平成23年度　修士論文

邦文題目

自宅からのリモートアクセスを可能にするGSRAv2の提案と評価

英文題目

Proposal of GSRAv2 That Enables Remote Access from Home and Its Evaluation

情報工学専攻

(学籍番号: 103430015)

鈴木　健太

提出日: 平成24年3月16日

名城大学大学院理工学研究科

内容要旨

遠隔地のネットワークにアクセスできる既存のリモートアクセス技術は，端末がグローバルアドレスを持つことを想定しているものが多い．しかし，実際には端末が家庭内のプライベートアドレス空間にあることを想定するのが現実的である．現在広く利用されているリモートアクセス技術のうち，IPsec-VPN は，きめ細かな設定が可能であるが，NAT との相性問題があり，利用できない場合がある．SSL-VPN は，NAT 配下からでも手軽に利用できるが，使用するアプリケーションが限定されるという課題がある．OpenVPN は，様々な環境で使用できるが，NAT の存在によりプライベートアドレスが重複し，通信が行えなくなる可能性がある．PacketiX VPN は，非常に機能が豊富であるが，セキュリティ上の危険を招く怖れがある．これらの方式の課題をまとめて解決した方式として GSRA（Group-based Secure Remote Access）があるが，NAT 配下からの使用は想定されていない．本論文では，これらの課題を解決するため，GSRA を NAT 配下のプライベートアドレス空間からでも利用できるように改良した GSRAv2 を提案する．また，一般的に想定される利用シーンに沿った形での性能評価を行い，提案方式の有用性を確認した．

目 次

第1章　はじめに

モバイル端末の小型・高性能化や，モバイルブロードバンドの普及に伴って，リモートアクセスのニーズが高まっている．リモートアクセスとは，遠隔地から社内や家庭内のネットワークに接続し，そのネットワーク内の資源を利用する技術である．リモートアクセスを実現する手法としては，インターネット上に VPN（Virtual Private Network）を構築するインターネット VPN が一般的である．

インターネット VPN を構築する方式には，PPTP（Point-to-Point Tunneling Protocol）[1]，L2TP（Layer 2 Tunnneling Protocol）[2]，IPsec-VPN（Security Architecture for Internet Protocol）[3]，SSL-VPN（Secure Socket Layer）[4]，OpenVPN [5]，PacketiX VPN 3.0 [6]（以下 PacketiX VPN）などがある．PPTP は, 認証に MS-CHAPv2（Microsoft version of the Challenge-handshake authentication protocol version 2）[7] を使用する．MS-CHAPv2 が採用しているハッシュ関数 MD4 [8] は脆弱性が見つかっており, 暗号化アルゴリズム DES [9] は解析可能であることが知られている．L2TP はトンネリングプロトコルであり，単体ではセキュリティ機能を備えていない．そこで最近は，IPsec-VPN，SSL-VPN，OpenVPN，PacketiX VPN の 4 手法に注目が集まっている．

しかし，これらの手法にも，一長一短がある．IPsec-VPN は，きめ細かな設定が可能であるが，設定が煩雑となり，高い専門知識が要求される．SSL-VPN は手軽に利用できるものの，使用できるアプリケーションが制限される．また，確実なクライアント認証を行う場合は，端末に証明書を持たせる手間が生まれ，利点である手軽さが失われる．OpenVPN は，高セキュリティと手軽さを兼ね備えた方式として注目されているが，パケットのカプセル化による追加のオーバヘッドやフラグメントの発生によりスループットが低下するという課題がある．PacketiX VPN は，多様な機能を備えており，フレキシブルに利用できるという特長があるが，通信を SSL に見せかけるという性質上，ネットワーク管理者が社員の VPN 接続を認知できず，その結果ウィルスの侵入や情報の漏洩など，組織単位で危険をもたらす場合がある．また，イーサネットフレームを TCP でカプセル化するため，TCP over TCP [10] の問題が発生し，パケットロスが発生する環境では通信性能が著しく低下する可能性がある．

これらの課題を解決する方式として, GSRA（Group-based Secure Remote Access）[11,12] が提案されている．GSRA は，NAT 越え技術 NAT-f [13] の仕組みを利用し，そこにアクセス制御やセキュリティの機能を追加することで安全なリモートアクセスを実現した方式である．GSRA では，通信グループの概念を取り入れることにより，簡単かつ柔軟にアクセス制御を行うことができ，アプリケーションが制限されないという利点がある．ま

た，パケットをカプセル化せず，アドレス変換のみによってリモートアクセスを実現するため，高スループットが得られる．

既存のリモートアクセス技術には，リモート端末がグローバルアドレスを持つことを前提としているものがある．しかし，現実的なリモートアクセスの利用シーンとしては，学生が自宅から大学の学内ネットワークへアクセスしたり，社員が勤務先の社内ネットワークに接続し，在宅勤務を行うことなどが考えられる．このようなケースでは，リモート端末は NAT 配下のホームネットワーク内に存在し，プライベートアドレスを保持しているのが一般的である．このような利用シーンを想定し，既存技術を比較し直すと，IPsec-VPN は NAT との相性が悪く，使用する NAT によっては利用できないケースがある．SSL-VPN は，NAT が存在しても利用できる．IPsec-VPN，OpenVPN，PacketiX VPN は，リモート側とリモート先のネットワークで使用しているプライベートアドレスが重複しないように管理する必要がある．GSRA は，グローバル空間からの利用を想定していたため，リモート端末がホームネットワークにある場合は利用できない．

そこで本稿では，GSRA に，ホームネットワーク側の NAT のマッピング情報をリモート端末に通知する処理を追加し，NAT 配下からの利用を可能とした GSRAv2 を提案する．提案方式では，GSRA の利点がそのまま活かせるとともに，ホームネットワーク側でいかなる NAT を使用していても，その配下からリモートアクセスを行うことが可能である．GSRAv2 の実装を行い，既存の方式と比較して，高スループットを実現できることを確認した．

以降，2 章で既存技術について述べる．3 章で提案方式の要素技術となる GSRA について述べ，4 章で GSRAv2 の提案を行う．5 章で実装について述べ，6 章で既存技術との比較評価を行い，7 章でまとめる．

第2章　既存技術

本章では, 既存のリモートアクセス技術の代表として, IPsec-VPN, SSL-VPN, OpenVPN, PacketiX VPN の概要について述べる．なお，本論文ではリモートアクセスを行う端末を EN（External Node），アクセス先の端末を IN（Internal Node） と表記する．

2.1　IPsec-VPN

IPsec-VPN は IPsec の仕組みを利用することにより VPN を構築する．アクセス先ネットワークに設置された IPsec-VPN 装置と EN 間で IKE（Internet Key Exchange）[14] による認証と暗号鍵の共有を行い，IPsec ESP トンネルモードによる暗号通信を行うことでリモートアクセスを実現する．IPsec は IP 層においてデータの改ざん防止や秘匿機能を提供するプロトコルであるため，アプリケーションを限定することなく，通信経路上で通信内容の改ざんや盗聴を防止することができる．また，セキュリティポリシの設定やネゴシエーションの設定等を端末毎に設定でき，柔軟なアクセス管理ができる．しかしその分，専門的知識が要求され，管理負荷が大きいという課題がある．また，ホームネットワークから IPsec-VPN によるリモートアクセスを行う場合，NAT によるアドレス変換を，アドレス偽装と認識されてしまい，IPsec-VPN 装置でパケットが破棄されてしまう．そのような場合，IPsec パススルーに対応した NAT を使用するなどの対策が必要となる．

2.2　SSL-VPN

SSL-VPN は，SSL を用いて VPN を構築する方式である．アクセス先ネットワークの DMZ（DeMilitarized Zone）などに SSL-VPN 機能を持った装置を設置し，それがプロキシサーバの役割を果たすことによりリモートアクセスを実現する．SSL は一般的な Web ブラウザに標準で搭載されているため，ユーザ側で特別な設定やソフトのインストールをせずとも，サーバを認証しアクセスすることができる．ただし，企業等の高セキュリティなネットワークへアクセスを行う場合は，EN にも証明書を持たせる必要があり，手軽さという利点が損なわれる．また，ブラウザベースであるため，Web ブラウザを利用した Web 閲覧やメール送信などに用途が限定されるという課題がある．

2.3 OpenVPN

OpenVPN は，仮想ネットワークデバイス TUN/TAP [15] 間でパケットをトンネリングすることによりリモートアクセスを実現する．OpenVPN は，暗号化に OpenSSL を用いるが，Ethernet フレームをカプセル化して通信を行うため，任意のアプリケーションを使用できる利点がある．しかし，カプセル化によるヘッダオーバヘッドやフラグメントの発生により，スループットが低下する．また，サーバからクライアントに対して IP アドレスや DNS サーバなどの設定情報を配布する必要があり，配布された設定情報と，クライアント側の LAN 内の端末の設定情報が重複した場合，通信が行えなくなるという課題がある．

