Vol.2009-SE-164 No.22
Vol.2009-EMB-13 No.22
Vol.2009-CSEC-45 No.22
2009/5/29

P2P ファイル交換ソフトウェア Winny を対象としたオーバーレイネットワークの制御実験

寺田真敏　重本倫宏　仲小路博史

P2P(Peer to Peer)ファイル交換ソフトウェア利用が広がる中，P2P ファイル交換ソフトウェアから構成されるオーバーレイネットワーク自身が持つ潜在的な脅威について言及されることは少ない．本制御実験の目的は，P2P ネットワーク自身が持つ潜在的な脅威のひとつであるトラフィック誘導による P2P ネットワーク外へのサービス運用妨害攻撃について，その影響を定量的な数値として示すことと，P2P ネットワークを含むオーバーレイネットワーク制御の課題について問題提起することにある．本稿では，国内に利用者が集中している Winny を対象に，P2P ファイル交換ソフトウェアが使用するファイル所在情報(キー情報)を外的に制御することで発生しうるサービス運用妨害について，大規模ネットワーク実験環境 StarBED 上に構築した 1,000 台規模の閉域環境下での実験結果について報告する．

The experiment of the overlay network for P2P file exchange software Winny

Masato Terada Tomohiro Shigemoto
and Hirofumi Nakakoji

P2P file exchange software is spreading on the Internet. The requirements of investigation reports such as threats about P2P network are increasing. When a P2P network "Winny" has two hundred thousand of concurrently active peers, there is the risk that it could serve as a DDoS engine for attacks against a targeted host. In this paper we describe index poisoning approach to creating a DDoS engine out of a P2P network. For this approaches, the targeted host does not have to be a participant in the P2P network, and could be a web server or a mail server. Also, we show some experiment results for P2P network "Winny" enforced on StarBED that is a Large Scale Network Experiment Environment.

1. はじめに

P2P(Peer to Peer)ファイル交換ソフトウェア利用が広がる中，マルウェア流布や情報漏えいなどのコンテンツ流通について取り上げられることはあっても，P2P ファイル交換ソフトウェアから構成されるオーバーレイネットワーク(以降, P2P ネットワーク)自身が持つ潜在的な脅威について言及されることは少ない．本制御実験の目的は，P2P ネットワーク自身が持つ潜在的な脅威のひとつであるトラフィック誘導による P2P ネットワーク外へのサービス運用妨害攻撃について，その影響を定量的な数値として示すことと，P2P ネットワークを含むオーバーレイネットワーク制御の課題について問題提起することにある．

本稿では，まず，P2P ネットワークを利用したサービス運用妨害に関する事例，関連研究について報告する．次に，国内に利用者が集中している Winny を対象に，P2P ファイル交換ソフトウェアが使用するファイル所在情報(キー情報)を外的に制御することで発生しうるサービス運用妨害について，大規模ネットワーク実験環境 StarBED[1]上に構築した 1,000 台規模の閉域環境下での実験結果について報告する．

2. 関連研究

P2P 通信技術については，ネットワーク上のトラフィック分散を実現する技術として期待されている一方，2008 年 11 月に出現したマルウェア Conficker/Downadup の亜種が，感染したマシン間でアップデート操作のために P2P 通信を利用するなど，侵害活動に悪用される事例も報告され始めている[2]．本章では，P2P ネットワークを利用したサービス運用妨害に関する事例ならびに関連研究の視点から整理する．

2.1 サービス運用妨害に関する事例

文献3)，4)では 2007 年に P2P ファイル交換ソフトウェア DC++を用いたサービス運用妨害攻撃の観測について報告している．DC++には，P2P ネットワークを稼動させるための経路／検索情報の中継として機能するハブが存在する．このハブを悪用することで，1 ノード当たり 4～5 コネクションを，DC++が構成する P2P ネットワーク外にトラフィック誘導できることを示唆している．文献5)では P2P ネットワーク自体が，P2P ファイル交換ソフトウェアを使っていないユーザに接続要求を送信する状況について報告している(表 1)．これは，P2P ファイル交換ソフトウェアの稼動ノードの IP アドレスが解放され, 別のノードに同一の IP アドレスが割り振られた場合に発生するトラフィック誘導である．

† (株)日立製作所
Hitachi Ltd.

Vol.2009-SE-164 No.22
Vol.2009-EMB-13 No.22
Vol.2009-CSEC-45 No.22
2009/5/29

表 1：P2P ソフトウェアを 24 時間稼働後に終了させた場合の接続要求発生状況[5]

調査ソフトウェア	接続要求発生頻度の高い期間
Skype	利用終了後 12 時間まで
Winny	利用終了後 9 時間まで
Winnyp	
Share	利用終了後 24 時間まで

2.2 P2P を利用したサービス運用妨害

P2P モデルで構成されたファイル交換システムには，Napster[6]のようにノード情報やファイルの所在を中央サーバで管理するハイブリッド型 P2P ファイル交換システムと，Winny，Share，Gnutella のように，全ての処理を P2P で行なうピュア型 P2P ファイル交換システムがある．ピュア型の場合，P2P ネットワーク外にトラフィック誘導するサービス運用妨害の手法として，インデックスポイズニングとルーティングテーブルポイズニングが知られている[7].

