社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
TECHNICAL REPORT OF IEICE.

サイバーソサイエティを実現するリング型 P2P-VPN 技術

八木　幸太郎† 　本田　治† 　大崎　博之† 　松田　和浩†† 　今瀬　眞†

† 大阪大学 大学院情報科学研究科
〒 565-0871 大阪府吹田市山田丘 1-5
†† 日本電子電話株式会社 NTT 情報流通プラットフォーム研究所
〒 180-8585 東京都武蔵野市緑町 3-9-11
E-mail: †{kou-yagi,o-honda,oosaki,imase}@ist.osaka-u.ac.jp, ††matsuda.kazuhiro@lab.ntt.co.jp

あらまし　本稿では、P2P (Peer-to-Peer) 技術を応用することにより、膨大な仮想組織に対して安全かつ信頼性の高いネットワークを提供できる、リング型 P2P-VPN を提案する。リング型 P2P-VPN は、自律的に動作するノードをネットワーク上で論理的にリング状に配置することにより、リング構造の VPN を構築する。リング型 P2P-VPN は、リング型のネットワークトポロジを採用することにより、VPN 数に対して高いスケーラビリティを持つ。本稿では、リング型 P2P-VPN の有効性を、数学的解析により定量的に評価する。その結果、VPN に参加するノード数が比較的少数である場合、提案するリング型 P2P-VPN が、VPN 構築時間や TCP スループットに関して良好な性能を示すことが分かった。

キーワード　P2P (Peer-to-Peer)、VPN (Virtual Private Network)、リング型ネットワーク、IPsec

Ring-Based P2P-VPN for Realizing Cybersociety

Koutaro YAGI†, Osamu HONDA†, Hiroyuki OHSAKI†, Kazuhiro MATSUDA††, and Makoto IMASE†

† Graduate School of Information Science and Technology, Osaka University
1-5 Yamadaoka, Suita, Osaka, 565-0871 Japan
†† NTT Information Sharing Platform Laboratories, NTT Corporation
3-9-11 Midori-cho, Musashino-shi, Tokyo 180-8585, Japan
E-mail: †{kou-yagi,o-honda,oosaki,imase}@ist.osaka-u.ac.jp, ††matsuda.kazuhiro@lab.ntt.co.jp

Abstract　In this paper, we propose a ring-based P2P-VPN (Peer-to-Peer Virtual Private Network) that provides a secure and reliable network to a large number of virtual organizations. The ring-based P2P-VPN establishes VPN by logically connecting nodes that operate autonomously in a ring topology. The ring-based P2P-VPN has an advantage of a high scalability in terms of the number of VPNs accommodated. In this paper, we quantitatively evaluate the performance of ring-based P2P-VPN using mathematical analysis. Through numerical examples, we show that the ring-based P2P-VPN shows satisfactory performance in terms of, for example, VPN construction time and TCP throughput for a relatively small number of VPN nodes.

Key words　P2P (Peer-to-Peer), VPN (Virtual Private Network), Ring Network, IPsec

1 はじめに

近年、インターネットに代表される情報ネットワーク技術が広く普及し、様々な社会活動がネットワーク上で行われつつある。ネットワーク上で安全かつ信頼性の高い通信を実現するための技術として、仮想私設網を構成する VPN (Virtual Private Network) 技術が注目を浴びている [1–3]。

VPN を用いることで、安全かつ信頼性の高い通信を従来の専用線に比べてはるかに安価に実現することができる。現在、MPLS (Multi Protocol Label Switching) [4] に代表される PP-VPN (Provider Provisioned VPN) [5] が広く利用されているが、(1) VPN への参加単位 (帰属単位) がサイトであり、個々の利用者間の VPN を構築することができない、(2) プロトコルの制限もしくはハードウェアの制限により、数十〜数千程度の比較的少数の VPN しか構築することができない、といった問題がある。また、VPN を構築する他の技術として、IPsec VPN が存在する [6] 。IPsec VPN は、VPN への端末単位の帰属が可能であり (1) の問題を解決している。しかし、IPsec VPN では、VPN に参加する端末間でフルメッシュに IPsec トンネルを生成する必要がある。このため、VPN に参加できるノード数が増加する

