち、5.05 Mbps がアクティブピアのアドレスを収集する機能の

ために使用されており、ダミーキーの拡散には 0.24 Mbps のみを要した。

6. 考 察

本提案手法の実運用に向けた課題と、他の P2P ファイル共有ネットワークに対する本提案手法の適用について考察する。

6.1 Winny ポイズニングピアの特定

提案手法ではダミーキーの寿命を 0 秒に設定しているため、ダミーキーを受け取った Winny ピアから他の Winny ピアに対してダミーキーが拡散していかない。そのため、インデックスポイズニングを受けている Winny ピアは、自発的にインデックスポイズニングを行っている Winny ポイズニングピアを特定することができる。Winny ポイズニングピアが特定された場合は、掲示板や SNSなどを介して Winny ポイズニングピアの IP アドレスなどが共有される可能性がある。そして、特定の IP アドレスとの通信のみを遮断するソフトウェア²³⁾ などを使用することで、提案手法によるファイル流通制御が無効化する可能性がある。

そこで、提案手法を実際に運用していく際には、ダミーキーの寿命を完全に 0 秒にするのではなく、数秒から数十秒程度の小さな寿命に設定することで、複数の Winny ピアにダミーキーを交換させ、Winny ポイズニングピアの特定を困難にする方法が考えられる。しかし、数百万のファイルを同時に制御するような大規模運用を行った際に、数秒程度の寿命が設定されたダミーキーが、各 Winny ピアのインデックスにどの程度影響を与えるかということに関しては、今後、大規模分散環境を用いた提案手法の大規模な運用を行い、評価していく必要がある。

また、ダミーキーを検索クエリに載せて複数の Winny ピア上をホップさせ、Winny ネットワーク上に拡散させる方法も考えられる。Winny プロトコルでは検索クエリにキーが載っている場合に、検索クエリの経路上にキーが複製されるという特徴がある。このような拡散方法であれば、複数の Winny ピアがダミーキーの拡散に貢献することになるため、Winny ポイズニングピアの特定が困難になる。しかし、Winny ネットワーク上を大量の検索クエリがホップするようになると、ネットワークの通信が検索クエリで溢れてしまうという問題²⁴⁾ が発生することもある。検索クエリを用いた拡散方法を適用する際には、ダミーキーを載せた検索クエリの発行数を限定することや、検索クエリのホップ数を調節することで、ネットワークの通信が検索クエリで溢れてしまう問題を起ささないようにする必要がある。

6.2 大量の亜種ファイルの作成

制御対象ファイルに 1 バイトの無意味なファイルを加えたアーカイブのような大量の亜

表 7 代表的な P2P ファイル共有ネットワークの特性
Table 7 Characteristics of popular P2P file sharing networks.

	キーの検証	同一ファイル ID	キーの寿命
Winny	なし	上書き	設定可
Share	なし	追加	設定可
WinMX	なし	追加	設定不可
LimeWire	なし	追加	設定不可

種ファイルを作成し、それらのファイル ID を変えることで制御を困難にするようなケースが考えられる。このようなケースでは、大量の亜種ファイルを制御するために拡散しなければならぬダミーキーの数が多くなる。従来手法を用いた制御では、制御用のダミーキーが長時間ネットワーク上に残るため、ダミーキー拡散後の一定期間はファイル流通制御効果が持続する。しかし、提案手法を用いた制御は 3.1 節で示した課題を解決しているが、制御期間中はダミーキーの拡散を継続する必要がある。そのため、このようなケースでは提案手法を用いた制御に要するトラフィックが、ポリューションや、長時間ネットワークに残るダミーキーを使用したインデックスポイズニングなどの従来手法よりも多くなる可能性がある。

しかし、制御対象ファイルやその亜種ファイルを故意に拡散させているユーザを、Winny クローリングシステムを用いて特定することが可能である。大量の亜種ファイルを作成し制御を無効化しようとする問題に対しては、該当のユーザを特定し、ISP を介した通信帯域制御やユーザへの通告などにより対処可能であると考えられる。

6.3 他の P2P ファイル共有ネットワークへの適用

本論文の評価結果から、P2P ファイル共有ネットワークへの影響を抑えるように十分に考慮されたファイル流通制御手法でなければ、大規模なファイル流通制御を行うことは困難であるといえる。そして、そのような特徴を持つ本論文の提案手法は、Winny プロトコルの特性を利用することで実現している。しかし、Winny 以外の P2P ファイル共有ネットワークが、Winny プロトコルと同じ特性を持っているとは限らない。そのため、Winny と同様のインデックスポイズニングの適用方法で、本論文の提案手法のような特徴を持つファイル流通制御が実現できるわけではない。たとえば、日本国内で Winny 以外に人気のある P2P ファイル共有ネットワークに Share, WinMX, LimeWire などがあげられる。これらのプロトコルの特性を表 7 に示す。Share, WinMX, LimeWire は、Winny と同様にファイルのメタデータ（キー）の内容を検証しないため、インデックスポイズニングを用いたファイル流通制御が可能である。しかし、同じファイル ID を持つがファイル位置情報が

