

IP データグラム群の複数経路配送を用いた VPN 装置の実装と性能評価実験

埼玉県産業技術総合センター
森田 俊英
東京電機大学 理工学部 情報システム工学科
有泉 徹也 寺西 貴 横山 雄一 桧垣 博章

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 装置の実装について述べる。IP 通信拡散手法は、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て IP データグラム群を配送する手法である。本手法を VPN 装置として実装するためには、異なる LAN 間を配送される IP データグラムについては、暗号通信と拡散通信を組み合わせることが必要である。一方、LAN 内のコンピュータとインターネット上のコンピュータとの間を配送される IP データグラムについては、アドレス変換が必要とされる。これらの機能を Linux 上に実装した。また、IP 通信拡散手法の経路制御において中継点として使用されるルータの処理オーバーヘッドおよび拡散通信トラフィックによる中継ルータにおける他の IP 通信のスループットの低下を実験により評価した。

Performance Evaluation of Dynamic Multiple-Route IP Transmissions

Toshihide Morita
Saitama Industrial Technology Center

Tetsuya Ariizumi Takashi Teranishi Yuichi Yokoyama Hiroaki Higaki
Department of Computers and Systems Engineering
Tokyo Denki University

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 routes determined 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. In addition, performance degradation of another IP transmission through the intermediate router for processing of ICMP encapsulated packets is also evaluated. The result shows the proposed method is reasonably 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、企業や個人のインターネット利用環境が広く普及している。また、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ネットワークセキュリティ技術への要求が高まっている。TCP/IP インターネットにおけるセキュリティへの脅威には、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。

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する。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を同一 LAN 内の通信と同等に見せることができる。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。これは、IPsec [5, 14] などを利用した暗号通信を用いることで実現される。暗号通信は、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 [16]、IDEA [6] 等がある。また、後者には、RSA [11, 12]、Diffie-Hellman [1]、Merkle-Hellman [18] 等がある。暗号通信は、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によって、使用されている暗号通信技術は陳腐化することになる。

しかし、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、盗聴者がデータの全体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ることのみが必要であり、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。特に、VPN 装置に実装する場合、暗号通信を実現する IPsec、アドレス変換を実現する IP マスカレード (iptables) と共存する必要がある。本論文では、拡散通信と暗号通信 (VPN 装置間通信) の機能をアプリケーションプロセスとして実装し、OS カーネルに実装されたアドレス変換機能との複合実装方法について述べる。さらに、IP 通信拡散手法では、経路を拡散させるための中継点として使用するルータの処理オーバーヘッドが、通常の IP データグラム配送に比べて大きくなることが考えられる。そこで、このオーバーヘッドを評価し、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 提案手法

2.1 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 との間で、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 $G_D = \{IP_0, \dots, IP_{n-1}\}$ を、 N 個のサブグループ $SG_D^i \subset G_D (i = 0, \dots, N-1)$ (ただし、 $\cup_i SG_D^i = G_D$ かつ $\forall i \neq i', SG_D^i \cap SG_D^{i'} = \emptyset$) に分割する。また、 c_s は、 c_s から c_d への N 個の経路 $r_{(s,d)}^i = \langle c_0^i = c_s, c_1^i, \dots, c_{l(i)-1}^i, c_{l(i)}^i = c_d \rangle (i = 0, \dots, N-1)$ を決定する。そして、 SG_D^i に属する IP データグラムを $r_{(s,d)}^i$ を用いて配送する。これによって、 M が D を配送するための 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 $\forall i, 0 < \exists k(i) < l(i), c_{k(i)}^i$ もしくは通信路 $\forall i, 0 \leq \exists k(i) < l(i), \langle c_{k(i)}^i, c_{k(i)+1}^i \rangle$ において、 SG_D^i に属する IP データグラム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 $D = \text{encrypt}(D_{orig})$ が配送される場合には、 SG_D^i 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。

ここで、 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。

[要求条件]

- $r_{(s,d)}^i$ を M が事前に入手することが不可能 (困難) である。
- $r_{(s,d)}^i, r_{(s,d)}^{i'}$ に共通に含まれるルータが存在しない (少ない)。□

また、2 つの経路 $r_{(s,d)}^i, r_{(s,d)}^{i'} (0 \leq i < i' < N)$ に共通のルータ $\exists cc_{\{i,i'\}} \in r_{(s,d)}^i \cap r_{(s,d)}^{i'}$ (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、 $cc_{\{i,i'\}}$ あるいはこれに直接接続する共通の通信路に M_i を配置することによって D 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 $\exists cc \in \cap_i r_{(s,d)}^i$ (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。各 IP データグラムは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。

