マルチメディア通信と分散処理　111－6
コンピュータセキュリティ　20－6
（２００３．２．２７）

IP通信拡散法を用いたVPN装置の性能評価

東京電機大学 理工学部 情報システム工学科
齊藤 孝紀　堀池 唯人　長田 慎司　宮崎 正光　桧垣 博章
埼玉県工業技術センター 北部研究所
森田 俊英　斉藤 弘美

TCP/IP インターネットを介して、物理的に離れた複数の LAN を論理的に接続する VPN(Virtual Private Network) への要求が高まっている。ここでは、LAN を相互接続するインターネットにおいて、IP データグラムを盗聴されることなく、安全に配送することが求められる。本論文では、暗号技術と組み合わせてより安全な通信路を実現するための IP 通信拡散手法と、それを利用した VPN 装置について述べる。本手法は、IP の機能であるソースルーティングを用いずに、動的に決定する複数の経路を用いた配送を実現する。また、この経路制御において中継点として利用されるルータへのオーバヘッドを評価し、実用的なオーバヘッドであることを明らかとした。

Performance Evaluation of Dynamic Multi-Path IP Transmission

Takanori Saitou, Tadato Horiike, Shinji Osada, Masamitu Miyazaki and Hiroaki Higaki
Department of Computers and Systems Engineering
Tokyo Denki University
Hidetoshi Morita, Hiromi Saitou
North Laboratory
Saitama Industrial Technology Center

For achieving secure communication against snooping, encryption is applied in the TCP/IP Internet. It is based on that too much computation is required for snooper to get an original data from an encrypted data. Hence, the higher performing computers are developed, the more complex encryption algorithms have to be designed and implemented. This paper proposes a novel methodology that IP datagrams are transmitted through multiple paths detected dynamically. Since no additional function is introduced in routers, it is highly applicable. Finally, we evaluate overhead on the router in which ICMP encapsulated packets are processed and the result shows the proposed method is reasonablly implemented in the Internet.

1　背景と目的

電子メールや WWW (World Wide Web) サービスの普及により、企業や個人の多くにインターネットを利用する環境が普及してきている。また、近年の ISDN、ADSL、CATV、光ファイバーの普及により、アクセスネットワークの高速広帯域化が著しく、これにともなって ISP (Internet Service Provider) のバックボーンネットワークの高速広帯域化も進み、マルチメディアデータの実時間配送など、サービスの高度化、多様化が可能となっている。このように、企業活動、社会活動のインフラストラクチャとしてのインターネットの地位が高まるなかで、第三者に情報が遺漏することなく、安全にコンピュータ間で情報を交換するためのセキュリティ技術への要求が高まっている。インターネットを用いて交換しているデータを悪意のある第三者が不当に入手することを避けるために、暗号通信が広く利用されている。TCP/IP インターネットにおけるネットワーク層プロトコルである IP (Internet Protocol) [2] には、暗号通信の機能は含まれていない。そこで、アプリケーションにおいてデータの暗号化を行なったり、IPsec を用いて IP データグラムのデータ部を暗号化するなどの手法が採られている。

暗号通信を実現するために、様々な暗号アルゴリズムが提案されているが、いずれの方法も、復号鍵を持たないで暗号文から平文を入手する (あるいは復号鍵を推定する) ために必要とされる計算量の大きさのみに、その安全性の根拠を置いている。そのため、悪意のある第三者が、ある暗号アルゴリズムを用いて作られた暗号文から平文を入手するために十分な計算能力を持つコンピュータを入手するたびに、新しい暗号アルゴリズムを導入しなければならない。多数のコンピュータが相互接続されているインターネット環境においては、新しい機能をすべてのコンピュータに頻繁に導入することは困難である。したがって、コンピュータの計算能力の向上とは無関係に、暗号通信をより頑強にする手法の導入が求められている。

