

盗聴に頑強な通信路のための IP 通信拡散手法

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
E-mail: {sai, tadato, shinji, miya, hig}@higlab.k.dendai.ac.jp

TCP/IP インターネットに接続された 2 つのコンピュータ間に盗聴に対して頑強な通信路を実現するために、暗号化通信が利用されている。この方式は、暗号文を復号して平文を得るための計算量が、盗聴のために利用されるコンピュータの計算能力に対して十分大きいことを安全性の根拠としている。そのため、コンピュータの計算能力の向上とともに既存の暗号方式は陳腐化し、新しい暗号方式を導入する必要がある。本論文では、IP パケット群のすべてを盗聴者が入手することを困難にすることによって、コンピュータの性能向上とは無関係に安全性を提供できることに注目し、IP パケット群を動的に決定される複数の経路に分割して配送する IP 通信拡散手法を提案する。本方式は、インターネット上のルータに新たな機能を導入する必要がある点で実用性に優れている。また、これを用いた VPN 装置のプロトタイプ実装について報告する。

Dynamic Multi-Path IP Transmission for Secure Communication

Takanori Saitou, Tadato Horiike, Shinji Osada, Masamitsu Miyazaki and Hiroaki Higaki
Department of Computers and Systems Engineering
Tokyo Denki University
E-mail: {sai, tadato, shinji, miya, hig}@higlab.k.dendai.ac.jp

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 snoopers 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, design of VPN (virtual private network) based on the proposed methodology is discussed.

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、これにともなう 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、第三者に情報が漏洩することなく、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) [4] 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こ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ある点で適用性に優れている。最後に、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も論じる。

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 [14]、IDEA [2] 等がある。また、後者には、RSA [6]、Diffie-Hellman [13]、Merkle-Hellman [15] 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。

複数の経路を用いて 2 つのコンピュータの間の通信を行なう技術は、主に以下の目的で研究開発されている。

1 つ目は、高速広帯域通信の実現である。複数の通信路を「束ねる」ことによって、より大量のデータを短時間に配送する。これは、バックボーンネットワークにおけるルータ間の通信路のように固定の相手との間に広帯域な通信路を設けるものと、LAN に接続されたコンピュータ間の通信のように、通信相手が可変であり、これらとの間に広帯域な通信を提供するものがある。例えば、IEEE802.3ad では、イーサネットを対象としてリンクアグリゲーションを実現する技術である。これは、2 台のスイッチの間に張られた複数のリンクを統合し、1 本の論理的なリンクと同様に取り扱うものである。一方、LAN 内で動的に決定される通信相手との間に複数のリンクを張る手法に、[9,10] がある。ここでは、ARP (Address Resolution Protocol) を拡張することで、ひとつの IP アドレスを複数の MAC アドレスへと対応付けること可能としている。

2 つ目は、耐故障性の実現である。ある通信経路が切断されたとしても、あらかじめ探索しておいた別の経路

を用いて通信を継続することが可能である [11,12]。

3 つ目が、本論文で実現する安全性の実現である。複数の経路を用意して IP データグラムを分割配送することによって安全性を提供する方法は、既に提案されている。しかし、経路はあらかじめ設定されたものを用いることから、盗聴者の継続的な監視により、安全性が低下することが考えられる。これに対して、本論文で提案する手法は、通信要求が発生することに新しい経路を設定し直すことによって、盗聴者がネットワークを配送される IP データグラムを監視する位置を決定することを困難にしている。

動的に複数経路を決定する手法には、[8-10] などがある。[9,10] は、LAN 内の通信に適用を限定している。[8] は、インターネットを適用対象としているが、インターネット内にある一定数以上のルータに、提案手法を実現する機能が導入されていることが前提となっている。これに対して、本論文で提案する手法は、送信元コンピュータと送信先コンピュータに提案機能が実装されれば、中継ルータには特別な機能を必要としないため、適用性に優れている。

