

新世代モバイルインターネットサービスにおけるプロトコルに関する研究

メタデータ	言語: ja 出版者: 静岡大学 公開日: 2012-03-08 キーワード (Ja): キーワード (En): 作成者: 高橋, 修 メールアドレス: 所属:
URL	https://doi.org/10.14945/00006438

理工学研究科

高

GD

K

0003528346

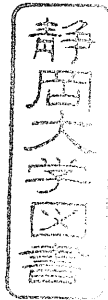
R

365

静岡大学附属図書館

静岡大学 博士論文

新世代モバイルインターネットサービスにおける
プロトコルに関する研究



平成 15 年 9 月

大学院理工学研究科

設計科学専攻

高橋 修

論文要旨

インターネットおよび移動通信の発展とあいまって、携帯電話から電子メールや Web アクセスを提供するモバイルインターネットサービスが、世界で初めて NTT ドコモより i-mode サービスとして PDC を利用して 1999 年 2 月より始まった。その後、他社でも同様のサービスが提供されるに伴い、利用の簡便さと、豊富なサービス、手ごろな価格が功を奏し、爆発的に普及し、現在では日本の携帯所有者のうち携帯インターネット加入者の割合は、75%に達し、世界を大きくリードするに至るまで成長している。一方、携帯電話は、第 3 世代のサービスが開始されており、この高速移動通信環境（上り：64Kb/s, 下り：384Kb/s）を利用して、よりリッチなコンテンツを使用しかつ多様な新世代モバイルインターネットサービスが期待されている。

新世代モバイルインターネットサービスを実現するために解決すべき種々の課題があるが、本論文では、第 3 世代移動通信ネットワークに適用する新しいモバイルインターネットサービスの実現に向け、以下の 5 つの研究の目的と対象を設定し、研究を進めた。

(1) 移動機向けモバイルインターネットアーキテクチャ

本研究では、移動機専用のプロトコルとして開発された WAP プロトコル（旧 WAP フォーラムで標準化）とインターネットプロトコル（HTTP/TCP）の性能を比較評価し、IMT-2000 などの高速移動通信ネットワークで想定されるマルチメディアなどの大容量コンテンツを配信する場合、HTTP/TCP などのインターネットプロトコルを適用することが可能であることを示し、それに基づくモバイルインターネットアーキテクチャを提案する。

(2) 移動通信ネットワークの特徴を生かす新サービス

本研究では IMT-2000 等の高速移動通信ネットワークに適した HTTP/TCP をベースとした移動機向けプッシュプロトコルを新たに提案する。また、実証評価により、提案方式は WAP1.1 のプッシュプロトコルと比較し、プッシュ完了までの通信時間が短くなることを示し、特にデータサイズが大きいデータの場合には提案方式が有効であることを示す。さらに本論文では、XHTML とプッシュ機能を組合せた差分プッシュ方式を提案し、テストベッド試作によりその有効性を検証する。

(3) TCP プロトコルプロファイルの最適化

第3世代移動通信ネットワークの代表的な方式であるW-CDMAのリンク層再送動作を検討し、リンク層における遅延ジッタ抑制と伝送効率のトレードオフ関係を分析して、評価すべきリンク層およびTCPの動作パラメータを明確にする。リンク層プロトコル(RLC)における調整パラメータであるTimer_Status_Prohibitをシミュレーションによって評価し、その最適値が200[ms]であることを示す。また、リンク層での再送が有効であること、ブロック誤り率(BLER)が0~10%では5回の再送で十分であることを示す。さらに、TCPの受信ウィンドウサイズは、リンクの帯域幅遅延積を反映した48-64[KB]が適正值であることを示す。

(4) ゲートウェイ(GW)の実現方式

本論文では、W-CDMAパケットネットワークを介して、インターネットアクセスを高速に行う場合のGW方式として、End-Endでアドレス情報が透過となるステルス型GW方式を提案すると共に、実装評価を行う。その結果、インターネット上に多数存在するW-TCPが適用されていないサーバに対するアクセスにおけるスループットと応答時間を、提案方式で2-3倍程度に改善できることを明らかにする。更に、GWでの処理遅延時間は、数msec(CPU使用率:0%)~数十msec程度であり、提案方式は、欠点であるオーバーヘッドは無視できるくらい小さく、かつその特徴(保守性・運用性等に優れる)を十分生かすことが可能である実用的な方式であることを明らかにする。

(5) 企業通信向けセキュアモバイルサービス

本論文では、VPNをW-CDMAネットワークに適用する場合のモバイルVPN方式として、広く使用されているIPsecをベースとし、新しいVPNセッション管理方式を提案する。また、TCPの性能問題を解決するためプロキシ機能をモバイルVPNルータ上で実現することとし、その際に新たに発生するセキュリティ問題を防止するセキュアTCPアクセラレータの実現方式を提案する。更に、信頼性を向上させるための冗長化ルータ構成を可能とし、系の切り替えを効率の良く実現する方式を提案する。最後に、実装評価結果により、提案した方式の機能が有効に働き、かつ性能上もTCPスループットを最大3倍向上させると共に、モバイルVPNルータの障害時に系の切り替え時間が3秒程度であり、十分実用的な方式であることを示す。

最後に、本研究の成果をとりまとめ、結論を示すとともに、今後の課題について述べる。

目次

第1章 緒論	1
1.1 研究の背景	1
1.2 研究の目的と対象	4
1.3 論文の構成	8
第2章 移動機向けモバイルインターネットアーキテクチャ	12
2.1 はじめに	12
2.2 WAP 仕様の概要	13
2.3 WAP クライアントおよび WAP ゲートウェイの実装	15
2.4 バイナリ符号化の性能評価	18
2.5 WAP プロトコルの性能評価	23
2.6 次世代モバイルインターネットアーキテクチャの提案	29
2.7 おわりに	31
第3章 移動機向けプッシュプロトコルの提案と評価	32
3.1 はじめに	32
3.2 プッシュプロトコルの提案	33
3.3 プッシュプロトコルの性能評価	38
3.4 差分プッシュ方式	47
3.5 おわりに	53
第4章 W-CDMA ネットワークでのリンク層 ARQ と TCP の特性評価	55
4.1 はじめに	55
4.2 W-CDMA ネットワークとリンク層再送機構	55
4.3 関連研究	59
4.4 RLC 再送のもとでの TCP 伝送性能	60
4.5 エミュレーションとシミュレーションによる特性評価	62
4.6 おわりに	73
第5章 高速インターネットアクセスのための行列型ゲートウェイの提案と実装評価	75

5.1	はじめに	75
5.2	インターネットアクセスの高速化のためのプロトコル手法の概要	76
5.3	ステルス型ゲートウェイ実装方式の提案	78
5.4	実装評価	88
5.5	おわりに	95
第6章 モバイルVPN方式		96
6.1	はじめに	96
6.2	VPNの概要	97
6.3	モバイルVPNの要件	100
6.4	モバイルVPN方式の提案	104
6.5	実装評価	110
6.6	おわりに	115
第7章 結論		116
謝辞		120
参考文献		121
筆者発表論文等		129

第1章 緒論

1.1 研究の背景

(1) インターネットの発展経緯

インターネットは、1969年にアメリカ国防総省高等研究計画局（DARPA: The Defense Advanced Research Projects Agency）によって実験運用が開始された ARPA ネットに端を発する。ここでは、分散配置された異機種のコピュータを相互接続し、コンピュータ資源を共有するための分散型ネットワーク技術の確立が目的であった。インターネットでは、仮想端末 (telnet) とかファイル転送 (FTP) などのアプリケーションに代表される分散配置されたコンピュータ資源を旧有するための手段が提供され、主に大学や先端研究機関を中心に利用され発展してきた。その過程で TCP/IP などの通信プロトコルの原形も開発された。その後、フリーウェアであるバークレー版 UNIX で TCP/IP がバンドルされたこともあり、爆発的に普及していった [1]。

インターネットは、学術研究用のネットワークとして発展してきた経緯から、ネットワークの運営・管理主体が存在せず、コンピュータ資源や管理の手間はボランティアによって提供されてきた。しかし、このような運用方法はネットワークおよび利用者の拡大とともに次第に破綻をきたしてきたため、アメリカでは1990年に利用料金を設定し、より安定したサービスを提供するための商用サービスが始まった。日本においても、1992年から商用サービスが始まり、商用インターネットサービスの時代が幕を開けた。また、パソコンのハードウェアおよびOSの高機能化にともない TCP/IP が標準的に搭載されるようになり、その普及は加速された。加えて、初期の目的であった資源共有のためのアプリケーションである仮想端末やファイル転送に加えて、個人間のコミュニケーション手段である電子メールや、情報検索手段である WWW (World Wide Web) のような GUI (Graphic User Interface) をベースとしたアプリケーションが提供されるようになって、それまでインターネットは、UNIX ワークステーションを利用する研究者やエンジニアの道具だったものが、一般のユーザにより身近なものとなって、指数関数的に普及した。

2002年2月における世界のインターネット利用者総数は、5億4,420万人で、もっとも利用者数の多い米国が1億6,614万人、次いで日本が5,593万人となっている (図 1-1, 1-2) [2]。

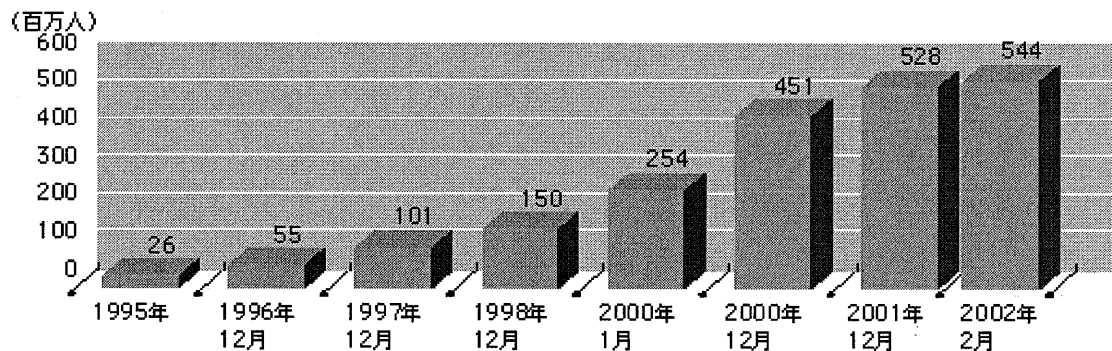
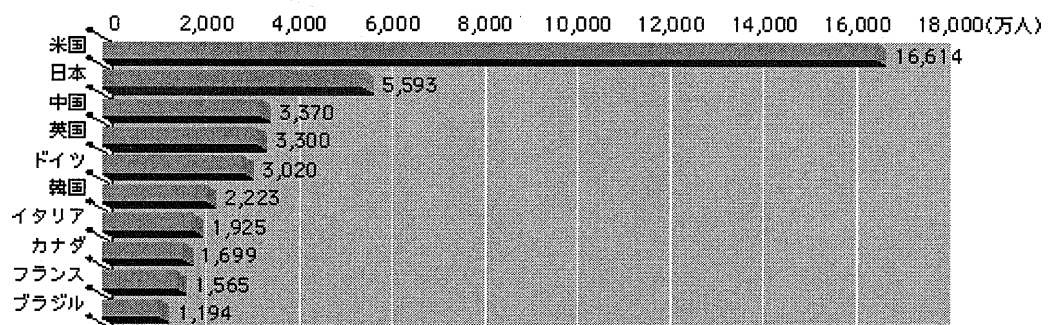


図 1-1 世界のインターネット利用者の推移 (文献 [2] より抜粋)



総務省「通信利用動向調査」、NUA 社調べ (平成 14 年 3 月) より作成

図 1-2 世界のインターネット利用者数の上位 10 カ国 (文献 [2] より抜粋)

また、最近日本では、DSL (Digital Subscriber Loop) を初めとする 1.5M-12Mbps のブロードバンドサービスが定額・低料金で提供されるようになり、その利用者は平成 14 年 3 月末現在で約 400 万人に達している。

今や、日本におけるインターネットの世帯普及率は 60% を超え (平成 13 年末)、ほぼ当たり前のように日常生活の中でインターネットが利用されるようになっている。

(2) 移動通信ネットワークの発展経緯

移動通信ネットワークは、次のように進展してきた。日本では、アナログ方式による自動車電話が 1979 年に、また携帯電話が 1987 年に音声中心のサービスとして開始され、第 1 世代の移動通信サービスと呼ばれている。第 2 世代の移動通信サービスは、デジタル方式である PDC 方式によって 1993 年に開始され、音声サービスと低速データ通信 (9.8Kbps~28.8Kbps) を提供している。

更に、移動通信におけるマルチメディア化の対応として、高速広帯域化（移動時 384Kbps, 静止時 2Mbps）等を実現する第 3 世代方式として世界的な標準である IMT-2000 の規格が 1999 年末に制定された。これを受けて日本では、NTT ドコモが 2001 年 5 月より「FOMA」の試行サービスを、また同年 10 月より本サービスを開始し、移動通信による高速な情報通信（32kbps～384Kbps）が可能となった [3], [4]。更に、より一層の高速広帯域（第 3 世代の 10 倍）なサービス実現を目指した第 4 世代移動通信ネットワークの研究も始まっている [5]。

携帯電話の加入契約者の推移を図 1-3 に示す。

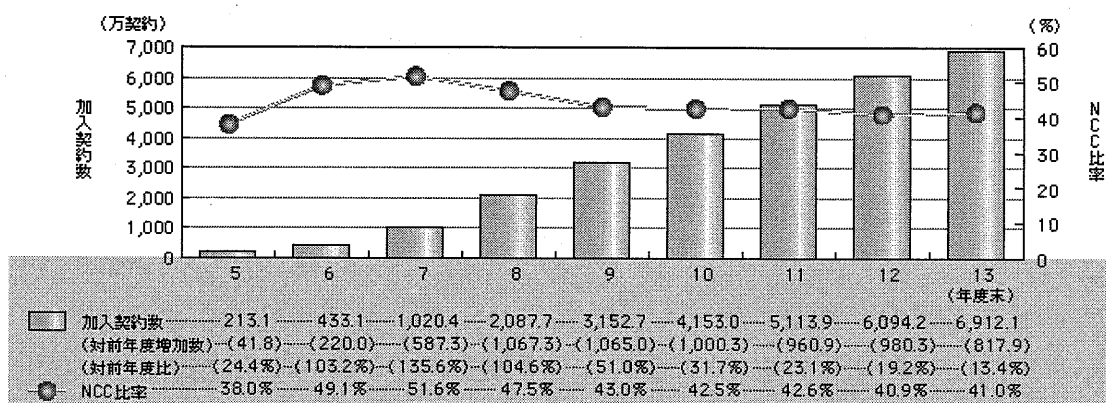
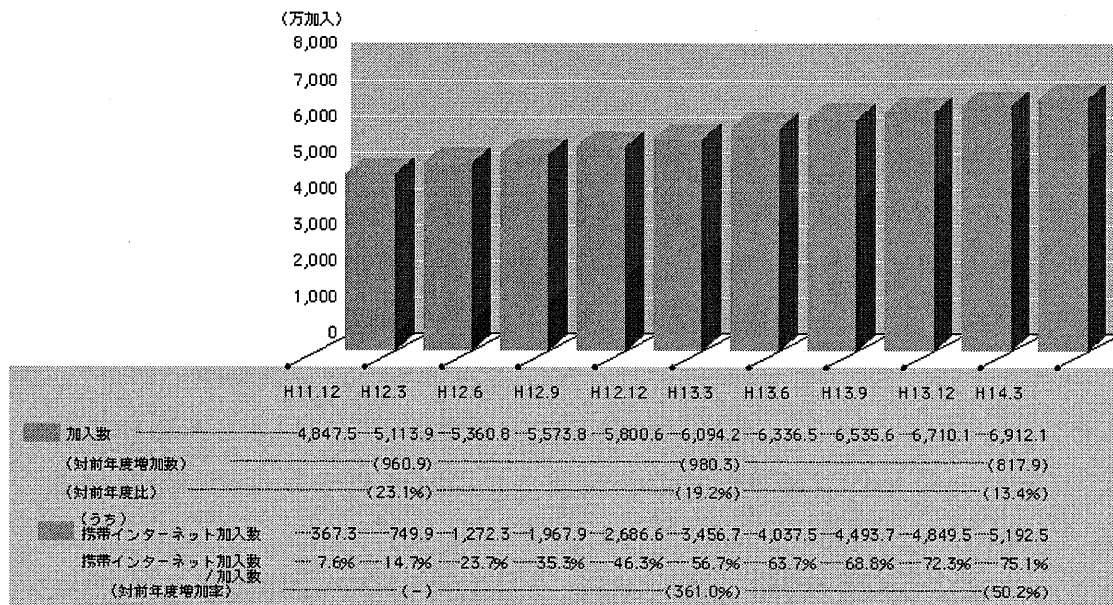


図 1-3 携帯電話の加入契約者数の推移（文献 [2] より抜粋）

(3) インターネットと移動通信の融合

インターネットおよび移動通信の発展とあいまって、携帯電話から電子メールや Web アクセスを提供するサービスが、世界で始めて NTT ドコモより i-mode サービスとして PDC を利用して 1999 年 2 月より始まった。いつでも、どこでも手軽に利用できる簡便さと、低料金（従量課金）であったことが功を奏し、爆発的に普及した（図 1-4 参照）。i-mode サービスは、上述の FOMA でも提供されており、高速通信環境を利用して、より豊富な情報通信サービスが提供されている [4]。日本における携帯所有者のうち携帯インターネット加入者の割合は 75% に達し、この分野のサービスおよび技術は日本が世界を大きくリードしている。



※ 携帯インターネット加入数は、携帯電話事業者によるiモード、EZweb（旧EZaccessを含む）、J-Skyのサービスの加入数合計

図 1-4 携帯電話からのインターネットアクセス加入者数（文献 [2] より抜粋）

今後もこのようなモバイルインターネットサービスを健全に発展させるためには、移動通信ネットワークの特徴を生かす新しいモバイルインターネットサービスとそれらを支えるプロトコルに関する研究が必要である。

1.2 研究の目的と対象

次世代のモバイルインターネットサービスにおけるプロトコル技術には解決すべき種々の課題があるが [6] - [12]，本論文では，第 3 世代移動通信ネットワークに適用する新しいモバイルインターネットサービスの実現に向け，以下の観点から，研究の目的と対象を設定した．なお，次世代モバイルインターネットサービスとしてマルチキャスト [13] を利用した放送・通信融合型サービスが有望と考えられるが，移動通信ネットワークでの具体的なサポート方式が未確定なため，本研究では検討対象外としている．

(1) 移動機向けモバイルインターネットアーキテクチャ

モバイルインターネットサービスを普及させる上での重要な要素は，その基本技術としてオープンなデファクトスタンダードを採用することである．しかしながら，現在インターネットで利用されているプロトコル (TCP/IP) は，有線ネットワークを前提に設計された経緯があり，高誤り率，高遅延等の無線

通信環境の特徴を十分に考慮していないため、そのままでは十分な性能を得られないという問題がある。OMA (Open Mobile Alliance) (旧 WAP フォーラム) では、無線環境に最適化した新しいプロトコルとして WAP (Wireless Application Protocol) (WAP1.x) を標準化した。ただし、機能的、性能的な評価がまだ十分行われていないのが現状であり、その実用性も不明確な部分が多い。以上のような状況を鑑み、WAP の特徴的な機能に関して、その効果を定量的に評価するとともに、第 3 世代移動通信ネットワークに適したモバイルインターネットアーキテクチャを明確にすることが重要である。

(2) 移動通信ネットワークの特徴を生かす新サービス

移動通信ネットワークを利用した特徴的なサービスにプッシュサービスがある。

このサービスを実現するプロトコルは、上述の WAP1.x で既に規定されているが、インターネットで利用されているプロトコルを必要に応じて最適化 (サブセット化) するなどして実現できれば、インターネットのアプリケーションと親和性の高いシームレスなサービスを提供することが可能となる。このため、インターネットプロトコルベースのプッシュプロトコルを新たに検討する必要がある。更に、次世代マークアップ言語として有力な XHTML (Extensible HTML) を前提に、効率の良いプッシュ方式について検討する必要がある。

(3) TCP プロトコルプロファイルの最適化

インターネット通信の 90%以上は TCP が使用されており、大部分のアプリケーションは Web とメールである。一般に移動通信ネットワークは、伝送誤りがあり、IP ネットワークに比べ伝送単位長が小さな無線区間を含むのが特徴であり、この場合無線区間のデータリンク層で誤り回復を使用することによって、エンド-エンドの誤り回復だけを用いた場合に起こる性能低下を補償することができる。しかし、トランスポート層の TCP とデータリンク層の再送機構を併用する場合、プロトコルパラメータを最適値に設定しないと性能を逆に低下させる可能性もある。第 3 世代の移動通信ネットワークを介して TCP を利用して通信する場合に、その性能を最大限に引き出せるようなデータリンク層と TCP のプロトコルパラメータの最適値を明確にする必要がある。

(4) ゲートウェイの実現方式

上記 (3) で述べた最適化された TCP プロファイルをクライアントに設定することは、移動機に接続するためのドライバと一緒にプロファイル設定ソフトウ

エアを配付することなどによって比較的容易に実現可能であると予想される。一方、インターネットに無数にあるすべてのサーバに適用するのは非現実的である。このため、クライアントとインターネット上のサーバとの間にゲートウェイを設置し、通常の TCP と最適化 TCP を相互に変換する必要がある。この時、このゲートウェイは、今後新規に定義される任意のアプリケーションプロトコルを使え、IP アドレスがエンド-エンドで透過的になることが重要となる。このため、第 3 世代移動通信ネットワークを介した高速インターネットアクセスのためのゲートウェイの実現方式を検討する必要がある。

(5) 企業通信向けセキュアモバイルサービス

第 3 世代移動通信ネットワークや、無線 LAN によるホットスポットサービスの本格的な普及により、モバイルコンピューティングにおけるインターネット接続環境は大幅に向上することが期待されている。また、近年頻発しているクラッキング事件によってユーザのセキュリティ意識はますます向上している。これらより、今後モバイル環境におけるインターネット VPN (Virtual Private Network) の利用が急速に増加することが予想される。固定ネットワークを前提とした VPN は既に実用になっているが、移動通信ネットワーク経由でサーバにアクセスするモバイル環境にそのまま適用しても、広帯域が特徴である W-CDMA ネットワークのポテンシャルを十分に引き出せない可能性等がある。このため、移動通信ネットワーク特有の性質が VPN に及ぼす影響を明確にし、その対策を検討することがモバイル VPN を普及させる上で重要である。

上述した課題のモバイルインターネット基本システムとの関連を図 1-5 に示す。

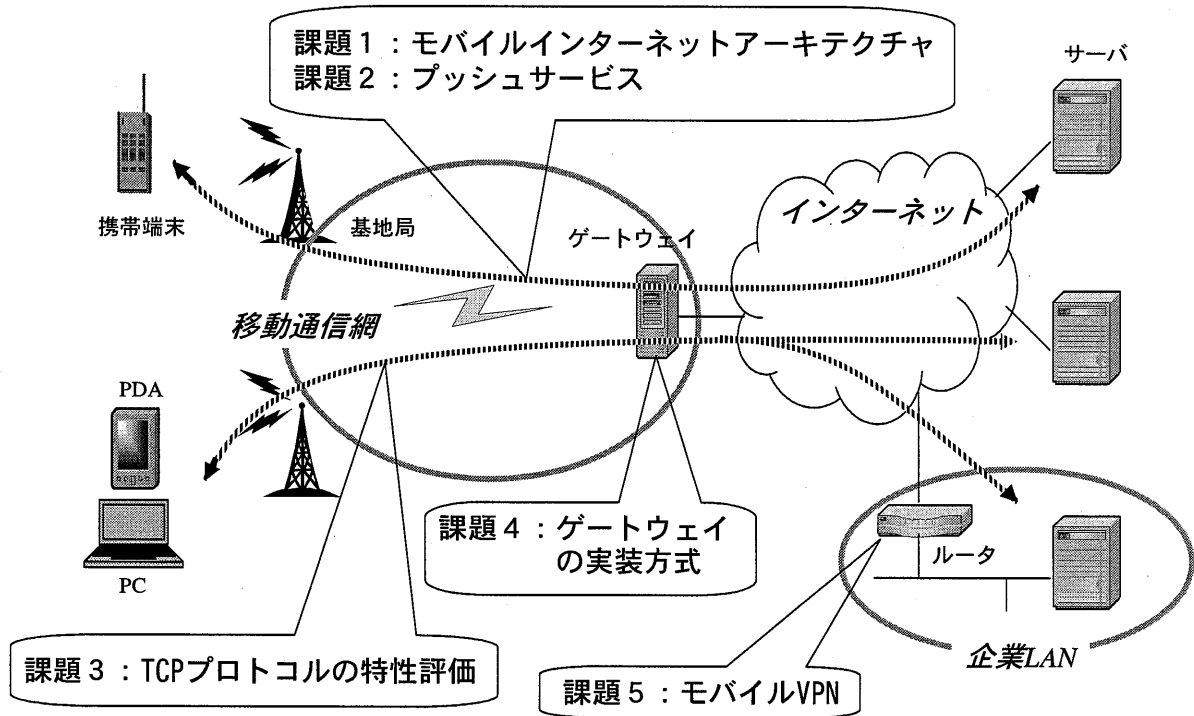


図 1-5 モバイルインターネットの基本システム構成と研究課題

1.3 論文の構成

本論文では、上述した新世代モバイルインターネットサービスにおけるプロトコルに関する研究課題について以下の構成で研究結果を示す（図 1-5）。

第 2 章 移動機向けモバイルインターネットアーキテクチャ

第 3 章 移動機向けプッシュプロトコル

第 4 章 W-CDMA ネットワークでのリンク層 ARQ と TCP の特性評価

第 5 章 高速インターネットアクセスのためのステルス型ゲートウェイ

第 6 章 モバイル VPN 方式

第 7 章 結論

以下に各章の概要を述べる。

第 2 章では、WAP プロトコル（WAP1.1 仕様）とインターネットプロトコル（HTTP/TCP）の応答時間などを実装したプロトタイプシステムにより比較評価する。特に、WAP の特徴的な機能であるヘッダおよびコンテンツのバイナリ符号化についての効果も定量的に評価する。これらの結果、小容量のコンテンツを配信する場合、両プロトコルはほぼ同等の性能を持つが、第 3 世代移動通信ネットワークなどで想定されるマルチメディアなどの大容量コンテンツを配信する場合には、HTTP/TCP などのインターネットプロトコルが有利であることを示す。更に、これらの評価結果に基づき、第 3 世代移動通信ネットワークに代表される高速移動通信ネットワークに適した次世代モバイルインターネットアーキテクチャを提案する。

第 3 章では、IMT-2000 等の 3G 高速無線ネットワーク向けプッシュ機能の実現を目的とし、インターネットで用いられているプロトコルを用いてプッシュ機能を実現する方式を提案する。提案方式では、無線向け TCP プロファイルと HTTP を用い、WAP1.x と同様なオリジンサーバ起動型のプッシュ機能を実現する。その為のプロトコルとして、HTTP の機能の中からプッシュ機能を実現するために必要な部分をサブセット化すると共に、必要な機能を追加してプッシュ機能を実現する。また、次世代のマークアップ言語として有力な XHTML (Extensible HTML) 1.0 と XSLT (Extensible Stylesheet Language Transformations) に着目し、それと提案したプッシュ機能を組合せた新しい差分プッシュ方式を提案する。本提案は、オリジンサーバ側で古いデータと更新後の新しいデータとの差分を自動的に生成し、移動機にプッシュするものである。これによって移動機は、

常にアップデートされた最新のデータを表示可能となり，ネットワーク上でのチャット画面の自動更新や，株式情報チャートの自動更新等のサービスへ応用することが可能になる．なお，XHTML1.0は，HTML4.01をXML (extensible Markup Language) に基づいて再定義したものであり，HTML4.01の後継となるマークアップ言語としてW3C (World Wide Web Consortium) で標準化されたものである．XSLTは，XMLデータの自動変換機能を提供するものであり，同じくW3Cにて標準化されたものである．最後に，提案方式に基づいて実装したテストベッドシステムにより，提案方式の有効性について検証した結果について述べる．

第4章では，現在市場にあるTCP実装で適用可能な範囲でTCPの性能を最大限に引き出せるようなW-CDMA (IMT-2000) リンク層プロトコルおよびTCPの動作パラメータの最適値を求める．本論文は以下のアプローチを取る．W-CDMAにおけるTCPの性能を評価するには，リンク層の誤り回復メカニズムであるRadio Link Control (RLC) とTCPの相互作用を調べるのが重要である．そのため，現在用いられているTCP実装で性能を引き出すために，TCPでの無駄な再送の原因となるリンク層での遅延ジッタを抑制する方法を検討し，W-CDMAリンク層で用いられるSelective Repeat型ARQを詳細に再現したシミュレーションモデルにおいて，各種プロトコルパラメータを変化させ，リンク層における性能と効率のトレードオフについて検討を加えることとする．

最初にW-CDMAネットワークの特性を概説し，関連研究と我々のアプローチについて述べ，W-CDMAネットワーク特性に影響を与えるリンク層の再送メカニズムについて調べ，ネットワークエミュレータによる実際のTCP実装を用いた実験と，計算機上のシミュレーションにて無線ネットワーク上でのTCPによるデータ伝送特性の評価と考察を行い，得られた結果と今後の課題をまとめる．

第5章では，最初にW-CDMAパケットネットワーク等の高速移動通信ネットワークを経由してインターネットアクセスを高速に行うためのプロトコル手法の概要について述べる．次に，IPアドレス等の透過性を保ちつつ，W-TCPとTCPの相互変換とHTTP (Hypertext Transfer Protocol) リクエストパイプラインを含む任意のAPプロトコルの中継を可能とするステルス型GWを提案する．更に，提案したステルス型GW方式の試作による実証評価結果について述べる．これらの結果，ステルス型GW方式によりEnd-Endのアドレス情報の透過性を維持したまま，スループット及び応答時間をそれぞれ2-3倍程度向上すること，及びGWに於ける中継処理時間が無視できるほど小さいことを明らかにし，提案方

式が実用的なものであることを示す。

第 6 章では、最初にモバイル環境での VPN 利用の要件と課題を明確にする。具体的には、VPN を実現する際に標準的に使用されているプロトコル (IPsec) をモバイル環境に適用させるために考慮すべき課題、モバイル VPN ルータでのプロキシ機能 (TCP アクセラレータ機能) の必要性とそれを実現する際のセキュリティ上の課題、更に、信頼性向上のための仮想ルータ方式 (VRRP : Virtual Router Redundancy Protocol) をモバイル VPN ルータに適用する際の課題について明確にする。

次に、これらの課題を解決する方式として、キープアライブによらない新しい VPN セッション管理方式、TCP セッションハイジャックを防御するセキュア TCP アクセラレータ方式、及び冗長化された VPN ルータ間 (現用/予備) の切り替えを短時間に効率的に行う方式を提案する。

更に、これらの方式のプロトタイプによる評価システムとその評価結果について述べる。移動通信ネットワークとして W-CDMA を想定した評価結果から、提案した VPN セッション管理方式がキープアライブなしでも VPN セッションを維持出来ること、セキュア TCP アクセラレータ方式により TCP セッションハイジャックを防止しつつ、スループットを最大 3 倍程度向上できること、冗長化されたルータ間の系の切り替えが 3 秒程度で行われ、ほぼ実アプリケーションに影響を与えず実現可能なこと等を示す。これらにより、本文で提案するモバイル VPN 方式は、固定ネットワークとほぼ同じセキュリティレベルと移動通信ネットワークの特徴を最大限に活かす性能が得られ、モバイル環境に適用できる実用的なものであることを示す。最後に、残された課題と今後の検討計画について述べる。

第 7 章では、各章で得られた結果のまとめと今後の課題について述べる。

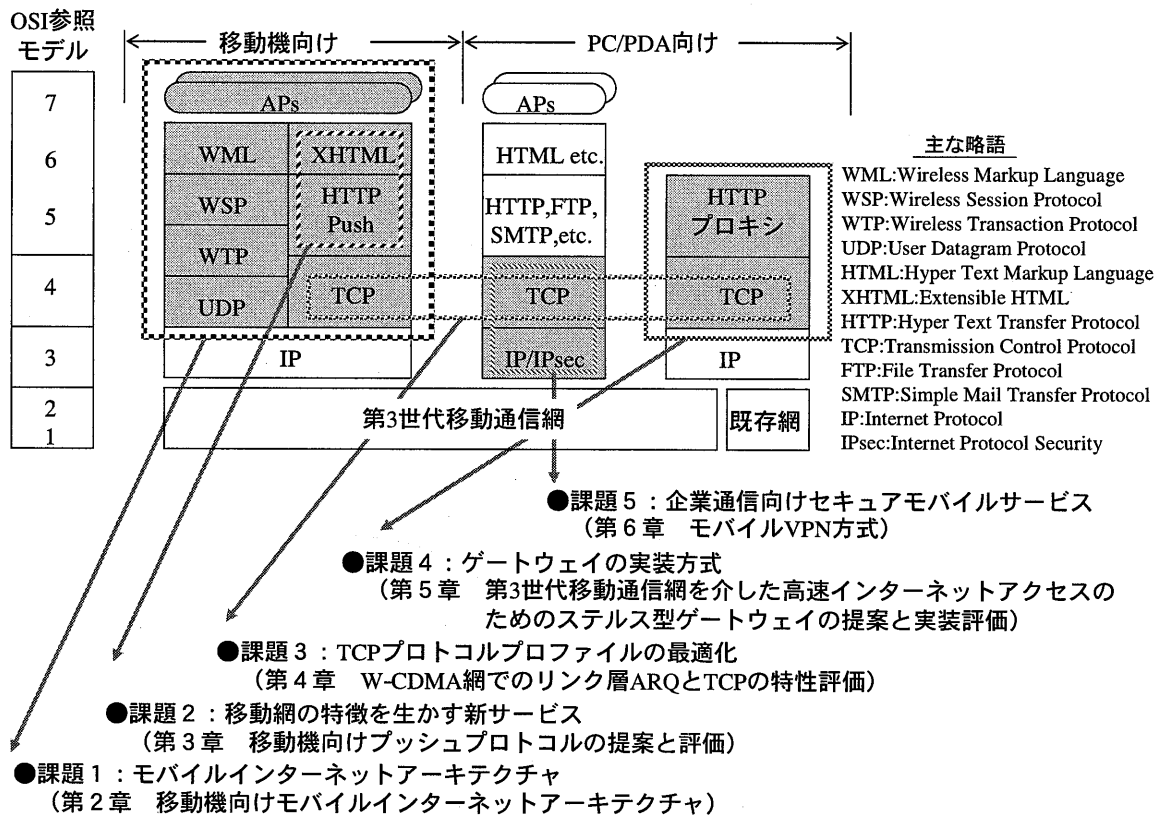


図 1-6 研究課題と論文の構成

第2章 移動機向けモバイルインターネットアーキテクチャ

2.1 はじめに

携帯電話, PDA などから, ニュースや天気予報, モバイルバンキングなどのインターネット上のコンテンツにアクセスするサービスが注目を集めている. 今後このようなモバイルインターネットサービスの需要は急速に増加することが予想され, 現在のインターネットアクセスやメールなどのサービスだけでなく, 携帯電話や PDA の特徴を生かしたアプリケーションの開発が進展することが期待されている.

しかしながら, 現在インターネットで用いられているプロトコルは, 高誤り率, 高遅延等の無線環境の特徴を十分に考慮していないため, そのままでは十分な性能が得られないという問題がある. そこで, OMA (Open Mobile Alliance) (旧 WAP フォーラム) では, 無線環境に最適化したプロトコルとして, WAP (Wireless Application Protocol) の標準化を進めている.

WAP を用いたサービスが各国で開始されているが, そのサービスの種類は少なく, 機能的, 技術的にもその評価が十分に行われていないのが現状であり, その実用性について不明確な部分が多い.

そこで, 本章では, WAP プロトコル (WAP1.1 仕様 [14]) とインターネットプロトコル (HTTP/TCP) の応答時間などをプロトタイプシステムにより実測し, 比較評価を行う. また, WAP の特徴的な機能であるヘッダ及びコンテンツのバイナリ符号化については, その効果を定量的に評価する.

より高速な移動通信ネットワークとして, GPRS (General Packet Radio Service) などの第 2.5 世代移動通信ネットワーク, 第 3 世代移動通信ネットワーク (IMT-2000: International Mobile Telecommunication-2000) (以下 3G ネットワークと略す) のサービスが開始されている. 最後に, WAP の評価結果に基づいて, IMT-2000 に代表される高速移動通信ネットワークに適したモバイルインターネットアーキテクチャを提案する [15].

本章の構成は, 以下のとおりである. 2.2 章では, WAP 仕様の概要について述べる. 2.3 章では, 1999 年に公開された WAP1.1 仕様に基づく WAP クライアントおよび WAP ゲートウェイの試作について述べる. 2.5 章では, 無線シミュレータを用いて行った, WAP プロトコルとインターネットプロトコル (HTTP/TCP) の比較評価について述べる. 2.6 章では, WAP プロトコルとインターネットプロトコ

ルの性能評価の結果に基づいて、IMT-2000 に適したモバイルインターネットアーキテクチャを提案する。

2.2 WAP 仕様の概要

WAP とは、携帯電話などのモバイル端末からインターネットのコンテンツへのアクセスを実現することを主な目的に、OMA で標準化が進められているプロトコルとアプリケーション環境である。以下では、WAP の基本である WAP 1.1 仕様に基づいて、WAP のアーキテクチャ、プロトコルの概要について述べる。

2.2.1 WAP アーキテクチャ

WAP のアーキテクチャは、WAP クライアント、WAP ゲートウェイ、オリジンサーバから構成される。WAP クライアントは移動機、PDA などの小さい画面のモバイル端末を想定している。オリジンサーバとしては、WWW サーバなどの既存のインターネット上のサーバを使用することを前提としている。

WAP クライアントと WAP ゲートウェイの間は、WAP フォーラムで標準化した WAP プロトコルを使用して通信する。WAP プロトコルは、高誤り率、高遅延などの特徴を持つ無線環境に最適化されたプロトコルで、幅広い無線ネットワーク (CDMA, GSM, PDC など) に対応している。WAP ゲートウェイとオリジンサーバの間は、TCP/IP, HTTP などの標準的なインターネットプロトコルを使用して通信する。従って、WAP のアーキテクチャは、基本的にインターネットの WWW アーキテクチャを無線環境向けに拡張したもので、WAP ゲートウェイは、無線環境とインターネットの間のゲートウェイの役割を果たしている。

2.2.2 WAP プロトコル

WAP プロトコルは、WDP (Wireless Datagram Protocol) , WTLS (Wireless Transport Layer Security) , WTP (Wireless Transaction Protocol) , WSP (Wireless Session Protocol) から構成される。

WAP は幅広い無線ネットワークへの適用を考慮しており、WDP において無線ネットワークの違いを吸収するベアラアダプテーションの概念がある。無線ネットワークが IP をサポートする場合は、WDP は UDP を使用する。

WTLS は、TLS [16] をベースに、無線環境への最適化を図ったプロトコルで、暗号化、認証などのセキュリティ機能を提供する。

WTP は、3クラス(クラス 0, 1, 2)のトランザクション型通信機能を提供している。特にクラス2では、信頼性のある要求/応答型通信を実現している。また、オプションである分割・再組み立て機能がサポートされる場合には、パケット欠落の検出や選択的再送を行う。

WSP は HTTP をベースとしてセッション管理を行うプロトコルである。WSP は HTTP1.1 [17] 相当の機能に加えて、プッシュ、セッションの中断と再開、ヘッダのバイナリ符号化などの WSP 固有の機能を提供している。

2.2.3 WAP アプリケーション環境

WAE (Wireless Application Environment) は、WAP のアプリケーション環境の総称で、マークアップ言語である WML1.1 (Wireless Markup Language)、スクリプト言語である WML Script、WAP ゲートウェイから WAP クライアントにプッシュサービスを提供する WAP プッシュなどから構成される。

WML1.1 は WAP フォーラムで規定した XML 準拠のコンテンツ記述言語で、HTML 相当のタグに加えて、カード&デッキなどの WML 固有のタグを定義している。WML1.1 では、無線環境で WAP クライアントに転送する WML コンテンツのサイズを圧縮するため、WML1.1 のタグ、属性等のバイナリ符号化を規定している。また、WAP ゲートウェイで WML コンテンツのパーズング処理、バイナリ符号化を行うことにより、WAP クライアントの負荷軽減を図っている。

2.2.4 WAP 関連研究

インターネット上にあるコンテンツの多くは HTML を用いて記述されている。WAP1.x クライアントが HTML コンテンツに対してアクセスする場合には、WAP ゲートウェイにおけるコンテンツ変換が必要となる。論文 [18] は、HTML から WML への変換の差異の問題点等について整理しており、変換時のいくつかの問題点の解決法を提案している。しかし、HTML と WML は、元々互換性が無いため、あらゆるコンテンツを変換する際には問題がある。さらに、ユーザ数が増加した場合の変換のオーバーヘッドによるゲートウェイスケーラビリティの問題は非常に重要であるが、その点についても考察されていない。

WAP プロトコルの評価に関しては、WTP のクラス2の実装とその評価をした論文 [19] が存在する。この論文は、WAP 仕様のいくつかの不具合を指摘しているが、無線ネットワーク上で WTP の性能を評価したものではない。

論文 [20] は、モバイルブラウザアプリケーション利用時のネットワーク利用状況について分析している。この研究では、日々と毎週のサイクルについて測定し、ネットワークトラヒックの特徴として自己相関関係があることを導いている。また、この研究では、モバイルブラウザアプリケーションによるトラヒックの特徴について WWW トラヒックと比較している。この研究は、無線ネットワークの設計に非常に有用であるが、1G、2G ネットワークを対象に測定しており、3G ネットワークを対象にはしていない。3G ネットワークでは、ネットワークの性質及び提供されるコンテンツのサイズ等も劇的に変化することから、3G ネットワークにおける同様な評価に関する研究が求められる。

2001 年に、FOMA サービス等の 3G サービスが開始された。WAP が 3G ネットワークにおいてどのような性能特性が得られるかを把握することは非常重要であるが、現在までに、3G サービス上での WAP のプロトコルに関する研究はされていない。

2.3. WAP クライアント及び WAP ゲートウェイの実装

WAP1.1 に基づいて WAP クライアント及び WAP ゲートウェイの実装を行った。本試作システムは、100Mbps LAN (100BASE-TX) で接続された WAP クライアント、WAP ゲートウェイ、オリジンサーバから構成される。IMT-2000 における無線環境を擬似するために、WAP クライアントと WAP ゲートウェイの間に無線シミュレータを設置した。無線シミュレータ (4.5.1.2 参照) は無線ネットワークにおけるレイヤ 2 以下の処理を擬似するものであり、ベアラ特性として伝送速度、遅延時間、誤り率、最大再送回数等の値を予め設定することにより、IMT-2000 などの無線ネットワーク上を流れるパケットの動作を擬似できる。また、WAP ゲートウェイはインターネット上のオリジンサーバにアクセス可能である。本試作システムの構成を図 2-1 に、実装した WAP プロトコルスタックを図 2-2 に示す。

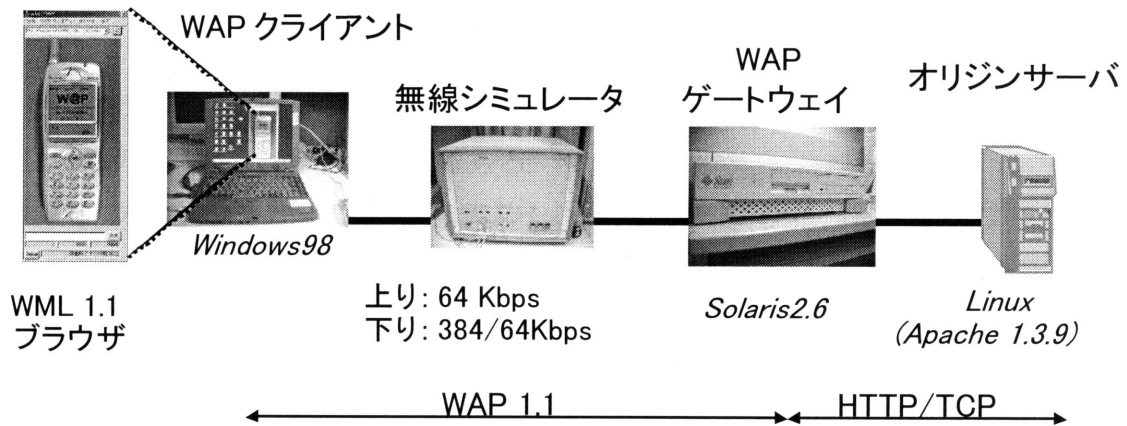


図2-1 WAP試作システムの構成

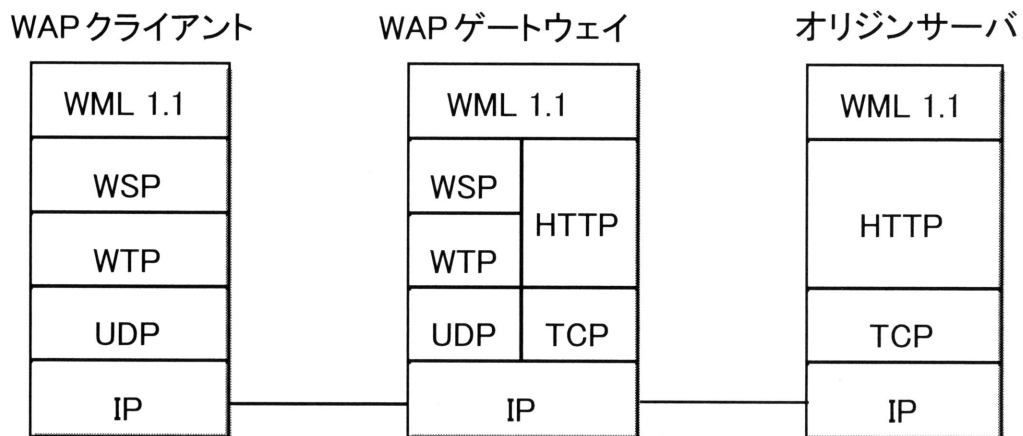


図2-2 WAP試作システムのプロトコルスタック

2.3.1 WAP クライアント

WAP クライアントは、Pentium3 550MHz、メモリ 256MB の PC (Windows98) 上で C++言語を用いて実装した。WAP クライアントは WML1.1 ブラウザ、WAP プロトコル管理、WAP プロトコル制御などから構成される。