本論文では、ひとつのデータを配送するための複数の IP データグラムを複数の経路を用いて配送することによって、盗聴者がデータを得ることを困難にする手法

を提案し、その実現プロトコルを設計する。ここで、複数の経路を固定的に定めるのではなく、通信要求が発生するごとに動的に決定することによって、盗聴者が IP データグラムの通過するルータを特定することを困難にしている。また、提案手法を実現するためには、送信元コンピュータと送信先コンピュータに本論文で提案する機能が導入されていればよく、インターネットのルータには、特殊な機能を導入する必要がない点で適用性に優れている。提案手法を Linux オペレーティングシステムがインストールされたパーソナルコンピュータに実装する方法について論じる。本手法では、経路を拡散させるために中継点として利用するルータへのオーバヘッドが通常の IP データグラム配送に比べて多きくなることが考えられる。そこで、このオーバヘッドを評価し、インターネット環境での適用可能性について議論する。

2 従来手法

TCP/IP インターネットにおけるセキュリティの脅威として主なものには、組織 LAN への攻撃と組織 LAN 間の通信への攻撃がある。前者の解決策としてファイアウォールがある。これは、インターネットと組織 LAN との境界にファイアウォールの機能を持つルータ装置を配置することによって実現される。ファイアウォール装置では、プロトコル各階層において、通過させるパケットと通過させないパケットとを振り分けるパケットフィルタリングが機能する。例えば、送信元IP アドレス、送信先 IP アドレス、送信先ポート番号の 3 項組に対して、通過と破棄の基準を与えるものがある。一方、後者の解決策として VPN (Virtual Private Network) がある。VPN は、インターネットに接続されている複数の組織 LAN をインターネットを介して論理的に接続し、アプリケーションに対しては、異なる組織 LAN に属するコンピュータ間の通信が同一 LAN 内の通信と同等に見せることができる技術である。このとき、各組織 LAN 間は専用線ではなく、インターネットを用いていることから、組織 LAN 間の通信の安全性を確保することが必要である。これを実現するには、IPsec などを利用した暗号通信を用いることが必要である。暗号通信技術は、送信元と送信先で共通の秘密情報 (鍵) を持つことを前提とする秘密鍵暗号技術と秘密情報を持つことを前提としない公開鍵暗号とがある。前者には、DES、IDEA 等がある。また、後者には、RSA、Diffie-Hellman、Merkle-Hellman 等がある。これらの暗号通信技術は、暗号文を入手した盗聴者であっても、そこから平文を入手するために必要な計算を、現在のコンピュータ技術では十分短時間には実行できないことに安全性の根拠を置いている。したがって、コンピュータの計算能力の向上とともに、使用されている暗号通信技術は陳腐化していくことになる。本論文で提案する IP 通信拡散手法は、この暗号通信技術の強度を、コンピュータの計算能力の向上に無関係に補完する技術である。ここでは、あるデータを搬送する IP データグラム群を複数の経路に分割することによって、データを盗聴するのに十分な IP データグラムの入手を困難にする。

3 提案手法

3.1 IP 通信拡散手法

TCP/IP インターネットに接続された 2 台のコンピュータ c_s と c_d の間で、悪意のある第三者 M (以下では盗聴者とよぶ) にデータを盗聴されることなく安全に通信する方法として、本論文では、IP 通信拡散手法を提案する。IP 通信拡散手法では、c_s から c_d へデータ D を配送するための IP データグラム群 $G_D = \{IP_0, \ldots, IP_{n-1}\}$ を、N 個のサブグループ $\forall SG^i_D \subset G_D$ $(i = 0, \ldots, N-1)$ (ただし、$\cup_i SG^i_D = G_D$ かつ $\forall i \neq \forall i'$, $SG_i \cap SG_{i'} = \emptyset$) に分割する。また、$D$ を送信するコンピュータ c_s は、c_s から c_d への N 個の経路 $r^i_{\langle s,d\rangle} = \langle c^i_0 = c_s, c^i_1, \ldots, c^i_{l(i)-1}, c^i_{l(i)} = c_d\rangle$ $(i = 0, \ldots, N-1)$ を探索する。そして、サブグループ SG^i_D に属する IP データグラムを経路 $r^i_{\langle s,d\rangle}$ を用いて配送する。これによって、盗聴者 M がデータ D を配送する IP データグラム群 G_D のすべてを入手するためには、N 個の経路すべてを監視しなければならない。すなわち、ルータ $\forall i, 0 < \exists k(i) < l(i), c^i_{k(i)}$ もしくは通信路 $\forall i, 0 \leq \exists k(i) < l(i), \langle c^i_{k(i)}, c^i_{k(i)+1}\rangle$ において、SG^i_D に属する IP パケットをすべて入手しなければならない。特に、c_s に存在するアプリケーションプロセス AP_s から c_d に存在するアプリケーションプロセス AP_d へ渡されるデータ D_{orig} の暗号化データ $D = encrypt(D_{orig})$ が配送される場合には、サブグループ SG^i_D の分割方法によって、D の獲得をより困難にすることも可能である。

