6W-7

ハイブリッド型 P2P アプリケーショントラヒック制御方式の一考察

伊藤　洋†　　貫名　東†　　大坐畠　智††　　川島　幸之助††

†東京農工大学工学部情報コミュニケーション工学科

††東京農工大学大学院共生科学技術研究院

1. はじめに

近年 ADSL，光ファイバー回線の普及によるインターネットの高速化と一般家庭での常時接続環境がほぼ整いつつある．インターネットの利用形態も日々変化しており，クライアントサーバ型通信から，Peer-to-Peer(P2P)通信がインターネットトラヒックの大きな部分を占めるようになっており，他のアプリケーションの通信品質に大きな影響を与えている．これまでのインターネットトラヒック制御は，それぞれのトラヒックのアプリケーションをポート番号[1]やシグニチャマッチング[2]により特定し行われてきた．

本論文では，ハイブリッド型 P2P アプリケーションのオーバレイネットワーク構築の際の手順に注目し，オーバレイネットワーク構築を未然に防ぐことにより，ファイル交換を遮断する方式を提案する．ファイアウォールシステムを試作し，WinMX[3]でその評価を行う．

2. トラヒック制御方式

2.1 WinMX 検索ネットワーク構築手順

WinMX の P2P ネットワーク構成は，ハイブリッド P2P 型と呼ばれている．これは，中央サーバ型のファイル交換機能と，レジューム機能を搭載している．WinMX ネットワークに接続する端末は，はじめに中央サーバに接続し，自分がアップロードしているファイル情報を送信し接続が完了する．サーバは，接続している WinMX ユーザのファイル情報を管理し，ユーザからのファイル検索要求を受け付ける．WinMX におけるファイル交換の手順を図 1 に示す．

手順 1.，2.　中央サーバを検索するため，ルートとなるサーバ(IP アドレス，www.winmx.com)にアクセスする．ルートサーバは中央サーバ情報を返す．

手順 3.　中央サーバにログオンし，端末情報，アップロードするファイル情報を送信する．

端末から，ファイルの検索要求を出し，中央サーバが検索を行う．

手順 4.　検索要求に合致したファイル情報がサーバにあれば，そのファイルを所有する端末情報を送信する．

手順 5. ファイルのダウンロードに必要な情報を得た端末は，ファイルを所有する端末にアクセスし，ダウンロードを行う．

上記の手順 1-5 を繰り返し、ファイル交換が行われる．

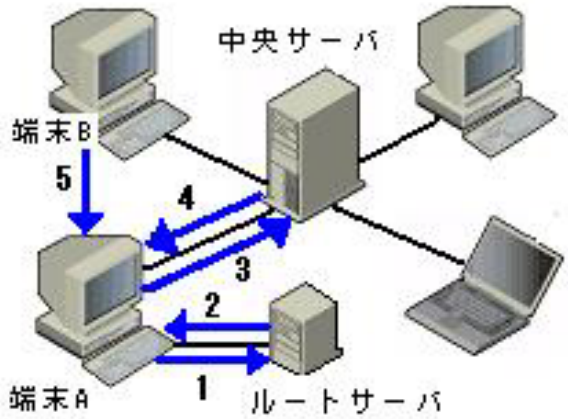

図 1　　WinMX 検索手順.

2.2 WinMX トラヒック制御方式

今回、WinMX のオーバレイネットワーク構築を制御する方式として，WinMX 独自のオーバレイネットワーク構築手法に注目し，ファイル検索，交換トラヒックを完全に遮断する方法を提案する．具体的には，節 2.1 で示したように，ユーザが WinMX を実行した際，中央サーバを検索するためにルートサーバに必ずアクセスしている点に着目した．ルートサーバへの接続を禁止することで WinMX が使用不可能になる．

ルートサーバの IP アドレスを調査した結果，以下の 4 つを特定した．

66.98.186.**，66.132.146.**，216.127.74.**，64.246.15.**

“A traffic control method for a hybrid type P2P application,” Hiroshi Ito, Azuma Nukina, Satoshi Ohzahata, Konosuke Kawashima.

