Symmetric NAT における NAT 越え実現方式

李慧

目次

概要

TCP/IP ではプライベートIP アドレスを利用することが一般的であるが,NAT（Network Address Translator）越え問題と呼ぶ通信の制約が課題となっている.既存のNAT越え技術として様々な方式があるが,最も普及している方式としてSTUN（Simple Traversal of UDP through NATs）がある.STUNはCone型NATの場合にのみ有効な技術である.外部ネットワークにSTUNサーバを設置し,あらかじめ内部端末とSTUNサーバの間で通信を実行し,NATテーブルを生成しておく.そのテーブルを使って外部端末から通信を開始することができる.しかしSTUNはSymmetric NAT には対応できないという制約がある.世の中にはSymmetric NATも多く存在するため,この問題は解決することが重要である.そこで本論文ではSymmetric NATであってもNAT越えを実現できる方式を提案する. 具体的には改良STUNサーバを使うことによって,グローバルアドレスからプライベートアドレスに通信を開始することができる.まずグローバルアドレス側の端末は改良STUNサーバに通信をしたいことを伝える.そのメッセージはプライベートアドレス側の端末に届けられる.次にプライベートアドレス端末からグローバルアドレス端末に直接通信を行いNATテーブルを生成する.グローバルアドレス端末はここで生成したNATテーブルを用いて,通信を開始することができる.

1. はじめに

TCP/IP は通信インフラとして広く普及しているが,近年のネットワーク環境は TCP/IP が当初に想定していた状況を遥かに越えている.例えば,急速なインターネットの普及によって IPv4 アドレスが枯渇しつつある.この問題に対応するために,組織のネットワークはプライベート IP アドレスで構築することが一般的となっている.しかしプライベート IP アドレスを用いると,グローバルアドレス空間上のノードがプライベートアドレス空間上のノードを個別に識別できないため,NAT（Network Address Translator）1）越え問題と呼ぶ通信の制約が生じる.近い将来,IPv6 へ移行すれば NAT が不要になるといわれているが,IPv6 は IPv4 との互換性がないことから普及が滞っている.そのため,IPv4 における NAT 越え問題の解決は今後も重要な課題である.

NAT はプライベートアドレスによる内部ネットワークとグローバルアドレスによる外部ネットワークの間に設置される.内部ネットワークから外部ネットワークへ送信されるパケットは,送信元 IP アドレスがグローバルアドレスに変換されて宛先へ送られる.この時内部端末を識別するためにポート番号も変換される.変換前と変換後の関係は NAT テーブルに記憶される.外部ネットワークから NAT に返信されてきたパケットは,NAT テーブルの内容に従って宛先 IP アドレスとポート番号に変換され,対応する内部ネットワークの宛先端末に届けられる.

NAT越え問題とは,グローバルアドレス側からプライベートアドレスに対して通信開始ができないという制約のことである.外部からみるとNAT配下のネットワークは１台の端末に見えるため,内部の端末を個別に指定できないためである.

NATは大きく分類するとSymmetric型NATとCone型NATがある.Symmetric型NATはNATテーブルを生成するときに,グローバルアドレス側のアドレスを記憶しておく.これをフィルタリングと呼ぶ.外部ネットワークからパケットを受信したとき,フィルタリングの内容からIPアドレスとポート番号が正しいかどうかをチェックする.プライベートアドレスからグローバルアドレスにパケットを送信するとき,通信識別子のうちどれか一つでも異なる場合,別のテーブルを生成する.

Cone型NATはフィルタリングのチェックを行わないNATである.従って,フィルタリングには何も記述されない.他の通信で生成したNATテーブルを用いて,グローバルアドレス空間側からの通信の開始ができる.NATとしては不完全な方式であるが,世の中の7割がCone型NATと言われている.

既存のNAT越え技術として様々な方式があるが2)―5),最も普及している方式としてSTUN（Simple Traversal of UDP through NATs）5)がある.STUNはCone型NATの場合にのみ有効な技術である.外部ネットワークにSTUNサーバを設置し,あらかじめ内部端末とSTUNサーバの間で通信を実行し,NATテーブルを生成しておく.そのテーブルを使って外部端末から通信を開始することができる.しかしSTUNはSymmetric NAT には対応できないという制約がある.世の中にはSymmetric NATも多く存在するため,この問題は解決することが重要で

ある.

