SYNパケットの呼応に着目したP2Pトラフィックの表示

三浦明日香[1]　梅村恭司[2]　阿部洋丈[2]　岡部正幸[3]
豊橋技術科学大学院情報工学専攻[1]　豊橋技術科学大学 情報工学系[2]
豊橋技術科学大学　情報メディア基盤センタ[3]

1．はじめに

Ｐ２Ｐ通信はファイル共有などで著作権の侵害の温床になっている。またウィルスがＰ２Ｐ通信を通じて蔓延し、機密情報や個人情報が漏れるという事件も起きていて重大な社会問題にもなった。

このことから手軽にＰ２Ｐトラフィックを特定することで注意を促し、事故を未然に防ぐ手助けが出来るツールがあればいいのではないかと考え、Ｐ２Ｐトラフィック表示ツールの作成を行った。

2．Ｐ２Ｐトラフィック

Ｐ２Ｐは、特定のサーバを持たず対等の役割を果たす各ノードが状況に応じてサービス利用者になったり提供者になったりする。実際の接続手順でも、ピアは受動的に接続を受け付ける一方で、能動的に他のノードへ接続を要求する側となる。

Ｐ２Ｐトラフィックの特定方法は他の研究でも様々な手法が検討されている[1][2]。今回の表示ツールではＳＹＮパケットフラグの呼応に着目した。ＳＹＮパケットフラグは通常クライアント側から出されるが、Ｐ２Ｐのようにサーバとクライアントの役割が一定でないノード間では双方向からのＳＹＮパケットフラグが観測される。このＳＹＮパケットフラグの呼応がＰ２Ｐトラフィックの弁別に有用であることは他の研究[3]でも行われている。

このＰ２Ｐトラフィックを特定したいと考えたため、Ｐ２Ｐトラフィックの可視化ツールを必要だと考えた。

A method of showing P2P traffic based on correlated pairs of SYN packets.
Asuka Miura[1] Kyouji Umemura[2]
Hirotake Abe[2] Masayuki Okabe[3]
Toyohashi University of Technology[1]
The Department of Information and Computer Sciences Toyohashi University of Technology[2]
Information and Media Center Toyohashi University of Technology[3]

3．実験環境

Ｐ２Ｐトラフィックを得るために実験環境（図１）の作成を行った。Ｐ２Ｐトラフィックのターゲット以外も稼動しているような環境ではどのトラフィックがターゲットなのか分かり辛い。そこで、Ｐ２Ｐ以外のトラフィックが極力少ない、ターゲットのふるまいを正確に分析できるトラフィックを得られる環境が必要であると考えたからである。３台のサーバマシンと３台のクライアントマシンを使い、仮想マシンを用いて仮想空間を作りネットワークを構築した。その中でＰ２Ｐソフトを動作させパケットキャプチャを行った。

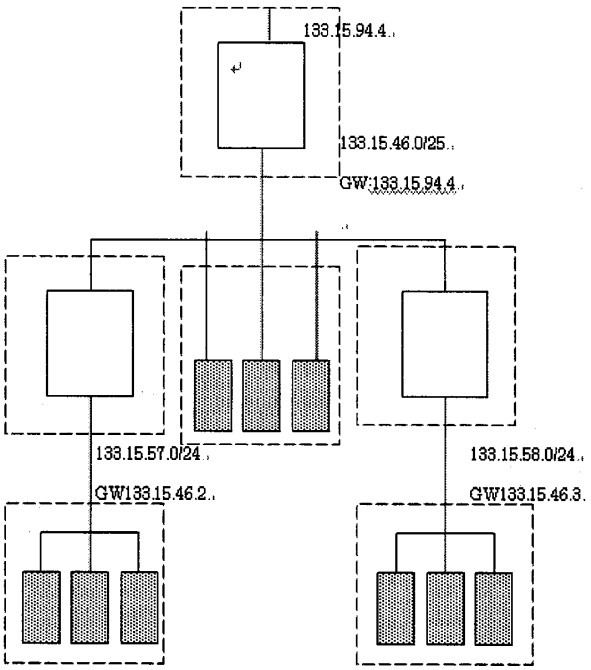

図１：実験環境のネットワーク構成

実験環境を構築する際に、Ｐ２ＰソフトはＷｉｎｎｙ[4]、仮想マシンはＶMware を用いた。

パケットキャプチャソフトにはＷｉｒｅＳｈａｒｋ[5]を用いた。

４・プログラムの概要

今回のプログラムはＷｉｒｅＳｈａｒｋのパケットダンプファイルを読み込んで表示する。パケットダンプのファイルは時間データとパケットが時系列順に並べられている。パケットダンプファイルを読み込み、画面上に通信が行われた区間の表示を行えるものとした。その上で表示する時間の指定が行えるもの、Ｐ２Ｐトラフィックを特定できるものをとる。