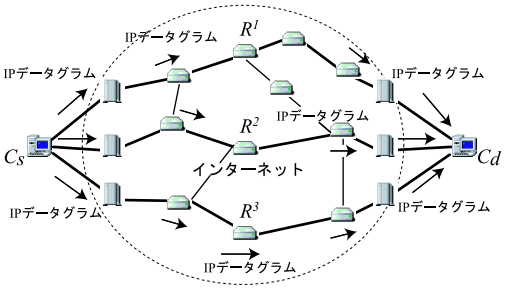

図 1: IP 通信拡散における中継ルータ

ここで、盗聴者 M によるデータ入手を困難にするためには、以下の条件を満たすことが求められる。

- 経路 $r^i_{\langle s,d\rangle}$ を M が事前に入手することが不可能 (困難) である。
- 経路 $r^i_{\langle s,d\rangle}$ に共通するルータが存在しない (少ない)。

事前に盗聴者 M が経路 $r^i_{\langle s,d\rangle}$ $(i = 0, \ldots, N-1)$ を知ることが可能であるならば、それぞれの経路上のルータ $c^i_{m(i)} \in r^i_{\langle s,d\rangle}$ あるいは通信路 $\langle c^i_{m(i)}, c^i_{m(i)+1}\rangle$ (ただし、$0 \leq m(i) < l(i)$) に盗聴者 M_i を配置することによって、データ D を入手することが可能である。これを回避するために、IP 通信拡散手法においては、データの配送要求が発生するごとにオンデマンドで経路を探

索し、決定する。このとき、経路探索手続きにランダムネスを入れることによって、盗聴者 M が M_i の配置位置を決定することを困難にしている。

また、2つの経路 $r^i_{\langle s,d\rangle}, r^{i'}_{\langle s,d\rangle}$ $(0 \leq i < i' < N)$ に共通のルータ $\exists cc_{\{i,i'\}} \in r^i_{\langle s,d\rangle} \cap r^{i'}_{\langle s,d\rangle}$ (ただし $cc_{\{i,i'\}} \neq c_s$ かつ $cc_{\{i,i'\}} \neq c_d$) が存在するならば、このルータ $cc_{\{i,i'\}}$ あるいはこれに直接接続する共通の通信路に盗聴者 M_i を配置してデータ D を配送するためのIPデータグラム群 G_D の一部を入手する可能性が高くなる。最も極端な場合として、ルータ $\exists cc \in \cap_i r^i_{\langle s,d\rangle}$ (ただし、$cc \neq c_s$ かつ $cc \neq c_d$) が存在するならば、盗聴者 M_i が cc もしくはこれに接続する共通の通信路に配置された場合、D を配送するためのすべてのIPデータグラムを入手することが可能となる。この問題を回避するためには、経路拡散の度合 (以下では、拡散度とよぶ) を大きくすればよいと考えられる。すなわち、c_s から c_d への最短経路 (一般的にルーティングテーブルに従って配送される経路は、この経路である) からより離れた複数の経路を選択することで、選択の自由度が大きくなり、共通のルータを含む可能性が低下する。しかし、拡散度を大きくすると、経路長 $l(i)$ が大きくなることが一般的に成立する。IPネットワークでは、各IPデータグラムが独立に配送されるが、上位層のプロトコルを介してアプリケーションプロセス AP_s と AP_d との間でデータ D_{orig} を配送するために要する時間は、最も遅延したIPデータグラムの配送時間によって支配される。すなわち、$\max_i l(i)$ をより小さく抑えることが要求される。

