マルチメディア通信における
通信性能の改善に関する研究

上野 英俊

システム情報工学研究科

筑波大学

２００６ 年 ３ 月

要旨

本論文では，インターネットや移動通信網等の各種通信ネットワークにおいて，様々なアプリケーションやネットワークサービスを実現するためのマルチメディア通信に着目し，これらの通信性能を改善するために既存の通信プロトコルの改善や新規通信プロトコルの提案を行うことを目的としている．

これを達成するため，本論文の前半では，インターネットにおける基本通信プロトコルである TCP（Transmission Control Protocol）に着目する．そしてこの TCP 上でマルチメディア通信において重要となる優先制御を実現するため, RED（Random Early Detection）ゲートウェイを用いた明示的輻輳通知方式を改良した優先輻輳制御アルゴリズムを提案する．その後，計算機シミュレーションによる性能評価を行うことで，提案方式は従来方式と同等な平均スループットを保ちながら優先制御が可能であり，通信ネットワークの利用効率の向上を図ることができることを示す．次に，W-CDMA（Wideband Code Division Multiple Access）等の第三世代移動通信網において効率の良い通信を提供するため，第一世代，第二世代移動通信網で利用されている通信プロトコル WAP（Wireless Application Protocol）とインターネットで利用されている HTTP（Hypertext Transfer Protocol）/TCP のどちらが第三世代移動通信網に適するのかを検討する．そのため，W-CDMA シミュレータ上に WAP と HTTP/TCP を実装し，それぞれの通信プロトコルの性能を評価する．その結果，第三世代移動通信網等の高速なネットワークにおいては HTTP/TCP を利用する方がより適することを示すとともに，以上を踏まえた第三世代移動通信網向け通信プロトコルとネットワークアーキテクチャの提案を行う．

本論文の後半では，特定多数の受信者に対してデータの同報配信を可能とし，通信ネットワークの利用効率を飛躍的に向上させる IP マルチキャストに着目する．そして，IP マルチキャストにおける課題であった，データ秘匿のためのグループ鍵の配布，DoS（Denial of Service）攻撃対策のための受信者アクセス制御，およびユーザ課金のための受信者認証の 3 つの機能を提供する目的から，マルチキャスト用受信者認証グループ鍵配布プロトコル AKDP（Receiver Authentication and Group Key Delivery Protocol）を提案する．また AKDP では，状況に応じて必要な機能を適切に提供するためのネゴシエーション機能を持つことから，IP マルチキャストを利用する多様なアプリケーションの要求に応えることが可能であることを示す．そして，プロトタイプシステムにおける処理時間の測定と受信者数に対する通信オーバヘッドの理論解析により，本プロトコルによる処理遅延は十分小さくシステム運用上の問題は少ないこと，ネゴシエーション機能により必要となる機能に応じて処理遅延を低減させることが可能であることなどを示す．次に，無線 LAN や移動通信網等の無線を利用したネットワークでの利用を想定し，受信者が移動する状況における制御パケット数の削減や，受信端末の消費電力の低減を目的としたモバイルマルチキャスト向けグループ管理プロトコル MMGP（Mobile Multicast Group Management Protocol）を提案する. 同プロトコルはセキュリティについても考慮されており, マルチキャスト DoS への対策が可能である．そして，計算機シミュレーションにより，制御パケット数と受信者の送受信パケット数を評価し，提案方式は従来方式と比べて通信コストを低くすることが可能であることを示す．また，AKDP と MMGP の併用に関しても議論する．

最後に，本論文のまとめとして，本論文で提案した研究とマルチキャスト通信プロトコルと他のプロトコルとの関連を示すとともに，本論文に残された課題について述べる．

目次

図目次

表目次

第1章 はじめに

近年，半導体技術の高度化と省電力化技術の向上等により，コンピュータは高性能になる一方で，小型軽量化が進んでいる．また，ADSL（Asynchronous Data Subscriber Line）や光ファイバ等によるブロードバンド通信や，無線 LAN（Local Area Network）や携帯電話等による移動通信の普及に伴い，これらの通信ネットワークを用いた様々なアプリケーションやサービスが時間や場所に関係なく，より手軽に利用出来る環境が整備されつつある．その結果，今後さらに多様化が進むと予想されるアプリケーションやサービスを効率良く提供するためのマルチメディア通信の重要性が高まっている．

例えば，インターネット利用開始当初は電子メールや FTP（File Transfer Protocol）などのファイル転送が主に利用されていたことから，伝送されるデータの信頼性が特に重要であった．このため，IETF（Internet Engineering Task Force）では，1981 年に TCP（Transmission Control Protocol）[1]の仕様化を行い，TCP データの再送制御や輻輳制御などの機能が提供された．この TCP は，インターネットにおける最も基本的な通信プロトコルとして今日も多くのアプリケーションによって利用されている．その一方で，ネットワークの利用環境の向上に伴い，音声や動画像などのデータを伝送することが要求されるようになった．これらのデータの転送はリアルタイム性を持つのが典型であり，データの信頼性よりも高速かつ低遅延に伝送することが要求される．このため，TCP ではこれらのサービスが要求する通信品質を満たすことが困難であった．さらに，一対多の放送型のデータ配信サービスやビデオ会議アプリケーションなどでは，送信者から送信されたリアルタイム性を持つデータを特定グループに属するメンバ全員に対して送信する必要があり，TCP とは異なる仕組みによる効率の良い通信を提供することが急務となっていた．

そこで本論文では，インターネットや移動通信網等の各種通信ネットワークにおいて，多様化するアプリケーションやサービスを提供するマルチメディア通信を対象に，その通信性能を改善するためのプロトコルの提案とその評価を行う．

本論文の構成は以下の通りである．まず第 2 章では，マルチメディア通信を実現するための通信プロトコル技術について整理し，本論文で最初に取り上げる TCP についてその概要を説明する．次に多数の受信者に対してデータの同報配信を実現することにより飛躍的に通信効率を向上させるマルチキャストについて取り上げ，特に IP（Internet Protocol）上でマルチキャストを実現する IP マルチキャスト[2][3]とその関連技術の整理を行う．

続いて第 3 章，および第 4 章では，TCP 上で多様なアプリケーションやサービスを提供するためのプロトコルを提案する．

まず第 3 章では，TCP が要求通信品質の異なるコネクションを公平に扱う問題を解決するため，各コネクションに与えられた優先度に基づく制御を行う優先制御機能を導入する．本方式では，IPv6（IP version6）[4]を対象に，TCP の輻輳制御を効果的に行うために設置される RED（Random Early Detection）ゲートウェイを用いた明示的輻輳通知方式を改良する．また，本方式の性能評価により，従来方式と同等な平均スループットを保ちながら提案方式による優先制御が可能であることを示す[5].

一方，携帯電話等による移動通信網では，速度が低く，エラー発生率が高いといった無線通信特有の性質から，データ通信に TCP をそのまま適用することは問題があった．そこで，第一世代移動通信網，および第二世代移動通信網向けに，携帯電話等から Web ページなどを参照するための通信プロトコルとして WAP（Wireless Application Protocol）[6]が 1998 年に提案された．第 4 章では，第一世代移動通信網と第二世代移動通信網と比べて通

信速度が格段に向上した第三世代移動通信網において，WAP とインターネットにおいてこれと同等の機能を提供する HTTP/TCP（TCP 上で実行した HTTP（Hypertext Transfer Protocol））のいずれが好ましいのかを，W-CDMA（Wideband Code Division Multiple Access）を用いた評価実験を通じて比較検討する．そして，第三世代移動通信網以降の高速なネットワークの場合，HTTP/TCP を利用することが好ましいことを示し，ここで得られた結果に基づき，第三世代移動通信網向けに適する通信プロトコルとネットワークアーキテクチャを提案する[7].

以上で検討の対象とした TCP は，送受信者が 1 対 1 のユニキャスト通信でのみ利用される．しかし，放送型のデータ配信サービスやビデオ会議アプリケーションなどを TCP により提供した場合，個々の送信者が配信対象となるグループに属する全てのメンバに対してデータを逐次的に送る必要があるほか，メンバの加入や離脱を適切に管理する必要があり，その実現は容易ではない．そこで，第 5 章，第 6 章では，グループに属するメンバに対してデータの同報配信を可能とすることで，通信ネットワークの利用効率を飛躍的に向上させる IP マルチキャストに着目した．この IP マルチキャストでは，ルータにおいて受信者を送信インタフェース単位で集約しながら送信データを複製して中継するため，1 つのネットワーク内でグループメンバが増加した場合でもデータの通信量は増加しないという特徴があり，マルチメディア通信の品質向上のために非常に重要である[2][3]．しかし，マルチキャストを利用するには解決すべき課題が数多く残されている．

そこで第 5 章では，これらの課題のうち，マルチキャストセキュリティに着目し，マルチキャスト配信経路が不正構築されるマルチキャスト DoS（Denial of Service）攻撃が可能となる問題とユーザ課金が実現困難な問題に対処するため，マルチキャスト用受信者認証グループ鍵配布プロトコル AKDP（Receiver Authentication and Group Key Delivery Protocol）を提案する．このプロトコルでは，データ秘匿のためのグループ鍵の配布，受信者アクセス制御，およびユーザ課金を実現するための受信者認証の 3 つの機能を提供する．そして，AKDP の実装システムを用いた性能評価により，その有効性を示す[8].

続いて第 6 章では，既存のグループ管理プロトコルを移動通信網や無線 LAN で適用した場合，通信コストが高くなるほか，電源断や移動によりクライアントとの接続が突然途絶えた場合の対策が行われていない問題を解決するため，モバイルマルチキャスト向けのグループ管理プロトコル MMGP（Mobile Multicast Group Management Protocol）[9]を提案する．そして，MMGP と既存のマルチキャスト向けグループ管理プロトコル IGMP（Internet Group Management Protocol）[10][11]の制御パケット数などを比較することにより，提案方式の方がより少ない通信量でグループ管理の実現が可能であることを示す[9].

最後に第 7 章では，本論文のまとめと今後の課題について述べる．

第2章 マルチメディア通信を実現する技術の概要

本章では，マルチメディア通信を実現するための技術，特に通信ネットワークと通信プロトコルについて整理し，その中で最初に本論文で取り上げる TCP[1]についてその概要を説明する．次に多数の受信者に対してデータの同報配信を実現するマルチキャストについて取り上げ，特に IP 上でマルチキャストを実現する IP マルチキャスト[2][3]とその関連技術の整理を行う．

2.1. 通信ネットワークと通信プロトコル

通信ネットワークは，WAN（Wide Area Network）と LAN （Local Area Network），そして主に LAN を WAN のバックボーンネットワークまで接続するアクセス回線の 3 種類に大別出来る．

WAN は，地域や国，世界全体といった規模をカバーする広域なネットワークであり，バックボーンネットワークとしての役割を担う．このうち，1990 年頃に登場した ATM（Asynchronous Transfer Mode）により各種アプリケーションが要求するサービス品質に応じた非同期通信が可能となり，マルチメディア通信性能の向上に大きく貢献した．この数年では，ATM から広域イーサネット等の IP ネットワークへの移行が進み，数 Gbps～数 10Gbps のバックボーンネットワークが構築されるなど，その高速化は加速している．

LAN は，室内や建物内，組織内といった比較的小規模なネットワークであり，ユーザが直接接続するネットワークとして位置付けられる．1980 年代から 10Mbps の通信速度を持つイーサネットが利用され始め，その後，100Mbps から 1Gbps へと通信速度が向上した．最近では 10Gbps の通信速度を持つ 10 ギガビットイーサネットに移行しつつあるなど，その高速化はますます加速している．また，通信媒体に無線を利用する無線 LAN の出現により，LAN におけるネットワークケーブルの敷設が不要となるなど，ネットワーク設計の自由度が増している．無線 LAN については，理論上 11Mbps の通信速度を実現する IEEE（Institute of Electrical and Electronic Engineers）802.11b や，理論上 54Mbps の通信速度を実現する IEEE802.11g や IEEE802.11a 等が存在し，本論文執筆時点ではより高い通信速度を提供する IEEE802.11n 等について標準化が進められている．

アクセス回線は，主に LAN を WAN のバックボーンネットワークまで接続するために用いられ，1990 年代までは電話回線を用いたモデム接続や ISDN （Integrated Service Digital Network）による低速回線が主流であった．しかし，2000 年前後から ADSL や光ファイバを用いた高速回線へとシフトしてきており，その普及率の高さと価格の安さの面で我が国は世界をリードする水準に達している．また，携帯電話のデータ通信機能を用いることにより，移動通信網をアクセス回線として利用する形態が出現している．これらの移動通信網は，アナログ回線を用いて 1979 年にサービスが開始された第一世代移動通信網（1G）から，その伝送方式をデジタル化し 1993 年からサービスが開始された第二世代移動通信網（2G）を経て，ここ数年では CDMA（Code Division Multiple Access）技術を用いた第三世代移動通信網（3G）が普及し，その伝送速度が第二世代移動通信網までと比較し

て飛躍的に向上している（図2.1）．移動通信網は，利用場所に対する自由度が極めて高く，また，ユーザが移動しながら利用可能であることから利便性が高い．その一方で，有線ネットワークと比較するとその伝送速度は相対的に低く，伝搬遅延やデータ誤り率が高いといった通信品質を持つという問題も存在する．