2.4 PacketiX VPN

PacketiX VPN は，コンピュータ上に独自の仮想 NIC を作成し，その仮想 NIC 間でパケットをトンネリングすることによりリモートアクセスを実現する．PacketiX VPN による VPN の構築は，パケットを SSL に偽装して行われるため，NAT やファイアウォールを透過して行うことができる．しかし，この性質上，一般社員がネットワーク管理者に無断で PacketiX VPN を利用して自宅との間で VPN を構築することが可能となる．ネットワーク管理者からは，VPN が利用されていることを認知できず，社内情報の流出や，ウィルスの侵入を許してしまう可能性がある．また，Ethernet フレームを TCP でカプセル化して通信を行うため，パケットロスが発生する環境では，通信性能が大幅に低下する可能性がある．

第3章　GSRA

本章では，提案方式の要素技術となる GSRA について説明する．なお，本論文で使用する記号の定義は付録 A に示す通りである．

3.1　概要

GSRA は，NAT 越え技術 NAT-f（NAT-free Protocol）にセキュリティの機能を追加することにより，安全なリモートアクセスを実現した技術である．通信グループを定義することにより簡単かつ柔軟なアクセス制御を行うことができる．また，独自の暗号化プロトコル PCCOM（Practical Cipher Communication Protocol）[16] を採用し，NAT をまたがるエンドエンドの通信を暗号化することができる．

GSRA によるリモートアクセスの構成例を図 3.1 に示す．EN はグローバルアドレスが割り当てられているものとする．GSRA の機能を実装したルータを GSRA ルータと呼ぶ．GSRA では，管理を容易にするため，内部端末へのアクセスをグループ単位で制御する．図 3.1 の例では，EN は Group1 に所属しており，IN1 は Group1 端末との通信を，IN2 は Group2 端末との通信を許可している．この場合，EN は IN1 へアクセス可能であるが，IN2 へのアクセスは拒否される．IN のグループ情報は GSRA ルータに登録されており，この情報を基に GSRA ルータがアクセス制御を行う．

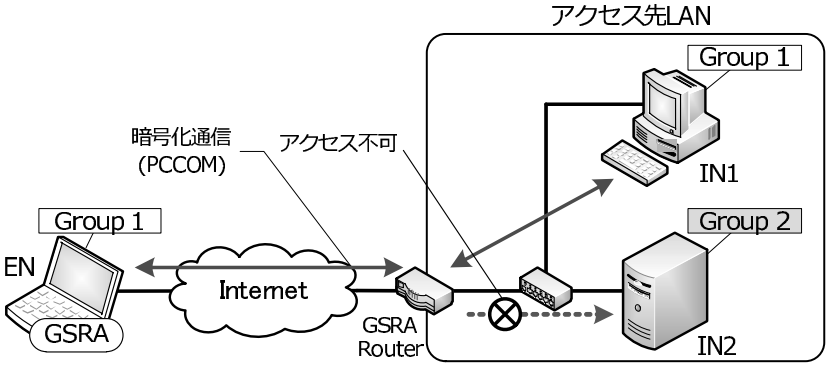

図 3.1　GSRA によるリモートアクセスの構成例

3.2 通信シーケンス

図 3.2 に EN が IN へリモートアクセスを行うための GSRA ネゴシエーションのシーケンスを示す．前提として，EN と GSRA ルータは各通信グループに対応したグループ鍵 *GK* をあらかじめ所持している．グループ鍵は，グループ毎に固有の暗号鍵であり，EN が当該グループに所属していることを証明するものである．DNS サーバには，IN のホスト名と GSRA ルータのグローバル IP アドレス G_{GR} との関係が登録されている．また，GSRA ルータには ACT（Access Contorol Table）と呼ぶテーブルに，IN のホスト名，プライベート IP アドレス，サービス情報（ポート番号，プロトコル），グループ番号，外部からのアクセス許可情報（allow または deny）が登録されている．ACT の設定により，サービス毎にリモートアクセスを許可するグループとサービスが決まる．グループ番号として，複数のグループを指定することも可能であり，簡単かつ柔軟にアクセス制御を行うことができる．ACT の例を表 3.1 に示す．表 3.1 の例では，Group1 にのみ属する端末は，Alice が公開している TCP の d 番ポートに該当するサービスは利用可能であるが，UDP の e 番ポートに該当するサービスは利用できない．また，Alice は PCCOM をサポートしているため，エンドエンドで暗号化通信が可能である．

以下に EN が IN と通信を開始するまでの手順を説明する．なお，括弧付きの数字は図 3.2 中の数字と対応している．

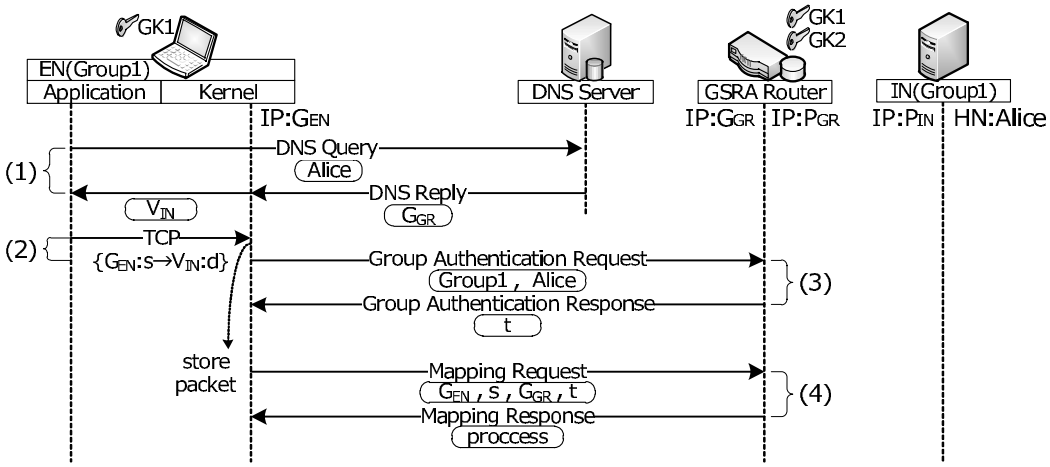

図 3.2　GSRA ネゴシエーションの流れ

表 3.1　ACT の例

Host Name	IP Address	PCCOM Support	Service	Group	Permit
Alice	P_{IN}	Yes	d (tcp)	Group1	allow
			e (udp)	Group2	allow

(1) 名前解決

EN は DNS サーバに IN（ホスト名：Alice）の名前解決を依頼し，GSRA ルータのグローバル IP アドレス G_{GR} を取得する．ここで EN はカーネル領域において，DNS Reply に記載されているアドレス G_{GR} を仮想 IP アドレス V_{IN} に書き換える．これにより EN のアプリケーションは IN の IP アドレスを V_{IN} と認識する．IN はプライベート IP アドレスしか保持していないため，本来 EN 側から通信を開始することはできない．しかし，仮想 IP アドレスとして通知することにより，EN 側から IN を指定して通信を開始することが可能になる．この時，Alice と G_{GR}，および V_{IN} の関係を NRT（Name Relation Table）に登録しておく．これにより，EN は GSRA ルータ配下の複数の端末を仮想 IP アドレスで区別することができる．

(2) 通信開始

EN のアプリケーションから宛先が V_{IN} のパケットが送信されると，EN はカーネルにて VAT（Virtual Address Translation table）を検索する．VAT は，（1）の処理で EN に通知した仮想アドレス宛のパケットを，実アドレス宛へと書き換えるために使用するテーブルである．初回は対応する VAT のエントリが存在しないため，送信されたパケットをカーネル内に待避してから，（3），（4）の処理を行う．

(3) グループ認証処理

グループ認証処理は，EN からのアクセスを許可するかどうかの認証を行う処理である．EN は通信したい IN のホスト名 “Alice” と自身のグループ情報 “Group1” を記載した Group Authentication Request を GSRA ルータへ送信する．GSRA ルータはこれを受信すると，ACT をチェックし，EN から IN へのアクセス可否の認証を行う．アクセスが許可されていた場合，GSRA ルータは EN と IN 間の当該セッションに使用するエフェメラルポート番号 t を予約し，t を記載した Group Authentication Response を EN へ送信する．エフェメラルポート番号とは，リモートアクセスのために一時的に使用するポート番号であり，GSRA ルータの未使用ポートの中から選ばれる．EN は Group Authentication Response メッセージから t を取得して，VAT を更新する．