3.2 中継ルータ決定方法

IPデータグラム群 $G_D = \{IP_0, \ldots, IP_{n-1}\}$ を、送信元コンピュータ c_s から送信先コンピュータ c_d まで複数の経路 $r^i_{\langle s,d\rangle}$ を用いて配送するための方法を考える。IPv4には、ソースルーティングの機能がある。これは、オプション機能として定義されており、送信元コンピュータ c_s において、送信するIPデータグラムのヘッダのオプション部に中継点のルータのIPアドレスを列挙することによって、このIPデータグラムをそれらのルータを順番に通過して、送信先コンピュータ c_d へと配送することができる。しかし、IPヘッダの最大サイズは60バイト (ヘッダ長を格納するフィールドのサイズは4ビットであり、ここには4バイトを単位とした値を格納することから) に制限されており、必修フィールドのサイズが20バイトであることから、オプションの最大サイズは40バイトであり、ソースルーティングのための中継ルータを最大10個 (IPアドレスが4バイトであることから) しか格納することができない。基地局を含まないモバイルネットワークであるアドホックネットワークを対象として、送信元モバイルコンピュータがオンデマンドに送信先モバイルコンピュータまでの経路を探索し、データパケットをソースルーティングするプロトコルが研究開発されている [1,4]。このように、IPデータグラムを中継するルータのアドレスのすべてをヘッダ部に列挙する専用プロトコルを導入し、ソースルーティングを実現する方法が考えられる。しかし、IP拡散通信手法を実現するためにこのような方法を導入するには、インターネットに存在するすべてのルータが新しいプロトコルに従ってIPデータグラムを処理することが必要となる。このように、インターネットに対して変更を加えることなく、既存のルータが持つ機能の範囲内で提案手法を実現することが必要である。

[要求条件]
IP通信拡散手法を適用するための特殊な機能を中継ルータに導入することを前提としない。□

本論文では、送信元コンピュータが中継ルータを1つだけ指定することとする。すなわち、送信元コンピュータ c_s は、データ D を配送するためのIPデータグラム群 $G_D = \{IP_0, \ldots, IP_{n-1}\}$ を、N 個のサブグループ SG^i_D $(i = 0, \ldots, N-1)$ に分割するとともに、N 個の中継ルータ R^i を決定する。そして、各サブグループ SG^i_D に属するIPデータグラムを中継ルータ R_i を含む経路 $r^i_{\langle s,d\rangle} = \langle c^i_0 = c_s, c^i_1, \ldots, c^i_{r(i)} = R_i, \ldots, c^i_{l(i)-1}, c^i_{l(i)} = c_d\rangle$ を用いて配送する。ここで、送信元コンピュータ c_s から中継ルータ R_i までの $r^i_{\langle s,d\rangle}$ の部分経路 $\langle c^i_0 = c_s, c^i_1, \ldots, c^i_{r(i)-1}, c^i_{r(i)} = R_i\rangle$ および $\langle c^i_{r(i)} = R_i, c^i_{r(i)+1}, \ldots, c^i_{l(i)-1}, c^i_{l(i)} = c_d\rangle$ に含まれるルータ $c^i_1, \ldots, c^i_{r(i)-1}$ および $c^i_{r(i)+1}, \ldots, c^i_{l(i)-1}$ は、それぞれ R_i および c_d を送信先コンピュータとするルーティングテーブルのエントリを参照することによって、各ルータが決定する。

[中継ルータの決定]

1. 送信元コンピュータ c_s は、送信先コンピュータ c_d までのホップ数 $hop_{\langle s,d\rangle}$ を以下の手順を用いて測定する。なお、このホップ数が c_s のキャッシュに保存されている場合には、その値を用いる。
   - 1-1. c_s は、送信元と送信先をそれぞれ c_s と c_d、TTLの初期値を T_{init} としたホップ数測定要求のためのIPデータグラム $hreq$ を送信する。
   - 1-2. c_d は、受信した $hreq$ のTTL値 T_{obsv} を得る。
   - 1-3. c_d は、送信元と送信先をそれぞれ c_d と c_s とし、T_{obsv} をデータ部に含むホップ数測定応答のためのIPデータグラム $hrep$ を送信する。
   - 1-4. c_s は、$hrep$ を受信すると、c_s から c_d までのホップ数 $hop_{\langle s,d\rangle} = T_{init} - T_{obsv}$ を得る。
2. c_s は、ルータのルーティングテーブルに従って配送された場合の c_d までの経路のホップ数 $hop_{\langle s,d\rangle}$ に対して、最適な拡散ホップ数 $hop_{\langle s,m\rangle} = dhop(hop_{\langle s,d\rangle})$ を求める。
3. c_s は、32ビットの乱数値を N 個生成することにより、仮想目標アドレス $vadd^i$ $(i = 0, \ldots, N-1)$ を得る。
4. c_s は、送信元を c_s、送信先アドレスを $vadd^i$、TTLを $hop_{\langle s,m\rangle}$、上位プロトコルを未定義のプロトコルとする中継ルータ検出のためのIPデータグラム $mreq$ を送信する。
5. c_s が、4. で送信したIPデータグラムに対応するICMPメッセージを受信する。