そこで本論文ではSymmetric NATであってもNAT越えを実現できる方式を提案する. 具体的には改良STUNサーバを使うことによって,グローバルアドレスからプライベートアドレスに通信を開始することができる.まずグローバルアドレス側の端末は改良STUNサーバに通信をしたいことを伝える.そのメッセージはプライベートアドレス側の端末に届けられる.次にプライベートアドレス端末からグローバルアドレス端末に直接通信を行いNATテーブルを生成する.グローバルアドレス端末はここで生成したNATテーブルを用いて,通信を開始することができる.

以下２章で,既存技術とその課題ついて,３章で提案方式について説明する.４章で提案方式を評価し,最後に５章でまとめと今後の展開を述べる.

2. 既存技術とその課題

2.1 NAT の原理とその種類

(1) Symmetric 型 NAT の動作原理

図 1 に Symmetric 型 NAT の動作原理を示す.ノード A はグローバルアドレス G5 を持つ NAT の配下に存在し,プライベートアドレス P1 を持つ.ノード B,ノード C はそれぞれグローバルアドレス G2,G3 を持つ.ノード A がノード B に送信元アドレスとポート番号 P1:s,宛先アドレスとポート番号 G2:d のパケットを送信したものとする.ここで s はノード A が選ぶ任意の空ポート番号,d はノード B のアプリケーションが待ち受けるポート番号である.このパケットは宛先がグローバルアドレスなので,途中のルータでルーティングされた後,必ず NAT に届く.さらに,パケットの送信元アドレスとポート番号 P1:s を G5:m に変換して転送する.ここで,m は NAT が選ぶ任意の空ポート番号である.同時に,G5:m と P1:s が変換されたことをしめす NAT テーブルを生成する.これを G5:m⟺ P1:s と記述する.

NAT テーブルには,上記変換情報とともに,フィルタリングを記述する.フィルタリングとはグローバル空間側の端末のアドレスとポート番号が正しいかどうかをチェックする機能である.これを参照しグローバルアドレス側から送信されてきたパケットを通過させるかどうかが決定される.通過できなかったパケットは破棄される.

図 1 の場合,フィルタリングは IP アドレスとポート番号は G2:d となる.ここで,ノード B からノード A に新たな通信として,送信元アドレスとポート番号 G2:k,宛先アドレスとポート番号 G5:m のパケットを送信したものとする.このパケットは宛先が NAT なので,必ず NAT に届く.しかし,フィルタリングにはアドレスとポート番号 G2:d と記述されているため,このパケットは捨てられる.即ちノード A に対して新たな通信を開始することはできない.

ノード B がポート番号 k を用いた通信を開始するためには,ノード A があらかじめ G2:k 宛

にパケットを送信して NAT テーブルに G5:n ⟺P1:s,フィルタが G2:k という情報を作っておく必要がある.

上記動作はノード C とノード A の場合でも同様であり,あらかじめ NAT テーブル G5:o⟺P1:s,フィルタが G3:h を生成しておく必要がある.