WML1.1 ブラウザは、図 2-1 に示すような携帯電話の画面上で WML コンテンツの表示を行う。マウスやキーボードを用いて携帯電話の画面に URL を入力することで、オリジンサーバ上の WML コンテンツを取得、表示することが可能であ

る。

WAP プロトコル管理は、WAP プロトコルの各レイヤ間のインタフェース制御、通信パラメタの管理などを行う。各プロトコルのパラメタ値の設定、性能評価のためのデータ取得等が可能である。

WAP プロトコル制御は、今回実装した WSP ライブラリ、WTP ライブラリ、UDP ライブラリなどから構成され、OS 標準の Windows Sockets を用いて WAP ゲートウェイと通信を行う。

2.3.2 WAP ゲートウェイ

WAP ゲートウェイは、Ultra Sparc333MHz、メモリ 512MB の WS (Solaris2.6) 上で C 言語を用いて実装した。WAP ゲートウェイはインターネットプロトコル制御、ゲートウェイアプリケーション、WAP プロトコル管理、WAP プロトコル制御などから構成される。

インターネットプロトコル制御は、インターネットプロトコル (HTTP/TCP) を用いてオリジンサーバと通信を行う。

ゲートウェイアプリケーションは、オリジンサーバから受信した WML コンテンツのパーズ処理、バイナリ符号化を行った後、WML クライアントに送信する。XML パーサにはフリーソフト (RXP beta15) を使用し、XML パーズの際には、RXP beta15 独自の API を用いている。なお、バイナリ符号化は、WAP 仕様にあわせて新たに実装した。

WAP プロトコル管理、WAP プロトコル制御は WAP クライアントと同等の処理を行う。

2.3.3 オリジンサーバ

オリジンサーバは、Pentium2 200MHz、メモリ 64MB の PC (Linux) 上で WML コンテンツのオリジンサーバとして、WWW サーバとして広く利用されている Apache1.3.9 を使用した。Apache の CGI 機能を使用して、CGI を含む WML コンテンツを作成することも可能である。

2.3.4 WAP アプリケーション

本システム上のアプリケーションとして、プッシュアプリケーションを試作した。プッシュアプリケーションでは、WAP ゲートウェイがプッシュサーバとな

り、WSP のプッシュ機能を用いて WAP クライアントに画像、テキストをプッシュする。更に、WSP の POST メソッド (CGI 機能) を使用した電子メールの送信アプリケーションと WSP のプッシュ機能を応用した電子メールの受信アプリケーションを試作した。

2.4 バイナリ符号化の性能評価

WAP のバイナリ符号化には、WBXML で規定された WML コンテンツのバイナリ符号化と、WSP ヘッダのコンパクト符号化の 2 種類が存在する。それぞれの符号化の性能を評価した。WAP のバイナリ符号化は、WAP 1. x の特徴の一つであり、その圧縮率と符号化時間を測定することにより、3G のような高速ネットワークに適用した場合の効果について明らかにする。

2.4.1 WML コンテンツのバイナリ符号化

WML コンテンツのバイナリ符号化は、以下の 2 つの要素から構成される。

1) XML パーサによる構文解析

WML コンテンツの構文解析を行う。

2) WBXML 符号化

タグや改行コード等の制御コードに対して WBXML 符号化を行う。WBXML 符号化は、バイナリ化モードとテキストモードの 2 種類のモードを切り替えて以下のように行われる。例えば、WML コンテンツ中に wml というタグが存在したとすると、そのバイナリ化ルールに従って WBXML バイナリ化を行う。タグの値など、WBXML のバイナリ化ルールに存在しない値については、テキストモードに切り替えてテキストをそのまま表現し、終了後にまたバイナリ化モードを元に戻すことによって続けて WBXML 符号化を続ける。

WML コンテンツのバイナリ符号化は、対象となるコンテンツにより符号化の効果が異なり、あらゆるコンテンツについて定量的な評価結果を求めることは不可能であるため、典型的なコンテンツについて評価を行った。今回の測定に用いた WML コンテンツを図 2-3 に示す。

<pre><?xml version="1.0"?> <!DOCTYPE wml PUBLIC"/WAPFORUM//DTD WML 1.1//EN" "http://www.wapforum.org/DTD/wml_1.1.xml"></pre>	①
<pre><wml> <card id="card2" ontimer="/auto500-2wml#card1" <timer value="50"/> <p mode="wrap"></pre>	②
<pre> *50オクテットのテスト *
 ***deck1 ***
 WAPは無線環境に適したプロトコルであり 携帯電話、PDA等からインターネットへアクセスを行うた めのプロトコルである。 (以下省略)</pre>	③
<pre> </p> </card> </wml></pre>	④

図 2-3 評価対象 WML コンテンツ

図 2-3 では WML を構成する最低限の種類タグ (“wml”, “card”, “p”) 及び改行タグの “br” を使用しており、それ以外はテキストデータで構成している。従って、他のタグが含まれるコンテンツを用いた場合には、さらに圧縮率は高くなることも考えられる。

今回の評価では、図 2-3 の③に示すテキスト領域のサイズを変化させることにより、複数サイズのコンテンツ (500, 1000, 1400, 20480, 368640 バイト) を用意した。また、符号化の圧縮率と処理時間に着目し、以下の評価を行った。

- ・ WML バイナリ符号化と gzip 圧縮率の比較評価 (図 2-4)
- ・ WML バイナリ符号化の処理時間とそれに含まれる XML パーサの処理時間の評価 (図 2-5)

バイナリ符号化は、先述したように、XML パーサによる構文解析が行われた後、タグや改行コード等の制御コードに対して符号化が行われる。WML バイナリ符号化の処理時間は、XML パーサの処理時間と、WBXML 符号化の合計時間を示しており、そのうちの XML パーサの処理時間についてを、図 2-5 中に示している。なお、XML パーサにはフリーソフト (RXP bata15) を用いた。

図 2-4 に示すエンコード前後のサイズの比率とは、エンコードによって減少したサイズを元のサイズで割った比率のことを示しており、圧縮されたサイズ

が大きいほど、圧縮率が高いということを示している。WML バイナリ符号化では、コンテンツサイズが大きくなるに従い圧縮比率が下がる。これは、図 2-3 の①に示すコンテンツの先頭部分の圧縮率が高く、この部分が 3 バイトに圧縮されるため、コンテンツサイズが大きくなるに従い先頭部分の圧縮の効果が全体としては小さくなるからである。また、gzip 圧縮では、逆にコンテンツサイズが大きくなるに従い圧縮効果が高い。以上のことから、タグ等の圧縮対象部分のみの圧縮を行う WML バイナリ符号化は、その圧縮効果は高いものの、今回の評価対象のようにサイズが大きくなるに従い相対的にテキスト部が増加するコンテンツでは圧縮効果は低い。

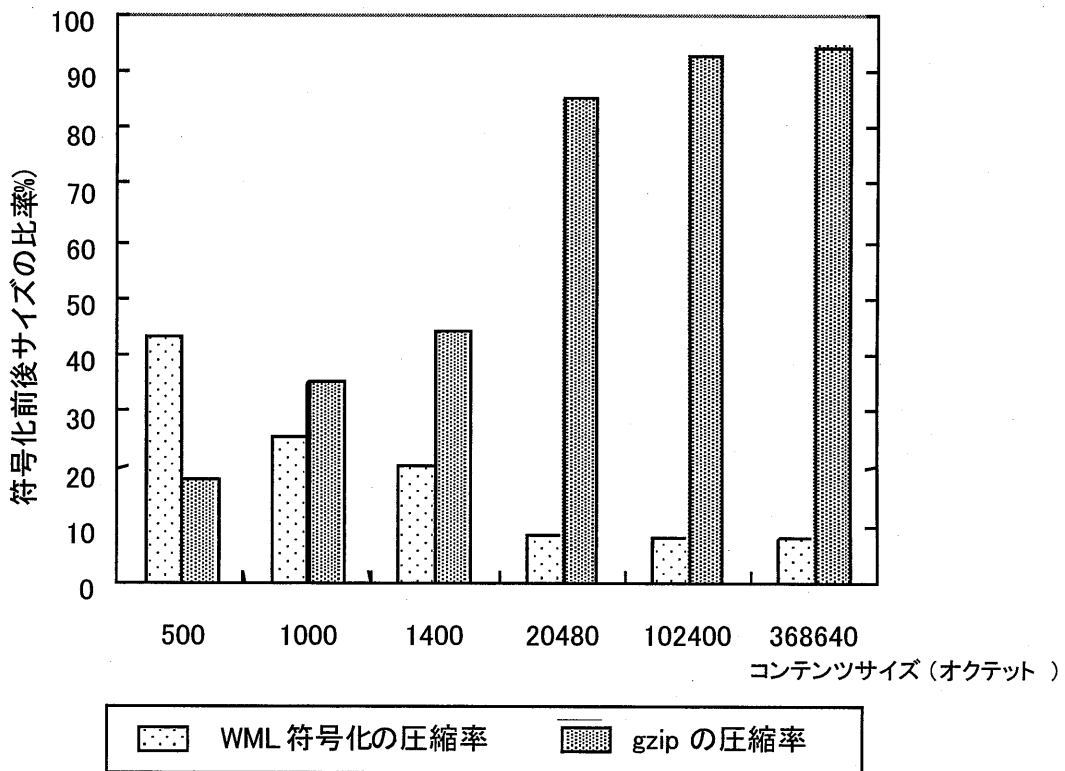


図 2-4 符号化の圧縮率

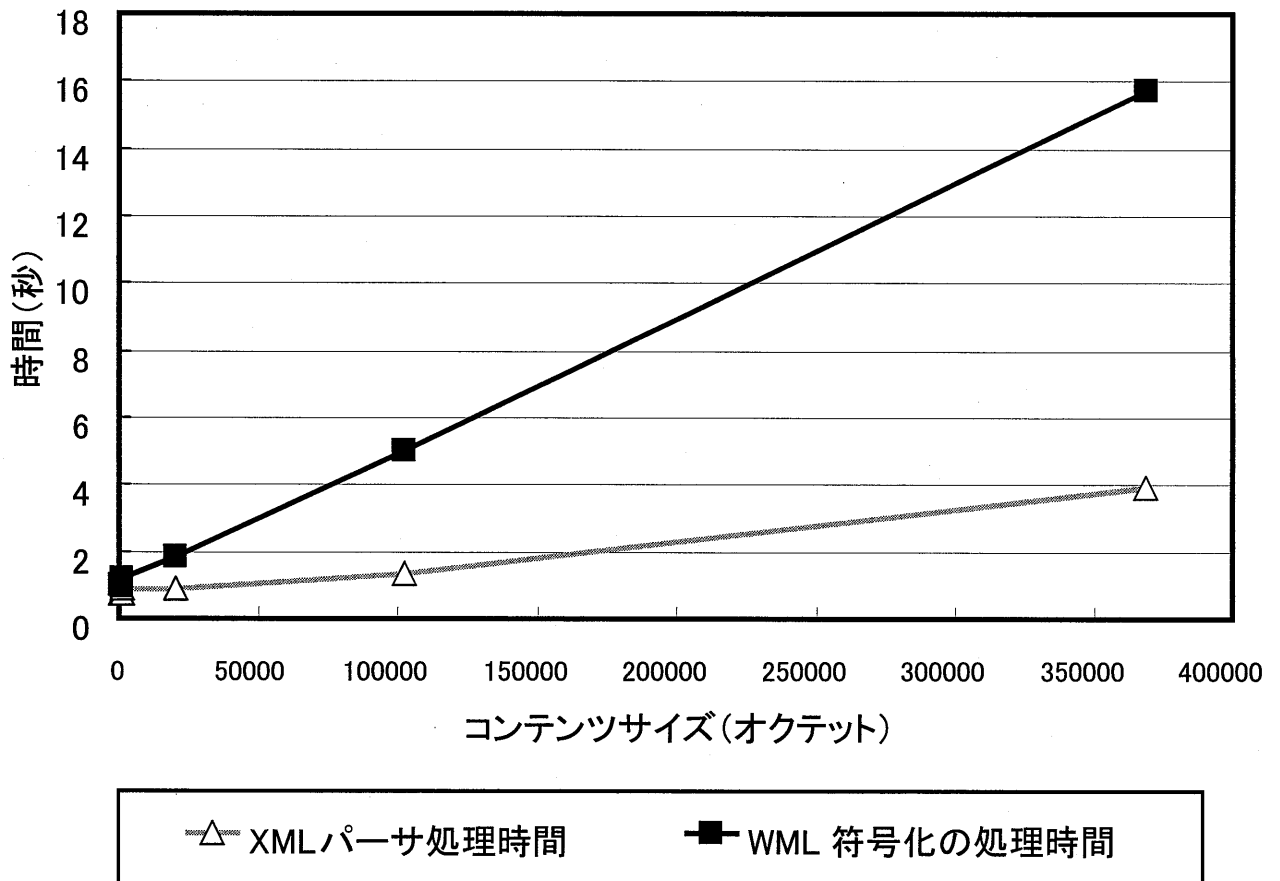


図 2-5 符号化の処理時間

図 2-5 に示す符号化の処理時間は、XML 構文解析及び WML バイナリ符号化の処理時間のいずれもコンテンツサイズにほぼ比例して増加している。ただし、コンテンツサイズが 500 オクテット及び 1000 オクテットの場合の WML エンコード処理時間はそれぞれ 1.00 秒、0.96 秒であり、コンテンツサイズにかかわらず約 1.00 秒要している。これは、コンテンツサイズが小さいときには、コンテンツの WML エンコード処理時間よりも、むしろ XML パーサの起動時間及び、バイナリ符号処理を起動するために必要な時間が全体の処理時間に深くかかわっているものといえる。また、WML バイナリ符号化処理全体のうち XML パーサの処理時間が占める割合は、500 バイトのコンテンツ時に 72.7%、386640 バイトのコンテンツ時に 24.9%であり、コンテンツサイズが大きくなるに従い低下している。つまり、コンテンツサイズが大きくなるに従い、XML パーサの処理時間よりもバイナリ符号化に多く時間を要することを示している。

以上の評価結果から、圧縮率と処理時間のいずれについても、コンテンツサ

イズが小さい場合において WML バイナリ符号化がより有効に機能することが分かる。また、WAP ゲートウェイで XML パース処理を行うことで、WAP クライアントでは WML のレンダリングのみを行えば良いという WAP アーキテクチャ特有のメリットも挙げられる。しかしその反面、WAP ゲートウェイで XML パース処理が必要となるため、加入者が増加した場合の WAP ゲートウェイのスケラビリティを確保することとのトレードオフになることに注意する必要がある。更に、コンテンツサイズが大きくなった場合、WML エンコードに要する処理時間がほぼ比例して増加するため、コンテンツサイズが大きい場合には、応答時間に大きな影響を与える可能性がある。

以下では、3G のような高速ネットワークに WML バイナリエンコーディングを適用した場合について述べる。1400 バイトのコンテンツをバイナリ化すると 1117 バイトに圧縮されるため 283 バイトの圧縮効果があるが、この 283 バイトを 384Kbps のネットワークで送信する際の伝送遅延は約 6 ミリ秒である。また、この 283 バイトを 9600bps のネットワークで送信する際の伝送遅延は 236ms である。本測定結果により、この 1400 バイトのコンテンツをエンコードするのに約 130 ミリ秒を要しているため、ネットワーク速度が 9600bps のように低速のネットワークの場合には、バイナリ化してネットワークの伝送速度を低くすることに対して効果が大きい。反面、3G のような高速のネットワークの場合、バイナリ化してコンテンツサイズを減少させるよりは、コンテンツをそのまま送信したほうが良いことが明らかになった。

また、本測定結果では、コンテンツサイズが大きくなるにつれ、WBXML によるエンコーディングの圧縮率が低下することを示した。IMT-2000 で提供されるアプリケーションのコンテンツサイズは相対的に大きくなることを考慮すると、WBXML によるバイナリ符号化は、効果的ではないことが確かめられ、一般的に用いられている gzip などのデータ圧縮方式の採用を考慮する必要がある。gzip を採用する際には、能力の低い移動機において実装が可能であるか、また可能であるとしてもその実装サイズが実現性のあるサイズであるかといった別の側面の考慮も重要であるが、本論文では、この点での考慮はしていない。この結果の位置付けとしては、gzip をコンテンツの圧縮方法として採用することが出来たと仮定した場合を述べており、この仮定の下では、gzip を採用することによる圧縮率の効果は高いことを示した。

2.4.2 WSP ヘッダのコンパクト符号化

WSP ヘッダのコンパクト符号化については、WSP で規定されているデフォルトのヘッダコードページを用いた。測定に用いた WAP テストベッドシステムでは、WSP CONNECT メソッドのヘッダ圧縮の処理時間として約 10 ミリ秒程度の時間を要し、185 バイトから 50 バイトに 135 バイト圧縮された。もし、ネットワークの速度が高速である場合には、この圧縮は効果が無いものになる。例えば、ネットワーク速度が 384kbps である場合の 135 バイトデータの伝送遅延は約 3 ミリ秒であり、ヘッダ圧縮を行わずにそのままデータ転送を行った方が全体の転送時間という点においては効率が良いことになる。しかし、もしネットワーク速度が 9600bps である場合には、その伝送遅延は約 112 ミリ秒であり、その場合には WSP ヘッダ圧縮を行ったほうが全体の転送時間という点においては効率が良いことになる。

以上のことから、WSP ヘッダコンパクト符号化は、ヘッダサイズを減少させるためには役に立つが、IMT-2000 などの高速ネットワークにおいては、全体の転送時間という点に着目すると必ずしもその効果が高いとはいえないことを示した。

2.5. WAP プロトコルの性能評価

2.2 章で述べたように WAP は通信プロトコルからコンテンツ記述言語まで幅広い仕様を規定しているため、システム全体として見たスループットを理論的に定量評価することは難しい。そこで、WAP プロトコルと同じ機能を提供するインターネットプロトコルである HTTP/TCP との比較によって、WAP プロトコルの性能評価を試みた。評価実験では、無線ネットワークに IMT-2000 (W-CDMA) を用いることを想定して無線シミュレータを介在させた擬似無線環境を構築し、WAP プロトコルと HTTP/TCP に関して、リクエスト送信開始からレスポンス受信終了までの時間（以下、応答時間と呼ぶ）を測定し、比較評価を行った。

2.5.1 WAP プロトコルと TCP の機能比較

WAP プロトコルと TCP について、トランスポート層相当の機能比較を表 2-1 に示す。TCP のコネクションは WAP における WSP のセッションが同等の機能を提供するものと考えられる。

表 2-1 WAP プロトコルと TCP の機能比較

項目	WAP プロトコル	TCP
コネクション (セッション) 確立手順	コネクトとコネクトリ プライによる WSP セ ッション確立	3ウェイハンドシェ ークによるコネクシ ョン確立
順序制御	WTP のパケット シーケンス番号	TCP のパケット シーケンス番号
フロー制御	WTP の最大グループ サイズ	ウィンドウサイズ の更新
再送制御	WTP の選択式再送	Go -Back - N方式、 早期再送・早期回復 方式
誤り検出	ベアラ依存	チェックサム

TCP はコネクション型のストリーム転送を提供するが、WAP は WSP のセッション管理のもと、非同期的に要求可能なトランザクション型のメッセージ転送を提供する。TCP のコネクション確立シーケンスは 3 ウェイハンドシェイクの手順に従うが、WAP では WSP のコネクトメッセージとその応答でセッションを確立する。また、WAP プロトコルの特徴として、非同期的なトランザクション要求が可能であるため、コネクトメッセージの応答を待たずにリクエストメッセージを送信可能である。これによって、WAP プロトコルではセッション確立手順のための遅延時間を短縮することができる。TCP ではセグメントの順序制御を行うが、WAP では WTP におけるパケットシーケンス番号を用いて順序制御を行う。TCP ではフロー制御は受信側から受信可能なウィンドウサイズを通知、更新することによって実現している。一方 WAP は画面の小さなモバイル端末を主な対象として開発されたプロトコルであり、シングルパケットの転送が標準でサポートさ

れている。これは、例えばネットワークにイーサネットを用いる場合には、最大転送サイズ (MTU サイズ) が 1500 バイトであることを意味する。その場合にはフロー制御のための特別な手順は必要としない。次世代のモバイルインターネットサービスとして、動画や音楽の配信を想定した場合には、数 10 k ~ 数 100 k バイトの大容量データ転送のニーズが想定される。WAP プロトコルにおいて大容量データ転送をサポートするために、データの分割・再組み立て機能 (SAR: Segmentation And Reassembly) が、WTP のオプション機能として規定されている。SAR の通信パラメタの 1 つである最大グループサイズを用いてフロー制御を行うことができる。最大グループサイズは WAP ゲートウェイが WAP クライアントから ACK を待たずに連続的に送信できるパケット数である。これを用いてパケットの流量を制限できる。ただし、この値は通信開始時に WAP ゲートウェイから WAP クライアントへ通知されて決まり、通信中に動的に変えることはできないので、TCP のウィンドウ制御のような柔軟性はない。TCP の再送制御は、Go-BACK-N 方式を基本に早期再送・早期回復方式 (Fast Retransmit/Fast Recovery) を加えたものであるが、WAP では WTP におけるパケットシーケンス番号を用いて欠落パケットを検出し、欠落パケットのみを再送する選択式再送機能を規定している。本機能は、WAP クライアントがパケット受信の ACK を返す時に正しく受信できなかったパケット番号を NACK (Negative ACK) として通知することにより実現している。誤り検出は TCP ではヘッダにチェックサムがありその結果により再送制御を行うが、WAP では WDP のヘッダチェックサムを用いて誤りを検出し、それを WTP 層に通知して再送制御を行う。

2.5.2 WAP プロトコルと HTTP/TCP の性能評価

本節では、図 2-1 に示す WAP テストベッドシステムを用いて WAP プロトコルと HTTP/TCP の性能評価を行った結果を示す。HTTP/TCP については、図 2-1 における WAP1.1 のプロトコル部分を、HTTP/TCP に置き換えて実験した。つまり、HTTP/TCP を WAP クライアントと WAP ゲートウェイに実装したことになる。なお、本実験中で用いた TCP は、IETF で標準化されている無線向け TCP [21] を採用している。本実験では、初期ウィンドウサイズ拡張 [22] により初期ウィンドウサイズを 2 セグメントとし、受信側バッファサイズにはネットワークの帯域遅延積に基づいて 32K バイトを採用し、さらに SACK (Selective Acknowledgement) 機能 [23] を用いている。なお、WAP では、TCP と同様に最大グループサイズを

32K バイトとしている。

性能評価で用いた無線シミュレータの各パラメタの値を表 2-2 示す。無線シミュレータは、ベアラのエラー率、遅延などの各種パラメタの値の設定が可能である(4.5.1.2 節参照)。本研究では、ベアラに W-CDMA を用いることを想定しており、本性能評価における各パラメタの値は、FOMA サービスで用いたネットワークで得られる値に基づいて設定した。ここで説明しているベアラのエラー率は、W-CDMA の 1 FEC フレームごとのエラー率を示している。つまりこのエラー率は、無線通信時のフェージング現象等により発生したビット誤りを、FEC フレームごとにエラー訂正を行い、その結果エラー訂正が行えなかった FEC フレームの比率を示している。したがって、ビットのバースト的な誤りが発生し、その誤り率が高い場合には、FEC により誤り訂正が行えず、フレームのエラーとして上位層に通知されることになる。我々は、このエラー率を、FOMA サービスで用いたネットワークの測定を基に導き出した値を採用した。WAP クライアントから WAP ゲートウェイまでのラウンドトリップ時間 (RTT : Round Trip Time) は 350 ミリ秒~400 ミリ秒程度であった。

表 2-2 無線シミュレータのパラメータ

パラメタ	値
ベアラ速度(上り)	64 Kbps
ベアラ速度(下り)	384Kbps, 64Kbps
エラー率	5% (FECフレーム毎)
レイヤ 2	RLCプロトコル [24]
ベアラ MTU	1500 バイト

本測定では、3 種類 (1K, 10K, 100K バイト) のサイズのコンテンツを用意した。1K バイトのコンテンツは、HTML などのテキストデータのブラウジングを想定しており、WAP 及び HTTP/TCP では、1 パケットに収まるデータサイズ (MTU=1500 バイトの場合) である。また、100K バイトのコンテンツは、W-CDMA などの高速無線ネットワーク上での、MPEG4 データ、Java データなどのダウンロードを想

定しており、WAP においては WTP の分割再組み立て (以下 SAR : Segmentation and Reassembly とする) 機能を用いることにより 1 パケットのサイズを越えるデータの転送が可能となる。

表 2-2 に示すパラメタを基に測定を行った結果を図 2-6 に示す。なお、図 2-6 は縦軸が対数スケールになっている。図 2-5 に示すように IMT-2000 などの高速ネットワークでは、当初考えられた無線ネットワークにおける TCP の性能低下は見られず、WAP と HTTP/TCP はほぼ同じ性能が得られる。また、100K バイトデータ送信時に、ベアラ速度 384Kbps で約 160Kbps、64Kbps で約 50Kbps のスループットが得られている。

WAP1.x と HTTP/TCP の比較

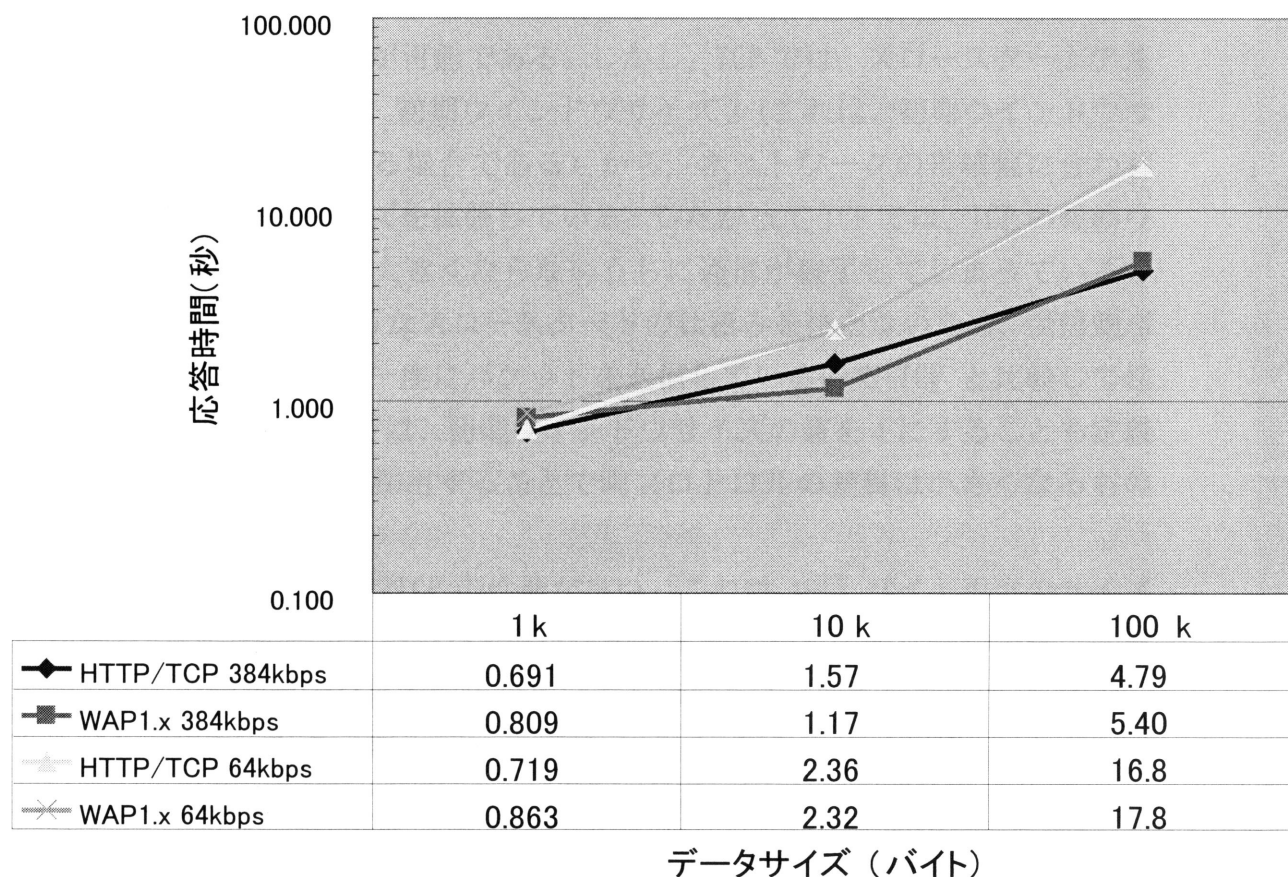


図 2-6 WAP1.x と HTTP/TCP の応答時間の比較

2.5.3 評価結果の考察

WAP と HTTP/TCP のトランスポート特性を比較し、図 2-5 の測定結果について考察する。

1K バイトでは HTTP/TCP の性能がよい。1 K バイトは 1 パケットに収まるデータサイズであるので、TCP のスロースタートなどのウィンドウ制御が性能に影響しないことが原因である。WAP の性能低下の原因は、WAP ゲートウェイにおけるプロトコル変換のオーバーヘッドであると考えられる。しかしこの差は無視できる位に小さいため、プロトコル変換のオーバーヘッドは実質無視できる範囲である。

10K バイトでは WAP の性能がよい。これは、両プロトコルのフロー制御アルゴリズムの違いが原因となっている。WTP では 10K バイトの転送に 7 パケットを必要とするが、WAP ゲートウェイは、最大グループサイズの範囲内でその 7 パケットを一度に送信することが可能である。しかし、TCP では、スロースタートアルゴリズムを採用するため、初期ウィンドウサイズ 2（これは、初期ウィンドウサイズ拡張が採用されている場合である）から、ネットワークの帯域幅に合わせて徐々にウィンドウサイズを拡張している。したがって TCP では、TCP の輻輳ウィンドウサイズが十分に大きくならないうちに通信が終了してしまっているのに対し、WAP は TCP のようなスロースタートの仕組みを持たないため、受信側バッファサイズの範囲内で一度にパケットを送信しているため TCP と比較して性能がよい。しかし、TCP では、初期ウィンドウサイズの値を 4 にすることも定義されており [25]、これを採用することで両プロトコルの差異は小さくなるものと予想できる。

100K バイトでは、HTTP/TCP の性能が良い。これは 100K バイト程度のサイズになると、TCP の輻輳ウィンドウサイズ十分に大きくなってから通信が終了するので、TCP の性能が十分に引き出せているためである。WTP の性能が HTTP/TCP と比較して低かったその理由として、WTP のフロー制御方式が原因となっていることが考えられる。TCP では、ピギーバック方式によりデータの受信中に必要に応じて ACK を返信しているのに対し、WTP では、最大グループサイズに基づいてパケットを一度に送信したあと、ACK が返信されてくる間に待ち時間が生じるためである。この待ち時間は無線ネットワークのような遅延の大きいネットワークの場合、性能低下の原因となる。この様子を図 2-7 に示す。

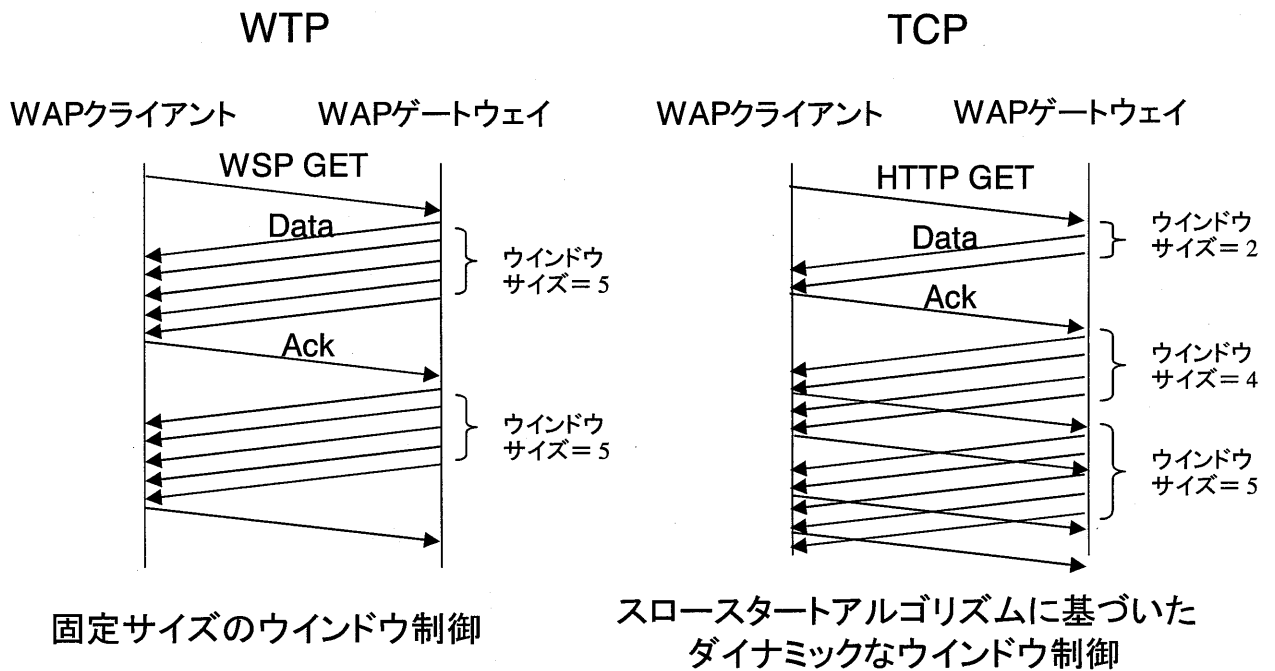


図 2-7 WTP と TCP のフロー制御方式の比較 (概略)

2.5.2 節で述べたように、本測定では、FOMA サービスで用いられたネットワークから得られたネットワーク特性を測定のパラメタとして用いている。このことと以上の測定結果から、FOMA 等の高速無線ネットワークにおいては、インターネットで用いられているプロトコルを基本として、無線向け TCP のように無線ネットワークの特性に合わせて最適化したトランスポートプロトコルを採用することにより、WAP1.x と同等か場合によってはそれ以上の性能が得られることが確認できた。その理由として、WAP1.x は、フロー制御のウィンドウサイズを動的に変化させる機能を持ち合わせていないなど、本来低速なネットワーク向けに設計されたプロトコルであり、それに対して TCP は、ウィンドウサイズを動的に変化することが出来るフロー制御機能と輻輳制御機能を備えているため、高速ネットワークへの柔軟な対応が可能である。

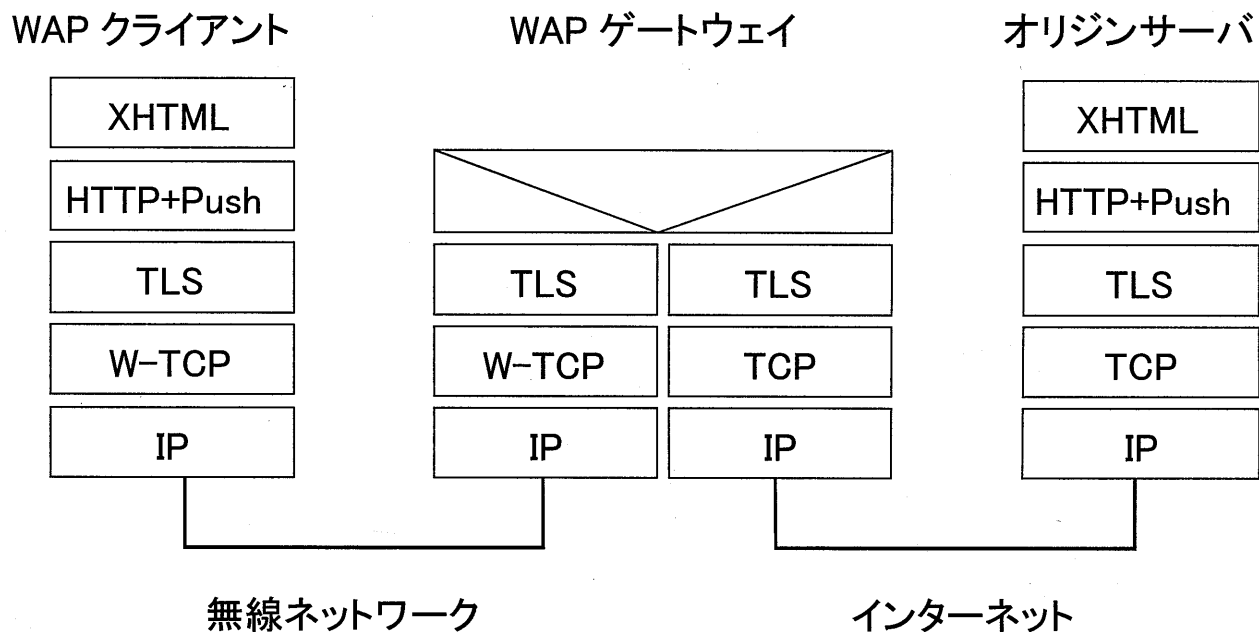
2.6 次世代モバイルインターネットアーキテクチャの提案

2.4 章及び 2.5 章で考察したように、WAP1.1 は低速ネットワークで小さなコンテンツを配信する場合には有効であるが、より大きなコンテンツを配信することが予想される IMT-2000 などの高速ネットワークでは、HTTP/TCP でも十分な性能を得ることができる。WAP1.1 プロトコルに機能面、性能面で明らかな優位

性が無い限り，インターネットのセグメント化を避けるためにも，移動通信ネットワークにおいても標準的なインターネットプロトコルを採用すべきである。これらの考察に基づいて，IMT-2000 に代表される高速移動通信ネットワークに適した次世代モバイルインターネットアーキテクチャを提案する [26]。

提案するアーキテクチャは，TCP，TLS，HTTP，Push，XHTML から構成される (図 2-7)。TCP は 5 章で述べた無線ネットワークに最適化された TCP [21] (W-TCP) である。トランスポート層セキュリティとして TLS を採用することにより，WAP 1.1 では完全には実現できなかったエンド・エンドセキュリティが可能となる。プッシュはモバイル環境で有効な機能であるため，WSP のプッシュ機能と同等の機能を HTTP 上で実現する [27]。この場合，WAP ゲートウェイが HTTP のクライアントとなり，WAP クライアントが HTTP サーバとして動作する。WAP ゲートウェイとオリジンサーバの間は既に WAP フォーラムで規定している PAP (Push Access Protocol) を使用する。マークアップ言語としては，次世代の標準マークアップ言語である XHTML [28] を提案する。XHTML を採用することにより，XHTML のモジュール化機能を利用したモバイル端末向けのサブセット定義，XML の拡張性を利用した機能拡張などが可能となる。

我々は本アーキテクチャを WAP フォーラムに提案し，次世代 WAP (WAP 2.0) として採用された。本アーキテクチャは次世代モバイルインターネットの標準的なアーキテクチャとなることが期待されている。



W-TCP: Wireless Optimized TCP

図 2-8 次世代モバイルインターネットアーキテクチャの提案

2.7 おわりに

IMT-2000 (W-CDMA) の無線環境を疑似する無線シミュレータを利用して、WAP プロトコルとインターネットプロトコル (HTTP/TCP) の性能を測定し、比較評価を行った。その結果、両プロトコルはほぼ同等の性能を持つが、IMT-2000 などの高速移動通信ネットワークで想定されるマルチメディアなどの大容量コンテンツを配信する場合、HTTP/TCP などのインターネットプロトコルを適用することが可能である。

本評価結果に基づいて、IMT-2000 に代表される高速移動通信ネットワークに適した次世代モバイルインターネットアーキテクチャを提案した。本提案は、WAP フォーラムで次世代 WAP (WAP 2.0) として採用され、次世代モバイルインターネットの標準的なアーキテクチャとなることが期待されている。

今後は、第 4 世代移動通信ネットワークなどのより高速な無線ネットワークを対象としたインターネットプロトコル (TCP など) の最適化、WAP プッシュなどを応用した新しいモバイルインターネット向けアプリケーションなどについて研究を進める予定である。

3. 移動機向けプッシュプロトコルの提案と評価

3.1 はじめに

WAP (Wireless Application Protocol) [29] では, WAP version 1.1 (WAP1.1) からプッシュ機能が提供され, このプッシュ機能を用いた製品やサービスが市場に提供され始めている. しかし WAP version 1.x (WAP1.x) は, 低速, 高遅延といった特徴を持つ第 1 世代 (1G), 第 2 世代 (2G) の移動通信ネットワークを対象に検討されたものであり, IMT-2000 等の第 3 世代 (3G) の高速な移動通信ネットワークには必ずしも適しているとはいえない. 現在 3G の移動通信ネットワークに適したプロトコルの研究や開発が行なわれており, インターネット で用いられているプロトコル (HTTP, TCP 等) をそのまま用い, そのサブセットの定義や必要な機能の拡張を行うことにより無線への最適化が図られている [30]-[32]. これによって, インターネット上のアプリケーションと親和性の高いシームレスなサービスを提供することが可能となる. しかし, プッシュプロトコルについては, インターネットにおいて標準化されたものが存在しないため, 新たに提案する必要がある.

本章では, IMT-2000 等の 3G 移動通信ネットワーク向けプッシュ機能の実現を目的とし, インターネット で用いられているプロトコルを用いてプッシュ機能を実現する方式を提案する. 提案方式では, 無線向け TCP プロファイル [32] と HTTP [33] を用い, WAP1.x と同様なオリジンサーバ起動型のプッシュ機能を実現する. さらに, HTTP の機能の中からプッシュ機能を実現するために必要な部分をサブセット化すると共に, 必要な機能を追加してプッシュ機能を実現する. また, 次世代のマークアップ言語として有力な XHTML (Extensible HTML) 1.0 [34] と XSLT (Extensible Stylesheet Language Transformations) [35] に着目し, それと提案したプッシュ機能を組合せた新しい差分プッシュ方式を提案する. 本提案は, オリジンサーバ側で古いデータと更新後の新しいデータとの差分を自動的に生成し, 移動機にプッシュするものである. これによって移動機は, 常にアップデートされた最新のデータを表示可能となり, ネットワーク上でのチャット画面の自動更新や, 株式情報チャートの自動更新等のサービスへ応用することが可能になる. なお, XHTML 1.0 は, HTML4.01 [36] を XML (extensible Markup Language) [37] に基づいて再定義したものであり, HTML4.01 の後継となるマークアップ言語として W3C (World Wide Web Consortium) で標準化されたものである.