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 $\forall SG_D^i \subset G_D$ ($i = 0, \dots, N-1$) (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、 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 $r_{(s,d)}^i = \langle c_0^i = c_s, c_1^i, \dots, c_{l(i)-1}^i, c_{l(i)}^i = c_d \rangle$ ($i = 0, \dots, N-1$) を探索する。そして、サブグループ SG_D^i に属する IP データグラムを経路 $r_{(s,d)}^i$ 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 $\forall i, 0 < \exists k(i) < l(i), c_{k(i)}^i$ 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 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 $D = \text{encrypt}(D_{orig})$ が配送される場合には、サブグループ 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、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 $r_{(s,d)}^i$ を M が事前に入手することが不可能 (困難) である。
- 経路 $r_{(s,d)}^i$ 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 $r_{(s,d)}^i$ ($i = 0, \dots, N-1$) を

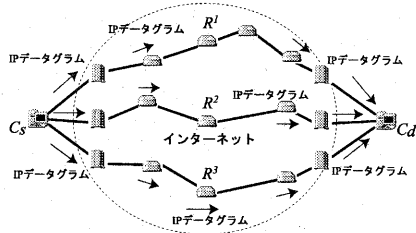


図 1: IP 通信拡散における中継ルータ

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 $c_{m(i)}^i \in r_{(s,d)}^i$ あるいは通信路 $\langle c_{m(i)}^i, c_{m(i)+1}^i \rangle$ (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こ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 $r_{(s,d)}^i, r_{(s,d)}^{i'}$ ($0 \leq i < i' < N$) 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、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 $\exists cc \in \cap_i r_{(s,d)}^i$ (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 $l(i)$ が大きくなるの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 $G_D = \{IP_0, \dots, IP_{n-1}\}$ 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。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, 7]。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の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 $G_D = \{IP_0, \dots, IP_{n-1}\}$ を、 N 個のサブグループ 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、各サブグループ SG_D^i に属する IP データグラムを中継ルータ R_i を含む経路 $r_{(s,d)}^i = \langle c_0^i = c_s, c_1^i, \dots, c_{r(i)}^i = R_i, \dots, c_{l(i)-1}^i, c_{l(i)}^i = c_d \rangle$ を用いて配送する。ここで、送信元コンピュータ c_s から中継ルータ R_i までの $r_{(s,d)}^i$ 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 $\langle c_{r(i)}^i = R_i, c_{r(i)+1}^i, \dots, c_{l(i)-1}^i, c_{l(i)}^i = c_d \rangle$ 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 R_i の決定においては、以下の要求条件を満たすことが求められる。

[要求条件]

1. 盗聴者 M がルータ R_i ($i = 0, \dots, N-1$) の位置を推測することが十分に困難となるように、その決定手順にランダムネスが含まれていること。
2. 盗聴者 M がデータ D の全体を推測するだけの十分な数の IP データグラムを入手することが困難となるように、各経路 $r_{(s,d)}^i$ と他の経路 $r_{(s,d)}^{i'} (i \neq i')$ との間に共通に含まれるルータ $cc_{\{i,i'\}} \in r_{(s,d)}^i \cap r_{(s,d)}^{i'}$ の数が十分に少なくなること。すなわち、経路 $r_{(s,d)}^i$ の長さ (ホップ数) $l(i)$ がこの条件を満足する程度に十分大きいこと。
3. 前項の要求を満たすために迂回している経路長 (ホップ数) $l(i)$ の経路 $r_{(s,d)}^i$ を用いて IP データグラム

を配送する際の伝達遅延時間が、アプリケーションプログラムの要求を充足しない程には大きくならないこと。すなわち、経路 $r_{(s,d)}^i$ の長さ $l(i)$ がこの条件を満足する程度に十分小さいこと。□