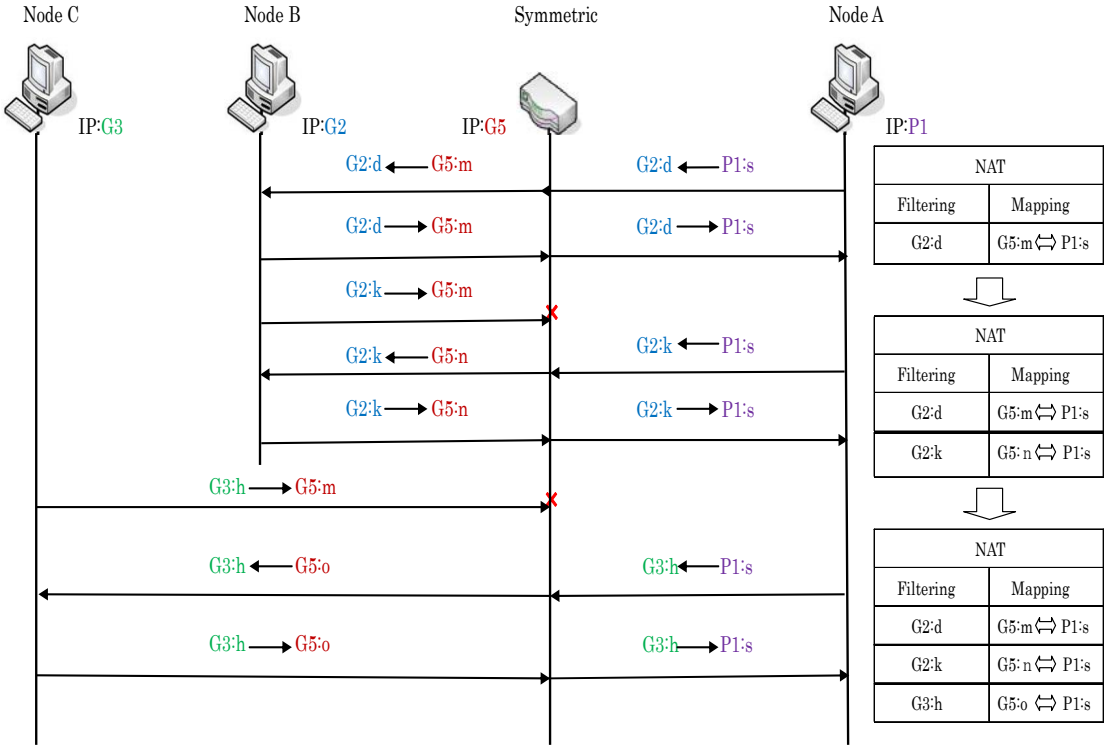

図 1　Symmetric 型 NAT の動作原理

(2) CONE 型 NAT の動作原理

図 2 に Cone 型 NAT の動作原理を示す.IP アドレスの関係は図 1 と同様である.

ノード A がノード B に送信元アドレスとポート番号 P1:s,宛先アドレスとポート番号 G2:d のパケットを送信すると,このパケットは必ず NAT に届く.NAT はパケットの送信元アドレスとポート番号 P1:s を G5:m に変換して転送する.さらに NAT テーブルに P1:s⟺G5:m を記述する.ただし Cone 型 NAT では,フィルタリングに何も記述しない.即ち,グローバルアドレス側の端末の IP アドレスをチェックしない.

ここでノード C からノード A に送信元アドレスとポート番号 G3:k,宛先アドレスポート番号 G5:m のパケットにより通信を開始したものとする.このパケットは宛先が NAT なので,必ず NAT に届く.NAT は NAT テーブルに G5:m の情報が存在し,なおかつフィルタリングには何も記述されていないので,宛先アドレスとポート番号 G5:m を P1:s に変換して転送する.このようにして Cone 型 NAT では,他の通信で生成した NAT テーブルを用いて,グローバルアドレス空間側からの通信開始が可能である.

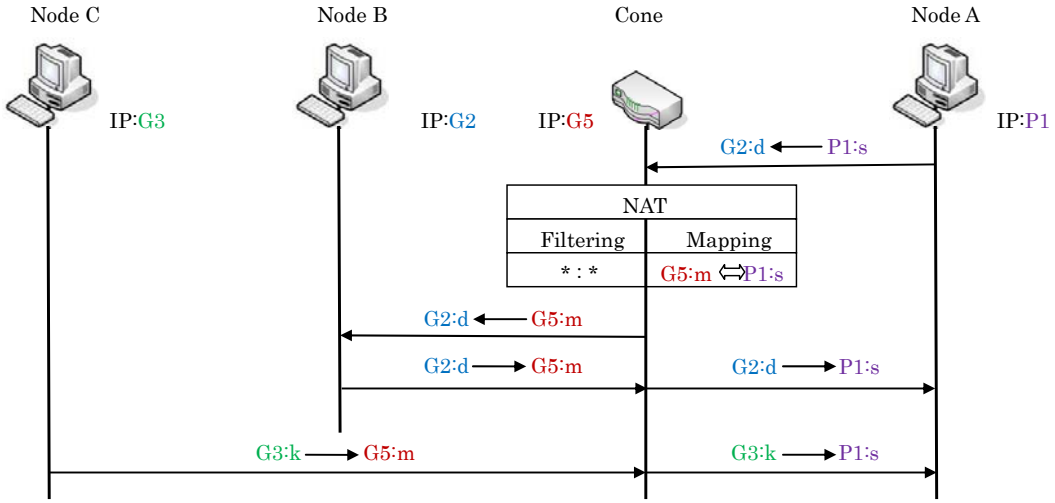

図 2　CONE 型 NAT の動作原理

2.2 STUN

まず,Cone 型 NAT の場合,STUN サーバを使うことによって,ノード B からノード A に通信を開始することができることを示す.図 3 に Cone 型 NAT の場合の STUN の動作を示す.ノード B が Cone 型 NAT 配下に存在するノード A に対して通信を開始する場合を想定する.ノード A はグローバルアドレス G5 を持つ NAT の配下に存在し,プライベートアドレス P1 を持つ.STUN サーバはグローバルアドレス G2 を持つ.ノード B はグローバルアドレス G3 を持つ.