(1) インデックスポイズニング

インデックスポイズニングを用いたトラフィック誘導は，P2P ファイル交換ソフトウェアが使用するファイル所在情報(インデックス情報，キー情報と呼ばれる)に格納されている IP アドレスやポート番号に，Web サーバやメールサーバなど P2P ネットワーク外のノードを指定する手法である．詐称されたインデックス情報を参照した場合，ファイル保持ノードとして誘導されたノードに接続要求を送信することになる(図 1).

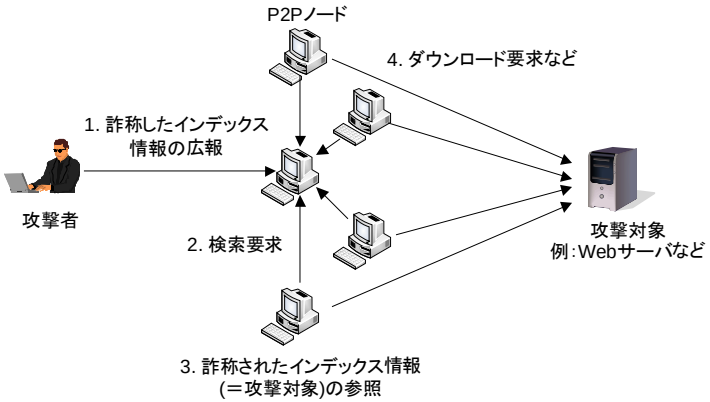

図 1：インデックスポイズニングによるトラフィック誘導

(2) ルーティングテーブルポイズニング

ルーティングテーブルポイズニングを用いたトラフィック誘導は，P2P ファイル交換ソフトウェアが使用する接続すべきノードに，Web サーバやメールサーバなど P2P ネットワーク外のノードを指定する手法である．詐称されたノード情報を参照した場合，誘導されたノードに接続要求を送信することになる(図 2).

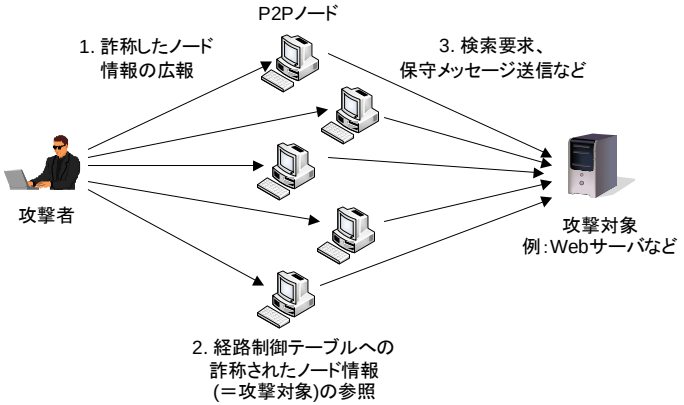

図 2：ルーティングテーブルポイズニングによるトラフィック誘導

2.3 P2P を利用したサービス運用妨害よる影響評価

文献8)では構造型 P2P(Overnet など)と非構造型 P2P(FastTrack など)を対象としたインデックスポイズニングによる流通制御について，文献 7)では P2P システムを利用したサービス運用妨害の手法として，ルーティングテーブルポイズニングを用いた場合，Overnet においてダウンストリームで平均 1.3Mbps の誘導トラフィックが発生したこと実環境での実験を通して示している．文献9)ではトラフィック誘導先を BitTorrent の Tracker(サーバの役割を果たすソフトウェア／Web サイト)として広報することで，平均 1,400TCP コネクション/秒，平均 137～176Kbps の誘導トラフィックが発生したとしている．文献10)は Gnutella を用いた Web サーバへのトラフィック誘導について，1,000 件/秒を越える Web サーバログが記録されたことを実験結果として示している．シミュレーションにより影響を把握する研究も行なわれており，文献11)は Gnutella の検索操作を対象としたサービス運用妨害について報告している．

なお，インデックスポイズニングについては，P2P ネットワーク上に不要あるいは，おとりの情報を流すことで，ファイルを取得しにくくする技術としての利用側面がある．このような不要あるいは，おとりの情報を流した場合の影響を検討した研究とし

Vol.2009-SE-164 No.22
Vol.2009-EMB-13 No.22
Vol.2009-CSEC-45 No.22
2009/5/29

て，eDonkey，FastTrack，Gnutella を対象とした文献12)，KaZaA を対象とした文献13)，Winny を対象とした文献14)，15)がある．