XSLT は、XML データの自動変換機能を提供するものであり、同じく W3C にて標準化されたものである。

最後に、提案方式に基づいて実装したテストベッドシステムを紹介し、提案方式の有効性について検証した結果について述べる。

3.2 プッシュプロトコルの提案

3.2.1. WAP1. x プッシュ

WAP1. x では、インターネット上のホストから移動機へのプッシュ機能を提供するために、移動通信向けのプッシュアーキテクチャを規定している。図 3-1 に WAP1. x のプッシュアーキテクチャを示す [38]。WAP1. x のプッシュアーキテクチャでは、プッシュメッセージの送信ホストである PI (Push Initiator)、メッセージプッシュのプロキシ機能及び移動機のアドレス解決等を行う PPG (Push Proxy Gateway) [39]、及び移動機から構成される。

図 3-2 に WAP1. x で用いられるプッシュプロトコルの構成を示す。PI と PPG 間のインターネット部では、PAP (Push Access Protocol) [40] が用いられ、その運搬用に HTTP の POST メソッドが用いられる。PAP は、XML により記述されるプロトコルであり、メッセージのプッシュ、結果通知、状態問合せ等の機能を持つ。PPG と移動機間の移動通信ネットワーク区間では、トランスポートとして WDP (Wireless Datagram Protocol) [41]、プッシュプロトコルとして、WSP (Wireless Session Protocol) [42] を用い、その上で動作するプッシュ用のアプリケーションレベルのプロトコルを Push OTA (Over the Air) [43] と呼ぶ。Push OTA は、PPG から移動機へのデータのプッシュ機能の実現や、移動機アプリケーションのアドレッシング、及び各種制御情報の交換等の機能を提供する。なお、Push OTA では、コネクション型プッシュとコネクションレス型プッシュの 2 種類のプッシュ機能が提供され、プッシュするデータに求められる信頼度等の性質を基に、両者を使い分けることができる。

のみ更新データを受信するプッシュの形態があり [44], スマートプルと呼ばれる。スマートプルは, HTTP 等のプル型のプロトコルを使用して擬似的にプッシュ機能を実現する。しかし, スマートプルの欠点として, 1) データが更新されていない場合にも, 不必要なデータ更新問合せが発生する, 2) データが更新されたとしても, クライアントからのデータ更新問合せがあるまでは, クライアントにデータ提供が不可能であるため, 更新されたデータを即時的に提供出来ない場合がある, 等の問題点がある。携帯電話等による E-mail の例にあげられるように, 移動機向けプッシュ機能では, スマートプル方式ではなく, WAP1.x プッシュのようなオリジンサーバ起動型のプッシュ方式を利用し, 移動機に対して即時的なデータ提供が出来るようにする必要性が高い。これまでの研究では, 3G 移動通信ネットワークを対象としたサーバ起動型のプッシュプロトコルに関する研究や, 3G 移動通信ネットワークにおける WAP1.x プッシュプロトコルの性能を明らかにした研究は存在しない。

プッシュ機能を提供する場合, クライアントが増えた場合のスケーラビリティが問題となる。特に大量のクライアントに対して同時にプッシュするときのプッシュセッションを同時に確立するかシーケンシャルに確立するかなどの方式が考えられる。また, 複数クライアントへ同時配信を実現する等の方法としてマルチキャスト [45], [46] を採用し, 配信サーバのスケーラビリティを高める方法が存在する。

3.2.3 プッシュアーキテクチャ

提案するアーキテクチャは, WAP1.x のプッシュアーキテクチャ (図 3-1) に基づき, 移動機, PPG, および PI からなり, 以下のプロトコル構成とする (図 3-3)。移動機と PPG 間には, 3G 移動通信ネットワークの高速性の特徴を有効利用する新しいプロトコルを採用する。すなわち, 移動通信ネットワーク部分におけるトランスポートプロトコルとして現在 IETF で議論されている無線向け TCP プロファイルと, その上に HTTP1.1 の POST メソッドを用いる。プッシュ型配信では, インターネット上の PI から PPG を経由して移動機へのオリジンサーバ起動型のプッシュ機能を実現するため, PPG が HTTP のクライアントとして動作し, 移動機が HTTP のサーバの機能を提供する。移動機は, CPU 能力や搭載可能なメモリの制限があるため, プッシュ機能の実現に必要な HTTP 機能のみを抽出し, サブセット化するとともに, 必要な機能を拡張ヘッダとして新たに定義

する。このプッシュ機能を持つ HTTP のことをプッシュ向け HTTP プロファイルと呼び、3.2.4 節にて詳細を説明する。なお、インターネット側では、既存方式をそのまま用いる。すなわち、PI 上のアプリケーション、及び PAP の変更を行う必要が無く、既に WAP1.x 移動機向けにサービスを開始している PI については、そのまま提案方式を実装した移動機に対してもサービス提供を可能とする。

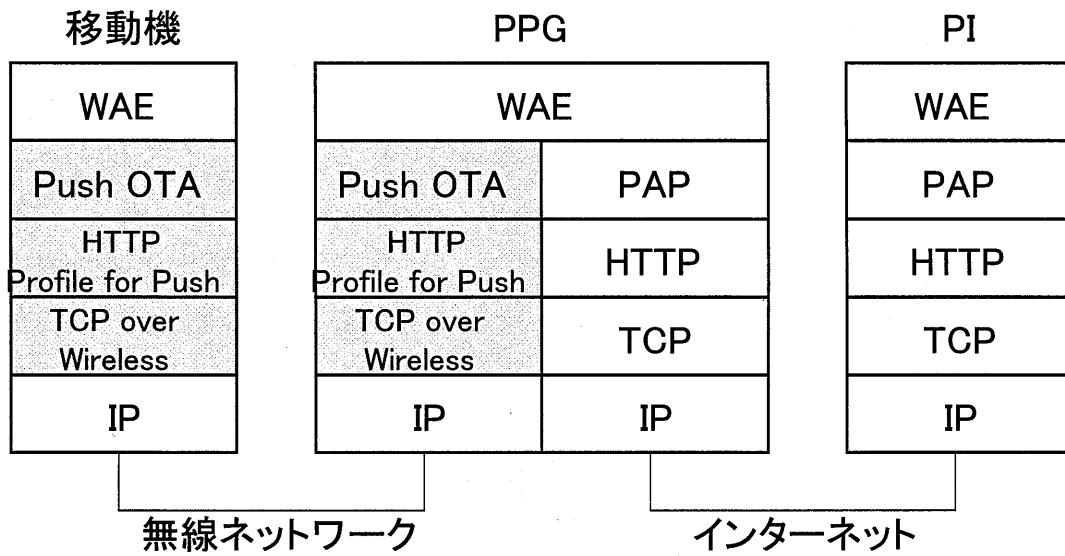


図3-3 提案プッシュプロトコル

3.2.4 プッシュ向け HTTP プロファイル

プッシュ向け HTTP プロファイルでは、HTTP の必須項目のうちプッシュ機能を提供する上で必要としないものについてはサポートをオプションとし、HTTP のオプション項目のうち必要な機能についてはサポートを必須と定義する。以下では、プッシュ向け HTTP プロファイルについて説明する。

(a) メソッド：HTTP メソッドには、HTTP POST を用い、他のメソッドのサポートはオプションとする。HTTP では、GET と HEAD メソッドが必須項目であるが、プッシュ機能の実現に必須でないためサポートをオプションとする。

(b) HTTP ヘッダ：HTTP ヘッダとして、Host, Content-Length, Content-Type に加え、Connection ヘッダのサポートを必須とする。Connection ヘッダは、TCP コネクションの持続的接続（パーシステントコネクション）を制御するために用いる。パーシステントコネクションは、連続するプッシュで同じ TCP コネクションを再利用できるようにしたものであり、TCP コネクションの開設フェーズ、

切断フェーズを省略することができるため、通信コストが高い移動通信ネットワークにおいては有効である。

(c) 拡張ヘッダ：WAP1.x の Push OTA で提供する機能を実現するため、以下に示す新たな Push OTA プロトコル用ヘッダを定義する。ここで定義する拡張ヘッダは、http のシンタックスに従って記述され、HTTP ヘッダ部に追加される。

(ア) X-Wap-Application-Id: 移動機に複数実装されたアプリケーションを識別し、プッシュプロトコルがデータを渡すアプリケーションを選択する。

(イ) X-Wap-Client-Id: 移動機を識別する ID を PPG と移動機間で共有することにより、セッション管理等を実現する。

(ウ) X-Wap-Push-Flag: WAP1.x Push OTA 仕様と同様に、データや PI の各種情報を定義する。

(エ) X-Wap-Push-Id: 複数のプッシュを識別するための ID を設定する。

3.2.5 提案方式のプッシュ通信例

提案プッシュ方式用いたプッシュ通信例を図 3-4 に示す。まず PI は、PPG に対して PAP の push-message メッセージを用いてデータをプッシュし(図 3-4 の①)、それを受け取った PPG は、PI に対して PAP の push-response メッセージを返す(図 3-4 の②)。PPG は、push-message メッセージを受け取ると、移動機に対して無線向け TCP のコネクションを開設し、プッシュ向け HTTP プロファイルによって、移動機へとプッシュを実行する(図 3-4 の③)。その後、データを受け取った移動機は、PPG に対してレスポンスを返す(図 3-4 の④)。なお PI は、プッシュが正しく実行されたか確認することができ、もし PI が、図 3-4 の①で確認応答を要求した場合には、PPG は、resultnotification-message を PI に返す(図 3-4 の⑤)。

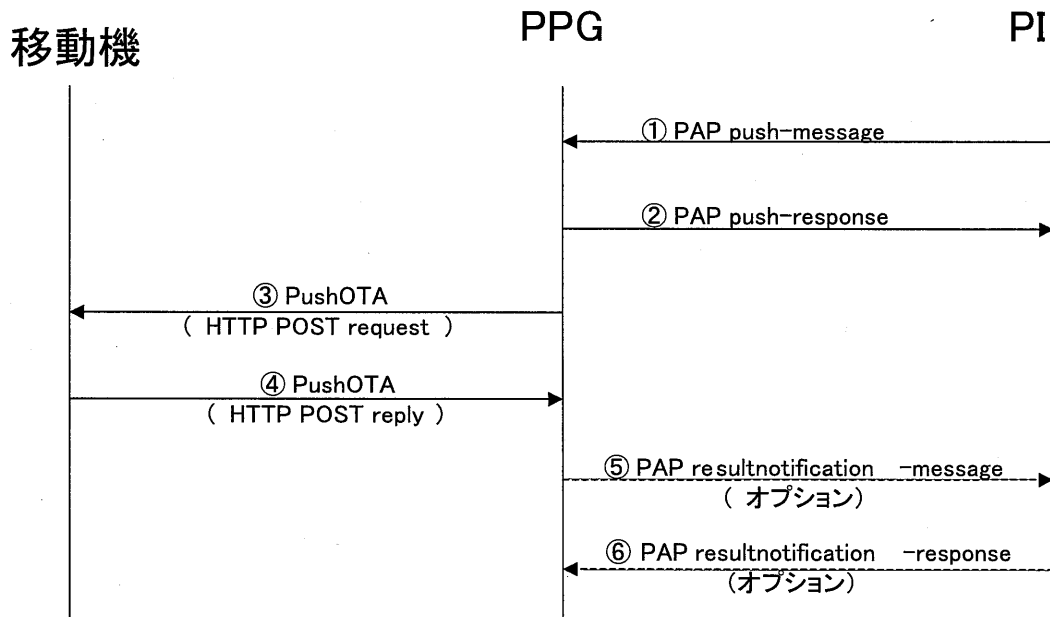


図 3-4 提案方式の通信例

3.3 プッシュプロトコルの性能評価

3.3.1 性能評価

IMT-2000 ネットワークを想定したシミュレーション環境において、提案方式と WAP1.x との比較によって、提案方式の特性把握を行う。本研究では、WAP1.x のうち最初にプッシュ機能が提供された WAP1.1 を選択し、WAP1.1 と提案方式のテストベッドを試作し、PPG から移動機へのプッシュに関して、WAP1.1 プッシュプロトコルと提案方式のリクエスト、レスポンスに要する時間（以下応答時間とする）の測定を行った。なお、ベアラに W-CDMA (Wideband CDMA) を用いることを想定するため、無線環境を擬似する W-CDMA シミュレータ (4.5.1.2 節参照) を移動機と PPG の間に介在させた。図 3-5、および表 3-1 に性能測定環境を示す。表 3-1 に示すように、本測定では、レイヤ 2 のプロトコルとして RLC (Radio Link Control) プロトコル [24] を使用し、ベアラ MTU (Maximum Transfer Unit) サイズを 1500 バイトとした。これらの各パラメタの値は、FOMA サービスで使用されているパラメタ値に基づいて設定してある。表 3-1 のエラー率は、W-CDMA の 1 FEC (Forward Error Correction) フレームごとのエラー率を示しており、無線通信で発生したビットエラーを、FEC フレームごとにエラー訂正を行い、その結果エラー訂正が行えなかった FEC フレーム数の平均比率を示している。なお、

FECにより誤り訂正が行えない場合には、フレームのエラーとして上位層に通知され RLC プロトコル [24] にて再送制御が行われる。本論文では、このエラー率を、FOMA サービスで用いたネットワークの測定を基に導き出した標準的な値を採用している。上記の環境で、移動機（エミュレータ）から、PPG までのラウンドトリップ時間（RTT: Round Trip Time）は 350 ミリ秒～400 ミリ秒程度であった。

本測定では、3 種類（500, 10K, 100K バイト）のサイズのデータを用意した。500 バイトのデータは、XHTML 等のテキストデータのプッシュを想定しており、TCP における最大セグメント長（MSS: Maximum Segment Size）や WAP1.1 の 1 パケットに収まる最大のデータサイズに収まる。また、100K バイトのデータは、i-mode サービス等における、MPEG4 データや Java データのプッシュを想定しており、WAP1.1 においては WTP (Wireless Transaction Protocol) の分割再組み立て（以下 SAR: Segmentation and Reassembly とする）機能 [20] を用いることにより、WAP1.1 の 1 パケットに収まる最大のデータサイズを越えるデータの転送が可能となる。この SAR 機能は、WAP1.1 において本来オプションであるが本テストベッドシステムでは実装を行っている。

なお、今回行った評価では、図 3-5 に示す OS（PPG=Solaris2.6, 移動機=Windows98SE）に実装されている TCP とその初期設定値をそのまま用いており、無線向け TCP プロファイルに準拠していない。

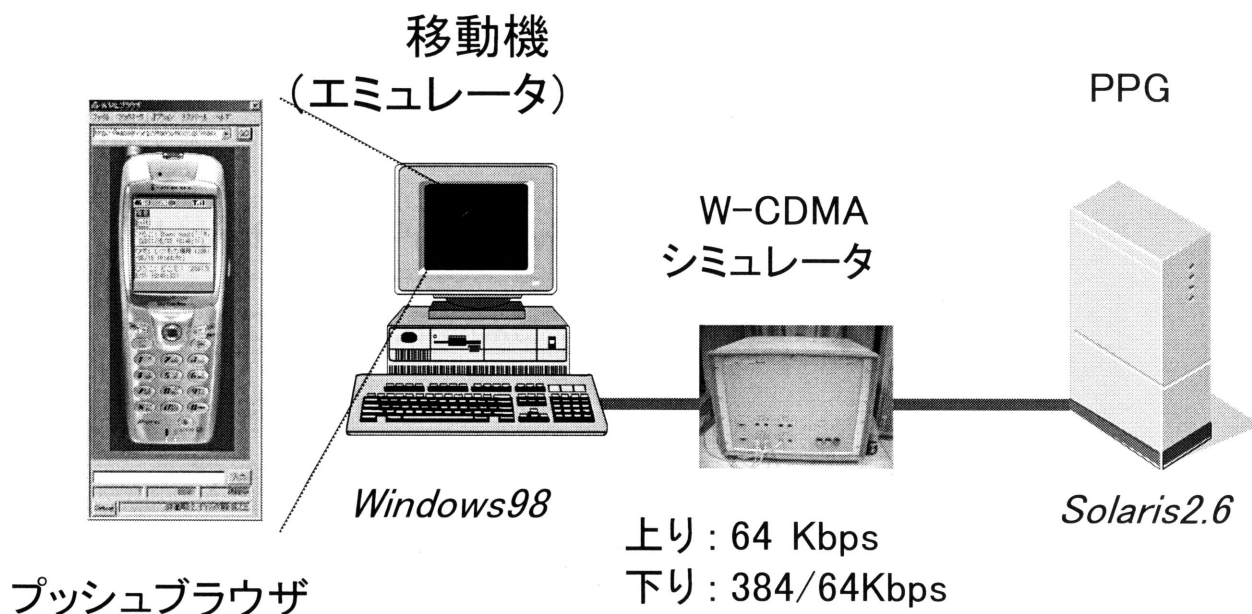


図 3-5 性能測定環境

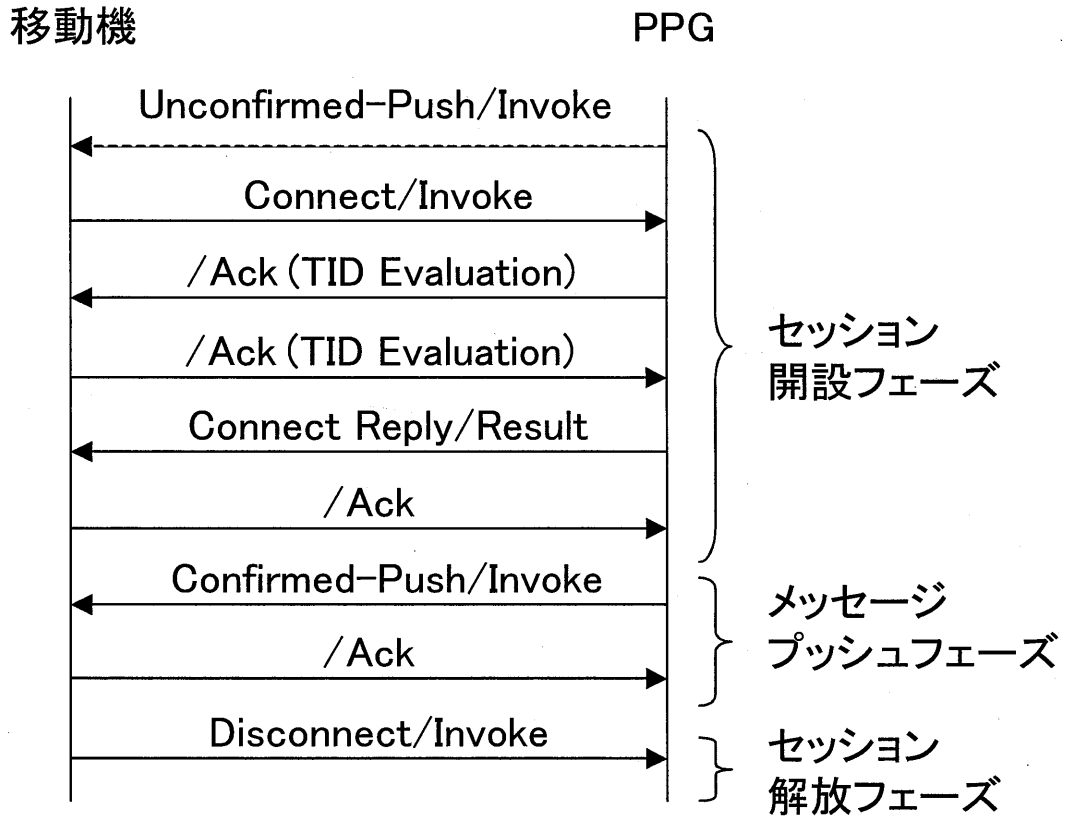
表 3-1 W-CDMA シミュレータパラメータ

パラメタ	値
ベアラ速度(上り)	64 Kbps
ベアラ速度(下り)	384Kbps, 64Kbps
エラー率	5% (FECフレーム毎)
レイヤ 2	RLCプロトコル [24]
ベアラ MTU	1500 バイト

3.3.2 通信シーケンスの比較

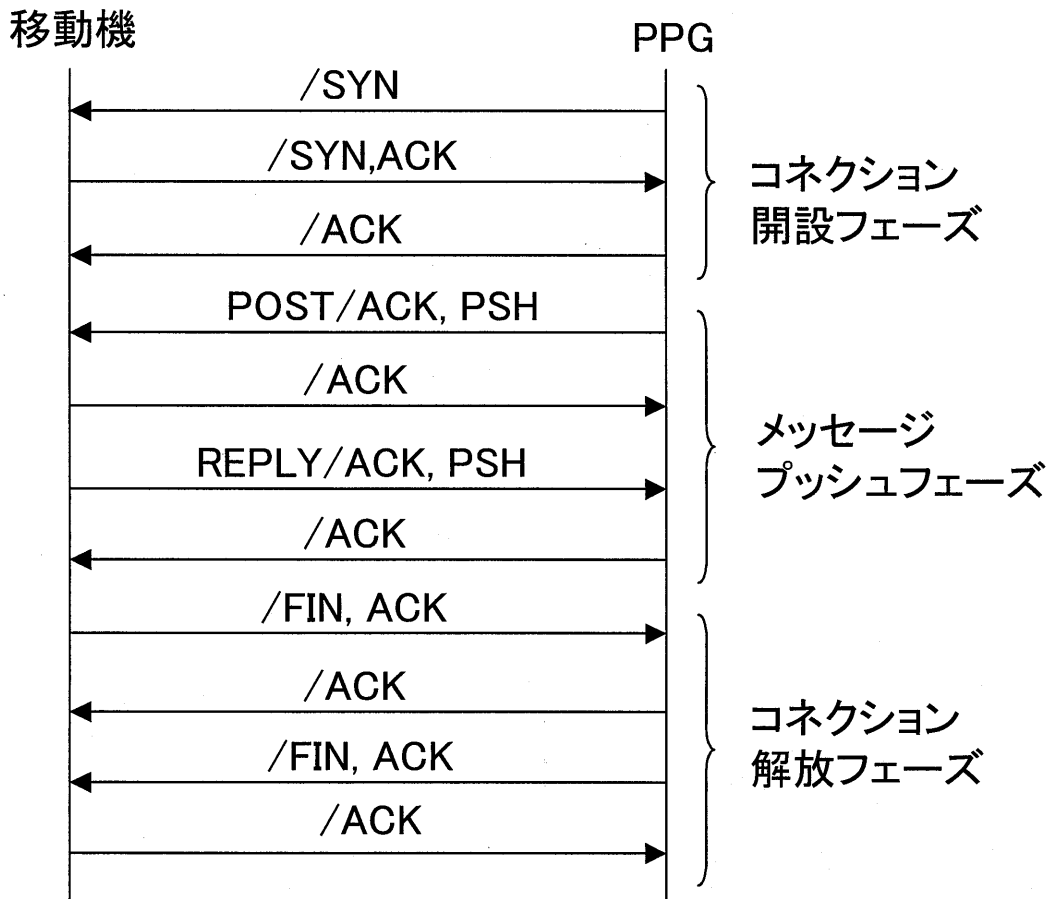
PPG と移動機間におけるコネクション型プッシュの WAP1.1 の通信手順を図 3-6 に、提案方式の通信手順を図 3-7 に示す。いずれの方式も、1) WSP セッション/TCP コネクション開設フェーズ (以下開設フェーズとする)、2) プッシュ実行フェーズ、3) WSP セッション/TCP コネクション切断フェーズ、から構成される。なおプッシュを連続して行う場合には、WSP セッションの共用、または HTTP1.1

のパーシステントコネクションを用いることにより、新たな開設フェーズは必ずしも必要無い。



(左)/(右)=(WSP メソッド)/(WTP トランザクションタイプ)

図 3-6 WAP1.1 の通信シーケンス



(左)/(右)=(HTTP メソッド)/(TCPフラグ)

図 3-7 提案方式の通信シーケンス

3.3.3 開設フェーズ

図 3-8 に開設フェーズに要する時間の測定結果を示す。提案方式は、WAP1.1 よりも開設フェーズに要する時間が短い。この理由は WSP セッション開設に要するシーケンス数 (=本測定結果では 5 シーケンス) が TCP コネクション開設に要するシーケンス数 (=本測定結果では 3 シーケンス) よりも多いことが考えられる。また、ベアラの下り速度が 64Kbps から 384Kbps と高速になっても、それぞれに要する時間を比べるとそれほど向上しないことが分かる。これは、開設フェーズで用いられるパケットはヘッダのみで構成されており、そのサイズは大きくないことが原因と考えられる。すなわち、ベアラが高速になってもパケットサイズが大きくないため、それが開設フェーズの時間短縮にはつながらず、むしろ

るネットワーク遅延等が開設フェーズに要する時間に影響していることを示している。なお、WSPセッションは移動機のみ開設することが可能であるため、図 3-6 の破線で示す unconfirmed-Push (非確認型プッシュ) を行うことにより、移動機のセッション起動を要求することが可能である。図 3-5 に示す本測定環境では、移動機が受信可能状態に入る際 (移動機の電源を ON にする等) に、WSPセッションを開設し、PPG と移動機間でそれを保持するという状況を想定しているため、図 3-8 に示す開設フェーズの通信時間の測定では、この unconfirmed-push のシーケンスが測定時間には含まれていない。

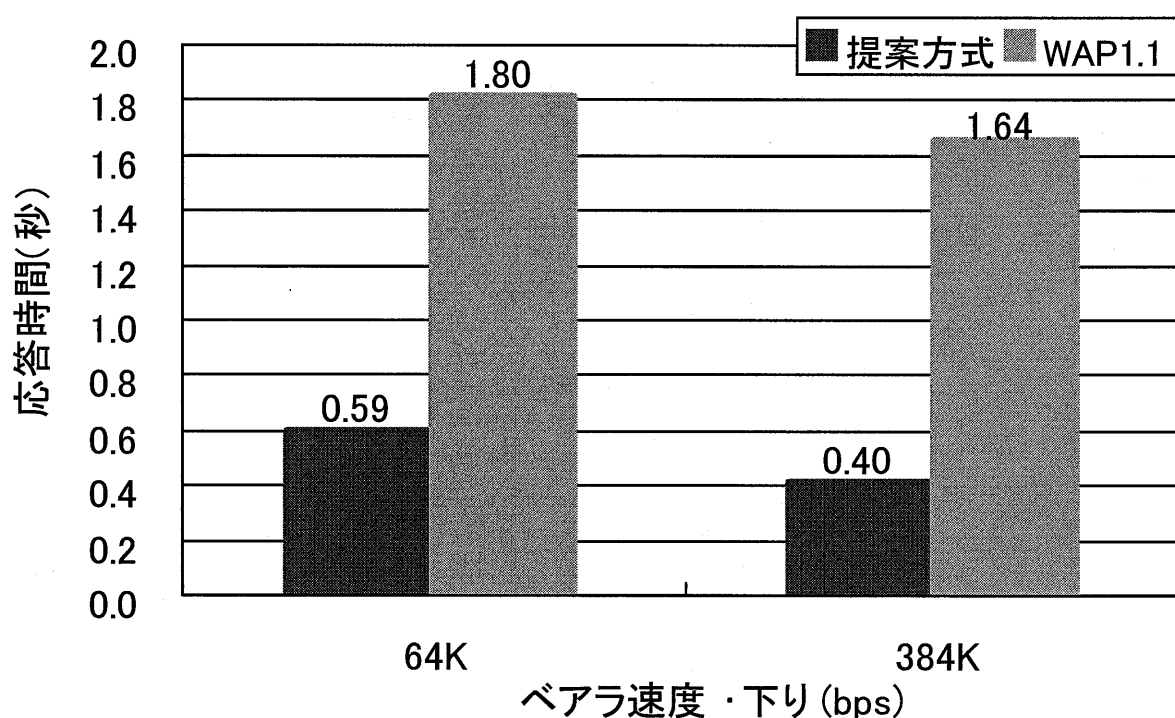


図 3-8 開設フェーズの比較

3.3.4 プッシュ実行フェーズ

図 3-9 は、プッシュ実行フェーズの応答時間を示す。データサイズが小さい場合 (=500 バイト) には、WAP1.1 の応答時間が優れるという結果が得られた。また、データサイズが大きくなるに従いその応答時間の差は小さくなり、データサイズが大きな場合 (=100K バイト) には、逆に提案方式の応答時間が優れるという結果が得られた。なお、応答時間は、ベアラの下り速度が高速になれば WAP1.1 及び提案方式共に短くなるものの、ベアラ速度が変化することによって各プロトコルで得られる応答時間に逆転が生じる等の違いは得られなかった。

すなわち、これらのプロトコルは、両方ともベアラ速度にほぼ比例して応答時間が変化することが分かる。

プッシュ前に開設フェーズを必要とする単独プッシュでは、プッシュ実行フェーズ（図 3-8 の結果）に開設フェーズ（図 3-9 の結果）が加わるため、提案方式が WAP1.1 よりもプッシュ完了までの時間が短い。以上から、サイズが大きいデータや単独のプッシュ時には、提案方式は WAP1.1 よりも有利であることが明確となった。一般的な利用方法では、多くのプッシュは単独で行われるため、提案方式の応答時間は WAP1.1 の応答時間よりも短いことを示した。

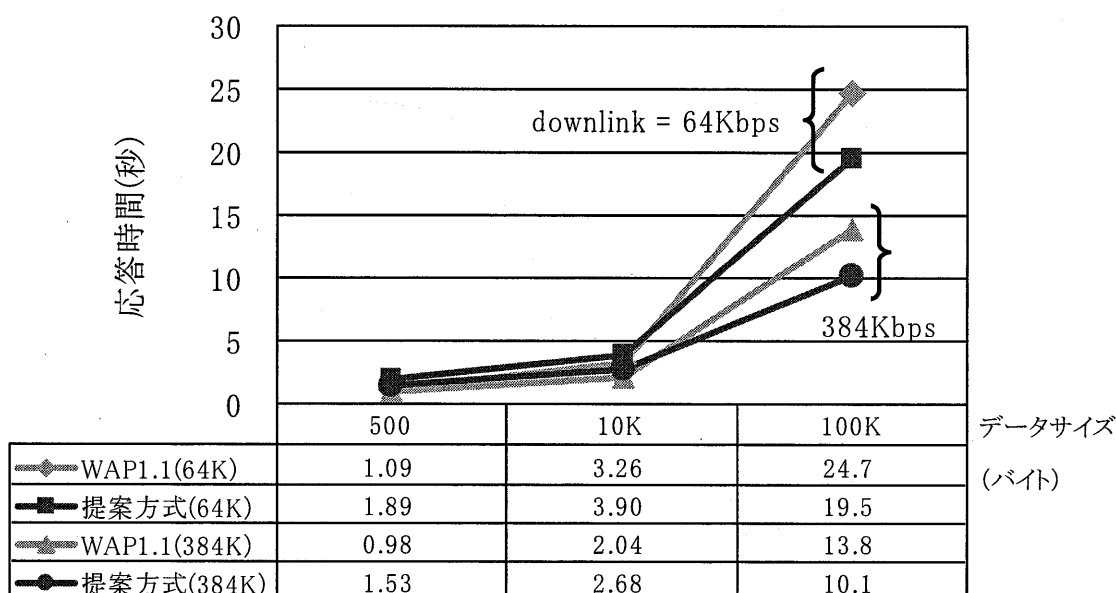


図 3-9 プッシュ実行フェーズの比較

3.3.5 性能測定 of 考察

本節では、WAP1.1 と HTTP/TCP のデータ転送の仕組みを比較し、図 3-8, 9 の結果について考察する。

小さいデータで WAP1.1 が優れた理由として TCP の初期輻輳ウィンドウサイズの決定方法がその理由として挙げられる。TCP では、通信初期の輻輳ウィンドウサイズを最大セグメントサイズ (MSS) に設定し、その後、スロースタートアルゴリズムにしたがってウィンドウサイズを徐々に伸張する。したがって、小さいデータのプッシュの場合には、ネットワークの帯域幅を十分に使い切るためのウィンドウサイズの伸張が無いままデータ転送が終了する。反面 WAP1.1 のフロー制御を提供する WTP [47] では、固定のウィンドウサイズを用いたウィンドウ

制御方式を採用している。したがって、小さいサイズのデータの場合には、通信初期の段階からウィンドウサイズの範囲内でデータ転送が行えるため、WAP1.1が有利であるという結果が得られた。

小さいデータでWAP1.1が優れたもう一つの理由として、それぞれのプロトコルで必要なパケット数の違いが挙げられる。WSPのconfirmed-pushメソッドの確認応答は、WTPのAckの2パケットを要している(図3-6)。それに対しHTTP/TCPでは、HTTP POSTメソッドとそれに対するTCPのACKと、HTTP POSTリプライとそれに対するACKということで4パケットを要している(図3-7)。つまり、HTTPでは、“200 OK”といったHTTPレイヤでの確認応答に対するTCP ACKが必要となり、HTTP/TCPでは、必要なパケット数が多くなっている。以上のことから、小さいデータ送信時には、必要とするパケット数の差についても応答時間に影響したものと考えられる。

移動通信パケットネットワークの多くは、固有のネットワーク規制メカニズムを備えるため、ネットワークの輻輳対策は、ベアラネットワークにて対処を行うことが可能である。したがって、どこで輻輳が発生するか推定しにくいインターネットの場合には、スロースタートを用いた輻輳回避対策が有効であるが、提案方式のように移動通信ネットワークに閉じた環境でTCPを適用する場合には、トランスポート層でスロースタートアルゴリズムを提供する必要性があるかどうか疑問である。むしろ小さいデータ向けに初期ウィンドウサイズ伸張等の対処を行うことで、サイズが小さいデータに対して有効なデータ転送が行えることが期待できる。

大きいデータでTCPが優れる理由については、TCPとWTPのウィンドウ制御方式の違いが考えられる。TCPでは、ピギーバック方式を採用し、データパケットの送受信ともにACKパケットが送受信される。対してWTPでは、ACK用の独立したパケットが存在し、さらに、ウィンドウサイズ内のデータパケットをすべて受信した後にACKパケットを送出する。すなわち、TCPでは、データの送受信中にあわせてACKの送受信を行っているのに対し、WTPでは、データ送受信と、ACKの送受信が明確に区別されている。したがってWAPでは、データサイズが大きくなるに従い、このACK応答のための待ち時間(図3-10)が全体的な応答時間に影響したものと考えられる。なお、図3-10は、WTPとTCPの通信シーケンスを模式的に示したものである。WTPでは、ACK応答のための待ち時間が存在し、TCPでは、通信初期のスロースタートフェーズにおいて、帯域幅を使い切ってい

ない様子が確認できる。

TCP では、一定時間パケットの到着がない場合には、その監視タイマの満了により ACK を返す制御を行うため、移動機から PPG 方向（上りリンク）に送信される TCP ACK の数は、WAP1.1 の WTP の Ack 数と比較して多い。また先に述べた HTTP とそれに対する TCP ACK の存在のために、必要なパケット数が WTP よりも多くなる傾向にある。しかし、W-CDMA 等の移動通信ネットワークでは、下りと上りリンクで別々の帯域を確保しており、さらに、TCP ACK サイズとその発生頻度に対して上りリンクの帯域は十分に余裕がある容量であるため、大きいサイズのデータのプッシュ時においては、上りの TCP ACK パケット数が全体的な性能には影響しないことが分かった。

トランスポートの性能のほかに WSP のヘッダコンパクトエンコーディング [42] も小さいデータで WAP が有利であった原因の一つに考えられる。WSP においては、ヘッダのバイナリ化を行うことによって約 35% のデータ量を減少させるため、小さいデータにおいて WAP1.x の応答時間が短縮された。しかし、WSP ヘッダのコンパクトエンコーディングは、データサイズが小さい場合には有効であるが、データサイズが大きい場合には、データパケット全体から見て、ヘッダが占めるデータ量が相対的に小さいため、コンパクトエンコーディングの効果が出にくい。

以上の結果から、サイズの大きいデータが提供されることが予想される。W-CDMA 等の高速ベアラにおいては、提案方式が採用する HTTP/TCP により実現したプッシュプロトコルの有効性が示された。なお、今回の評価では、現在インターネットで用いられている TCP をそのまま用いており、高速移動通信ネットワーク向け TCP プロファイル [4] に準拠していない。本研究では、W-CDMA のような高速な移動通信ネットワークを想定しているため、W-CDMA の回線性能を更に引き出すことが可能な TCP プロファイルを用いることにより、提案方式の応答時間がさらに短くなることが予想できる。

本研究結果に基づいた提案プッシュプロトコルを WAP フォーラムに提案し、提案方式は、WAP2.0 プッシュプロトコル仕様のベースとして採用された。WAP2.0 プッシュプロトコルは、提案方式に加えて、移動機の機種等の能力情報を PPG に伝達する手段や、移動機と PPG の相互認証機能等が追加されている [48]。したがって本研究結果は、IMT-2000 等の高速移動通信ネットワークにおける WAP1.x と WAP2.0 プッシュプロトコルの性能比較の上で参考になるものと考えられる。

ただし、WAP2.0 と提案方式の詳細な比較については、今後の研究対象としたい。

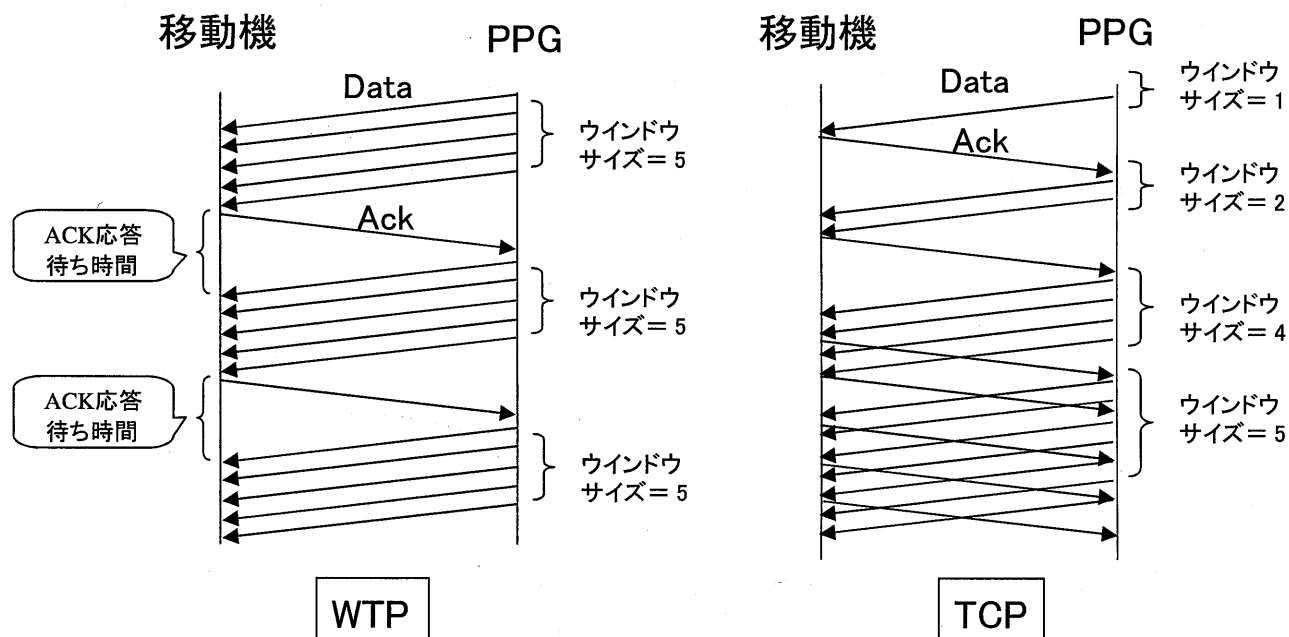


図 3-10 WTP と TCP のウィンドウ制御方式の比較

3.4 差分プッシュ方式

3.4.1 提案の背景

WWW (World Wide Web) のプルモデルやスマートプルでは、データが更新された後すぐにクライアント側に反映できないといった即時性の問題がある。また、一般にプッシュ型サービスでは、プッシュしたデータが移動機にとって必要な情報かどうか送信側が判断出来ないという問題がある。ネットワークリソースの浪費を防ぐためには、プッシュデータのサイズを出来る限り小さくすることが課題となる。本論文では、データの更新を契機として、オリジンサーバから移動機に対してデータをプッシュすることによって即時性を確保し、さらに更新されたデータの差分のみをプッシュすることによってネットワーク利用効率にも優れる新しいプッシュ方式を提案する。

関連する研究として、スマートプル方式を応用したデータの差分情報転送方式がある。この方式では、HTTP 等のプル型プロトコルを用いて、クライアントがオリジンサーバに対して定期的にデータの更新問合せを行い、オリジンサーバ側にてデータが更新されている場合には、以前にクライアントに提供した更

新前データと、更新後データの差分データを提供する方式である。HTTP において、この機能を実現するための方法として、HTTP のデルタエンコーディング [49] が仕様化されている。HTTP デルタエンコーディングでは、UNIX の diff コマンド等により任意のテキストデータの差分を抽出することができるとしているが、XHTML 等の XML のデータ構造に着目した差分データの検出法については述べられていない。また、オリジンサーバ起動型のプッシュ方式における差分プッシュ方式に着目した研究は行われていない。そこで本論文では、3.2.2 節で説明したスマートプル方式の問題点を解決するオリジンサーバ起動型プッシュを応用した差分プッシュ方式を提案する。

3.4.2 差分プッシュ方式の提案

移動通信ネットワークは有線ネットワークと比較して、ネットワーク利用コストが高いため出来るだけネットワーク利用効率を高める必要がある。このため、差分情報のみを転送することによって、ネットワークを流れるデータ量の削減を図ることが重要となる。本論文では、XHTML 等の XML の文書構造に着目した差分プッシュ方式を提案する。

提案プッシュ方式の処理内容を以下に示す (図 3-11)。①初めに移動機は、プル型もしくはプッシュ型にて差分データの元となるデータを取得する。②PI (=オリジンサーバ) にてそのデータが更新された場合、PI は XSLT [7] で記述されたスタイルシートで表現した差分データを生成する。③PI は更新前のデータを以前に提供した移動機のリスト (ユーザリスト) を保持しており、ユーザリストに登録されている移動機に対して差分データをプッシュする。④差分データを受け取った移動機は、XSLT を用いて更新前の旧データと差分データから新データを自動生成する。

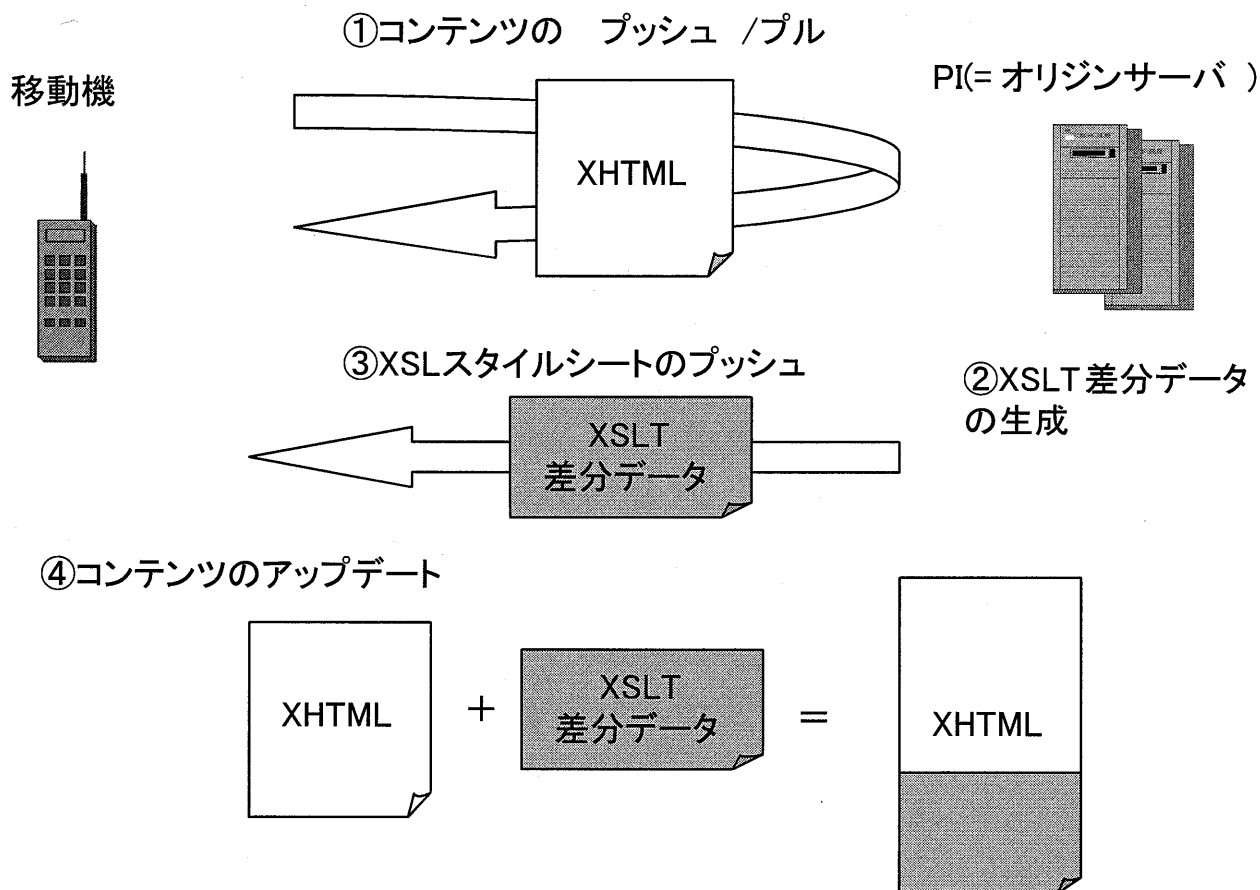


図 3-11 差分プッシュ基本構成

XSLT は、XML 文書の構造変換機能を提供するための W3C 仕様であり、ある XML データに対して特定範囲だけを指定した体裁で表示・出力することや、構成要素の並べ替えを行うことが可能である。この技術を応用することにより、更新前データから更新後データへの差分情報を、XSLT を用いた変換ルールとして記述することが可能である。更新前データに XSLT 差分データを適用するソフトウェアを用いて、自動的に更新後データを生成できる。任意に与えられた 2 つの XML 文書の差分データの生成方法として、更新前後の XML 文書の DOM (Document Object Model) [50] ツリーを生成し、その 2 つの DOM ツリーを比較することによって、XML の差分箇所を検出し、その XSLT 差分データを生成する方法等がある [51]。掲示板の新たな発言内容の追加等の例で考えられるように、決まった更新箇所にデータが追加されるような単純な XML データの更新の場合には、更新がある箇所の追加情報を XML テンプレートで記述するといった単純な方法で