ノード B からノード A に通信を開始したい場合,事前の準備が必要である.ノード A は STUN サーバに向けてノード B にパケットを送信する.送信元アドレスとポート番号 P1:s,宛先アドレスとポート番号 G2:d のパケットを送信する.このパケットは必ず NAT に届く.NAT は NAT テーブル G5:m⇔ P1:s を作る.さらにパケットの送信元アドレスとポート番号 P1:s を G5:m に変換して転送する.Cone 型 NAT であるため,フィルタリングには何も記述されない.STUN サーバはこのパケットを受信すると,ノード A の名前と G5:m の関係を登録する.ここまでで事前の準備が終わる.

ノード B からノード A に通信を開始するとき,ノード B は STUN サーバにノード A の情報を問い合わせる.STUN サーバはノード A のアドレスとポート番号 G5:m をノード B に答える.ノード B は送信元アドレスとポート番号 G3:k,宛先アドレスとポート番号 G5:m のパケットを送信する.このパケットは宛先が NAT なので,必ず NAT に届く.NAT は NAT テーブルに G5:m の情報が存在し,なおかつフィルタリングには何も記述されていないので,宛先アドレスとポート番号 G5:m を P1:s に変換して転送する.このパケットはノード A に到着する.逆の方向のパケットはこれと逆の変換により,通信ができる.このようにしてノード B が Cone 型 NAT 配下に存在するノード A に対して通信を開始することができる.

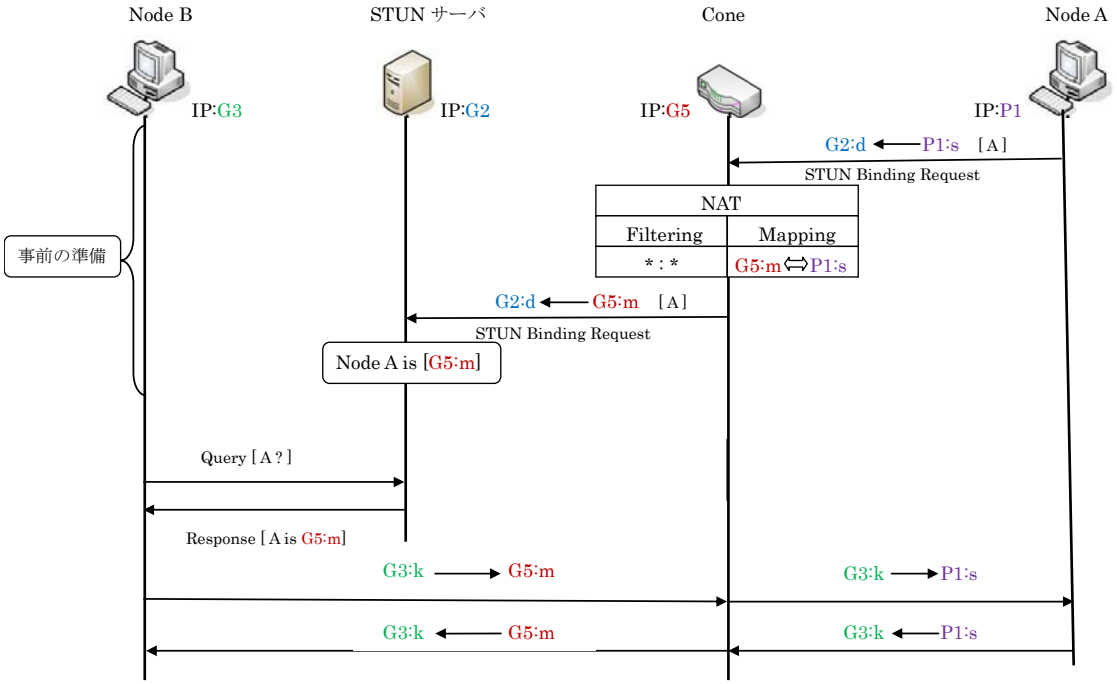

図 3　Cone 型 NAT の場合の STUN の動作

次に,Symmetric 型 NAT の場合,STUN サーバを使っても,ノード B からノード A に通信を開始することができないことを示す.図 4 に Symmetric 型 NAT の場合の STUN の動作を示す.IP アドレスの関係は図 3 と同様である.また,事前の準備も図 3 とほぼ同様である.ただし,Symmetric 型 NAT では,フィルタリング条件として IP アドレスとポート番号 G2:d を登録する.