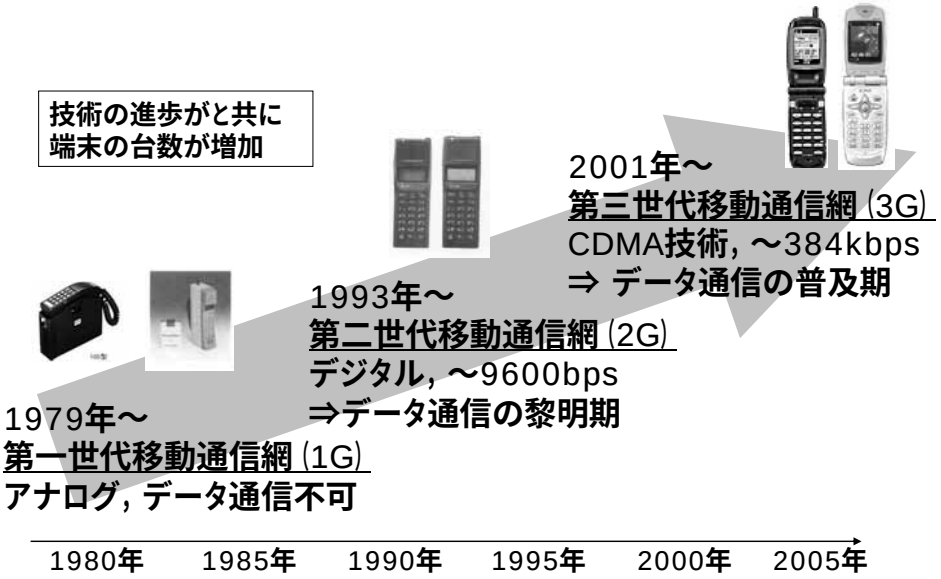


図2.1 移動通信網の歴史

上述のように通信ネットワークの利用開始当初は，その通信速度も低速であったため，利用可能なデータは，電子メールやネットワークニュース等により扱われるテキストに限定されていた．しかし近年のネットワークの高速化により，それを利用するアプリケーションやサービスについても多様化して来た．

例えば 1990 年前後に発明された WWW（World Wide Web）の爆発的普及により，HTML（Hypertext Markup Language）からハイパーリンクされた JPEG（Joint Photographic Experts Group）等の静止画像が送受信されるようになった．さらに近年では，MPEG（Moving Pictures Experts Group）の動画像や MP3（MPEG Audio Layer-3）や AAC（MPEG-2 Advanced Audio Coding）等の音楽を取り扱うアプリケーションが出現するようになった．また，このようにアプリケーションやサービスが多様化することにより，通信ネットワークの更なる高速化や新たな通信ネットワークの出現を導くボジティブフィードバックを繰り返してきた．現在では，アプリケーションやサービスの更なる多様化に伴い，単一のアプリケーションで複数のメディアタイプを同時に扱うケースも増加している．例えば，音声通話を IP ネットワーク上で実現する VoIP（Voice over IP）の利用と共に，ユーザのプレゼンス情報や電話帳等のユーザデータを合わせて送受信する例が挙げられる．また，ビデオ電話アプリケーションのように，音声通話と同時に通話者の動画像の送受信を行いながら，会議ファイルのやり取りを行う場合がある．さらにデータ配信型アプリケーションに着目すると，動画像のストリーミング画像に合わせて関連するテキストのニュース記事をテロップとして流すアプリケーションが存在する．

以上のように，近年の通信技術の発展によって，データ通信だけではなく，複数のメディアタイプを統合的に扱うマルチメディア通信を効率よく提供することが重要になってきている．それとともに，マルチメディア通信を支える技術である通信プロトコルについても様々な改良が加えられて来た．また，新たに出現した各種アプリケーションを実現するために，数々の新しい通信プロトコルも提案されてきた．

通信プロトコルは，OSI（Open System Interconnection）階層モデル[12]に代表されるように，様々な機能を持つ通信プロトコルを複数組み合わせて一連の通信機能を提供することが一般的である．図2.2は，マルチメディア通信に用いられる代表的な通信プロトコルのうち特にインターネットで用いられる通信プロトコル TCP/IP の階層構造を図示したものである．TCP/IP は，アプリケーション層，トランスポート層，ネットワーク層，ネットワークインタフェース層に分けられ，それぞれの階層で提供する通信機能を組み合わせることにより一連の通信機能を提供している．

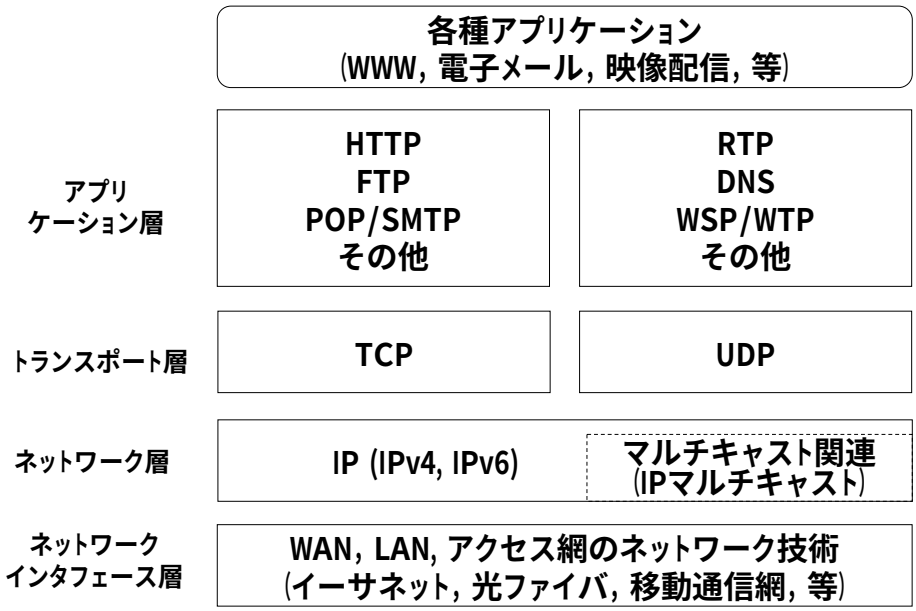


図2.2 マルチメディア通信を実現する通信プロトコル

例えば，WWW で扱われるデータは， アプリケーション層プロトコルとして HTTP（Hypertext Transfer Protocol）[13]を用い，トランスポート層の通信プロトコルである TCP とネットワーク層の通信プロトコルである IP を用いて通信が行われる．他にも TCP を用いるアプリケーション層プロトコルには，ファイル転送を実現する FTP や，電子メールの送受信を実現する POP（Post Office Protocol）や SMTP（Simple Mail Transfer Protocol）など多数の通信プロトコルが存在する．また，映像配信アプリケーションで扱われるデータは，アプリケーション層として RTP（Real-time Transport Protocol）を用い，トランスポート層の通信プロトコルである UDP（User Datagram Protocol）と IP を用いて通信が行われる．他にも UDP を用いるアプリケーション層プロトコルには，ホストの名前解決を実現する DNS（Domain Name System）など多数の通信プロトコルが存在する．なお，本研究で取り上げる WAP の通信プロトコルである WSP（Wireless Session Protocol）と WTP（Wireless Transaction Protocol）も UDP 上で動作するアプリケーション層プロトコルであり，その詳細は第 4 章にて述べる．

TCP では信頼性のあるデータ転送をエンドトゥエンドで提供するため，再送制御や順序制御，エラー検出などを行う[1]．TCP については2.2節で詳細に説明する．反面 UDP は，TCP で提供する信頼性のあるデータ転送が必要とされない場合に使用される通信プロトコルであり，TCP で提供する機能の多くは提供しない代わりにプロトコルオーバヘッドを抑えるように設計されている．なお，文献[14]における通信解析によれば，インターネット上の通信の 98%以上がトランスポート層に TCP を用いている．現在ではその比率がやや低下しているものの，TCP はインターネットにおける最も重要な通信プロトコルといっても過言ではない．そこで，本論文ではマルチメディア通信の性能を改善するため，この TCP に

着目してその通信性能の改善を図ることを目的の一つとする．その準備として，本章ではTCP の概要について2.2節において説明し，さらに2.3節において TCP の残存課題を整理することで，本論文で取り組むべき研究課題を整理する．

ネットワーク層の通信プロトコルである IP は，パケット配送の機能を提供し，主にネットワークの経路制御（ルーティング）に関する制御を行う．IP では，送信相手を識別する IP アドレスを用いている．現在インターネットで幅広く用いられている IPv4（IP version4）[15]では，近年のインターネットの爆発的な普及により，IP アドレスの枯渇が問題となっており，IETF により IP アドレスを 128 ビットに拡張した IPv6 の標準化が行われた[4]．IPv6 では，ネットワークアドレスの部の他に，様々な拡張が行われており，ルーティングテーブルの肥大化対策や，プラグアンドプレイの実現などが盛り込まれている．さらに，セキュリティ対策として IPSec（IP Security）の利用が必須となるほか，オプションを必要に応じて標準ヘッダに付加出来るなどの柔軟性があり，次世代の IP として注目を浴びている．

なお，IP アドレスには，ユニキャストアドレスとマルチキャストアドレスの 2 種類が定義されている[3][4][15]．ユニキャストは，ネットワークの通信相手を 1 台に限定して通信を行うために用いられるアドレスであり，ネットワーク内の通信相手を一意に識別するためにユニキャストアドレスを用いる．それに対してマルチキャストは，複数の通信相手を指定して同じデータを送信するために用いられるものであり，複数の通信相手をグループとして一意に識別するためにマルチキャストアドレスを用いる．マルチキャストでは，複数の宛先を指定して一回データを送信すれば，通信経路上のルータがデータを複製しながら宛先にデータを送信するため，回線を圧迫することなく効率よく配信することが出来る．TCP ではエンドトゥエンドの制御をすることからユニキャストのみに対応しており，従って，現在利用されるアプリケーションの多くがユニキャストを利用する．しかし，音声や動画像といったリアルタイム性の通信に対する需要の高まりから，ユニキャストだけではインターネットにおける通信量が爆発的に増加することが予想され，IP ネットワーク上でマルチキャスト配信を実現する IP マルチキャストが注目されている．特に，通信に無線を用いる移動通信網等では，利用可能なネットワークリソースが有線を利用した通信と比較して限られているため，マルチキャストのような通信効率の良い通信方式への要求が非常に高い．また，文献[16]から裏付けられるように，IP マルチキャストを用いた通信量は年々増加傾向にあり，その重要性が非常に高まっている．

IP マルチキャストにはこれまでに数多くの研究例があり，IETF においても様々な技術の標準仕様が策定されたが，様々な要因からその普及には至っていないのが現状である[17][18]．そこで，本論文のもう一つの目標として IP マルチキャストの課題を解決することを挙げ，IP マルチキャストの普及の阻害要因を取り除くことにより，結果的に IP マルチキャストの普及を促進し，マルチメディア通信全体の利用効率の向上を目指す．その準備として本章では，2.4節において IP マルチキャストの概要を紹介した後，2.5節において IP マルチキャストにおける課題を整理し，本論文で対象とする研究内容について述べる．

2.2. TCP 概要

TCP では信頼性のあるデータ転送をエンドトゥエンドで提供するため，以下に示す機能を提供する[1]．

- 再送制御
  ネットワークの輻輳やエラーにより欠落したパケットを再送する．
- フロー制御
  ネットワークや受信側の受信能力に合わせて送信側がデータの流量を制御する．
- 輻輳制御

ネットワークの輻輳を避けるため送信側が送信データ量を調整する．

- 順序制御
  到着順序が送出順序と異なるパケットを正しく並び替える．
- エラー検出
  通信中に発生したパケットのビットエラーを検出する．

以上の TCP の機能の中でも特に重要な機能の一つが再送制御である．再送制御により欠落したパケットを確実に相手に届けることが出来るため，FTP や HTTP 等のデータを確実に相手に届ける必要があるアプリケーションの実現が容易に可能となる．

さて，データを確実に相手に届ける方法として，再転送付き肯定確認応答方式がある（図2.3左参照）．この方式では，送信側はパケットを送信すると，これに対する確認応答（ACK：Acknowledgement）を受け取るまで次のデータを送信しない．受信側はパケットを受信するたびに ACK を送り返す．この ACK は次に受信側が求めるパケット番号を示している．また，パケットが失われた場合に備えて，送信側はパケットを送る際にタイマをスタートさせ，確認応答が到着する前にタイマが切れた場合（タイムアウト）にはパケットを再送する（図2.3右参照）．なお，TCP では ACK として特別なパケットを用意するのではなく，図2.4に示すように，返信するデータのヘッダの中に確認応答番号フールドを設け，データとともに ACK を送信する方式を採用している．これをピギーバック（Piggyback）という．このピギーバックを用いることにより，ネットワークに流入する通信量を減少させる効果がある[1].