と IPsec トンネルの数が増加し、比較的少数の VPN しか構築することができない。

これまで、既存の IP ネットワーク上に、オーバーレイネットワークを構築するシステムがいくつか提案されている [7–9]。DVC (Dynamic VPN Controller) [7] は各ノード間に IPsec トンネルを動的に生成、削除することで安全かつ信頼性の高い VPN を構築するシステムである。しかし、DVC は、VPN を構築する際に、ノード間でフルメッシュに IPsec トンネルを生成する必要がある。このため、ノード数が増加するにつれ、必要な IPsec トンネルの数が膨大になり、比較的少数の VPN しか構築することができない。また X-Bone [8] および UMU-PBMN (the University of Murcia Policy-Based Network Management) [9] も VPN を構築することができるシステムである。これらは [7] と異なり任意のトポロジを構築することができるため、IPsec トンネル数を抑えることができる。しかし、これらのシステムは、一度トポロジを構成するとノードの参加と離脱ができないため、ノードの故障などに対応できず高い信頼性を実現できない。

本稿では、P2P 技術を応用することにより、膨大な仮想組織に対して安全かつ信頼性の高いネットワークを提供できる VPN 技術を提案する。提案するリング型 P2P-VPN (Peer-to-Peer VPN) では、P2P 技術によって自律的に動作するノードを、ネットワーク上で論理的にリング状に配置することにより、安全かつ信頼性の高い VPN をスケーラブルな手法で実現する。

さまざまな社会活動をネットワーク上で実現するためには、ある程度広域なネットワーク上で、数十程度の利用者間で VPN を構築する必要がある。しかし、リング型 P2P-VPN はリング型のネットワークトポロジを採用しているため、VPN に参加するノード数が増加すると、伝送遅延やスループットなどの性能が極端に劣化することも予想される [10,11]。また、VPN にとって、VPN を構築するのに必要な時間 (VPN 構築時間) や、VPN が故障状態から回復するのに必要な時間 (VPN 回復時間) も重要な性能指標である。しかし、リング型 P2P-VPN が、どの程度の規模のネットワーク上で、どの程度の数のノードを収容できるかは明らかではない。

本稿では、数学的解析により、提案するリング型 P2P-VPN の有効性を定量的に評価する。具体的には、VPN に参加するノード数や、リンクの帯域および伝搬遅延が、リング型 P2P-VPN の性能 (VPN 構築時間、VPN 回復時間、VPN スループット等) に与える影響を評価する。その結果、VPN に参加するノード数が比較的少数な場合、提案するリング型 P2P-VPN が、VPN 構築時間や TCP スループットなどに関して良好な性能を示すことが分かった。

本稿の構成は以下の通りである。まず、2 章で、提案するリング型 P2P-VPN を説明する。特に、リング型 P2P-VPN の通信制御、VPN への参入制御、VPN からの離脱制御を詳細に説明する。3 章では、数学的解析により、リング型 P2P-VPN における VPN 構築時間、VPN 回復時間、TCP フローのスループット、ラウンドトリップ時間およびパケット棄却率を導出する。またいくつかの数値例により、リング型 P2P-VPN の特性を明らかにする。最後に、4 章で本章のまとめと今後の課題を述べる。

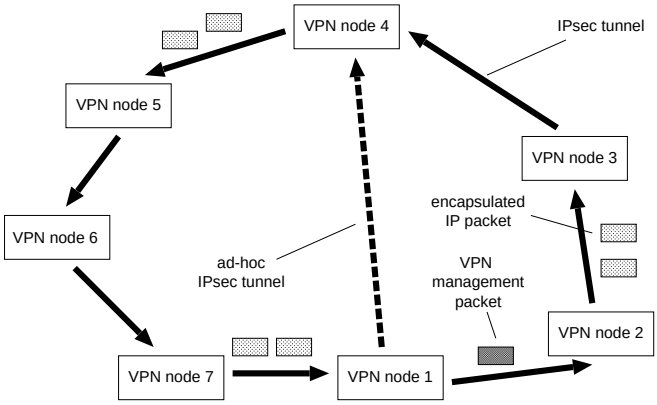

図 1　リング型 P2P-VPN の概要
Fig. 1　Overview of ring-based P2P-VPN.