ノード B からノード A に通信を開始するとき,ノード B は STUN サーバにノード A の情報を問い合わせる.STUN サーバはノード A のアドレスとポート番号 G5:m をノード B に答える.ノード B は送信元アドレスとポート番号 G3:k,宛先アドレスとポート番号 G5:m のパケットを送信する.このパケットは宛先が NAT なので,必ず NAT に届く.Symmetric 型 NAT では,フィルタリングは IP アドレスをチェックするので,送信元アドレスとポート番号 G3:k と,フィルタリングに記述されているアドレスとポート番号 G2:d が異なるので,このパケットを破棄する.そのため,ノード B からノード A に通信を開始することができない.

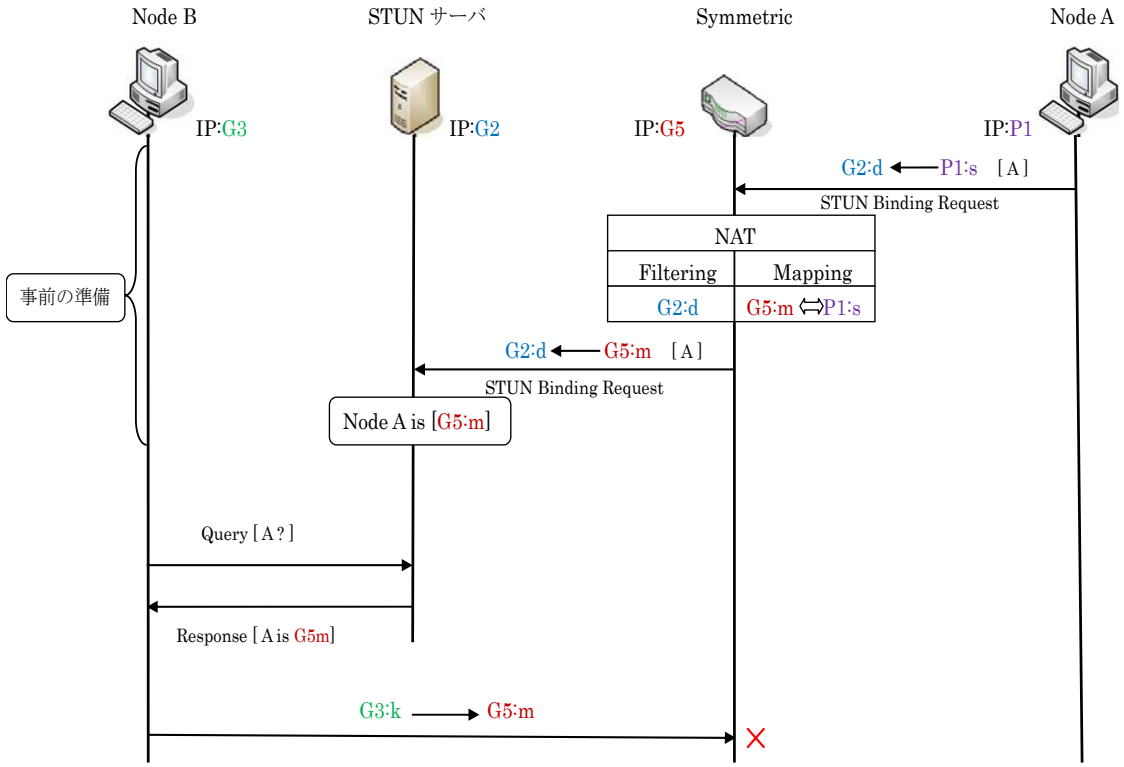

図 4　Symmetric 型 NAT の場合の STUN の動作

3．　提案方式

本論文では Symmetric 型 NAT の場合においても,改良 STUN サーバを使うことによって,ノード B からノード A に通信を開始することができることを示す.図 5 に,改良 STUN サーバによる通信開始を示す.IP アドレスの関係は図 3,図 4 と同様である.また,事前の準備は図 4 と同様である.

