暗号通信を用いた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
寺西 貴　有泉 徹也　横山 雄一　桧垣 博章

前橋工科大学 工学部 情報工学科
遠山 宏明

TCP/IP インターネットに接続された 2 台のコンピュータの間に、盗聴に対して頑強な通信路を実現する手法として、暗号化通信が利用されている。この手法は、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生じる。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。本手法は、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ない点で適用性に優れている。また、本手法を暗号化と組み合わせる手法について述べる。暗号化された複数の IP データグラムを分割し、組み替えて得られたデータをカプセル化したものを異なる経路を用いて配送することによって、盗聴をより困難にしている。この手続きに要する同期オーバーヘッドをプロトタイプシステムで測定した結果、IPsec に要するオーバーヘッドとほぼ同じであり、十分実用的であると結論づけることができる。

Dynamic Multiple-Route IP Transmission with Data Encription

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

Hiroaki Toyama
Department of Information Engineering
Maebashi Institute of Technology

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 into routers, it is highly applicable. In addition, this paper proposes a method to combine dynamic multi-route transmission and block encription. Here, multiple IP datagrams are encripthed and devided into multiple blocks. Then a reconstructed datagram is formed by concatinating the blocks each of which is selected from a distinct encripted IP datagram.

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。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) [9] 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 [6,15] 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 [5, 7, 16, 17] 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。コンピュータの計算能力の向上は著しく、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ことは可能となり得る。通信の安全性を保つためには、新しい暗号アルゴリズムを導入しなければならない。例えば、DES [17] は現在では十分に安全な暗号アルゴリズムであると言うことはできず [16]、3-DES [5] やIDEA [7] といった新しいアルゴリズムへの移行が必要となっている。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IP 通信拡散手法を提案し、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。このIP 通信拡散手法は、暗号アルゴリズムの適用と競合、対立するものではなく、相互に補完するものであるといえる。そこで、本論文では、これら2 つの技術を組み合わせることによって、盗聴に対してより頑強な通信路を実現する手法を提案する。また、Linux コンピュータへ実装したプロトタイプシステムの性能評価について報告する。

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 [6,15] 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 [17]、IDEA [7] 等がある。また、後者には、RSA [12,13]、Diffie-Hellman [2]、Merkle-Hellman [19] 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。本論文で提案するIP 通信拡散手法は、この暗号通信の安全性を、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、あるデータを配送するIP データグラム群を複数の経路を用いて配送することによって、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 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 $G_D = \{IP_0, \ldots, IP_{n-1}\}$ を、N 個のサブグループ $SG^i_D \subset G_D (i = 0, \ldots, N-1)$ (ただし、$\cup_i SG^i_D = G_D$ かつ $\forall i \neq \forall i', SG^i_D \cap SG^{i'}_D = \emptyset$) に分割する。また、$c_s$ は、c_s から c_d への N 個の経路 $r^i_{\langle s,d \rangle} = \langle c^i_0 = c_s, c^i_1, \ldots, c^i_{l(i)-1}, c^i_{l(i)} = c_d \rangle$ $(i = 0, \ldots, N-1)$ を決定する。そして、SG^i_D に属するIP データグラムを $r^i_{\langle s,d \rangle}$ 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 $\forall i, 0 < \exists k(i) < l(i), c^i_{k(i)}$ 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 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 $D = encrypt(D_{orig})$ が配送される場合には、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が可能である。

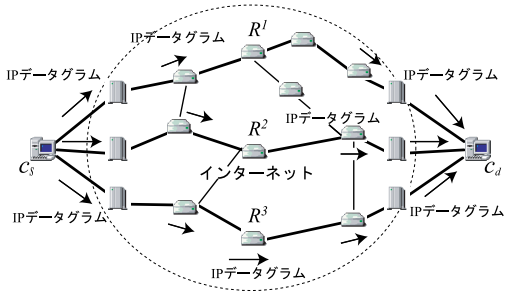

図 1: IP 通信拡散における中継ルータ

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]

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

事前に M が $r^i_{\langle s,d \rangle}$ $(i = 0, \ldots, N-1)$ 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、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、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、$cc_{\{i,i'\}}$ 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 $\exists cc \in \cap_i r^i_{\langle s,d \rangle}$ (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。