5-1. これが ICMP 時間切れメッセージであるならば、この ICMP メッセージの送信元 R^i を中継ルータのひとつに加える。

5-2. これが ICMP 到達不可能メッセージであるならば、$vadd^i$ を再生成し、4. へ戻る。

6. c_s は、自身から $hop_{\langle s,m \rangle}$ ホップだけ離れた N 個の中継ルータ R^i $(i = 0, \ldots, N-1)$ を得る。□

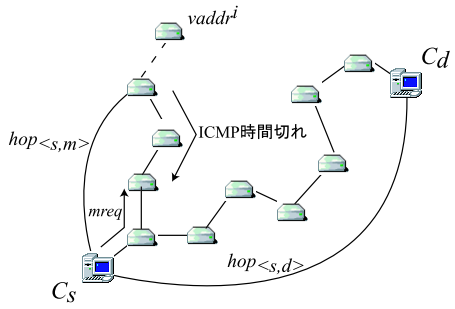

図 2: 中継ルータの決定

3.3 データ配送方法

送信元コンピュータ c_s から送信されるデータ D のための IP パケット群 G_D を分割した N 個のサブグループ SG_D^i $(i = 0, \ldots, N-1)$ のそれぞれを中継ルータ R^i を経由して、送信先コンピュータ c_d に配送する方法について論じる。

インターネット上のルータに特別な機能を導入することなく、特定のルータを経由して、IP データグラムを送信先コンピュータまで配送する方法として、以下の 2 つが考えられる。

- IP のソースルーティングオプションの利用
- IP トンネリングの利用

IPv4 には、オプションとしてソースルーティングが定められている。送信元コンピュータが IP ヘッダのオプション部に経由したいルータの IP アドレスを列挙し、各ルータが次に指定されたルータを経由するように転送することによって、指定されたルータを順番に経由して送信先コンピュータまで IP データグラムを配送することが実現されている。しかし、配送経路を指定した IP データグラムは、DoS 攻撃のための IP データグラムの配送や、悪意のあるデータを含んだ IP データグラムの送信元を偽るための踏台攻撃に利用される。そのため、現在利用されている多くのルータでは、ソースルーティングされた IP データグラムを受信してもそれを転送することはなく、ただちに破棄するように設定されている。

ルータが持つ機能で、受信したデータをそのまま送信するものとして、ICMP エコー [3] がある。ICMP エコー要求メッセージを受信したコンピュータ (ルータを含む) は、エコー要求の送信元コンピュータに対して、ICMP エコー応答メッセージを送信する。このとき、エコー要求メッセージに含まれるデータは、エコー応答メッセージにコピーされる。本論文では、この ICMP エコーを用いて、c_s からルータ R を経由して c_d へと IP データグラムを配送することを実現する。

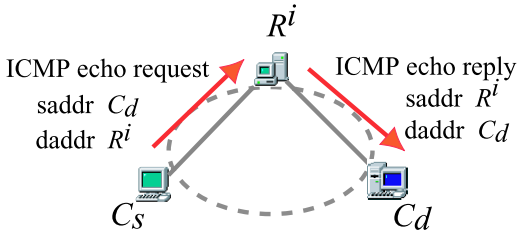

図 3: ICMP echo 処理を用いた経路制御

[IP データグラム配送]

