

研究種目：基盤研究 (C)

研究期間：2007～2009

課題番号：19560392

研究課題名 (和文)

ネットワーク上への流失情報に対する対策技術に関する研究

研究課題名 (英文)

A study on countermeasure technologies against information leakage through information networks

研究代表者

石田 賢治 (ISHIDA KENJI)

広島市立大学・情報科学研究科・教授

研究者番号：70221025

研究成果の概要 (和文)：

P2P システムで発生する情報流出の対策となる基本技術を検討した。具体的に、代表的な P2P システムの一つである BitTorrent に着目し、流出情報を制御するためのダミーデータ等を効率的に拡散できるデータ配布技術、および、流出情報の拡散速度を低減させる技術を開発した。シミュレーション実験により、提案した拡散速度制御技術を評価した。その結果、従来技術よりも効果的にデータ拡散を制御可能なことが明らかになった。

研究成果の概要 (英文)：

This study proposes some basic technologies for solving information leakage problems in P2P file sharing systems. To begin with, we focus on a typical P2P system, BitTorrent, and propose both (1) an efficient data distribution technology for controlling leaked information (e.g. dummy data distribution) and (2) a control technology on diffusion of leaked information. Next, we evaluate these technologies by using network simulator. As a result, it is found that our proposals can control data diffusion more effectively than the previous methods.

交付決定額

(金額単位：円)

	直接経費	間接経費	合計
2007 年度	1,100,000 円	330,000 円	1,430,000 円
2008 年度	600,000 円	180,000 円	780,000 円
2009 年度	900,000 円	270,000 円	1,170,000 円
年度			
年度			
総計	2,600,000 円	780,000 円	3,380,000 円

研究分野：工学

科研費の分科・細目：電気電子工学・通信・ネットワーク工学

キーワード：P2P システム、情報流失、情報流出、データ収集技術、データ拡散技術

1. 研究開始当初の背景

P2P システムの急激な普及や悪意をもつプログラムであるコンピュータウイルスやスパイウェアの登場により、多くの情報がネ

ットワーク上に、同意なく流失する事態が続いている。例えば、端末のコンピュータが暴露ウイルスというコンピュータウイルスに感染すると、このコンピュータの中に保存さ

れている情報が他のコンピュータに次々にコピーされる形で流失する。この結果、個々のコンピュータに情報のコピーが分散するので、いったん流失すると、その回収や無効化は大変困難である。

また、流失する情報は、著作権のあるコンテンツ、個人のプライバシー情報、企業の内部情報、公的機関の内部情報など、本来外部に流失すべきでないものも含まれており、その流失の影響は、個人レベルから国レベルに及び甚大な影響が出る場合もある。

このようなほぼ回収不可能な情報の無効化を目指した技術として、ポイズニング技術[1]が、2005年ごろから注目されている。この技術では、流失ファイルと同じ特徴を持つファイルを大量かつ故意に流通させることで流出情報が発見されることを困難にするとともに、これを探している人たちの意欲を低下させることをねらっている。[1]では、主に音声や映画やソフトウェアなどの著作権情報に関して検討を行っている。しかしながら、単純なポイズニングは、ネットワーク全体に対して、大きな副作用があり脅威になることが指摘[2]されている。

また、朝日新聞の平成18年8月29日の報道[3]や総務省の発表によると、「ウィニー関係の情報流失では官庁や警察の情報が漏れるなど社会的な反響が大きいものの、対策が収益事業にはなりにくいとみて、(総務省)自ら乗り出すこととした。2007年度予算の概算要求に盛り込み、3年計画で通信機器メーカーなどに研究開発委託する考えだ。」とのことである。この事業による構想は、情報を書き込んだファイルに目印をつけておき、流失の際には特定のサーバを経由するようにして、そのサーバで目印つきのファイルを一網打尽で消去する仕組みの開発を目指したものである。

[1] Nicolas Christin, Andreas S. Weigend, and John Chuang, "Content availability, pollution and poisoning in file sharing peer to peer networks," Proceedings of ACM EC'05, Vancouver, June 2005.

[2] Kevin Walsh and Emin G. Sirer, "Fighting peer-to-peer SPAM and decoys with object reputation," Proceedings of SIGCOMM'05 Workshops, Philadelphia, August 2005.

[3] 朝日新聞, "ウィニー対策システムを開発へ", 平成18年8月29日.