3.1 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 [9]。これは、オプション機能として定義されており、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、c_d へと配送する。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) 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 9 個 (ソースルーティングオプションの固定フィールドに 3 バイトを要し、IP アドレスは 4 バイト長である) しか格納することができない。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 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 $G_D = \{IP_0, \ldots, IP_{n-1}\}$ を 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 SG^i_D に属する IP データグラムを 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、c_s から 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 R_i から c_d までの $r^i_{\langle s,d \rangle}$ の部分経路 $\langle c^i_{r(i)} = R_i, c^i_{r(i)+1}, \ldots, c^i_{l(i)-1}, c^i_{l(i)} = c_d \rangle$ 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 $vadd^i$ $(i = 0, \ldots, N-1)$ 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 $(i = 0, \ldots, N-1)$ を得る。□

3.2 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^i_D $(i = 0, \ldots, N-1)$ 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。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。経路上のすべてのルータを指定するストリクトソースルーティングは、3.1 節で述べたように、IP ヘッダの最大サイズの制約のために使用することは難しい。しかし、中継ルータを 1 つだけ指定する方法であれば、ルースソースルーティングを用いることにより実現が可能である。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利用される [8]。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 [10] 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。

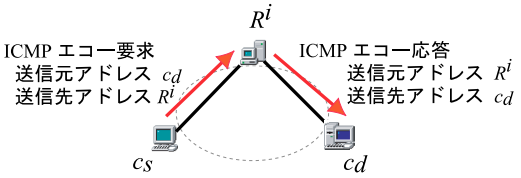

図 2: ICMP エコーを用いた経路制御

[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。□

4 暗号化 IP 通信拡散手法

論文 [21] においては、IP データグラム群に含まれる各データグラムを暗号化し、それらを複数の経路に分割して配送する手法が提案されている。すなわち、送信元コンピュータ c_s において、データ D を配送するための IP データグラム群 $G_D = \{IP_0, \ldots, IP_{n-1}\}$ に含まれる各データグラム IP_i をブロック暗号化することで $EG_D = \{encript(IP_0), \ldots, encript(IP_{n-1})\}$ を得て、

これを N 個のサブグループ $ESG_D^i(i = 0, \ldots, N-1)$ に分割する。中継ルータ R^i の異なる N 個の経路 $r^i_{\langle s,d\rangle}(i = 1, \ldots, N)$ を定め、各 ESG_D^i に属する暗号化 IP データグラムを $r^i_{\langle s,d\rangle}$ を用いて配送する。暗号化に IPsec を用いた Linux アプリケーションとしての実装方法が論文 [21] で論じられている。本手法は、IP データグラム IP_i が生成されると直ちに暗号化、IP 通信拡散手法のためのカプセル化、送信の手続きを行うことができる。そのため、これらの手続きにともなうスループットの低下を最小限におさえることができる。しかし、各 IP データグラムが独立に暗号化されているため、十分に高い計算能力を有するコンピュータを所有する盗聴者が暗号化された IP データグラム群 EG_D の一部を入手し、復号化することで D の一部を入手することが可能である。

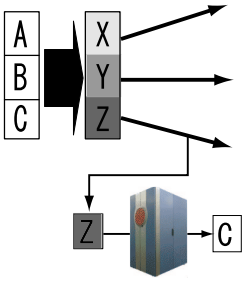

図 3: IPsec による IP 通信拡散手法

例えば図 3 において、送信元コンピュータ c_s が 3 つの IP データグラム A, B, C を送信する場合、これらを暗号化して得られた IP データグラム $X = encript(A),\ Y = encript(B),\ Z = encript(C)$ を各々に与えられた経路を用いて配送する。これらの配送経路すべてを盗聴者が観測し、X, Y, Z を得ることは困難であるが、その一部の経路を検出し、例えば Z を入手する可能性はある。この場合、十分高い計算能力を持つコンピュータを使用することによって盗聴者が $C = decript(Z)$ を入手することが考えられる。