異なるようなメタデータは、Winny のインデックスでは上書きされるが Share, WinMX, LimeWire では追加される。さらに、WinMX, LimeWire はメタデータに寿命を設定できない。このように、各ネットワークが備えるプロトコルの特性はそれぞれ異なっている。そのため、特定のファイルの流通を正確に制御でき、なおかつ、P2P ファイル共有ネットワークへ与える影響を極力抑えたファイル流通制御を実現するためには、それぞれのプロトコルに合わせたインデックスポイズニングの適用方法が必要である。また、ポリューションなどの他の制御手法とインデックスポイズニングを組み合わせることで、本論文の提案手法のような特徴を持つファイル流通制御手法を実現できる可能性もあり、今後それらを明らかにしていく必要がある。

7. ま と め

本論文では、Winny ネットワーク上を流通するファイルを制御するためにインデックスポイズニングを適用し、評価実験によりその効果を確認した。提案手法は、ファイルのダウンロードに必要なキーを Winny ネットワーク上から消去することで、Winny ピアがそのキーを入手できる確率を大きく低下させることを確認した。また、制御のために拡散するダミーキーは、Winny ピアのインデックスにほとんど影響を与えないことも確認した。これより、提案手法は Winny ネットワークの社会的な利用を実現するための有効な制御方式であると考えられる。

今後は、インデックスポイズニングを適用するためのシステムを PlanetLab, CoreLab²⁵⁾ 上に実装し、大規模な分散制御用システムを用いた提案手法の評価、ならびに、多数のファイルを効率良く制御するための提案手法の改良を行う予定である。また、Winny 以外のネットワークに対するファイル流通制御に関しても同様に研究を進めることで、複数のネットワークで共通した性質や現象を明らかにし、P2P ファイル共有ネットワークに対するファイル流通制御方式を開発する予定である。

謝辞 本研究の一部は科研費基盤 B (No.20300025) の研究助成の支援を受けている。ここに記して感謝する。

参 考 文 献

- 1) Rasti, A., Stutzbach, D. and Rejaie, R.: On the Long-term Evolution of the Two-Tier Gnutella Overlay, *Proc. 9th IEEE Global Internet Symposium*, pp.1-6 (2006).
- 2) Pouwelse, J., Garbacki, P., Epema, D. and Sips, H.: The Bittorrent P2P File-