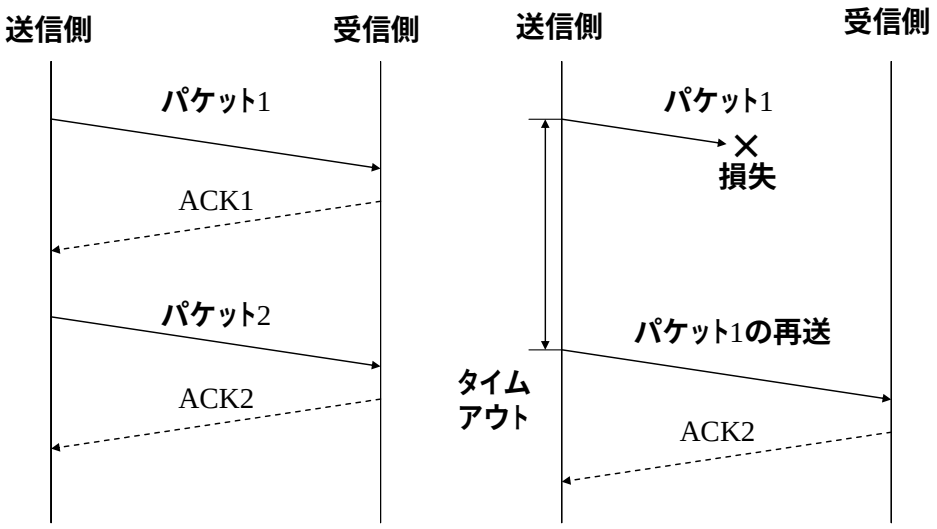


図2.3 肯定確認応答とタイムアウトによる再送

発信元ポート (16)			**着信元ポート** (16)
シーケンス番号 (32)			
確認応答番号 (32)			
データオフセット (4)	**予約** (6)	**コード** (6)	**ウィンドウ** (16)
チェックサム (16)			**緊急ポインタ** (16)

図2.4 TCP ヘッダの構成

ところで，再転送付き確認応答方式では，個々のパケットに対する確認応答を受け取るまで次のパケットを送ることができず，その間ネットワークは利用することができない．そこで TCP では，フロー制御にスライディングウインドウを用いた再転送付き確認応答方式を採用することでこの問題を解消している．この方式では，ACK を待たずに送信出来る最大のサイズであるウインドウサイズを設定し，このウインドウを ACK の到着状況に応じてスライドさせることで ACK を待たずに複数のパケットを送信出来るようにしている[19]．図2.5左はウインドウサイズが 4 の場合のスライディングウインドウの動作の様子を表している．まず 1〜4 までの 4 つのパケットを ACK なしで送信し，1 に対する ACK を受け取ると，ウインドウサイズをスライドさせ，5 まで送れるようになる（図2.5右）．以下同様に送受信が繰り返される．ここで，図2.5左において 2 に対する ACK が途中で失われても 2 のパケットが再送されていないことに注意されたい．スライディングウインドウ制御では，ACK はその前の番号までのパケットを受け取ったことを意味している．なお，実際の TCP ではパケットサイズは可変長であるため，ウインドウサイズはパケット数単位でなくバイト単位で表される．

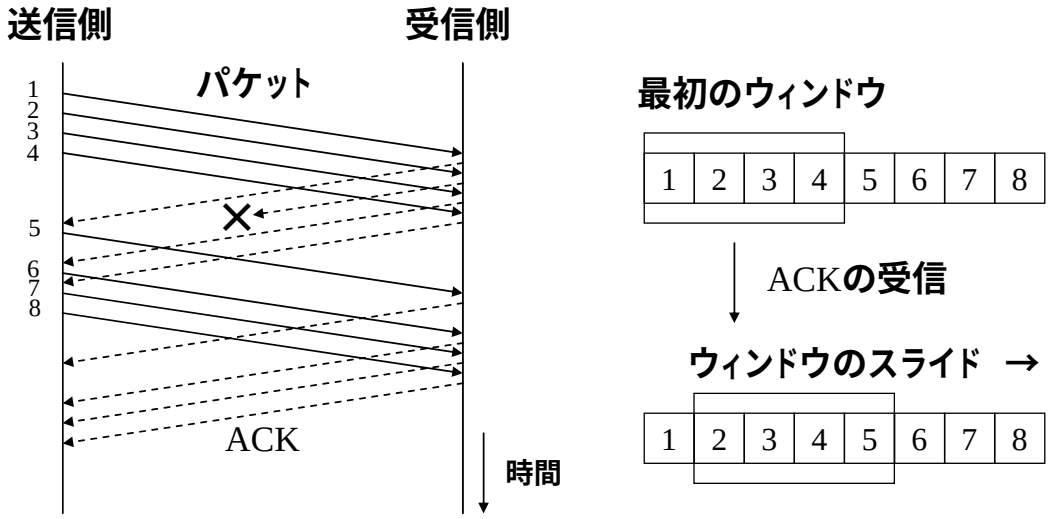


図2.5 スライディングウインドウ制御（ウインドウサイズ 4 の場合）

このようにスライディングウインドウ制御により，再転送付き肯定確認応答方式よりもネットワークの利用効率が高まったが，ウインドウサイズを大きくしすぎると，ネットワークが扱える容量を越えたパケットが送信され，輻輳が生じる場合がある．輻輳とはネッ

トワークの内のルータが処理能力を越えた量のデータを受け取り，処理が追いつかない状態や，特定のネットワークインタフェースにトラヒックが集中した状態のことを示す[20]. 輻輳になるとデータの再送が頻発し，データの転送効率が落ち，さらに，遅延が増大する. 上述したスライディングウインドウ方式で用いるウインドウサイズは固定であったが，コネクションの増減によるトラヒック量の増減により，そのウインドウサイズが定常的に最適とはならなくなる. そこで TCP では, ネットワークの状況をより正確に反映させるため, ウインドウサイズをネットワークの状況に応じて動的に変化させる方式を取りいれている.

ウイドウサイズは, 図2.4に示す TCP ヘッダのウインドウサイズフィールドを用いて受信側から送信側へ通知している. これにより，受信側の処理能力が十分でなくなった時には，ウインドウサイズを小さくすることでネットワークに流入出来るデータ量を制限し，受信側に十分な処理能力がある時には逆に大きくすることでフローを調節する. 特に，受信側はウインドウサイズ 0 を通知することで送信側からの送出を完全に止めることが出来る. 従って，このウインドウサイズは，TCP ヘッダにより受信側から送信側へと通知され，パケット受信側の受信能力を示しているので，広告ウインドウ（Receiver Advertised Window：rwnd）と呼ばれる[19][20].

図2.6では広告ウインドウの通知の様子を表している. ウインドウサイズ 4 で送信を開始し，受信側はウインドウサイズ 3 を報告しているので，それを受け取った送信側はウインドウサイズを 3 に変更して送信を行っている. また，この図では，ウインドウサイズ 0 を報告することで送信側のパケットの送出が停止している様子も示している.

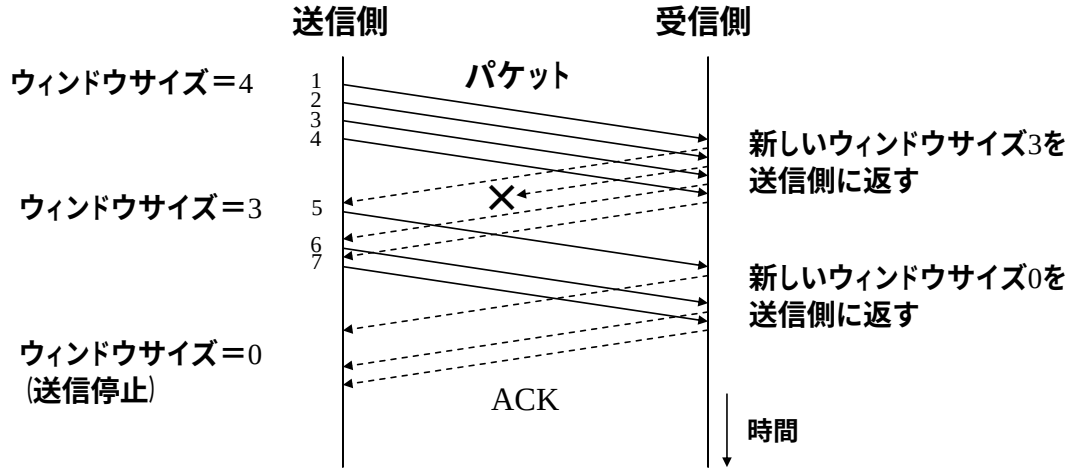


図2.6 受信側広告ウインドウの報告

TCP の広告ウインドウは，フロー制御としての機能は提供することが出来るが，ネットワークの内部の輻輳に関しては十分な対応ができない. これは，受信側の受信能力とネットワーク内の混雑状態は独立しているためである. このため，TCP では輻輳制御のための別のウインドウがあり，これを輻輳ウインドウと呼ぶ. 輻輳ウインドウ（Congestion Window：cwnd）は，以下で説明するラウンドトリップ時間に密接に関係している.

TCP では，ネットワーク混雑状態を調べる機能がないため，パケットを送信してからそれに対する ACK が返って来るまでのラウンドトリップ時間（Round-Trip Time：RTT） を測定し，次の式でタイムアウトの値を決定している. このタイムアウトは今までの RTT（Old_RTT）の平均に，現在測定した RTT（Now_RTT） をある割合で加えることにより得ている[1][19].

$$DIFF = Now\_RTT - Old\_RTT$$
$$Smoothed\_RTT = Old\_RTT + \delta \cdot DIFF$$
$$DEV = OLD\_DEV + \rho\ (|DIFF| - OLD\_DEV)$$
$$Timeout = Smoothed\_RTT + \eta \cdot DEV$$

DIFF ：	RTT の平均と新しい RTT との差.
Smoothed _ RTT ：	RTT の平均と *DIFF* に係数δをつけた値との総和.
DEV ：	RTT の分散の近似．なお *OLD _ DEV* は今までの *DEV* の値を示す.
Timeout ：	パケットを送信してからタイムアウトを発生するまでの時間.
係数：	それぞれ $\delta = 1/2^3$ ， $\rho = 1/2^2$ ， $\eta = 4$ に設定されている.

さて，TCP はエンドトゥエンドでの制御のみを行うので，送信者と受信者は輻輳がどこで起こったのか，またなぜ輻輳が起こったかの詳細について知ることはできない．送信者と受信者が輻輳について知ることが出来るのは, RTT の計測による遅延の増加だけである．そこで TCP では，タイムアウトの発生を輻輳によるものと仮定し，輻輳ウインドウを次に説明する方式を用いて変化させる．この変化をモデル的に表したものを図2.7に示す．これは輻輳ウインドウの典型的な変化の様子を表している.

1. 送信開始直後はスロースタートモードとなり，最初に輻輳ウインドウは送信側最大パケットサイズ（Sender Maximum Segment Size：SMSS）の 2 倍またはそれ未満の初期ウインドウサイズにセットされ，ACK 受信により送信終了を確認したパケットサイズ分ずつ輻輳ウインドウを増加する．これにより輻輳ウインドウは指数的に増加する（図2.7の（a)).

2. 一定時間内に ACK が戻らないと送信タイムアウトとなり, 輻輳ウインドウを SMSS に戻す．そして, スロースタートスレッショルド（Slow Start Threshold：ssthresh）を式(2.1)に従ってセットする．この式における FlightSize とは送信されたが ACK がまだ帰って来ていないデータの総計を表す．実装によっては FlightSize の代わりに単に輻輳ウインドウを使っているものもあるが，これは好ましくない[19]．タイムアウトによるパケットの再送が発生した時には輻輳ウインドウを減少させるとともに，タイムアウトを今までの 2 倍に変更する．これは，パケットの再送がさらに発生することによる輻輳の増加を避けるためである（図2.7の（b)).

$$ssthresh = \max(FlightSize/2, 2 \cdot SMSS) \qquad (2.1)$$

3. スロースタート動作を再開する（図2.7の（c)).

4. 輻輳ウインドウが ssthresh を越えると輻輳回避に入り, ACK 受信によりウインドウサイズを式(2.2)の計算に従って増加させることにより, 指数的な増加を抑える（図2.7の（d)).

$$cwnd += SMSS \cdot SMSS / cwnd \qquad (2.2)$$

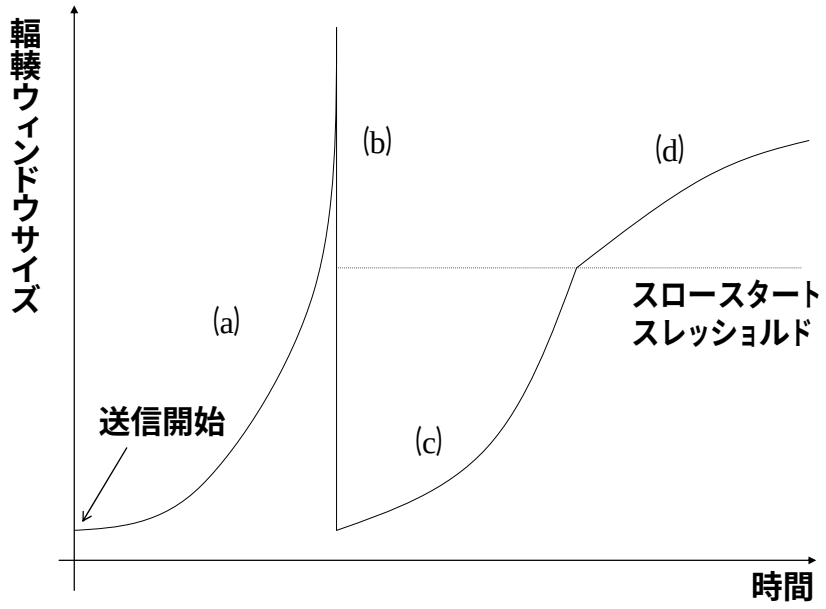


図2.7 スロースタートと輻輳回避

以上のように，TCP のウインドウサイズには，TCP ヘッダにより受信側から送信側へと通知され，パケット受信側の受信能力を示す広告ウインドウ（rwnd）と，送信側がネットワークに徐々にパケットを送出する機能を持つ輻輳ウインドウ（cwnd）の 2 種類が存在する．送信側は広告ウインドウと輻輳ウインドウのうち小さい値を実際のウインドウサイズとして用いるので，送信側において輻輳ウインドウを減らせばネットワークに投入されるトラヒックは減少し，輻輳を回避することが出来る．これら 2 つのウインドウの制御により，ネットワークが非輻輳時にはウインドウサイズを大きく取り，逆に輻輳時にはウインドウサイズを下げる動的な制御を行う[21] - [23].