2.2 中継ルータ決定方法

IP データグラム群 $G_D = \{IP_0, \dots, IP_{n-1}\}$ 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 $r_{(s,d)}^i$ 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 [8]。これらにおいては、 c_s において経路 $r_{(s,d)}^i$ 、すなわち中継ルータの列 $\langle c_1^i, \dots, c_{l(i)-1}^i \rangle$ を決定しなければならない。このためには、 c_s がネットワークトポロジ情報を保持し、常に最新であるように維持管理するか、通信要求発生時に c_s から c_d に至る複数の経路を探索するかのいずれかの方法を用いることとなる。しかし、前者では、すべてのコンピュータにネットワークトポロジの変化の情報を通知するオーバーヘッドが不可避である。一方、後者では、通信開始時に経路探索のための遅延が避けられず、探索プロトコルの通信オーバーヘッドも必要となる。また、 $l(i) - 1$ の中継ルータのアドレスを IP ヘッダのオプション部や拡張ヘッダに含めることによるオーバーヘッドも考慮する必要がある。論文 [20] のように、ルータに専用プロトコルが導入されていることを前提とする手法によってこの問題を解決することが考えられる。しかし、IP 通信拡散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、 c_s は、 D を配送するために $G_D = \{IP_0, \dots, IP_{N-1}\}$ を SG_D^i ($i = 0, \dots, N-1$) 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 SG_D^i に属する IP データグラムを R_i を含む経路 $r_{\langle s,d \rangle}^i = \langle c_0^i = c_s, c_1^i, \dots, c_{r(i)}^i = R_i, \dots, c_{l(i)-1}^i, c_{l(i)}^i = c_d \rangle$ を用いて配送する。ここで、 c_s から R_i までの $r_{\langle s,d \rangle}^i$ の部分経路 $\langle c_0^i = c_s, c_1^i, \dots, c_{r(i)-1}^i, c_{r(i)}^i = R_i \rangle$ および R_i から c_d までの $r_{\langle s,d \rangle}^i$ の部分経路 $\langle c_{r(i)}^i = R_i, c_{r(i)+1}^i, \dots, c_{l(i)-1}^i, c_{l(i)}^i = c_d \rangle$ に含まれるルータ $c_1^i, \dots, c_{r(i)-1}^i$ および $c_{r(i)+1}^i, \dots, c_{l(i)-1}^i$ は、それぞれ R_i および c_d を送信先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. c_s は、 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メッセージ $hreq$ 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メッセージ $hrep$ 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 $vadd^i$ ($i = 0, \dots, N-1$) を得る。
4. c_s は、送信元を c_s 、送信先を $vadd^i$ 、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 $mreq$ 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を中継ルータ R^i とする。
 - 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 ($i = 0, \dots, N-1$) を得る。□

2.3 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 ($i = 0, \dots, N-1$) のそれぞれの中継ルータ

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。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。ソースルーティングを用いることにより1つの中継ルータを指定した配送の実現が可能である。ところが、配送経路を指定した IP データグラムは、DoS(Denial of Service) 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使用される [7]。そのため、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存在する。このようなルータが経路上に1つでも存在する場合には、この IP データグラムの配送に失敗する。ルータが持つ機能のうち、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 [9] 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、エコー要求メッセージ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^i 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。

[IP データグラム配送]

1. 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、この IP データグラムを R^i へと配送する。
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、 $ereq$ に含まれるデータ、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、この IP データグラムを c_d へと配送する。
8. c_d は、 $IP_{caps}(erep)$ を受信すると、そこから IP_{real} を取り出す。□

ICMP エコー要求も DoS 攻撃の手段として使用可能であり、受信後直ちに破棄するような設定が施されたルータが存在する。しかし、提案手法では、中継ルータ R_i にこのような設定がなされていないならば、配送は成功する。

3 VPN 装置の実装

3.1 拡散通信の実装

3章で述べた IP 通信拡散手法により、TCP/IP インターネットに接続された複数の LAN L^i ($i = 0, \dots, P-1$) 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) と契約する場合はこれにあたる。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 通信拡散手法を用い、 v^i と v^j との間に複数の経路を動的に決定し、それを用いて IP データグラム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。VPN 間の拡散通信機能は、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る。VPN 装置における TCP/IP 通信には、UDP ソケット、Raw ソケット、Packet ソケットを用いる。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。