そこで本論文では、図 4 に示す手法を提案する。

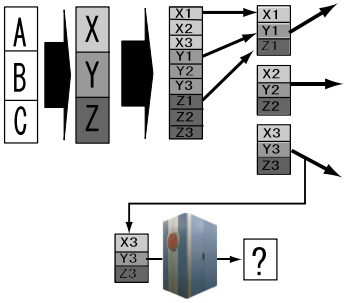

図 4: 暗号化 IP 通信拡散手法

図 4 では、送信元コンピュータ c_s は、IP データグラム A, B, C それぞれの送信要求が発生しても、直ちに暗号化、IP 通信拡散手法のためのカプセル化、送信という手続きを開始しない。まず、3 つの IP データグラム A, B, C の送信要求が発生するまで、各 IP データグラムをバッファに保存する。その後、各 IP データグラムを暗号化することによって、$X = encript(A),\ Y = encript(B),\ Z = encript(C)$ を得る。ここで、X, Y, Z をそれぞれ一定の大きさのブロックへと分割する。図 4 では、$X = (X1, X2, X3)$, $Y = (Y1, Y2, Y3)$, $Z = (Z1, Z2, Z3)$ と分割している。この分割ブロックを組み合わせた新しいデータ $(X1, Y1, Z1)$, $(X2, Y2, Z2)$, $(X3, Y3, Z3)$ をそれぞれカプセル化し、送信する。この場合、もし盗聴者が $(X3, Y3, Z3)$ というデータを得たとしても、それを用いて IP データグラム A, B, C の一部を得ることは困難である。ブロック暗号化と IP 通信拡散手法を組み合わせる本提案手法により、盗聴者がデータの全体を入手することを困難にするのみならず、その一部を解読することも困難になる。ただし、論文 [21] の手法と比較すると、複数の IP データグラムを受信してはじめて暗号化、分割ブロックの作成と組み替え、送信の手続きを開始することができるため、同期オーバーヘッドを要するところが欠点となる。図 4 では 3 個の IP データグラムによる実現例を示したが、一般に k 個の IP データグラムを対象として、各 IP データグラムをブロック暗号化したものを k 分割し、それぞれを組み合わせることによって k 個の新しいデータを作成した後、カプセル化し、送信する。このとき、k を大きくするとより安全性が高くなるが、k 個の IP データグラムの送信要求が発生するまで送信が遅延されることになる。つまり、安全性と同期による遅延がトレードオフの関係にある。同期オーバーヘッドによる影響を削減するために、前回の分割暗号化 IP データグラムの送信以降の最初の IP データグラム送信要求発生時にタイマを設定する。このタイマが時間切れとなる前に k 個の IP データグラム送信要求が発生したならば、タイマをリセットし、ブロック暗号化、分割ブロックの組み換え、カプセル化、送信の処理を行う。逆に、タイマが時間切れとなるまでに $k'(< k)$ 個の IP データグラム送信要求しか発生しない場合には、k' 個の IP データグラムを暗号化し、それぞれを k' 個のブロックへと分割して組み替え、カプセル化の後に送信することとする。

5 評価

前章で提案した暗号化 IP 通信拡散手法の性能評価について述べる。前章でも考察したように、論文 [21] で述べられている暗号通信の IP 通信拡散手法への導入法と比較して、バッファリングによる同期オーバーヘッドが大きい点が本論文の提案手法の欠点である。送信元コンピュータにおいては、閾値 k 個以上の IP データグラム送信要求が発生するか、タイムアウトするかのいずれかまでに発生した送信要求は IP データグラムをバッファに格納して待機する。一方、送信先コンピュータにおいては、ある IP データグラムを復号化するためには、その暗号化分割ブロックを含むすべてのカプセル化 IP

データグラムを受信することが必要であり、その受信が完了するまではカプセル化された IP データグラムをバッファに格納して待機する。これらのバッファリングによって、送信元コンピュータと送信先コンピュータとの間のスループットが低下することが考えられる。このスループットの低下に影響を与える主たるパラメータとして、送信元コンピュータについては、(1) 送信要求発生頻度、(2) 分割ブロック数 k、(3) タイムアウト値の 3 つがあり、送信先コンピュータについては、(1) 分割ブロック数 k、(2) 経路拡散度の 2 つがある。本論文では、論文 [21] で述べられている IP 通信拡散手法の実装に対して前章で述べた暗号ブロック化の機能を付加したプロトタイプ装置を作成し、図 5 のような VPN 装置構成において IPsec のみを提供する環境とスループットを比較することによって評価を行った。VPN 装置には、Pentium 4 1.7GHz、メモリ容量 256Mbyte、Linux カーネルバージョン 2.4 の PC に 3Com 3C905-J-TX を装着したものを用いた。