2.4 サービス運用妨害の回避について

文献16)ではインデックスポイズニング対策として，暗号学的にインデックスの検証を行なう Reliable Index Exchange Protocol を，文献17)では単一あるいは複数のノード検証による回避手法を提案している．

3. 制御実験の概要

本章では，制御実験の目的ならびに実験環境について述べる．

3.1 目的

本制御実験の目的は，Winny を対象に，P2P ファイル交換ソフトウェアが使用するファイル所在情報(キー情報)を外的に制御することで発生しうるトラフィック誘導について，その影響を定量的に示すことにある．

(1) **誘導によって発生するトラフィック量**

Web サーバへのアクセスを誘導するキー情報の配布により発生するダウンロード操作トラフィックを，データ転送速度，TCP コネクション確立数，TCP コネクション継続時間の視点から調査する．

(2) **トラフィックの誘発傾向**

ダウンロード条件が同一の場合，キー情報に格納されているファイル名，ハッシュ値などが異なることにより，誘発されるトラフィックに偏りが発生するか否かを確認する．

(3) **トラフィックを誘導するキー情報の残存状況**

P2P ネットワーク上に残存しているトラフィックを誘導するファイル所在情報(キー情報)の量と，誘導によって発生するトラフィック量との関係を確認する．

3.2 実験環境

3.2.1 ネットワーク構成

StarBED のグループ F に属するノード(Pentium4，メモリ 8GB，HDD80GB x 2) 125 台に，WMware ESXi を用いて 8 仮想ノード／物理ノードとした．各仮想ノード上では Windows XP と表 2 に示す設定をした Winny2.0β7.1 を稼動させ，1,000 台の Winny ノードによる P2P ネットワークを構成し(図 3)，トラフィック誘導先の Web サーバとして，Fedora Core 上に xinetd 経由で稼動する Apache 1.3.41 を用意した．

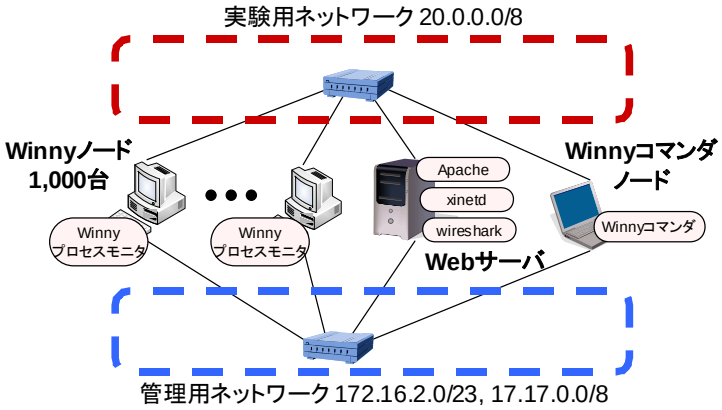

図 3：ネットワーク構成

表 2：Winny の設定(全ノード共通)

項目	設定値
回線速度	120 バイト/秒
クラスタワード (自動ダウンロード設定)	winny txt
アップロードファイル	なし

3.2.2 ツール

本制御実験において使用したツールの概要について述べる．

(1) **Winny コマンダ**

Winny コマンダは Winny ノードに接続した後，通信コマンド群を送信するツールである．図 4 に示すモジュールから構成されている．Winny コネクタモジュールは指定された IP アドレスとポート番号にアクセスして，コネクションを確立し維持する．Winny コマンダモジュールは Winny の通信で使用する通信コマンド群を送信し，通信コマンド 13 では表 3 に示すキー情報を送信する．

Vol.2009-SE-164 No.22
Vol.2009-EMB-13 No.22
Vol.2009-CSEC-45 No.22
2009/5/29

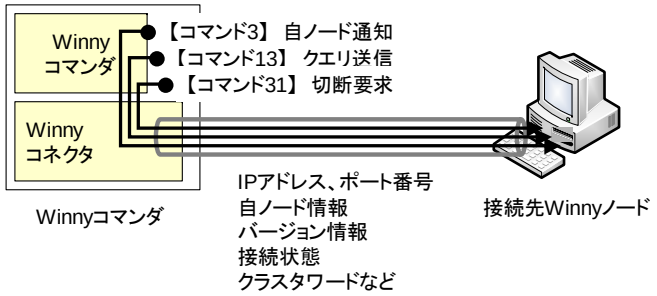

図 4：Winny コマンダのモジュール構成

表 3：Winny コマンダで送信可能なキー情報

項目	例
IP アドレス	20.20.167.1
ポート番号	2000
ファイルサイズ	2000
ファイルハッシュ	20007e0f3f06b84cee05d43bdb544b31
ファイル名	winny2000.txt
トリップ	436865636b596f75725043
TTL	1500
被参照ブロック数	112
キー更新日時	2009/01/01 01:01:01