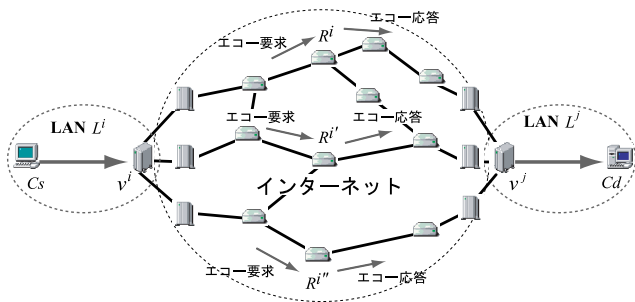


図 1: IP 通信拡散手法を用いた VPN 間通信

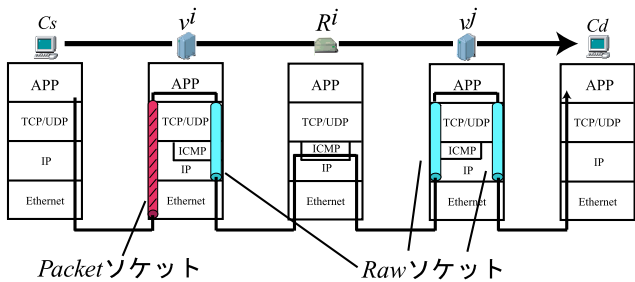


図 2: ソケットインタフェースを用いた実装

$[C_s-v^i$ 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、この IP データグラムを v^i へと配送する。
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。□

3.2 暗号通信/アドレス変換との共存

本論文で提案する IP 通信拡散手法は、暗号通信と対立、競合するものではなく、暗号通信の欠点のひとつを補完するものである。したがって、VPN 装置間の通信においては、拡散通信と暗号通信を組み合わせることが望ましい。VPN 装置間の暗号通信を実現するものとして、IPsec [5, 14] がある。IPsec には、公開鍵暗号を用いたデータ配送のための秘密鍵の配送機能 (IKE) と、この鍵を用いた秘密鍵通信によるデータ配送機能とが含まれている。データ配送には、3-DES が用いられている。IPsec の Linux への実装として FreeS/WAN プロジェクト [19] によるものがある。ここでは、IPsec の機能は、Linux カーネルモジュールとして実装されている。一方、拡散通信機能はアプリケーションプログラムとして実装されている。ここで、送信側の VPN 装置における処理を考えると、LAN に接続するインタフェースから受信した IP データグラムの IP ヘッダを拡散通信プログラムが読み取る必要があることから、拡散通信プログラムによる処理の前に IPsec による処理を行なうことはできない。また、拡散通信プログラムが作成した ICMP エコー要求の送信先は VPN 装置ではなく中継ルータであることから、拡散通信プログラムによる処理の後に IPsec による処理を行うこともできない。受信側の VPN 装置においても同様のことが成り立つことか

ら、暗号通信はカーネルの機能を流用するのではなく、拡散通信プログラムの一部として実現する必要があるといえる。VPNを利用するLANでは、プライベートアドレスが広く利用されている [10]。LANに接続されたクライアントコンピュータがインターネット上のサーバにアクセスし、WWWやFTPなどのサービスを利用する場合には、プライベートアドレスをグローバルアドレスに変換しなければならない。このアドレス変換は、LANとインターネットとを接続するルータで行われるのが一般的であり、VPNを使用する環境ではVPN装置において実現される。実現には、IPアドレス変換のみを行うNAT(Network Address Translator) [2]とIPアドレスとポート番号の変換を行うIPマスカレード [13]があり、Linuxではiptablesというカーネルモジュールとして実装されている。本実装では、iptablesを使用する。

以上をまとめると、VPNに属するLAN間の暗号通信/拡散通信はアプリケーションによって実現し、LANとインターネットとの間の通信は、カーネルの機能によって実現するしたがって、LANに接続するインタフェースから受信したIPデータグラムについては、その送信先がインターネット上のサーバコンピュータであるかVPNに含まれる他のLAN上のコンピュータであるかによって、その処理をカーネルで行うかアプリケーションで行うかが異なる。同様に、インターネットに接続するインタフェースから受信したIPデータグラムについても、その送信元がインターネット上のサーバコンピュータであるか、VPNに含まれる他のLAN上のコンピュータであるかによって、その処理をカーネルで行うかアプリケーションで行うかが異なる。4.1節で示したように、拡散通信プログラムはこれらのIPデータグラムをPacketソケットもしくはRawソケットで受信する。この場合、受信したIPデータグラムのコピーはアプリケーションによって受理、処理されるとともに、カーネルのTCP/IPモジュールでも受理、処理される。そこで、拡散通信プログラムとiptablesの処理のはじめに送信先あるいは送信元のアドレスを確認し、処理が不要であるモジュールではこのIPデータグラムの処理を中止することとする。

