Symmetric NAT に対応する TCP/UDP NAT 越えの新技法

魏 元　後藤 滋樹　山田 大輔　吉田 傑
早稲田大学大学院 基幹理工学研究科 情報理工学専攻

本論文は NAT 越えの新しい技法を提案する。従来から幾つかの NAT 越えの方法が提案されている。本論文は、従来の方法では最も難しいとされている Symmetric NAT を越える方法を提案する。ここで提案する方法の特徴は，NAT のポートマッピングを予測して、通信に使用できるポートを多数オープンする。これにより、NAT を経由する通信が成功する確率を高める。この方法を UDP Multi Hole Punching と呼ぶ。本論文では新しい方法を実装してその特性を評価・考察する。併せて家庭用ルータに対応した TCP Hole Punching の新しい手法も提案する。

1　既存の技術

NAT 下のホストからでも P2P 通信を可能にするために、NAT 越え (NAT traversal) の研究が TCP、UDP の両方を対象として研究されている。UDP の NAT 越えについては、既に UPnP、Teredo、STUN[2] などの方法が提案されている。UPnP はルータ自体が UPnP に対応しなければならない。また特定のソフトウェア以外の動作を保障していないメーカーもある。UPnP は広く知られている方法であるが、万全とはいえない。また Teredo と STUN は Symmetric NAT を越えられるか、という問題がある。さらにメーカー独自のセキュリティ機能により NAT 越えが阻害さえるという問題がある。

TCP の NAT 越えについても盛んに研究されている。既に STUNT、P2PNAT、NAT Blaster などが提案されているが、まだ万全とはいえず、課題が残っている。

2　提案手法の概要

本論文では、2 台のサーバとの通信を用いて port prediction を行う。また小さい値の TTL を設定した UDP パケットを大量に送ることにより、Multi Hole Punching を実現する。システムの概要を図 1 に示す。さらに、ルータのセキュリティ (SPI) 機能に対応した TCP Hole Punching の新規手法も併せて提案する。これは Hole Punching によるパケット送受信のタイミング制御や通信例外処理の接続サポートにより実現する。

3　提案手法の特徴

自然な UDP 通信

提案手法では、Hole Punching をする Echo Server 側では、小さい値 (2 ～ 3) の TTL を設定して、NAT b を通り抜けるが、NAT a には到達しないようにする。これにより、図 1 の F8 ～ F11 のように、NAT a および NAT b の双方から見て通常の UDP 通信と同様に扱われる。このようにすると、NAT のセキュリティ機能によるパケット破棄の可能性を下げることができる。

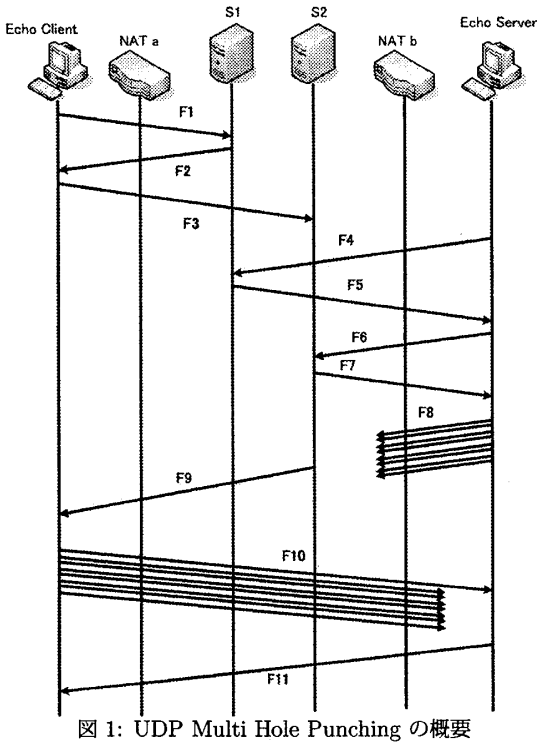

図 1: UDP Multi Hole Punching の概要

正確なポート予測

多くの NAT のポート変換アルゴリズムはインクリメント型、デクリメント型、一個飛び型、その他（ランダム型）である。本提案では 2 台のサーバを使うことにより、インクリメント型、デクリメント型、一個飛び型、のいずれにも対応できる。

発信ポートをコントロール

提案手法では通信に使うポートを固定してから使う。このようにすることで、NAT のポート変換アルゴリズムがランダム型の場合でもコントロールできる場合がある。ソースポートが「x, x+1, x+2...」のように送った場合には、「n, n+1, n+2 ...」のように規則正しくポート変換される。

1000 個の異なるポートから送る

1000 個の異なるポートから送り合うことで、NAT a が想定外のポート変換をするときでも、Echo Server 側の NAT b のマッピングと一致していれば P2P 通信が成り立つ。これにより、NAT 越えが成功する確率を高めることができる。