2.3. TCP を取り巻く歴史的背景とその課題

TCP は，1970 年代に最初に利用され，1981 年に IETF によって RFC として仕様化されてから徐々に利用が広がった．1990 年頃に WWW が発明されるとその後 1995 年頃から徐々にインターネットの利用が爆発的に普及して一般家庭でも利用されるようになった．この 1995 年頃からはトラヒックの爆発的の増加によりネットワークの輻輳に対する問題が顕著になりその必要な対策が求められた．また 1999 年に日本で開始された i モードサービスにより携帯電話からインターネット上のコンテンツにアクセスし利用することが可能となり，それがまた移動通信の普及につながるポジティブフィードバックに結びついた（図 2.8）.

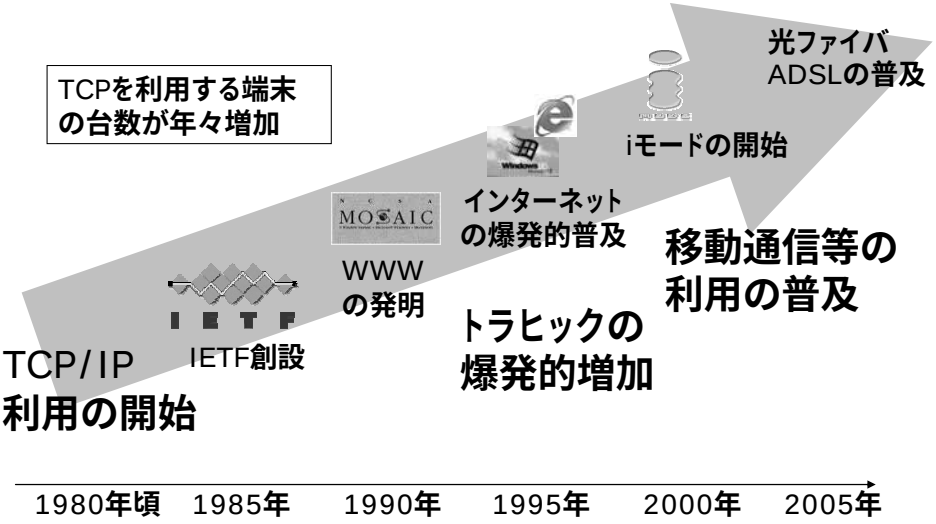


図2.8 TCP の普及とその歴史的背景

以上に説明した背景から 1990 年代以降，TCP に関する研究が活発に行われた．TCP に関する研究はこれまでに多岐に渡っており，非常に多くの関連研究が存在する[24]－[29]．その中でも TCP における課題について述べた論文[25][26]によると TCP の課題として大きく分けて以下の 2 点が存在すると述べている．

1. TCP の輻輳制御の性能改善

前述のように輻輳になるとデータの再送が頻発するため，データの転送効率が落ち，さらに遅延が増大する．このことから，輻輳制御の性能はネットワークの効率を左右する重要な要素の一つであり，オーバヘッドが小さく公平性を満たす輻輳制御方式は必要不可欠である．そこで従来の TCP のスロースタートを用いたエンドトゥエンドの輻輳制御の機能を改善し，効率的な輻輳制御を行うことは非常に重要である[21]－[23]．特にトラヒックが爆発的に増加した 1990 年代には TCP の性能改善の必要性が特に高まった．

その後，通信速度の高速化とネットワークの普及に伴い，マルチメディア通信への需要が高まり，様々な要求通信品質を持ったトラヒックが利用されるようになった．しかし，公平性を満たす TCP の輻輳制御では，高速性が要求されるトラヒックも低速でよいトラヒックも一様に扱われることとなる．このため，各サービスが要求する通信品質に応じた優先制御を提供し，効率的なネットワーク利用を実現することが重要な課題となった．そこで第 3 章では，IPv6 を対象に，TCP の輻輳制御を効果的に行うために設置される RED（Random Early Detection）ゲートウェイ[24]を用いた明示的輻輳通知方式を改良し，各コネクションに与えられた優先度に基づく優先制御機能を実現する．また，本方式の性能評価により，従来方式と同等な平均スループットを保ちながら提案方式による優先制御が可能であることを示す．

2. 無線通信における TCP の性能改善

公衆無線 LAN や移動通信網等の無線を利用したネットワークにおいては，有線を利用したネットワークと比較して，高エラー率，高遅延といった特性に対処する必要がある[27]．また利用可能な無線リソースは限られているため，その利用コストは有線を利用したネットワークと比較して相対的に高くなるという傾向にある．無線通信のように高エラーなネットワーク特性の元では，TCP のパケット欠落による再送が頻繁に発生するため，このような環境の下でも性能の著しい低下を防止する対処が必要である．高遅延のネットワーク特性の元では，TCP のラウンドトリップ時間（RTT）の変動が大きく，TCP の再送制御に

重要なタイマのチューニングが必要な場合がある．以上のことから無線の特性に合わせたTCP の改善はとても重要な課題である[27] - [29].

無線通信の中でも特に移動通信網は，無線 LAN と比較しても高遅延であり，さらにデータの伝送速度が低速で，エラー発生率が高いという特徴がある[27]．このため，データ通信に TCP をそのまま適用することは問題があり，第一世代移動通信網，および第二世代移動通信網向けに，携帯電話等から Web ページなどを参照するための通信プロトコル WAP（Wireless Application Protocol）が 1998 年に WAP フォーラムで提案された. その後, 2000 年頃にそれまでの世代と比べて通信速度が格段に向上した第三世代移動通信網が提供される際，同通信網において，WAP とインターネットにおいてこれと同等の機能を提供する HTTP/TCP のいずれが好ましいのかが不明確であり，これを検討することが重要な課題となった．そこで第 4 章では，第三世代移動通信網として W-CDMA を用いた場合の両プロトコルにおける通信実験を通じ，それぞれの方式の性能を比較する．その結果，第三世代移動通信網以降の高速なネットワークの場合は，WAP よりも HTTP/TCP を利用することが好ましいことを示す．さらに，ここで得られた結果に基づき，第三世代移動通信網向けに適する通信プロトコルとネットワークアーキテクチャを提案する．

2.4. IP マルチキャスト概要

ネットワーク内で単一のアドレスを指定して特定の相手にデータを送信するユニキャストと比べて，マルチキャストは，ネットワーク利用効率の良いデータ伝送技術である[2][3]. 例えば，図2.9に示すように送信者が同一のデータを複数の受信者に配信する場合，ユニキャストではデータの受信者数に比例してネットワークを流れるデータ量が増加するのに対し，マルチキャストでは，ルータにおいてデータを複製しながら受信者へと配信するため，送信者付近のネットワークにおけるデータの多重効果が高く，受信者数とネットワークを流れるデータ量が比例しないという特徴がある．近年では，インターネットを用いて TV 向け動画像データを配信する IPTV サービスなどが提供されているが, マルチキャストはこのような大多数の受信者に対して大量のデータを同報配信するサービスに対して有効であり，マルチキャストをこれらのサービスへ効率よく適用することが重要な検討課題になっている．また，無線 LAN や移動通信網などの無線を利用した通信では有線と比べて通信コストが高いことから，単一の無線チャネルを複数の受信者で共有し，使用する無線リソースの大幅な低減が可能となるマルチキャストの適用は，非常に重要なテーマの一つといえる．

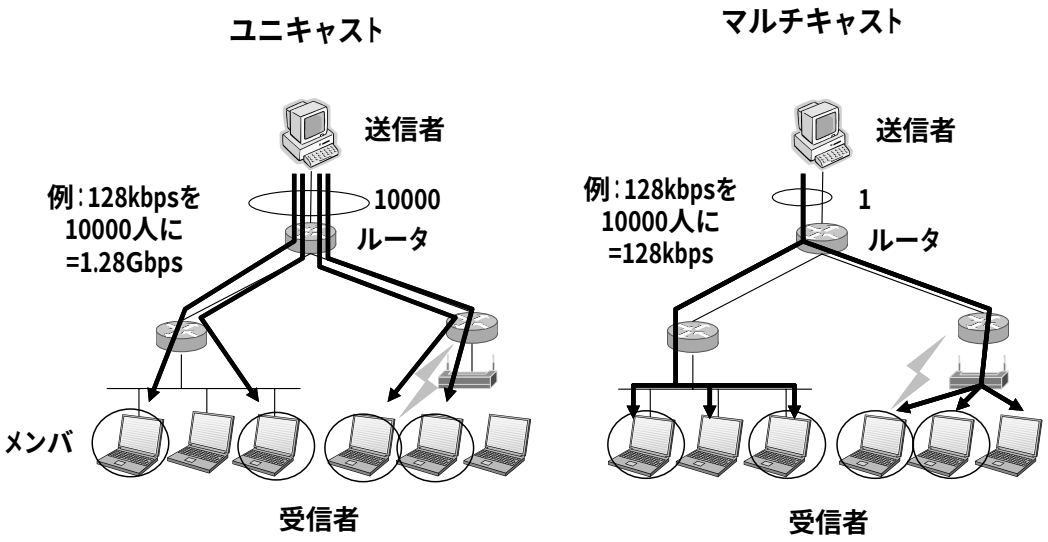


図2.9 ユニキャストとマルチキャストの比較

IP ネットワーク上でマルチキャストを実現する IP マルチキャストは, 古くから研究が行われており，受信者のグループ管理，IP マルチキャストの経路制御，アプリケーションプロトコルなどの技術分野が存在する（図2.10）[30][31]．IP マルチキャストを用いたアプリケーションの例として，IPTV などのストリーム型データ配信アプリケーションと，電子新聞や Java プログラムなどを配信するファイル型データ配信アプリケーションがある. また, 小規模なグループ型通信の例としてマルチメディア会議システムなどが挙げられる.

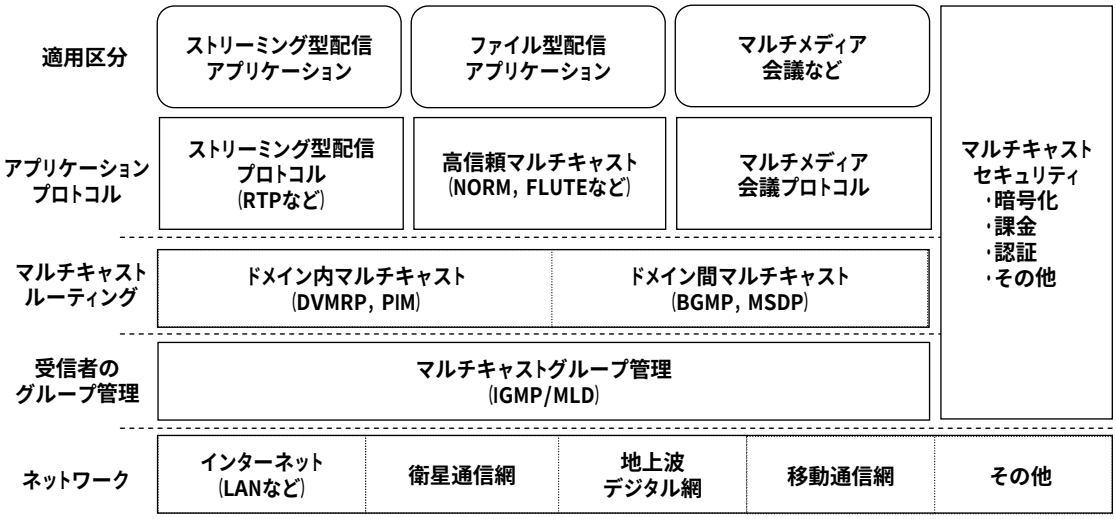


図2.10 マルチキャストの技術分野

ストリーミング型配信アプリケーションを実現するアプリケーションプロトコルの代表的なものとしては RTP が存在する[32]．RTP はユニキャストおよびマルチキャストにおけるストリーミング配信に用いられる通信プロトコルであり，ストリーミング型配信アプリケーションの普及と共に近年になってその利用が増加している.