2. 研究の目的

まず、ネットワーク上へ流失した情報に対する対策技術の動向やそれらの技術の日本国内における適用可能性について調査・検討を行う。対象として考えている技術は、P2P

ピアの可視化技術、流失ファイル回収技術、流失ファイル無効化技術などである。

次に、情報流失直後に効果的に機能する技術に的を絞って考察する。そして、情報流失を早期に発見して、ネットワーク全体ではなく、できるだけ局所的に対処可能な技術の開発を行う。火事というならば初期消火を行うための基礎技術の開発を目指す。

また、開発した技術の性能をネットワークシミュレータや閉じたネットワークを使って評価する。実ネットワークでの評価も検討する。得られた成果は、国内や海外の学会発表などを通じて公表し社会に還元する。

3. 研究の方法

(1) ネットワーク上への流出情報に対する対策技術の整理

ネットワーク上へ流出した情報に対する既存の対策技術を調査、検討する。次に、情報流出直後に効果的に機能する技術に的を絞って考察する。

(2) P2P システムにおける効率的なデータ収集技術

P2P システムにおけるデータ収集とデータ配布は表裏一体のものであり、効率的なデータ収集はデータ提供元から見た場合、効率的なデータ配布(拡散)と見なすことができる。効率的なデータ収集および配布(拡散)技術は、制御対象のファイル情報に似せたダミーファイル等を P2P システムに効率的に拡散する際に重要となる。

(3) P2P システムにおけるファイル拡散制御技術

(2) の成果を利用し、最近、利用者が増加している、代表的な P2P システムであるスーパーシードモードをもつ BitTorrent システムに注目したファイル拡散技術の検討を行う。

4. 研究成果

(1) ネットワーク上への流出情報に対する対策技術の整理

まず、ネットワーク上へ流出した情報に対する既存の対策技術を調査した。特に、P2P ファイル共有ソフトウェアに着目して調査した。その結果、P2P ファイル共有ソフトウェアを用いたファイル流出問題への対策方式として、下記の4つの方式があることが分かった。

(a) ファイルの検索を攪乱、阻害するインデックスポイズニング

(b) 偽物のファイルをネットワークに流通させるアイテムポイズニング

(c) 悪意のあるピアをネットワークから排除する方式

(d) ファイル自体の拡散速度を低減させる方式

これらの方式の内、(a) (b) (c) は、P2P ファイル共有ソフトウェアの変更が必要な場合があり、いつも適用できるとは限らない。また、(d) は既存の P2P ファイル共有ソフトウェアの変更を必要としない。そこで、本研究では、まず、(d) に着目した制御を検討した。また、流出した情報を制御するためのデータを配布可能な場合、迅速に P2P ネットワークに拡散させる必要がある。そこで、効率的なデータ拡散方式の検討も行った。

(2) P2P システムにおける効率的なデータ収集技術

まず P2P システムにおいて、データ収集および配布を効率化する方式を検討した。P2P システムで複数のピアからファイルを並列的に分割取得する場合、ファイル完成に必要な部分ファイルを低速なピアから取得しようとする、P2P システムに参加するピア全体のファイル取得時間が長期化する、という問題が生じる。この問題を解決する方法として、ファイル完成に必要な最後の部分ファイルのリクエストを、接続している全てのピアに送信する End-game Mode 方式が提案されている。しかし、多数のピアに対して、同じ部分ファイルのリクエストを行うと、冗長なトラフィックの発生という問題が生じる。そこで、本研究ではこのような重複リクエストを行わず、低速なピアへのリクエストを抑制する方式を提案する。この方式により、冗長なトラフィックを発生させることなく、ファイル取得時間の長期化を抑制することを目指す。そして、複数のピアからファイルを分割取得する P2P システムの中で注目されている BitTorrent を対象に、End-game Mode 方式と提案方式を、シミュレーション実験により比較評価する。P2P ネットワークに低速なピアと高速なピアが混在し、ピアがファイル取得後にネットワークから離脱しない場合と、離脱する場合の双方を想定し、各ピアのファイルダウンロード時間とネットワーク全体の冗長トラフィック量を評価した。その結果、提案方式は、ピアがネットワークから離脱しない場合、離脱する場合の双方において、End-game Mode 方式と比較して、冗長なトラフィックを削減し、同等の効率でファイルを取得可能であることが分かった。

また P2P システムで利用されるファイルの分割並列取得に適したトランスポートプロトコルについて検討し、トランスポートプロトコルにおける効率化の可能性を探った。従来の TCP だけでなく、データグラム型の UDP、DCCP、さらに TCP の後継として期待されてい