(4) マッピング処理

GSRA では，EN のカーネル及び GSRA ルータにアドレス変換テーブルを生成し，テーブルのエントリに従ってパケットのアドレス変換を行う．マッピング処理は，そのためのテーブルを生成する処理である．EN は（2）で待避したパケットのセッション情報と，宛先情報 $G_{GR}:t$ を記載した Mapping Request を GSRA ルータへ送信する．GSRA ルータは Mapping Request から取得した情報を用いて GSRA マッピングテーブルと PIT（Process Information Table）を生成し，EN における動作処理情報を記載した Mapping Response を EN へ送信する．GSRA マッピングテー

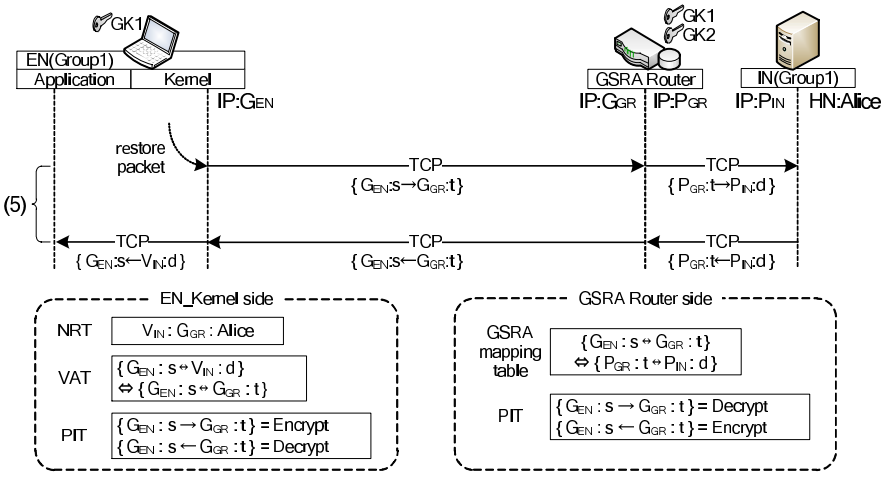

図 3.3　アドレス変換処理による IN へのアクセス

ブルは，（3）で割り当てたポート番号宛の通信を，IN 宛へと書き換えるために使用するテーブルである．PIT には，通信の送信元/宛先の組み合わせ毎に，パケットを暗号化するか復号するかといった情報（動作処理情報）が記載される．EN は受信した Mapping Response から動作処理情報を取得し，EN 側の PIT を生成する．

以後は（2）で待避したパケットを復帰させて通信を開始する．

(5) IN へのアクセス

以後の通信の様子と，生成されたテーブルの内容を図 3.3 に示す．EN から IN 宛の通信は，まず EN のカーネル内で VAT に従い宛先 IP アドレス/ポート番号を変換する．さらに PIT に従ってパケットを PCCOM で暗号化してから GSRA ルータへ送信する．GSRA ルータでは，受け取ったパケットを復号後，GSRA マッピングテーブルに基づいて宛先/送信元の IP アドレス/ポート番号を変換し，IN へと転送する．ここでは，通常の NAT の動作とは違い，送信元アドレス/ポート番号も GSRA ルータのものに書き換える．送信元情報を書き換えることで，GSRA ルータをデフォルトゲートウェイと別の入り口として設置するような場合に，応答パケットがデフォルトゲートウェイへと送信されてしまうのを防いでいる．IN から EN への応答は上記と逆の順序でアドレス変換および暗号化処理を行い，EN まで届ける．以上の手順により，EN から IN へのリモートアクセスが実現される．

第4章　提案方式

本章では，提案方式 GSRAv2 の仕組みについて述べる．EN がホームネットワークの NAT 配下に位置する場合に対応するため，GSRA のシーケンスを見直した．以後，ホームネットワーク側の NAT を HR（Home Router）と呼ぶ．

4.1　解決すべき課題

HR が存在する場合，EN から送信されるパケットの送信元は HR によってマッピングされた IP アドレス/ポート番号（HR のマッピングアドレス）へと変換される．GSRA のマッピング処理では，Mapping Request のメッセージに記載した EN のアドレス/ポート番号を元に GSRA マッピングテーブルを生成するため，HR でヘッダ情報が書き換えられたとしても，生成されるテーブルエントリにはそれを反映することができない．従って，経路上に HR が存在する場合には，EN の送信元情報として，HR のマッピングアドレスを Mapping Request に記載し，GSRAM ルータへ送信する必要がある．そのためには，EN があらかじめ HR のマッピングアドレスを知っている必要がある．

あらかじめ HR のマッピングアドレスを内部の端末に通知する手法として，STUN [17] が採用している UDP ホールパンチング [18] がある．UDP ホールパンチングは，HR 配下の端末同士が UDP の通信を行うための手法である．まず，通信を開始したい双方の端末から，グローバル空間にあるサーバ装置に対して UDP のパケットを送信し，HR にマッピングを行わせる．サーバ端末は受け取ったパケットのヘッダ情報から，HR のマッピングアドレスを取得する．次に，取得したマッピングアドレスを，メッセージ内に格納して，通信相手側の HR 配下の端末へ通知する．以上の仕組みにより，互いの端末が，相手側の HR のマッピングを得て，HR 配下同士の通信が可能となる．

この UDP ホールパンチングの仕組みを GSRA に応用することを考える．EN からあらかじめ GSRA ルータへ UDP パケットを送信し，GSRA ルータはそのヘッダ情報から HR のマッピングを得る．GSRA ルータは，取得した HR のマッピングアドレスを UDP パケットのメッセージに格納し，EN へ通知する．EN は UDP パケットのメッセージから HR のマッピングアドレスを取得して，これを送信元情報として GSRA のマッピング処理を行う．以上により，GSRA を HR 配下から使用することが可能になると考えられる．

しかし，HR によるマッピングは，セッション毎行われ，それぞれ別々のポート番号が割り当てられる．従って，TCP の通信を行う場合には，上記手順を，TCP で行う必要がある．また，近年の NAT ルータには SPI（Stateful Packet Inspection）機能が搭載されて

いることが多い．SPI とは，ルータを通過するパケットの状態をログに記録しておき，記録されたログの内容と到着したパケットの内容を照合することで整合性を確認する動的なパケットフィルタリング機能である．SPI 機能により，過去の通信と整合性のとれないパケットは，不正パケットとして HR で破棄されてしまう．この SPI 機能により，単純な 1 往復シーケンス追加による上記の方法は，TCP の場合では上手くいかない．

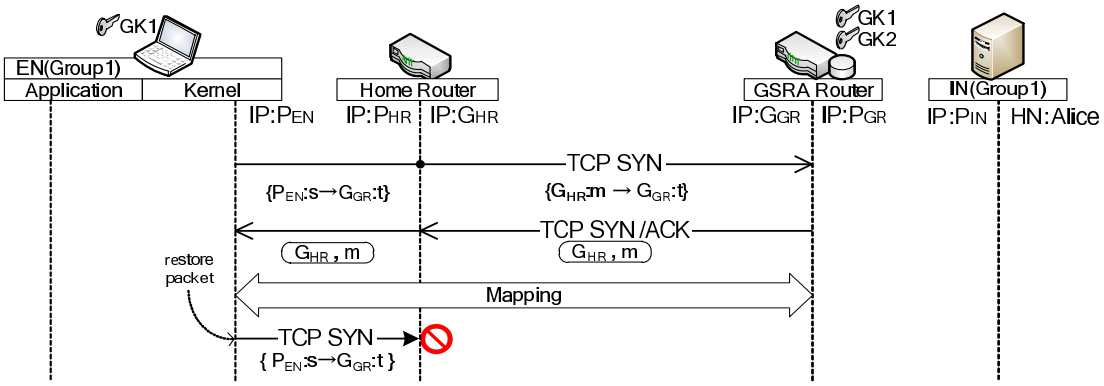

図 4.1　TCP1 往復シーケンスを追加した場合

単純に TCP の 1 往復シーケンスを追加した場合のシーケンスを図 4.1 に示す．通信開始時には，EN と GSRA ルータ間では TCP コネクションが確立していないため，追加する往復パケットのフラグは，SYN と SYN/ACK の組とし，3-way handshake に見せかけてホールパンチングを行う．EN から送信された SYN パケットは，HR による変換を経て GSRA ルータへと届けられる．GSRA ルータでは，SYN パケットのヘッダ情報から HR のマッピングアドレスを取得し，これを SYN/ACK のメッセージに格納して EN へ送信する．EN は SYN/ACK パケットメッセージから HR のマッピングアドレスを取得する．EN は HR のマッピングアドレスを送信元情報としてマッピング処理を開始する．以上の手順により，HR に対応した GSRA のマッピングテーブルを生成することが可能である．

この時点で，HR では SPI 機能により，EN から GSRA ルータへの SYN パケットと，その応答 SYN/ACK パケットの通過を記録している．正常な 3-way handshake では，この次に SYN/ACK パケットの応答として ACK パケットが EN から送信されるはずである．しかし，GSRA ネゴシエーションが完了した後に送信されるパケットは，アプリケーションから送信され，ネゴシエーション開始前に退避しておいた SYN パケットである．よって，この SYN パケットは過去の通信ログと不整合であると判断され，HR にて破棄されてしまう．