実現することもできる。本提案方式では、この方法を用いて XSLT 差分データを生成することによって、差分プッシュを実現した。

新データの画面への表示は、XHTML に新たな onpush イベントタグを定義し、差分データ受信時の、画面更新のための動作を規定する。該当する旧データが画面上に表示されておらず、移動機のローカルキャッシュ中にそのデータが存在するような場合においても、移動機はそのローカルキャッシュを書き換えても良い。これによってユーザは、ローカルキャッシュ中に存在するものについては再読み込み（リロード）をせずとも最新情報を取得することが可能になる。

以下では、最初のデータをプル型で取得し、差分データをプッシュ型で移動機に提供する方式について述べる。WWW のブラウジングでは、リンクをたどりながら目的のデータを探す、もしくはたどり着くのが一般的であることから、オリジンサーバが提供するデータのうち、あるユーザにとって最も必要となる可能性の高いデータは、当該ユーザがオリジンサーバ上でアクセスした最後のデータである確率が高い。この考えに基づけば、オリジンサーバにおいてユーザリストを作成する際に、そのデータを最後にアクセスしたユーザのみをリストアップし、そのユーザにのみ差分データをプッシュすることによって、ユーザにとって重要なデータの更新情報のみを送信するようにすることも可能である。

移動機は、差分データを受信し、その処理を行った後に PI に対してリプライメッセージを送信し、データ更新が成功したか、あるいは失敗したか等の情報を含めることも可能である。この方法を用いれば、PI は移動機へのプッシュの成功、不成功を確認できると共に、その理由を知ることができ、次回からのプッシュに反映させることが可能である。

本提案に基づく差分プッシュ方式は、3.2 節において説明した提案に基づくオリジンサーバ起動型のプッシュを用いて動作する。したがって、オリジンサーバにおいてデータが更新された場合に、即時にデータを移動機に提供することが可能であり、移動機において常に最新のデータを保持することが可能である。また、データが更新された場合に差分プッシュを実行することになるため、スマートプル方式を利用した従来の差分プッシュ方式で問題となっていた、定期的に問合せすることによる不必要な問合せが発生しないという点を特徴とする。

3.4.3 テストベッドの試作

提案したプロトコル及び差分プッシュ方式を基に試作したテストベッドにつ

いて紹介する。テストベッドでは、データの更新があった場合に、その更新部分を自動生成し、移動機へとプッシュを行うことが可能である。試作では、アプリケーションの例としてチャットを実現するアプリケーションの構築を行った。図 3-12 を用いてそのチャットアプリケーションの概要を説明する。チャットアプリケーションでは、移動機の画面表示のためのコンテンツ記述方法として XHTML を想定している。チャットアプリケーションでは、あるユーザが新たな発言を行った場合にその新たな発言内容を差分データとする XSLT 差分データを自動生成し、チャットに参加しているメンバーに対してプッシュを行う。チャットにおける新たな発言は、決まった更新箇所にデータが追加されるような単純な XML データの更新であり、更新がある箇所の追加情報を XML テンプレートで記述するといった単純な方法で XSLT 差分データを生成できる。その XSLT 差分データを受け取った移動機は、XSLT 変換を行うことで古いデータからの更新を行い、新しい発言内容が画面上に反映される仕組みになっている。図 3-13 は、あるユーザの発言により画面が更新された様子を示している。

テストベッド試作により、差分データの生成、差分データのプッシュ、及び旧データと差分データからの新データの生成が全て自動で行えることを確認した。図 13 に示す例における XSLT 差分データサイズは 793 バイトであり、これに対する更新後データのサイズは 2090 バイトであった。以上のことから、差分データ XSLT で表現することにより、1297 バイトのデータが削減された(図 3-14)。差分プッシュ方式では、図 3-14 に示す XSLT 差分データを更新前 XHTML データに適用することによりデータが更新される。このデータサイズの差は、チャットアプリケーションを用いた場合の例であり、用いる XHTML データにより傾向は異なるが、一般的にデータの差分を用いることによりデータサイズの減少を図ることができる。また、チャットデータを差分データの生成時間と、旧データと差分データから新データの生成時間を測定したところ、差分データを生成しない場合と比較して、110ms 余分に要することが分かった。この時間によるユーザへのサービス性の低下への影響は小さく十分実用性があると考えられる。

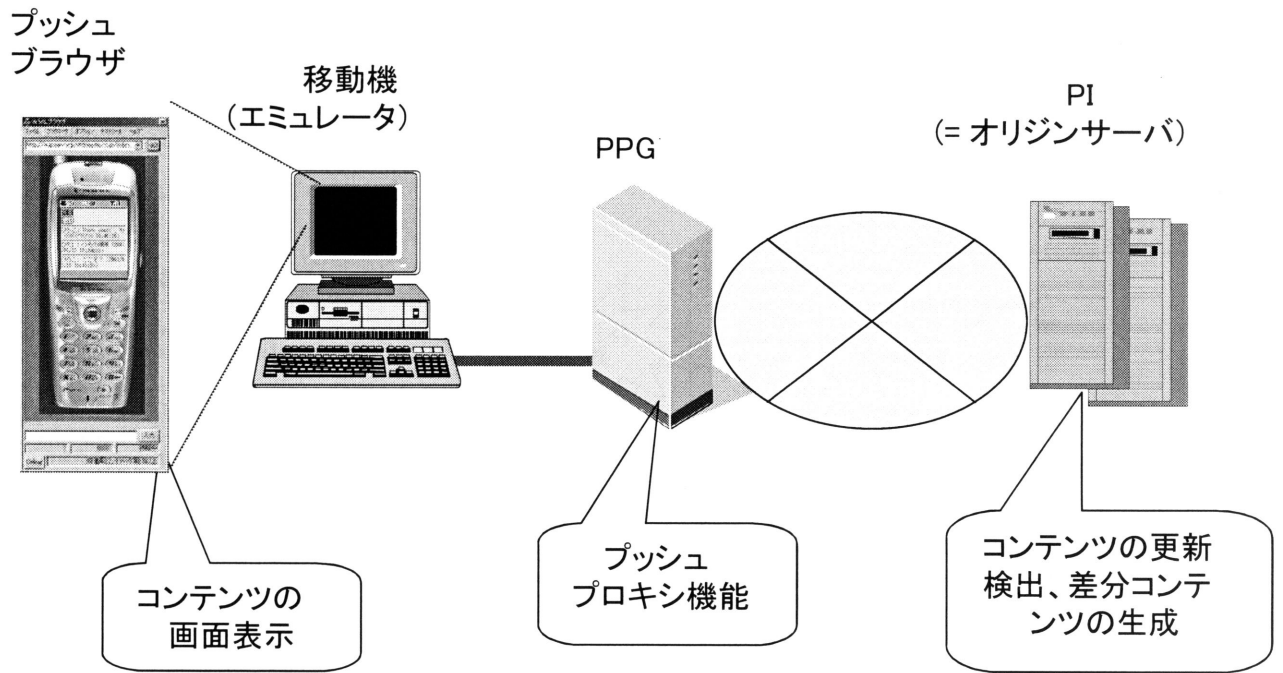


図 3-12 チャットアプリケーションデモシステム

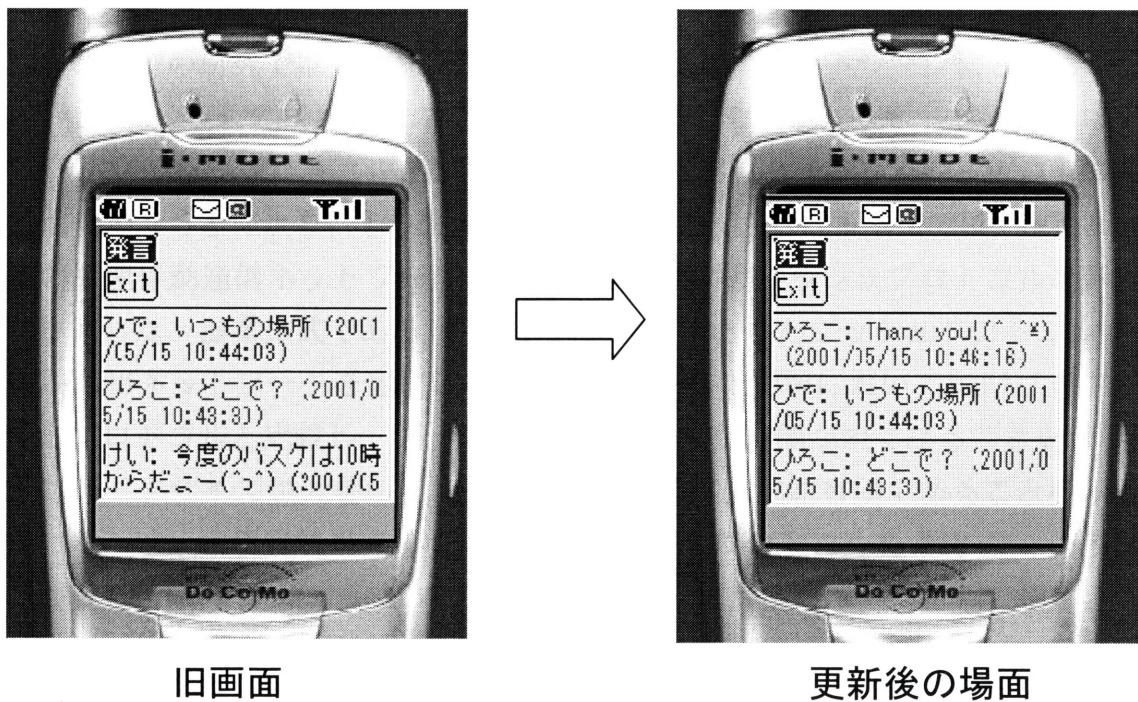


図 3-13 画面更新イメージ

XHTML データ

```
<? xml version="1.0" encoding="EUC-JP"?>
<!DOCTYPE html PUBLIC "-//WAPFORUM//DTD XHTML Mobile 1.0//EN "
"http://www.wapforum.org/DTD/xhtml-mobile10.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
</head>
<body style="background-color:#ffff00">
<form>
( フォーム定義省略: 703 バイト )
</form>
<hr/>
<div style="color:#ff0000">
<div style="color:#ff0000">
<hr/>
<div style="color:#ff0000">
<hr/>
<div style="color:#800080">
<hr/>
<div style="color:#ff0000">
<hr/>
<div style="color:#ff0000">
<hr/>
<div style="color:#ff0000">
<hr/>
<div style="color:#ff0000">
<hr/>
<div style="color:#ff0000">
<hr/>
<div style="color:#ff0000">
<hr/>
</div>
</body>
</html>
```

2090 バイト

新たな
発言内容

1297 バイト
削減

XSLT 差分データ

```
<? xml version="1.0" encoding="Shift_JIS "?>
<xsl:stylesheet version="1.0"
xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
xmlns:xhtml="http://www.w3.org/1999/xhtml"
exclude-result-prefixes="xhtml">
<xsl:output ( アウトプット定義省略 ) />
<xsl:template match="*[@node()]">
<xsl:copy>
<xsl:apply-templates select="*[@node()]" />
</xsl:copy>
</xsl:template>
<xsl:template match="/" xhtml:html/ xhtml:body/ xhtml:hr[1]">
<xsl:copy>
<xsl:apply-templates select="*[@node()]" />
</xsl:copy>
<div style="color:#ff0000">
<hr/>
</xsl:template>
</xsl:stylesheet >
```

793 バイト

新たな
発言内容

図 3-14 チャットアプリケーションにおける XSLT 差分データの例

3.5 おわりに

これまでの研究では、IMT-2000 等の高速移動通信ネットワークにおける WAP 1. x プッシュプロトコルの性能評価は行われていなかった。本研究では、WAP1. 1 プッシュプロトコルと HTTP/TCP をベースとした提案プッシュプロトコルと比較することにより、その性能を明らかにした。さらに本論文では、IMT-2000 等の高速移動通信ネットワークに適した移動機向けプッシュプロトコルを新たに提案した。提案方式である HTTP/TCP をベースとしたプッシュプロトコルは、IMT-2000 ネットワークを想定したシミュレーション環境において WAP1. 1 のプッシュプロトコルと比較し、プッシュ完了までの通信時間が短くなることを示し、特にデータサイズが大きいデータの場合には提案方式が有効であることを示した。我々は、本研究結果に基づいた提案プッシュプロトコルを WAP フォーラムに提案し、WAP2. 0 プッシュプロトコル仕様は、本提案をベースとして採用された。

さらに本論文では、XHTML とプッシュ機能を組合せた差分プッシュ方式を提案し、テストベッド試作によりその有効性を検証した。

クライアントが増えた場合のスケラビリティに関しては、今後の検討課題

としたい。特に複数クライアントへ同時配信を実現する際のマルチキャスト方式 [45] [46] と本方式の共存方式等について検討し、それとあわせたスケーラビリティに関する詳細な検討について今後の検討課題とする予定である。

第4章 W-CDMA ネットワークでのリンク層 ARQ と TCP の特性評価

4.1 はじめに

移動通信ネットワークによるインターネットアクセスが急速に増大しつつあり、また第3世代移動通信ネットワーク (IMT-2000) による高速広帯域の通信サービスがわが国では2001年より開始されている。現状、インターネット通信の90%以上はTCPが使用されており、大部分のアプリケーションはWebとメールである。

一般に移動通信ネットワークのように、伝送誤りがあり、IP網に較べ伝送単位長が小さな区間を含む網では、リンク層での誤り回復を使用することによって、エンドトウエンドの誤り回復だけを用いた場合に起る性能低下を補償することができる。しかし、トランスポート層のTCPとリンク層の再送機構の2つの併用によって、望ましくない相互作用が起り得ることが指摘されている [52] - [54]。

本論文では実用性の観点から、現在市場にあるTCP実装で適用可能な範囲でTCPの性能を引き出せるようなW-CDMA (IMT-2000) [55] リンクおよびTCPの動作パラメータの最適値を求める。

本論文は以下のアプローチを取る。W-CDMAにおけるTCPの性能を評価するには、リンク層の誤り回復メカニズムであるRadio Link Control (RLC) [22] とTCPの相互作用を調べるのが重要である。現在用いられているTCP実装で性能を引き出すために、無駄な再送の原因となるリンク層での遅延ジッタ抑制を検討する。さらに、W-CDMAリンクで用いられるSelective Repeat型ARQを詳細に再現したシミュレーションモデルにおいて、各種プロトコルパラメータを変化させ、リンク層における性能と効率のトレードオフについて検討を加えることとする。

本論文は最初にW-CDMAの特性を概説し、関連研究と我々のアプローチについて述べ、W-CDMAの特性に影響を与えるリンク層の再送メカニズムについて調べ、ネットワークエミュレータによる実際のTCP実装を用いた実験と、計算機上のシミュレーションにて無線ネットワーク上でのTCPによるデータ伝送特性の評価と考察を行い、得られた結果と今後の課題をまとめる。

4.2 W-CDMA ネットワークとリンク層再送機構

W-CDMA は IMT2000 標準の一つであり，3GPP (3rd Generation Partnership Project) [56] で標準化されている．表 4-1 に示す諸元を持つ [57]．W-CDMA では利用者あたり最大 2 [Mbps] のデータ伝送帯域幅を提供することが可能である．しかしながら，無線伝送における誤りによって必ずしも常に最大帯域幅が利用可能な訳ではない．

表 4-1 W-CDMA の諸元

アクセス方式	Direct Sequence CDMA (DS-CDMA)
デュプレックス方式	Frequency division Duplex (FDD)
帯域幅	5Mhz
データ速度	最大 2Mbps
誤り訂正符号	ターボ符号，畳み込み符号
基地局間同期	非同期
音声符号化	AMR (Adaptive Multi Rate) (1.95-12.2Kbps)

W-CDMA で利用可能な伝送サービスには音声通話を目的としたものとパケットによるデータ伝送を目的としたものがある．パケットによるデータ伝送においては無線伝送物理層での回線品質を補うため，リンク層における再送機構 (ARQ: Auto-repeat ReQuest) によって誤り回復が行われる．W-CDMA では RLC という無線リンク層における再送プロトコルが用いられる．W-CDMA における TCP の性能を評価するには，RLC と TCP の相互作用を調べるのが重要である．

図 4-1 に W-CDMA のプロトコルスタックを示す．UE (User Equipment) は TCP やアプリケーションを実装した端末をあらわしている．RLC プロトコルは UE と RNC (Radio Network Controller) 間で動作する．CN (Core network) は，SGSN (Serving GPRS Support Node), GGSN (Gateway GPRS Support node) から構成され，それぞれ中継交換機である．TCP はその上位において，UE と Internet server との間で動作する．

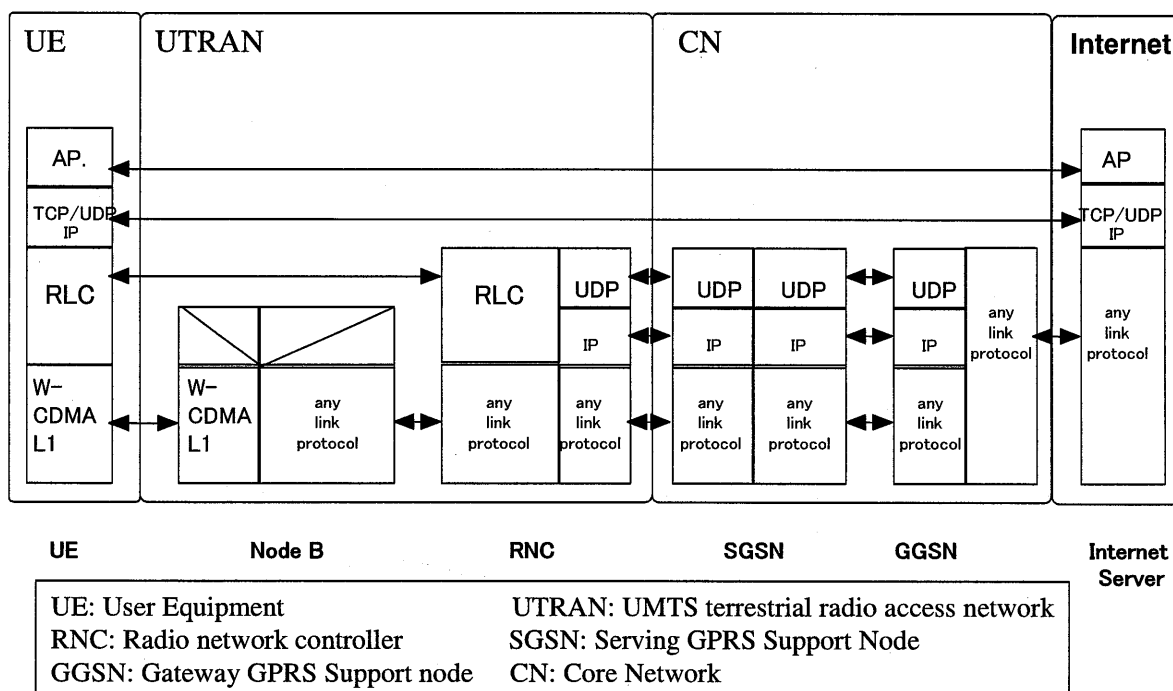
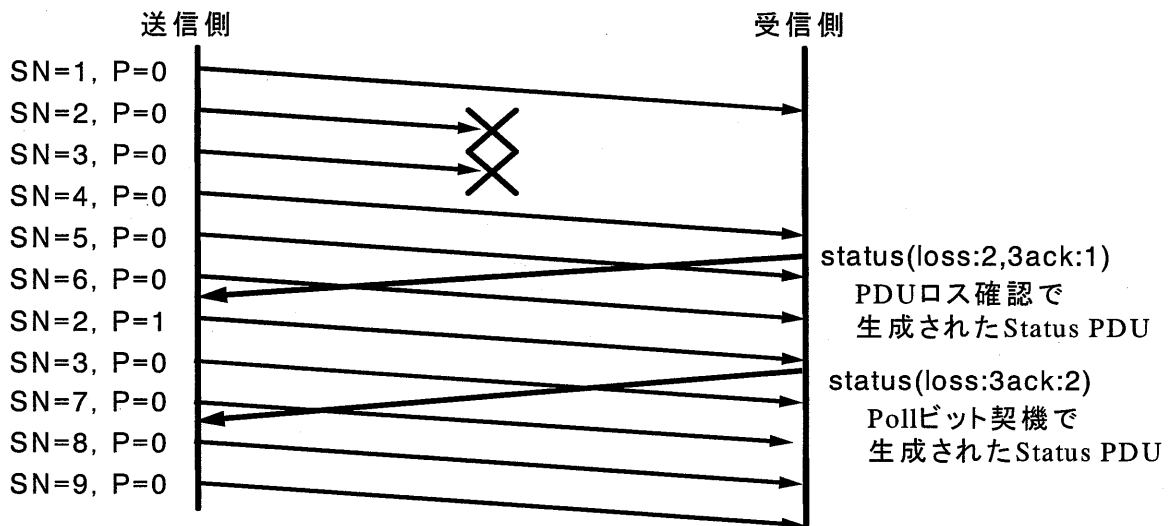


図 4-1 W-CDMA プロトコルスタック

RLC プロトコルは上位層から受け取った IP パケットを SDU (Service Data Unit) として扱い、2 オクテットのヘッダを付加し、40 オクテットのペイロードを持つ PDU (Protocol Data Unit) に分割し、PDU 単位で送受信を行う。再送は Polling/Status Report を用いた Selective Repeat 方式を採用している。図 4-2 に RLC プロトコルの送受信方式の概略図を示す。送信側は、送信する PDU のヘッダに含まれる P (Poll) ビットを立てることによって、受信側に PDU 受信状況報告 (Status PDU) を要求することができる。受信側では STATUS PDU を以下の条件で送出する。



左側: SN, PはデータPDUのヘッダ情報
 SN: シーケンス番号, P: Poll bit 状態
 右側: Status(loss: X, ack Y) はStatus PDUの示す情報
 シーケンス番号X(複数可)がロス、Yまでを一括送達確認

図 4-2 RLC の再送動作

- (1) シーケンス番号の新たな抜けを検出した場合
 (即ち新たな PDU ロスを検出した場合)
- (2) P ビットが立った PDU を受信した場合

送信側は受信した STATUS PDU を基に PDU の再送を行う。

RLC プロトコルは順序制御を行うため、PDU の再送が発生した場合、上位プロトコルには IP パケット単位の遅延として見える。

エンドトウエンドのロス回復を行う TCP に加えて、RLC の再送機構を用いると以下のメリットがある。

- (1) RLC では PDU が小さいため、ロスを回復するための再送にかかる転送量が少なくてすむ。IP パケット長は一般に、数百オクテットから 1500 オクテットであるのに対し、PDU 長はわずかに 42 オクテットである。
- (2) TCP で行われるエンドトウエンドのロス回復においては経路の両端まで送達確認のフィードバックをする必要がある。一方、無線区間で終端されるリンク層の再送によりロス回復できるなら、送達確認のフィードバックに要する時間はより短くて済む。従って、エンドーエンドで行うよりも迅速な再送が可能になることが期待できる。

4.3 関連研究

無線ネットワークへの TCP の適用に関する研究として、低速・高遅延環境におけるスループット向上のための TCP 制御手法と、リンク層の再送制御手法とがある。

(1) TCP 制御手法

低速かつ高遅延即ち Long Thin Network [58] において TCP を用いた時の回線利用効率の向上に関する研究には以下のものがある。例えば、スロースタート期間の短縮のために、輻輳ウインドウの制御粒度の変更 [59] や Delayed Ack を停止しスロースタート期間の Ack の返りを早める手法 [60] がある。これらの手法は有効であるものの、TCP の実装の変更が求められるため直ちに利用可能という訳ではない。また、無線ネットワークにおける伝送誤りを回復するために、中間ノードが TCP を終端し、コネクションを分割する手法として I-TCP [61]、Snoop [62] がある。これらの提案で導入される中間ノードは総称して PEP (Performance Enhancement Proxy) と呼ばれる。PEP では TCP のエンドトゥエンドの通信モデルが維持されない、PEP の導入のために経済性、スケーラビリティ、信頼性等への運用における配慮が必要である。

(2) リンク層の再送制御技術

リンク層と TCP の関連を特定のネットワークの特性の観点から扱った研究として CDMA2000 1xRTT での報告 [53] がある。基地局における資源の周期的な割当てにより端末から見た利用可能な帯域幅の変動が起り、遅延ジッタによる TCP のタイムアウトから無駄な再送が引き起こされる問題を報告している。資源割り当ての方法を始め、詳細において異なるため、同一の結論が本論文で扱う W-CDMA に直接適用可能かについては明かではない。

遅延ジッタによる無駄な再送を起す原因となるタイムアウトは Spurious time out と呼ばれている。Spurious time out による性能低下を改善する手法として例えば Eifel アルゴリズム [63] などが提案されているが、まだ現在の TCP 実装には普及していない。

TCP とリンク層 ARQ の相互作用について、IS-707 リンクでの計算機シミュレーションによる報告 [52] がある。TCP の受信広告ウインドウを適切に設定することとリンク層での再送を十分に行うことの 2 つが重要であることを述べている。但し、実装を前提としてリンク層パラメータ間の相関関係 (トレードオフ) の議論は行われていない。

文献 [64] では UMTS に基づく ARQ が働く無線リンク上での TCP のスループットや RTT (Round Trip Time) の数学モデルが構築され、リンク層での再送を十分に行うことが重要であると示している。しかし本文献では GO-BACK-N ARQ をモデルとしており、W-CDMA で用いられる Selective Repeat 型 ARQ については検討されていない。

文献 [65] は W-CDMA 仕様に基づく計算機シミュレーションを実施し、リンク層再送機構における順序制御の重要性について議論している。但し、対象としたリンク層のパラメータやその値が限定されている。

(3) 本論文での前提条件とアプローチ

上記の研究動向を踏まえて以下の前提条件を設定した。

- (a) TCP 制御手法は現在市場にある TCP 実装で適用可能な範囲とする。
- (b) エンドーエンドの通信モデルを維持するため、中間ノードの手法は採らない。
- (c) Selective Repeat 型 ARQ である RLC の詳細なモデルを基に検討を行う。

上記の前提条件に基づき、W-CDMA の特性に関して既存研究では十分に検討されていない以下の観点から論ずる。

- (a) リンク層での遅延ジッタを抑制し、TCP の無駄な再送を低減する。
- (b) TCP スループットの最大化の観点からリンク層でのジッタ抑制と伝送効率におけるトレードオフを明らかにする。
- (c) リンク層および TCP に設定すべきパラメータを明らかにする。

4.4 RLC 再送のもとでの TCP 伝送性能

本章では TCP における伝送性能を向上するために最適化する必要のあるリンク特性と、調整すべき TCP や RLC の相互関係について述べる (表 4-2 参照)。

4.4.1 帯域幅遅延積

伝送路の帯域幅と遅延時間の積が TCP の受信ウィンドウサイズの最適値を規定する。一般に遅延時間は伝播遅延と処理遅延の和で表わせるが、無線区間の RLC プロトコルによる誤り回復のため動的に変化する。

第 3 世代移動通信ネットワークでは、一般的な符号化に加え FEC (Forward Error Correction) や interleaving も用いられるなど、多くの処理を要するた

め処理遅延も無視できない [66].

無線区間の誤りが発生し、リンク層再送動作が始まると遅延時間が増大する。RLC は SDU の送信順序を保証するため、後続 SDU は送信中の SDU の送信終了まで待たされるからである。さらに、本来データを伝送すべき帯域幅が再送に費やされるため、実質的に利用可能な帯域幅が狭くなる。

4.4.2 リンク層再送動作の粘り強さ

RLC の再送制御において、PDU の再送回数には上限が規定されている。再送回数が上限に達した場合には RLC コネクションが切断され、転送中の SDU は破棄されて IP パケットロスとなる。この IP パケットロスは TCP の再送機構によって回復されるが、4.2 章での送達確認のフィードバックに要する時間についての議論の通り効率の低下が予想される。RLC において PDU 再送の再試行回数の上限值は MAX_DAT というパラメータによって規定される。

4.4.3 遅延ジッタ抑制と利用可能帯域幅の増大

前述のとおり、RLC での再送回数に応じて遅延時間は変動する。遅延時間が急に増加した場合、TCP はタイムアウトを起し、セグメントが失なわれたと判断して再送を始める。これを回避するためには遅延ジッタを抑える必要がある。RTO (Retransmission Time Out) を起動する再送タイマの計算アルゴリズム [67] を以下に示す。

$$RTO = SRTT + \max (G, K * RTTvar)$$

$$\text{where } K=4$$

ここで、G はクロック粒度、SRTT は平滑化 RTT、RTTvar は RTT の分散、K は定数である。

上記アルゴリズムによると、平均 RTT に対する偏差の 4 倍を越える変動が起ると RTO が起る。RTO の初期値は 3 [s]、最小値は 1 [s]、最大値は 60 [s] が推奨されている。

W-CDMA において、リンク層で発生する遅延ジッタを抑えるためには RLC のパラメータを適切に設定する必要がある。そのようなパラメータのひとつとして、Timer_Status_Prohibit がある。これは、受信側が STATUS PDU を送信側に送出する最小時間間隔を規定する。例えば、この値が 0 に設定された場合、PDU ロスが起ると即座に STATUS PDU が送出され再送が行われる。本パラメータを 0 より

大きな値に設定することで一定の送出禁止期間をおくことが出来、一つの STATUS PDU で複数のロスを通知することが可能となる。しかし禁止期間が長すぎる場合、送達確認が速やかに行えずフローが停止し遅延ジッタが発生する。

従って、スループット向上の観点から、リンク層での遅延ジッタ抑制と伝送効率の間にトレードオフが成立する。即ち、Timer_Status_Prohibit の値が小さい場合には送出される STATUS PDU の数が多くなり、受信側からのロス通知が速やかに行われるが、STATUS PDU それ自体の転送と PDU の重複再送が利用可能帯域幅を圧迫することになる。Timer_Status_Prohibit の値を大きくすると送出される STATUS PDU が減少し、帯域幅が本来のデータ伝送に利用されリンク層での伝送効率が上昇するが、受信側からのロス通知が遅れるため再送間隔が開くことで遅延ジッタが大きくなり、RTO を引き起して TCP のスループットは低下する。

表 4-2 リンク特性と調整パラメータ

リンク特性	調整パラメータ
帯域幅遅延積	TCPの受信ウィンドウサイズに設定
リンク層再送動作の粘り強さ	RLCのMAX_DATに反映
遅延ジッタ抑制	RLCのTimer_Status_Prohibitに反映
利用可能帯域幅の増大	RLCのTimer_Status_Prohibitに反映

4.5 エミュレーションとシミュレーションによる特性評価

本章では、前章で述べた調整パラメータ (表 4-2 参照) について TCP スループットを引き出すための最適値をエミュレーションとシミュレーションにより評価・検証する。

評価の前提となるネットワークの動作条件と評価ツール (エミュレータとシミュレータ) について述べた後、以下の手順で検討を進める。

最初に、TCP の再送タイムアウト機構について代表的な OS (オペレーティングシステム) での動作をエミュレータを用いて評価する。次に、シミュレーションによって Timer_status_prohibit の値を変化させることで遅延ジッタ抑制と伝送効率のトレードオフ点から Timer_status_prohibit の最適値を求める。更に最大再送回数 (MAX_DAT) を変更することでリンク層再送動作の粘り強さを

変化させ、TCP によるデータ転送シミュレーションを行い、得られたスループットとパケットロス率の特性を明らかにし、MAX_DAT の最適値を求める。最後に、前 2 ステップで最適化されたリンク特性のネットワークを対象にして、受信広告ウィンドウを変化させ、TCP によるデータ転送シミュレーションを行い、そのスループットを観察することで W-CDMA リンクの帯域幅遅延積を反映した適正な受信広告ウィンドウサイズを求める。

4.5.1 擬似対象ネットワークの動作条件

図 4-3 に検討対象としたネットワークの構成図を示す。図中のアンテナは図 4-1 における RNC の位置に対応し、RLC の終端点を示している。

無線区間の RTT を 300 [ms] と仮定し、上り下りに 150 [ms] ずつ均等に配置した。有線区間は高速であるとし、帯域幅を 10 [Mbps]、ネットワーク内処理遅延を見込んで区間 RTT を 100 [ms] とする。従ってエンドトゥエンドの RTT は 400 [ms] である。帯域幅はサーバ側から見て下り 384 [kbps]、上りを 64 [kbps] とし、TCP にて 2MB のストリームをサーバから基地局を経て端末に転送した。W-CDMA は方式上利用者当たり 2 [Mbps] までの帯域を提供可能であるが、執筆時点で商用サービスとして利用可能な 384 [kbps] を選択した。本評価で用いる TCP の実装オプションやパラメータ等は、特に明記しない限り次節のプロファイルに従うものとする。PDU 単位のブロック誤り率は 0~10%の間を評価対象とする。

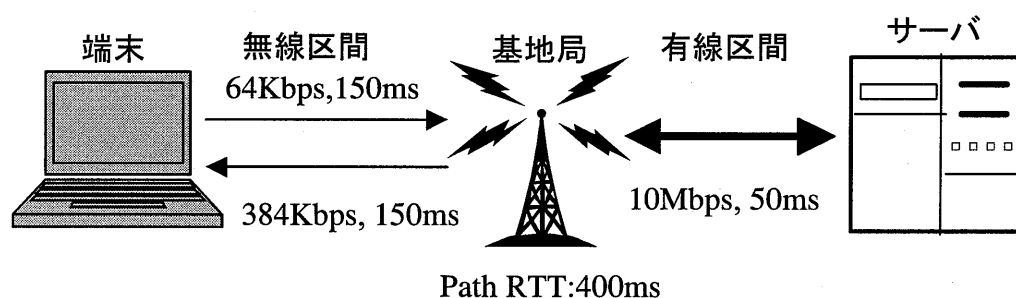


図 4-3 疑似ネットワーク環境

4.5.1.1 無線向け TCP プロファイル

Long Thin Network における回線利用効率の向上のため、現状の実装で利用可能なエンドトゥエンドの技法としての TCP プロファイルの提案がある [68], [69]。本論文は、現在市場にある TCP 実装で適用可能な範囲での対処を前提とするの

で、本プロファイルを従うべき条件とする。その主要な構成要件には以下のものがある。

- ・ 広告受信ウィンドウサイズの拡大:

W-CDMA に代表される第 3 世代無線ネットワークの大きな帯域幅遅延積を考慮して受信ウィンドウサイズを適切に拡大する。

- ・ 初期輻輳ウィンドウサイズの拡大:

転送初期・小容量伝送時の高速なパケット送出のためコネクション開始直後の送出量の拡大を計る。この設定は RFC2414 [25] で規定されている。

- ・ 最大転送パケット長の拡大:

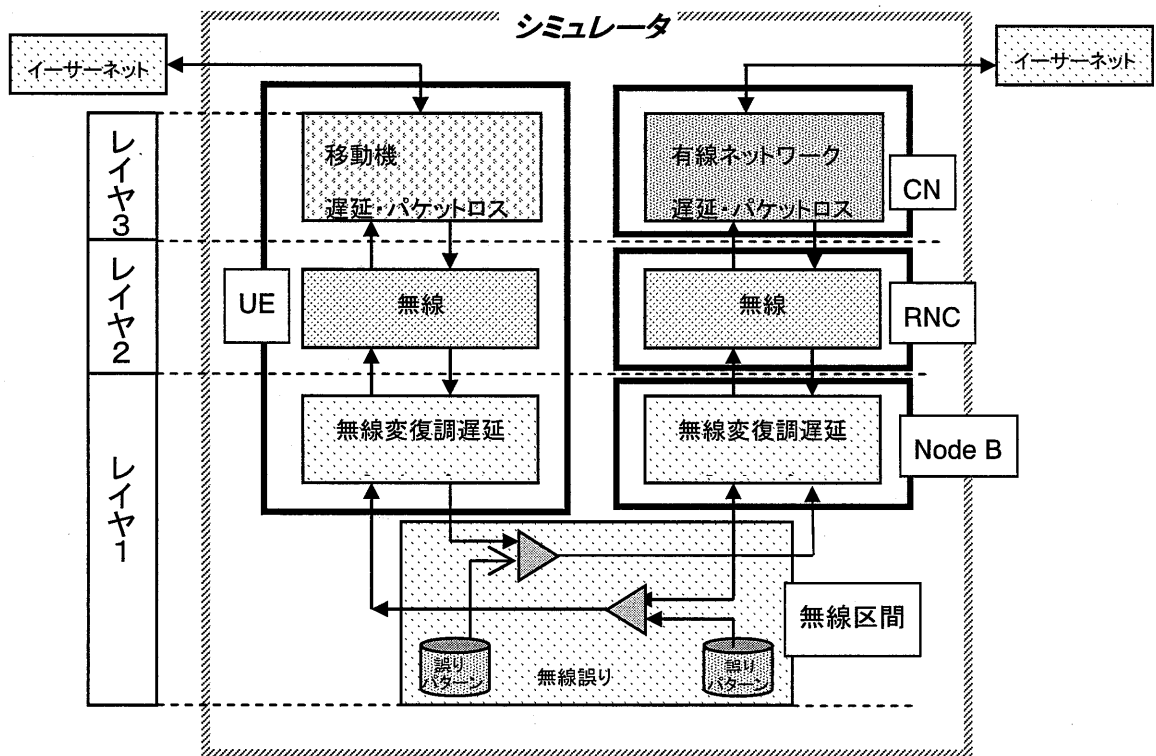
輻輳ウィンドウは最大 TCP セグメント長 (MSS: Maximum Segment Size) を基準にした値で管理されている。従ってスロースタート期間短縮のためには MSS を長くすることが有効である。MSS はリンク毎の最大転送パケット長 (MTU: Maximum Transfer Unit) を基に決まるため、MTU は運用実績のある値で最大の 1500 オクテットを基本とする。

- ・ 選択再送機構の利用:

ロス耐性向上のための選択再送機構 (SACK: Selective ACKnowledgement) [23] の利用を推奨する。リンクレイヤ再送機構が無線区間の伝送誤りを回復できなかった場合や、無線区間以外で起るパケットロスの回復における効率の向上が期待できる。

4.5.1.2 エミュレーション環境

エミュレーションには、筆者らが開発した W-CDMA エミュレータを用いる。W-CDMA エミュレータはリンク層プロトコル RLC と有線ネットワーク部分の振舞いを模擬する装置である。本装置は RLC を実行することで動的な遅延を再現し、有線ネットワーク部分は固定遅延を加えることで W-CDMA ネットワークを模擬している。無線の状態は、PDU 単位のロス率 (BLER: Block Error Rate) で表示する。PDU 単位のロスを指定するエラーパターンにより変更可能である。RLC パラメータ値の設定機能を持つ。W-CDMA エミュレータの機能構成を図 4-4 に示す。



UE : User Equipment

UTRAN : UMTS (Universal Mobile Telecommunications System)
terrestrial radio access network

RNC : Radio Network Controller

図 4-4 W-CDMA エミュレータの機能構成

外部インターフェースとして網側，端末側にイーサネットポートを計 2 つ持ち，それぞれにホストを接続して実際にアプリケーションを動作させて評価を行う。バルク転送にはそれぞれの OS 附属の ftp を用いている。外観を図 4-5 に示す。

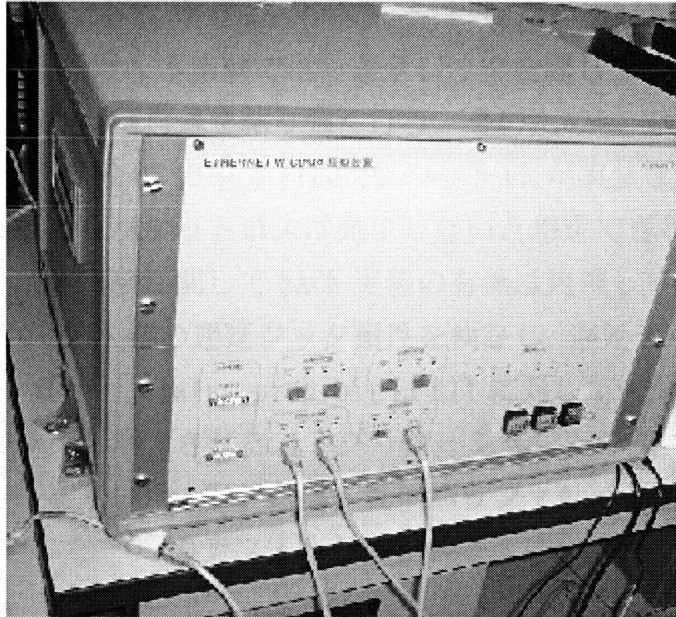


図 4-5 W-CDMA エミュレータ外観

4.5.1.3 シミュレーション環境

シミュレーションには OPNET Technologies 社の opnet [68] を使用し、RLC プロトコルを独自に実装した。エラーパターンによる BLER 設定により W-CDMA の無線伝送を模擬している。エミュレータと同様に RLC パラメータ値の設定機能を持つ。シミュレータ上の TCP の実装は 4.4BSD-Lite に準拠しており、SACK も利用可能である。シミュレーション結果は、1 サンプルあたり 20 回の試行の平均値をプロットする。

4.5.2 実装の違いによる TCP の再送タイムアウト機構の評価

TCP の再送タイムアウト機構の振舞いの実装による違いを確認し、以後のタイムアウトに関する検討で利用するモデルを選択する。

TCP の再送タイムアウトアルゴリズムの振舞いは現実には OS 毎の実装に依存する。商用 OS ではソースコードが公開されないのが一般的であるので、ハードウェア上で動作する実際の OS の動作を調べる手段が必要である。

そこでソフトウェアシミュレータと同様の機構を持ちハードウェアとして動作する W-CDMA エミュレータを用い、遅延ジッタに対する TCP 実装毎の再送タイムアウトの振舞いを検証した。

検証対象 OS として、サーバ OS に採用されることの多い Linux-2.2,

FreeBSD2.2.8, Solaris8 を送信側ホストとした。受信側ホストとして FreeBSD2.2.8 を用いた。本実験では、遅延ジッタを起しつつパケットロスに至らせないためにリンク層再送を粘り強く行う。そのために MAX_DAT を十分大きい 10 に設定した。対象 OS の中で FreeBSD のみ SACK が実装されていないが、上記 MAX_DAT 設定によりパケットロスは発生しないと想定できるため SACK が使われることはなく、本実験に関して SACK 実装の有無は無視してよい。再送タイムアウト発生回数から OS 毎の遅延ジッタ耐性を検証し、遅延ジッタ耐性が低い OS を選択するため、Timer_status_prohibit は RTT に対して十分大きな 500 [ms] に設定し、遅延ジッタを増大させた。アプリケーションとして ftp による 1MB のバルク転送フローを用いた。TCP 送信・受信バッファサイズは各 OS につきそれぞれ 64KB に設定した。OS のデフォルト値を表 3-3 に示す。

表 4-3 OS ごとの TCP ウィンドウサイズデフォルト値

OS	受信ウィンドウサイズ	送信ウィンドウサイズ
Linux2.2	32KB	32KB
FreeBSD2.2.8	16KB	16KB
Solaris8	24KB	16KB

各 OS につき BLER 毎に ftp の転送を 10 回行い、RTO が発生した回数を測定した。図 4-6 に誤り率に対する TCP 実装毎の再送タイムアウト発生度数を示す。Linux は平均して RTO 発生が見られる。Solaris はばらつきがあるもののやはり RTO 発生が見られる。FreeBSD は RTO 発生がわずかである。図 4-6 より FreeBSD では RTO が起りにくいことが分る。実装を参照すると、Linux における RTO の下限は 200 [ms], 初期値 3 [s], 最大値が 120 [s] であるのに対し、FreeBSD の RTO の下限は 1 [s], 初期値 3 [s], 最大値が 64 [s] となっている。さらに BSD の RTO が極めて保守的である理由として以下が指摘されている [69]。即ちどのセグメントに対するものかを問わずに各 Ack の到着によって RTO タイマがリスタートされるため、RTO 値が RTT 分だけ長くなるのと等価となり、タイムアウトが発生しにくくなる。図 4-6 に同じ条件で誤り率に対するスループットを示す。図より、RTO の発生によってスループットが低下することが分る。

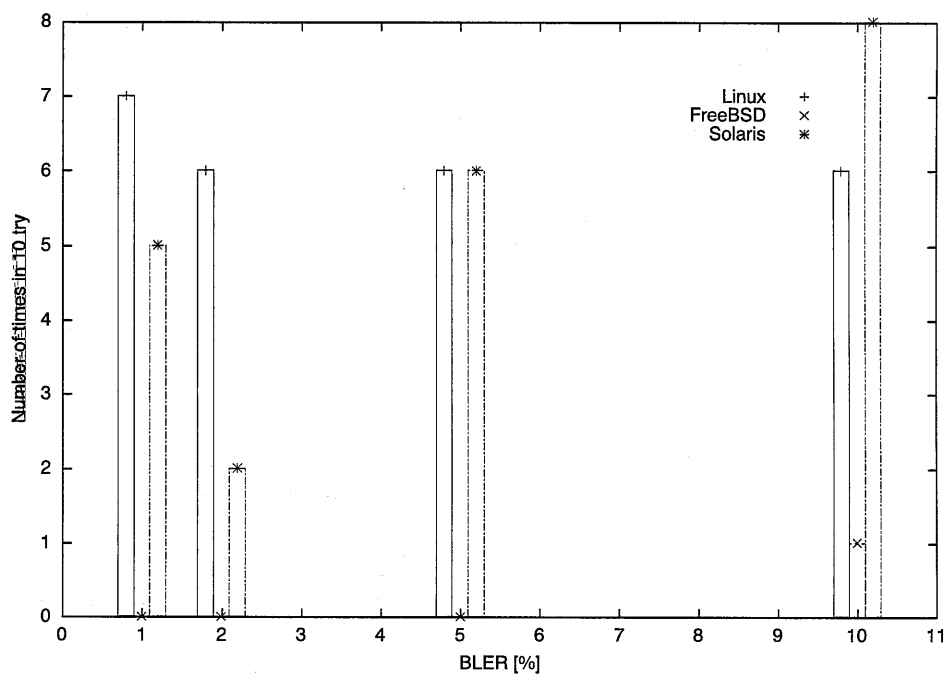


図 4-6 RTT 発生回数 vs. BLER (W-CDMA シミュレータを用いた測定)