上記の 2. と 3. とは、互いに相反する要求条件となっていることから、経路の重複度と伝達遅延とは互いにトレードオフの関係にある。この関係は、あらかじめ測定実験によって求めておく必要があるが、その概略は図 2 に示すようになる。そこで、データ D の盗聴の困難さと伝達遅延の大きさがアプリケーションの要求を満足するように、拡散度を定める必要がある。これは、図 2 に示される区間 $[\min l_{\text{toff}}, \max l_{\text{toff}}]$ に含まれる拡散度 l_{toff} の経路を探索することによって実現される。実際には、 c_s と c_d への定められた長さの経路を検出することは困難である。そこで以下では、 c_s から中継ルータ R^i までの経路長をもって拡散度とする。要求条件 1. をも満足するために、仮想目標コンピュータのアドレス $vaddr^i$ をランダムに決定し、 c_s から仮想目標コンピュータに向かって拡散度だけ離れたルータを中継ルータと定める。これは、 R^i のアドレスを獲得するために c_s から送信される IP データグラムの TTL の初期値を拡散度と等しくすることによって、 R^i から ICMP 時間切れメッセージが c_s に返送されることを利用する。この ICMP メッセージを配送するための IP データグラムのヘッダから、 c_s が R^i の IP アドレスを得ることが可能である。 c_s から仮想目標コンピュータまでのホップ数が拡散度よりも小さい場合や、仮想目標コンピュータに対するルーティングが不可能な場合に対処するために、IP の上位プロトコルには、未定義のプロトコルを指定する。

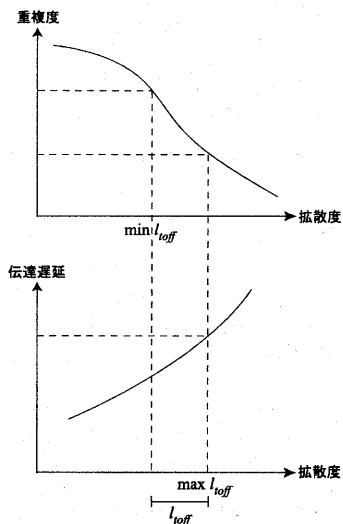


図 2: 拡散度と重複度

[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 $hop_{(s,d)}$ を以下の手順を用いて決定する。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 $hop_{(s,d)} = T_{init} - T_{obsv}$ 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 $hop_{(s,d)}$ に対して、最適な拡散ホップ数 $hop_{(s,m)} = dhop(hop_{(s,d)})$ 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 $vaddr^i$ ($i = 0, \dots, N-1$) を得る。
4. c_s は、送信元を c_s 、送信先アドレスを $vaddr^i$ 、TTL を $hop_{(s,m)}$ 、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、 $vaddr^i$ を再生成し、4. へ戻る。
6. c_s は、自身から $hop_{(s,m)}$ 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。□

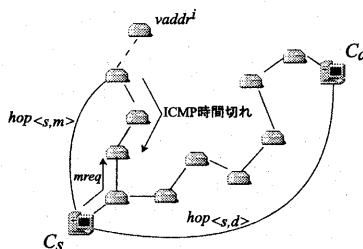


図 3: 中継ルータの決定

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 ($i = 0, \dots, N-1$) 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元コンピュータまで 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み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ではなく、ただちに破棄するように設定されている。

一方、IP トンネリング [3] とは、IP データグラムのデータ部に別の IP データグラムを格納する方法である。すなわち、送信元を c_s 、送信先を c_d とする IP データグラム IP_{real} をデータ部とし、送信先を c_s 、送信元を R 、上位プロトコルを IP とした IP データグラム IP_{caps} を c_s が送信する。 IP_{caps} は、各ルータがルーティングテーブルを参照して転送し、中継ルータ R に配送される。 R は IP_{caps} の送信先であるから、データ部を上位プロトコルに渡す。ここでは、データ部は IP_{real} であり、上位プロトコルは IP であることから、 R は IP_{real} を転送する。 IP_{real} は、各ルータがルーティングテーブルを参照して転送することによって、最終的に c_d に到着する。こうして、 IP_{real} は c_s から R を経由して、 c_d に配送されることになる。しかし、IP データグラムのデータ部に別の IP データグラムが含まれているときに、このデータ部に含まれる IP データグラムをルータが転送するためには、トンネリングをサポートする機能が R に含まれていることが必要である。この機能は、現在利用されている多くのルータがサポートしているが、実際にこの機能が利用できるように設定されているルータは必ずしも多くはない。これは、IP トンネリングは、互いに合意の取れているコンピュータでカプセル化、非カプセル化の操作を行なうものであり、不特定多数のコンピュータから送信されたカプセル化 IP データグラムを受信して、データ部に含まれる IP データグラムを受信や転送するように設計されていないことによるものである。