このように，単純に 1 往復パケットを追加するだけでは，TCP の場合，通信を開始することができない．従って，SPI 機能による破棄を回避しつつ，TCP の場合でも HR 配下から使用可能にする工夫が必要となる．

4.2 解決策

本稿ではこの問題を解決するため，TCP の再送制御に着目した．具体的には，追加するパケットを，1 往復ではなく，EN から GSRA にルータへの片道のみに変更し，HR のマッピングアドレスの通知には ICMP を使用する．TCP の場合，追加パケットは SYN パケットのみとなり，これに応答を返さないことで，HR では SYN パケットが失われたと判断する．よって，ネゴシエーション完了後にアプリケーションから送信される SYN パケットは，HR にて “追加した SYN パケットの再送パケット” として扱わせることができる．しかし，片道のみでは HR のマッピングアドレスを EN に通知することができないため，1 往復の ICMP パケットを追加する．ICMP であれば，過去の通信ログなどと関係なく，いつ送受信しても不自然でないため，SPI に影響されず EN に通知することができる．また，GSRA ルータから EN への通知用 ICMP パケットを通すため，あらかじめ EN から GSRA ルータに ICMP パケットを送信しておく．

追加するシーケンスを図 4.2 に示す．まず EN から GSRA ルータへ ICMP パケットを送信し，続けて SYN パケットを送信する．GSRA ルータでは，受信した ICMP パケットを退避し，続いて受信した SYN パケットのヘッダ情報から HR のマッピングアドレスを得たあと，応答を返さずこのパケットを破棄する．ここで得た HR のマッピングアドレスを，退避していた ICMP パケットの応答メッセージに記載して EN に送信する．以上のシーケンスを追加することで，HR のマッピングアドレスを得ると同時に，SPI による破棄を回避して通信を開始することができる．

4.3 GSRAv2

本稿では，4.2 節で説明したシーケンスを GSRA に追加し，HR 配下から利用可能にした GSRAv2 を提案する．また，追加するシーケンスをバインディング処理と呼ぶ．バインディング処理で追加する TCP パケット名を $BReq_t$，ICMP パケット名を $BReq_i$，$BRes_i$ とする．ここで，$BReq_t$ は，GSRA ネゴシエーションのトリガとなった SYN パケットをコ

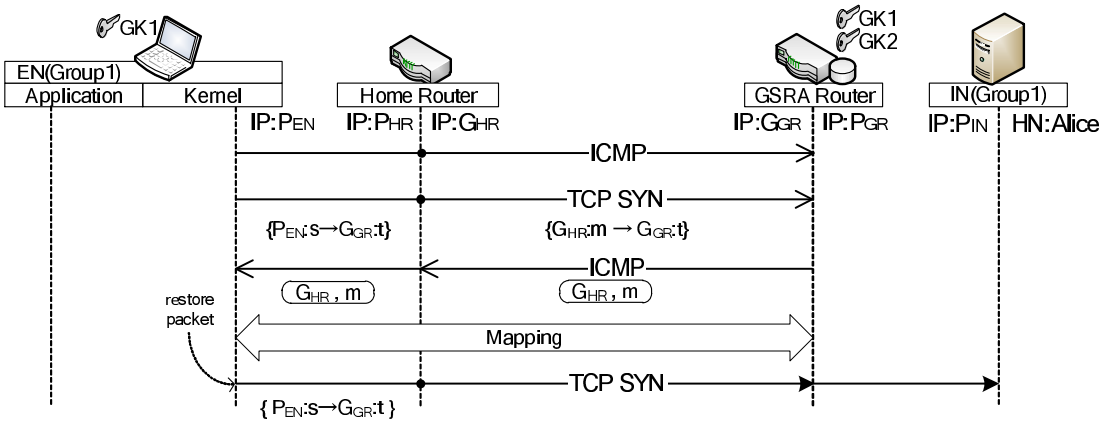

図 4.2　追加するシーケンス

ピーし，宛先を GSRA ルータに書き換えたものとする．トリガパケットの内容をコピーすることで，TCP フラグ以外のシーケンス番号等の情報も，ネゴシエーション完了後に送信されるパケットと整合性が保たれる．バインディングの処理手順は，4.2 節で説明した通りである．

一方，通信経路上に HR が存在するかどうかは定かでなく，HR が存在しないような状況では，バインディング処理を行う必要がない．そのため，バインディング処理はグループ認証処理とマッピング処理の間に行うものとする．HR が存在するか否かは，Group Authentication Request のメッセージ内に記載された EN の送信元情報と，ヘッダ内の送信元を比較し，一致するかどうかで判定する．両者が等しい場合は，HR が存在しないと判断し，バインディング処理をスキップする．これにより，続いて行われるマッピング処理は，HR の有無に関わらず共通の処理内容とすることができる．

以上を全てふまえた最終的な GSRAv2 のネゴシエーションシーケンスを図 4.3 に示す．GSRAv2 では，基本的な GSRA の処理内容をそのままに，通信経路上に HR が存在する場合のみバインディング処理を行う．これにより，GSRA の方式的に優れた特長を活かしつつ，HR 配下からも利用することが可能となり，追加の処理時間も最小限に抑えることができる．

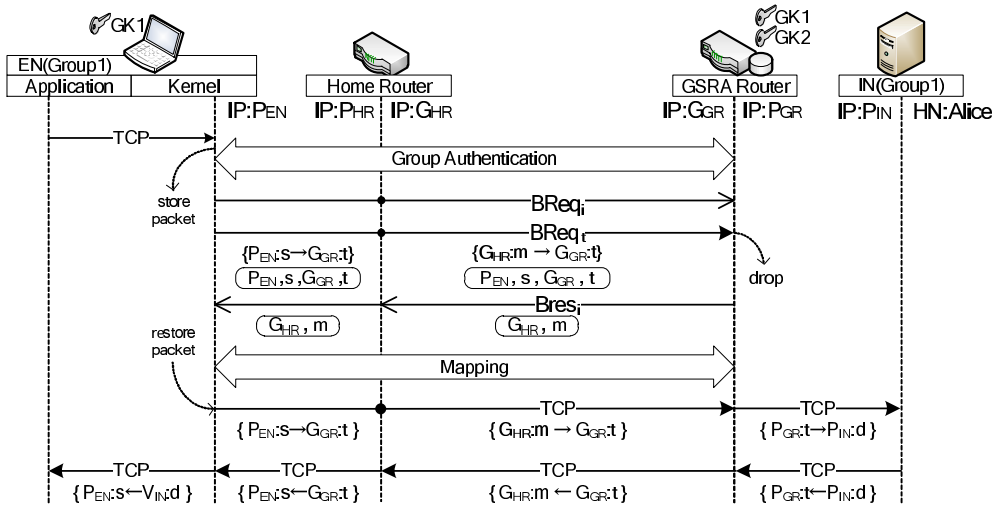

図 4.3　GSRAv2 ネゴシエーションの流れ

第5章　実装

本章では，提案方式の実装について述べる．提案方式は既に FreeBSD に実装済みである．GSRA では，EN および GSRA ルータに，GSRA 用の処理を行う GSRA モジュールを IP 層に実装している．カーネルは GSRA モジュールの呼び出し部のみを変更しており，その他の IP 層の処理は一切変更しない．

5.1　EN への実装

EN における実装を図 5.1 に示す．パケットを送受信する際，IP 層にて入出力関数 `ip_input()`，`ip_output()` から GSRA モジュールを呼び出す．GSRA ネゴシエーションに使用する各制御パケットは，GSRA モジュール内で生成する．ネゴシエーション完了後は，GSRA モジュールが NRT，VAT，PIT の情報を保持することとなり，GSRA モジュールへ渡されたパケットは，これらのテーブルのエントリに従ってアドレス変換等の処理を行ったうえで元の位置に差し戻す．GSRAv2 では，GSRA モジュールにバインディング処理の機能を追加する形で実装を行った．

5.2　GSRA ルータへの実装

GSRA ルータにおける実装方法を図 5.2 に示す．GSRA ルータでは，GSRA モジュールに加えて，NAT の機能を有する `natd` を動作させる．`natd` は，FreeBSD で利用できる，ユーザランドで動作するアプリケーションである．GSRA ルータが受信したパケットは，divert ソケットを通じて，natd へと渡され，そこでアドレス変換を行う．また，GSRA モジュールには ACT と PIT の情報が保持され，アクセス制御及び暗号化などの処理を行う．