ファイル型データ配信アプリケーションを実現するアプリケーションプロトコルには様々な技術が存在する[33]．マルチキャストの場合，全ての受信者に正しくデータを受信さ

せるには様々な障害があり，近年になって NORM（Negative-acknowledgment Oriented Reliable Multicast）[34]や FLUTE（File Delivery over Unidirectional Transport）[35]等の様々な高信頼マルチキャストプロトコルが IETF において標準化されるなど[36]－[42]，非常に活発な研究が行われている．なお，これら高信頼マルチキャストプロトコルに関する標準化は 2005 年になって多くの標準仕様の策定が完了し，一定の研究成果を得ている．

IP マルチキャストを利用する各種アプリケーションを実現するために基本となる通信プロトコルとしては，マルチキャストルーティングとマルチキャストグループ管理が存在する（図2.11）．マルチキャストルーティングプロトコルは，ルータとルータ間で動作する通信プロトコルであり，マルチキャストデータの配信経路を設定されるために用いられるものである．マルチキャストルーティングプロトコルには，ドメイン内で用いられるドメイン内マルチキャストルーティングプロトコルである PIM（Protocol Independent Multicast）[43]や DVMRP（Distance Vector Multicast Routing Protocol）[44]等が存在する．またドメイン間で用いられるドメイン間マルチキャストルーティングプロトコルの BGMP（Border Gateway Multicast Protocol）[45]や MSDP（Multicast Source Discovery Protocol）[46]等が存在する．これらのマルチキャストルーティングプロトコルにより，配信データを適切に受信者に届けるための制御を行うことが可能となる．

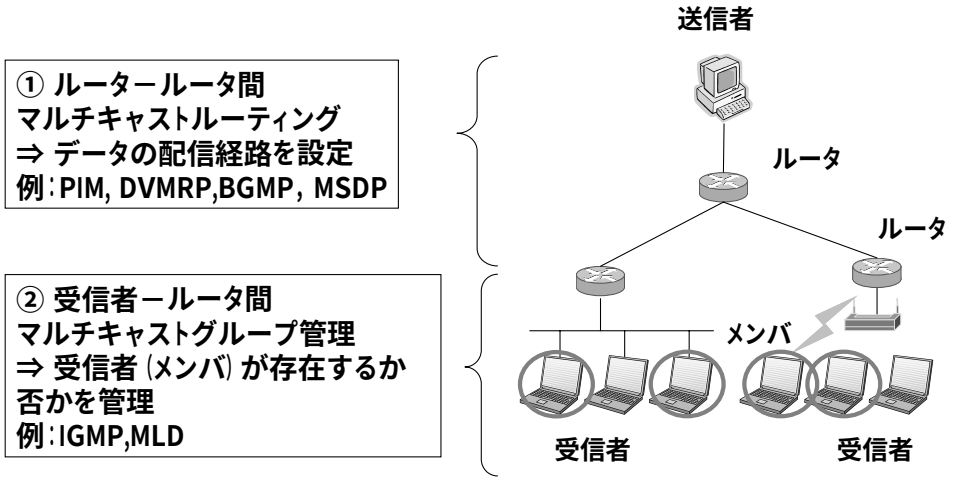


図2.11 IP マルチキャストの基本となる通信プロトコル

IP マルチキャストでは，受信者が任意の時点でデータ受信を開始または停止できるため，データを届けるべき受信者の管理が重要であり，これを提供する通信プロトコルが IGMP [10][11]である．IGMP は，受信者が接続するサブネットワーク上に存在するルータ（本論文ではこのルータを特にアクセスルータと呼ぶ）間で使用されるプロトコルであり，マルチキャストアドレスで配信されるデータの受信者がサブネットワーク内に存在するか否かの管理をする．このような管理のことをマルチキャストグループ管理と呼ぶ．なお，IGMP は IPv4 で用いられるマルチキャストグループ管理プロトコルであり，IPv6 では MLD（Multicast Listener Discovery）[47][48]が用いられる．IGMP と MLD は，対象とする IP のバージョンが異なる以外の基本動作は同じであるため，本論文では IGMP と MLD の区別なく単に IGMP として説明する．2.4.1節では IGMP の概要を説明する．

2.4.1. IGMP 概要

IGMP は，アクセスルータ配下に，マルチキャストの配信データの受信者（メンバ）が存在するか否かを判断するために用いられる通信プロトコルである．この目的のため，IGMP では以下の 3 つのメッセージが定義されている．

① IGMP Membership Report（加入要求）
受信者がルータに受信を希望するマルチキャストアドレスを通知する．

② IGMP Leave Group（離脱要求）
受信者がマルチキャストの受信を停止するためマルチキャストアドレスのグループへの参加の取りやめをルータに通知する．

③ IGMP Query（問い合わせ）
ルータが受信者に受信を希望するマルチキャストアドレスを問い合わせる．

以下では IGMP の動作について具体例を挙げながら説明する．なお，以下では最初に IGMPv2（IGMP version2）[10]の動作について説明を行い, 次に IGMPv3（IGMP version3）[11]の説明を行う．

図2.12に示すように, 受信者があるマルチキャストアドレスで配信されるデータの受信を希望する場合は，接続しているネットワークに IGMP 加入要求を送信する．この IGMP 加入要求には受信を所望するマルチキャストアドレスが含まれており，これにより，ルータは当該マルチキャストアドレスの配信データの受信を所望する受信者が存在することを知る．そして，このルータはマルチキャストルーティングプロトコル（PIM，DVMRP，他）を用いてマルチキャスト配信経路であるマルチキャストツリーを作成する．これより，このルータにマルチキャスト配信データが届くため，その中継を行うことによって自身のサブネットワークに接続する受信者は配信データの受信をすることが出来る（図2.13）．ここで，マルチキャストによって配信されるデータを受信する受信者のことを特にメンバと呼ぶ．また，特定のマルチキャストアドレスによる配信データを受信するメンバの集合をマルチキャストグループと呼ぶ.

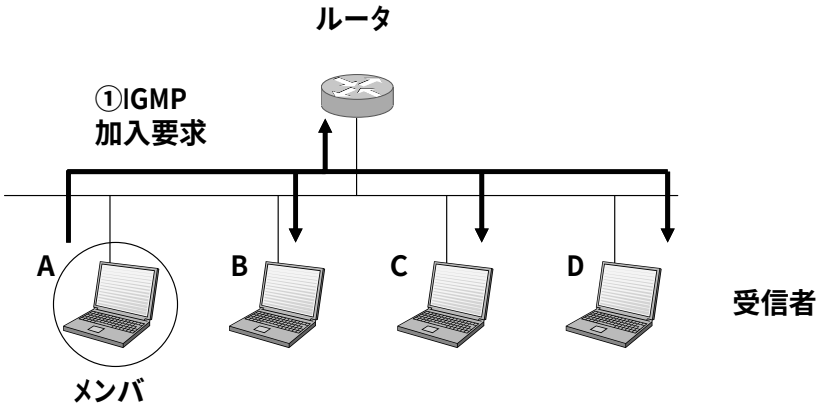


図2.12 IGMP 加入要求

なお, 図2.13に示すように, マルチキャスト配信データはサブネットワーク上の全てのネットワーク上に伝わるため，当該データを受信する必要のない他の受信者に対してもデータが届く．ただし，通常，配信を希望しないマルチキャストアドレス宛のデータはネット

ワークインタフェースにおいてフィルタリングすることによって廃棄されるため，これらのデータが受信者中のアプリケーションに渡されることはない.

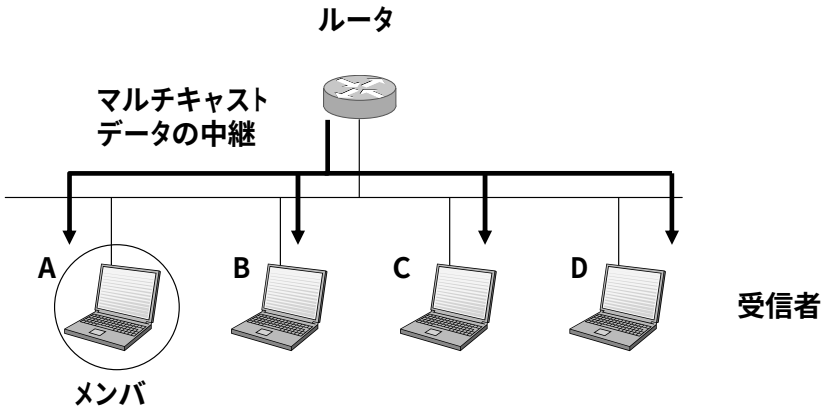


図2.13 マルチキャスト配信データの中継

図2.14に示すように, あるマルチキャストアドレスで配信されるデータの受信の終了を希望する場合，メンバは接続しているネットワークに IGMP の離脱要求を送信する．これにより，ルータは配信データの受信停止を所望するメンバが存在することを知るが，この時点では当該マルチキャストアドレス宛の配信データの中継を終了することが出来ない．その理由は，ルータがサブネットワーク中に他のメンバ（図2.14の例では，受信者 C）が存在するか否かという情報を管理していないためである.

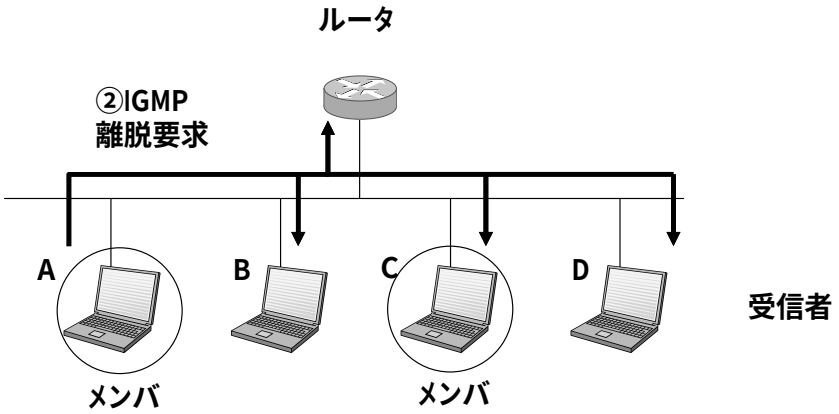


図2.14 IGMP 離脱要求

このため，図2.15に示すように，ルータは IGMP 離脱要求を受信する度に IGMP 問い合わせを送信し，他のメンバが存在するか否かの確認を行う．そのようなメンバ（図の例では，受信者 C）が存在する場合，同メンバは図2.16に示す IGMP 加入要求を送信し，当該マルチキャストアドレス宛に配信されるデータの受信を希望する旨をルータに伝える．なお，この IGMP 加入要求は，図2.12で受信者 A が送信したものと同じメッセージである．さて，IGMP 加入要求を受信したルータは，受信を所望するメンバが他に存在することが確認出来るので，配信データの中継を継続する．しかし，IGMP 問い合わせを送信後，タイマ満了時刻までに IGMP 加入要求を受信しなかった場合には当該マルチキャストアドレ

ス宛データの中継を停止し，マルチキャストルーティングプロトコルを用いてマルチキャストツリーから当該ルータを配信先から除外することを要求する（図2.17）.

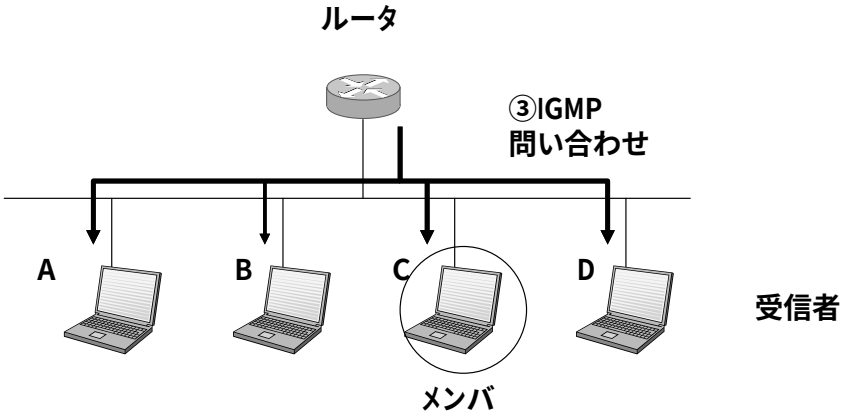


図2.15 IGMP 問い合わせ

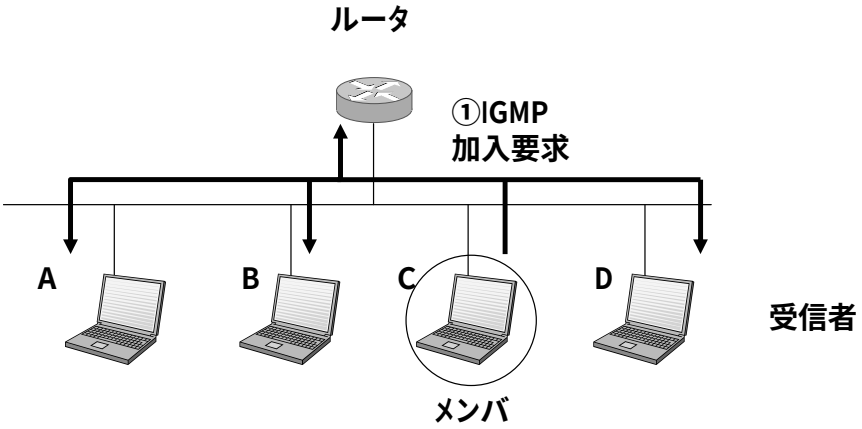


図2.16 IGMP 問い合わせの後の IGMP 加入要求

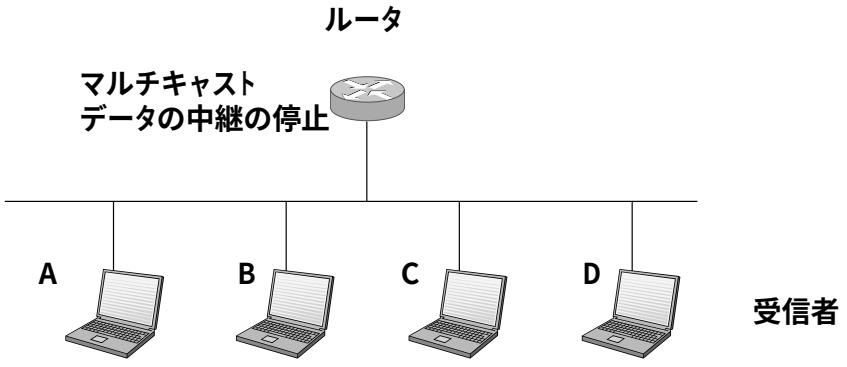


図2.17 マルチキャストデータ中継の停止

IGMP 問い合わせには，図2.15で説明したようにメンバからの IGMP 離脱要求を契機として問い合わせを行う IGMP Group-Specific Query （グループ特定問い合わせ）の他に，サブネットワークに存在するメンバを定期的に監視する IGMP General-Query（一般問い合わせ）の二種類が存在する．IGMP 一般問い合わせでは，受信者の突然の電源断により IGMP 離脱要求を出さずにメンバで無くなってしまうような場合に対処することが可能である．これにより，移動通信網において IGMP 離脱要求を送信せずにサブネットワークの変更を伴うハンドオフを行った場合への対処にもなる．なお，IGMP 一般問い合わせは，マルチキャストグループを限定せずにメンバの問い合わせを行うメッセージであるため，一般問い合わせを受信したメンバは,加入しているマルチキャストグループを問わず IGMP 加入要求を送信することが要求される．