る SCTP について、分割並列取得への適性をシミュレーション実験により評価した。特に SCTP については方式を決定づけるパラメータである同時リクエスト数、ストリーム数に加え、ブロックサイズにも注目して解析を行った。その結果、十分大きなブロックサイズでは安定して高い性能を保つことと、同時リクエスト数をあまり大きくしなくとも SCTP マルチストリームによりパケットロス耐性を向上させることが可能であることが明らかとなった。

(3) P2P システムにおけるファイル拡散制御技術

P2P ファイル共有ソフトウェアの一つである BitTorrent に着目して新たな制御技術の検討を行った。ここで、BitTorrent は、高いファイル共有効率を持つため、近年利用者が増加している P2P ファイル共有ソフトウェアである。本研究では、(i) BitTorrent のファイル交換機能の一部である Tit-For-Tat 戦略を考慮した方式、(ii) 自身がシーダになった場合、通信回線を効率的に利用するために用意された機能であるスーパーシードモードを利用した方式、を提案した。以下、それぞれについて説明する。

(i) Tit-For-Tat 戦略を考慮した方式

BitTorrent はトラッカーと称するサーバを用いたハイブリッド型 P2P であり、ファイル毎にネットワーク (BitTorrent ネットワーク) を形成する。ユーザは、torrent ファイルという属性情報記録ファイルを用いてトラッカーに接続し、BitTorrent ネットワークに参加し、ファイルを交換する。ファイルはピースに分割されており、BitTorrent ネットワーク内の各ピアはピースを順不同に収集していく。

BitTorrent では Choking 機能と Optimistic Unchoking 機能を用いた Tit-For-Tat 戦略に基づいてピア選択を行い、ファイルを交換する。また、全てのピースを持つピアをシーダという。Choking 機能とは、接続ピアの貢献度 (アップロードする割合) により自身が持つピースをダウンロードさせるか否かを決定する機能である。ピースの提供が速いピアに対してはダウンロードを許可し、提供が遅いピアに対してはダウンロードを禁止する。Optimistic Unchoking 機能とは、一定時間おきに順に接続ピアに対してダウンロードを許可することで、相手に貢献し、相手からのダウンロードを禁止されないようにする機能である。また、Tit-For-Tat 戦略とは、始めは協調して、その後に相手が協調するなら協調し、相手が裏切れば裏切るという戦略である。本研究では、Tit-For-Tat 戦略を逆手にとった方式として方式 (1)、(2)

を、シーダによるピース配布の高速化の効果を削減するための方式として方式(3)を提案した。

方式(1): 高速な妨害ピア(本研究では、制御ピアと呼ぶ)を導入することで、希少ピースを持つピアからの希少ピース配布を阻害し、ネットワーク全体のファイル完成速度の低下を狙う。妨害ピアの制御対象は、希少ピースをもつピアである。

方式(2): 方式(1)と同様に制御ピアを利用する。方式(2)では、希少ピースを持つピアではなく、貢献度の高い(アップロード速度が速い)ピアを被制御ピアとする。

方式(3): シーダになったピアに対して膨大な数のTCPコネクションを張り、シーダのアップロード速度を低下させる。

ネットワークシミュレータ ns2 を利用して提案方式を評価した。シミュレーションでは、各提案方式において、ピアがすべてのピースを取得してファイルを完成させるまでの時間を計測した。その結果、方式(1)および方式(2)では、従来の BitTorrent と比較して、拡散速度の低減が実現できないことが分かった。しかし、制御対象をシーダとした方式(3)を利用すると、拡散速度の低減が可能であることが明らかとなった。

(ii) スーパーシードモードを利用した方式

まず、本提案方式は、スーパーシードモードと呼ばれるアルゴリズムを備えた BitTorrent ネットワークを対象とする。スーパーシードモードは、初期シーダのピース配布方針の一つである。通常の初期シーダは、すべてのリクエストに対して無条件にアップロードを行う。一方、スーパーシードモードを使用しているシーダ(スーパーシーダ)は、いくつかの制約に基づいて自身の帯域を節約しながらアップロードを行う。現在、多くの BitTorrent の実装が、このスーパーシードモードを実装している。