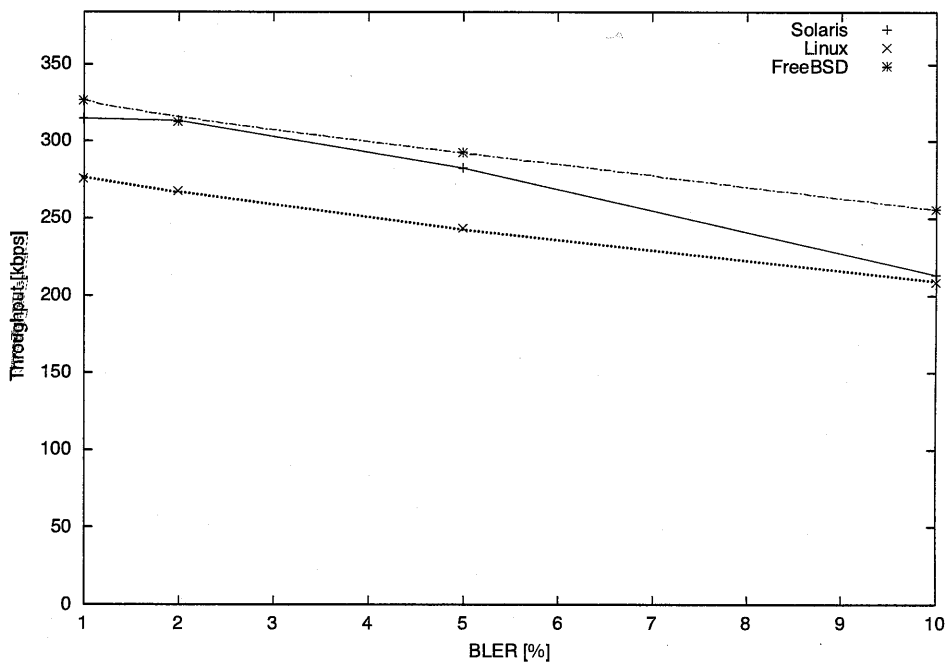


図 4-7 スループット vs. BLER (W-CDMA エミュレータを用いた測定)

図 4-6, 図 4-7 より検証対象中で最も保守的な BSD に比較して Linux の再送タ

タイムアウト機構の遅延ジッタ耐性が低いことが分った。また Linux はソースコードが公開されており、実装を調べることは容易である。そこで以後の評価においては Linux を基準とする。具体的には、シミュレータに組み込まれている 4. BSD-Lite 準拠の TCP の再送タイムアウト部分を、Linux と同様のタイムアウト処理が行われるように変更した。

4.5.3 遅延ジッタ抑制と伝送効率のトレードオフの評価

本節では遅延ジッタ抑制と伝送効率についてシミュレーションを用いて考察する。4.4 章で議論したとおり、Timer_Status_Prohibit の設定は、リンク層における遅延ジッタ抑制と伝送効率の間のトレードオフの調整に他ならない。

まず、TCP のスループット低下要因として Timer_Status_Prohibit の変化に対する STATUS PDU 数と TCP の RT0 発生数を図 4-8 に示す。伝送誤りによる PDU ロスがある時、Timer_Status_Prohibit が小さい場合には PDU ロスを検知する度に STATUS PDU が送出され再送が起こる。従って、遅延ジッタは小さいもののリンク層での伝送効率が低下している。Timer_Status_Prohibit が大きい場合には、PDU ロスがあっても Timer_Status_Prohibit 期間内は STATUS PDU が送出されず、リンク層での伝送効率は向上するものの遅延ジッタは大きくなる。図 4-8 において STATUS PDU 数は Timer_Status_Prohibit が大きくなるにつれて同一 BLER において減少し、リンク伝送効率が向上していることが分る。また、遅延ジッタによる TCP の RT0 発生数は Timer_Status_Prohibit が大きくなるにつれて増加し、特に 200 [ms] 以降から増大している。

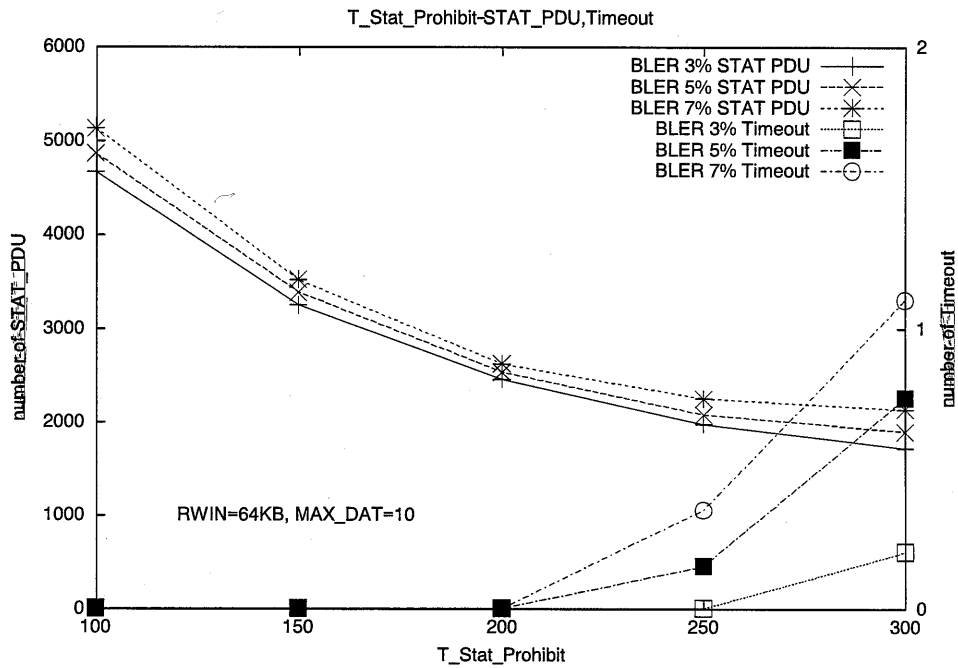


図 4-8 STATUS PDU 数, RTO 数 vs. Timer_Status_Prohibit (Opnet シミュレーション)

次に, Timer_Status_Prohibit の変化と TCP スループットの関係を図 4-9 に示す. 前記の通り図 4-9 の左側で TCP スループットが低下しているのは小さな Timer_Status_Prohibit によるリンク層での伝送効率の低下によるものである. 図 4-9 の右側で TCP スループットが低下しているのは遅延ジッタによる spurious timeout 発生が原因である.

図 4-9 において 200 [ms] にピークがある. TCP スループット最大化の観点から, Timer_Status_Prohibit は 200 [ms] が最適値であることが分った. 以後, Timer_Status_Prohibit の設定値を 200 [ms] として評価を進める.

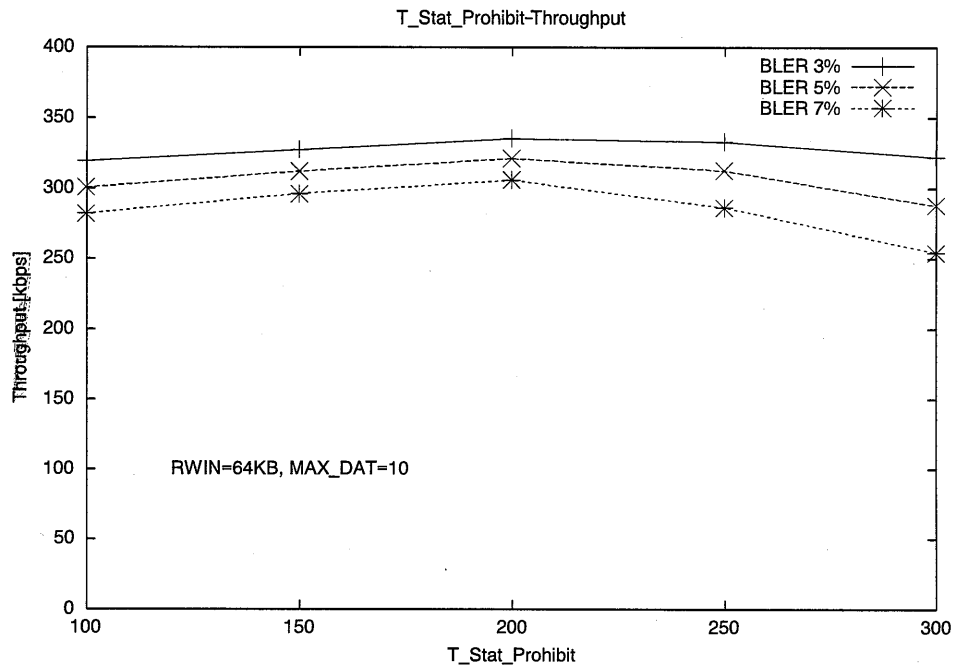


図 4-9 スループット vs. Timer_Status_Prohibit (Opnet シミュレーション)

4.5.4 リンク層再送動作の粘り強さの評価

本章ではリンク層再送動作の粘り強さについてシミュレーションを用いて考察する。再送動作の粘り強さと TCP スループットの関係を示すため、リンク層再送における再送回数の最大値を指定する MAX_DAT パラメータとスループットの関係を図 4-10 に示す。例えば MAX_DAT 値が 2 であればリンク層は失われたひとつの PDU を 2 回まで再送し、そこで失敗するとその PDU が構成する IP パケット全体を破棄する。図 4-10 に示す結果から 5 回程度の再送で十分であることが分った。

図 4-10 に下り TCP セグメントロス率を示した。例えば MAX_DAT が 3 の時にはリンク層で十分な再送が行われず、下り TCP セグメントは 3~4% のロス率があり、TCP スループットもそれぞれの BLER において 50~100 [kbps] の低下が見られるが、MAX_DAT を 5 以上に設定しリンク層での再送を充分行えば TCP スループットの低下は見られない。従って W-CDMA においてもリンク層での再送を十分に行うことが重要であることが確認された。

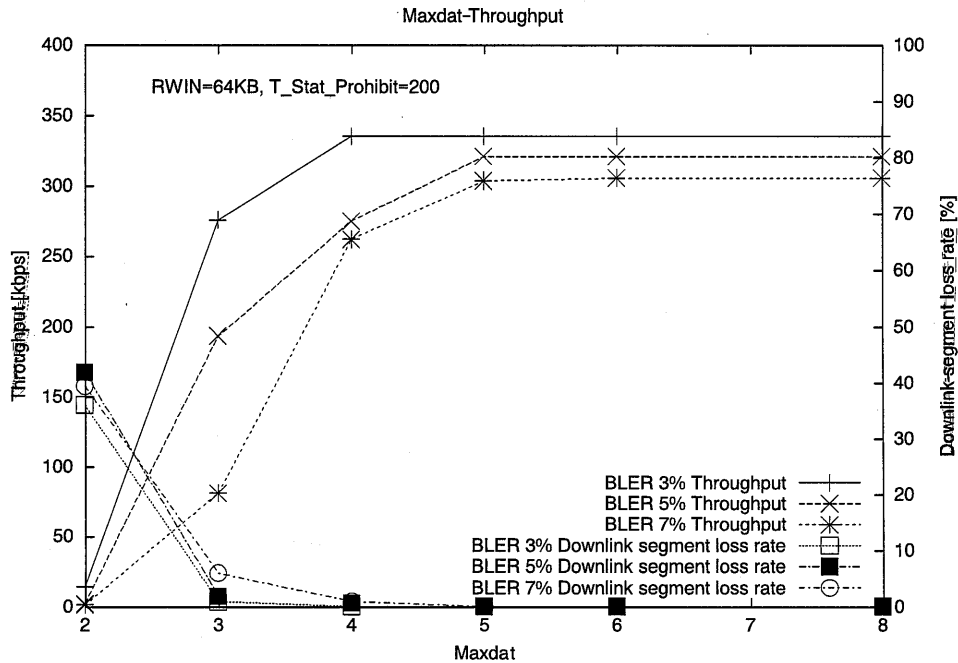


図 4-10 スループット, 下り TCP セグメントロス率 vs. MAX_DAT (Opnet シミュレーション)

4.5.5 TCP 受信ウィンドウサイズの評価

本節ではシミュレータを用いて TCP 受信ウィンドウサイズを変化させ、TCP トラフィックのスループットの変化を観察することで帯域幅遅延積を反映した適切な TCP 受信ウィンドウサイズの大きさを調べる。BLER 毎の TCP 受信ウィンドウサイズとスループットの関係を図 4-11 に示す。シミュレータにおいて送信ホストは受信ウィンドウサイズに合わせてセグメントを送信する。無線区間のエラーが増えるに従いスループットが低下する。TCP 受信ウィンドウサイズが 48-64KB でスループットはほぼ上限に達する。通常の OS でデフォルト設定されている TCP の受信ウィンドウサイズは 8-16KB が多い。W-CDMA を始めとする第 3 世代移動通信ネットワークのような高遅延ネットワークに対してその性能を引き出すためには受信ウィンドウサイズを広げる必要がある。しかし、ウィンドウサイズが大きいほど輻輳を発生させ得る機会が増えることになる。そのためリンクの帯域幅遅延積を反映した上記の 48-64KB が最適値であることが分った。

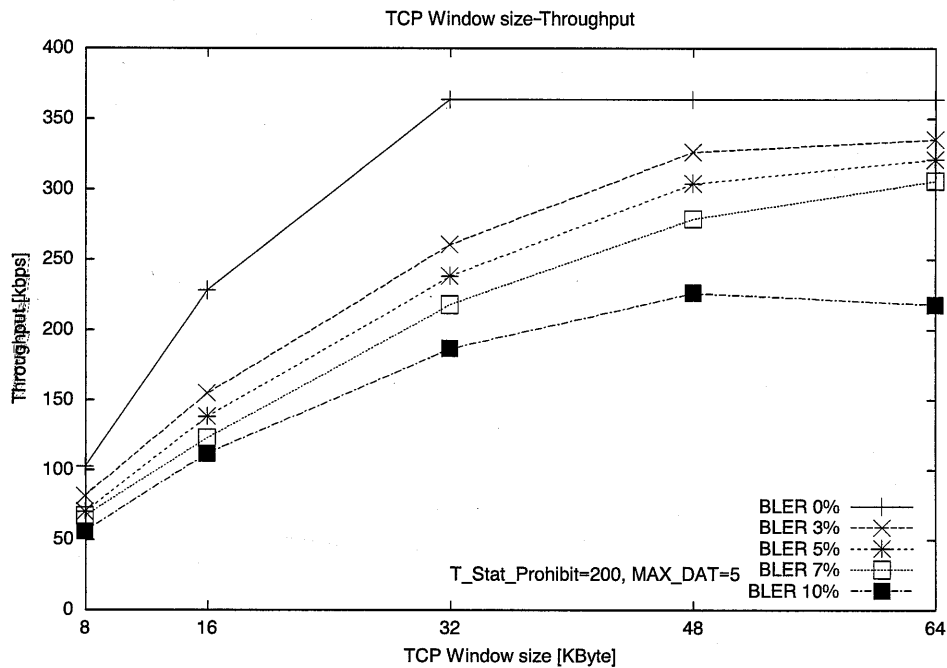


図 4-11 BLER ごとのスループット vs. TCP 受信ウィンドウサイズ (Opnet シミュレーション)

4.6 おわりに

第3世代移動通信ネットワークの代表的な方式である W-CDMA のリンク層再送動作を詳細に検討し、リンク層における遅延ジッタ抑制と伝送効率のトレードオフ関係を分析して、評価すべきリンク層および TCP の動作パラメータを明確にした。次にシミュレーションによりそれぞれのパラメータの最適値を求めた。

現実の TCP 実装間のタイムアウトの振舞いの違いに着目し、ネットワークエミュレータを用いた遅延ジッタ耐性の検証結果から、遅延ジッタ耐性が低く、ソースコードによる調査の容易さから Linux を選び、以降のモデルとした。

リンク層で遅延ジッタの抑制が必要なのは、トランスポート層の TCP とリンク層のそれぞれの再送機構の併用から、遅延ジッタによる TCP 再送タイムアウトが発生し、無駄な再送が行われるという望ましくない相互作用が起りえるためである。リンク層における遅延ジッタ抑制と伝送効率の間にトレードオフがあり、その調整パラメータとして RLC の Timer_Status_Prohibit を使い、シミュレーションによって最適値 200 [ms] を明らかにした。

W-CDMA においてはリンク層 ARQ での再送が有効であった。リンク層再送回数を変化させることで評価し、対象の BLER0~10%では5回の再送で十分であるこ

とが分かった。

W-CDMA を始めとする第 3 世代移動通信ネットワークのような高遅延ネットワークに対しては OS のデフォルト設定に対して受信ウィンドウサイズを広げる必要がある。しかし、ウィンドウサイズが大きいほど輻輳を発生させ得る機会が増えるため、

リンクの帯域幅遅延積を反映した 48-64 [KB] が適正值である。

本論文の議論は TCP による信頼性のあるストリーム伝送を目的としているが、VoIP (Voice over IP) やストリーミングのようなリアルタイム伝送においては再送機構への要求が異なる [70], [71] ため、今後はそれらに最適なプロトコルパラメータの検討を行いたい。更に、無線 LAN などの異なるリンクを扱うことができるように本研究で用いた手法を一般化してゆきたい。

第5章 高速インターネットアクセスのためのステルス型ゲートウェイ

5.1 はじめに

第3世代移動通信ネットワーク (IMT-2000) の商用サービスとして W-CDMA をベースとした FOMA 等の商用サービスが既に始まっている。FOMA では、高速パケット交換サービス (上り最大 64kbps, 下り最大 384kbps) が提供されており、従来に比較してより高速なインターネットアクセスが可能となっている。この高速移動パケット通信ネットワークの特性として、無線区間を含むネットワーク内伝送遅延時間が、伝送帯域幅に比較して大きい (すなわち帯域幅遅延積が大きい) ことが分かっている。このような特性を持つ移動通信ネットワークにおいて、帯域幅遅延積が比較的小さい有線ネットワークを前提に設計された TCP を利用したアプリケーションが高速移動通信ネットワークの特徴を生かすことができず、十分な性能 (スループット, 応答時間) を得られないことが明らかになっている [30]。

プロトコル最適化による性能改善の試みとして、無線区間と有線区間の TCP コネクションを分離する Split TCP [72], [73] や、PEP (Performance-Enhancing Proxy) [4, 5] がある。しかし、これらは TCP コネクションをプロキシで終端させることが前提となっており、TCP コネクションは、クライアント-プロキシ間とプロキシ-サーバ間でそれぞれ独立に設定・管理され、一方の End のアドレス情報 (例えば、IP アドレス, ポート番号, 等) が他方の End で認識できなくなる。すなわち、End-End でアドレス情報の透過性はなくなる。このような状況においては、インターネットで提供される各種サービスの中で利用できないものが発生する可能性がある。また、アプリケーションプロトコル (以下 AP プロトコルと略す) には種々のものがあり、今後も新サービスの登場に伴い、新しいプロトコルが開発されることになる。このため、プロキシでは任意の AP プロトコルを使える仕組みを用意する必要があるが、現状のプロキシは AP プロトコルを限定して実装しており、汎用性がない。

一方、End-End に TCP を適用することを前提とした TCP のプロファイルとして W-TCP (TCP over 2.5G and 3G Wireless Networks) が提案されている [21], [30]。この場合、例えば W-CDMA パケットネットワークに接続するためのパソコン等のドライバソフトウェアの配布と併せて TCP プロファイル設定ソフトウェアを配布することなどによって、クライアントを比較的容易に W-TCP に変更可能で

ある。しかし、インターネット上に無数に存在するホストのすべてにこのプロファイルセットを適用することは非現実的である。

上記 2 つの問題を解決するためには、クライアントとインターネット上のサーバ間で W-TCP と TCP を変換し中継するゲートウェイ（以下、GW と略す）が必要となる。GW では、W-TCP と TCP の変換を行いつつ、End-End レベルでの IP パケットの透過性と任意の AP プロトコルを使える仕組みが必要であるが、これらを実現したものはまだない。

本論文では、最初に W-CDMA パケットネットワーク等の高速移動通信ネットワークを経由してインターネットアクセスを高速に行うためのプロトコル手法の概要について述べる。次に、上述した課題を解決するため、IP アドレス等の透過性を保ちつつ、W-TCP と TCP の相互変換と HTTP (Hypertext Transfer Protocol) リクエストパイプラインング [76] を含む任意の AP プロトコルの中継を可能とするステルス型 GW を提案する。更に、提案したステルス型 GW 方式の試作による実証評価結果について述べる。これらの結果、ステルス型 GW 方式により End-End のアドレス情報の透過性を維持したまま、スループット及び応答時間をそれぞれ 2-3 倍程度向上すること、及び GW に於ける中継処理時間が無視できるほど小さいことを明らかにし、提案方式が実用的なものであることを示す。

5.2 インターネットアクセスの高速化のためのプロトコル手法の概要

FOMA パケット交換サービスでは、高速パケット交換サービス（上り最大 64kbps, 下り最大 384kbps）が提供されており、またそのパケット遅延時間（RTT: Round Trip Time）は実測で平均 600msec 程度であり、電波の状態によって大きく変動する。このような環境で Web アクセスを含む各種インターネットアプリケーションの高速化を行うために必要なプロトコル（IETF 等で標準化されているものを前提としている）のうち、基本的なプロトコルである TCP と HTTP の検討状況について概説する。

(1) W-TCP

W-CDMA パケットネットワークの特徴は高速・高遅延であり、これを有線ネットワークを前提に開発された TCP にそのまま適用すると回線の使用率（スループット）が低下することが課題となる。このような特性を有する無線ネットワークにおける TCP の最適化のため様々な解決方法が提案されている [77], [78]。

これらの手法は、スロースタート期間の短縮のために輻輳ウィンドウの制御方法の変更を行うなど、いずれも現在流通している TCP の実装の大幅な変更が必要となったり、既存 TCP との相互接続性が損なわれる可能性がある。一方、現状の各種 TCP の実装に適用可能であり、かつ、既存の TCP との相互接続性を考慮した最適化手法を取りまとめたのが W-TCP であり、IETF で標準化されている [21].

W-CDMA パケットネットワークでは、無線区間で発生するパケットロスに対処するためデータリンクレベルで再送制御が行われ、TCP から見ると、あたかも RTT が増大したかのように見える。W-TCP で規定されている各種手法の中から、このような特性を持つ W-CDMA パケット網に TCP を適用するとき性能向上に特に有効と想定されるものを選択して利用することが提案されている (4 章参照)。具体的には、以下の TCP 関連パラメタを W-CDMA パケットネットワークの特性に合わせてチューニングする。

1) TCP バッファサイズの拡大

帯域幅遅延積に対して十分な広告受信ウィンドウサイズを確保するため TCP 受信ウィンドウサイズを 64KB まで拡大する [79].

2) 初期ウィンドウサイズの拡大

TCP コネクション確立後の転送初期のスループット向上のため送出量の拡大を図るために初期ウィンドウサイズを 3 セグメントまで拡大する [23].

3) 最大転送パケット長の拡大

輻輳ウィンドウは最大 TCP セグメント長 (MSS: Maximum Segment Size) を単位に管理されているが、スロースタート期間の短縮のためには MSS を長くすることが有効である。MSS はリンク毎の最大転送パケット長 (MTU: Maximum Transfer Unit) を基に決まるため、MTU は運用実績のある値で最大の 1.5KByte とする。

4) 選択的確認応答

ネットワークの輻輳などにより、パケットロスが発生したときの再送を効率よく行うために、選択的再送機構 (SACK: Selective ACKnowledgement) [21] を使用する。

(2) HTTP パイプラインニング

HTTP/1.1 では、パーシステントコネクションの利用が可能となっている。パ

一システムコネクションでは、1つの TCP コネクションの中で、Web オブジェクトの取得 (HTTP の Request-Response) を順次連続して行うことが可能となる。リクエストパイプラインはパーシステントコネクションの利用を前提とし、1つの TCP コネクションの中で、複数の Request を Response の受信を待たずに一括して連続的に送信することができる (図 5-1)。リクエストパイプラインは、特に RTT の大きいネットワークで用いた場合にその効果が大きいと実測評価されている [80]。

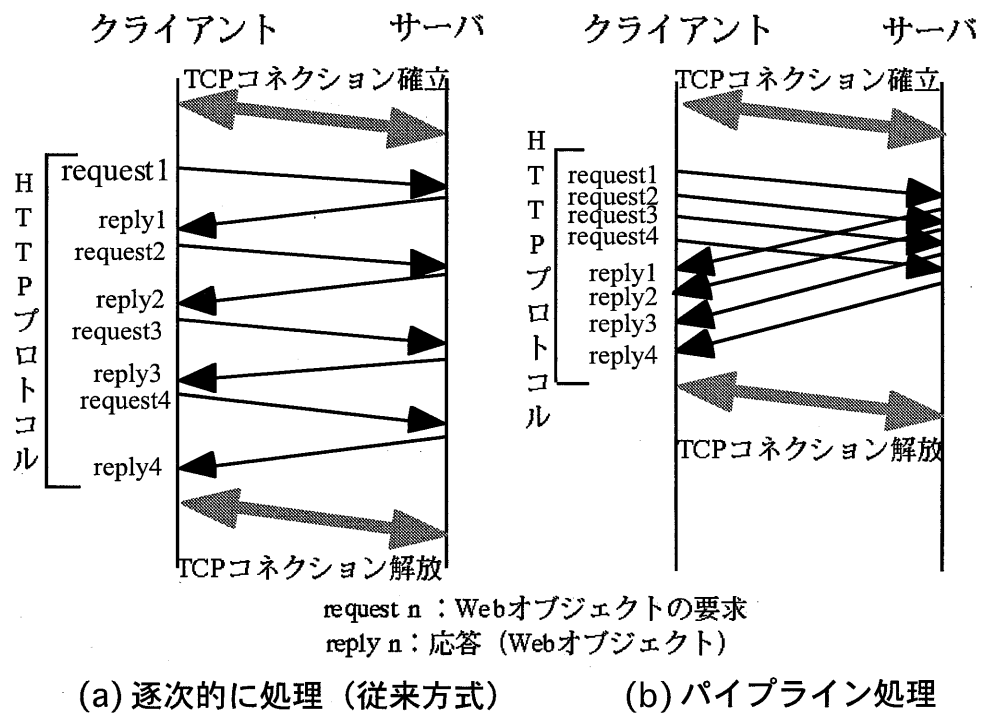


図 5-1 HTTP/1.1 パイプライン処理の概要

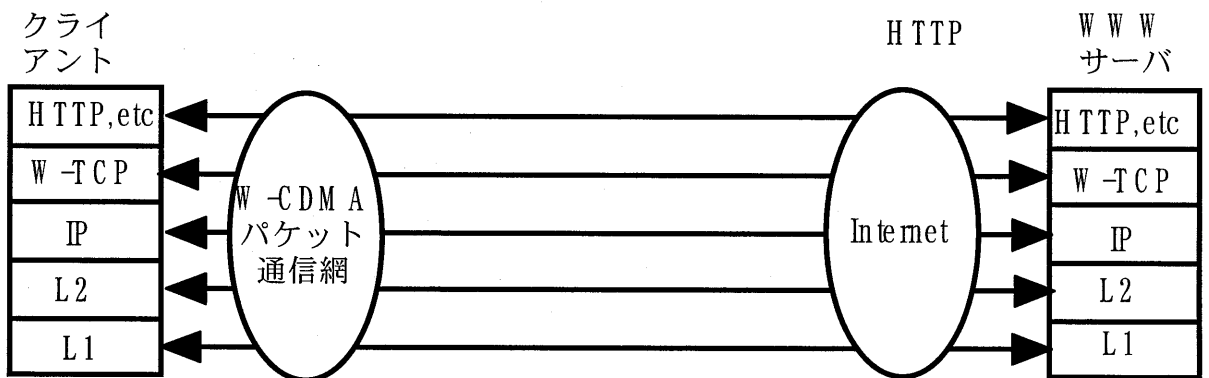
5.3 ステルス型 GW 実装方式の提案

5.3.1 基本アーキテクチャと GW への要求条件

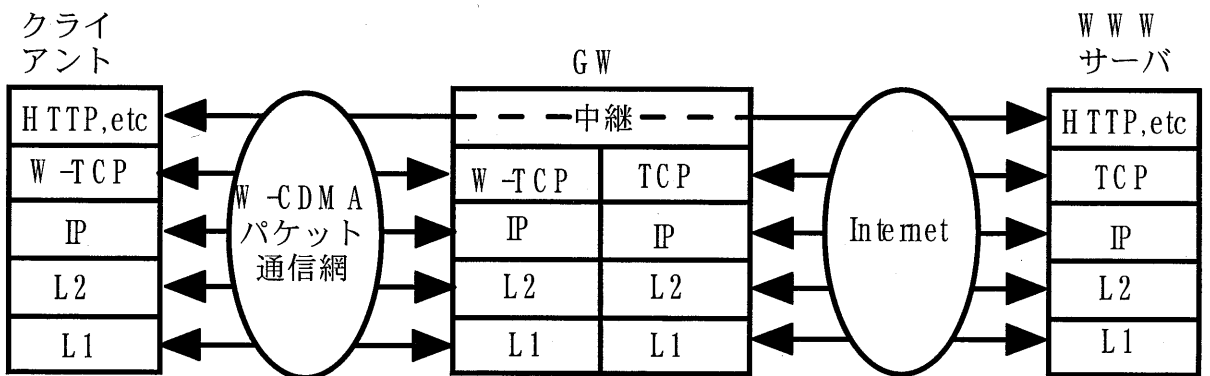
(1) 基本アーキテクチャ

5.2 章で述べたプロトコルを実装する基本アーキテクチャとして、End-End でこれらを実装する方式と両 End の中間に GW を設置する方式がある (図 5-2, 表 5-1)。W-TCP は End-End の通信モデルを前提とし、IETF で標準化された拡

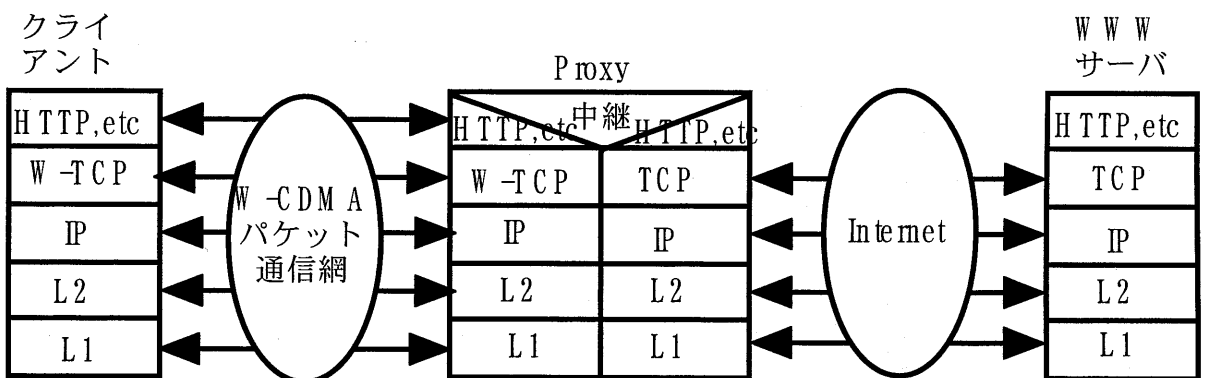
張技術のみを利用しているが、現在市場に出荷されている各種 OS の TCP の実装は初期値で W-TCP のプロファイル (5.2 章で示した TCP パラメタ) が有効でない OS も多数存在することが分かっており、OS の TCP パラメタの設定変更が必要になる。クライアント側は、W-CDMA パケットネットワークへ接続するために必要となるドライバソフトウェアのインストールに合わせて、W-TCP への設定変更が比較的容易に実現可能である。しかし、インターネットに無数に存在するサーバに対して W-TCP を適用するには、OS のパラメタ変更や最新版への改版を待たねばならず、現実的にはすべてのサーバ側 OS の設定変更は不可能である。以上の理由により、本論文では GW 方式を採用することとした。



a) End-Endモデル



b) GWモデル (提案方式)



c) (参考) Proxy方式モデル

HTTP : HyperText Transfer Protocol

W-TCP : TCP over 2.5G and 3G Wireless Networks

図 5-2 基本アーキテクチャモデル

表 5-1 基本方式の特徴

	APプロトコルの透過性	アドレス情報の透過性	W-TCPの適用
End-Endモデル	○	○	× (すべてのサーバへの適用は困難)
GW モデル	○	○	○
(参考) Proxyモデル	× (APプロトコルがスプリットされる)	× (TCPがスプリットされる)	○

(2) GW への要求条件

GW で実現すべき機能の要求条件を整理する。

1) W-TCP と TCP の変換

クライアント側は W-TCP に設定されているという前提で、GW で W-TCP と TCP を変換する。

2) 各種アドレスの透過変換処理

GW でプロトコル変換処理を実施すると、IP アドレスや TCP ポート番号等のアドレス情報も同時に変換される場合があり、例えば、サーバからは、クライアントの IP アドレスが解らないことになる。このことが、サービスによっては大きな制約になる可能性がある。このため、クライアント側及びサーバ側から見て、互いに直接通信しているように見做せることが重要であり、GW では、アドレス情報の透過性を保証する必要がある。

3) AP プロトコルの透過性

HTTP パイプラインングをはじめとして、任意の AP プロトコルの中継を可能とするためには、TCP で運ばれる情報をそのまま中継できる必要がある。

5.3.2 ステルス型 GW 実装方式

移動通信ネットワークや衛星回線などの RTT の大きなネットワークを経由したインターネットアクセスを効率よく行うための GW 実装の研究例 [81] - [83] はいくつかあるが、前節で述べた要求条件を満たす GW の実装例はまだない。このような要求条件を実現する GW は、IP アドレス等のアドレスの透過性を実現し、両 End のホストからは認識する必要がないため、本論文では「ステルス型 GW」

と呼ぶ。ステルス型 GW の特徴は、クライアント及びサーバからはあたかも End-End で通信しているように見做せ、かつスループット及び応答時間の向上が図れることである。このため、サーバ及びクライアント側では、GW に関する情報を一切事前に設定する必要がない利点がある。

ステルス型 GW では、W-TCP と TCP との変換処理、及び AP プロトコルのトランスペアレントな中継を実現する。更に、IP アドレス/TCP ポート番号変換処理によりアドレス情報の透過性を実現する。これらの変換中継機能を GW で実装する方式として以下の方式がある（図 5-3、表 5-2）。

方式 1：GW でアプリケーション (APPL) として実現する

方式 2：OS (カーネル) で実現する

方式 1 は、方式 2 と比較して、アプリケーションであるためソケットインタフェースを経由した制御および情報の受け渡しがあるためオーバーヘッドが大きいが、保守・運用性、移植性に優れ実用的であるため、これらを重視し方式 1 を採用することとした。

以下では、方式 1 を前提にステルス型 GW の特徴的な機能であるアドレス透過変換方式と、TCP コネクション確立方式について述べる。

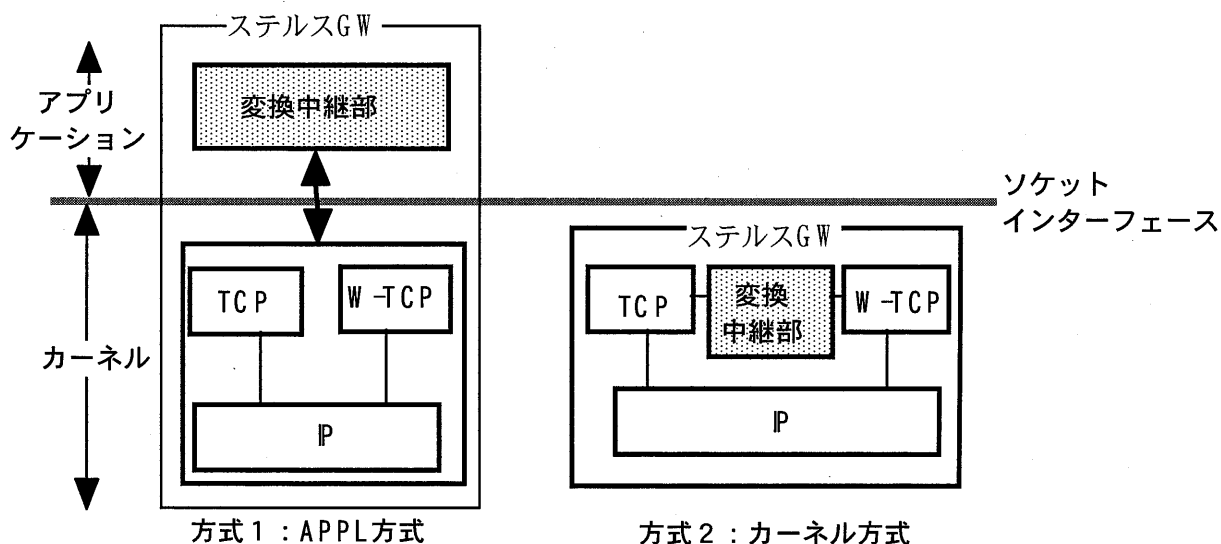


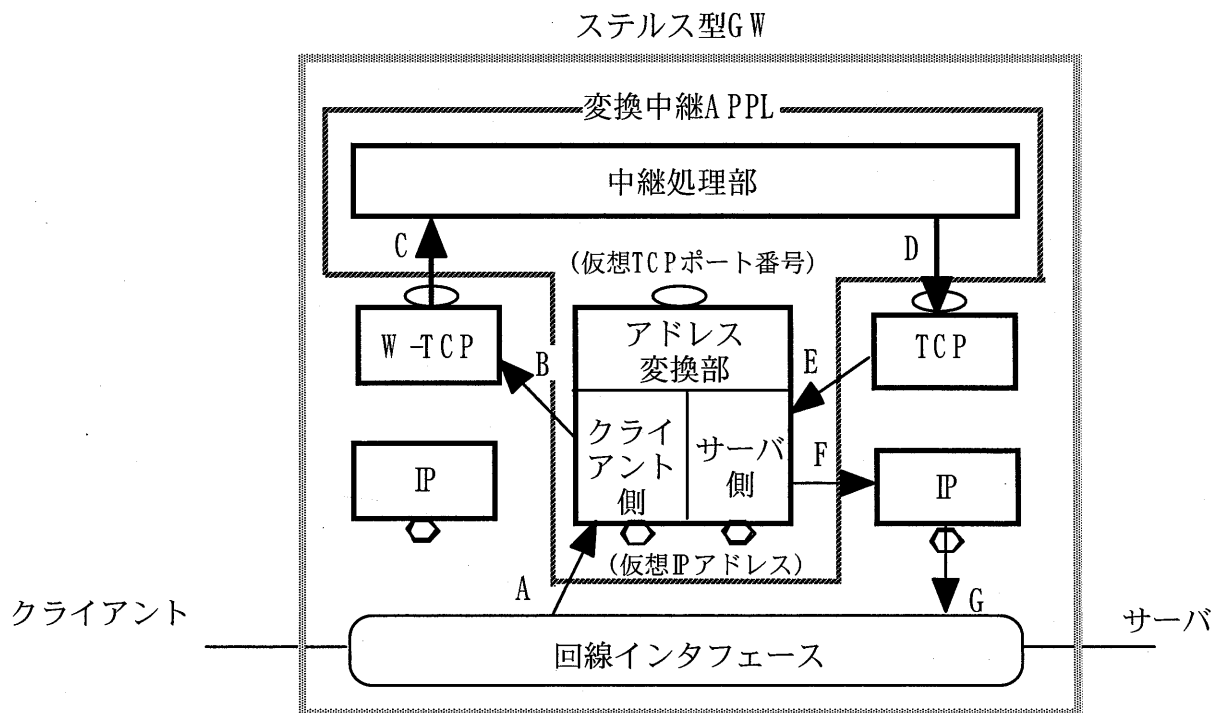
図 5-3 GW 変換中継部の実装方式

表 5-2 GW の変換中継部の実装方式の比較

	性能	保守性・運用性	移植性（流通性）	開発規模・期間
方式 1	× (オーバヘッド大)	○	○	○
方式 2	○	× (カーネルの知識が必要)	× (カーネル種別毎に必要)	△ (カーネル構造に依存)

5.3.3 アドレス透過変換方式

提案するステルス型 GW では End-End レベルでの IP アドレス及び TCP ポート番号の透過性を実現するために以下の透過変換処理方式を実現する。透過変換処理は IP パケットの透過処理を行うアドレス変換部、TCP コネクション管理・TCP セグメントの中継処理部（すなわち、W-TCP と TCP の相互変換のための中継処理）、プロトコル処理部（TCP, W-TCP, IP）からなる（図 5-4）。



備考1: A-HはIPパケットをGWで受信してから透過変換処理を行い送信するまでの処理の流れ

2: 各機能部が持つアドレス情報

○はTCPポート番号, □はIPアドレスを示す

アドレス変換部は、1つの仮想TCPポート番号と、2つの仮想IPアドレスを持つ

図 5-4 透過型アドレス変換方式の構成

アドレス変換部は、一方の回線経由で受信した IP パケットの IP アドレス、及び TCP ポート番号を記憶すると共に、GW 内部での中継処理のため、それぞれの GW 内部処理用アドレス情報に変換し、中継処理部に渡す。中継処理部で中継された IP パケットは、再びアドレス変換部に渡され、記憶されたアドレス情報を基に、GW 内部処理用アドレスからオリジナルアドレス情報に再び変換され、他方の回線経由で送出される。

これらのアドレス変換処理は、TCP コネクション対毎に行う必要がある。このため、TCP コネクション対を識別するためにアドレス変換部に付与する仮想 TCP ポート番号を使用する。また、受信した IP パケットがクライアント側あるいはサーバ側なのかを識別するためにアドレス変換部にクライアント側/サーバ側に対応する二つの仮想的な IP アドレスを付与する。アドレス変換に使用される

各種アドレス情報をまとめて表 5-3 に示す。

表 5-3 アドレス変換で使用する各種情報

TCPコネクション 対識別子	IPアドレス	TCPポート番号
アドレス変換部 仮想TCPポート番号 (任意)	クライアント (任意)	クライアント (任意)
	サーバ (任意)	サーバ (AP固定)
	GW クライアント側 (固定)	GW クライアント側 (固定)
	GW サーバ側 (固定)	GW サーバ側 (任意)
	アドレス変換部クライ アント側 (固定)	アドレス変換部 仮想TCPポート番号 (任意)
	アドレス変換部サーバ側 (固定)	

備考：網掛部がステルス型GW の中継処理部，アドレス変換部で新たに定義したアドレス情報

IPパケットの透過変換処理の具体的な手順をクライアント側ホストからIPパケットを受信し，サーバ側ホストに送り出すまでの例を以下に示す（図 5-4 参照）。

手順1：アドレス変換部（クライアント側）でIPパケット受信（図 5-4 の A）

IP アドレス変換：送信元 IP アドレス→仮想 IP アドレス（クライアント側）

宛先 IP アドレス→GW の IP アドレス（クライアント側）

TCP ポート番号変換：送信元 TCP ポート番号→仮想 TCP ポート番号（TCP コネクション確立時は新規に取得する。以降，これをキーに各種アドレス情報を参照する）

宛先 TCP ポート番号→中継処理部の TCP ポート番号（クライアント側）

手順2：変換後の IP パケットを TCP/IP 処理部へ送信（図 5-4 の B）

手順3：中継処理部で中継（図 5-4 の C）

宛先 IP アドレス：仮想 IP アドレス（サーバ側）

宛先 TCP ポート番号：仮想 TCP ポート番号

手順 4：TCP 処理部へ送信（図 5-4 の D）

手順 5：アドレス変換部（サーバ側）で IP パケット受信，変換テーブルを参照し以下の処理を実行（図 5-4 の E）

IP アドレス変換：宛先 IP アドレス→サーバホスト IP アドレス

送信元 IP アドレス→クライアントホスト IP アドレス

TCP ポート変換：宛先ポート番号→サーバホストポート番号

送信元ポート番号→クライアントホストポート番号

手順 6：IP 処理部へ送信（図 5-4 の F, G）

備考：A→B：A 欄を B 欄で置き換えることを意味する

また，アドレス変換部では，アドレス変換した後に必要に応じて IP ヘッダと TCP ヘッダのチェックサムの再計算を行う。

5.3.4 TCP コネクション確立方式

TCP コネクションは，クライアント側とサーバ側で同期して確立する必要があるが，クライアントと GW 間の TCP コネクションが先に確立される従来方式では，サーバの障害などにより，サーバ側 TCP コネクション確立が失敗した場合においても，クライアントから HTTP リクエストが送出され，無効なパケット送出が発生する可能性がある（図 5-5-a）。

