6X-3

TCPにおけるSTUNを用いた対称型NAT越え手法の実装と評価

黒田隼之輔† 中山泰一†

†電気通信大学 情報工学科

1 はじめに

近年，IPv4のアドレス空間の不足問題が深刻化しており，近い将来に国内におけるIPv4アドレスが枯渇すると予想されている．このIPv4におけるアドレス枯渇問題に対する解決策の1つとしてNAT(Network Address Translation)があり，様々な環境において用いられている．

NATは，1つのグローバルIPに対し複数のプライベートIPを割り当てることができるため，アドレス空間の拡張には有効な手段である．しかし，これらを用いた環境においては，プライベートIPの割り当て及びアドレス変換によるアドレスの隠蔽や，NATに付帯して実装されているフィルタリング機能によりホスト間の直接接続が困難になるという問題点が存在し，結果として一部のP2P Applicationが動作しないということが予想される．

これらの問題に対しては既にSTUN[1]，TURN[2]などの技術が存在し，多くの種類のNATについてはそれを越えた通信の確立が可能となっている[3]．しかし，NATの挙動は標準化されておらず，これらの技術では越えることのできないNATが存在する．

本論文では，そのような既存の技術を用いて越えることの難しいNATの1つである対称型NATにおいて，NATを越えてTCP通信を確立する手法の実装及び評価を行った．

2 関連研究

2.1 Hole Punching

Hole Punchingとは，NAT内ホストと外部サーバ（STUNサーバ）との通信に際し行われるアドレス変換を，他のNAT外ホストから用いることでNATの外側からの接続を開始するという手法である．STUNは主にこの技術を用いて，NATの外側からの通信開始を可能にしている．

STUN-based connection sequence through symmetric NATs for TCP connections

Junnosuke KURODA† and Yasuichi NAKAYAMA†

†Department of Computer Science, The University of Electoro-Communications, Chofu, Japan

kuroda-j@igo.cs.uec.ac.jp

2.2 対称型NATの特徴と問題点

対称型NATはRFC3489及びRFC4787[4]で定義されている中で最も通信に関する制限の厳しいものである．対称型NATの特徴として，宛先アドレスとポートを用いて接続先を区別し，一つの接続先に対し一つのアドレス変換を用いる（図1）．

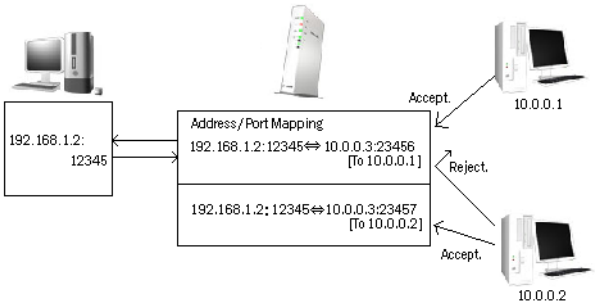


図 1: 対称型NATの動作

この特徴により，対称型NATに対してSTUNを用いた場合，STUNサーバとの接続のために生成されたアドレス変換は他のホストとの接続には適用されないため，NATの外側からの接続要求が配送されずNATを越えた通信路の確立を行うことができないという問題が存在する．

2.3 対称型NATに対する研究

対称型NATに対しては既に，多数のHole Punching を行い接続確立の可能性を高めるMulti Hole Punching[5]やポート番号予測を用いた手法が提案されている．しかしながら，これらの研究は主にUDP通信におけるものが多く，それと比較してTCP通信に対する研究は少ないといえる．

3 実装

本論文では，STUNを拡張することで対称型NATを越えてNATの外側からTCP通信を開始する手法の実装を行った．本手法の通信開始から通信確立までのシーケンスを図2に示す．また，本手法ではSTUNプロトコルに基づいてNAT-Bind，NAT-Connectという新たなメソッドを定義した．また，図2内のClientは対称型NATの外側にあるホストを，ServerはSTUN

Copyright ©2011 Information Processing Society of Japan.
All Rights Reserved.