1. 送信元コンピュータ c_s は、送信元を c_s、送信先を c_d とする IP データグラム IP_{real} を作成する。
2. c_s は、IP_{real} をデータ部に含む ICMP エコー要求メッセージ $ereq$ を作成する。
3. c_s は、$ereq$ をデータ部に含む IP データグラム $IP_{caps}(ereq)$ を作成し、送信する。このとき、送信元を c_d、送信先を R^i とする。
4. $IP_{caps}(ereq)$ を受信した各ルータは、ルーティングテーブルを参照し、R^i へと配送するように転送する。
5. R^i は、$IP_{caps}(ereq)$ を受信すると、対応する ICMP エコー応答メッセージ $erep$ を作成する。ここで、$erep$ のデータ部には、ICMP エコー要求メッセージに含まれていたデータ、すなわち IP_{real} がコピーされる。
6. R^i は、$erep$ をデータ部に含む IP データグラム $IP_{caps}(erep)$ を作成し、送信する。このとき、送信元は R^i、送信先は c_d となる。
7. $IP_{caps}(erep)$ を受信した各ルータは、ルーティングテーブルを参照し、c_d へと配送するように転送する。
8. c_d は、$IP_{caps}(erep)$ を受信すると、そこから IP_{real} を取り出す。□

4 VPN 装置の設計

前章で述べた IP 通信拡散方法により、TCP/IP インターネットに接続された複数の LAN L^i $(i = 0, \ldots, N-1)$ を論理的に接続し、ひとつの LAN としてアプリケーションに提供する VPN を実現することができる。それぞれの LAN L^i とインターネットとは、VPN 装置 v^i によって接続されている。v_i には、少なくとも 1 つの L^i へのインタフェースと少なくとも 1 つのインターネットへのインタフェースが存在する。インターネットへの接続が複数存在する場合もある。例えば、複数の ISP (Internet Service Provider) と契約する場合がこれにあたる。2 つの LAN L^i と L^j との間は、一般的には、v^i と v^j との間のトンネリングを利用することによって接続する。本章では、IP 通信拡散方法を用い、v^i と v^j の間に複数の経路を動的に決定し、それを用いて IP パケット群を配送することによって、盗聴が困難な通信環境を

実現するプロトタイプシステムの構築について述べる。ここで、提案する VPN の実現手法は、Linux オペレーティングシステムがインストールされた PC 上のアプリケーションプログラムとして実装されている。VPN 装置における TCP/IP 通信には、以下の 3 種類のソケットを利用している。

- UDP ソケット
- Raw ソケット
- Packet ソケット

なお、以下では、LAN L^i に接続されたコンピュータ C_s から LAN L^j に接続されたコンピュータ C_d へ IP データグラム群 G_D を配送する場合を例として説明する。

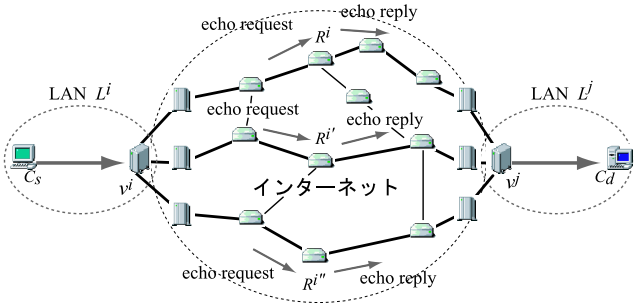

図 4: IP 拡散法を用いたセキュア VPN 環境

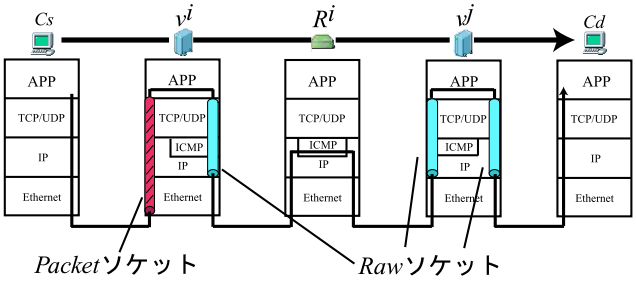

図 5: socket インタフェースを用いた実装

[C_s–v^i 間 (L^i 内) の配送]