なお，ルータはマルチキャストグループ毎にメンバが存在するか否かのみを管理すれば十分であるため，同じマルチキャストアドレスに対して複数のメンバから IGMP 加入要求を受信しても無意味である．そこで，IGMP では，IGMP 加入要求と IGMP 離脱要求の宛先として加入もしくは離脱を要求するマルチキャストアドレスを指定し，これらのメッセージを当該マルチキャストグループの他のメンバにも届けている．そして，他のメンバからの IGMP 加入要求を検知したメンバは自身の IGMP 加入要求の送信を停止することで，サブネットワーク中の 1 台のメンバのみが IGMP 加入要求を送信することになる．この機能を Suppress（抑制）機能といい，これによりサブネットワークを流れる制御パケット数を削減することが可能となる[10]．ただし，マルチキャストによる通信は UDP を用いること，そして，IGMP では各メッセージに対する確認応答メッセージが存在しないことから，受信者は自身が送信したメッセージが実際にルータに到着したか否かを確認する手段を持たない．このため，IGMP では各メッセージを複数回送信することとしており，この機能を連送と呼ぶ．連送回数のデフォルト値は 2 回であるが，ネットワークの状況によってこの値を変更することが可能となっている．

さて，IP マルチキャストでは，送信者を限定しない ASM（Any Source Multicast）と送信者を限定する SSM（Source Specific Multicast）の二種類が存在する．IGMPv2 は，ASM を実現するために設計されたマルチキャストグループ管理プロトコルであり，任意の送信者が当該マルチキャストアドレスに対してデータを送信することが可能であった．しかし，ASM では，悪意のあるユーザが当該マルチキャストアドレス向けに無意味なデータを流すことによって受信者を混乱に陥れる攻撃が容易に可能であり，このことがマルチキャストの普及を阻害する要因の一つとなっていた．そこで，IGMPv3 では SSM を導入し，受信者が受信を希望するマルチキャストアドレスのほかに，当該マルチキャスト配信データを送信する送信者のユニキャストアドレスを IGMP メッセージに含むことで明示的に送信者を指定する機能が提供されている．SSM により，ルータにおけるソースアドレスフィルタリング[49]が可能になるなど，ASM で問題になっていた各種の問題を解決することが可能となった．

さらに IGMPv3 では，アクセスルータがサブネットワーク中の全てのメンバを管理する方式が採用された．つまり，アクセスルータは，全てのメンバのユニキャストアドレスと，加入するマルチキャストアドレスの関連テーブルを持っており，どのマルチキャストアドレスに何人のメンバが存在するのかが把握可能になった．これに伴い，IGMPv3 ではグループ特定問い合わせと，その後の IGMP 加入要求に必要な制御パケットが不要となった．これは，ルータが全てのメンバのグループ加入状況を管理しているために，あるメンバから IGMP 離脱要求を受信したとしても残存メンバが存在するか否かをアクセスルータがあらかじめ知ることが出来るからである．なお，このグループ問い合わせを省略する機能を Fast Leave 機能と呼ぶ.

2.5. IP マルチキャストに関する課題

IP マルチキャストは，そのネットワーク利用効率がユニキャストと比較して著しく優れるために，一対多の放送型のデータ配信アプリケーションや，複数メンバ間のビデオ会議アプリケーションの実現方式として期待されている．このため，近年になって，ADSL 上の動画像配信アプリケーションなど，IP マルチキャストを用いた商用サービスが開始されている. また, 移動通信網向けの国際標準化団体である 3GPP（3rd Generation Partnership Project）では, 各種データ配信の実現を目指した MBMS（Multimedia Broadcast Multicast Service）に関する国際標準化を進めている[50].

しかし，マルチキャストには，論文[51]に紹介されているように多数の残存課題が存在するため，未だ爆発的な普及には至っていない．同論文では，残存課題を，技術上の課題とビジネス上の課題，さらには利用環境整備の課題と区別し，それぞれの課題を整理している．さらに，IP マルチキャストの最大の課題は，ビジネスモデルの構築方法であると述べており，例えば，広告モデルやユーザ課金モデル等を用いることにより，IP マルチキャストを用いたビジネスを確立させることが普及の鍵であると説明している．しかしビジネス上の課題は時代背景によって状況が異なるものであり，近年のネットワークの高速化とインフラの整備によりビジネス上の課題は徐々に改善されるものと考えられる. 例えば, 2005 年に総務省の諮問機関である情報通信審議会が，IP インフラを使った地上デジタル放送の再送信を条件付きながら認めたため，IPTV 等の IP マルチキャストを用いた放送を，地上デジタル放送の再送信にも活用することが可能になるなどビジネス上の問題は改善されることが予想出来る．一方，論文[51]では，IP マルチキャストの技術課題として主に以下を挙げている．

- マルチキャストグループ管理
  マルチキャストグループの生成に関連する一連のグループ管理に関する機能であり，具体的には，アドレス発見，受信者権限認証（Receiver Authorization），配信権限認証（Transmission Authorization）や関連する課金ポリシに関連する課題である．特にマルチキャストグループ管理を実現する IGMP にはいくつかの課題が存在する．

- マルチキャストセキュリティ
  受信者認証，送信者認証，権限認証，データ秘匿，データ完全性検証等のユニキャストでも必要なセキュリティ機能をマルチキャストにおいても提供することが特に課金を伴うサービス提供のためにも重要である．

- マルチキャストアドレス割り当て
  IP マルチキャストの利用開始当初は, 各送信者が利用するマルチキャストアドレスを割り当てるための機関が存在せず，また使用するマルチキャストアドレスの重複を解消する技術的な方法が存在していなかったため，使用するマルチキャストアドレスが重複するという課題が存在していた．特に ASM では，任意の送信者がマルチキャスト配信データの送信者になることが可能であり，マルチキャストアドレスが重複することにより複数の異なる配信データを受信してしまうという課題が存在した．ただし，本問題は，SSM を採用した IGMPv3 により解決可能となった．SSM によりマルチキャストアドレスは送信者が自由に使用するマルチキャストアドレスを選択可能となったため，論文[51]で指摘されたマルチキャストアドレスの重複による問題は現在ではすでに解決されたといえる．

- マルチキャストサービスの課金方法

IP マルチキャストは，マルチキャストグループの加入はオープンであり，受信者のマルチキャストグループへの加入は送信者には伝えられないモデル（以下ではこのモデルことを匿名モデルと呼ぶ）を採用している[52]．この匿名モデルは，送信者が受信者の状態を管理する必要が無く，受信者がある程度の匿名性が担保されることになり，結果としてマルチキャストグループへの加入手続きを軽減化することが可能であるという特徴につながる．しかし，この IP マルチキャストの匿名モデルは，ユーザアカウンティングを実現することが出来ないため，ユーザに対して課金を行うサービスの実現が不可能であるなどの問題がある．マルチキャストサービスの課金方法の実現に関しては，先述したマルチキャストセキュリティとも関連したトータルな実現方式を検討する必要がある．

論文[51]で説明された以上の課題の他にも，論文[53]では，近年の移動通信網や無線 LAN 等の無線を利用したネットワーク上での課題として以下を挙げている．

- モバイルマルチキャスト
  無線 LAN や移動通信網など，メンバがサブネットワークを変更しながら移動する場合に，マルチキャストの配信経路やマルチキャストグループの再構築などモバイル環境ならではの課題が生じる．例えば，IGMP の場合，あるメンバが IGMP 離脱要求を送信せずにサブネットワークを変更する移動（ハンドオフ）を行った場合に影響が出る場合がある．例えば，IGMPv3 では，各メンバの状態管理テーブルを保持しているため，メンバの移動によりその保持している情報に誤りが生じる可能性がある．また，メンバがサブネットワークを変更した場合に，変更先サブネットワークにおいても継続してデータ受信を可能とするようにする必要がある．

以上のことから，本論文では，IP マルチキャストの最初の課題として，最も大きな問題であるマルチキャストセキュリティとマルチキャストサービスの課金方法に注目することにする．第 5 章では，マルチキャスト配信経路が不正構築されるマルチキャスト DoS 攻撃が可能となる問題とユーザ課金が実現困難な問題に対処するため，マルチキャスト用受信者認証グループ鍵配布プロトコル AKDP（Receiver Authentication and Group Key Delivery Protocol）を提案する．このプロトコルでは，データ秘匿のためのグループ鍵の配布，受信者アクセス制御，およびユーザ課金実現ための受信者認証の 3 つの機能を提供する．そして，AKDP の実装システムを用いた性能評価により，その有効性を示す．

次に本論文では，モバイルマルチキャストの問題とマルチキャストグループ管理の問題に注目することにする．既存のグループ管理プロトコルを移動通信網や無線 LAN で適用した場合，通信コストが高くなるほか，電源断や移動により受信者との接続が突然途絶えた場合の対策が行われていないという問題があった．これを解決するため，第 6 章では，モバイルマルチキャスト向けのグループ管理プロトコル MMGP（Mobile Multicast Group Management Protocol）を提案する．そして，MMGP と既存のマルチキャスト向けグループ管理プロトコル IGMP の制御パケット数と比較することにより，提案方式の方がより少ない通信量でグループ管理の実現が可能であることを示す．

第3章 明示的輻輳通知を用いた TCP の優先輻輳制御方式の提案

2.2節に説明したように，TCP は信頼性のあるストリーム転送をエンドトゥエンドで提供するトランスポート層の通信プロトコルであり，再送制御や順序制御，エラー検出等の機能を持つ．1990 年代になるとネットワークのデータ伝送速度は飛躍的に向上し，マルチメディア通信が実現可能となった．ここで扱われるデータは，主にリアルタイム性を要求する音声や動画などと，そうでないデータ通信などに分類される．これを利用し，サービスが要求する通信品質に応じて優先順位付けを行い，これに応じた優先制御を提供することで，マルチメディア通信におけるネットワークの全体的な利用効率を向上させることが期待された．しかし，TCP はデータ通信を行うことを前提に設計されたため，全てのコネクションは公平に扱われていた．このため，TCP に優先度制御を効率よく導入出来るかどうかは不明であった．

本章では，以上のような背景から，1990 年代後半において著者らが TCP の明示的輻輳通知に優先制御方式を導入した研究成果について述べる．まず，優先順位として IPv6 ヘッダで定義されている優先度を利用し，優先制御のための輻輳通知拡張ヘッダを定義する．次に，これを用いた RED ルータによる明示的輻輳通知方式を改良し，優先順位に応じた輻輳制御を行うための優先輻輳制御アルゴリズムを提案する．また，本方式の性能評価により，従来方式と同等な平均スループットを保ちながら提案方式による優先制御が可能であることを示す．

3.1. TCP の明示的輻輳通知

本節では，本研究に取り組むにあたり解決すべき課題と解決法について整理し，本節で取り組むべき課題を明らかにする．

2.2節で説明したように TCP では, 送信側はタイムアウトによりパケットの廃棄やネットワークの輻輳が発生したことを判断し，パケットの再送を行う．これは，内部のネットワークの輻輳状況を予想した制御方法であり，暗示的輻輳通知（Implicit Congestion Notification）と呼ばれる．この方式では輻輳発生時の性能回復が迅速でなく，さらに輻輳判断時の制御が実際のネットワークの状況を正確に反映していないため，スループットの低下を招く．伝搬遅延時間が大きい広域ネットワークではこの問題が特に顕著に現れる．インターネットの急速な拡大により伝搬遅延時間は増大することが予想され，この問題を改善することが急務となっている．

これに対し，ネットワーク内部の輻輳状況を明示的に送信側に通知する明示的輻輳通知方式（Explicit Congestion Notification：ECN）が提案されている[54]. 明示的輻輳通知は，ルータで軽度の輻輳が発生している，もしくは，輻輳発生の前兆があることを，送受信者へ通知する制御を加え，通知された輻輳情報を利用して，バッファがオーバーフローを引き起こす前に早期に輻輳回避を行う方式である．TCP/IP での明示的輻輳通知は，図3.1のように IP 層レベルで行われ，ルータにより検出された輻輳情報は IP パケットにより送受信者まで運搬され，輻輳制御を行う上位の TCP 層に渡される．