(2) Winny プロセスモニタ

Winny プロセスモニタは, Winny.exe のメイン制御ルーチンから取得したメモリ上のタスク，キー，ノード，リンク情報を参照し，その情報を標準出力に出力する(図 5). キー情報リストでは，「IP アドレス，ポート番号，ファイルハッシュ，ファイル名」を，ノード情報リストでは接続処理中の「IP アドレス，ポート番号」を取得できる．

3.3 実験方法

本節では，3.1 節で提示した目的に対する各実験方法について述べる．

(1) 誘導によって発生するトラフィック量

キー情報に Web サーバの IP アドレス，TTL 1500 と自動ダウンロード設定のトリガ対象となるファイル名を設定した，ハッシュ値とポート番号の異なる 50 個(ポート番号 2000～2049/tcp)のキー情報を Winny コマンダ経由で実験環境の Winny ノードに配布する．さらに，15 分後，同一のキー情報 50 個を実験環境の Winny ノードに再配布する．Web サーバ上では，自動ダウンロード設定をトリガとして誘導されたトラフィックを，パケット量(wireshark にて取得)，TCP コネクション確立数(xinetd にて取得)，TCP コネクション継続時間(xinetd ログにて取得)として観測する．同様な手順で，ハッシュ値の異なるキー情報を 100 個(ポート番号 2000～2099/tcp)，150 個(ポート番号 2000～2149/tcp)とした場合について観測する．

(2) トラフィックの誘発傾向

キー情報の配布手順は，項番(1)と利用する．Web サーバ上で観測した各ポート番号へのアクセス数(xinetd ログにて取得)を用いて誘発されるトラフィックの偏りについて確認する．

(3) トラフィックを誘導するキー情報の残存状況

キー情報の配布手順は, 項番(1)と利用する. Winny プロセスモニタを用いて各 Winny ノード上のメモリに残存しているキー情報を 1 分毎に取得する．

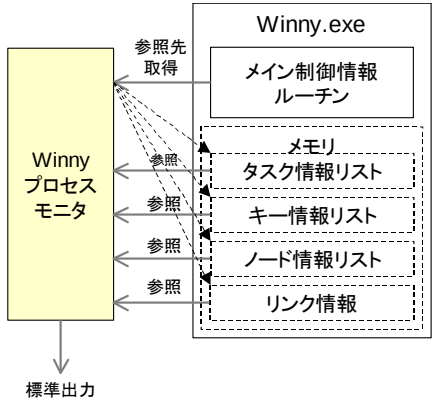

図 5：Winny プロセスモニタの概要

Vol.2009-SE-164 No.22
Vol.2009-EMB-13 No.22
Vol.2009-CSEC-45 No.22
2009/5/29

4. 制御実験結果

本章では，制御実験の結果について述べる．

4.1 観測結果

(1) 誘導によって発生するトラフィック量

(a) データ転送速度

図 6 に Web サーバとの間で発生したデータ転送速度を示す．ピーク時のデータ転送速度は約 260Kbps(パケット量は約 540pps)であり，キー情報配布数の影響をあまり受けていない．また，図 7 に示す Web サーバ宛の TPC SYN パケット数(／分)の推移からも TCP SYN パケットの送出数がキー情報配布数にあまり影響を受けていないことが見て取れる．

(b) TCP コネクション確立数

図 8 に TCP コネクション確立数(／分)の算出に利用した Web サーバ上での xinetd のアクセス件数(／分)の推移を示す．ピーク時のアクセス件数は約 1,500 件(≒25 件/秒)，キー情報配布数の影響をあまり受けていない．図 9 にキー情報配布数 150 個について，Web サーバ向けの TPC SYN パケット数(／分)，折り返しの TCP SYN/ACK パケット数(／分)，TCP コネクション確立数(／分)として xinetd のアクセス件数(／分)，発信元 IP アドレス数(／分)の推移を示す．図 9 から発信元 IP アドレス数からトラフィック発生期間中，約 900 台のノードがダウンロード操作に関与していること，トラフィック誘導が，TCP 層だけではなく，少なからず Web サーバプログラムにも負荷を与える要因となり得ることがわかる．