ノード B がノード A に通信を開始するためには,ノード A があらかじめ G3:k 宛にパケットを送信して NAT テーブルを作っておく必要がある.そこで,ノード B はまず改良 STUN サーバに対してノード A と通信をしたいことを伝える.改良 STUN サーバはこの通知を受けて,送信元アドレスとポート番号 G2:d,宛先アドレスとポート番号 G5:m のパケットを NAT に送信する.このパケットのメッセージフィールドにはノード B のアドレスとポート番号 G3:k が記載されている.このパケットは Symmetric 型 NAT に届く.NAT は NAT テーブルに G5:m の情報があり,なおかつフィルタリングは G2:d なので,宛先アドレスとポート番号 G5:m を P1:s に変換して転送する.G3:k のメッセージはそのままノード A に届く.

次にノード A は取得したメッセージから,ノード B にあてて送信元アドレスとポート番号 P1:s,宛先アドレスとポート番号 G3:k のパケットを送信する.

NAT は新しく NAT テーブル G5:n⇔ P1:s を作る.フィルタリングは IP アドレスとポー

ト番号 G3:k を登録する.NAT はこのパケットの送信元アドレスとポート番号 P1:s を G5:n に変換して転送する.

ノード B はこのパケットを受信すると,送信元アドレスとポート番号 G3:k,宛先アドレスとポート番号 G5:n のパケットを送信する.これを受信した NAT は NAT テーブル G5:n があり,なおかつフィルタリングは G3:k なので,宛先アドレスとポート番号 G5:n を P1:s に変換して転送することができる.このパケットはノード A に届く.逆の方向のパケットはこれと逆の変換により,通信ができる。このようにして Symmetric 型 NAT であっても,ノード B からノード A に対して通信を開始することができる.