WinMX 利用者端末から，上記アドレスを送信先とするパケットを破棄することによって，WinMX のオーバレイネットワークが構築できないことになる．そこで，図 1 で示した，端末 A，インターネット間に，ファイアウォール(以下 FW)サーバを構築し，端末からルートサーバへのアクセスを禁止する設定を行う．

2.3 トラヒック制御の実装方式

WinMX トラヒック制御を行うため，FW サーバの実装環境として，CPU 366MHz，メモリ 192MB，OS RedHatLinux7.3 にファイアウォールを設定するアプリケーションに iptables-1.2.7a-2(以下 iptables)を使用した．WinMX3.5.3.0，WinMX を(以下 WinMX)端末 A で実行した場合に WinMX ピアネットワークの状態を調べる実験を行った．iptables は，端末 A と FW サーバ間のネットワークを送信元とし，節 2.2 で示した 4 つのルートサーバを送信先とするパケットについて，パケット情報をログに保存した後，破棄する設定を行う．その際，4 つのルートサーバアドレスの内，3 つが WinMX ホームページのドメイン名(www.winmx.com)と一致しているため，それらの 80 番ポート以外のパケットについてログの保存とパケット自体の破棄を行う．

2.4 動作確認

FW サーバにおいて，2.3 で示した WinMX トラヒック制御を行わなかった場合と，行った場合について，図 2 における端末 A が，WinMX を実行した際の送受信パケットを監視することで，WinMX トラヒック制御の動作確認を行った．端末 A でのパケット監視のためにフリーソフトツール，NEGiES[4]を使用した．FW サーバで，トラヒック制御を行わなかった場合の端末 A で取得したパケットの一部を表 1 に，また，トラヒック制御を行った際の監視パケットの一部を表 2 に示す．

表 1，2 の IP アドレスにおいて，192.168.0.2 が端末 A，216.127.74.**がルートサーバ，154.201.27.**が中央サーバを表す．

表 1 よりトラヒック制御を行わなかった場合は，ルートサーバに接続した後(パケット番号 2)，中央サーバと接続し(パケット番号 33)，WinMX が使用可能な状態に移行する(パケット番号 35 以降)．

一方で，表 2 よりトラヒック制御を行った場合は，ルートサーバとの接続が確立せず，4 つのルートサーバに接続を試み続けることになる．中央サーバとの接続が不可能であり，WinMX でファイル検索及び，交換が可能な状態に移行することはない．

表 1　トラヒック制御を行わなかった場合のパケット測定結果.

パケット番号	送信元アドレス	送信先アドレス	TCP フラグ
1	192.168.0.2	216.127.74.**	SYN
2	216.127.74.**	192.168.0.2	ACK,SYN
3	192.168.0.2	216.127.74.**	ACK
.			
12	192.168.0.2	216.127.74.**	ACK,FIN
.			
33	192.168.0.2	154.201.27.**	SYN
34	154.201.27.**	192.168.0.2	ACK,SYN
35	192.168.0.2	154.201.27.**	ACK

表 2　トラヒック制御を行った場合のパケット測定結果.

パケット番号	送信元アドレス	送信先アドレス	TCP フラグ
1	192.168.0.2	216.127.74.**	SYN
8	192.168.0.2	216.127.74.**	SYN
9	192.168.0.2	216.127.74.**	SYN
10	192.168.0.2	216.127.74.**	SYN
.			
20	192.168.0.2	64.246.15.**	SYN
.			
25	192.168.0.2	64.246.15.**	SYN
.			
28	192.168.0.2	66.98.186.**	SYN

3. おわりに

本論文ではハイブリッド型 P2P アプリケーションである WinMX のトラヒック制御方式を提案した．ファイアウォールを試作することにより，その有効性を確認した．本方式は他のハイブリッド型 P2P アプリケーションに対しても有効であると考えられるが，その検証は今後の課題とする．

参考文献

[1] M. St. Johns and G. Huston,
"Considerations on the use of a Service Identifier in Packet Headers," RFC 3639, 2003.
[2] S. Sen, O. Spatscheck and D. Wang, "Accurate, Scalable In-Network Identification of P2P Traffic Using Application Signatures," Proc. of ACM WWW'04, 2004.
[3] WinMX, http://www.winmx.com
[4] NEGiES,
http://hp.vector.co.jp/authors/VA036210/