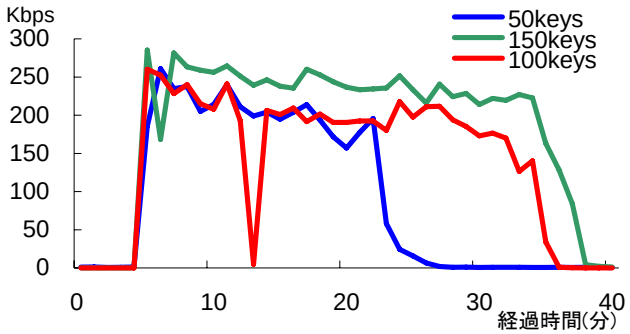

図 6：誘導されたトラフィックのデータ転送速度の推移

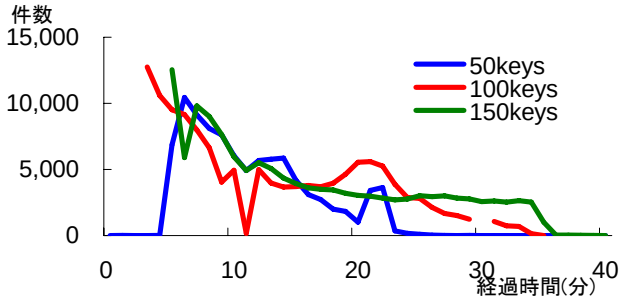

図 7：TCP SYN パケット数(／分)の推移

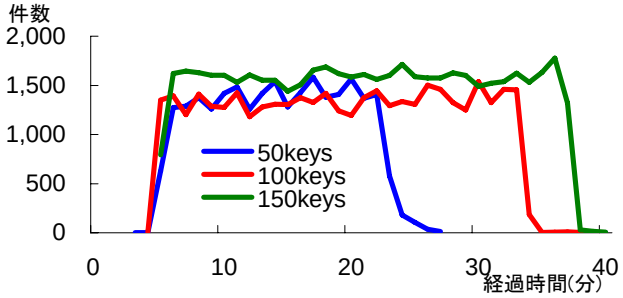

図 8：xinetd のアクセス件数(／分)の推移

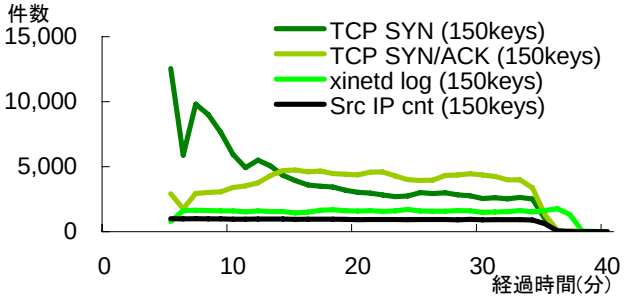

図 9：TCP パケット数と xinetd アクセス件数(／分)の推移

Vol.2009-SE-164 No.22
Vol.2009-EMB-13 No.22
Vol.2009-CSEC-45 No.22
2009/5/29

(c) TCP コネクション継続時間

図 11 にキー情報配布数 150 個について，TCP コネクション継続時間の算出に利用した Web サーバ上での xinetd の接続時間の分布を示す．0 秒から 30 秒と，300 秒前後に接続時間の分布の山が現れ，キー情報配布数 50 個，100 個の場合も同様な傾向が見られた．

(2) トラフィックの誘発傾向

図 12 にハッシュ値の異なるキー種別数(／分)の算出に利用した Web サーバ上での xinetd のポート番号の出現数(／分)の推移を，図 13 にキー毎の Web アクセス数(／分)の算出に利用した Web サーバ上での xinetd のポート番号毎のアクセス件数(／分)の推移を示す．トラフィック誘導に関する時間的な継続性の点，ハッシュ値の異なるキー毎のアクセス数頻度の点からも，ダウンロード条件が同一の場合には，キー情報に格納されているファイル名，ハッシュ値などが異なることによってトラフィックの誘発に偏りが発生していないことがわかる．

(3) トラフィックを誘導するキー情報の残存状況

Winny プロセスモニタを用いて全ノードから取得したキー情報リストから作成した，メモリに残存している Web サーバの IP アドレスが格納されたキー情報と，キー情報総件数の推移を図 10 に示す．キー情報配布直後から IP アドレスの書き換えが始まっている．また，キー情報全体の消失度合いに比べ，特定の IP アドレスが格納されたキー情報の書き換え度合いの方が早い．