SPI 機能を考慮した TCP 通信

SPI (Stateful Packet Inspection) は、最近の多くの NAT に搭載されている TCP 通信におけるフィルタリング機能である。SPI が適用されている場合には、NAT を通過するパケットの順序は、必ず次のようでなければならない。

1. [SYN] - out
2. [SYN, ACK] - in
3. [ACK] - out

NAT は、このパターンに反するパケットを破棄する。本論文で提案する手法では各 NAT の動作を調べて、このような場合でも破棄されないような通信方法を探る。

4 実証実験

4.1 実験の概要

実験 1 (WinStun を使った NAT の分類) および実験 2 (パケットキャプチャ) で Symmetric NAT ルータを識別する。WinStun は Stun を使って NAT 越えをできるかどうか、またどのような性質 [3] の NAT なのかを測定するソフトである。

実験 3 では、提案手法との比較のために Skype による NAT 越えの実験をする。

実験 4 では、提案手法による NAT 越えの実験をして、Skype の結果と比較する。

実験 5 では、提案手法による Symmetric NAT 以外の NAT に対して、UDP ではなく TCP 通信の実験をする。

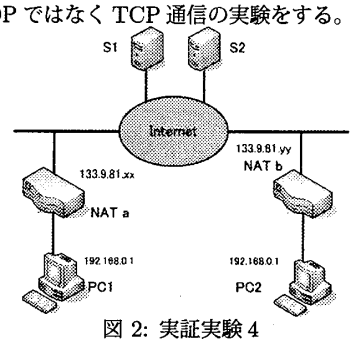

図 2: 実証実験 4

4.2 Symmetric NAT の判定

実験 1 での WinStun の判定結果の集計と実験 2 の結果から、今回の実験の対象とした 9 種類のルータの内で 3 台が Symmetric NAT の挙動をするルータであると判定した。

4.3 実験 3 の考察

Skype の正確な動作は公開されていない。実際に検証してみると、Skype の通信には 3 種類の通信方法が存在する。その 3 種類は UDP による P2P 通信と UDP の中継通信 (UDP-RELAY) と TCP の中継通信 (TCP-RELAY) である。今回の調査の対象としたルータの場合には、Skype の UDP による P2P 通信の割合が 46% であった。この事実から通信の品質が下がらない場合は、Skype は UDP Hole Punching を積極的に実行しないと推測される。また Symmetric NAT の場合は P2P 通信を行わない (0%)。

4.4 実験 4 の結果

提案手法を用いて、発信ポートをコントロールすることができた。また特定のルータの組み合わせで成功率が 80% であった以外は、すべて P2P 通信に成功した。さらに本論文の目的である、Symmetric NAT ルータの組み合わせに対しては、すべて通信に成功した。

4.5 実験 5 の結果

今回の実験のために用意した Symmetric NAT 以外の 6 種類の NAT で，実装したプログラムを検証したところ、1 種類を除く 5 種類の NAT で TCP Hole Punching が成功した。

5 結論

本論文では、2 台のサーバとの通信による port prediction と、小さい TTL の値に設定した UDP パケットを大量に送ることによる UDP Multi Hole Punching の方法を提案した。また提案手法を実装して、その特性について評価し、考察を行った。今回の実証実験の結果、提案手法のほうが既存の方法よりも優れていることが分かった。また Symmetric NAT でない家庭用のルータにおいても、試用した 6 種類中で 5 種類の NAT に対して TCP Hole Punching が成功した。

表 1: 従来の方法との比較 (実験 1,2,4 の結果を比較)

	WinStun	Skype	提案手法
Symmetric NAT	33%	0%	100%
すべてのルータ	66%	46%	99%

6 今後の課題

本論文の提案手法では、ある特定のルータの組み合わせでは数回に一回 P2P 通信に失敗した。この原因を今後探求する必要がある。また一瞬ではあるがポートを 1000 個開けるときにリソースが大量に使われている恐れがある。その点をさらに調査検討する必要がある。最後に提案手法にある低 TTL のパケットを大量に送ってポートを開けるアイディアを TCP Hole Punching に応用できるか否かを検討することは意義があると考えている。

参考文献

[1] 村山公保『基礎からわかる TCP/IP ネットワーク実験プログラミング』第 2 版，オーム社開発局 (編)，株式会社オーム社，2002.

[2] Rosenberg, J., Weinberger, J., Huitema, C., and R. Mahy, "STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)", RFC 3489, March 2003.

[3] F. Audet, Ed., C. Jennings, "NAT Behavioral Requirements for Unicast UDP draft-ietf-behave-nat-udp-08", October 10, 2006.

[4] 魏　元，"SymmetricNAT に対する UDP Multi Hole Punching の技法"，早稲田大学 理工学部 卒業論文, 2007, http://www.goto.info.waseda.ac.jp/~wei/file/wei.pdf