作成したプログラムが図２である。画面上部にある「Open」ボタンからＷｉｒｅＳｈａｒｋでパケットキャプチャしたファイルを選択する。「draw」で描画を開始する。

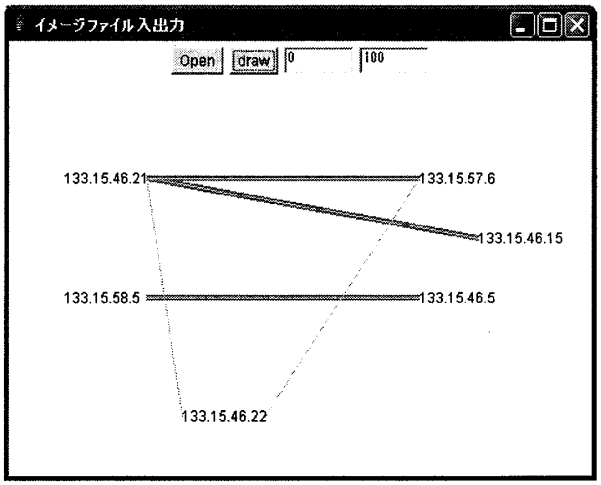

図２：プログラムの画面

・　表示する時間の指定

テキストボックスが二つあり、左に開始時刻、右に終了時刻を入力し、指定することが出来る。開始時刻、終了時刻共にファイルの最初から計測時刻である。指定することで開始時刻から何秒後に何処で通信が行われていたかを調べることができる。テキストボックスに数字の入力をせずに描画を行った場合はファイルのトラフィックが最初から最後まで描画されることになる。

・Ｐ２Ｐトラフィックの特定

トラフィックの中で、特にＰ２Ｐ通信と考えられるものは他の通信とは異なる表示をした。今回の方法として、ＳＹＮパケットの呼応が確認された場合に赤い線で表示されるようになっている。線の太さでも区別がつくように赤線は平常の線より太くなっている。

一定時間の閾値は、ＳＹＮパケットの呼応が行われている例100件を調べ、100件の呼応時間の平均をとり0.022秒とした。

今回使用したトラフィックはＰ２Ｐ以外のトラフィックはほぼ無いが、画面（図２）を見るとＰ２Ｐ通信ではないと判定されている通信が存在する。これは誤判定である。誤判定が起きた原因は、今回の実験に用いた他の通信は接続と切断を繰り返しているため検出が出来たがこのアドレス間ではデータのやりとりを行っていたため検出が出来なかった。これは検出方式の特性を示しているものといえる。

５．今後の課題とまとめ

今回は、まだこのツールが実際に有効であるか検証を行えていない。今後、実験環境以外でのトラフィックでこのツールを使えるか検証する。

謝辞

この研究は，平成２０年度科学研究補助金課題番号(19500120)の研究成果です。

参考文献

[1] 松田 崇　中村 文隆　若原 恭　田中 良明　大崎 淳　千田 浩一　加藤 圭　飯塚 正 PureP2P ファイル共有トラヒックの特性解析 信学会技術研究報告. NSIEICE Vol.105, No.627(20060223) pp. 133-136 NS2005-191 ISSN:09135685

[2] 松田 崇　中村 文隆　若原 恭　田中 良明 P2P 弁別のためのトラヒック特徴量の提案(トラヒック，一般)信学会技術研究報告. NSIEICE Vol.105, No.12(20050414) pp. 5-8 NS2005-2 ISSN:09135685

[3] 松田 崇　中村 文隆　若原 恭　田中 良明 相互接続における順逆接続間隔を利用した P2P トラヒック弁別手法　信学会技術研究報告. NSVol.106, No.577(20070301) pp. 415-420 NS2006-237

[4] 金子　勇、Winny の技術、ASCII、東京、2005

[5] Chris Sanders, 園田 道夫, 一瀬 小夜,実践 パケット解析 Wireshark を使ったトラブルシューティング,オライリー・ジャパン,2008