サーバを，NAT-Client は対称型 NAT の内側にいるホストを指し，括弧内の語句は STUN に準拠したクラス名を表している．以下に接続確立までの流れを示す．

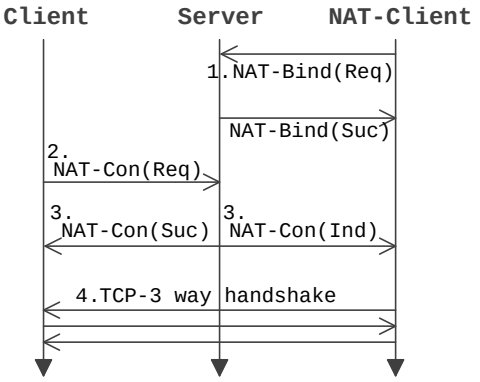


図 2: 提案手法のシーケンス

1. NAT 内ホストからサーバへ NAT-Bind パケットを送信する．これによりサーバは対応する ID を持つホストが対称型 NAT 内にいることを記憶する．
2. NAT 外ホストからサーバへ NAT-Connect パケットを送信し，NAT 内ホストへの接続を要求する．
3. サーバが NAT 内，外双方のホストへ NAT-Connect パケットを送信する．これにより NAT 外ホストは NAT 内ホストからの接続を待ち，NAT 内ホストは NAT 外ホストへの接続を開始する．
4. NAT 内，外ホストの間で 3 way handshake が行われ，通信が確立する．

4 実験と評価

4.1 実験環境

本手法の評価実験において用いた環境を表 1 に示す．

表 1: 評価における計算機環境

ホスト	使用したオペレーティングシステム
NAT-Client	Virtual PC 上の WindowsXP
Server	Windows7
Client	Windows7

対称型 NAT としては，Microsoft Virtual PC における仮想マシンへのアドレス変換法則が対称型 NAT と同様であるためこれを用い，実装には C 言語を用いた．

4.2 評価

実験環境において本システムを動作させたところ，NAT 外ホストからの接続によって NAT 内ホストとの接続を確立させることができた．また，接続にかかる時間を NAT 外ホストの接続要求の送信から NAT 内ホストからの ACK の受信までとして，WireShark によるパケットキャプチャリングにより計測した．この結果をまとめたものが表 2 である．

表 2: 接続時間の計測結果

実験環境	計測時間 (単位 msec)
NAT 内–外，本システムあり	5.3
NAT 外–外，本システムあり	5.2
NAT 内–外，本システムなし[1]	1.4
NAT 外–外，本システムなし	1.5

5 おわりに

本論文では対称型 NAT 内ホストに対し NAT 外ホストから接続を開始することを可能にするシステムの実装及び評価を行った．結果として NAT 外ホストを起点とする NAT 内ホストへの接続は可能であり，その際に本システムを用いることで 4msec 程度の時間的オーバヘッドが掛かることが解った．このオーバヘッドは，接続の開始時のみにかかるものであるため，通信に際して無視できる程度に小さいと考えることができる．今後は，NAT 内のホスト数が増加した場合，サーバ内での処理によりオーバヘッドが増大すると考えられるため，より多くのホストを用いた環境において計測を行うことが必要であると考えている．

参考文献

[1] Rosenberg, J., “Session Traversal Utilities for NAT (STUN)” , RFC5389, IETF, 2008.

[2] Rosenberg, J., Mahy, R. and Matthews, P., “Traversal Using Relays around NAT(TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)” , RFC5766, IETF, 2010.

[3] Ford, B., “Peer-to-Peer Communication Across Network Address Translators”, USENIX Annual Technical Conference, 2005.

[4] F. Audet, Ed., Jennings, C., “Network Address Translation (NAT) Behavioral Requirements for Unicast UDP”, RFC4787, IETF, 2007.

[5] Y. Wei, D. Yamada, S. Yoshida and S. Goto, “A New Method for Symmetric NAT Traversal in UDP and TCP” , APAN Network Research Workshop 2008, pp. 11–18, 2008.

[1] NAT 内ホストから通信を開始した際にかかる時間を計測した．

Copyright ©2011 Information Processing Society of Japan.
All Rights Reserved.