- Sharing System: Measurements and Analysis, *Proc. International Workshop on Peer-To-Peer Systems* (2005).
- 3) Liang, J., Kumar, R. and Ross, K.: The FastTrack Overlay: A Measurement Study, *Computer Networks Journal*, Vol.50, No.6, pp.842–858 (2006).
 - 4) Steiner, M., Biersack, E. and Ennajjary, T.: Actively Monitoring Peers in Kad, *Proc. International Workshop on Peer-To-Peer Systems* (2007).
 - 5) 寺田真敏, 鶴飼裕司, 金居良治, 畑田充弘, 松木隆宏, 宮川雄一: クローリング手法を用いた P2P ネットワークの観測, 情報処理学会 CSEC 研究報告, Vol.2007, No.48, pp.51–56 (2007).
 - 6) Sen, S. and Wang, J.: Analyzing Peer-to-Peer Traffic Across Large Networks, *Proc. 2nd ACM SIGCOMM Workshop on Internet Measurement*, pp.137–150 (2002).
 - 7) Karagiannis, T., Broido, A., Faloutsos, M. and Claffy, K.: Transport Layer Identification of P2P Traffic, *Proc. 4th ACM SIGCOMM Workshop on Internet Measurement*, pp.121–134 (2004).
 - 8) Cho, K., Fukuda, K., Esaki, H. and Kato, A.: The Impact and Implications of the Growth in Residential User-to-User Traffic, *Proc. ACM SIGCOMM 2006*, pp.207–218 (2006).
 - 9) Johnson, M., McGuire, D. and Willey, N.: The Evolution of the Peer-to-Peer File Sharing Industry and the Security Risks for Users, *Proc. 41st Annual Hawaii International Conference on System Sciences*, pp.383–383 (2008).
 - 10) Liang, J., Kumar, R., Xi, Y. and Ross, K.: Pollution in P2P File Sharing Systems, *Proc. Infocom 2005*, pp.1174–1185 (2005).
 - 11) Lee, U., Choi, M., Cho, J., Sanadidi, M. and Gerla, M.: Understanding Pollution Dynamics in P2P File Sharing, *Proc. International Workshop on Peer-to-Peer Systems* (2006).
 - 12) Christin, N., Weigend, A. and Chuang, J.: Content Availability, Pollution and Poisoning in File Sharing Peer-to-Peer Networks, *Proc. 6th ACM Conference on Electronic Commerce*, pp.68–77 (2005).
 - 13) ネットエージェント株式会社 (オンライン). <http://www.netagent.co.jp/> (参照 2008–12–1)
 - 14) Liang, J., Naoumov, N. and Ross, K.: The Index Poisoning Attack in P2P File-Sharing Systems, *Proc. IEEE Infocom 2006*, pp.1–12 (2006).
 - 15) 金子 勇: Winny の技術, 株式会社アスキー (2005).
 - 16) Yoshida, M., Ohzahata, S., Nakao, A. and Kawashima, K.: Controlling File Distribution in Winny Network Through Index Poisoning, *Proc. 23rd of International Conference on Information Networking* (2009).
 - 17) Naoumov, N. and Ross, K.: Exploiting P2P systems for DDoS attacks, *Proc. 1st International Conference on Scalable Information Systems* (2006).
 - 18) El Defrawy, K., Gjoka, M. and Markopoulou, A.: BotTorrent: Misusing BitTorrent to Launch DDoS Attacks, *Proc. 3rd USENIX Workshop on Steps to Reducing Unwanted Traffic on the Internet Table of Contents* (2007).
 - 19) Steiner, M., En-Najjary, T. and Biersack, E.: Exploiting KAD: Possible Uses and Misuses, *Computer Communications Review*, Vol.37, No.5, pp.65–70 (2007).
 - 20) Athanasopoulos, E., Anagnostakis, K. and Markatos, E.: Misusing Unstructured P2P Systems to Perform DoS Attacks: The Network That Never Forgets, *Lecture Notes in Computer Science*, Vol.3989, pp.130–145 (2006).
 - 21) WinDump (オンライン). <http://www.winpcap.org/windump/> (参照 2008–12–1)
 - 22) アップル iTunes Top100 (オンライン). <http://www.apple.com/jp/itunes/> (参照 2008–12–1)
 - 23) PeerGuardian2 (オンライン). <http://phoenixlabs.org/pg2/> (参照 2008–12–1)
 - 24) Daswani, N. and Garcia-Molina, H.: Query-Flood DoS Attacks in Gnutella, *Proc. 9th ACM Conference on Computer and Communications Security*, pp.181–192 (2002).
 - 25) Nakao, A., Ozaki, R. and Nishida, Y.: CoreLab: An Emerging Network Testbed Employing Hosted Virtual Machine Monitor, *Proc. ACM CoNEXT ROADS Workshop* (2008).

(平成 20 年 12 月 1 日受付)

(平成 21 年 6 月 4 日採録)



吉田 雅裕 (学生会員)
昭和 60 年生 . 平成 18 年東京農工大学工学部情報コミュニケーション工学科卒業 . 現在, 同大学大学院工学府情報工学専攻修士 2 年 . P2P ネットワークの研究に従事 .



大坐畠 智 (正会員)

昭和 49 年生。平成 15 年筑波大学大学院博士課程工学研究科電子・情報工学専攻修了。同年東京農工大学工学部情報コミュニケーション工学科助手。平成 19 年同大学助教。平成 21 年電気通信大学大学院情報システム学研究科准教授。ネットワーク性能評価の研究に従事。平成 17 年度電子情報通信学会学術奨励賞受賞。IEEE, ACM, IEICE 各会員。博士(工学)。



中尾 彰宏 (正会員)

平成 3 年に東京大学理学部物理学科を卒業。平成 6 年に同大学大学院情報工学専攻修士課程修了。IBM Texas Austin 研究所, IBM 東京基礎研究所等を経て, 米国 Princeton 大学大学院情報学科にて修士および博士取得。平成 17 年東京大学大学院情報学環助教授(平成 19 年に准教授)に就任, 現在に至る。また平成 19 年より情報通信研究機構にて客員研究員プロジェクトリーダー兼務。



川島幸之助 (正会員)

昭和 44 年東京大学工学部計数工学科卒業。同年日本電信電話公社入社, 研究所所属。通信トラヒック研究部長等を歴任。平成 9 年 NTT アドバンステクノロジー株式会社入社。平成 14 年東京農工大学工学部教授, 現在に至る。主に, 通信トラヒック工学, 通信網, システム性能評価の研究・開発・教育に従事。主な著書として, 『最新コンピュータネットワーク技術の基礎』(共著, 電気通信協会), 『情報通信トラヒック—基礎と応用』(共著, 電気通協会)。昭和 56 年電子通信学会論文賞(共著), 昭和 61 年日本オペレーションズ・リサーチ学会文献賞, 平成 19 年同学会業績賞, 等受賞。日本オペレーションズ・リサーチ学会, 電子情報通信学会各フェロー。IEEE, ACM SIGCOMM, IFIP WG6.3 各会員。博士(工学)。