提案方式は、特定のピアのアップロードを独占する従来方式を参考にした。従来方式は、主にリーチャを制御対象としていたのに対し、提案方式は初期シーダを制御対象としている。具体的に、提案方式は、スーパーシーダに申告するアップロード速度をすべての一般ピアより十分高速とし、スーパーシーダから取得したピースのアップロードを1台のピアに限定することで制御を行う。また、提案方式では、オプション仕様として、アップロード対象のピア以外にピース保持情報を通知しない機能、および、スーパーシーダから取得したピースをアップロードする際に、一時的にアップロード速度を低下させる機能を持つ。

提案方式はネットワークシミュレータ ns2 を利用して評価した。その結果、提案方式は、ファイル拡散速度を大幅に低下できることが分かった。

5. 主な発表論文等

(研究代表者、研究分担者及び連携研究者には下線)

[雑誌論文] (計 4 件)

[1] Junichi Funasaka, Toshio Niyagawa, and Kenji Ishida, Effect of SCTP Multistream Function Applied to Parallel Downloading, Proc. IACSIT 2nd International Conference on Communication Software and Networks (ICCSN 2010), pp.237-241, 2010. (査読有)

[2] Junichi Funasaka, Akihiko Ishizu, and Kenji Ishida, A File Fetching Method to Avoid Performance Deterioration on BitTorrent-Like P2P Networks, IEICE Transactions on Commun., E92-B, 8, pp.2591-2599, 2009. (査読有)

[3] Junichi Funasaka, Evaluation on Parallel Downloading Method using HTTP over UDP, Proc. IEEE 9th International Symposium on Autonomous Decentralized Systems (ISADS2009; Presented at AHSP2009), pp.333-338, 2009. (査読有)

[4] Junichi Funasaka, Akihiko Ishidu, and Kenji Ishida, A File Fetching Method to Reduce the Redundant Traffic on BitTorrent-like P2P Networks, Proc. 28th IEEE ICDCS Workshops, pp.593-598, 2008. (査読有)

[学会発表] (計 7 件)

[1] 桑原 祐樹, 舟阪 淳一, 石田 賢治, P2P ネットワークにおけるスーパーシードモードを対象としたファイル拡散制御方式, 電子情報通信学会情報ネットワーク研究会, IN2010-8, 2010. (東京都)

[2] 内藤 成文, 小畑 博靖, 村瀬 勉, 石田 賢治, 無線 LAN 環境における TCP 制御と MAC 制御を共に用いたフロー-QoS 保証について, 電子情報通信学会情報ネットワーク研究会, IN2009-118, 2010. (広島市)

[3] 舟阪 淳一, 二矢川 敏夫, 石田 賢治, SCTP マルチストリームを用いた分割ダウンロードの制御パラメータについての考察, 電

子情報通信学会ネットワークシステム研究会, NS2009-128, 2009. (松山市)

(3)連携研究者
なし

[4] 仲島 智, 石田 賢治, 高野 知佐, 舟阪 淳一, 小畑 博靖, BitTorrent ネットワークにおけるファイル拡散速度の制御, 電気・情報関連学会中国支部第 60 回連合大会, pp. 220-221, 2009. (広島市)

[5] 舟阪 淳一, 二矢川 敏夫, 石田 賢治, 分割ダウンロードにおける SCTP マルチストリームの効果についての一考察, 電子情報通信学会ネットワークシステム研究会, NS2009-20, 2009. (広島市)

[6] 舟阪 淳一, 高ロス率ネットワークにおける分割ダウンロードの性能向上を目指すトランスポートプロトコルについての一検討, 電子情報通信学会情報ネットワーク研究会, IN2007-201, 2008. (名護市)

[7] 石津 明彦, 舟阪 淳一, 石田 賢治, P2P ネットワークにおける冗長トラフィックの削減を目指したファイル取得方式, 電子情報通信学会情報ネットワーク研究会, IN2007-117, 2007. (広島市)

[図書] (計 0 件)

[産業財産権]

○出願状況 (計 0 件)

○取得状況 (計 0 件)

[その他]

6. 研究組織

(1)研究代表者

石田 賢治 (ISHIDA KENJI)
広島市立大学・情報科学研究科・教授
研究者番号: 70221025

(2)研究分担者

高野 知佐 (TAKANO CHISA)
広島市立大学・情報科学研究科・准教授
研究者番号: 60509058

舟阪 淳一 (FUNASAKA JUNICHI)
広島市立大学・情報科学研究科・准教授
研究者番号: 60322377

小畑 博靖 (OBATA HIROYASU)
広島市立大学・情報科学研究科・助教
研究者番号: 30364110