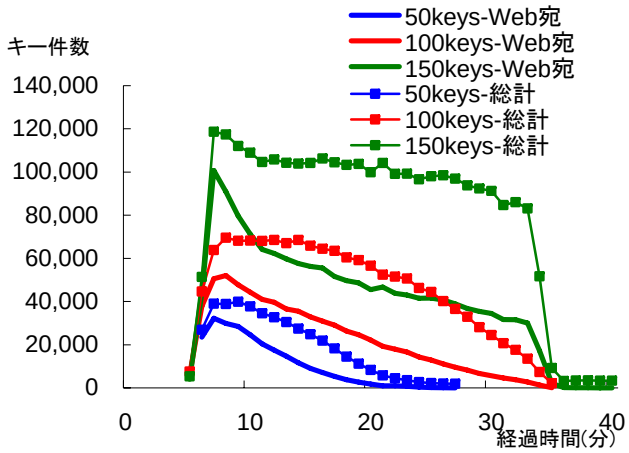

図 10：キー情報の残存状況(／分)の推移

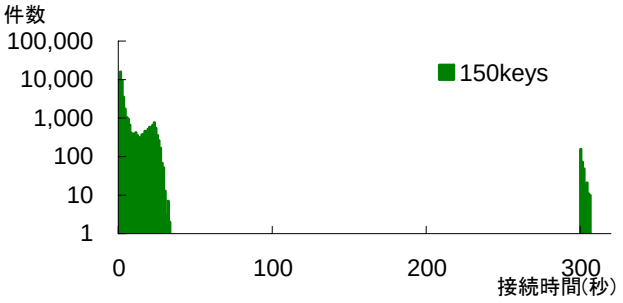

図 11：TCP コネクション継続時間

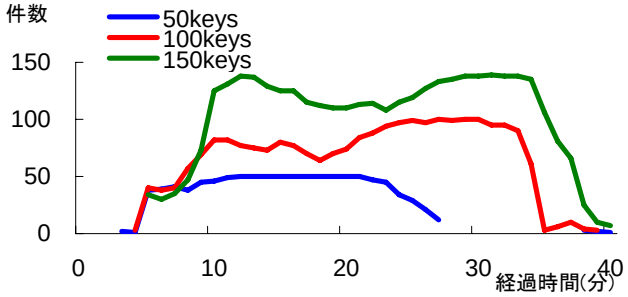

図 12：ハッシュ値の異なるキー種別数(／分)の推移

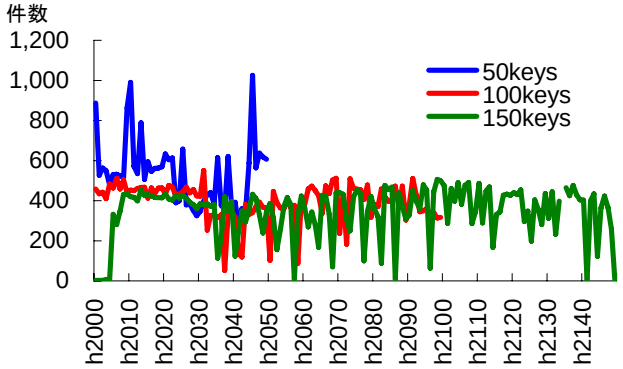

図 13：ハッシュ値の異なるキー毎のアクセス数(／分)

Vol.2009-SE-164 No.22
Vol.2009-EMB-13 No.22
Vol.2009-CSEC-45 No.22
2009/5/29

4.2 考察

(1) 誘導によって発生するトラフィック量

Web サーバとの間で発生するトラフィックの約 80%が TCP コネクション確立ならびに維持のパケットであることから，Winny におけるファイル所在情報(キー情報)を外的に制御することで発生しうるトラフィック誘導については，TCP 層に与える影響の方が大きい(図 14)．ただし，Apache のアクセス記録であるログファイルには，トラフィック誘導により図 15 に示すようなログが記録され，各ログエントリサイズ(1 行に記載されている文字数)の分布に示す通り(図 16)，250～300 バイトのログエントリサイズが約 57%を占めている．このため，キー情報を制御することによるトラフィック誘導が少なからず Web サーバプログラムに対するサービス運用妨害の要因となり得る．

(2) トラフィックの誘発傾向

図 17 にキー情報配布数 150 個について，発信元 IP アドレス毎の xinetd のアクセス総数を示す．各ノード平均 52 件であり，観測時間 40 分としてみた場合 1.3 件/分のアクセスとなる．このことからも，ダウンロード条件が同一の場合には，キー情報に格納されているファイル名，ハッシュ値などが異なることによってトラフィックの誘発に偏りは発生していないと判断できる．

(3) トラフィックを誘導するキー情報の残存状況

Web サーバの IP アドレスが格納されたキー情報の残存率(=Web サーバの IP アドレスが格納されたキー情報の件数／キー情報総件数)を図 10 から算出すると図 18 となる．