1. G_d に含まれる IP データグラムは、送信元を C_s、送信先を C_d として、C_s から送信される。
2. L^i 内のルータは、1. で送信された IP データグラムを受信すると、ルーティングテーブルを参照し、v^i へと配送するように転送する。
3. v^i は、この IP データグラムを Packet ソケットを通して受信する。Packet ソケットを用いることによって、v^i を送信先としない IP データグラムの全体をアプリケーションで処理することが可能となる。□

[v^i–v^j 間 (インターネット内) の配送]

1. C_s から C_d へと配送される IP データグラム群を受信した VPN 装置 v^i は、3.2 節で述べた方法により N 個の中継ルータを決定する。
   1-1. v^i と v^j との間のホップ数の測定には、UDP を用いる。各 VPN 装置では、定められたポート番号でホップ数測定要求のための UDP メッセージを受信する。このとき、送信側では TTL の初期値をアプリケーションで設定し、受信側では TTL の現在値をアプリケーションで利用することから、Raw ソケットを用いる。なお、ホップ数測定応答のための UDP メッセージは、UDP ソケットを用いて送受信する。
   1-2. N 個の中継ルータを決定するための $mreq$ メッセージは、TTL の初期値をアプリケーションで設定するため、Raw ソケットを用いて送信する。一方、$mrep$ メッセージは、ICMP のヘッダを参照する必要があること、送信元の IP アドレスを取得する必要があることから、Raw ソケットを用いて受信する。
2. 1. で受信した IP データグラムを ICMP エコー要求メッセージにカプセル化して R^i へ送信する v_i は、IP データグラムの送信元を v^j とすることから、Raw ソケットを使用する。
3. 2. で送信された ICMP エコー要求メッセージに対応して、R^i が送信した ICMP エコー応答メッセージを受信する v^j は、これを Raw ソケットで受信する。v^j は、ICMP メッセージのデータ部に格納された IP データグラムを取り出す。□

[v^j–C_d 間 (L^j 内) の配送]

1. 受信した ICMP エコー応答メッセージのデータ部から IP データグラムを取り出した v^j は、この IP データグラムを Raw ソケットを用いて送信する。□

5 評価

前章までで説明した IP 通信拡散手法とそれを利用した VPN 装置では、経路の拡散に用いる中継点のルータにおいて、ICMP エコーの処理が必要になる。具体的には、受信した IP データグラムのデータ部に格納された ICMP エコー要求メッセージに対応する ICMP エコー応答メッセージが作成され、これをデータ部に格納した IP データグラムが送出される。このとき、ICMP エコー要求メッセージのデータ部にカプセル化された IP データグラムが ICMP エコー応答メッセージのデータ部にコピーされることで、中継点を経由した IP データグラムの配送およびこれを利用した LAN 間の VPN 通信を実現している。したがって、通常の IP データグラムを処理する場合と比較して、ICMP エコーの処理を必要とする分だけ、中継点のルータには負荷が増えることになる。そこで、図 4 のネットワーク構成において、通常の IP データグラムを配送する場合と IP 通信拡散法によって配送する場合とのスループットの違いを測定した。測定に用いたルータ装置は、以下の通りである。

- Cisco 2621: MPC860 50MHz, 32MB Memory, IOS 12.2(2)T
- Cisco 2651XM: MPC860P 80MHz, 96MB Memory, IOS 12.2(12a)
- Cisco 7206VR: MPE300 262MHz, 128MB Memory, IOS 12.0(7)T

• PC ルータ: Celeron 700MHz, 256MB Memory, LINUX(Kernel 2.4.17-14k)

netperf を用いて測定した結果を図 6、図 7、図 8、図 9 に示す。グラフには、それぞれの最高スループット値が記載されている。

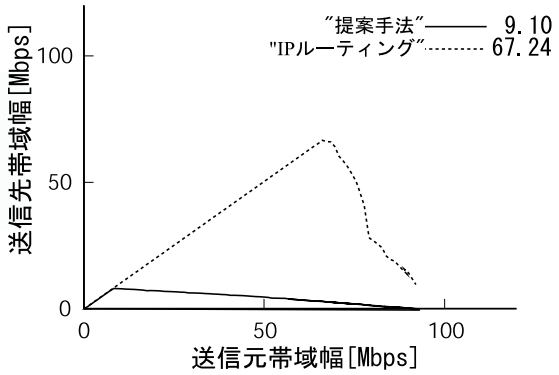

図 6: スループット測定結果 (Cisco 2621)