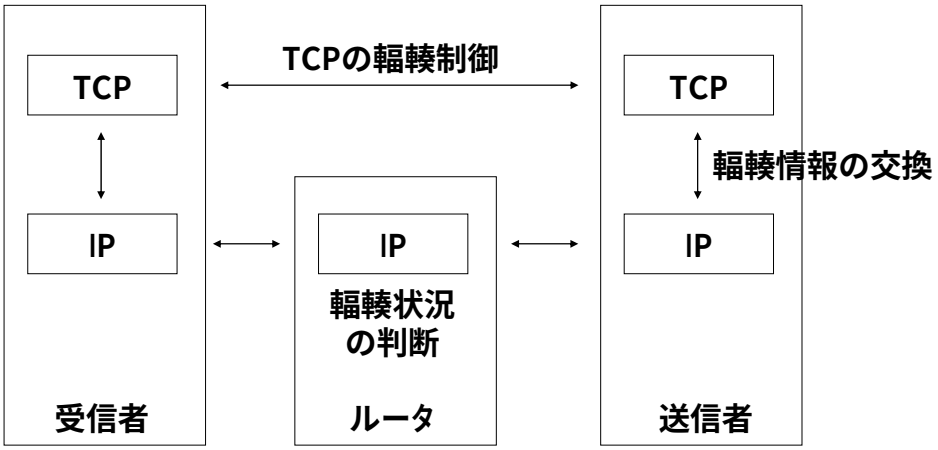


図3.1 TCP/IP の明示的輻輳通知

一方，従来のルータは，出力ポートのバッファが一杯になったあとにそのポート宛の IP パケットを廃棄する．これをドロップテイル（drop tail）と呼ぶ．ドロップテイルにより複数のコネクションからの IP パケットを連続して廃棄することがあり，これらのコネクションはタイムアウト発生により同時にウインドウサイズを低下さる（図3.2）．これにより，ネットワーク全体が同期するグローバルシンクロナイゼーション（Global Synchronization）を発生させるという欠点がある．グローバルシンクロナイゼーションはネットワークの利用効率を必要以上に低下させてしまうという不都合がある．

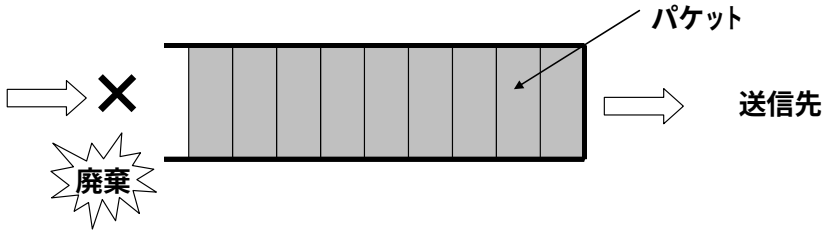


図3.2 ドロップテイルによるパケットの廃棄

このグローバルシンクロナイゼーションの問題を解決するため，ルータがバッファサイズとパケット廃棄の管理を行うバッファ管理方式 RED（Random Early Detection）が提案されている[24]．RED では，輻輳が発生し始めた段階になると，RED ルータが出力ポート中のパケットをキュー長に応じた確率でランダムに廃棄する．これにより，当該コネクションのスループットを一時的に下げ，その後に発生しうる重度の輻輳を避けるとともに，上述のグローバルシンクロナイゼーションを回避している．以下に RED ルータのアルゴリズム概要を示す．

RED ルータは，過去の履歴と現在のバッファ長に基づき，IP パケット到着ごとに平均バッファ長 avg を計算する．バッファ長に関してあらかじめ定義した $\min_{th}$（最小スレッショルド）と $\max_{th}$（最大スレッショルド）を比較し，$\max_{th} \le avg$ のときには IP パケットを廃棄し，$avg < \min_{th}$ のときには IP パケットの廃棄は行わない．$\min_{th} \le avg < \max_{th}$ のときは，確率 p_a で IP パケットを廃棄する．ただし，p_a は式(3.1)～(3.3)で計算される．p_a は avg の関数となっており，式(3.1)によって求められる加重平均を用いている．ここで，w_q

はバッファに対してバーストトラヒックおよび過渡的輻輳の許容限度を決める加重パラメタ，q は現時点でのバッファの長さ，$\max_p$ は P_b の上限値であり，*count* は最後に IP パケットが廃棄されてから廃棄されないで送出された IP パケット数のカウントである. IP パケットがバッファを占める割合が高い場合には式(3.2)により，また IP パケットを廃棄しない期間が長く続いたときには式(3.3)によって IP パケットが破棄される確率は高くなるよう計算される.

$$avg = (1 - w_q)avg + w_q \cdot q \tag{3.1}$$

$$P_b = \max_p (avg - \min_{th}) / (\max_{th} - \min_{th}) \tag{3.2}$$

$$P_a = P_b / (1 - count \cdot P_b) \tag{3.3}$$

以上に説明した RED を実装した RED ルータの特徴を以下に示す.

- 適切な $\min_{th}$ と $\max_{th}$ の値により長期間にわたっての平均バッファサイズが制御可能である.

- 廃棄される IP パケットの確率が，ルータにおいてそれらが属するコネクションの使用帯域に比例する仕組みになっているため各コネクションに対するフェアネスも保たれる.

- ランダムな確率 P_a で IP パケットが廃棄されることから, 連続して複数のコネクションの IP パケットを廃棄する確率が低く，既存の TCP の問題点であったグローバルシンクロナイゼーションを避けることが出来る.

- 加重平均により *avg* を決定するため，短期間のバーストトラヒックや過渡的な輻輳は許容される.

- あるコネクションの IP パケットがバースト的にルータに到着した場合でも，特定のコネクションからの IP パケットが連続してバッファ溢れを起こし，バーストデータの大部分が廃棄されることが少なくなる[55].

なお，先述した RED ルータにおいて，IP パケットの廃棄を行う代わりに，パケットヘッダに輻輳情報通知のフィールドを設けエンドホストへと通知するものが，RED ルータを用いた ECN である．この方式は，文献[56]で提案され，文献[54]で補足されている．以下で RED ルータを用いた ECN について概要を説明する.

ECN を行うために IP ヘッダと TCP ヘッダに次のフィールドを設ける．IP ヘッダには，ECT（Congestion Capable Transport）と CE（Congestion Experienced）ビットを設ける．これらのビットは文献[54]によると，IPv6 におけるトラヒッククラスフィールド[4]に，また，IPv4 では ToS（Type of Service）フィールド[15]に置かれる．TCP ヘッダには，ECN-Echo フラグと，CWR（Congestion Window Reduced）フラグを設け，これらのフラグは TCP ヘッダの使用されていない予約フィールド[1]に置かれる．なお，全ての値は 0 がデフォルトである.

以下では，図3.3を用い，RED ルータを用いた ECN の動作について以下に説明する.

1. データの送信側と受信側は，TCP コネクションセットアップ時に，ECN 対応であるかどうかを判断し，もし ECN 対応可能であれば，IP ヘッダの ECT ビットをセットする．これにより，エンドホストが ECN 対応であることをルータに知らせることが

出来る．また，CE ビットはデフォルトである 0 のままにして送信する（図3.3の IP パケット 6 から 8）．

2. 中継ノードとなる RED ルータでは前述した RED アルゴリズムの計算を行う．これにより，IP パケットを廃棄すると判断した時には，IP ヘッダの ECT ビットがセットされていることを確かめ，IP パケットを廃棄する代わりに CE ビットを 1 にセットする（図3.3の IP パケット 4，5）．もし，ECT ビットがセットされてない場合にはエンドホストが ECN 対応でないことになるので，従来どおり IP パケットの廃棄を行う．

3. 受信側 IP は CE ビットがセットされた IP パケットを受け取ると（図3.3の IP パケット 3），その情報を IP のデータ部とともに上位の TCP へと渡す．

4. 受信側 TCP は，受信パケットに対する ACK を含む TCP パケットの ECN-Echo フラグをセットし（図3.3のパケット 2），送信側へ報告する．以後，送信側の輻輳ウインドウを減少させたことを意味する CWR フラグの立ったパケットを受信側が受信するまで，返送する ACK 中の ECN-Echo フラグはセットし続ける．

5. 送信側 TCP で ECN-Echo フラグの立った ACK を受信すると（図3.3のパケット 1），受信側に輻輳ウインドウを減少させたことを知らせる役割をする CWR フラグをその後に返信するパケット中に立てた上で，以下の手順に従って輻輳回避を行う．

   (ア) TCP 送信側が ECN-Echo フラグの立ったパケットを受信すると，輻輳ウインドウサイズ（cwnd）と ssthresh を半減させ，輻輳回避モードに入る．このパケットを受信した時刻を t とすると，この時点以降，時刻 t までに送信したパケットの ACK が返信されるまでは，他のパケットの ECN-Echo フラグは無視する．この時点では，実際にパケットの消失が発生している訳ではなく，軽輻輳状態と言えるのでスロースタートを行う必要はない．

   (イ) 時刻 t に 3 つ目のデュプリケイト ACK（前に受信した ACK 番号と同じ ACK 番号である ACK のこと）[19]を受信し，直前のラウンドトリップ時間に ECN-Echo フラグに対応していないならば，文献[19]にて提案されている早期再送と早期回復の制御を行う．なお，早期再送，早期回復の制御は受信側にて受信したパケットの順序が入れ替わった状況に対処するために用いられるものであり，パケットの欠落による輻輳と判断することで輻輳ウインドウサイズを小さくしてしまう過剰な制御を防ぐ効果がある．また，（ア）と同様に，時刻 t までに送信されたデータの ACK が返る前に，他の ECN-Echo フラグがセットされているパケットを受信したとしても無視する．

   (ウ) 時刻 t に 3 つ目のデュプリケイト ACK を受信し，直前のラウンドトリップ時間に ECN-Echo フラグに対応していたならば，TCP の送信側は輻輳ウインドウサイズ（cwnd）と ssthresh の減少を行わずに消失したパケットの再送のみを行う．その後は早期回復の制御[19]に従う．

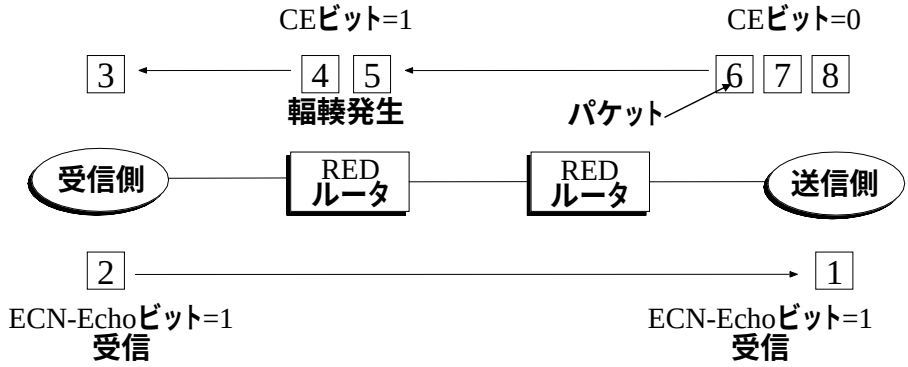


図3.3 RED ルータを用いた ECN の動作

以上に説明した RED ルータと ECN を既存のネットワークに適用することにより，これまでの TCP における，1）ネットワーク内部の輻輳状況を輻輳制御に反映できない問題と，2）Drop Tail により発生するグローバルシンクロナイゼーションの問題を解決することが可能となる．

しかし本章の冒頭に述べたように，通信のマルチメディア化に伴い，異なる要求品質を持つトラヒックごとに優先度を設け，各々を適切に処理することによりネットワーク全体の性能を向上させることが求められている．そこで次節では，RED ルータで設定する CE ビットのセット率 p_a を優先度に応じて適切に変更する優先輻輳制御方式を提案する．

3.2. 優先度を考慮に入れた輻輳通知方式

RED ルータを用いた ECN により優先度に応じた輻輳制御を行うため，本節では，高優先の IP パケットには CE ビットのセット確率 p_a を下げ，逆に低優先のものについては相対的に確率 p_a を高める方式を提案する．具体的な p_a の決定方法については3.2.3節で後述する．

優先度の通知には IP ヘッダを用いる．その際，本節では IPv6 を対象とすることにし，このヘッダで定義される優先度を用いる．また，3.1節で説明した ECT ビットや CE ビット，また，ECN-Echo フラグや CWR フラグを標準ヘッダ上に置くのは拡張性に乏しいため，IPv6 ヘッダのオプションとして輻輳通知拡張ヘッダを新たに提案することで実現する．

3.2.1. 優先度フィールド

IPv6 ヘッダでは，IP パケットの優先度は IPv6 ヘッダのトラヒッククラスフィールドに記述される[4]．トラヒッククラスフィールドは，8 ビットで構成され，発信者からの異なったサービスクラス，または優先度を識別するために用いられる．この値は上位層プロトコルにより与えられるが，ユーザに最も都合の良いトラヒックのクラス分けを行うようにするため，その定め方は文献[4]では具体的に与えておらず，別に定義することとなっている．現在このフィールドについての使用法について様々な実験が行われているが，その一つとして文献[57]と文献[58]ではディファレンシエイテッドサービス（Differentiated Services：DiffServ）が標準化されている．しかし，本研究が行われた当時，DiffServ はまだ検討中であった．また，本節では TCP において基本的な優先制御が実現可能であることを確認することを目的としているため，本提案では文献[4]で標準化された IPv6 ヘッダを用い

ることとする（図3.4）．このヘッダでは，優先度フィールドが 4 ビット，フローラベルフィールドが 24 ビットで表されている. 提案方式では, IP パケットの優先度を表現するために, この優先度フィールドを用いる．