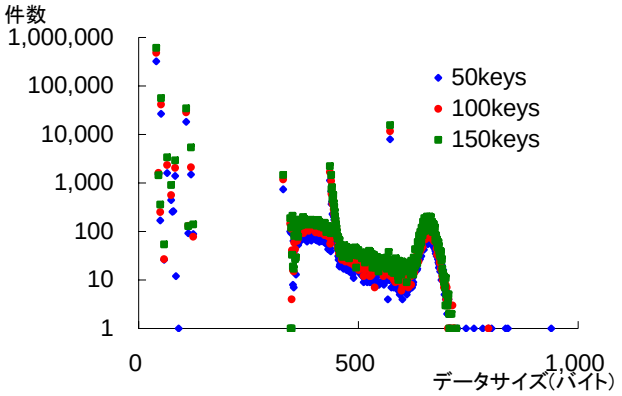

図 14：誘導されたトラフィックのデータサイズの分布

```
xx.xx.xx.xx - - [17/Feb/2009:20:47:08 +0900] "¥xb2N¥x8a ¥x9b¥xd9o¥xfa5s¥xb7" 400 -
yy.yy.yy.yy - - [17/Feb/2009:20:47:08 +0900] "¥x97¥xe2*0¥x186Dc¥x9d¥xe5¥xff¥x17¥v" 501 -
zz.zz.zz.zz - - [17/Feb/2009:20:47:09 +0900]
"¥xba8¥xcd0y(¥x8bve*¥xe8J¥xf5'¥xcb¥xca%¥x1cH¥x8d¥xf8^C¥x06¥x99
¥xab¥xfds=¥xac¥xbaGG¥x80¥xdcz'¥x05_l@¥x92¥x90¥xf6%¥xe8¥xe6)¥x15¥xaaUW¥xf8¥x1a¥xce¥xa
4b9¥xea¥x06¥x10D¥xa3¥xeb¥x0c{¥xd7}¥xc3¥x9e¥xd5¥x18¥x04m¥xbc¥xae2," 400 373
```

図 15：Winny からのダウンロード要求に伴う Apache のアクセス記録の例

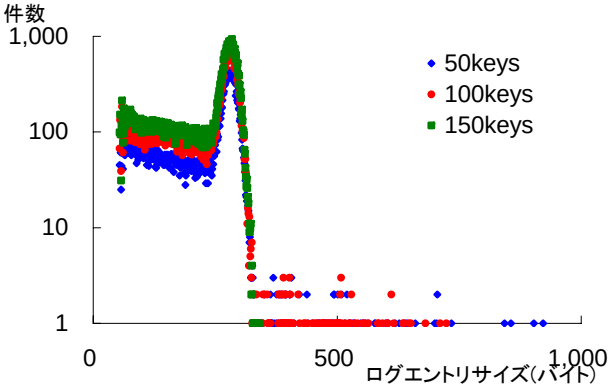

図 16：Apache のログエントリサイズの分布

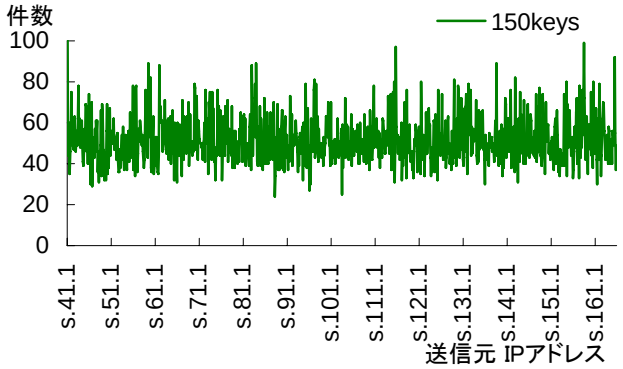

図 17：発信元 IP アドレス毎の xinetd のアクセス総数

Vol.2009-SE-164 No.22
Vol.2009-EMB-13 No.22
Vol.2009-CSEC-45 No.22
2009/5/29

これを図 7 に示す Web サーバ宛の TPC SYN パケット数(／分)の推移と比較すると，キー情報配布数のいずれにおいても類似性が見られる．このことから，トラフィック誘導は, 誘導先 IP アドレスを保持するキー情報の残存率で誘導を制御できる可能性がある．

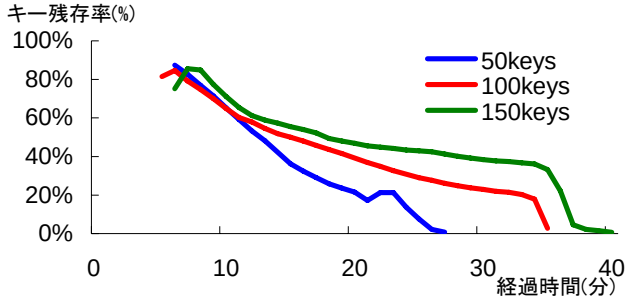

図 18：Web サーバの IP アドレスが格納されたキー情報の残存率

5. おわりに

本稿では, StarBED 上に 1,000 台の Winny ノードによる P2P ネットワークを構成し，ファイル所在情報(キー情報)を外的に制御することで発生しうるトラフィック誘導について，その影響を定量的に示した．また，Web サーバへのトラフィック誘導は，少なからず Web サーバプログラムに対するサービス運用妨害の要因となり得ることと，誘導先 IP アドレスを保持するキー情報の残存率で誘導を制御できる可能性があることを確認した．今後の課題は，キー情報の残存率を制御するなど，P2P ネットワーク自身が持つ潜在的な脅威を回避する手法についての検討が挙げられる．