2　リング型 P2P-VPN 技術

本章では、提案するリング型 P2P-VPN 技術を説明する。リング型 P2P-VPN は、MPLS に代表されるような集中型の VPN 技術とは異なり、それぞれのノードが、自律的に VPN に帰属しているノードを発見し、VPN を構築し、VPN から離脱する。それぞれのノードが自律的に動作することにより、ネットワーク機器の故障やルーティングなどのネットワーク障害に対しても信頼性の高い通信を実現する。また、隣接するノード間で IPsec トンネルを生成することにより安全な通信を実現する。特に、VPN に参加するノードを、物理ネットワーク上で論理的にリング状に配置することにより、IPsec トンネル維持に要するコストを抑え、ネットワーク全体として膨大な数の VPN の実現を可能とする。

図 1 において左回り方向を順方向とすると、各 VPN ノードは、下流の VPN ノードへ IPsec トンネルを形成する。この IPsec トンネルは、上流の VPN ノードから下流の VPN ノードへの一方向通信に使用される。VPN ノード間の通信は、リングに沿って VPN ノードを経由することで行われる。例えば、VPN ノード 1 から VPN ノード 4 へ転送されるパケットは、VPN ノード 2、VPN ノード 3 を順に通過し、VPN ノード 4 へと到着する。このようなリング型ネットワークでは、パケットが通過するノード数が多くなるため通信遅延が増大し、さらにそれに起因してスループットの低下が発生してしまうと予想される [10,11]。そこでリング型 P2P-VPN では、大量のデータや遅延に敏感なアプリケーションのデータを転送する際に、VPN ノード間で直接 IPsec トンネルをアドホックに生成することで、効率的な転送を実現する。

以下では、リング型 P2P-VPN の主な機能である VPN ノード間の通信制御、VPN ノードの VPN への参入制御、VPN ノードの VPN からの離脱制御について詳細に説明する。

2.1　VPN ノード間の通信制御

リング型 P2P-VPN では、VPN ノードは下流の VPN ノードへ IPsec トンネルを介してパケットの転送を行う。暗号化されたパケットの宛先 IP アドレスは、暗号化前のパケットの宛先がどの VPN ノードであるかにかかわらず、下流の VPN ノード

の IP アドレスとなる。

VPN ノードは、上流の VPN ノードから暗号化されたパケットを受け取ると、暗号化前のパケットの宛先 IP アドレスと、自身の IP アドレスを比較する。比較の結果、IP アドレスが一致した場合、VPN ノードは、IPsec による暗号化を解除し、パケットを受信する。一方、比較の結果 IP アドレスが一致しない場合、VPN ノードは、暗号化前のパケットの送信元 IP アドレスと、自身の IP アドレスを比較する。比較の結果、アドレスが一致した場合、VPN ノードは暗号化されたパケットを破棄する。暗号化前のパケットの送信元 IP アドレスと、自身の VPN ノードの IP アドレスの一致が、暗号化されたパケットがリング型ネットワークを一周しており、パケットを受信すべき VPN ノードが存在しないことを意味するからである。一方、IP アドレスが一致しない場合、VPN ノードは、暗号化されたパケットの宛先 IP アドレスを下流 VPN ノードの IP アドレスに変更し、暗号化されたパケットを転送する。

2.2 VPN ノードの参入制御

VPN ノードがリング型 P2P-VPN へ参入する際の制御を説明する。以下では、新たにリング型 P2P-VPN へ参入する VPN ノードを「新規 VPN ノード」と呼ぶ。

新規 VPN ノードは、VPN の管理者から、すでに VPN に参加している VPN ノードのリストとリングの構成情報を得る。そして、ICMP Echo [12] を利用して、新規 VPN ノードとすでに VPN に参加している各 VPN ノード間の、ラウンドトリップ時間を測定する。

次に、測定した値を用いて、リングのどの位置に、新規 VPN ノードが参入すべきかを決定する。具体的には、リングにおいて隣接関係にある各 VPN ノード対について、新規 VPN ノードと下流の VPN ノード間および新規 VPN ノードと上流の VPN ノード間のラウンドトリップ時間の和をそれぞれ計算する。計算した値が最小となる VPN ノード対が、新規 VPN ノードがリングに参加する位置となる。そして、新規 VPN ノードと上流の VPN ノード間で IPsec トンネルを生成し、また、新規 VPN ノードと下流の VPN ノード間で IPsec トンネルを生成する。最後に、不要となった上流の VPN ノードと下流の VPN ノード間の IPsec トンネルを削除する。