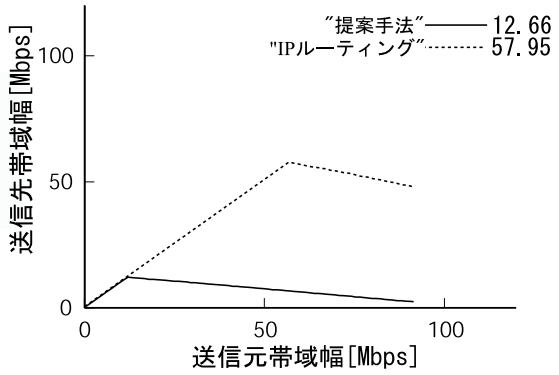

図 7: スループット測定結果 (Cisco 2651MX)

ICMP エコーカプセル化したパケットのスループットは、IP データグラムのスループットに比べて低くなっていることが測定結果から分かる。ただし、この差異は、ルータの CPU 性能、メモリ量の増加等により、必ずしも問題となる差異であるとはいえない。中継点に用いられるルータは、インターネットにある高性能なルータである場合が多く、組織 LAN を対象とした CPU 性能が低く、メモリも少量であるものとは異なる。以上の考察により、VPN としての適用環境においては、実用上は性能の問題はないと結論付けられる。

6 まとめと今後の課題

本論文では、暗号通信技術を補完し、盗聴者の使用するコンピュータの計算能力の向上に依存せずに、安全な通信路の提供に供する IP 通信拡散手法を提案した。ここでは、通信要求の発生に対して、動的に複数経路を探索する。提案手法は、インターネットのルータに特別な機能を導入する必要がない点で適用性に優れている。性能評価実験により、中継点となるルータには、通常の

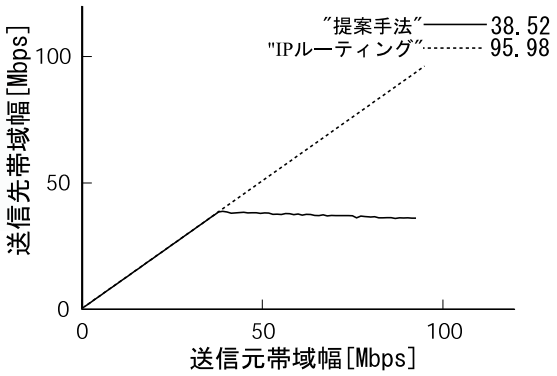

図 8: スループット測定結果 (Cisco 7206VR)

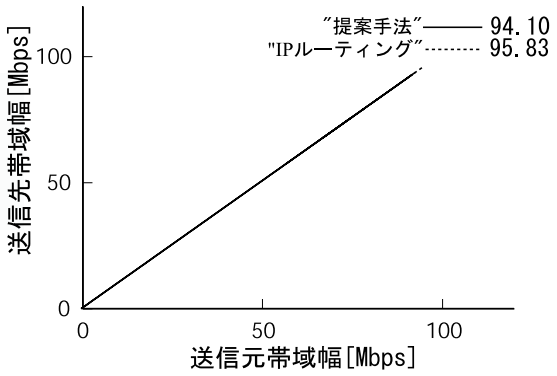

図 9: スループット測定結果 (PC ルータ)

IP データグラムに比べて大きなオーバヘッドを要すること、ただし、適切な CPU 性能、メモリ量を持つものでは、実用上問題がないことを明らかにした。本論文では、拡散度と重複度、伝達遅延との関係を定性的に述べた。実用システムの構築に向けて、インターネット環境における定量的関係を実験により求めることが今後の課題である。

参考文献

[1] David, B., David, A., Hu, Y.C., Jorjeta, G. and Jetcheva, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks," Internet Draft, draft-ietf-manet-dsr-04.txt (2000).

[2] Postel, J., "Internet Protocol," RFC791 (1981).

[3] Postel, J., "Internet Control Message Protocol," RFC792 (1981).

[4] Sagawa, Y., Asano, T. and Higaki, H., "Loop-Based Source Routing Protocol for Mobile Ad-hoc Networks," Proceedings of the International Conference on Communications and Computer Networks (2002).