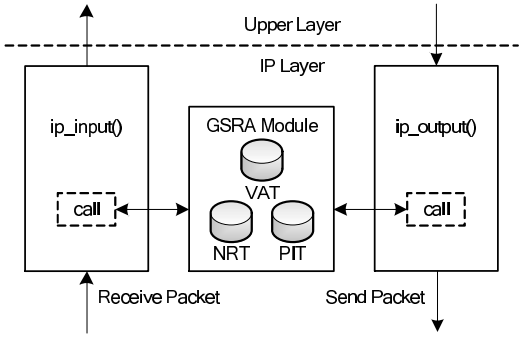

図 5.1　EN の実装

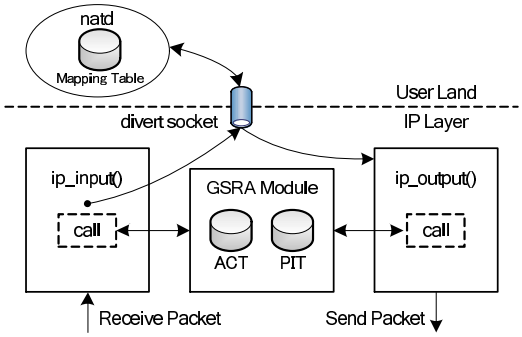

図 5.2　GSRA ルータの実装

第6章　評価

本章では，既存のリモートアクセス方式と GSRAv2 を，機能面および性能測定結果から比較評価する．

6.1　機能面の比較

表 6.1 にリモートアクセス方式の比較を示す．各項目の詳細は以下の通りである．

- E2E 暗号化の可否：GSRAv2 では，IN に PCCOM の機能を追加することでエンドエンドの暗号化通信が可能である．SSL-VPN では，VPN サーバ-IN 間も https 通信を行うことが可能である．その他の方式では，EN-VPN サーバ装置間が暗号化区間となる．社内犯等の存在を考慮すると，ローカルネットワークを通過するパケットも暗号化可能である方が望ましいといえる．
- スループット：パケットのカプセル化を行う方式では，ヘッダオーバヘッドが増加し，通信の性能が劣化する．パケットのカプセル化は，パケットを暗号化するためと，パケットをトンネリングするための 2 パターンがあり，OpenVPN と PacketiX VPN では 2 重のカプセル化オーバヘッドが発生する．PacketiX VPN はトンネリングのために Ethernet フレームを TCP でカプセル化するため，TCP over TCP の問題が起きる．GSRA ではパケットに変更を加えないため，カプセル化による性能の劣化は起こらない．表内の評価は，次節で述べる実測値を評価基準とした．
- HR 対応：IPsec-VPN は，HR が IPsec パススルー機能に対応している必要がある．その他の方式では，HR を通過することが可能である．しかし，HR が存在するこ

表 6.1　リモートアクセス方式の比較

	IPsec-VPN	SSL-VPN	OpenVPN	PacketiX	GSRAv2
E2E 暗号化の可否	×	○	×	×	○
スループット	×	△	△	×	○
HR 対応	△	○	△	△	○
クライアントソフトの必要性	△	△	×	×	×
アプリケーションの制約	○	×	○	○	○
アドレス管理の必要性	×	○	×	×	○

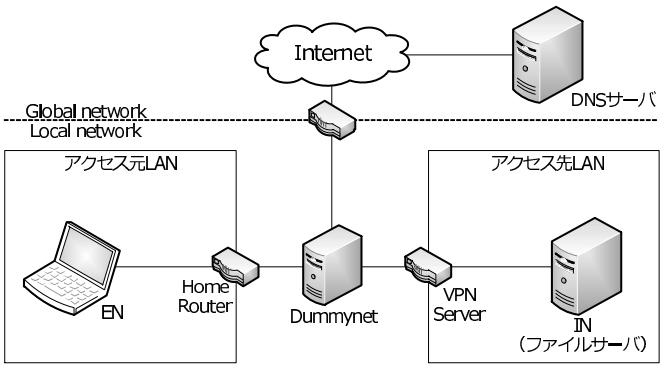

図 6.1　測定環境

とで，IPsec-VPN，OpenVPN，PacketiX VPN ではアドレス管理に注意する必要が出てくる．すなわち，EN のプライベートアドレスと，VPN の通信に使用するアドレスが重複しないように管理しなければならない．

- クライアントソフトの必要性：SSL-VPN は Web ブラウザさえあれば使用できるが，クライアントを認証する場合は証明書を持たせる必要がある．IPsec-VPN は，多くの OS で標準でサポートしているものの，機能を有効にするためにはユーザによる設定の変更を必要とする場合がある．OpenVPN と PacketiX VPN，GSRA の 3 方式では，クライアント端末に専用ソフトウェアをインストールする必要がある．

- アプリケーションの制約：SSL-VPN は，使用するアプリケーションが Web ブラウザベースのものに制限される．その他の方式ではアプリケーションの制限は無い．

- アドレス管理の必要性：IPsec-VPN，OpenVPN，PacketiX VPN では，リモートアクセスに使用するアドレスと実環境のアドレスが重複しないよう注意し，管理する必要がある．各方式とも，DHCP のように VPN サーバ側からアドレスを配布する仕組みが用意されており，これを使用することでアクセス先 LAN で元々使用されているアドレスとの重複は防げるが，配布されたアドレスがアクセス元 LAN 内で使用されているアドレスと重複してしまう可能性がある．

以上の比較から，GSRAv2 は既存方式に比べ，機能的に優れているといえる．

6.2　実装と性能評価

FreeBSD に実装した提案方式を使用し，通信開始時に発生するオーバヘッド時間及び，スループットを測定した．比較対象は，アプリケーションに制約のない IPsec-VPN，OpenVPN，PacketiX VPN の 3 方式とした． 本論文で使用した測定環境を図 6.1 に示す．各装置の諸元は表 6.2 に示す通りである．アクセス元 LAN とアクセス先 LAN の間はインターネットを想定し，擬似的に背景負荷をかけることができる Dummynet [19] を使用

表 6.2　諸元

	OS	CPU	Memory	NIC
EN	FreeBSD 7.2[1]	Pentium4 3.40 GHz	1 GB	1000Base-TX
Home Router	FreeBSD 7.2	Pentium4 3.00 GHz	512 MB	1000Base-TX
Dummynet	FreeBSD 8.0	Pentium4 2.80 GHz	512 MB	1000Base-TX
VPN Server	FreeBSD 7.2	Pentium4 3.40 GHz	2 GB	1000Base-TX
IN	FreeBSD 7.2	Pentium4 2.80 GHz	1 GB	1000Base-TX

[1]PacketiX VPN のみ Windows 7 32bit

表 6.3　Dummynet の設定値

	伝送遅延	パケットロス率
設定 A	0	0
設定 B	10 ms	0
設定 C	10 ms	0.05 %

した．Dummynet の設定値は，表 6.3 に示す 3 パターンを用意した．設定 A は，伝送遅延，パケットロス率ともに 0 で，Dummynet が無いものと等価である．この設定では，各方式の最大の性能を測定できる．これは，同一オフィス内の他部署との限定的なネットワーク接続などに使用する場合のスループット目安となる．設定 B は，伝送遅延のみ発生し，パケットロスがない設定である．距離は離れているが，回線が高品質であるなどの理由からパケットロスが発生しない場合のスループットの目安となる．設定 C は，伝送遅延とパケットロスの両方が発生する設定である．最も多い利用シーンとして想定される，インターネットを経由したリモートアクセス時の目安となる．パケットロス率の設定値は，自宅 LAN と大学の研究室 LAN 間の 4 週間分の実測値（付録 B）に基づいて決定した．公平な比較を行うため，各方式とも，暗号化アルゴリズムには AES（鍵長 128bit）を使用し，暗号化範囲は EN-VPN サーバ間とした．IPsec-VPN の鍵交換プロトコルは IKEv2 を使用した．OpenVPN のパケットのカプセル化は，TCP，UDP 両方に対応しているが，TCP over TCP の問題を避けるため，UDP を選択した．オーバヘッド時間，スループットの測定は全ての条件において 10 回ずつ行い，その平均値を測定結果とした．