2.3 VPN ノードの離脱制御

VPN ノード間の通信が何らかの理由で途絶した場合、リング型 P2P-VPN では、VPN ノードが自律的にリングを再構成する。リングを再構成する際の VPN ノードの離脱制御を説明する。

リング上では、VPN ノード間を管理パケットが巡回している。管理パケットには、リング VPN に参加している VPN ノードのリストとリングの構成情報が記録されている。VPN ノードは、管理パケットを受信すると、上流の VPN ノードに対し確認応答を返す。VPN ノードは、管理パケットを転送してから一定時間確認応答を受信できないと、下流の VPN ノードが故障したと判断する。

故障を検知した VPN ノードは、故障した VPN ノードのさらに下流の VPN ノードに対し、故障が発生したことを通知する。そして、その下流の VPN ノードとの間に、新たに IPsec トンネルを構築する。さらに、故障を検知した VPN ノードおよび新たな下流の VPN ノードは、故障した VPN ノードとの IPsec トンネルを削除する。最後に、故障を検知した VPN ノードは、管理パケットに記録されている、VPN ノードのリストとリングの構成情報を更新し、下流の VPN ノードに管理パケットを転送する。

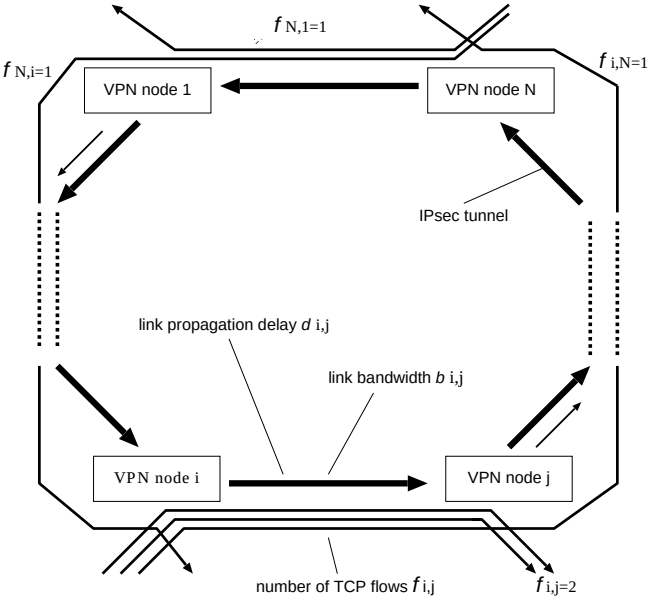

図 2　解析モデル
Fig. 2　Analytic model.

3 解　　析

本章では、まず、リング型 P2P-VPN のモデル化を行い、リング型 P2P-VPN における VPN 構築時間、VPN 回復時間、TCP フローのスループット、ラウンドトリップ時間およびパケット棄却率を導出する。さらにいくつかの数値例を示すことにより、リング型 P2P-VPN の性能を定量的に示す。

3.1 解析モデル

解析モデルを図 2 に示す。ネットワーク中に N 個の VPN ノードが存在する場合を考え、i 番目の VPN ノードを VPN ノード i $(1 \leq i \leq N)$ とする。VPN ノード i から VPN ノード j 間のリンク帯域を $b_{i,j}$、VPN ノード i から VPN ノード j 間の伝送遅延を $d_{i,j}$、送信元が VPN ノード i であり宛先が VPN ノード j である TCP フローの総数を $f_{i,j}$ と定義する。また、VPN ノードの接続行列を $M = (m_{i,j})$ とする。つまり、VPN ノード i から VPN ノード j に対して IPsec トンネルが設定されている場合に $m_{i,j} = 1$ とし、それ以外の場合は $m_{i,j} = 0$ と定義する。