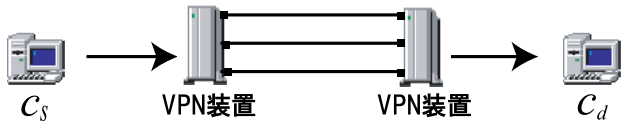

図 5: VPN 装置構成図

ただし、VPN 装置間にはルータ装置を設置せず、各 VPN 装置に装着した 3 個の NIC をそれぞれ UTP ケーブルで直結した。なお、すべての NIC は 100BaseTX である。表 1 に netperf [4] を用いた測定の結果を示す。

表 1 : netperf を用いた測定結果

	スループット
IP ルーティング	88.04(Mbps)
IPsec	27.90(Mbps)
提案手法	24.14(Mbps)

提案手法では、24.14Mbps のスループットが得られた。これは通常の IP データグラムのルーティングに対して 27%の性能となっている。一方、IPsec(FreeS/WAN) を用いた測定では、スループットが 27.90Mbps となっている。この結果から、提案手法におけるバッファリングに起因する同期オーバーヘッドによるスループットの低下は、約 13.5%にとどまっていることが分かる。参考までに、VPN ルータ製品である YAMAHA RTX1000 を用いた場合のスループットは 23.00Mbps となっている [1] ことから、実用的な性能を得ることができているといえる。

6 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 通信拡散手法とブロック暗号との組合せによって盗聴に対してより頑強な通信路を実現する方法を提案した。ブロック暗号化した複数の IP データグラムを分割し、それらを組み替えたものをカプセル化することにより、盗聴者が平文を入手することをより困難にしている。本提案手法によって必要となるバッファリングの影響をスループットの測定によって評価した結果、IPsec を用いた場合との比較で約 13.5%のスループット低下にとどまっていることが分かった。今後は、様々なパラメータ設定における性能比較と安全性向上の評価お行うことが課題である。

参考文献

[1] http://www.yamaha.co.jp/news/2003/03012201.html.

[2] Diffie, W. and Hellman, M.E., “New Directions in Cryptography,” Proceedings of AFIPS National Computer Conference, pp. 109–112 (1976).

[3] Egevang, K. and Francis, P., “The IP Network Address Translator (NAT),” RFC1631 (1994).

[4] Jones,R., “Netperf Homepage,” http://www.netperf.org/netperf/NetperfPage.html

[5] Karn, P., “The ESP Triple DES Transform,” RFC1851 (1995).

[6] Kent, S. and Atkinson, R., “Security Architecture for the Internet Protocol,” RFC2401 (1998).

[7] Lai,X., “On the Design and Security of Block Ciphers,” ETH Series in Information Processing (1992).

[8] Perkins, C., “IP Encapsulation within IP,” RFC2003 (1996).

[9] Postel, J., “Internet Protocol,” RFC791 (1981).

[10] Postel, J., “Internet Control Message Protocol,” RFC792 (1981).

[11] Rekhter, Y., Moskowitz, B., Karrenberg, D., Groot, G.J. and Lear, E., “Address Allocation for Private Internets,” RFC1918 (1996).

[12] 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).

[13] 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).

[14] Srisuresh, P. and Holdrege, M., “IP Network Address Translator (NAT) Terminology and Considerations,” RFC2663 (1999).

[15] Thayer, R., Doraswamy, N. and Glenn, R., “IP Security Document Roadmap,” RFC2411 (1998).

[16] Wiener,M,J., “Efficient DES Key Search,” TR-244, School of Computer Science, Carleton University (1994).

[17] ANSI X3.92,” American National Standard for Data Encryption Algorithm(DEA),” American National Standards Institute (1981).

[18] ANSI X9.17(Revised),“American National Standard for Financial Institution Key Management(Wholesale),” American Bankers Association (1985).

[19] “Merkle-Hellman,” http://www.wikipedia.org/wiki/Merkle-Hellman.

[20] “FreeS/WAN Project,” http://www.freeswan.org.

[21] 有泉, 寺西, 横山, 桧垣, 遠山, “IP 通信拡散法を用いた VPN 装置の実装と性能評価,” 第 11 回情報処理学会マルチメディア通信と分散処理ワークショップ論文集 (2003).