[LANから受信したパケットの処理]

LANから受信したIPデータグラムは、Rawソケットを通した受信によってコピーされる。このIPデータグラムがVPNに含まれるLANを送信先とする場合、アプリケーションプログラムによってICMPエコーカプセル化とデータ部の暗号化が行われ、送信される。OSカーネルでは、iptablesによってIPデータグラムが破棄される。受信したIPデータグラムがインターネット上のサーバを送信先とする場合、アプリケーションプログラムではIPデータグラムは破棄される。カーネルでは、iptablesによってIPマスカレードの処理が施されたIPデータグラムが送信される。

[インターネットから受信したパケットの処理]

インターネットから受信したIPデータグラムは、Rawソケットを通した受信によってコピーされる。このIPデータグラムがVPNに含まれるLANを送信元とする場合、アプリケーションプログラムによって暗号化されたデータ部の復号化が行われ、送信される。OSカーネルでは、iptablesによってIPデータグラムが破棄される。受信したIPデータグラムがインターネット上のサーバ

を送信元とする場合、アプリケーションプログラムではIPデータグラムは破棄される。カーネルでは、iptablesのアドレス変換テーブルに従ってIPマスカレードの処理が施されたIPデータグラムが送信される。

4 評価

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となる。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、中継ルータの負荷が増えることになる。そこで、図3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netperf [3]を用いて測定した結果を表1に示す。

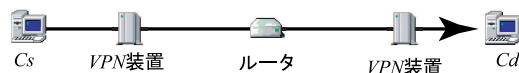


図3: 中継ルータのスループット測定環境

表1: netperfを用いた測定結果 (Mbps)

ルータ	提案手法	IP通信
PC(Celeron 700MHz)	94.10	95.83
HP ProCurve5304(PowerPC 200MHz)	8.09	95.76
Cisco 7296VR (MPE300 262MHz)	38.52	95.98
Cisco 2651MX (MPC860 80MHz)	12.66	57.95
Cisco 2621 (NPC860 50MHz)	9.10	67.24

表1の結果からICMPエコーカプセル化されたパケットのスループットがIPデータグラムのスループットよりも低くなっていることが分かる。しかし、その差異はルータの性能そのものとは直接的な関係がない。ICMPエコーの処理は上で述べたようなデータのコピーがともなう処理である一方、通常のIPデータグラムの処理は、このようなコピーをできるだけ行わないようなチューニングが設けられている。そのため、コピーをともなうICMPエコーの処理に対してプロセッシング能力のどれだけの割り当てかは、ルータの実装法と設定によるものであると考えられる。次に、HP ProCurve5304とCisco7296VRを用いて、ICMPエコーカプセル化されたパケットの処理による他のIPデータグラムのスループットの低下を測定した。図4に実験環境の概略を示す。ルータを中継点としたICMPエコーカプセル化パケットのスループットを変化させた場合のIPパケットの最大スループットの変化を図5、図6に示す。

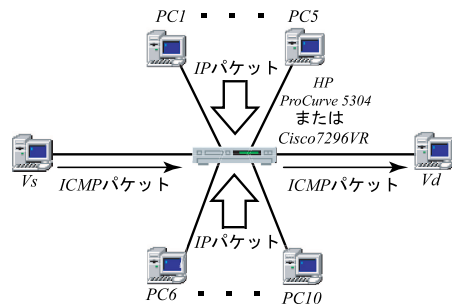


図 4: 測定環境

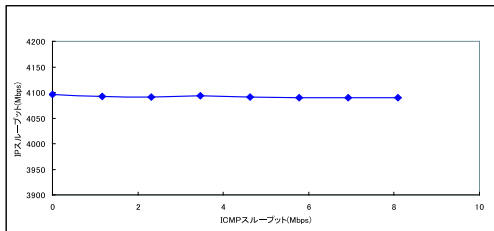


図 5: IP のスループット (HP ProCurve5304)