この現象を回避するため，クライアントからの TCP コネクション確立要求 (SYN) パケット受信後，クライアントへ応答 (SYN+ACK) パケットの送信を保留し，サーバ側の TCP コネクションの確立を先に行う方式を提案する。

提案方式では，クライアントへ SYN+ACK の送信を保留している間，クライアント側の TCP コネクション確立処理は待機状態とし，サーバ側の TCP コネクション確立処理が完了した時点で，クライアント側の TCP コネクション確立処理を再開する（図 5-5-b）。なお，サーバ側の TCP コネクション確立失敗時は，クライアントへ応答を破棄することによって TCP コネクションの確立を行わない。この場合，クライアントから無用な SYN 再送の発生の可能性があるが，ステル

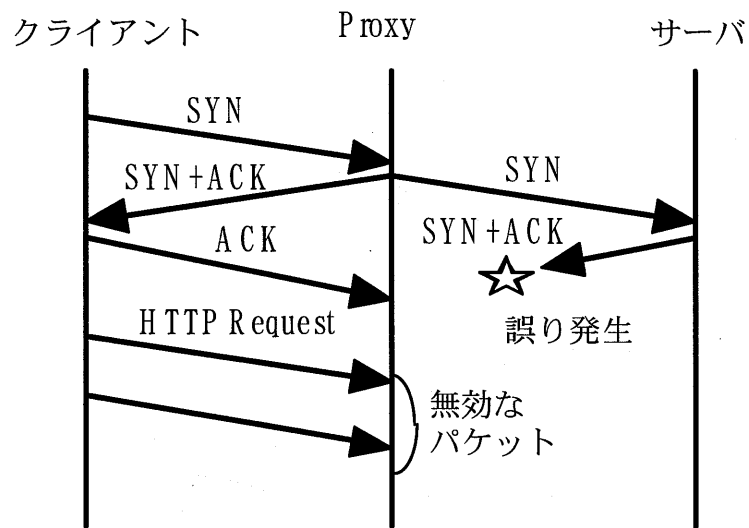
ス型 GW では、End-End の一方で発生している事象を可能な限り忠実に他方に伝えることを基本としているため、受信した SYN は全てサーバ側に送信する。また、サーバ側の TCP コネクション確立中に、クライアントの TCP コネクション監視タイマがタイムアウトし、クライアント側から SYN を重複受信する可能性がある。この場合、重複受信した SYN は廃棄し、最初の SYN 受信時に行ったサーバ側 TCP コネクション要求に対する応答を待つ。

具体的には以下の手順で TCP コネクションの確立を行う。

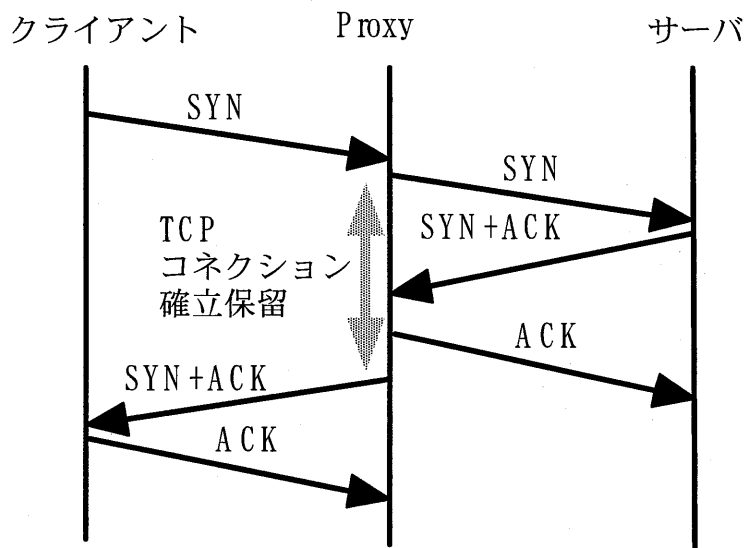
- a) クライアントからの SYN 受信後、タイマ（以降、Connect タイマと呼ぶ）をスタートし、サーバ側の TCP コネクション確立を行う。
- b) クライアントから再度 SYN を受信した場合、受信した SYN を廃棄する。
- c) サーバ側 TCP コネクション確立が失敗した場合、Connect タイマをストップし、処理を終了し、関連する情報をリセットする。
- d) サーバ側 TCP コネクション確立が成功した場合、Connect タイマをストップし、クライアント側の SYN 受信以降の TCP コネクション確立処理を行う。
- e) Connect タイマがタイムアウトした場合は、処理を終了し、関連するテーブル情報をリセットする。

この手順により、サーバ側の TCP コネクションは、クライアント側の TCP コネクションよりも先に確立されることになり、宛先不明のサーバへの TCP パケットがクライアントから送出されることを避けることが出来る。

なお、Connect タイマは、サーバ側の TCP コネクション確立要求がリトライアウトするまでの最大時間を考慮し、十分大きな値とする。



a) 従来方式 (既存のプロキシ)



b) 提案方式

図 5-5 TCP コネクション確立方式

5.4 実装評価

5.4.1 ステルス型 GW の試作

試作したソフトウェアの構成を図 5-6 に示す。試作したソフトウェアは、ア

ドレス変換処理を行う TCP-Agent と、TCP セグメントの中継の中継処理を行うプロキシ-APPL (Application) の 2つのプロセスと、IP アドレス変換前後の IP アドレス等と TCP コネクションの状態を保持するコネクション管理テーブルからなる。

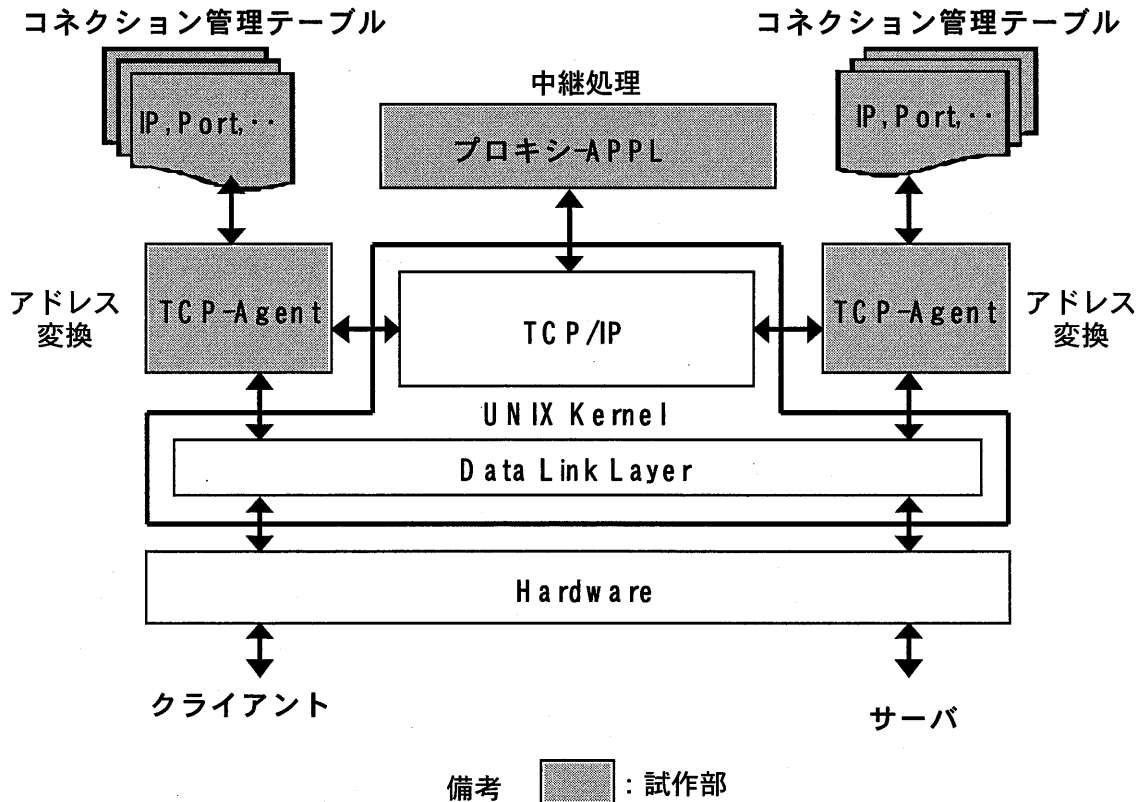


図 5-6 ステルス型 GW 試作ソフトウェア構成

(1) TCP-Agent

TCP-Agent は、GW 装置のネットワークインタフェースに入ってきたすべての IP パケットのキャプチャリングを行い、取り込み条件に一致した IP パケットのアドレス変換処理を行い、ソケットへ送信する。取り込み条件に一致しなかった IP パケットは破棄する。具体的な取り込み条件は、

- a) プロトコル番号が 6 (TCP)
- b) 宛先 IP アドレスが GW 装置のネットワークインタフェースの IP アドレス以外
- c) SYN であるか又は、SYN 以外であるが、送信元及び宛先 IP アドレス

対が既にコネクション管理テーブルに登録されている場合である。

SYN 受信時には、IP ヘッダの送信元 IP アドレス、宛先 IP アドレス、TCP ヘッダの送信元 TCP ポート番号、宛先 TCP ポート番号の変換処理を行い、これらの情報をコネクション管理テーブルに登録する。

仮想 TCP ポート番号は、TCP コネクション設定要求毎に 1 つ取得され、受信 IP パケットとコネクション管理テーブルを関係づけるキーとして使用するためユニークとなるよう管理する。すなわち、割り振られた仮想 TCP ポート番号は、その TCP コネクションが解放するまで再利用されないようにする。

(2) プロキシ-APPL

プロキシ-APPL は、5.3.4 節で記述した TCP コネクションの確立処理を行うと共に、透過 TCP-Agent から送信されてくるパケットを受信し、TCP で運ばれる情報のトランスペアレントな中継を行う。このことにより、通常の HTTP の処理に加え、HTTP リクエストパイプラインングの中継をはじめとして、任意の AP プロトコルの中継を可能としている。

5.4.2 評価環境

評価環境を図 5-7 に示す。W-CDMA パケットネットワークには、W-CDMA パケットネットワークを擬似するシミュレータを使用し、クライアント、ステルス型 GW、サーバを接続した。

クライアントには、Windows2000 に W-TCP のプロファイルを適用し、WWW ブラウザとして Internet Explorer 5 にリクエストパイプラインングのプラグインを実装したものをを用いた。WWW サーバには FreeBSD 4.4 (通常の TCP) 上で Apache (WWW サーバソフトウェア) を動作させたものをを用いた。また、ステルス型 GW は、商用 UNIX (ハードウェア : HP9000/CPU440Mhz x 2, OS : HP-UX 11.1) 上に構築した。W-CDMA パケット網シミュレータは上り 64kbps, 下り 384kbps とし、RTT に関しては、200msec から 1000msec まで変化させ、ステルス型 GW の効果を確認した。なお、本評価環境では、ネットワークの輻輳は考慮していないためパケットロスが発生しない。

実験方法は、Internet Explorer より 2Mbyte のバイナリファイルのダウンロードと、8kbyte の画像ファイルを 100 個貼り付けた HTML ファイルの取得の 2 通

りを、それぞれステルス型 GW を経由した場合と、しない場合の 2 通りのルートで測定を行った。

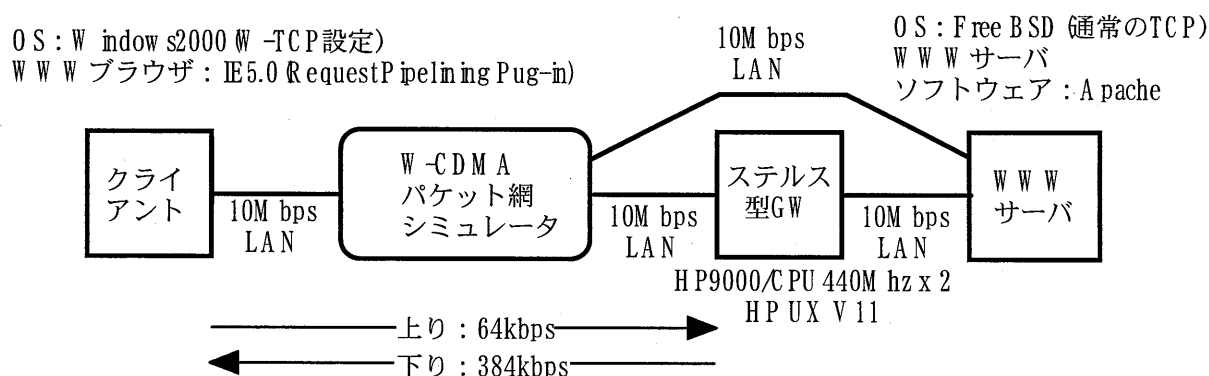
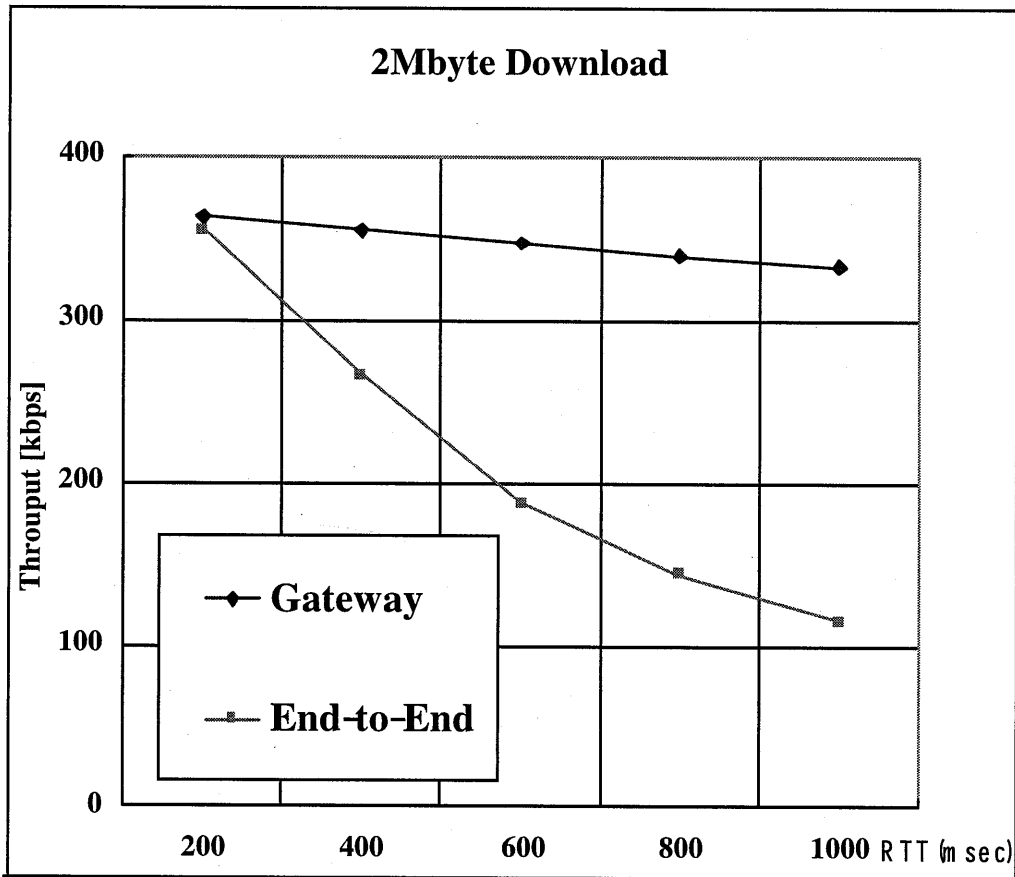


図 5-7 実証評価システム構成

5.4.3 評価結果と考察

1) 性能評価結果とその考察

2Mbyte のバイナリファイルのダウンロードを行った場合の RTT とスループットの関係を図 5-8 に示す。GW を経由しない場合 (W-TCP を適用しない場合), RTT が小さい場合 (200msec 程度) では, ほぼ回線の持つ帯域幅の理論限界値に近い値が得られているが, RTT が増えるに従い TCP の受信バッファの枯渇が発生し, 急激に低下する。例えば, FOMA パケットサービスの RTT の実測値は約 600msec 程度であり, W-TCP を適用しなければ FOMA の帯域幅を効率的に利用できていないことが分かる。一方, GW を経由し W-TCP と TCP の相互変換をした場合, RTT を 1000msec まで増やした場合でも 300kbps を越える値が得られており, GW を経由しない場合に比べ, 約 2-3 倍の性能改善が可能なことが分かる。なお, End-End に W-TCP を適用した場合も図 5-8 の GW 方式と同等の評価結果が得られており, GW のオーバーヘッドによるスループット低下はほとんど認められなかった。



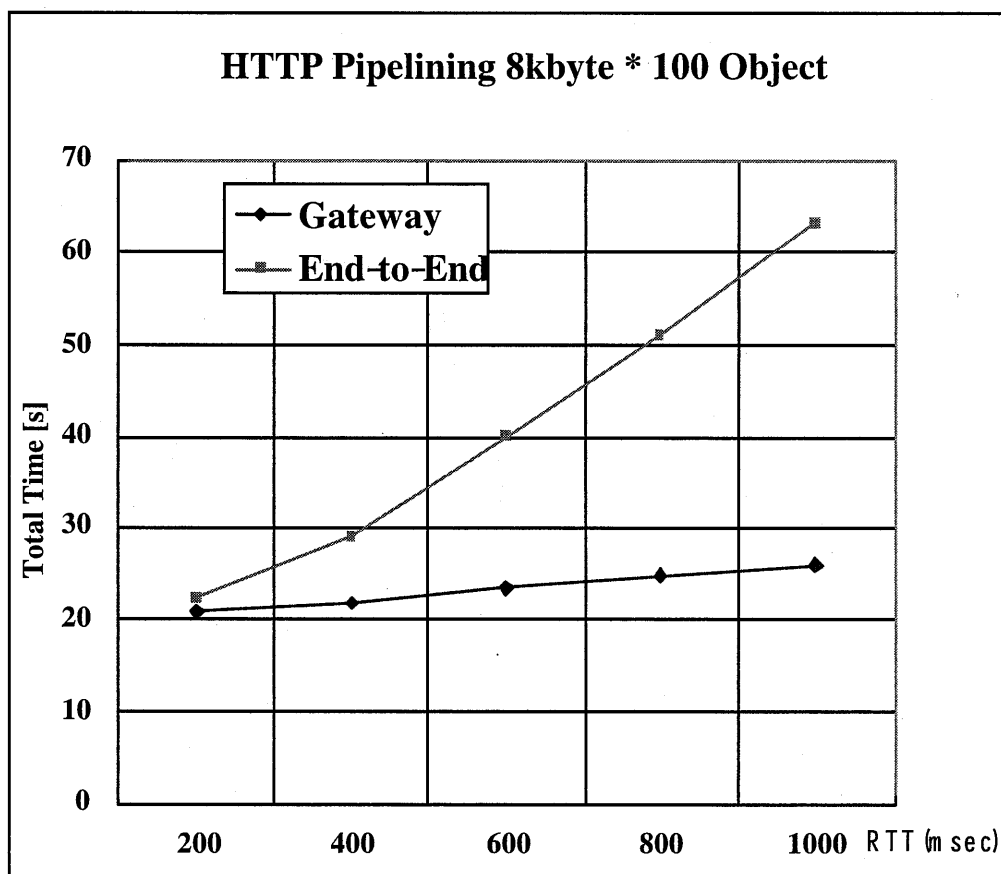
Gateway:ステルス型GW あり (W-TCP ON)
 End-to-End:ステルス型GW なし (W-TCP OFF)

図 5-8 HTTP によるファイルダウンロードのスループット

また、実際の W-CDMA パケットネットワークでは、ネットワーク輻輳等によるパケットロスが発生する事が想定されるが、W-TCP では、選択的再送機構を使用しており、より効果的に誤り回復が行われ、性能の改善率がより顕著になることが期待できる。

HTTP リクエストパイプラインングで HTML ファイルを取得した場合の遅延時間と応答時間（すべてのオブジェクトをダウンロードし表示し終るまでの時間）を図 5-9 に示す。RTT が小さい場合（200msec 程度）では、GW の効果はないが、RTT が大きくなるに従い、2-3 倍の性能改善が可能となることが解る。リクエストパイプラインングを適用するとバルクデータのダウンロードとほぼ同じ状況になり（本実験の場合は 800kbyte のファイルダウンロード相当）、W-TCP の受信バッファ拡大の効果が顕著に表れている。一般に、リクエストパイプライン

グは、RTT が大きく、Web のページを構成するオブジェクトのサイズが小さく、かつオブジェクト数が多い時に有効である。これに対して、W-TCP を適用するときには、RTT が大きく、転送データ量（オブジェクトサイズ x オブジェクト数）が大きいほど効果があり、リクエストパイプラインがより有効に機能することが予想できる。



Gateway:ステルス型GW あり (W-TCP ON)
 End-to-End:ステルス型GW なし (W-TCP OFF)

図 5-9 http によるホームページアクセスの応答時間

更に、GW を設置することのオーバーヘッドを測定するため、GW の CPU に負荷をかけた場合の、処理遅延時間（IP パケットを受信してから、回線に送り出すまでの時間）を測定した。処理遅延時間は、数 msec（CPU 使用率：0%）～数十 msec（CPU 使用率：70%）程度であった。このオーバーヘッドは、GW での変換中継処理部をカーネル内に実装する方式（5.3.2 節の方式 2）の方がより小さくなることが期待できるが、スループットの評価結果から APPL で実現する提案方式（5.3.2

節の方式 1) でも、ほぼ無視できるといえる。すなわち、提案方式は、欠点であるオーバーヘッドは無視できるくらい小さく、かつその特徴（保守性・運用性等に優れる）を十分生かすことが可能であることを意味している。

これらの評価結果により、提案したステルス型 GW 方式は、End-End レベルの IP パケットの透過性を実現しつつ、W-TCP により、大幅な性能（スループット、応答時間）の改善を可能とする実用的な方式であることが解った。

2) GW システム構成法に関する考察

GW 装置として実際のシステムを構築するためには、TCP だけではなく広くインターネットで使用されている UDP [84] や IPsec [85] 等の各種プロトコルに対応する必要がある。そのためには、GW 装置の前段にレイヤ 4 スイッチ (L4SW) を設置し、変換対象とする IP パケットのみをステルス型 GW に方路制御し、他の IP パケットは、2 台の L4SW を直接つなぐ回線を設定し、そこに方路制御することで変換対象としないことが実用的な構成と考える (図 5-10)。

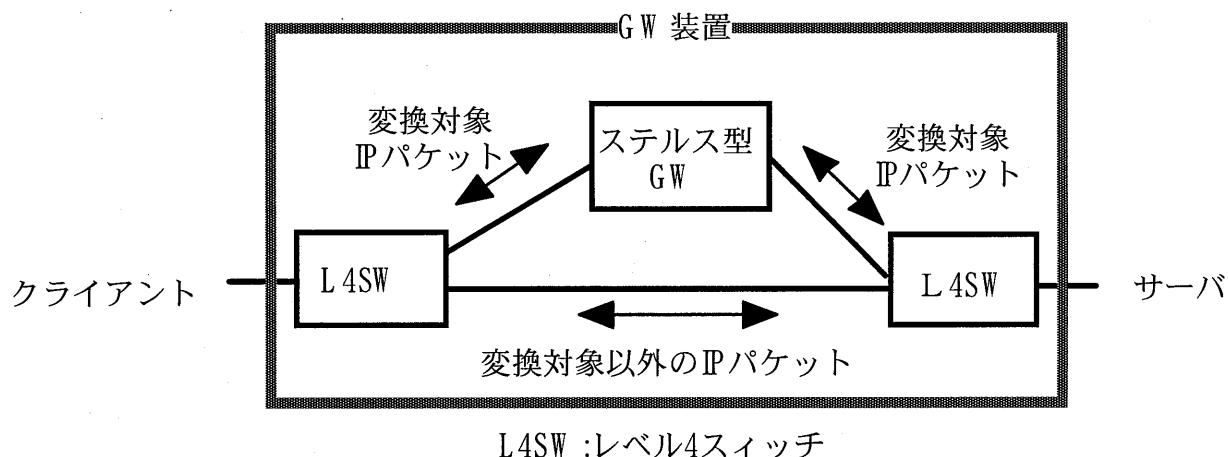


図 5-10 GW 装置の構成

また、W-CDMA ネットワークは大きく無線ネットワークとコアネットワークからなり、GW 装置の設置場所として、無線ネットワークの終端、コアネットワークの終端、等が考えられる。実用化に当たっては、GW 開発の簡素化・効率化を図ること、ネットワークの輻輳や故障が発生したときに容易に回避が可能なこと等、を考慮する必要がある。そのためには、コアネットワークから独立させ、コアネットワーク終端（インターネットとの接続ポイント）に設置するのが最

も適切と考えられる (図 5-11)。この場合、GW 装置にトラフィックが集中することになるため、負荷分散や信頼性が課題となり、実用化の際のシステム設計時に配慮する必要がある。

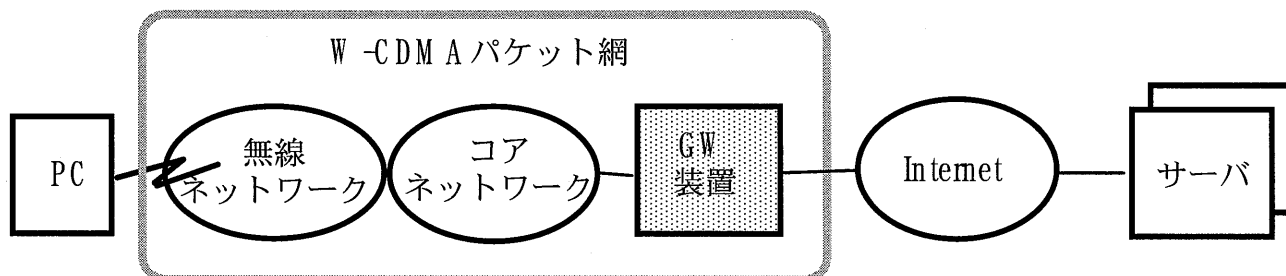


図 5-11 W-CDMA パケットネットワークへの導入位置

5.5 おわりに

本章では、W-CDMA パケットネットワークを介して、インターネットアクセスを高速に行う場合の GW 方式について述べた。具体的には、End-End でアドレス情報が透過となる W-TCP と TCP の相互変換を行うステルス型 GW 方式を提案すると共に、実装評価を行った。その結果、インターネット上に多数存在する W-TCP が適用されていないサーバに対するアクセスにおけるスループットと応答時間を、提案方式で 2-3 倍程度に改善できることを明らかにした。更に、GW での処理遅延時間は、数 msec (CPU 使用率：0%) ~ 数十 msec (CPU 使用率：70%) 程度であり、提案方式は、欠点であるオーバーヘッドは無視できるくらい小さく、かつその特徴 (保守性・運用性等に優れる) を十分生かすことが可能である実用的な方式であることを明らかにした。

実際の GW の運用に際しては、1つの GW でいくつまでの TCP セッションの同時運用が可能であるか等のスケーラビリティが重要である。このため、GW 装置のハードウェア/OS を含めたプラットフォームの性能と、同時にサポートできる TCP コネクション数の関係については、今後の課題としたい。同様に、実際の W-CDMA パケットネットワークでは、コアネットワークの輻輳等によるパケットロスが発生することが予想されるため、FOMA 等の実環境を利用した評価を今後実施することとしたい。

第6章 移動網を介したモバイル VPN 方式の提案と評価

6.1 はじめに

第3世代の移動通信ネットワークである IMT-2000 (W-CDMA) ネットワークの商用サービスが開始されたり、無線 LAN によるホットスポットサービスの本格的な普及により、モバイルコンピューティングにおけるインターネット接続環境は大幅に向上することが期待されている。また、近年頻発しているクラッキング事件によってユーザのセキュリティ意識はますます向上している。これらより、今後モバイル環境におけるインターネット VPN (Virtual Private Network) の利用が急速に増加することが予想される。固定ネットワークを前提とした VPN は既に実用になっているが、移動通信ネットワーク経由でサーバにアクセスするモバイル環境にそのまま適用しても、広帯域が特徴である W-CDMA ネットワークのポテンシャルを十分に引き出せない可能性等がある。このため、移動ネットワーク特有の性質が VPN に及ぼす影響を明確にし、その対策を検討することがモバイル VPN を普及させる上で重要である。

本論文では、最初にモバイル環境での VPN 利用の要件と課題を明確にする。具体的には、VPN を実現する際に標準的に使用されているプロトコル (IPsec) をモバイル環境に適用させるために考慮すべき課題、モバイル VPN ルータでのプロキシ機能 (TCP アクセラレータ機能) の必要性とそれを実現する際のセキュリティ上の課題、更に、信頼性向上のための仮想ルータ方式 (VRRP : Virtual Router Redundancy Protocol) をモバイル VPN ルータに適用する際の課題について明確にする。

次に、これらの課題を解決する方式として、キープアライブによらない新しい VPN セッション管理方式、TCP セッションハイジャックを防御するセキュア TCP アクセラレータ方式、及び VPN が実現するセキュリティ機能を低下させずにモバイル VPN を構成する冗長化されたルータ間 (現用/予備) の切り替えを短時間に効率的に行う方式を提案する。

更に、これらの方式のプロトタイプによる評価システムとその評価結果について述べる。移動ネットワークとして W-CDMA を想定した評価結果から、提案した VPN セッション管理方式がキープアライブなしでも VPN セッションを維持出来ること、セキュア TCP アクセラレータ方式により TCP セッションハイジャックを防止しつつ、スループットを最大 3 倍程度向上できること、冗長化された

ルータ間の系の切り替えが3秒程度で行われ、ほぼ実アプリケーションに影響を与えず実現可能なこと等を示す。これらにより、本文で提案するモバイル VPN 方式は、固定ネットワークとほぼ同じセキュリティレベルと移動ネットワークの特徴を最大限に活かす性能が得られ、モバイル環境に適用できる実用的なものであることを示す。最後に、残された課題と今後の検討計画について述べる。

6.2 VPN の概要

6.2.1 VPN の特長

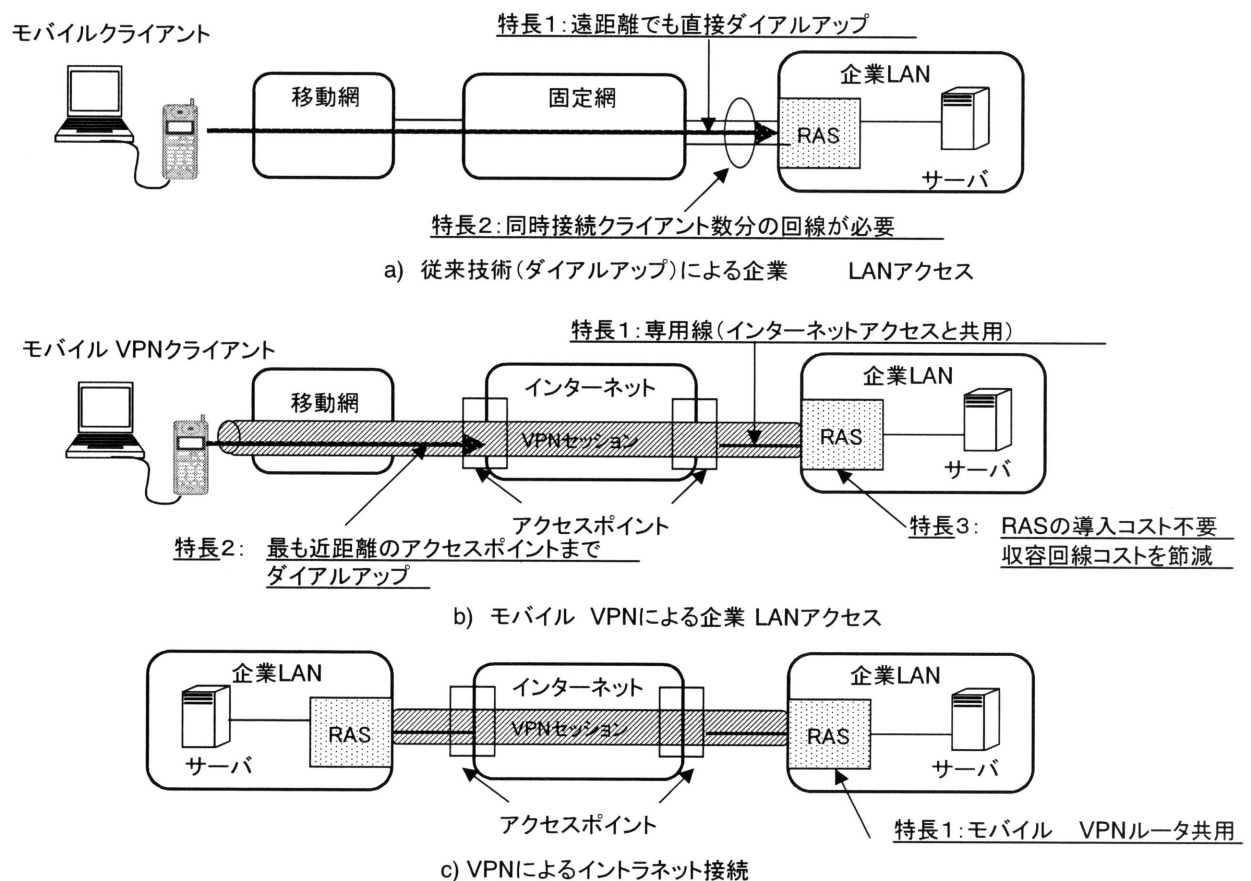
VPN は、インターネットのように多数のユーザによって共用されるネットワークを、あたかも専用線と同等のセキュアな環境で利用するための技術である(図 6-1)。モバイル環境下においてユーザ(クライアント)は、移動ネットワーク経由でダイヤルアップし VPN を利用する(以下では、この形態をモバイル VPN という)ことによって次のメリットを得ることができる。

(1) 通話料金の削減

電話料金は距離に比例して高額になる。遠距離から企業 LAN にアクセスする必要がある場合 VPN によって最も近接の ISP のアクセスポイント経由で企業 LAN にアクセスすることが可能になる。企業 LAN の RAS (Remote Access Service) に直接ダイヤルアップする場合と比較して、通信料金の距離に比例する部分を節約することができる。

(2) RAS の導入、維持管理コストの削減

RAS を利用する際には、RAS 側で同時接続するユーザ数分だけ固定電話回線を導入する必要があるのに対して、VPN の場合は、これらの固定電話回線をインターネットとの接続回線で兼用することができ、回線導入コストを節減可能である。また、RAS そのものの導入及び維持管理コストも削減できる。



備考 LAN : Local Area Network (構内通信網), RAS : Remote Access Service, VPN : Virtual Private Network

図 6-1 モバイル VPN の概要と特長

6.2.2 VPN プロトコル

有力な VPN プロトコルとして L2TP (Layer two Tunneling Protocol) [86] と IPsec (Internet Protocol Security) [87] - [97] の 2 つのプロトコルがある。

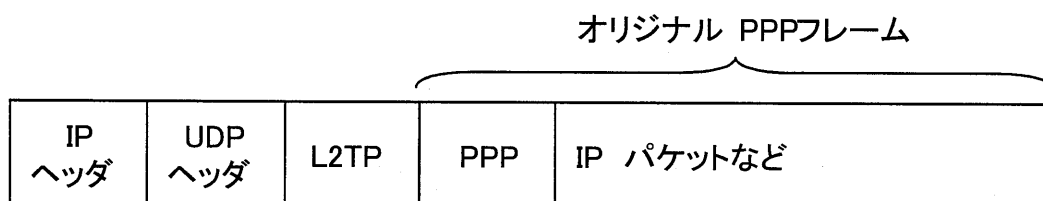
(1) L2TP

L2TP は, PPP (Point to Point Protocol) [107] のフレームを UDP (User Datagram Protocol) [84] のパケットでカプセル化し, IP 以外のパケットも IP ネットワーク上で転送可能とするものである (図 6-2)。セキュリティ機能に関しては, トンネルの認証機能以外は規定されていない。

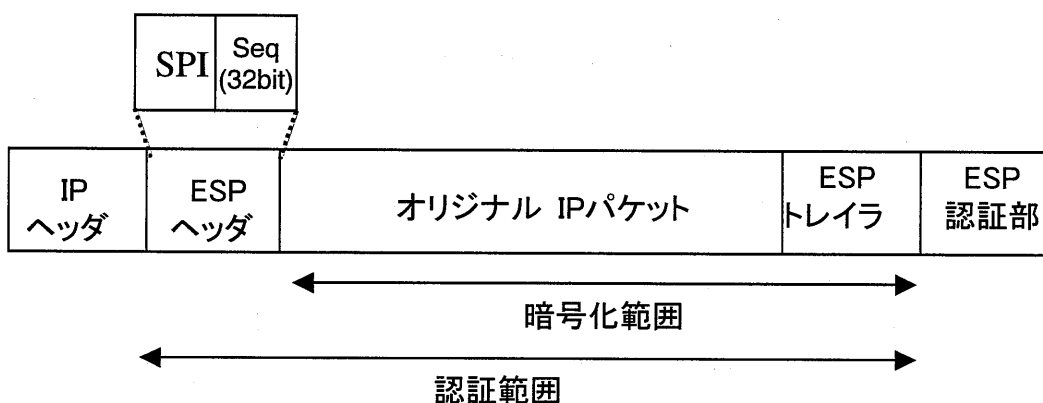
(2) IPsec

IPsec には, AH (Authentication Header) [88] と ESP (Encapsulating security Payload) [92] があり, それぞれにトランスポートモードとトンネルモードがあるが, 以下では, 代表的なトンネルモード ESP について述べる。

トンネルモード ESP の特徴は IP パケットを IP パケットでカプセル化していることであり，これにより企業 LAN 内のローカルな IP パケットを，インターネットに転送できる．カプセル化の際に，オリジナルの IP パケットは盗聴防止と企業 LAN 内サーバの IP アドレス秘匿のためにすべて暗号化され，VPN セッションを識別するための ESP ヘッダと ESP トレイラが付加されるとともに，改ざん検出とパケット認証のための ESP 認証部を付加し，新たな IP ヘッダ付加する(図 6-2)．このように，IPsec はセキュリティ機能が充実しているのが特徴である．



(a) L2TP パケット



(b) IPsec (トンネルモード ESP) パケット

- | | |
|--------------------------------------|-------------------------------------|
| ESP : Encapsulating security Payload | L2TP : Layer Two Tunneling Protocol |
| IP : Internet Protocol | PPP : Point to Point Protocol |
| IPsec : Internet Protocol Security | UDP : User Datagram Protocol |
| SPI : Security Parameters Index | Seq : シーケンス番号 |

図 6-2 主要 VPN プロトコルのパケット構造

(3) モバイル環境での VPN プロトコル

上記 2 つの VPN プロトコルの機能比較を表 6-1 に示す．本論文では，セキュ

リティ機能の充足性を重視し、モバイル VPN のセキュリティプロトコルとして IPsec を選択した。更に、IPsec の中から、モバイル VPN の利用形態（図 6-1）との親和性及び暗号化機能を優先し、トンネルモード ESP をモバイル VPN のベースプロトコルとし、以下では、これを前提に検討する。

表 6-1 主要 VPN プロトコルの機能比較

要件		L2TP	IPsec
トンネリング		○(レイヤ 2)	○(レイヤ 3) ^{*1}
セキュリティ	認証	○	○
	秘匿	×	○ ^{*2}
	改竄防止	×	○
	鍵交換	×	○

*1:トンネルモードでサポート

*2: ESP(Encapsulating Security Payload)でサポート

6.3 モバイル VPN の要件

モバイル VPN を実現する上で考慮すべき要件に以下のものがある。

6.3.1 モバイル VPN プロトコルへの要件

移動ネットワーク経由でインターネットにダイヤルアップ接続を行う場合には、一般には接続するごとに、異なる IP アドレスが割り当てられる。IPsec では、通信相手（IP アドレス）毎に SA (Security Association) を管理する必要がある。SA は、IP パケットの送受信元双方で合意したセキュリティポリシー、暗号鍵、認証鍵、IPsec パケットの ESP ヘッダ部にあるシーケンス番号値 (Seq 値) 等を格納するオブジェクトであり、VPN セッション開設時に作成し、終了時に削除する必要がある。しかし、接続が異常終了した場合等には VPN ルータ側はこの状態を検出できない場合がある。このため、一般に VPN クライアントと VPN ルータ間でキープアライブパケットを送受し、状態を定期的に監視する必要がある（図 6-3）。しかし、モバイル VPN の場合には、キープアライブ方式には以下の問題がある。

(1) 誤切断

VPN クライアント側の電波状態の悪化により、一時的な遅延時間の増大が発生

した場合、VPN ルータはキープアライブパケットが規定時間内に戻らないことにより、VPN クライアントが正常である場合でも、VPN セッションを切断してしまう可能性がある。

(2) 課金

クライアントが接続している移動ネットワークがパケットネットワークの場合、パケットネットワークは情報量課金が基本であるのに係わらず、キープアライブパケット自体に課金されるため、接続する時間によって通信料金が増えってしまう問題がある。

上記問題を解決するために、キープアライブをしない新しい VPN セッション (SA) の管理方式の検討が必要である。

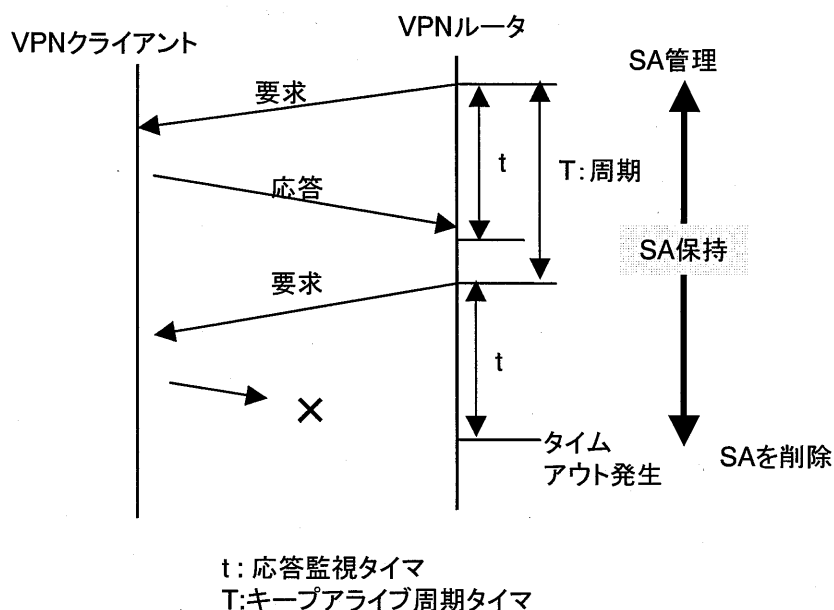


図 6-3 キープアライブによる SA 管理の例

6.3.2 モバイル VPN ルータへの機能要件

6.3.2.1 W-CDMA ネットワークの特性からの要件

1) TCP アクセラレータ機能の必要性

W-CDMA ネットワークでは高速パケット交換サービス（上り 64Kbps，下り 384Kbps）が提供されており，従来よりも高速なモバイルインターネットアクセスが可能となっている．このパケットチャネルの特性として一般に無線区間を含むネットワーク内伝送遅延時間が，転送速度に比較して，大きな値になることが分かっており，既存の TCP を利用した各種アプリケーションが十分なスル

ーットを得られない等の性能低下を生じることが明らかになっている。この対策として、受信バッファサイズの拡大等の TCP パラメタの最適化が必要になる [21], [30]。更に、IPsec パケットの組立て/分解によるオーバーヘッドが加わるため、モバイル VPN で実効的に利用可能な帯域は、通常の利用形態に比較して著しく制限され、利便性を損なうことになる。これらの理由により、TCP パラメタの最適化は必須となる。ユーザが所有している端末側は、TCP パラメタの最適化は自分自身で実施できるが、サーバ側は一般には困難である。この場合の性能向上策として、ネットワーク上にゲートウェイ (GW) を設置することにより、クライアント側と GW 間、GW とサーバ間で TCP セッションを独立に設定し、クライアント側と GW 間の TCP パラメタを移動ネットワークの特性に合った最適値に設定という手法が提案されている [98]-[101]。以下では、この方式を TCP アクセラレータと称し、これをモバイル VPN ルータで実現する際の課題について検討する。

一般に VPN プロトコルとして IPsec を利用する場合、IP 層以上が暗号化されるため、例えば暗号通信区間に TCP アクセラレータが設置されたとしてもそのままではこの機能を利用できない。このため、IPsec を処理するモバイル VPN ルータにおいて暗号化前のパケットに対して、TCP アクセラレーションを行うことが必須となる。

2) TCP アクセラレータ実現上の課題

モバイル VPN ルータで TCP アクセラレータを実現するには新たなセキュリティ問題を考慮する必要がある。TCP セッションハイジャックは、TCP における送信元認証が、送信元の IP アドレス及び TCP ヘッダ中のシーケンス番号 [102] のみによって行われることを利用する非常にポピュラーな攻撃方法である [103]。概要を以下に示す (図 6-4)。なお、以下では TCP (RFC793) のシーケンス番号を SN 値、初期シーケンス番号を ISN 値と記す。また SYN (ISN_i) は初期シーケンス番号 ISN_i の SYN, ACK: ISN_i は SYN (ISN_i) 要求に対する応答 (ACK) を示す。