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 [5] 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 IP データグラムを配送することを實現する。

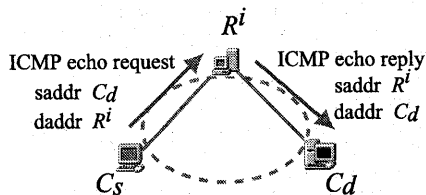


図 4: ICMP echo 処理を用いた経路制御

[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 ($i = 0, \dots, N-1$) 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 を實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實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 の實現手法は、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。

[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

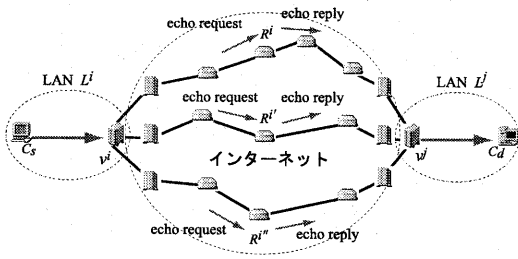


図 5: IP 拡散法を用いたセキュア VPN 環境

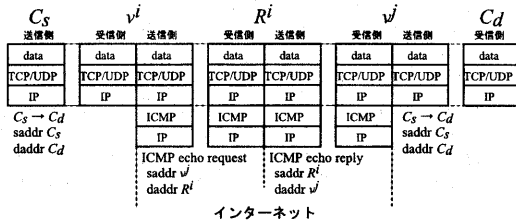


図 6: セキュア VPN 環境でのヘッダ処理

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 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ある点で適用性に優れている。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] Lai, X. and Massey, J.L., "A Proposal for a New Block Encryption Standard," Proceedings of EURO-CRYPT'90, pp. 389-404 (1991).
- [3] Perkins, C., "IP Encapsulation within IP," RFC2003 (1996).
- [4] Postel, J., "Internet Protocol," RFC791 (1981).
- [5] Postel, J., "Internet Control Message Protocol," RFC792 (1981).
- [6] Richard, A., "RSA and Public-Key Cryptography," CRC Press (2002).
- [7] 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).
- [8] 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).
- [9] 出口, 桧垣, "複数 NIC とスイッチングハブを用いた広帯域通信機構の構築と評価," 情報処理学会第 62 回全国大会論文集, No. 1, pp. 25-26 (2001).
- [10] 林, 梅島, 桧垣, "複数 NIC とスイッチングハブを用いた広帯域通信の LINUX への実装," 情報処理学会第 64 回全国大会論文集, No. 3, pp. 505-506 (2002).
- [11] 林, 山崎, 森田, 相田, 武市, 土居, "インターネットを用いた複数経路データ伝送方式の性能評価," 電子情報通信学会論文誌, Vol. J84-B, No. 3, pp. 523-533 (2001).
- [12] 渡辺, グランディダー・ロットウィブンチャイ, "インターネットにおける複数経路データ転送手法," 情報処理学会第 63 回全国大会論文集, No. 3, pp. 427-428 (2001).
- [13] "Diffie-Hellman," <http://www.hack.gr/users/dij/crypto/overview/diffie.html>.
- [14] "FIPS PUB 46-2," <http://www.itl.nist.gov/fipspubs/fip46-2.htm>.
- [15] "Merkle-Hellman," <http://www.wikipedia.org/wiki/Merkle-Hellman>.