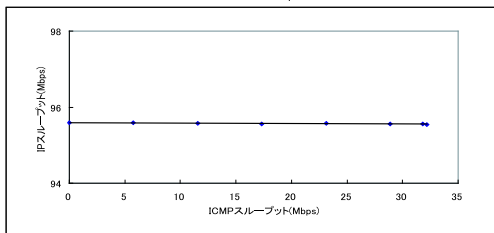


図 6: IP のスループット (Cisco 7296VR)

HP Procurve5304 と Cisco7296VR のいずれにおいても ICMP のスループットを変化させても、このルータを同時に通過する IP データグラムのスループットはほとんど変化しないことが分かる。これによって以下のような考察を行なうことができる。(1) 現在のルータの設定、実装においては、ICMP エコーパケットに対するプロセッシング能力の割り当ては制限されたものになっており、この制限の範囲内では ICMP エコーカプセル化パケットの処理によって中継ルータの他の IP データグラムに対する処理能力がほとんど低下することがない。(2) 表 1 の PC での測定結果から、IP データグラムの処理と ICMP エコーカプセル化パケットの処理とに要するプロセッシング能力との間には大きなものではない。種々の手法による最適化がなされていることを考慮しても、現在の ICMP エコー処理に対するプロセッシング能力の割り当て制限は過度に厳しいものであると考えられる。

5 まとめと今後の課題

本論文では、暗号通信を補完し、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、安全な通信路を提供する 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、決定

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。また、本手法の VPN 装置への実装方法について述べた。性能評価実験により、中継ルータには、通常の IP データグラムに比べて大きなオーバーヘッドを要すること、ただし、他の IP データグラムの配送スループットには大きな影響を与えないことを明らかにした。VPN 装置そのものにおける処理オーバーヘッドを測定すること、拡散度と安全性、伝達遅延との関係について実験的に明らかにすることが今後の課題である。

参考文献

- [1] Diffie, W. and Hellman, M.E., "New Directions in Cryptography," Proceedings of AFIPS National Computer Conference, pp. 109-112 (1976).
- [2] Egevang, K. and Francis, P., "The IP Network Address Translator (NAT)," RFC1631 (1994).
- [3] Jones, R., "Netperf Homepage," <http://www.netperf.org/netperf/NetperfPage.html>
- [4] Karn, P., "The ESP Triple DES Transform," RFC1851 (1995).
- [5] Kent, S. and Atkinson, R., "Security Architecture for the Internet Protocol," RFC2401 (1998).
- [6] Lai, X., "On the Design and Security of Block Ciphers," ETH Series in Information Processing (1992).
- [7] Perkins, C., "IP Encapsulation within IP," RFC2003 (1996).
- [8] Postel, J., "Internet Protocol," RFC791 (1981).
- [9] Postel, J., "Internet Control Message Protocol," RFC792 (1981).
- [10] Rekhter, Y., Moskowitz, B., Karrenberg, D., Groot, G.J. and Lear, E., "Address Allocation for Private Internets," RFC1918 (1996).
- [11] Rivest, R.L., Shamir, A. and Adleman, L.M., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, vol. 21, no. 2, pp. 120-126 (1978).
- [12] Rivest, R.L., Shamir, A. and Adleman, L.M., "On Digital Signatures and Public Key Cryptosystems," MIT Laboratory for Computer Science, Technical Report, MIT/LCS/TR212 (1979).
- [13] Srisuresh, P. and Holdrege, M., "IP Network Address Translator (NAT) Terminology and Considerations," RFC2663 (1999).
- [14] Thayer, R., Doraswamy, N. and Glenn, R., "IP Security Document Roadmap," RFC2411 (1998).
- [15] Wiener, M.J., "Efficient DES Key Search," TR-244, School of Computer Science, Carleton University (1994).
- [16] ANSI X3.92, "American National Standard for Data Encryption Algorithm (DEA)," American National Standards Institute (1981).
- [17] ANSI X9.17 (Revised), "American National Standard for Financial Institution Key Management (Wholesale)," American Bankers Association (1985).
- [18] "Merkle-Hellman," <http://www.wikipedia.org/wiki/Merkle-Hellman>.
- [19] "FreeS/WAN Project," <http://www.freeswan.org>.
- [20] 越智, 北形, 菅沼, 木下, 白鳥, "動的最適化多重経路通信機構による適応型ルーティングの提案," インターネットコンファレンス 2000 論文集, pp. 85-94 (2000).