6.2.1　通信開始時に発生するオーバヘッド時間の比較

リモートアクセスによる通信の開始時には，専用の処理に伴う追加のオーバヘッド時間が発生する．それぞれの方式で発生するオーバヘッド時間を測定した．

(1) 測定方法

通信開始時のオーバヘッド時間の測定には，パケットキャプチャソフト Wire-

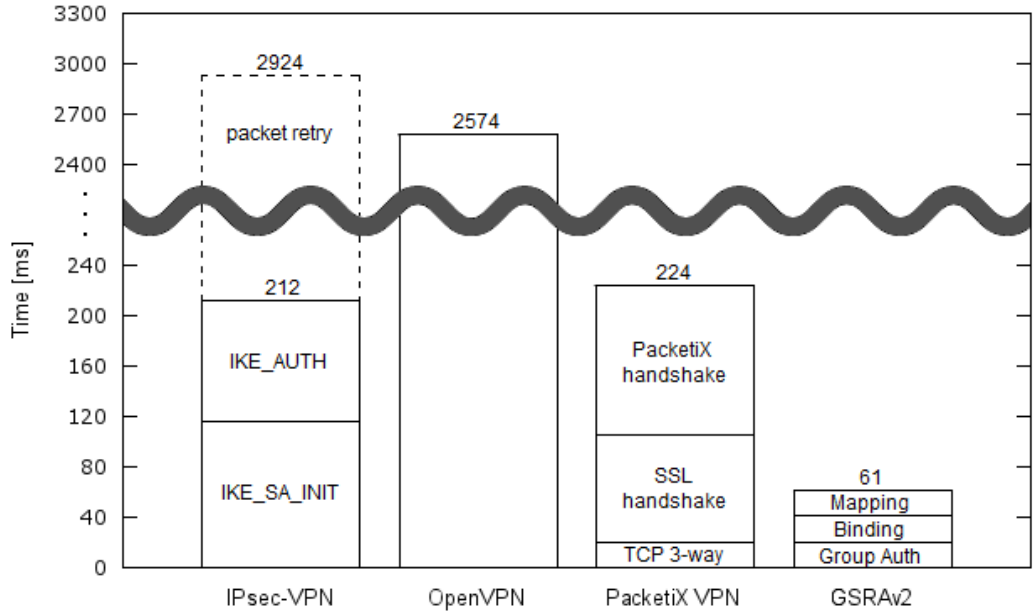

図 6.2　ネゴシエーション時間内訳

shark[2]を用いた．EN で Wireshark によるキャプチャを行い，ネゴシエーションパケットが送受信される時間の差から測定結果を得た．OpenVPN と PacketiX VPN は，ネゴシエーションのみを単独で行うことができるが，IPsec-VPN と GSRAv2 では，特定の宛先のパケットが初めて送信されるときにネゴシエーションが開始される．そのため，`wget` コマンド[3]を使用して IN 上のファイルにアクセスすることでネゴシエーションを開始させた．`wget` は UNIX のコマンドライン上で HTTP や FTP 経由のファイル取得を行えるツールであり，同時にスループットの計測も行うことができる．測定する区間は，ネゴシエーション開始から完了までの時間（ネゴシエーション時間）と，ネゴシエーション開始からネゴシエーション完了後に実際の通信が開始されるまでの時間（総オーバヘッド時間）の 2 区間とした．これは方式によって，実際の通信パケットが送信されるまでにタイムラグが生じる場合があるためであり，実際に利用する際には後者の数値が重要となる．

(2) 測定結果と考察

測定の結果を図 6.2 に示す．

IPsec-VPN によるネゴシエーションは，IKE 用の SA を確立する IKE_SA_INIT と，IPsec 通信用の SA の確立を行う IKE_AUTH の 2 往復からなり，200ms 程度のオーバヘッドが発生している．流れるパケットは 2 往復だけであるため，2RTT=40ms を除いた約 172ms が，暗号鍵の生成などの内部処理に費やされていることになる．また，総オーバヘッド時間を見ると，ネゴシエーション完了から大きなタイムラグが

[2]http://www.wireshark.org/
[3]http://www.gnu.org/software/wget/

発生し，合計で約 3 秒となっている．この理由は，IPsec-VPN ではネゴシエーション開始のトリガとなったパケットが失われるためである．失われたパケットは，アプリケーションにより再送されるのを待つ必要があるため，通信開始までの時間が大きくなる．今回は `wget`（TCP）による測定であり，標準的な TCP の再送時間である 3 秒程度が上乗せされる結果になっている．図 6.2 では，ネゴシエーション部の時間を実線で，パケットの再送待ち時間をを破線で示している．

OpenVPN は，ネゴシエーション完了までに約 2.5 秒の時間がかかっている．処理中のパケットはすべて SSL で暗号化されるため処理時間の内訳は分からないが，VPN 用トンネルの生成や，サーバ・クライアントの SSL による認証など，計 50 往復以上のパケットのやりとりが行われる．パケットの往復数が多いため，RTT が 20ms よりも長い環境では，オーバヘッド時間が大きく延びると考えれられる．

PacketiX VPN は，SSL による認証の他に行われる処理は多くなく，IPsec-VPN と同じく 200ms 程でネゴシエーションが完了している．本測定では，EN の仮想 NIC に割り当てる IP アドレスをあらかじめ固定で設定したため，アクセス先 LAN の DHCP サーバから IP アドレスを配布する場合や，PacketiX VPN の SecureNAT 機能などを使用する場合には，その分の時間が上乗せされることになる．

GSRAv2 は，通信開始まで約 60ms で完了している．GSRAv2 ネゴシエーションでは，バインディング処理が追加され，計 3 往復のパケットがやりとりされるが，通信経路上には Dummynet により 1 往復あたり 20ms の遅延が発生しており，3 往復の RTT だけで 60ms が必要となる．このことから，EN と GSRA ルータにおける内部処理時間は非常に短いと言える．また，トリガとなったパケットは，ネゴシエーション中も保持されるため，ネゴシエーション完了後すぐに通信を開始することができる．

以上から，インターネットを経由した場合の RTT を想定した環境において，GSRAv2 は最も短時間で通信を開始できることが確認できた．

6.2.2 スループットの比較

リモートアクセスによる通信は，通信経路上や端末で追加の処理が発生するため，通常よりもスループットが低下する．それぞれの方式で，リモートアクセスによる通信のスループットを測定した．

(1) 測定方法

スループットは，EN がリモートアクセスにより IN へ接続し，`wget` コマンドを用いて IN 上に保存されているファイルをダウンロードすることで測定した．測定値には `wget` による測定結果をそのまま採用した．ダウンロード対象のファイルには，1GB のダミーファイルを用意した．

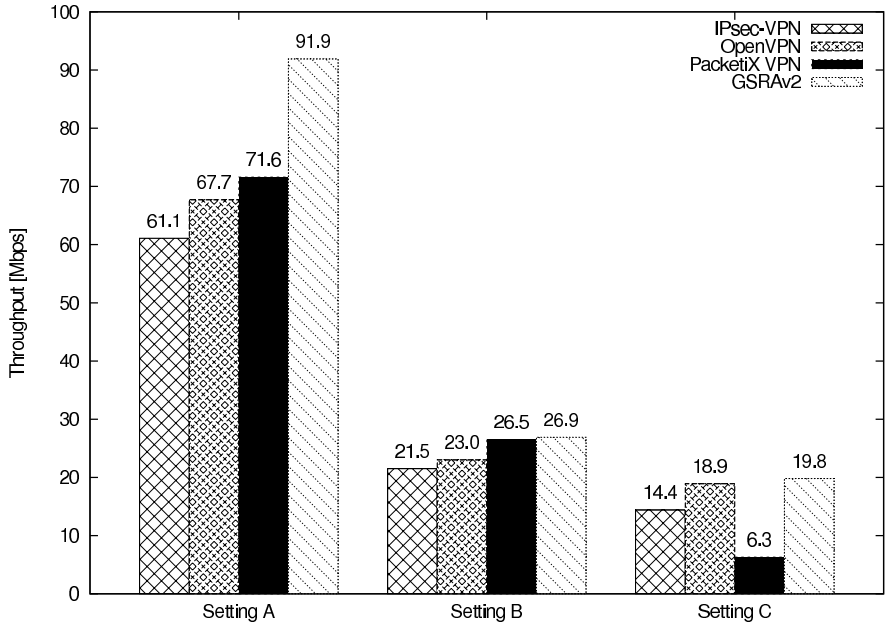

図 6.3　スループット測定結果

(2) 測定結果と考察

設定 A では，GSRAv2 のスループットが最も高く，他方式に比べ約 1.3 倍以上の速度を記録している．処理ネックとなる部分を解析したところ，HR で動作している NAT の処理がボトルネックになっていることが分かった．IPsec-VPN，OpenVPN，PacketiX VPN は，パケットをカプセル化して転送するため，追加のヘッダオーバヘッドやフラグメントが起こりスループットが低下する．GSRA で使用している暗号化プロトコル PCCOM は，暗号化時にパケットフォーマットを変更する必要がなく，カプセル化を必要としないため，上記の要因によるスループット低下が起きない．

設定 B では，1 秒間に送受信できる回数に制限が生まれる．RTT20ms の場合であれば，50 往復が上限となる．ここで，TCP のウィンドウ制御におけるウィンドウサイズの最大値は 64KB であるため，64 × 1024 × 50 × 8=26.2Mbps が理論上の上限となる．そのため，どの方式でもそれ以下のスループットに落ち着いている．その中でも GSRAv2 が最もスループットが高く，ほぼ理論値と同等の結果を得られている．理論値を若干超えているのは，`wget` による測定の誤差と考えられる．設定 A と同じく GSRAv2 が最も早いという結果となったが，他方式との差が小さくなっている．RTT やパケットロスが発生する環境（設定 B，C）では，通信路に起因するスループット低下のウエイトが大きく，カプセル化などの影響が小さくなっていると考えられる．