[ステップ 1] 攻撃者 X が正規のクライアント A になりすまして (すなわち送信元 IP アドレスを A のアドレスでスプーフィングして) サーバ B に SYN (ISN_x) を送る。

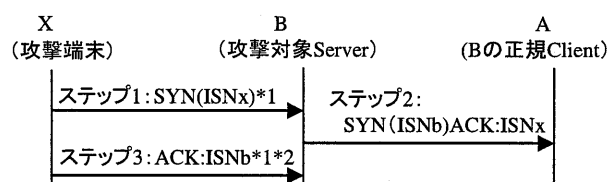
[ステップ 2] B は、SYN (ISN_b) ACK: ISN_x を A に送る。X はこの信号を直接受信することはできない。しかしながら、何らかの方法で ISN_b を推測できたとする。

[ステップ 3] X は、ACK:ISNb を B に送信する。この信号を B が受理した段階で、X から B への片方向の TCP セッションが設定され、X は B に対して任意のデータを送信することが可能になる。

この攻撃を成功させるためには、[ステップ 3]において ISNb を推測しなくてはならないが、TCP では ISN の値はタイマに連動してインクリメントされるので、X が直前に正規の手続きで B に TCP のセッションを設定し、その時の ISN 値を取得する等によりこの値と経過時間から ISNb を計算し推測することが可能となる。最近の OS では、ISN 生成のアルゴリズムをより複雑化し、簡単にはこの値の推測できない実装になっているものもあるが [104], [105], これらのアルゴリズムに関するセキュリティホールは指摘も後を絶たないため [106], 危険性は依然として残されている。

B が通常のホストサーバの場合、本攻撃により被害を被るのは、B のみに限定される。しかし、B が TCP アクセラレーション機能を有するモバイル VPN ルータの場合には、その ISN 値算出法が一旦破られると、B が TCP セッションを集約している全てのサーバがセッションハイジャックの危険にさらされるという意味で、この問題は非常に深刻となる。更に、各サーバは VPN ルータに対しては特別な認証無しに接続するので、サーバ毎の個別のアクセス権管理のみでは、ISN の予測を防止することができなくなる。

このように、通常のインターネットからの攻撃に対しては、IPsec の認証メカニズムにより防御可能である。しかし、VPN ルータを異種企業間等の LAN 間通信で利用する場合 (図 6-1 c) 参照) には、攻撃者 X が LAN 内に存在する可能性があり、X が遠隔の LAN 内から VPN を通じて TCP セッションハイジャックを試みた場合、どちらの VPN ルータもそれを検出ないし防御することは困難であり、この対策をモバイル VPN ルータで行う必要がある。



注) * 1: 送信元IPアドレスをAのIPアドレスに設定する
* 2: 直接ISNbを知ることができないが、何らかの方法で推定

図4 TCPセッションハイジャックの例
Fig. 4 Example of TCP Session Highjacking

図 6-4 TCP セッションハイジャックの例

6.3.2.2 モバイルVPNルータ冗長構成の要件

モバイル VPN の利用形態は、W-CDMA に出現によってますます多様化、高度化し、社内システム、社内のメールサーバへのリモートアクセスといった用途のみでは無く、サーバの遠隔制御や有料のコンテンツ配信、商取引等へ応用 [107] され、ユーザの数も膨大になると想定される。これらを考慮すると、サービスの継続性が重要な問題となり、信頼性向上のためモバイル VPN ルータ自体の冗長化が必要になる。

モバイル VPN ルータの冗長化方式として、最も単純には、予備のルータを設置しておき、通常利用しているルータ（現用系）からレスポンスが無いなどの問題が発生した場合に、予備系に切り替え新たに VPN セッションを設定し直す方式等が考えられる。しかし、この場合、系の切り替え時にルータ自身の IP アドレスが変更になるため、このルータは接続している全てのモバイル VPN クライアントと鍵交換をやり直す必要があり、非常に大きな負荷がかかりサービスが長時間中断する可能性が高い。このため、鍵の再交換を必要としない系切り替え方式として、現用系、予備系とも同一の IP アドレスを有し、かつ現用系と予備系で SA 情報を共有することが可能な VPN ルータ冗長化方式を検討する必要がある。

6.4 モバイル VPN 方式の提案

本節では、6.3 節で述べた各要件を解決する実現方式を提案する。

6.4.1 モバイル VPN プロトコル

IPsec をモバイル VPN に適用するために、以下の新しい VPN セッション管理方式を提案する。提案方式は、周期的なキープアライブによるリアルタイムの VPN セッション管理 (SA 情報管理) を行わずに、VPN セッション管理上問題が発生した時のみに、モバイル VPN ルータからクライアントに状態確認のための確認要求パケットを送信するように ISsec を拡張することで VPN セッション管理を行う [108]。

具体的には、モバイル VPN ルータは、クライアントから VPN セッション設定要求を受け、SA を作成する (VPN セッションが上限数に達するまで、要求を受け付ける)。VPN セッション数が同時接続上限に達した場合、モバイル VPN ルータは、その時廃棄すべき無効な SA 情報が存在しないか以下の手順で確認する。

- 1) FIFO (First in First out) か LRU (Least Recently Used) のいずれかのア

ルゴリズムにより、廃棄候補の VPN セッションを選択し、当該 VPN セッションの SA に登録されているクライアントに状態確認パケットを送信する。

2) クライアントから応答がなければ、当該 SA を削除し、資源を解放する。

3) クライアントから応答があれば次の廃棄候補を選択し、上記 1) の処理を継続する。

また、クライアントが既に SA に登録してあるものとは異なる新たな IP アドレスで VPN セッションを要求してきた場合には、当該クライアントの既にある SA を削除し、新たな SA を作成する。これにより、上記 1) -3) による削除を待たずに早期に無効な VPN セッションを検出し、削除することを可能とする。

6.4.2 セキュア TCP アクセラレータの実現方式

TCP セッションハイジャックに関連するのは、6.3.2.1 節で述べたように TCP ヘッダ中の SN 値に関する部分のみである。このため、モバイル VPN ルータで分割された 2 つの TCP セッションで使用する ISN 値を擬似的に透過（同じ値）になるように変換出来れば、モバイル VPN ルータで TCP アクセラレータを実現したとしても、ISN 値が予測されハイジャックされる危険性の増大を避けることが可能となる [109]。

提案する TCP アクセラレータ実現方式を図 6-5 に示す。TCP アクセラレータは、以下の TCP 処理部と SN 値透過変換処理部から構成される。

(1) TCP 処理部

サーバと VPN ルータ間の TCP は、通常実装されている TCP をそのまま利用する。また、モバイル VPN クライアントとモバイル VPN ルータ間の TCP には W-TCP (Wireless TCP) [30] と呼ばれる以下の TCP パラメタの拡張を行ったものを使用する。

- ・ TCP バッファサイズの拡張
- ・ 初期ウィンドウサイズの拡張
- ・ 選択的応答確認
- ・ 最大転送パケット長 (MTU:Maximum Transfer Unit) の拡張

(2) SN 値透過変換処理部

SN 値透過変換処理部は、ISN 読み取り機能と SN 変換機能からなる。ISN 読み取り部は、サーバ側に位置し、サーバ (B) の ISN 値 (ISNb) を取得して、SN 変換部に通知する。SN 変換部は、クライアント側に位置し、TCP プロトコル処理

部のクライアント側 (A) の ISN 値 (ISN_c) とサーバ側 (B) の ISN 値 (ISN_b) を取得し、これらの値から ISN 値及び SN 値の変換規則 (ISN_{offset} 値=ISN_c-ISN_b) を生成すると共に、その規則に従って変換を実行する。すなわち、TCP セッション開設時には、クライアント側 TCP プロトコル処理部が送信した SYN (ISN_c) ACK:ISN_a の ISN_c をサーバ (B) 側の ISN 値である ISN_b に変換し、クライアント (A) の ISN 値とサーバ (B) の ISN 値を同じ値にする。また、データ転送時は、クライアント (A) から受信した SN に ISN_{offset} 値を加え、TCP プロトコル処理部から受信した SN には ISN_{offset} 値を引く。

これにより、分割された TCP の各々の ISN 値をエンド-エンドレベルで透過性を確保することが可能になり、TCP セッションハイジャックの足掛りとなる ISN 値予測を困難とすることが出来る。

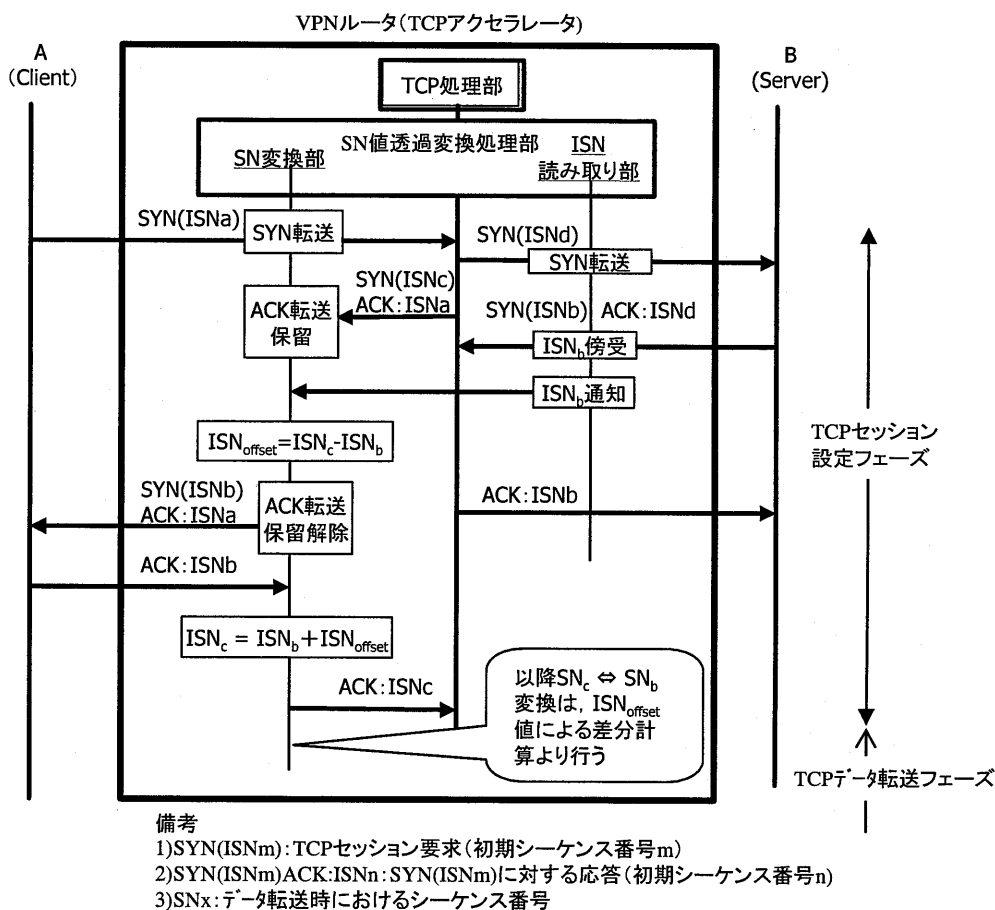


図 6-5 セキュア TCP アクセラレータにおける SN 値変換原理

6.4.3 冗長化モバイル VPN ルータ実現方式

(1) 基本方式

ルータの冗長化方式として、VRRP (RFC2338 : Virtual Router Redundancy Protocol) がある [110]. VRRP は、現用系ルータ (MR: Master Router) と予備系ルータ (BR : Backup Router) を一つの仮想ルータとして動作させるためのプロトコルである. すなわち、通信相手には一つの IP アドレスに見せ、BR は MR の運用状態を監視し、MR の障害を検出すると BR が自動的に MR に切り替わるメカニズムを実現する. 本論文では、VRRP をモバイル VPN に適用することを冗長化のための基本方式とした (図 6-6). 以下では、VRRP を前提に系の切り替え時の課題と提案方式について述べる.

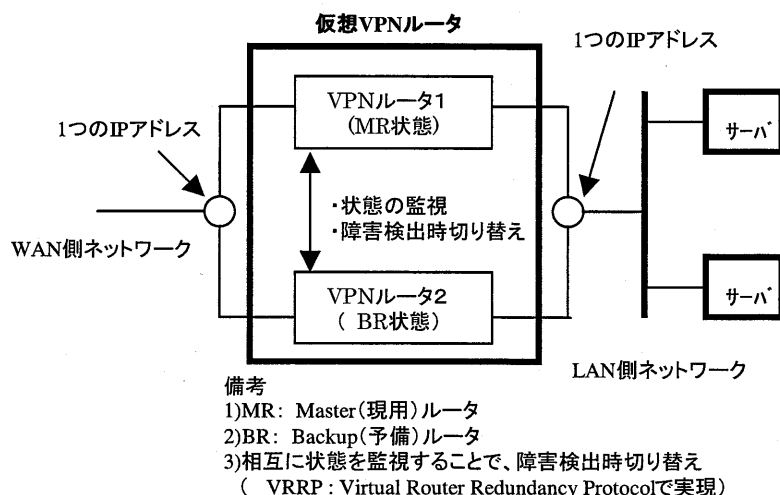


図 6-6 VRRP による仮想ルータ構成

(2) SA 情報共有の課題

SA 情報には、セキュリティポリシー、暗号鍵、認証鍵、及び IPsec パケットの ESP ヘッダにあるシーケンス番号 (以下では Seq 値と称する、図 6-2 参照) 等がある. これらの情報は、6.3.2.2 節で述べたように MR と BR で共有されている必要がある. なお、この両者での SA 情報のやり取りは、機密性保持のためローカルな通信手段で行われるものとする.

モバイル VPN ルータの受信側では、リプレイ攻撃を避けるために、IPsec パケットの受信履歴を Seq 値で管理し、以前受信したのと同じ Seq 値のパケットを受信した場合には、直ちに廃棄する必要がある. このため SA 情報のうちセキュ

リティポリシ、暗号鍵、認証鍵等は、鍵交換時（数分から数時間の頻度）に更新されるのに対し、IPsec パケットに付与される Seq 値に関する情報は、パケットを送受する毎に更新されるので、MR と BR で Seq 値を VPN ルータの性能を落とさずに完全に共有することは困難であり、新しい切り替え方式が必要である。

(3) 系切り替え方式

IPsec では、Seq 値の扱いに関して、送信側は送信パケットにシーケンシャルに Seq 値を付与し、受信側は、当該 Seq 値が以前に利用されたかどうかの履歴を管理する（すなわち Seq 値の順序に関しては関知しない）と規定している [92]。この性質を利用し、IPsec パケット送信側での Seq 値の付与範囲を仮想 VPN ルータを構成する各ルータ毎に限定使用することによって、通信する相手毎に Seq 値の使用範囲を異なる範囲とし、系切り替え時に Seq 情報の引き継ぎを不要に出来る。また、この Seq フィールドは 32 ビットあるので、複数に分割してもその範囲は十分大きいのでデータ転送に関する実質的な影響はほとんどないと予想される。筆者らが提案しているモバイル VPN ルータは、モバイルクライアントと LAN (モバイル VPN ルータ)、及び LAN (モバイル VPN ルータ) 相互間に適用することを想定している。このため、Seq 値の付与範囲は、LAN 相互間通信を考慮し以下の 4 つの領域に分割することとした [111]。

領域 1 : "00000000" - "3FFFFFFF"

領域 2 : "40000000" - "7FFFFFFF"

領域 3 : "80000000" - "BFFFFFFF"

領域 4 : "C0000000" - "FFFFFFF"

また、本提案方式では、通信する相手毎に Seq 値の付与範囲を変更するため、系を切り替えたモバイル VPN ルータは、そのことを陽に相手に通知する必要がある。このため、系が切り替わった際に VPN ルータ (新たに MR となったルータ) は、鍵交換プロトコルで規定される任意の情報の送受信が可能な通知情報フィールド (Notification Payload) [95] に新たな通知メッセージを定義し、相手側にそのことを通知することとした。具体的な処理手順を LAN (モバイル VPN ルータ) 相互間通信を例に説明する (図 6-7)。

1) LAN (A) の VPN ルータ a1 (MR) と LAN (B) の VPN ルータ b1 (MR) が VPN セッションを設定し IPsec で通信している。この場合、ルータ a1, b1 はそれぞれ Seq 値として、"00000000" - "3FFFFFFF" の範囲を使用する。

2) LAN (B) の b1 が故障した場合、系が切り替わり新たに b2 が MR となり、b2 はそ

のことを LAN (A) に通知する。b2 は Seq 値として "80000000" - "BFFFFFFF" の範囲を使用する。なお、b2 は以降、"00000000" - "3FFFFFFF" の範囲の Seq 値を持つ受信 IP パケットは全て廃棄する。

3) 上記の通知を受け取った LAN (A) の a1 は、以降 LAN (B) 向けの Seq 値として "40000000" - "7FFFFFFF" の範囲を使用する。

クライアントと LAN (モバイルVPNルータ) 間の場合も同等の手順を取るようになる。この方式によって、冗長化されたルータ相互間で Seq 値に関する情報を共有せずに、Seq 値のチェックが可能となり、リプレイ攻撃に対して十分な防御が可能となる。

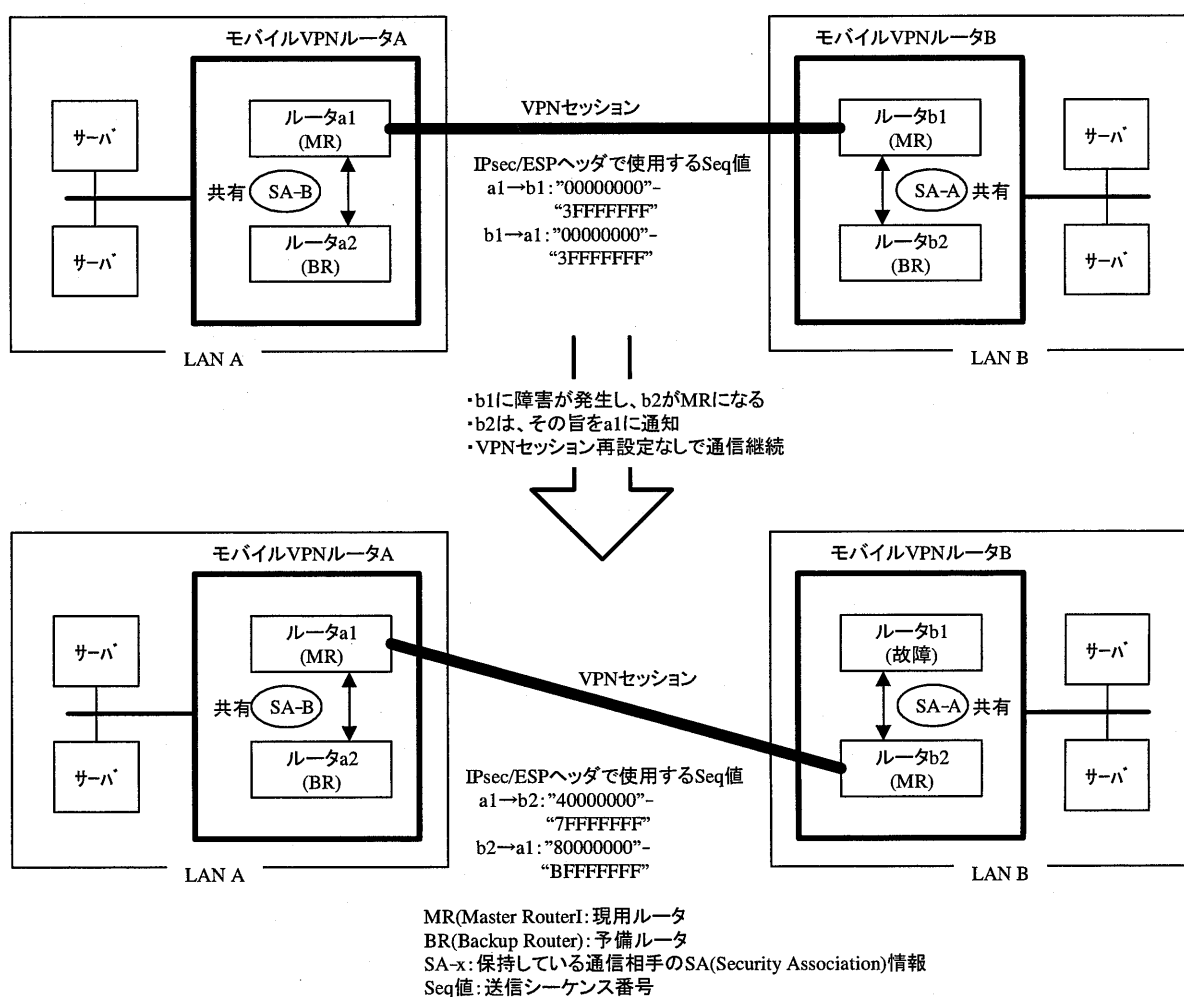


図 6-7 提案方式によるルータ切替え手順

6.5 実装評価

上記 6.4 節で提案したモバイル VPN 方式のプロトタイプシステムによる実装評価結果について述べる。

6.5.1 評価システムの構成

試作したモバイル VPN ルータとモバイル VPN クライアントのプロトタイプシステムを使用し、提案方式の有効性を評価した。その評価系を図 6-8 に示す。モバイル VPN ルータとクライアント間は、W-CDMA シミュレータ (4.5.1.2 節参照) を介して接続し、擬似的な通信環境とした。

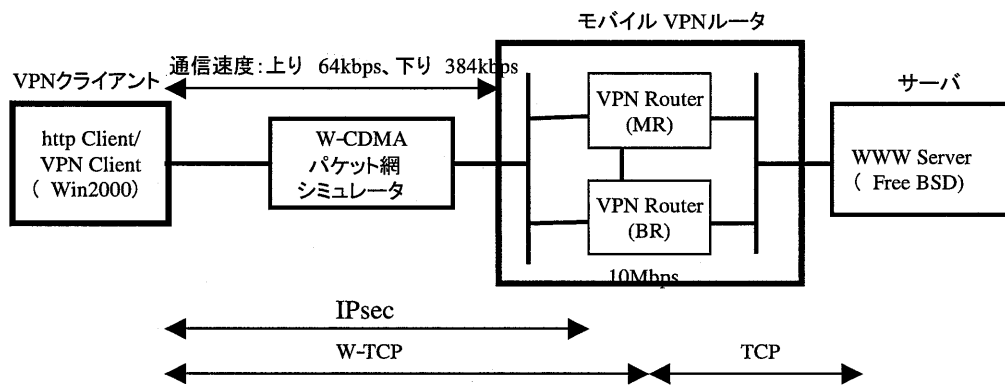


図 6-8 モバイル VPN 方式のプロトタイプ評価試験システム

6.5.2 VPN セッション管理方式の評価

VPN セッション管理方式の有効性を確認するため、提案方式とキープアライブ方式を採用している既存製品との VPN 維持パケット量の比較を行った。VPN セッション設定済みの状態で、上位のアプリケーションを一切起動せずに放置した場合に各々で送受された情報量を比較した結果を図 6-9 に示す。提案方式では、VPN セッション維持のために、無用なパケットが流れていないことが確認できる。なお、1 時間放置した後、それぞれローカル IP で ping を行って、VPN セッションが維持されていることも確認している。

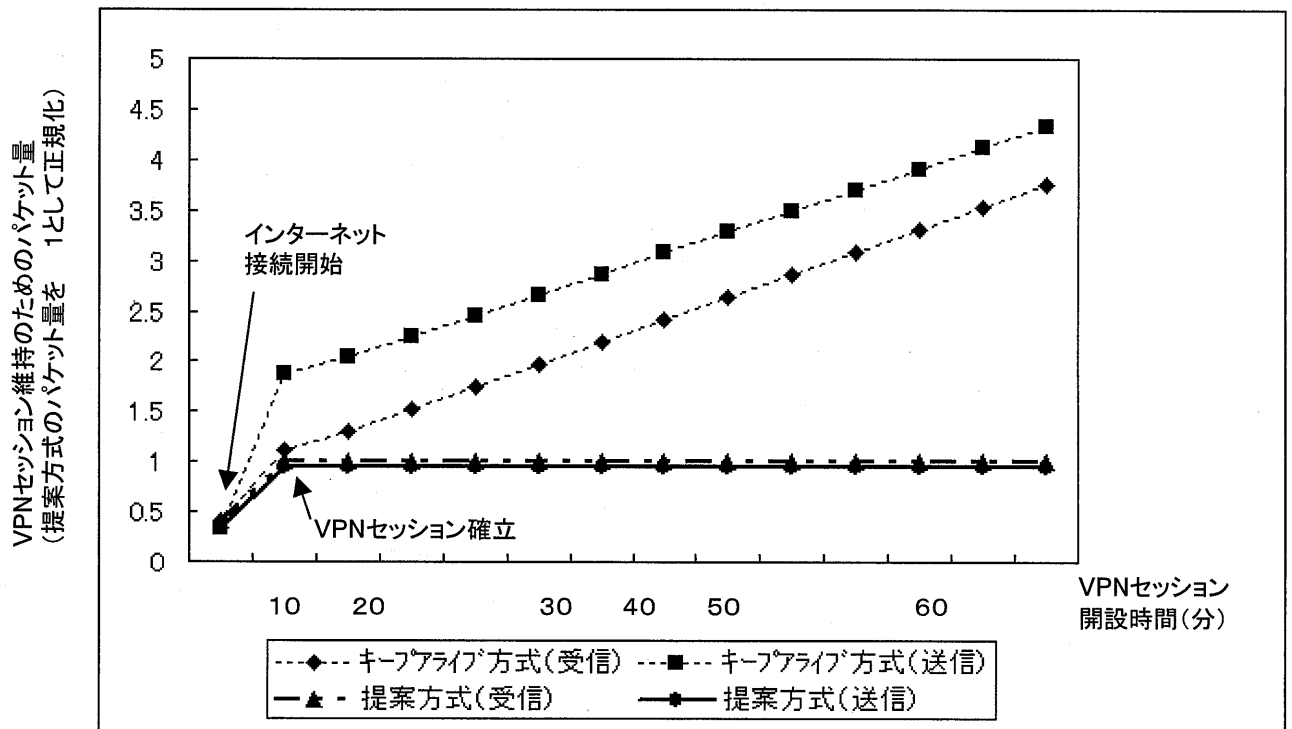


図 6-9 提案方式により得パケット削減効果

6.5.3 セキュア TCP アクセラレーションの評価

HTTP プロトコルを利用して、2MByte のファイルのダウンロードに要する時間を測定した。TCP アクセラレーション機能 ON/OFF それぞれの場合における、遅延時間 (RTT:Round Trip Time) とスループットの関係を図 6-10 に示す。アクセラレータ ON の場合、W-TCP (受信バッファサイズの拡大等) の効果が顕著にあり、ほぼ理論限界値に近い最大性能が得られおり、十分有効であることが解った。

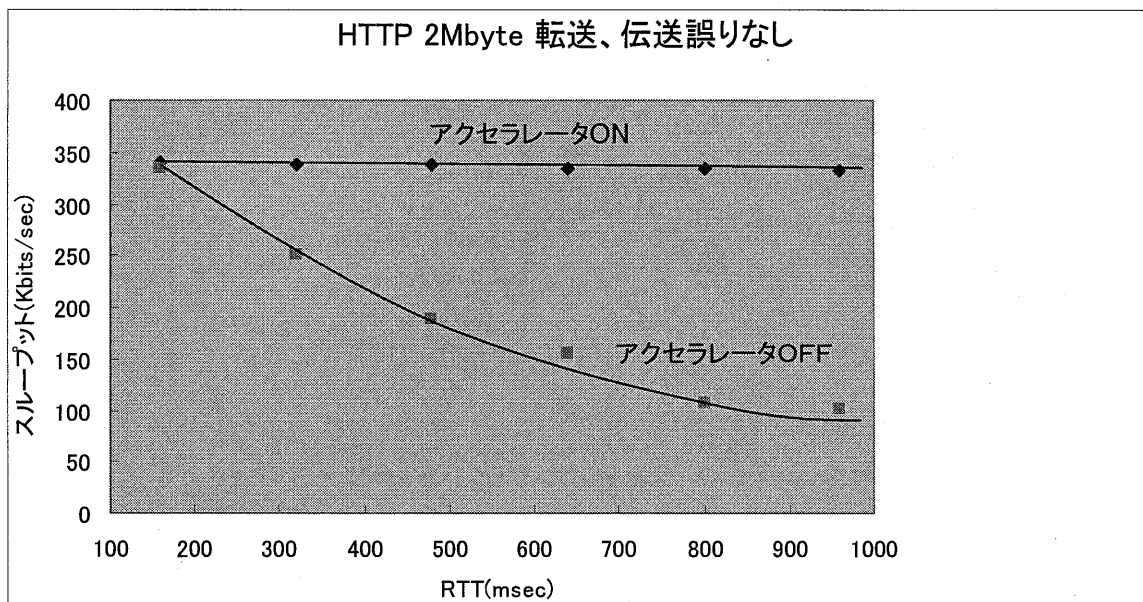
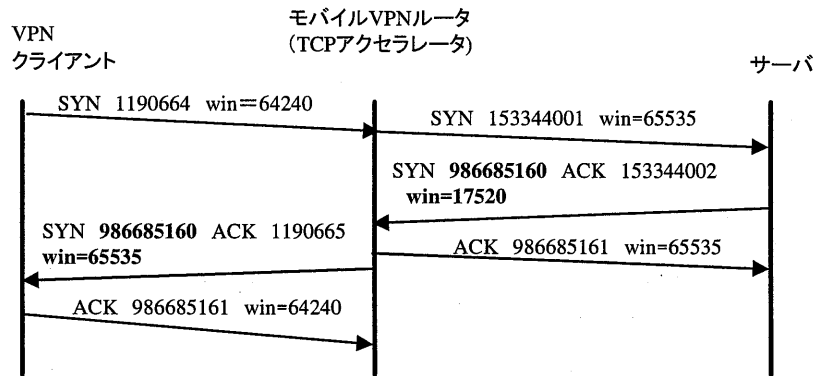


図 6-10 TCP アクセラレータの効果 (スループット)

TCP アクセラレータにおける、TCP セッション設定時 (3ウェイハンドシェイク) の処理シーケンスログを図 6-11 に示す。図 6-11 より、サーバ側 TCP の ISN 値を透過としたまま、クライアント側 TCP の初期ウィンドウサイズを拡張する (W-TCP の設定) ことに成功しており、TCP セッションハイジャック攻撃に有効に働く事が解った。なお、TCP セッションに対する攻撃法としては、この他にも、送受信間の SN 値の同期を崩す方式 [112] 等が知られているが、これらに関しては、TCP アクセラレータの有無に関わらず危険度は同一であり、本論文における検討対象としていない。また、LAN 内の個々のホストに対する ISN 値予測に関しても同様である。



(解説)

- ・クライアントに対してモバイルVPNルータのISN値2つのTCPのISN値が隠蔽され、サーバ側TCPのISN値(986685160)がそのまま設定されている
- ・クライアント側TCPの受信バッファサイズ(win=65535)が拡大(W-TCP設定)されている

備考

- 1)SYN mmmmmm :TCPセッション設定要求時のシーケンス番号初期値(ISN)
- 2)win=nnnnn :受信バッファサイズ
- 3)ACK xxxxxx :ACK送信側シーケンス番号の初期値

図 6-11 TCP セッション設定時の実測シーケンス

6.5.4 冗長化モバイルVPNルータ方式の評価

通信中に擬似的にVPNルータに障害を発生させ、その後系が切り替わり通信が正常に継続できるか否かの検証実験を行った。FTPプロトコルで1MByteのファイルのダウンロードを実行中に、VPNルータのMRの電源を手動で切った場合のクライアント側でのTCPシーケンス番号(SN値)の時刻変化を図6-12に示す。なお、提案方式の効果を明確にするため、VRRP方式(SA情報の共有を行わない場合)の同様の評価結果を図6-13に示す。

図6-12より、提案するモバイルVPNルータ冗長化方式により、3-4秒程度で系の切り替えが可能であることが解った。切り替え時間がこの程度であれば、上位アプリケーションに致命的な影響を与えず十分実用に耐えるといえる。また、図6-13と比較すると3割以上切り替え時間を短縮していることが解る。ただし、本評価においては、VPNセッションは1つのみで行ったが、複数のVPNセッションの場合(多数のユーザが同時に利用している環境)では、鍵交換処理のオーバーヘッドがVPNセッション数に比例して高くなり、提案方式の効果がより顕著になると考えられる。特に、鍵交換処理でオプションとなっているDiffie-Hellman法[113]を利用する場合には、その処理負荷はより高くなることが解っており、IPsecのセキュリティ機能を低下させずに冗長化ルータ構成を可

能とする提案方式は、このようなモバイル VPN 利用形態では必須になると言える。

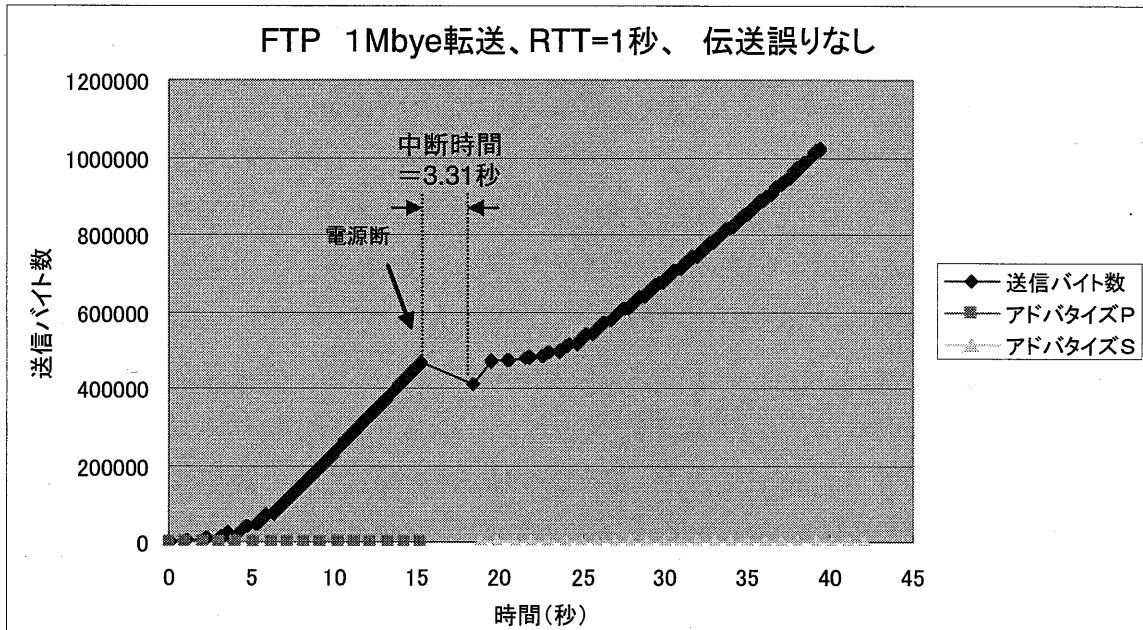


図 6-12 提案方式による系切替え時の TCP シーケンス

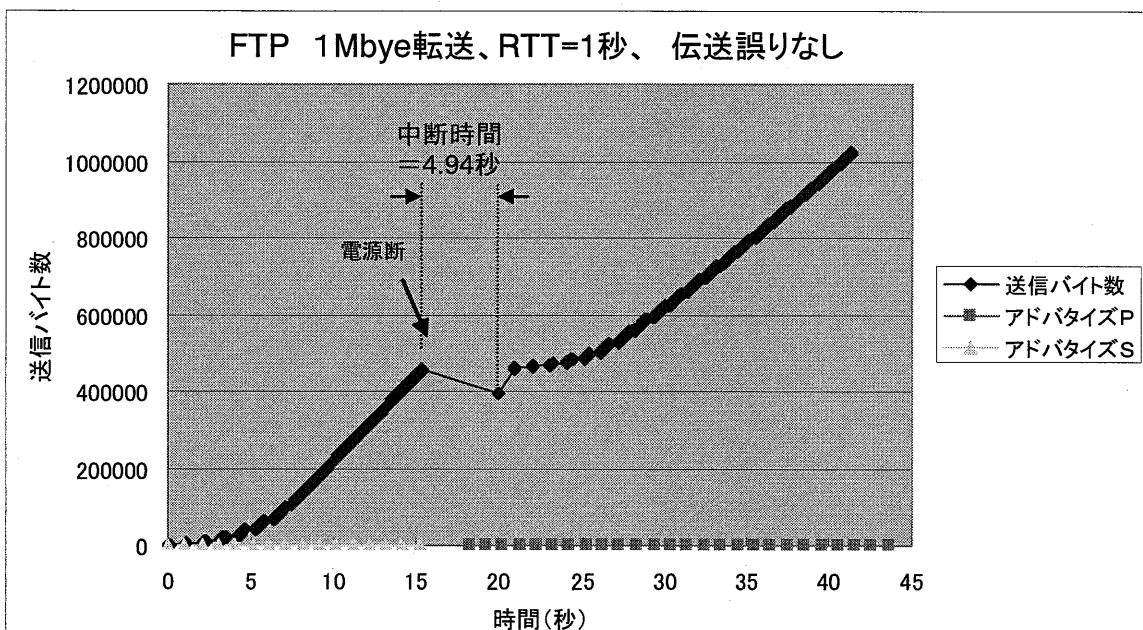


図 6-13 VRRP 方式 (SA 情報の共有なし) による系切替え時の TCP シーケンス

6.6 おわりに

本論文では、VPN を W-CDMA ネットワークに適用する場合のモバイル VPN 方式について提案した。提案した方式は、VPN として広く使用されている IPsec をベースとし、キープアライブをしない VPN セッション管理方式を提案した。また、TCP の性能問題を解決するためプロキシ機能をモバイル VPN ルータ上で実現することとし、その際に新たに発生する TCP セッションハイジャック問題を防止するセキュア TCP アクセラレータの実現方式を提案した。更に、信頼性を向上させるための冗長化ルータ構成を実現するため標準的なプロトコルである VRRP をベースにセキュリティレベルを保持したまま、効率の良く系の切り替えを実現する方式を提案した。また、本方式を実装したプロトタイプシステムを構築し、W-CDMA ネットワークを疑似するシミュレータを使用して、実測評価した。

この結果、提案した方式の機能が有効に働き、かつ性能上も TCP スループットを最大 3 倍向上させると共に、モバイル VPN ルータの障害時に系の切り替え時間が 3 秒程度であり、十分実用的な方式であることを示した。

今後は、FOMA ネットワーク等実際のモバイル環境での評価を継続すると共に、複数のクライアントが同時接続している場合の系の切り替え時間等の性能を明確にし、本提案方式に基づくモバイル VPN ルータを実用化する際のハードウェア条件等を設計指針として確立する予定である。

7章 結論

本論文では、第3世代以降の高速移動無線ネットワークに適用することを前提に、新世代モバイルインターネットサービスにおけるプロトコルを提案した。最初に、モバイルインターネットの発展経緯と今後の研究課題について整理し、次に、以下の5つの具体的な研究課題について検討した。なお、方式の評価に当たっては、前提とした移動無線ネットワークとして筆者らが開発した W-CDMA シミュレータを利用したが、FOMA 等の実ネットワークを使用した評価については今後の課題としている。

(1) 移動機向けモバイルインターネットアーキテクチャの提案

IMT-2000 (W-CDMA) の無線環境を疑似するシミュレータを利用して、WAP プロトコルとインターネットプロトコル (HTTP/TCP) の性能を測定し、比較評価を行った。その結果、両プロトコルはほぼ同等の性能を持つが、IMT-2000 などの高速移動通信ネットワークで想定されるマルチメディアなどの大容量コンテンツを配信する場合、HTTP/TCP などのインターネットプロトコルを適用することが可能であることを示した。

本評価結果に基づいて、IMT-2000 に代表される高速移動通信ネットワークに適した次世代モバイルインターネットアーキテクチャを提案した。本提案は、WAP フォーラムで次世代 WAP (WAP 2.0) として採用されており、次世代モバイルインターネットの標準的なアーキテクチャとなることが期待されている。

今後は、第4世代移動通信ネットワークなどのより高速な無線ネットワークを対象としたインターネットプロトコル (TCP など) の最適化、WAP プッシュなどを応用した新しいモバイルインターネット向けアプリケーションなどについて研究を進める予定である。

(2) 移動機向けプッシュプロトコルの提案と実証評価

本研究では、WAP1.1 プッシュプロトコルと HTTP/TCP をベースとした提案プッシュプロトコルの性能を比較評価することによって明らかにした。さらに、IMT-2000 等の高速移動通信ネットワークに適した移動機向けプッシュプロトコルを新たに提案した。提案方式である HTTP/TCP をベースとしたプッシュプロトコルは、IMT-2000 を想定したシミュレーション環境において WAP1.1 のプッシュプロトコルと比較し、通信時間が短くなることを示し、特にデータサイズが大きいデータの場合には提案方式が有効であることを示した。本研究結果に基づいた提案プッシュプロトコルは OMA (旧 WAP フォーラム) で、WAP2.0 プッシュ

プロトコル仕様として採用された。さらに本論文では、XHTML とプッシュ機能を組合せた差分プッシュ方式を提案し、プロトタイプシステムによりその有効性を実証した。

なお、クライアントが増えた場合のスケーラビリティに関しては、今後の検討課題としたい。特に複数クライアントへ同時配信を実現する際のマルチキャスト方式と本方式の共存方式等について検討し、それとあわせたスケーラビリティに関する詳細な検討について今後の検討する予定である。

(3) W-CDMA でのリンク層 ARQ と TCP の特性評価

最初に、第 3 世代移動通信ネットワークの代表的な方式である W-CDMA のリンク層再送動作を詳細に検討し、リンク層における遅延ジッタ抑制と伝送効率のトレードオフ関係を分析して、評価すべきリンク層および TCP の動作パラメータを明確にした。次にシミュレーションによりそれぞれのパラメータの最適値を求めた。

評価モデルの設定に当たっては、現実の TCP 実装間のタイムアウトの振舞いの違いに着目し、網エミュレータを用いた遅延ジッタ耐性の検証結果から、遅延ジッタ耐性が低く、ソースコードによる調査の容易さから Linux を選び、そのモデルとした。

リンク層における遅延ジッタ抑制と伝送効率の間にトレードオフがあることを明確にし、シミュレーションによってその調整パラメータである RLC の `Timer_Status_Prohibit` の最適値が 200 [ms] であることを明らかにした。

W-CDMA においてはリンク層 ARQ での再送が有効であり、その場合のリンク層再送回数は、W-CDMA の無線区間のブロック誤り率 BLER が 0~10% では 5 回で十分であることを示した。

W-CDMA を始めとする第 3 世代移動通信ネットワークのような高遅延ネットワークに対しては OS のデフォルト設定に対して受信ウィンドウサイズを広げる必要があるが、ウィンドウサイズが大きいほど輻輳を発生させ得る機会が増えることを明確にし、その最適値は、リンクの帯域幅遅延積を反映した 48-64 [KB] が適正値であることを示した。

本論文では TCP による信頼性のあるストリーム伝送を目的としているが、VoIP (Voice over IP) やストリーミングのようなリアルタイム伝送においては再送機構への要求が異なるため、今後はそれらに最適なプロトコルパラメータの検討を行いたい。さらに、無線 LAN などの異なるリンクを扱うことができるよう

に本研究で用いた手法を一般化してゆきたい。

(4)高速インターネットアクセスのためのステルス型ゲートウェイの提案と実装評価

本論文では、W-CDMA パケットネットワークを介して、インターネットアクセスを高速に行う場合の GW 方式とその実装方式を提案した。具体的には、End-End でアドレス情報が透過となる W-TCP と TCP の相互変換を行うステルス型 GW 方式を提案すると共に、実装評価を行った。その結果、インターネット上に多数存在する W-TCP が適用されていないサーバに対するアクセスにおけるスループットと応答時間を、提案方式で 2-3 倍程度に改善できることを明らかにした。更に、GW での処理遅延時間は、数 msec (CPU 使用率：0%) ~ 数十 msec (CPU 使用率：70%) 程度であり、提案方式は、欠点であるオーバーヘッドは無視できるくらい小さく、かつその特徴（保守性・運用性等に優れる）を十分生かすことが可能である実用的な方式であることを明らかにした。

実際の GW の運用に際しては、1つの GW でいくつまでの TCP セッションの同時運用が可能であるか等のスケーラビリティが重要である。このため、GW 装置のハードウェア/OS を含めたプラットフォームの性能と、同時にサポートできる TCP コネクション数の関係については、今後の課題としたい。

(5) モバイル VPN 方式の提案と実証評価

本論文では、VPN を W-CDMA ネットワークに適用する場合のモバイル VPN 方式について提案した。提案した方式は、VPN として広く使用されている IPsec をベースとし、キープアライブをしない新しい VPN セッション管理方式を提案した。また、TCP の性能問題を解決するためプロキシ機能をモバイル VPN ルータ上で実現することとし、その際に新たに発生する TCP セッションハイジャック問題を防止するセキュア TCP アクセラレータの実現方式を提案した。更に、信頼性を向上させるための冗長化ルータ構成を実現するため標準的なプロトコルである VRRP をベースにセキュリティレベルを保持したまま、効率の良く系の切り替えを実現する方式を提案した。また、これらの提案方式を実装したプロトタイプシステムを構築し、W-CDMA ネットワークを疑似するシミュレータを使用して、実測評価した。