まず N 個の VPN ノードが VPN に参加した場合の、VPN のラウンドトリップ時間 R_N は、VPN ノード間のリンクが一方向であるため、次式で与えられる。

$$R_N = \sum_{i=1}^{N} \sum_{j=1}^{N} m_{i,j} d_{i,j} \tag{1}$$

3.2 VPN 構築時間

VPN ノード 1 から VPN ノード N まで順次 VPN に参加する

ために要する時間 (VPN 構築時間) X_N を導出する。そこでまず、VPN ノード i が新たに VPN に参加する場合に要する時間 x_i を導出する。VPN ノード i は、すでに VPN に参加している各 VPN ノード間のラウンドトリップ時間を計測し、ラウンドトリップ時間の増加が最小限となるように VPN を再構築する。新規 VPN ノードが VPN に参加した時の、上流の VPN ノードと下流の VPN ノードをそれぞれ r および l とする。VPN ノード i および VPN ノード j 間のラウンドトリップ時間が、VPN ノード間の伝送遅延 $d_{i,j}$ を用いて $2d_{i,j}$ で近似できると仮定すれば、VPN ノード r および l は次式によって与えられる。

$$\min_{l,r}\left(\frac{2d_{l,i}+2d_{i,r}}{m_{l,r}}\right) \tag{2}$$

VPN ノード i は、(a) VPN ノード i および VPN ノード r 間に IPsec トンネルを生成、(b) VPN ノード l および VPN ノード i 間に IPsec トンネルを生成、(c) VPN ノード l および VPN ノード r 間の IPsec トンネルを削除、という手順により VPN の再構築を行う。VPN ノードに IPsec トンネルの生成通知および削除通知が届いてから、実際に IPsec トンネルが生成および削除されるまでの処理遅延を、それぞれ Δ_1 および Δ_2 とする。すでに VPN に参加している各 VPN ノード間のラウンドトリップ時間が既知 (つまり、ラウンドトリップ時間は事前に計測されており、時間とともに変化しない) と仮定する。VPN ノード i が (a) 〜 (c) の処理を順次実行すると仮定すれば、X_i は次式で与えられる。

$$\begin{aligned} x_i &= (2d_{i,r}+\Delta_1)+(2d_{l,i}+\Delta_1)+(\max(2d_{l,i},2d_{i,r})+\Delta_2) \\ &= 2\max(d_{l,i},d_{i,r})+\Delta_2+2(d_{l,i}+d_{i,r}+\Delta_1) \end{aligned} \tag{3}$$

1 番目に VPN に参加する VPN ノードは、 IPsec トンネルの生成・削除が不要であるため、x_1 は 0 である。また、2 番目に VPN に参加する VPN ノードは、IPsec トンネルの生成のみ必要であるため、x_2 は $2(d_{l,i}+d_{i,r}+\Delta_1)$ となる。このため、VPN 構築時間 X_N は次式で与えられる。

$$X_N = \begin{cases} 0 & \text{if } N=1 \\ 2(d_{l,i}+d_{i,r}+\Delta_1) & \text{if } N=2 \\ 2(d_{l,i}+d_{i,r}+\Delta_1)+\sum_{i=3}^{N} x_i & \text{otherwise} \end{cases} \tag{4}$$

3.3 VPN 回復時間

VPN ノード i が VPN から離脱した場合に、VPN を再構築するために要する時間 Y_i (VPN 回復時間) を導出する。VPN ノード i が何らかの障害により VPN から離脱する場合を考える。この時、VPN ノード i の前段の VPN ノード l ($m_{l,i}=1$) と、VPN ノード i の後段の VPN ノード r ($m_{i,r}=1$) との間で IPsec トンネルを生成する必要がある。具体的には、以下のような手順で VPN ノード障害の検出、新規 IPsec トンネルの生成、不要な IPsec トンネルの削除が行なわれる。(a) VPN ノード l が確認応答パケットの不着により VPN ノード i の障害を検出、(b) VPN ノード l から VPN ノード r への IPsec トンネルを生成、(c) VPN ノード l および VPN ノード i 間の IPsec トンネルを削除、(d) VPN ノード i および VPN ノード r 間の IPsec トンネルを削除。実際には、(c) および (d) は (b) と並行して処理することが可能であるため、VPN 回復時間 Y_i は次式で与えられる。

$$Y_i = 2d_{l,i}+2d_{l,r}+\Delta_1 \tag{5}$$

3.4 TCP フローのスループット・ラウンドトリップ時間・パケット棄却率

VPN 内を通過する全ての TCP フローのうち、TCP スループットが最小となる TCP フローのスループット T_{min} を導出する。以下、全ての TCP フローは連続的にデータを送出すると仮定する。まず、VPN ノード i と VPN ノード j 間を通過する TCP フロー数 $n_{i,j}$ は次式で与えられる。