設定 C では，パケットロスの発生により，どの方式でも設定 B よりスループットが低下している．中でも，PacketiX VPN は大きくスループットが低下した．こ

れは，TCP Over TCP の問題が顕在化した結果といえる．PacketiX VPN では，この問題を改善するための機能を実装しているが，今回の測定では効果が見られなかった（付録 C）．

測定結果より，GSRAv2 は全てのケースにおいて既存方式を上回るスループットを発揮することが確認できた．

第7章　まとめ

本論文では，GSRA のシーケンスを見直し，HR 配下からのリモートアクセスを可能にした GSRAv2 を提案した．GSRAv2 は，グループの概念を用いることにより，簡単かつ柔軟なアクセス管理が可能である点や，カプセル化をしないことで余計なヘッダオーバヘッドが発生しない点など，GSRA の特長をそのまま受け継いでいる．さらに，特殊なバインディング処理を追加することにより，SPI 機能の有無に関わらず，HR 配下からリモートアクセスを開始することが可能になった．

また，実機を使用した性能測定を通じ，既存の方式と比較を行った．その結果，GSRAv2 は通信開始までのオーバヘッド時間が最も短く，あらゆる環境において高スループットを発揮できることを確認した．

今後は，Windows をはじめとした他の OS のへの実装を進め，普及を目指していく．

謝辞

本研究を遂行するにあたり，多大なるご指導，ご鞭撻を賜りました，名城大学大学院理工学研究科渡邊晃教授に心より厚く御礼申し上げます．

本論文をまとめるにあたり，有益な御助言をして頂きました，名城大学大学院理工学研究科柳田康幸教授，鈴木秀和助教，旭健作助教に心より厚く御礼申し上げます．

日々の研究活動に対して様々な御指導を頂きました名城大学理工学部情報工学科の鈴木秀和助教に心より感謝致します．

本研究を遂行するにあたり，有益なご助言，適切なご検討をいただいた，渡邊研究室，鈴木研究室，旭研究室の皆様に心より感謝いたします．

参考文献

[1] Hamzeh, K., Pall, G., Verthein, W., Taarud, J., Little, W. and Zorn, G.: Point-to-Point Tunneling Protocol (PPTP), RFC 2637, IETF (1999).

[2] Townsley, W., Valencia, A., Rubens, A., Pall, G., Zorn, G. and Palter, B.: Layer Two Tunneling Protocol “L2TP”, RFC 2661, IETF (1999).

[3] Kent, S. and Seo, K.: Security Architecture for the Internet Protocol, RFC 4301, IETF (2005).

[4] Dierks, T. and Rescorla, E.: The Transport Layer Security (TLS) Protocol, RFC 5246, IETF (2008).

[5] OpenVPN Technologies, Inc.: OpenVPN - Open Source VPN. http://openvpn.net/

[6] Corporation., S.: PacketiX VPN 3.0 Web サイト. http://www.softether.co.jp/jp/vpn3/

[7] Zorn, G.: Microsoft PPP CHAP Extensions, Version 2, RFC 2759, IETF (2000).

[8] Rivest, R.: The MD4 Message-Digest Algorithm, RFC 1320, IETF (1992).

[9] Brown, R. H. and Good, M. L.: DATA ENCRYPTION STANDARD (DES), FIPS 46-3, NIST (1999).

[10] Olaf Titz: Why TCP Over TCP Is A Bad Idea. http://sites.inka.de/sites/bigred/devel/tcp-tcp.html

[11] 鈴木秀和，渡邊　晃：通信グループに基づくサービスの制御が可能な NAT 越えシステムの提案，情報処理学会論文誌，Vol. 51, No. 9, pp. 1881–1891 (2010).

[12] 鈴木健太，鈴木秀和，渡邊　晃：NAT 越え技術を応用したリモートアクセス方式の提案と設計，マルチメディア，分散，協調とモバイル（DICOMO2010）シンポジウム論文集，Vol. 2010, No. 1, pp. 288–294 (2010).

[13] 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).

[14] C.Kaufman, P.Hoffman, Y.Nir and P.Eronen: Internet Key Exchange Protocol Version 2 (IKEv2), RFC 5996, IETF (2010).

[15] M.Krasnyansky: Universal TUN/TAP device driver. http://www.kernel.org/pub/linux/kernel/people/marcelo/linux-2.4/Documentation/networking/tuntap.txt

[16] 増田真也, 鈴木秀和, 岡崎直宣, 渡邊　晃：NATやファイアウォールと共存できる暗号通信方式PCCOMの提案と実装，情報処理学会論文誌，Vol. 47, No. 7, pp. 2258–2266 (2006).

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

[18] Ford, B., Srisuresh, P. and Kegel, D.: Peer-to-Peer Communication Across Network Address Translators (2005).
http://www.brynosaurus.com/pub/net/p2pnat/

[19] L.Rizzo: Dummynet home page.
http://info.iet.unipi.it/ luigi/dummynet/

研究業績

学術論文

なし

国内会議（査読あり）

1. 鈴木健太, 鈴木秀和, 渡邊晃 “NAT 越え技術を応用したリモートアクセス方式の提案と設計”，マルチメディア，分散，協調とモバイル（DICOMO2010）シンポジウム論文集, Vol.2010，No.1，pp.288-294，Jul.2010.

2. 鈴木健太, 鈴木秀和, 渡邊晃 “リモートアクセス方式 GSRA の性能評価”，マルチメディア，分散，協調とモバイル（DICOMO2011）シンポジウム論文集，Vol.2011，No.1，pp.336-343，Jul.2011.

研究会・大会等

1. 鈴木健太, 鈴木秀和, 渡邊晃 “NAT-f を応用したリモートアクセス方式 GSRA の提案”，平成 21 年度電気関係学会東海支部連合大会論文集，Sep.2009.

2. 鈴木健太, 鈴木秀和, 渡邊晃 “NAT-f を応用したリモートアクセス方式 GSRA の提案と実装”，情報処理学会第 72 回全国大会講演論文集，Mar.2010.

3. 鈴木健太, 旭健作, 鈴木秀和, 渡邊晃 “自宅からのリモートアクセスを可能にする GSRAv2 の提案と評価”，情報処理学会研究報告，Vol.2012-DPS-150，No.30，pp.1–10，Mar.2012.

付 録A　記号の定義

- G_i （i = NodeID）：グローバル IP アドレス
- P_i：プライベート IP アドレス
- V_i：仮想 IP アドレス
- s,d,t,m：ポート番号
- $G_i : s$：トランスポートアドレス（IP アドレス G_i とポート番号 s の組）
- Group i：通信グループ番号
- GK i：Group i に対応するグループ鍵
- $G_i : s \leftrightarrow G_j : d$ ・・・ $G_i : s$ と $G_j : d$ の通信
- $G_i : s \Leftrightarrow G_j : d$ ・・・ $G_i : s$ と $G_j : d$ の変換

付 録B　パケットロス率の測定

スループットの測定に使用したパケットロス率の測定結果の詳細を表 B.1 に示す．また，曜日毎，1 時間毎の集計をグラフ化したものを図 B.1，図 B.2 に示す．

表 B.1　4 週間のパケットロス率集計

	日曜	月曜	火曜	水曜	木曜	金曜	土曜	平均
0 時	0.043	0.039	0.047	0.030	0.045	0.030	0.030	0.037
1 時	0.017	0.043	0.033	0.043	0.060	0.031	0.015	0.035
2 時	0.017	0.037	0.051	0.021	0.049	0.037	0.013	0.032
3 時	0.018	0.040	0.062	0.026	0.031	0.039	0.009	0.032
4 時	0.013	0.037	0.025	0.020	0.063	0.036	0.024	0.031
5 時	0.022	0.037	0.026	0.022	0.040	0.033	0.011	0.027
6 時	0.017	0.037	0.024	0.024	0.032	0.033	0.018	0.027
7 時	0.031	0.036	0.044	0.018	0.033	0.043	0.028	0.033
8 時	0.019	0.044	0.032	0.027	0.043	0.052	0.011	0.033
9 時	0.009	0.041	0.064	0.051	0.060	0.062	0.013	0.043
10 時	0.008	0.052	0.078	0.092	0.043	0.068	0.037	0.054
11 時	0.017	0.058	0.072	0.065	0.096	0.076	0.061	0.064
12 時	0.016	0.067	0.083	0.120	0.054	0.094	0.264	0.100
13 時	0.022	0.075	0.155	0.113	0.146	0.228	0.023	0.109
14 時	0.008	0.180	0.092	0.077	0.087	0.212	0.073	0.104
15 時	0.023	0.135	0.139	0.070	0.057	0.121	0.053	0.085
16 時	0.021	0.133	0.068	0.080	0.065	0.078	0.054	0.071
17 時	0.015	0.119	0.076	0.101	0.080	0.107	0.059	0.080
18 時	0.023	0.071	0.107	0.079	0.052	0.083	0.052	0.066
19 時	0.049	0.104	0.054	0.065	0.059	0.110	0.031	0.067
20 時	0.124	0.098	0.074	0.036	0.035	0.073	0.013	0.065
21 時	0.020	0.090	0.059	0.055	0.056	0.041	0.019	0.049
22 時	0.040	0.054	0.042	0.028	0.062	0.029	0.026	0.040
23 時	0.006	0.066	0.043	0.062	0.034	0.038	0.030	0.040
平均	0.025	0.070	0.065	0.055	0.058	0.073	0.040	0.055