この結果、提案した方式の機能が有効に働き、かつ性能上も TCP スループットを最大 3 倍向上させると共に、モバイル VPN ルータの障害時に系の切り替え時間が 3 秒程度であり、十分実用的な方式であることを示した。

今後は、複数のクライアントが同時接続している場合の系の切り替え時間等

の性能を明確にし，本提案方式に基づくモバイル VPN ルータを実用化の際のハードウェア条件等を設計指針として確立する予定である。

謝辞

本研究を進め論文としてまとめるにあたり、終始にわたり懇切丁寧にご指導励ましを賜りました指導教官である静岡大学情報学部水野忠則教授に心より感謝します。また、静岡大学大学院理工学研究科の各先生方にご指導頂きましたことに感謝の意を表します。特に、梅谷征雄教授、大坪順次教授、渡辺尚教授、石原進助教授、佐藤文明助教授には論文のまとめに際し懇切なるご指導を頂いたことに感謝致します。

静岡大学大学院への入学を会社の研究業務の一環として了承され、各種のご配慮・ご支援を頂きました(株)NTTドコモの常務取締役・木下耕太研究開発本部長、および常務理事・中野博隆マルチメディア研究所長に感謝致します。また、同僚としていろいろ相談に乗って頂いた渥美幸雄専修大学教授(元(株)NTTドコモ・マルチメディア研究所・4Gインターネット方式研究室長)に感謝致します。

また、これまで研究を共にし、多くの討論・協力・助力を頂いた(株)NTTドコモ・マルチメディア研究所石川憲洋主任研究員、稲村浩主任研究員、鈴木偉元主任研究員、三浦史光主任研究員、同・ネットワーク研究所尾上裕子主任研究員(元マルチメディア研究所主任研究員)、同・マルチメディア開発部高橋竜男主任技師(元マルチメディア研究所主任研究員)、(株)NTTドコモ東海・鶴巻宏治部長(元マルチメディア研究所主幹研究員)、並びに(株)NTTドコモ・マルチメディア研究所・モバイルインターネット研究室の皆様へ感謝致します。

終わりに、これまで常に暖かく見守ってくれた両親と妻に感謝致します。

参考文献

- [1] 白鳥則郎, 水野忠則, 佐藤文男, 高橋修: コンピュータネットワーク, オーム社, 平成9年4月
- [2] 総務省平成14年版情報通信白書
- [3] 立川敬二: 移動通信とIT, 情報処理, Vol. 42, No. 1, pp. 1-7, 2001年1月
- [4] 永田清人, 入江恵: IMT-2000 サービス特集, NTT DoCoMo テクニカルジャーナル, Vol. 9, No. 2, pp. 1-7, July 2001
- [5] 山尾泰, 梅田成視, 大津徹, 中島信生: 第4世代移動通信の展望 無線通信システムを中心にした課題について, 電子情報通信学会論文誌 B, Vol. J-83-3, No. 10, pp. 1364-1373, Oct. 2000
- [6] 宮原秀夫: 通信技術からみたインターネットの検証 総論, 電子情報通信学会誌, Vol. 80, No. 2, pp. 112-117, Feb. 1999
- [7] 青山友紀: ネットワークの進化と IP 技術, 電子情報通信学会誌, Vol. 83, No. 4, pp. 248-256, April 2000
- [8] Carpenter, E. B. : 通信インフラストラクチャを目指した IP ネットワーク, 電子情報通信学会誌, Vol. 83, No. 4, pp. 257-262, April 2000
- [9] 森川博之: ワイヤレスインターネットの概要と展望, 電子情報通信学会誌, Vol. 83, No. 4, pp. 321-326, April 2000
- [10] 村田正幸: マルチメディアネットワークと通信品質保証, 電子情報通信学会誌, Vol. 81, No. 4, pp. 362-370, April 1998
- [11] 特集 VoIP: 情報処理学会誌, Vol. 42, No. 2, pp. 119-150, 2001年2月
- [12] Takahashi, O., Yoshitake, S. and Kawano, S. : Experience with a Remote Conformance Testing System, ICC '88, pp. 186-190, Nov. 1988
- [13] Takahashi, O., Shiroshita, T., Sano, T., Yamashita, M. and Nakamura, Y. : A Proposal for Reliable Information Multicast Environment : its Implementation and Evaluation, Proc. on IFIP World Congress '96: Advanced IT Tools, pp. 384-394, Sept. 1996
- [14] WAP Forum: WAP Forum Specifications. Available from <http://www.wapforum.org/>
- [15] Ueno, H., Ishikawa, N., Suzuki, H. Sumino, H. and Takahashi, O. : Performance evaluation on WAP and Internet protocol over 3G wireless

- networks, 2nd IFIP-TC6 Networking Conference (May 2002)
- [16] Dierks, T. and Allen, C. : The TLS Protocol Version 1.0, RFC 2246 (Jan. 1999)
- [17] Fielding, R., et al. : Hypertext Transfer Protocol - HTTP/1.1, RFC 2616 (June 1999)
- [18] Metter, M., et al. : WAP enabling existing HTML applications, " Proceedings First Australasian User Interface Conference (Jan. 2000)
- [19] Gordon, S., et al. : Analyzing the WAP Class 2 Wireless Transaction Protocol Using Coloured Petri Nets, " Proceedings of the 8th International Aerospace Congress incorporating the 12th National Space Engineering Symposium (Sept. 1999)
- [20] Kunz, T., et al., "WAP traffic: Description and comparison to WWW traffic," Proceedings of the Third ACM International Workshop on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM 2000) (Aug. 2000)
- [21] Inamura, H., Montenegro, G., et al. : TCP over 2.5G and 3G Wireless Networks, RFC3481 (Mar. 2003)
- [22] Allman, M., Paxson, V. and Stevens, W. : TCP Congestion Control, RFC 2581 (Apr. 1999)
- [23] Mathis, M., Mahdavi, J., Floyd, S. and Ramnow, A. : TCP Selective Acknowledge Options, RFC 2018 (Oct. 1996)
- [24] 3rd Generation Partnership Project (3GPP) : RLC Protocol Specification. Available from <http://www.3gpp.org> (Sept. 2001)
- [25] Allman, M., Floyd, S. and Partridge, C. : Increasing TCP's Initial Window, RFC 2414 (Sept. 1998)
- [26] Ishikawa, N., et al. : Consideration on the Mobile Internet Architecture for High-Speed Wireless Networks, INET 2001 (June 2001)
- [27] 上野英俊, 角野宏光, 鈴木偉元, 高橋修 : 移動通信におけるプッシュプロトコルの提案と評価, DICO MO 2001 シンポジウム (June 2001)
- [28] Pemberton, S., et al. : XHTML 1.0: The Extensible HyperText Markup Language, W3C Recommendation. Available from <http://www.w3.org/> (Jan. 2000)

- [29] WAP Forum: WAP Architecture Specification, WAP-100-WAPArch-19980430-a (1998)
- [30] 鈴木偉元, 上野英俊, 角野宏光, 石川憲洋, 高橋修: 無線シミュレータを用いた WAP プロトコルの性能評価, IPSJ Symposium Series (DICO2000), Vol. 2000, No. 7, pp. 283-288 (2000)
- [31] 上野英俊, 角野宏光, 鈴木偉元, 石川憲洋, 高橋修: WAP プロトコルの実装とプッシュ型アプリケーションへの適用, IPSJ Symposium Series (DICO2000), Vol. 2000, No. 7, pp. 289-294 (2000)
- [32] 石川太朗, 稲村浩, 高橋修: W-CDMA 向け TCP プロファイル, 情報処理学会 MBL/ITS 研究会, MBL15-3, pp. 17-24 (2000)
- [33] R. Fielding, et al.: Hypertext Transfer Protocol- HTTP/1.1, RFC2616 (1999)
- [34] World Wide Web Consortium: XHTML 1.0: Extensible HyperText Markup Language (2000)
- [35] World Wide Web Consortium: XSL Transformations (XSLT) Version 1.0 (1999)
- [36] World Wide Web Consortium: HTML 4.01 Specification (1999)
- [37] World Wide Web Consortium: Extensible Markup Language (XML) 1.0 (1998)
- [38] WAP Forum: WAP Push Architectural Overview, WAP-165-PushArchOverview-19991108-a (1999)
- [39] WAP Forum: Push Proxy Gateway Specification, WAP-151-PPGService-19990816-a (1999)
- [40] WAP Forum: Push Access Protocol Specification, WAP-164-PAP-19991108-a (1999)
- [41] WAP Forum: Wireless Datagram Protocol Specification, WAP-200-WDP-20000219-a (2000)
- [42] WAP Forum: Wireless Session Protocol Specification, WAP-203-WSP-20000504-a (2000)
- [43] WAP Forum: Push OTA Protocol Specification, WAP-189-PushOTA-20000217-a (2000)
- [44] 神場知成, 他: プッシュ型とプル型を統合したパーソナライズ情報配信システムの提案と実装, 情報処理学会論文誌, Vol. 39, No. 5, pp. 1514-1522

- (1998)
- [45] S. Deering: Host Extensions for IP Multicasting, RFC1112 (1989)
- [46] W. Fenner: Internet Group Management Protocol Version 2, RFC2236 (1997)
- [47] WAP Forum: Wireless Transaction Protocol Specification, WAP-201-WTP-20000219-a (2000)
- [48] WAP Forum: Push Architectural Overview, WAP-250-PushArchOverview-20010703-a (2001)
- [49] Jeffrey C. Mogul, et al.: Potential benefits of delta-encoding and data compression for HTTP, Proceeding of SIGCOMM 97 (1997)
- [50] World Wide Web Consortium: Document Object Model (DOM) Level 2 Core Specification Version 1.0 (2000)
- [51] 上野英俊, 角野宏光, 鈴木偉元, 石川憲洋, 高橋修: XML コンテンツの差分生成法とプッシュ型配信への応用, 情報処理学会研究会 モバイルコンピューティングとワイヤレス通信, Vol. 2002, No. 24, pp.107-114 (2002)
- [52] Bai, Y., Ogielski, T. and Wu, G. :Interactions of TCP and Radio Link ARQ Protocol, VTC' 99 (1999)
- [53] Khafizov, F. and Yavuz, M. : Running TCP over IS-2000, International Conference of Communications, IEEE (2002)
- [54] Karn, P. : Advice for Internet Subnetwork Designers (2002) . Internet draft, draft-ietf-pilc-link-design-09.txt
- [55] Holma, H. and Toskala, A. (Eds.) : WCDMA for UMTS, Revised Ed., Wiley (2001)
- [56] 3GPP : 3rd Generation Partnership Project, WWW. 3gpp. org.
- [57] 尾上誠蔵, 山本浩治 : IMT2000 サービス特集 : 技術概要, NTT DoCoMo テクニカルジャーナル, Vol. 9, No. 2 (2001)
- [58] Montenegro, G., Dawkins, S., Kojo, M., Magret, V. and Vaidya, N. : Long Thin Networks, RFC 2757 (2000)
- [59] Allmall, M. : On the Generation and Use of TCP Acknowledgments, Computer Communication Review, Vol. 28, No. 5 (1998)
- [60] Balakrishnan, H., Padmanabhan, V. and Katz, R. : The effects of asymmetry on TCP performance, ACM Mobile Networks and Applications (MONET), Vol. 4,

No. 3, pp. 219-241 (1999)

[61] Bakre, A. and Badrinath, B. : I-TCP : Indirect TCP for Mobile Hosts, 15th International Conference on Distributed Computing Systems (ICDCS), IEEE (1995)

[62] Balakrishnan, H., Seshan, S., Amir, E. and Katz, R. : Improving TCP/IP Performance over wireless Networks, 1st Conf. on Mobile Computing and Networking (Mobicom), ACM (1995)

[63] Ludwig, R. and Katz, R. : The Eifel Algorithm : Making TCP Robust Against Spurious Retransmissions, Computer Communication Review, Vol. 30, No. 1 (2000)

[64] Canton, A.-F. and Chahed, T. : End-to-end Reliability in UMTS : TCP over ARQ, Global Telecommunications Conference (Globecom) 2001, IEEE (2001)

[65] 古閑宏幸, 池永全志, 堀良彰, 尾家祐二 : Wireless 環境における TCP の性能評価 : Layer 2 ARQ およびパケット管理による影響, 信学技報 IN2001-39, pp. 19-24, 電子情報通信学会 (2001)

[66] Stekas, J. C. : Meeting Demands of Mobile Internet Applications, SAINT-2001, IEEE (2001)

[67] Paxson, V. and Allman, M. : Computing TCP's Retransmission Timer, RFC 2988 (2000)

[68] OPNET Technologies, I. : OPNET Manual.

[69] Ludwig, R. and Sklower, K. : The Eifel Retransmission Timer, Computer Communication Review, Vol. 30, No. 3, pp. 17-27 (2000)

[70] 山内長承, 串田高車, 富田アルベルト, 尾上裕子, 渥美幸雄 : 再送を伴う無線区間を持つインターネットでの動画転送時のバッファ制御, マルチメディア通信と分散処理, pp. 37-42, 情報処理学会 (2001)

[71] 吉村健, 大矢智之, 河原敏朗, 松岡保静, 榮藤稔 : モバイル QoS テストベッドの構築とマルチメディアストリーミング伝送実験評価, 信学技報 IN2001-41, pp. 31-38, 電子情報通信学会 (2001)

[72] Bakre, A. and Badrinath, R. : Handoff and Systematic Support for Indirect TCP/IP, Proceedings of the Second USENIX Symposium on Mobile and Location-Independent Computing, Ann Arbor, Michigan, April 10-11, 1995

[73] Brown, K. and Singh, S. : M-TCP: TCP for Mobile Cellular Networks,

- ACM Computer Communication Review, Vol. 27 (5), 1997, pp. 19-43
- [74] Kojo, M., Raatikainen, K., Liljeberg, M., Kiiskinen, J. and Alanko, T. : An Efficient Transport Service for Slow Wireless Telephone Links, IEEE Journal on Selected Areas of Communication, Vol. 15, No. 7, Sep. 1997
- [75] Yavatkar, R. and Bhagawat, N. : Improving End-to-End Performance of TCP over Mobile Internetworks, Proceedings of Workshop on Mobile Computing Systems and Applications, Dec. 1994
- [76] Fielding, R., Gettys, J., et al. : Hypertext Transfer Protocol -- HTTP/1.1, RFC2616, June. 1999
- [77] Allman, M. : On the New Generation and Use of TCP Acknowledgements, Computer Communication Review, Vol. 28, No. 5, 1998
- [78] Balakrishnan, H., Padmanabhan, V., et. Al. : The effects of asymmetry on TCP performance, ACM Mobile Networks and Applications (MONET), Vol. 4, No. 3, pp. 219-241, 1999
- [79] Jacobson, V., Braden, R. and Borman, D. : TCP Extensions for High Performance, RFC1323, May. 1992
- [80] 関口克己, 北口雅哉, 鶴巻宏治, 高橋修 : モバイルインターネットアクセスにおけるリクエストパイプラインングの有効性, 情報処理学会 MBL/ITS 合同研究会, Nov. 2000
- [81] 原政博, 中川格, 藤野信次 : 携帯電話網での Wireless Enhanced TCP の実装, 情報処理学会, DICO2001 シンポジウム
- [82] 長谷川輝之, 長谷川亨, 加藤聰彦, 鈴木健二 : 広域 ATM 網を介した LAN 間接続のための TCP ゲートウェイの実装と性能評価, 電子情報通信学会論文誌, Vol. J79-B-I, No. 5, pp. 262-270, May. 1996
- [83] 三宅優, 長谷川輝之, 長谷川亨, 加藤聰彦 : TCP によるデータ転送速度を高速化する衛星インターネット用 TCP ゲートウェイの提案, 電子情報通信学会論文誌, Vol. J84-B, No. 12, pp. 2330-2341, Dec. 2001
- [84] Postel, J. : User Datagram Protocol, RFC768, Aug. 1980.
- [85] Kent, S. and Atkinson, R. : Security Architecture for the Internet Protocol, RFC2401, Nov. 1998
- [86] Townsley, W., Valencia, A., et al. : Layer Two Tunneling Protocol L2TP, RFC2661, Aug. 1999

- [87] Kent, S. and Atkinson, R. : IP Authentication Header, RFC2402, Nov. 1998
- [88] Madson, C. and Glenn, R. : The Use of HMAC-MD5-96 within ESP and AH, RFC2403, Nov. 1998
- [89] Madson, C. and Glenn, R. : The Use of HMAC-SHA-1-96 within ESP and AH, RFC2404, Nov. 1998
- [90] Madson, C. and Doraswamy, N. : The ESP DES-CBC Cipher Algorithm With Explicit IV, RFC2405, Nov. 1998
- [91] Kent, S. and Atkinson, R. : IP Encapsulating Security Payload (ESP), RFC2406, Nov. 1998
- [92] Piper, D. : The Internet IP Security Domain of Interpretation for ISAKMP, RFC2407, Nov. 1998
- [93] Maughan, D., et al. : Internet Security Association and Key Management Protocol (ISAKMP), RFC2408, Nov. 1998
- [94] Harkins, D. and Carrel, D. : The Internet Key Exchange (IKE), RFC2409, Nov. 1998
- [95] Glenn, R. and Kent, S. : The NULL Encryption Algorithm and Its Use With IPsec, RFC2410, Nov. 1998
- [96] Pereira, R. and Adams, R. : The ESP CBC-Mode Cipher Algorithms, RFC2451, Nov. 1998
- [97] Simpson, W. : The Point-to-Point Protocol (PPP), RFC1661, July 1994
- [98] 渋谷尚久, 加藤紀康, 高木雅祐 : ハイブリット MMAC システムでの TCP スループット向上の一検討と性能評価, 情報処理学会 DICOMO 2001 シンポジウム 論文集, pp. 79-84, Jun. 2001
- [99] Kojo, M., Raatikainen, K. and Alanko, T. : Connecting Mobile Workstations to the Internet over a Digital Cellular Telephone Network, University of Helsinki, Helsinki, Sep. 1994
- [100] Border, J., et al. : Performance Enhancing Proxies Intended to Multigate Link-Related Degradations, RFC3135, Jun. 2002
- [101] 加藤紀康, 鎌形英二 : 非対称無線リンク用 TCP ゲートウェイ, 電子情報通信学会通信ソ大, 分冊 2, No. B-7-32, pp. 153, Oct. 1998
- [102] Postel, J. : TRANSMISSION CONTROL PROTOCOL, RFC793, Sept. 1981

- [103] Morris, T. R. : A Weakness in the 4.2BSD UNIX TCP/IP Software, Computing Science Technical Report 117, AT&T Bell Laboratories, Murray Hill, NJ, Feb. 1985.
- [104] 久米原栄 : TCP/IP セキュリティ, pp. 159-160, ソフトバンクパブリッシング, 2000
- [105] Bellovin, S. : Defending Against Sequence Number Attacks, RFC1948, May 1996
- [106] CERT Advisory : Statistical Weakness in TCP/IP Initial Sequence Numbers, CA-2001-09, May 2001
- [107] モバイル・インターネット最前線 : i モードから次世代システム IMT-2000 まで, 日経コミュニケーション, 日経ニューメディア (共編), Sep. 2000
- [108] 高橋竜男, 竹下敦, 関口克己 : モバイル向け VPN プロトコルの検討, 情報処理学会研究会, MBL10-7, Oct. 1999
- [109] 西郷悟, 高橋竜男, 三浦史光, 高橋修 : TCP アクセルレータにおける TCP ハイジャック防止対策, 電子情報通信学会総大, 分冊通信 2, No. B-7-196, PP. 329, 2001
- [110] Knight, S., et al. : Virtual Router Redundancy Protocol, RFC2338, Apr. 1998
- [111] 高橋竜男, 三浦史光, 西郷悟 : VPN ルータ冗長化に関する一検討, 電子情報通信学会総大, 分冊通信 2, No. B-7-186, PP. 329, 2001
- [112] Joncheray, L. : Simple Active Attack Against TCP, Merit Network Inc., 1996
- [113] Rescorla, E. : Diffie-Hellman Key Agreement Method, RFC2631, Jun. 1999

筆者発表論文

1. 論文誌

- 1) 荒木哲郎, 高橋修, 吉武静雄: 双対オートマトンに基づいた適合性試験の誤りシーケンス実現手順, 情報処理学会論文誌 Vol. 34 No. 6, pp. 1361-1370, 1993. 6
- 2) Suzuki, H., Kohkichi Tsuji, K., Araki, T., Takahashi, O. and Yoshitake, S. : A Method to Validate the Correctness of Test Logic Programs Applied in a Protocol Conformance Test System Using Petri Nets, IEICE transactions VOL. E77-A, No. 10, pp. 1663-1671, 1994. 10
- 3) 山内長承, 城下輝治, 佐野哲央, 高橋修: 高信頼同報バルク転送機構, 情報処理学会論文誌 Vol. 39, No. 6, pp. 2009-2019, 1998. 6
- 4) Kinoshita, S., Shiroshita, T., Nagata, T., Sano, T. and Takahashi, O. : The RealPush Network: A New Push-Type Content Delivery System Using Reliable Multicasting, IEEE Trans. on Consumer Electronics, Vol. 44, No. 4, pp. 1216-1224, 1998. 11
- 5) Shiroshita, T., Sano, T., Takahashi, O. and Yamanouchi, N. : Performance Evaluation of Bulk-Data Reliable Multicast Transport Protocol, IEICE Trans. Information and Systems, Vol. E82-D, No. 4, pp. 804-814, April 1999
- 6) 石川憲洋, 山内長継, 高橋修: IP マルチキャストのユーザ認証機能の提案と実装, 情報処理学会論文誌 Vol. 40, No. 10, pp. 3728-3736, 1999. 10
- 7) 山内長承, 城下輝治, 佐野哲央, 高橋修: 再送を伴う高信頼マルチキャストの送信レートと性能, 情報処理学会論文誌 Vol. 40, No. 12, pp. 4344-4352, 1999. 12
- 8) 山内長承, 石川憲洋, 高橋修 : IP マルチキャストの配送制御とそのセキュリティへの応用, 情報処理学会論文誌 Vol. 41, No. 1, pp. 167-176, 2000. 1
- 9) 石川憲洋, 木下真吾, 高橋修: プッシュ型情報配信のためのプロトコルとそのコンテンツ配信システムへの適用, 情報処理学会論文誌 Vo. 41, No. 2, pp. 245-253, 2000. 2
- 10) 渥美幸雄, 高橋修, 西正博, 吉田彰顕: 次世代インターネットのためのアクティブネットのルート設定方法とANTSの拡張方法, 情報処理学会論文誌 Vol. 42, No. 12, pp. 2897-2908, 2001. 12

- 11) 石川憲洋, 上野英俊, 鈴木偉元, 角野宏光, 高橋修: WAP プロトコルとインターネットプロトコルの性能評価に基づく IMT-2000 向けモバイルインターネットアーキテクチャの提案, 情報処理学会論文誌 Vol. 43, No. 10, pp. 3097-3106, 2002. 10
- 12) 高橋修, 上野英俊, 鈴木偉元, 石川憲洋, 水野忠則: 移動機向けプッシュアッププロトコルの提案と評価, 情報処理学会論文誌 Vol. 43, No. 10, pp. 3107-3118, 2002. 10
- 13) 稲村浩, 石川太郎, 高橋修, 渥美幸雄: W-CDMA 網でのリンク層 ARQ と TCP の特性評価, 情報処理学会論文誌 Vol. 43, No. 12, pp. 3859-3868, 2002. 12
- 14) 高橋修, 高橋竜男, 三浦史光, 西郷悟, 水野忠則: 移動網を介したモバイル VPN 方式の提案と評価, 情報処理学会論文誌 Vol. 43, No. 12, pp. 3898-3910, 2002. 12
- 15) 高橋修, 関口克己, 鶴巻宏治, 稲村浩, 渥美幸雄, 水野忠則: 第 3 世代移動通信網を介した高速インターネットアクセスのためのステルス型ゲートウェイの提案と実装評価, 情報処理学会論文誌 Vol. 44, No. 3, pp. 637-646, 2003. 03
- 16) 尾上裕子, 萩野浩明, 渥美幸雄, 高橋修, 駒木寛隆, 串田高幸, 山内長承: マルチメディアストリーミング配信サーバにおけるネットワーク情報活用型レート制御方式, 情報処理学会論文誌 Vol. 44, No. 3, pp. 625-636, 2003. 03
- 17) Ueno, H., Ishikawa, N., Suzuki, H., Sumino, H. and Takahashi, O.: Performance Evaluation of WAP and Internet Protocols over W-CDMA networks, the Cluster Computing Journal (accepted)
- 18) 上野英俊, 田中希世子, 鈴木偉元, 石川憲洋, 高橋修: マルチキャスト通信のためのアクセス制御&グループ鍵配信プロトコル, 電子情報通信学会システムソサエティ/情報処理学会情報技術レターズ, Vol. 2 (accepted)

2. 国際会議 (査読付き)

- 1) Takahashi, O. and Morino, K.: A Technique for describing High-level Data Link Control (HDLC) Procedures, Proc. on IFIP Congress' 80, pp. 575-580, Oct. 1980
- 2) Takahashi, O., S. Anano, et al.: Heterogeneous Interconnection for Mutual Utilization of Distributed Databases on Chemical Substances, Proc. on ICC' 86, pp. 407-412, Sept. 1986

- 3) Takahashi, O. S. Yoshitake, S. et al. ; Experience with a Remote Conformance Testing System, Proc. on ICC '88, pp.186-190, 1988. 11
- 4) Takahashi, O., Shiroshita, T., Sano, T., Yamashita, M. and Nakamura, Y. : A Proposal for Reliable Information Multicast Environment : its Implementation and Evaluation, Proc on IFIP World Congress '96:Advanced IT Tools, pp.384-394, Sept. 1996
- 5) Shiroshita, T., Sano, T., Takahashi, O., Yamashita, M., Yamanouchi, N. and Kushida, T. : Performance evaluation of reliable multicast transport protocol for large-scale delivery, Proc. on IFIP Protocols for High-Speed Networks (PfHSN), pp.149-164, Oct. 1996
- 6) Shiroshita, T., Sano, T., Takahashi, O. and Yamashita, M. : Integrating Layered Security into Reliable Multicast, IEEE 3rd Intl. Workshop on Protocols for Multimedia Systems (PROMS'96), Oct. 1996
- 7) Shiroshita, T., Takahashi, O., Yamashita, M. and Nakamura, Y. : Reliable Data Distribution Middleware for Large-scale Massive Data Replication, Proc. on ACM/IEEE 4th Intl. Conf. on Parallel and Distributed Information Systems (PDIS'96), pp.196-205, Dec. 1996
- 8) Sano, T., Shiroshita, T. Takahashi, O. and Yamashita, M. : Monitoring-based Flow Control for Reliable Multicast Protocols and its Evaluation, IEEE intl. Performance, Computing, and Communication Conference (IPCCC) '97, Feb. 1997
- 9) Shiroshita, T., Takahashi, O. and Shiokawa, S. : A Large-scale Contents Publishing Architecture based on Reliable Multicast, Proc. on ACM SIGDOC97 Conference, pp.243-247, Oct. 1997
- 10) Kinoshita, S., Shiroshita, T., Nagata, T., Sano, T. and Takahashi, O. : RealPush Network:A New Push-type Content Delivery System using Reliable Multicast and Flexible Browser, Proc. on IEEE ICCE'98, pp.188-189, June. 1998
- 11) Kinoshita, S., Shiroshita, T., Nagata, T., Sano, T. and Takahashi, O. : RealPush Network: A Multicast Based Push System and Experimental Services, Proc. on IEEE MATC'98, pp.296-302, Sept. 1998.
- 12) Shiroshita, T., Sano, T., Takahashi, O. and Komatsu, T. : Evaluation

of Reliable Multicast over Unidirectional Satellite and Terrestrial Network, ACM/IEEE Workshop for Satellite Based Information Systems (WOSBIS' 98), 1998. 10

13) Sano, T., Shiroshita, T., Takahashi, O. and Yamanouchi, N. : Flow/Congestion Control for Bulk Reliable Multicast, Proc. on SPIE Int. Sympo. on Voice and Data Communication Conf., pp.329-339, Oct. 1998

14) Shiroshita, T., Takahashi, O. and Kokubun, Y. : A Large-scale Contents Distribution Architecture Based on Reliable Multicast, IEEE Internet Workshop (IWS)' 99, Mar. 1999

15) Ishikawa, N., Yamanouchi, N. and Takahashi, O. : An Architecture for User Authentication of IP Multicast and Its Implementation, IEEE Internet Workshop (IWS)' 99, Mar. 1999

16) Kinoshita, S., Nagata, T., Shiroshita, T., Ishikawa, N., Sano, T. and Takahashi, O. : Scalable, Real-time and Multicast/Unicast-Switchable Push technology, and Trial services, 8th International WWW Conference, May 1999

17) Ishikawa, N., Kinoshita, S. and Takahashi, O. : An Architecture for Push Information Delivery and its Application to News Delivery Systems, Proc. on ISOC INET' 99, June 1999

18) Onoe, Y., Atsumi, Y., Takahashi, O., Sato, H. and Mizuno, T. : An Efficient IP Mobility Control Scheme for Next-generation Mobile Communication Networks, Proc. on the 7th International Workshop on Mobile Multimedia Communication (MoMuC) 2000, pp. 2B/3/1-6, Oct. 2000

19) Ishikawa, N., Ueno, H., Sumino, H., Suzuki, H. and Takahashi, O. : Considerations on the Mobile Internet Architecture for High-Speed Wireless Networks, INET 2001, June 2001

20) Ueno, H., Ishikawa, N., Suzuki, H., Sumino, H. and Takahashi, O. : Performance evaluation on WAP and Internet Protocol over 3G wireless networks, IFIP Networking 2002, Lecture Note in Computer Science 2345, pp. 527-538, May 2002

21) Ishikawa, N., Hujiwara, H., Ueno, H., Suzuki, H. and Takahashi, O. : Domain Constrained Multicast : New Approach for IP Multicast Routing,

Internetworking 2003 International Conference, June 2003

22) Miyake, M., Inamura, H. and Takahashi, O. : TCP Enhancement using Spurious Timeout Detection and Congestion Window Control Algorithm, 8th International Workshop on Multimedia Communications MoMuC2003, Oct. 2003 (accepted)

3. 口頭発表 (研究会等)

- 1) 高橋修, 森野和好 : ハイレベルデータリンク制御手順の規定とその評価, 1 情報処理学会コンピュータネットワーク研究会, CN8-1, 1976. 11
- 2) 高橋修, 森野和好, : ハイレベルデータリンク制御手順の規定方法について, 昭和 51 年度情報処理学会全国大会, 1976
- 3) 高橋修, 森野和好 : HDLC 手順のシュミレーションによる性能評価, 昭和 52 年度情報処理学会第 18 回全国大会, 1977
- 4) 藤田勝美, 高橋修 : パケット交換網のバランス形 HDLC 手順, 昭和 53 年度信学会総合全国大会, 1978
- 5) 高橋修, 森野和好 : ネットワークアーキテクチャに基づいて設計された端末の性能に関する検討, 昭和 54 年度信学会総合全国大会, 1979
- 6) 高橋修, 梶原俊男, 大原康弘 : システム間接続に関する一考察, 昭和 55 年電子通信学会総合全国大会, 1980
- 7) 梶原俊男, 高橋修, 他 : DCNA と他ネットワークアーキテクチャとの相互接続法, 情報処理学会第 22 回全国大会, 1982
- 9) 高橋修 : DCNA 製品に関する検証項目抽出方法の一考察, 昭和 57 年電子通信学会総合全国大会, 1982
- 10) 高橋修, 高田賢次 : 複数ノード疑似方式による DCNA 検証システムの試作, 昭和 57 年電子通信学会総合全国大会, 1982
- 11) 高橋修, 梶原俊男 : 衛星回線による同報データ通信方式の一考察, 昭和 59 年度信学会通信部門全国大会, 1984
- 12) 川野繁一, 高橋修, 吉武静雄, 河岡司 : 異機種データベース共用ネットワーク構成方式とその評価, 情報処理学会マルチメディアと分散処理研究会 34-10, 1987. 7
- 13) 小林偉昭, 高橋修, 新田哲二 : INTAP における OSI コンフォーマンス試験 -ODA/ODIF, 第 37 回情報処理学会全国大会 (昭和 63 年後期), 1989

- 14) 河村浩光, 熊白侃彦, 高橋修, 和田豊, 武富章吾, 馬渡恭三郎: OSI 試験検証システムトランスポート層上位テストの開発, 第 38 回情報処理学会全国大会 (平成元年前期), 1989. 10
- 15) 吉田篤正, 櫃間しのぶ, 高橋修: プロファイルの適合性要求条件記述方式の適用-データリンク層及び物理層-, 第 39 回情報処理学会全国大会 (平成元年後期), 1990. 3
- 16) 松本孝純, 天野正康, 高橋修: プロファイルの適合性要求条件記述方式の適用-トランスポート層-, 第 39 回情報処理学会全国大会 (平成元年後期), 1990. 3
- 17) 高橋修, 吉武静雄, 那須野洋一: プロファイルの適合性要求条件記述方式 (総論), 第 39 回情報処理学会全国大会 (平成元年後期), 1990. 3
- 18) 高橋修, 吉田篤正, 中嶋正樹, 梅田伸明: OSI 実装規約: ISDN 実装規約-概要-, 第 43 回情報処理学会全国大会 (平成 3 年後期), 1992. 3
- 19) 福岡瑞枝, 高橋修, 香取勉: OSI プロトコル適合性試験方式の一考察, 第 43 回情報処理学会全国大会 (平成 3 年後期), 1992. 3
- 20) 鈴木博人, 荒木哲郎, 吉武静雄, 高橋修: オブジェクト指向による適合性試験システムの構成法, 信学会春季全国大会, 1993
- 21) 高橋修: 高速通信におけるプロトコルの課題, 信学会第 6 回情報電送と信号処理ワークショップ, 1993. 11
- 22) 城下輝治, 高橋修, 他: インターネットに適用可能な高信頼一斉分配システム, 画像通信学会オーディオビジュアル複合情報処理 11-2, 1995. 12
- 23) 佐野哲央, 城下輝治, 高橋修: 高信頼マルチキャストプロトコルにおけるフロー制御方式の検討, 信学会情報ネットワーク研究会, 信学技報 SSE95-197, IN95-141 (1996-3), 1996. 3
- 24) 城下輝治, 高橋修, 山下正秀, 山内長承, 串田高幸: 高信頼マルチキャスト通信プロトコル (RMTP) の各種ネットワークへの適用性, 信学会, 交換システム研究会/情報ネットワーク研究会, SSE95-196, IN95-140 (1996-03), pp. 137-144, 1996. 3
- 25) 城下輝治, 高橋修, 山内長承: 高信頼マルチキャスト通信プロトコル (RMTP) の大規模環境への適用性評価, インターネットコンファレンス' 96, 1996. 7
- 26) 佐野哲央, 城下輝治, 高橋修: 高信頼マルチキャストプロトコルに適したフロー制御方式の提案, 1997 年電子情報通信学会総合大会, 1997. 3
- 27) 山内長承, 城下輝治, 高橋修: 高信頼マルチキャストにおけるフロー制御・

- 輻輳制御, インターネットコンファレンス'97, 1997. 7
- 28) 城下輝治, 高橋修, 山内長承: モバイル環境対応の高信頼マルチキャスト通信プロトコル, 情報処理学会シンポジウム DICOMO' 97, 1997. 7
- 29) 山内長承, 城下輝治, 高橋修: 高信頼同報での再送機構の Ack Implosion の再評価, 情報処理学会第 55 回全国大会, 1997. 9
- 30) 高橋修, 城下輝治, 佐野哲央, 國分康彦, 山内長継: マルチキャストを利用したプッシュ型高信頼情報配信サービスとプロトコル, 信学会交換システム研究会 (SSE97-128), 信学技報 Vol. 97No. 353, pp. 13-18, 1997. 10
- 31) 佐野哲央, 城下輝治, 高橋修: TCP との共存を目指した Reliable Multicast の輻輳制御方式の提案, 情報処理学会, マルチメディア通信と分散処理研究会 (85-8), 1997. 11
- 32) 高橋修, 城下輝治, 木下真吾, 佐野哲央, 長田孝彦: マルチキャストを利用したプッシュ型高信頼情報配信サービスとプロトコル, UNCL 第 2 回通信プロトコルワークショップ, 1998. 5
- 33) 石川憲洋, 山内長承, 高橋修: IP マルチキャスト通信へのユーザ認証機能の導入, 情報処理学会マルチメディア通信と分散処理研究会 (89-6), 1998. 6
- 34) 木下真吾, 城下輝治, 高橋修, 他: RealPush Network: 高信頼マルチキャストを利用した新しいプッシュ型コンテンツ配信システム, 情報処理学会シンポジウム DICOMO' 98, pp. 273-280, 1998. 7
- 35) 山内長承, 佐野哲央, 城下輝治, 高橋修: 再送を伴う高信頼マルチキャストの送信レートと性能, 情報処理学会第 57 回全国大会論文集 (4F-11), 1998. 10
- 36) 山内長承, 石川憲洋, 高橋修: マルチキャストセキュリティにおける配送制御の効果と暗号の役割分担, インターネットコンファレンス'98, 1998. 12
- 37) 渥美幸雄, 高橋修: アクティブネットによるギャザリング方式の一検討, 信学総合大会, 2000. 3
- 38) 尾上裕子, 渥美幸雄, 高橋修, 佐藤文明, 水野忠則: Mobile IP 網における効率的 IP ベース・ハンドオーバー方式, 情報処理学会シンポジウム DICOMO' 00, 2000. 7
- 39) 鈴木偉元, 上野英俊, 高橋修, 他: 無線シミュレータを用いた WAP プロトコルの性能評価, 情報処理学会シンポジウム DICOMO' 00, 2000. 7
- 40) 鈴木偉元, 上野英俊, 高橋修, 他: WAP 通信プロトコルの実装と評価, 情報処理学会シンポジウム DICOMO' 00, 2000. 7
- 41) 上野英俊, 鈴木偉元, 高橋修, 他: WAP プロトコルの実装とプッシュ型アプリケーション, 情

報処理学会シンポジウム DICOMO' 00, 2000. 7

- 42) 関口克己, 鶴巻宏治, 北口雅哉, 高橋修: モバイルインターネットアクセスにおけるリクエストパイプラインの有効性, 情報処理学会第 15 回モバイルコンピューティングとワイヤレス通信 (MBL) 研究会, 2000. 11
- 43) 石川太郎, 稲村浩, 高橋修: W-CDMA 向け TCP プロファイル, 情報処理学会第 15 回モバイルコンピューティングとワイヤレス通信 (MBL) 研究会, 2000. 11
- 44) 西郷悟, 高橋竜男, 三浦史光, 高橋修: TCP アクセルレータにおける TCP ハイジャック防止対策, 2001 年信学総合大会, 2001. 3
- 45) 鈴木偉元, 藤原廣則, 上野英俊, 石川憲洋, 高橋修: モバイル端末向けマルチキャスト配信技術の検討, 情報処理学会第 17 回モバイルコンピューティングとワイヤレス通信 (MBL) 研究会, 2001. 5
- 46) 串田高幸, 富田アルベルト, 高橋修, 他: モバイルマルチメディア QoS の構成方式, 情報処理学会シンポジウム DICOMO' 01, 2001. 7
- 47) 安木成比古, 渥美幸雄, 高橋修, 他: エンストリーミングのための QoS 制御フレームワーク, 情報処理学会シンポジウム DICOMO' 01, 2001. 7
- 48) 石川憲洋, 藤原廣則, 高橋修, 他: ドメイン限定マルチキャストの提案, 情報処理学会シンポジウム DICOMO' 01, 2001. 7
- 49) 上野英俊, 石川憲洋, 高橋修, 他: 移動通信におけるプッシュバックの提案と評価, 情報処理学会シンポジウム DICOMO' 01, 2001. 7
- 50) 高橋修: IMT-2000 サービスとモバイルインターネットの研究開発の展望, 信学会北陸支部講演会, 2001. 8
- 51) 稲村浩, 石川太郎, 高橋修: W-CDMA 網での TCP トラヒック特性, 情報処理学会 MBL 研究会 (18-5), 2001. 9
- 52) 村尾高秋, 谷口雅昭, 串田高幸, 萩野浩明, 尾上裕子, 高橋修: ワイヤレス区間を想定したビデオストリーミングシステム, 情報処理学会第 104 回マルチメディアと分散処理 (DPS) 研究会 (104-11), 2001. 9
- 53) 西郷悟, 三浦史光, 高橋修: SSL におけるモバイル向け鍵管理システム, 情報処理学会 CSEC 研究会, 2002. 2
- 54) 鈴木偉元, 藤原廣則, 石川憲洋, 上野英俊, 高橋修: モバイル・マルチキャスト通信のための FEC/ARQ ハイブリット制御方式の検討, 情報処理学会第 20 回モバイルコンピューティングとワイヤレス通信 (MBL) 研究会, 2002. 3
- 55) 上野英俊, 鈴木偉元, 石川憲洋, 加藤剛志, 角野宏光, 高橋修: XML コン

- テンツの差分生成法とプッシュ型配信への応用, 情報処理学会第 20 回バイルコンピューティングとワイヤレス通信 (MBL) 研究会, 2002. 3
- 56) 三浦史光, 高橋修: ブラウザフォンにおける多国語ドメイン利用に関する 1 考察, 情報処理学会第 21 回バイルコンピューティングとワイヤレス通信 (MBL) 研究会 (21-16), 2002. 5
- 57) 上野英俊, 石川憲洋, 鈴木偉元, 高橋修: モバイル端末を対象としたプッシュサービス向けスクリプト言語の提案, 情報処理学会シンポジウム DICOM0'02, 2002. 7
- 58) 横田和久, 稲村浩, 高橋修: ワイヤレスネットワーク環境におけるメール受信の効率改善, 情報処理学会シンポジウム DICOM0'02, 2002. 7
- 59) 西郷悟, 三浦史光, 高橋修: 柔軟な多対一決済に関する研究, 情報処理学会第 19 回コンピュータセキュリティ研究会 (CSEC), 2002. 12
- 60) 三宅基治, 稲村浩, 高橋修: スプリアス・タイムアウト検出と輻輳ウィンドウ制御アルゴリズムに関する研究, 情報処理学会第 24 回モバイルコンピューティングとワイヤレス通信 (MBL) 研究会, 2003. 3
- 61) 石川太郎, 藤波勉, 稲村浩, 高橋修: TCP 実装試験手法の検討, 情報処理学会第 24 回モバイルコンピューティングとワイヤレス通信 (MBL) 研究会, 2003. 3
- 62) 西郷悟, 三浦史光, 高橋修: モバイル環境における多対一決済に関する考察, 情報処理学会シンポジウム DICOM02003, 2003. 6
- 63) 上野英俊, 石川憲洋, 高橋修, 他: マルチキャストセキュリティアーキテクチャの提案と実装, 情報処理学会シンポジウム DICOM02003, 2003. 6
- 64) 田中希代子, 上野英俊, 高橋修, 他: コンテキスト情報を用いたマルチキャスト配信アーキテクチャの提案, 情報処理学会シンポジウム DICOM02003, 2003. 6
- 65) 高橋竜男, 高橋修: モバイル向けシンクライアントシステムにおけるグラフィック制御機能の検討, 情報処理学会シンポジウム DICOM02003, 2003. 6
- 66) 三宅基治, 稲村浩, 高橋修: 移動体通信に有効なスプリアス・タイムアウト検出アルゴリズムに関する研究, 情報処理学会シンポジウム DICOM02003, 2003. 6
- 67) 鈴木偉元, 原下貴志, 田中希代子, 上野英俊, 石川憲洋, 高橋修: 無線 LAN での誤り回復方法の評価, 情報処理学会シンポジウム DICOM02003, 2003. 6
- 68) 殿内雅晴, 峰野博史, 石原進, 高橋修, 水野忠則: モバイル通信を指向した動的マルチリンク TCP の設計, 情報処理学会シンポジウム DICOM02003, 2003. 6

4. 著書, 解説記事, 等

- 1) 高橋修 (共著) : インタラクティブテレビ-通信放送融合へのチャレンジ, 日経ニューメディア別冊, 1994 年
- 2) 高橋修 (共著) : 情報処理ハンドブック, オーム社, 1995. 1
- 3) 白鳥則郎, 水野忠則, 高橋修, 佐藤文明 : コンピュータネットワーク, オーム社, 1997. 3
- 4) 高橋修 : プッシュ型情報配信サービス/技術の展望, 情報処理学会誌解説記事 Vol. 39, No. 11, pp. 1124-1131, 1998. 11
- 5) 石川憲洋, 高橋修 : モバイルインターネットプロトコル, 情報処理学会誌解説記事 Vol. 42, No. 12, pp. 1204-1209, 2001. 12
- 6) 石川憲洋, 高橋修 : モバイルインターネットの発展, 電子情報通信学会誌解説記事 Vol. 86, No. 3, pp. 169-173, 2002. 10
- 7) 高橋修 (共著) : 標準 MPEG 教科書, ASCII, 2003. 2