謝辞

大規模ネットワーク実験環境 StarBED を本実験環境として利用するにあたりご協力を頂いた独立行政法人情報通信研究機構北陸リサーチセンター，ICT 研究開発機能連携推進会議(HIRP)の関係者各位に深く感謝致します．また，StarBED 上の実験環境構築にあたり，有益な助言と協力を頂いた北陸先端科学技術大学院大学ならびに，独立行政法人情報通信研究機構北陸リサーチセンターの篠田陽一教授，三輪信介氏，宮地利幸氏，太田悟史氏，安田真悟氏に深く感謝致します．

本研究は総務省から委託を受けた「ネットワークを通じた情報流出の検知及び漏出情報の自動流通停止のための技術開発」の支援を受け実施している．本研究を進めるにあたって有益な助言と協力を頂いた関係者各位に深く感謝致します．

参考文献

1) StarBED Project
http://www.starbed.org/
2) トレンドマイクロ: "DOWNAD/Conficker Watch: New Variant in The Mix?", (2009-04-08)
http://blog.trendmicro.com/downadconficker-watch-new-variant-in-the-mix/
3) Prolexic Technologies: "P2P DDoS Attacks", (2007-05-14)
http://www.prolexic.com/content/moduleId/tPjJLKRF/article/aRQNVcBH.html
4) Prolexic Technologies: "Prolexic Announces New Capabilities to Defend Against Peer-to-Peer DDoS Attacks", (2007-05-23)
http://www.prolexic.com/content/moduleId/tPjJLKRF/article/L48MY9L7.html
5) 松崎吉伸: "P2P ソフトウェア利用の余波", (2008-09-10)
http://www.scat.or.jp/stnf/contents/p2p080910.html
6) Napster, http://www.napster.com/
7) N. Naoumov and K. Ross, "Exploiting P2P Systems for DDoS Attacks", Proc. of INFOSCALE (2006)
http://cis.poly.edu/~ross/papers/p2pddos.pdf
8) J. Liang, N. Naoumov and K. Ross, "The index poisoning attack in P2P file-sharing systems", Proc. Infocom (2006).
http://cis.poly.edu/~ross/papers/poison.pdf
9) K. El Defrawy, M. Gjoke and A. Markopoulou, "BotTorrent: Misusing BitTorrent to Launch DDoS Attacks", Proc. of the 3rd USENIX Workshop on Steps to Reducing Unwanted Traffic on the Internet Table of Contents (2007)
http://www.ece.uci.edu/~athina/PAPERS/BotTorrent.pdf
10) E. Athanasopoulos, K.G. Anagnostakis, and E.P. Markatos, "Misusing Unstructured P2P Systems to Perform DoS Attacks: The Network That Never Forgets", Proc. ACNS (2006).
http://dcs.ics.forth.gr/Activities/papers/gdos.acns06.pdf
11) N. Daswani and H. Garcia-Molina, "Query-Flood DoS Attacks in Gnutella", CCS (2002).
http://infolab.stanford.edu/~daswani/papers/p115-daswani.pdf
12) N. Christin, A. S. Weigend, and J. John Chuang, "Content Availability, Pollution and Poisoning in Peer-to-Peer File Sharing Networks", ACM E-Commerce Conference (2005)
http://p2pecon.berkeley.edu/pub/CWC-EC05.pdf
13) J. Liang, R. Kumar, Y. Xi and K. Ross, "Pollution in P2P File Sharing Systems", Proc. of IEEE INFOCOM (2005).
http://cis.poly.edu/~ross/papers/pollution.pdf
14) 吉田雅裕，大坐畠智，川島幸之助, "P2P ファイル共有ネットワークにおけるファイル ID 検索に対応したポイゾニング手法の提案", 信学技報, vol. 108, no. 31, NS2008-9, pp. 49-54, 2008 年 5 月
15) 吉田雅裕，大坐畠智，中尾彰宏，川島幸之助, "Winny ネットワークにおけるインデックスポイズニングの適用と評価", 信学技報, vol.108, no.203, NS2008-58, pp.93-98, 2008 年 9 月
16) X. Lou and K. Hwang, "Prevention of Index-Poisoning DDoS Attacks in Peer-to-Peer File-Sharing Networks," IEEE Trans. on Multimedia, Special Issue on Content Storage and Delivery in P2P Networks, November, 2006.
http://gridsec.usc.edu/files/TR/IEEE-TMM-Special-Issue-P2P-Nov8-06-Hwang.pdf
17) Xin Sun, Ruben Torres and Sanjay Rao, "Preventing DDoS Attacks with P2P Systems through Robust Membership Management", Technical Report TR-ECE-07-13, Purdue University (2007)
http://cobweb.ecn.purdue.edu/~isl/TR-EE-07-13.pdf