$$n_{i,j}=\sum_{l=0}^{N-1}\sum_{k=0}^{N-l-2} f_{i-k,j+k} \tag{6}$$

VPN ノード i と VPN ノード j 間のリンクがボトルネックとすると、VPN ノード i と VPN ノード j は、次式で与えられる。

$$\min_{i,j}\left(\frac{b_{i,j}}{n_{i,j}m_{i,j}}\right) \tag{7}$$

ここで、送信元が VPN ノード i であり宛先が VPN ノード j である TCP フローのラウンドトリップ時間 $R_{i,j}$ は、VPN ノード間のリンクが一方向であることから全て等しくなる。つまり

$$R_{i,j}=R_N \tag{8}$$

となる。従って T_{min} は、次式で与えられる。

$$T_{min}=\min_{i,j}\frac{b_{i,j}}{n_{i,j}} \tag{9}$$

TCP フローのパケット棄却率を p とすれば、TCP フローのスループット T_{min} は、近似的に次式で与えられることが知られている [13]。

$$T_{min}\simeq\frac{1}{2R_N}(-3+\frac{\sqrt{6+21p}}{\sqrt{p}}) \tag{10}$$

従って、TCP フローのパケット棄却率 p は次式で与えられる。

$$p\simeq\frac{3}{2R_NT_{min}(3+R_NT_{min})-6} \tag{11}$$

3.5 数 値 例

パラメータ (VPN ノード数、リンクの帯域、リンクの伝送遅延、IPsec トンネル生成時間、TCP フロー数) を変化させ、VPN 構築時間、VPN 回復時間、TCP フローのスループット、ラウンドトリップ時間およびパケット棄却率がどのように変化するのかを調べた。

リング型のネットワークでは、VPN ノード数が増加すると、特に伝送遅延やスループットなどの性能が劣化すると考えられる [10,11]。そこで、VPN に参加する VPN ノード数を、$N=4-40$ と変化させ、VPN ノード数 N が、VPN 構築時間 X_N、VPN 回復時間 Y_N、TCP スループット T_{min} およびラウンドトリップ時間 R_N に与える影響を調べた。なお、VPN ノード間の伝送遅延およびリンク帯域は、それぞれ 0–D_{max} および 0–B_{max} の一様分布によって与えた。数値例で用いたパラメー

表 1　数値例で用いたパラメータ

VPN ノード数	N	4-40
VPN ノード間の最大伝送遅延	D_{max}	50,100,200[ms]
VPN ノード間の最大リンク帯域	B_{max}	10 [Mbit/s]
IPsec トンネルの生成時間	Δ_1	10[ms]
IPsec トンネル削除時間	Δ_2	0[ms]

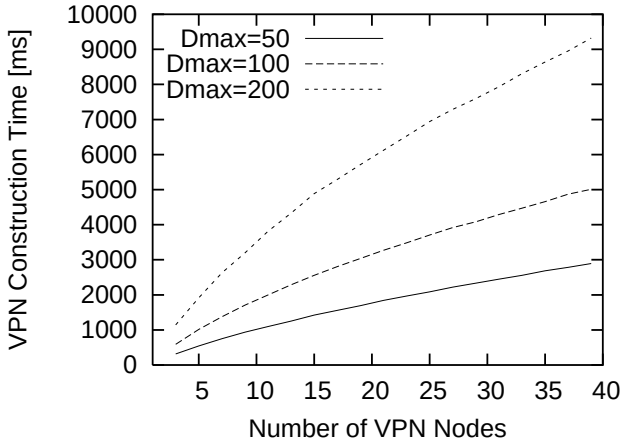

図 3　VPN ノード数 N と VPN 構築時間 X_N の関係

Fig. 3　Number of VPN nodes N vs. VPN construction time X_N.