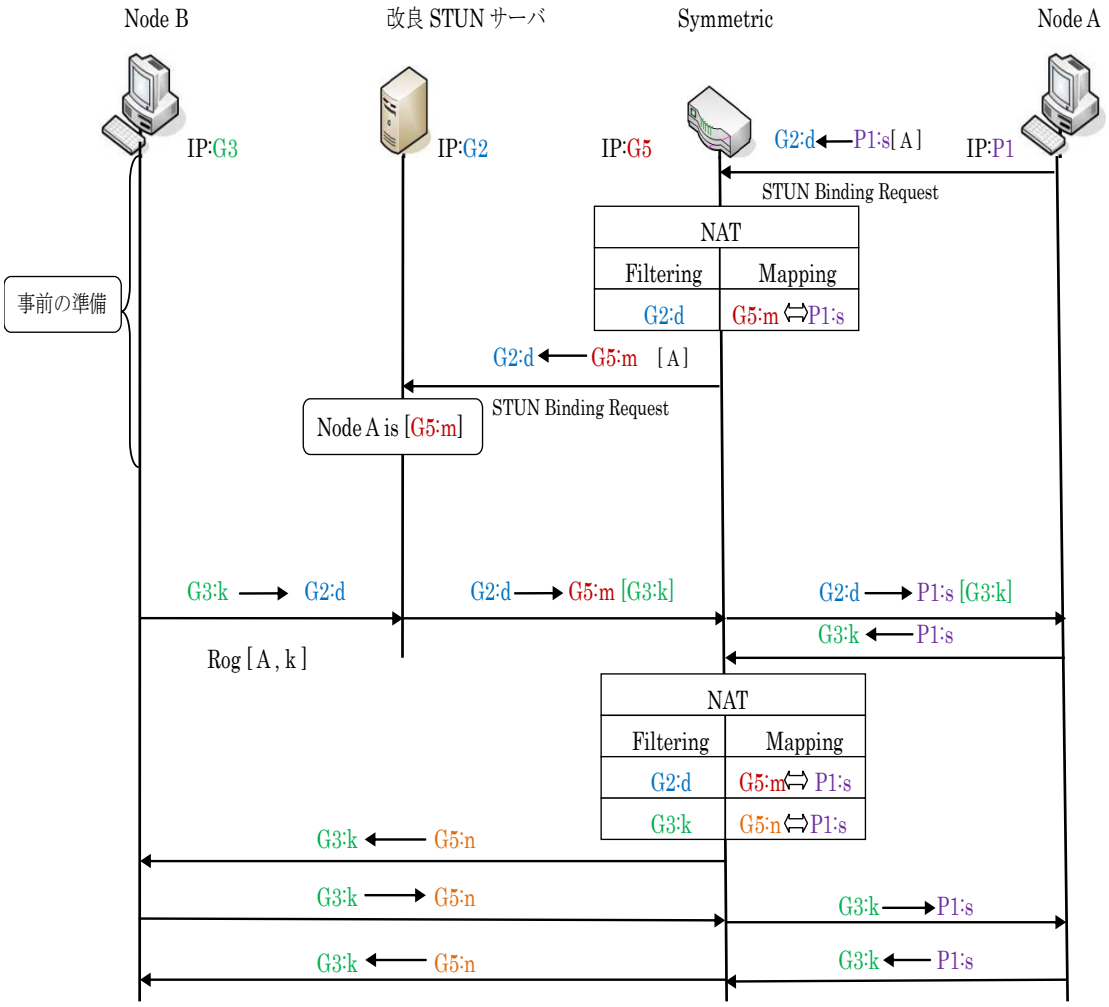

図５　改良 STUN サーバによる通信開始

４．　評価

表１に,既存 STUN と提案方式の比較を示す.NAT の方式に関して比較すると,Cone 型 NAT

の場合,既存 STUN と提案方式は両者ともグローバルアドレスからプライベートアドレスに通信を開始することができる.Symmetric 型 NAT の場合,既存 STUN ではグローバルアドレスからプライベートアドレスに通信を開始することができない,本提案方式では,改良 STUN サーバを使うことによって,グローバルアドレスからプライベートアドレスに通信を開始することができる.プロトコルに関して比較すると,UDP の場合,既存 STUN と提案方式は利用することが可能である.しかし,TCP に関しては両者とも利用できない.TCP の場合,NAT においてシーケンス番号のチェックなどを行っている場合があり,今回の方式では対応できない.今後は,TCP の NAT 越えを検討する必要がある.

表 1　　既存 STUN と提案方式の比較

		既存 STUN	提案方式
NAT 方式	CONE	○	○
	Symmetric	×	○
プロトコル	UDP	○	○
	TCP	×	×

5．　まとめ

Cone型NATの場合,STUNサーバを使うことによって,グローバルアドレスからプライベートアドレスに通信を開始することができる.しかし,Symmetric型NATの場合,STUNサーバを使っても,グローバルアドレスからプライベートアドレスに通信を開始することができない.そこで,この課題を解決するため,改良STUNサーバを使うことにより,外側から内部に通信を開始することができることを示した.今後はTCPにおいてもNAT越えができる方式を検討する.

謝辞

本研究に関して,研究の方向や進め方など終始御熱心なご指導と御教示を賜りました,名城大学理工学部情報工学科 渡邊晃教授に心より厚く御礼申し上げます.

本研究を進めるにあたり,研究内容に関して終始御熱心なご指導と御教示を賜りました,名城大学理工学部情報工学科 柳田康幸教授,宇佐見庄五准教授に心より厚く御礼申し上げます.

最後に,本研究を行うにあたり,有益なご助言,適切なご検討をいただいた,名城大学理工学部情報工学科渡邊研究室の皆様に心より感謝いたします.

参考文献

1) Egevang, K. and Francis, P.: The IP Network Address Translators (NAT), RFC1631, IETF (1994).
2) 鈴木秀和, 宇佐見庄五, 渡邊　晃 : 外部動的マッピングによりNAT 越え通信を実現するNAT-fの提案と実装，情報処理学会論文誌，　Vol.48, No.12, pp.3949-3961 (2007).
3) UPnP Forum: Internet Gateway Device(IGD) Standardized Device Control Protocol V 1.0, http://www.upnp.org/standardizeddcps/igd.asp (2001).
4) Rosenberg, J., Mahy, R. ,and Matthews, P.: Traversal Using Relays around NAT(TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN), Internet-Draftdraft-ietf-behave-turn-16, IETF (2009).
5) Rosenberg, J., Weinberger, J., Huitema, C., and Mahy,R., “STUN - Simple Traversal of User DatagramProtocol (UDP) Through Network Address Translators(NATs)”, RFC 3489, March 2003.