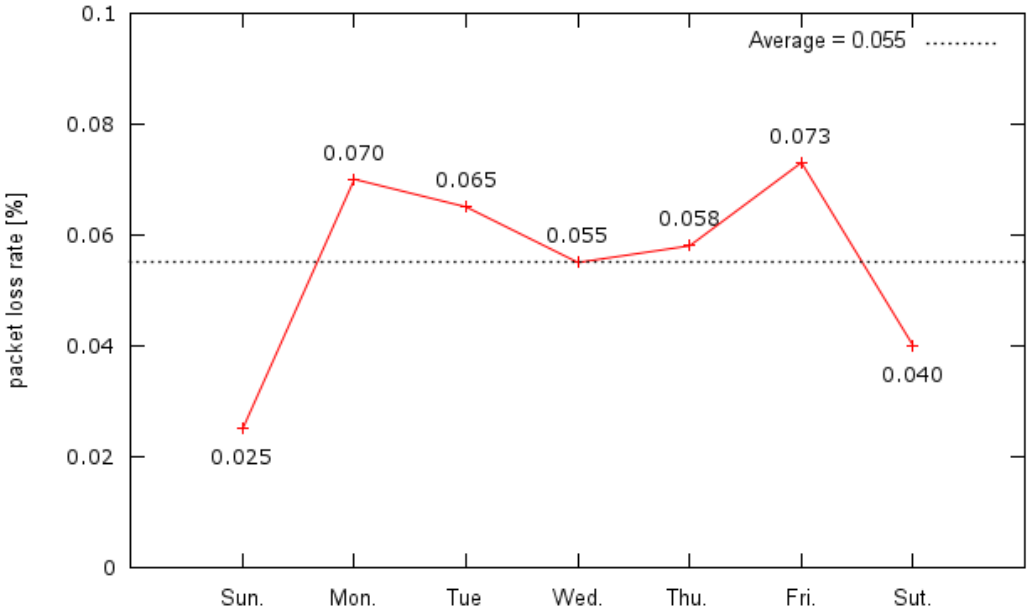

図 B.1　曜日毎のパケットロス率

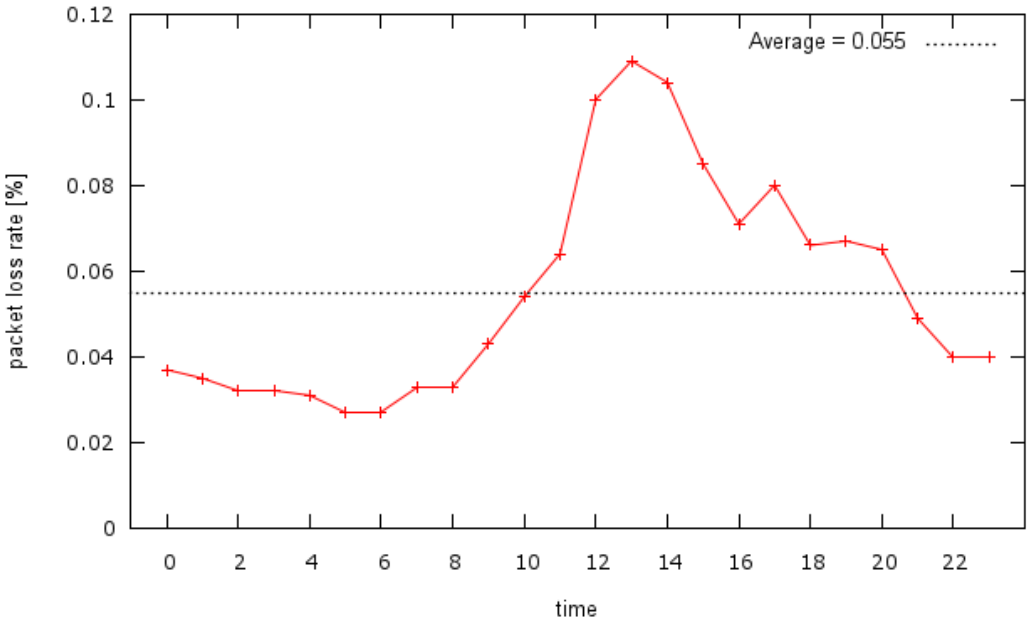

図 B.2　時間毎のパケットロス率

付 録C　PacketiX VPNの通信効率および安定性向上機能

PacketiX VPN では，1 つの VPN セッションに対して複数本の TCP コネクションを同時に確立し，並列的に使用して負荷分散させることによって，通信を高速化することができる機能がある．指定できる TCP コネクションの本数は，1 本〜32 本の範囲であり，デフォルトでは 1 本となっている．PacketiX VPN 3.0 のマニュアルでは，この機能を使用することで，通信遅延が大きいネットワークや，帯域を制限しているようなネットワークにおける通信効率を向上させることができるとしている[1]．本文中の測定結果は，TCP コネクション数 1 本の場合の結果である．この機能を使用して，TCP コネクション数を増加させた場合のスループットの変化を測定した．測定の環境，方法は本文中と同一であり，背景負荷は設定 C を適用した．結果を図 C.1 に示す．本測定環境においては，TCP コネクションの数を増加させてもスループットに向上が見られなかった．

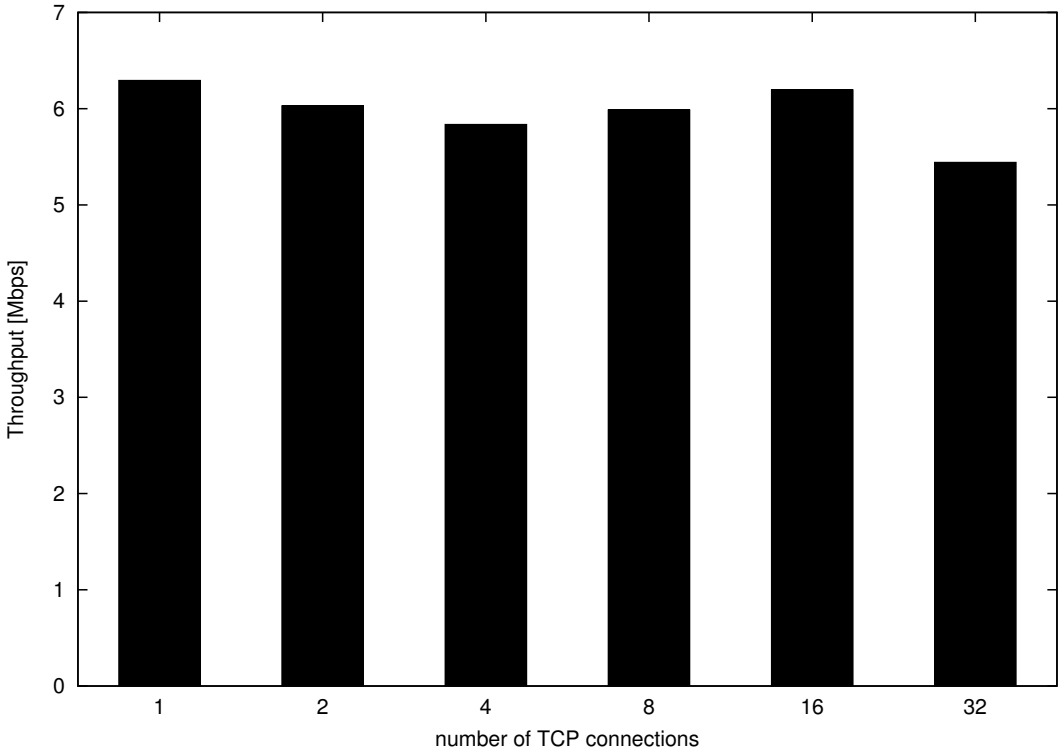

図 C.1　TCP コネクション数を変化させた場合のスループット

[1] http://www.softether.co.jp/jp/vpn3/manual/web/2-1.aspx#vpn_2_1_3