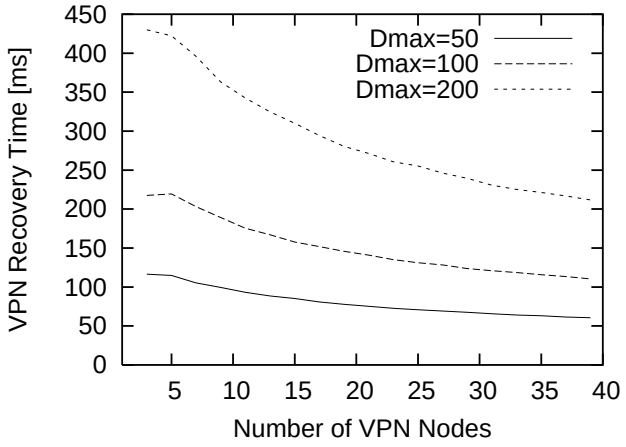

図 4　VPN ノード数 N と VPN 回復時間 Y_N の関係

Fig. 4　Number of VPN nodes N vs. VPN recovery time Y_N.

タを表 1 に示す。

図 3–図 6 に、VPN ノード数 N を変化させた時の、VPN 構築時間 X_N、VPN 回復時間 Y_N、TCP スループット T_{min}、ラウンドトリップ時間 R_N をそれぞれ示す。

図 3 より、VPN ノード数 N の増加につれて、VPN 構築時間 X_N も増加していることが分かる。これは、式 (4) から分かるように、VPN ノード数が増加すると、VPN ノード間に生成される IPsec トンネル数が増加するためと考えられる。またリンクの伝送遅延が増加すると、 VPN 構築時間も増加することが分かる。これは VPN ノード間の通信遅延が増加するためと考えられる。

図 4 より、VPN 回復時間は、VPN ノード数の増加につれて減少していることが分かる。これは、VPN ノード数が増加すると、各 VPN ノード間の平均遅延が小さくなるためと考えられる。また VPN ノード間の伝送遅延が増加すると VPN 回復時間も増加していることが分かる。これは式 (5) から分かるように、ノード間の伝送遅延が小さくなると、IPsec トンネルの生成および削除に要する時間が小さくなるためと考えられる。

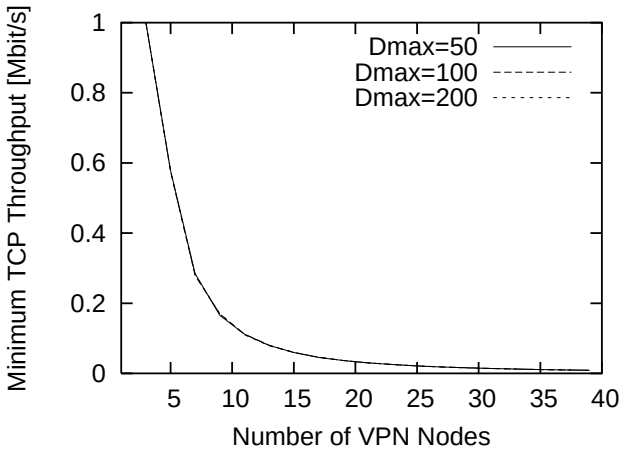

図 5　VPN ノード数 N と TCP スループット T_{min} の関係

Fig. 5　Number of VPN nodes N vs. minimum TCP throughput T_{min}.

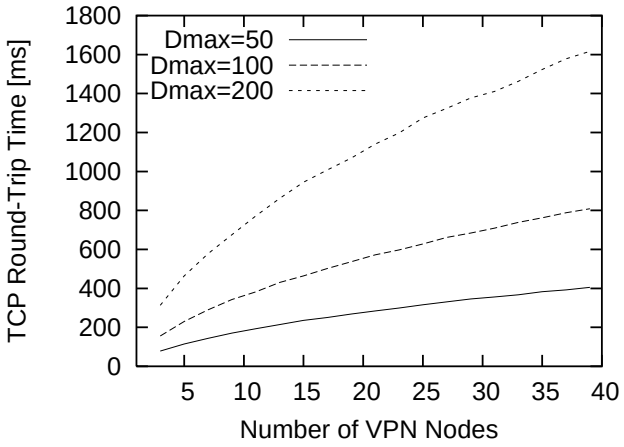

図 6　VPN ノード数 N と TCP ラウンドトリップ時間 R_N の関係

Fig. 6　Number of VPN nodes N vs. TCP round-trip time R_N.

図 5 より、VPN ノード数の増加につれて、TCP スループットが急激に減少していることが分かる。これは、VPN ノード数が増加すると、VPN ノード間のリンクを通過する TCP フロー数も増加し、1 本の TCP フローが利用可能な帯域が減少するからと考えられる。また VPN ノード間の伝送遅延は、TCP フローのスループットに影響を与えないことが分かる。これは式 (9) からも分かるように、TCP フローのスループットは、VPN ノード間のリンク帯域と TCP フロー数で決まるためである。

図 6 より、VPN ノード数の増加につれて、TCP フローのラウンドトリップ時間が、ほぼ線形に増加していることが分かる。これは、式 (1) からも分かるように、VPN ノード数が増加すると、リングを一周するために経由する VPN ノード数が増加するためと考えられる。また VPN ノード間の伝送遅延が大きくなると、ラウンドトリップ時間も増加することが分かる。

4 まとめと今後の課題

本稿では、P2P 技術によって自律的に動作するノードを、論理的にリング型に配置することで VPN を構築する、リング型 P2P-VPN を提案した。リング型 P2P-VPN は、IPsec トンネル維持に要するコストを抑え、ネットワーク全体として多数の VPN を実現できる。また、それぞれのノードが自律的に動作することで、ネットワーク障害に対しても信頼性の高い通信を実現する。さらに本稿では、リング型 P2P-VPN の性能を数学的解析により明らかにした。まず、リング型 P2P-VPN のモデル化を行い、VPN 構築時間、VPN 回復時間、TCP フローのスループット、ラウンドトリップ時間およびパケット棄却率を導出した。いくつかの数値例を示すことにより、リング型 P2P-VPN の性能を定量的に明らかにした。今後の課題として、アドホックトンネルによる通信制御の有効性の評価や、VPN ノードの障害が VPN 構築時間や VPN 回復時間に与える影響の評価が挙げられる。

文　　献

[1] B. Gleeson *et al.*, "A framework for IP based virtual private networks," *Request for Comments (RFC) 2764*, Feb. 2000.

[2] M. Carugi and J. D. Clercq, "Virtual private network services: Scenarios, requirements and architectural constructs from a standardization perspective," *IEEE Communication Magazine*, June 2004.

[3] A. Nagarajan, "Generic requirements for provider provisioned VPN," *Internet Draft* `<draft-ietf-ppvpn-generic-reqts-02.txt>`, Jan. 2003.

[4] E. Rosen and Y. Rekhter, "BGP/MPLS VPNs," *Request for Comments (RFC) 2547*, Mar. 1999.

[5] R. Callon, M. Suzuki, J. D. Clercq, B. Gleeson, A. G. Malis, K. Muthukrishnan, E. C. Rosen, C. Sargor, and J. J. Yu, "A framework for layer 3 provider provisioned virtual private networks," *Internet Draft* `<draft-ietf-ppvpn-framework-08.txt>`, Mar. 2003.

[6] S. Kent and R. Atkinson, "Security architecture for the Internet protocol," *Request for Comments (RFC) 2401*, Nov. 1998.

[7] "Dynamic VPN controller (DVC) demonstrator project report," Oct. 2003. available at `http://www-mice.cs.ucl.ac.uk/multimedia/meetings/vpnworkshop/documentat%ion/proceedings/2003-11-12/VPN-KMS-Issues.doc`.

[8] J. Touch, "Dynamic internet overlay deployment and management using the X-Bone," *Computer Networks*, vol. 36, pp. 117–135, July 2001.

[9] A. Gomez, G. Martinez, and O. Canovas, "New security services based on PKI," *Future Generation Computer Systems*, vol. 19, pp. 251–262, Jan. 2003.

[10] M. Ergen, D. Lee, R. Attias, S. Tripakis, A. Puri, R. Sengupta, and P. Varaiya, "Wireless token ring protocol," *SCI Orlando*, July 2002.

[11] R. Jain, "Performance analysis of FDDI token ring networks: Effect of parameters and guidelines for setting TTRT," *IEEE Lightwave Telecommunication Systems*, vol. 20, pp. 16–22, May 1991.

[12] J. Postel, "Internet control message protocol," *Request for Comments (RFC) 792*, Sept. 1981.

[13] H. Ohsaki, J. Ujiie, and M. Imase, "On scalable modeling of TCP congestion control mechanism for large-scale IP networks," in *Proceedings of IEEE SAINT 2005*, pp. 361–369, Feb. 2005.