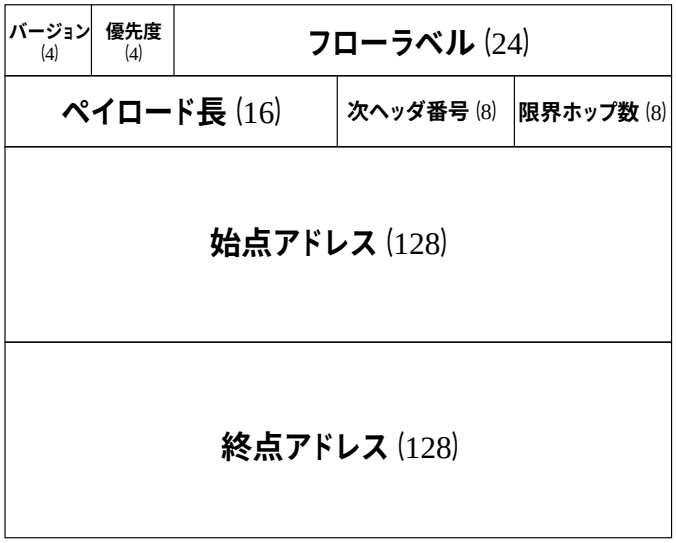


図3.4 IPv6 ヘッダの構成

IPv6 ヘッダの優先度フィールドは, 同じ発信者からの他の IP パケットと比較して, その望ましい配送優先権を識別することが出来る．優先順位の値は 0〜15 までであり，このうち 8〜15 までの値は相対的な優先度を表す．値 15 の優先度が一番高く，値 8 の優先度が一番低い．0〜7 までの値は別の目的で使用され，特定のアプリケーションに対して特別に割り当てられる．このため，以下では一般的に利用出来る 8〜15 までの値のみを優先度として使用することとした．この 8 段階の優先度では不十分な可能性も考えられるが，これは文献[4]の IPv6 での制約である．必要であれば IPv6 の拡張ヘッダを定義するなどして容易に拡張することも可能である．また，IPv6 の最新版である文献[59]では，優先度フィールドに相当する部分がトラヒッククラス部と再定義され，8 ビット長に拡張されている．この IPv6 の最新版を用いる場合には，トラヒッククラスフィールドのうちの４ビットを本研究で使用する目的のために割り当て, 8〜15 までの 8 段階の優先度を扱うことにより本章で述べる優先制御が可能である．

3.2.2. 輻輳通知拡張ヘッダ

各種輻輳通知のためのビットやフラグは，IP ヘッダの ToS フィールドや TCP ヘッダの将来の拡張のために予約された空きフィールドに置かれている[54]が，提案方式では，これらを輻輳制御拡張ヘッダにまとめることにする．これは，将来的に新たな拡張があり，輻輳通知のために新たなフィールドが必要とされた場合，標準 IP ヘッダまたは標準 TCP ヘッダを再定義するよりは，本来から拡張性のある IPv6 拡張ヘッダに輻輳制御用のフィールドを変更した方が再定義のオーバヘッドを減らせるためである．また，標準 TCP ヘッダを用いないことから，TCP 以外のトランスポート層プロトコルにおいて輻輳通知機能を用いる場合にも本提案方式は有効である．

図3.5に提案する輻輳制御拡張ヘッダを示す．本拡張ヘッダは 8 バイトで構成される．以下に各フィールドの役割について説明する．

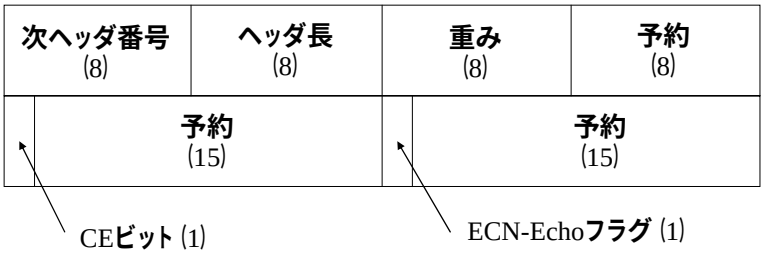


図3.5 輻輳通知拡張ヘッダ

- 次ヘッダ番号フィールドは，輻輳制御ヘッダのすぐ後に続くヘッダのタイプを識別する．

- ヘッダ長フィールドは拡張ヘッダの長さを表す．ヘッダ長は（ヘッダの総バイト数 － 8）となるため，提案ヘッダでは 0 になる．以上の 2 つのフィールドの使用法は，ルーティングヘッダなどの他の拡張ヘッダと同様である．

- 重みフィールドは，優先度の重みを考慮にいれるために用いられ，最小 0～最大 255 までの値を送信側のユーザがセットする．

- 輻輳の通知のため，CE ビット，ECN-Echo フラグを 1 ビットずつ用意する．本輻輳通知拡張ヘッダでは，ECT ビットと CWR フラグフィールドは設けない．ECT ビットについては，このビットをセットする代わりに，この拡張ヘッダが存在することでエンドホストが ECN 対応であることを意味するために削除可能である．また，CWR フラグフィールドについては，このフィールドを設けない代わりに，受信側は CE ビットを受信した後に，ECN-Echo フラグをセットした ACK を一度だけ返信することで実現する．この CWR フラグにおけるこの扱いは文献[60]の実装で用いられたものと同様である．

- その他の部分は，将来の拡張のための予約フィールドとする．今回はこのフィールドについては定義を行わない．

3.2.3. CE ビットのセット確率

本節では，提案方式における CE ビットのセット確率 p_a の定義を行う．本方式では高優先の IP パケットには CE ビットのセット確率 p_a を下げ，逆に低優先のものについては相対的に確率 p_a を高める．従って，3.1節で述べた CE ビットのセットアルゴリズムおいて，$\min_{th} \le avg < \max_{th}$ のときに CE ビットをセットする確率として以下の式(3.4)を用いることとする．これ以外のセット確率および輻輳制御については，3.1節に準じる．

$$P_{new} = P_a \frac{(15 - pri)^w}{(15 - b)^w} \tag{3.4}$$

- P_{new} ： 提案式により新たに得る CE ビットのセット率 $\max(P_{new}) = 1$
- p_a ： 式(3.2)と式(3.3)の RED ルータのアルゴリズムで与えられた CE ビットのセット率

- pri ： IPv6 の優先度フィールドで与えられる IP パケットの優先度
- b ： 基準となる優先度
- w ： 提案した輻輳制御ヘッダの重みフィールドで与えられる優先度の重み

式(3.4)において，基準となる優先度bの値を境に優先度の大小が区別される．ここでは優先度として文献[4]における IPv6 ヘッダの 8〜15 までの 8 段階の数値を扱い，優先度 15 は特に緊急度が高い IP パケットに対して付することにするので，提案方式ではbとして 8 と 14 の中間の値である 11 を用いる．この理由は，本方式では，各 IP パケットに与えられた優先度の分布が一様である状況を想定しているためである．この場合，優先度の平均値（=11）以外の値を基準として用いると，優先度が 8 段階しかないため IP パケットの廃棄率に大きな偏りが生じ，ユーザが求めた優先度と実際に得たスループットに隔たりが生じる場合があるため適切ではない．

優先度の重みwは値が大きいほど確率P_{new}の変動率が上がる．ただし，$w=0$ならば，$P_{new}=p_a$となるため，優先制御を行わない従来方式と同じになる．表3.1は，wを変化させたときのP_{new}のp_aに対する比率を優先度 9，11，13 の場合について比較している．表3.1より，wが大きくなるに従い，優先度 9 のP_{new}が上昇することが分かり，そのスループットは低下することが予想される．同様に，優先度 13 のP_{new}は下降するので，そのスループットは上昇すると予想出来る．また$w=0$と$w=1$以外の値の場合には，CE ビットのセット確率の平均値が上昇する．例えば，式(3.4)において$w=4$とするとき，p_aに対する優先度 9，13 のときのP_{new}の比率は，それぞれ 5.0625，0.0625 であり，優先度 9 の上昇率が優先度 13 の下降率よりも大きい．この場合，低優先の IP パケットに高確率で CE ビットがセットされることになるが，CE ビットがセットされる頻度が上がると，ウインドウサイズが小さくなる頻度も高くなる．このため，ルータのバッファを占める IP パケット量が減少し，式(3.2)によりP_bが減少する．さらに，式(3.3)により，CE ビットセット直後には$count$の値は 0 にリセットされてp_aも減少することになる．p_aの減少により，次に CE ビットをセットするまでの期間の延びが期待出来ることから，結果として CE ビットセット率はそれほど上昇せずに一様に調整されると考えられる．次節では，これらを確認し，本方式の有効性を示すため，計算機シミュレーションを用いた実験を行う．

表3.1 P_{new}のP_aに対する比率

重み	優先度 9	優先度 11	優先度 13
$w=0$	1.00	1.00	1.00
$w=1$	1.50	1.00	0.50
$w=2$	2.25	1.00	0.25
$w=3$	3.375	1.00	0.125
$w=4$	5.0625	1.00	0.0625

3.3. シミュレーションによる評価

前節で提案した優先度を考慮にいれた輻輳通知方式の有効性を確認するため，ネットワークシミュレータ ns[61]を用い，計算機シミュレーションにより実験を行う．ネットワークモデルを図3.6に示し，以下で本モデルの条件を示す．

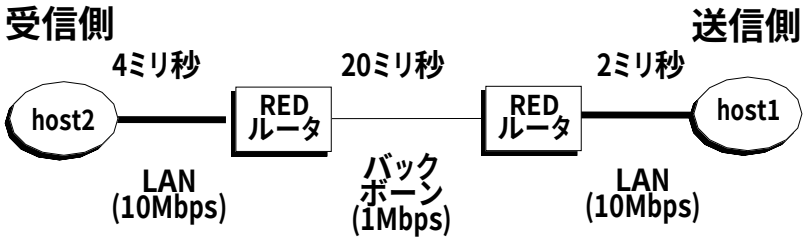


図3.6 ネットワークモデル

- ネットワークには WAN（Wide Area Network）を想定する．伝送速度は LAN（Local Area Network）内で host1 側，および host2 側ともに 10Mbps，バックボーンネットワークで 1Mbps とする．現在，LAN やバックボーンネットワークはこれ以上に高速なものも普及している．しかし，実際には他のユーザもこのリンクを使用しているなどの原因により，各コネクションはネットワークの最大帯域をすべて使用することができないのが典型である．このような状況を考慮し，シミュレーション上では図に示した値を用いた．また，伝搬遅延は LAN 内でそれぞれ 2 ミリ秒，4 ミリ秒とし，バックボーンリンクで 20 ミリ秒とする．

- エンドホストは ECN 対応とし，内部ホストは3.1節で説明した RED ルータによる ECN 動作が可能であるものとする．

送信側は無限大の送信データを保持し，ウインドウサイズの範囲内でパケットを送出し続ける状況を作る．これはボトルネックとなる 1Mbps のバックボーンネットワークが，つねに送信データを保持している状態にするためである．送信側が保持するデータを連続的に送信するために，FTP によるデータの転送を行う．実験では，ネットワークモデル上に 4 つの FTP コネクションを用意し，それぞれ表3.2に示す優先度を持つ．なお，表3.2での ftp1 などの表記は FTP コネクションの識別名を表す．

表3.2 シミュレーションで用いるコネクションと優先度

コネクション	識別名	FTP の種類	優先度
host1→host2	ftp1	低優先の FTP	9
host1→host2	ftp2	通常の FTP	11
host1→host2	ftp3	通常の FTP	11
host1→host2	ftp4	高優先の FTP	13

各実験に共通なシミュレーション条件は次のとおりである．

- ns には ns-2.0 を用いる．

- 4.3BSD Reno で実装された TCP を用いる．

- ACK のサイズは 68 バイトとする．これは標準 TCP ヘッダ（20 バイト）と標準 IPv6 ヘッダ（40 バイト）に輻輳通知拡張ヘッダ （8 バイト）を加えた総和である．

- $\max_p = 1/50$ とする．これは，この値を 0.1 以下にすることが望ましいとする文献[24]における値である．

- RED ルータのバッファの加重平均 $w_q = 0.002$ とする．これは文献[24]で 0.001 以上を推奨しており，この実験で用いられた値である．

- 精度検定は信頼区間 95%のバッチ平均法により行い，精度は 5%以内とした．

以下の実験では次に示す条件をもとに $\min_{th}$，IP パケットサイズ，優先度の重み w のそれぞれを変化させたときのスループットの様子について評価する．

- $\min_{th} = 12 \times 512$ バイトとする．また，文献[24]では，$\max_{th}$ は最低でも $\min_{th}$ の 2 倍が有益だとしてあり，文献[24]の実験でも用いられた $\max_{th} = 3 \times \min_{th}$ とする．しかし, この文献においてこれらの値についてはさらなる研究が必要だとしている．

- IP パケットサイズは，インターネットのトラヒックの IP パケットサイズは大部分が 512 バイトであることを調査した文献[62]の結果を踏まえて，512 バイトとするが，この値を変化させた実験も行う．

- 重みは，$w = 1$とする．重みの影響が最も小さい $w = 1$で他のパラメタに関する実験を行い，最後の実験で w を変化させたときの比較を行う．

3.3.1. 受信パケット数の比較

図3.7にコネクション開始から 60 秒間の受信パケット数を示す. ここでは ftp1（優先度 9）と ftp4（優先度 13）の 2 つのコネクションに対して，それぞれ優先制御を行ったときと行わないときの 2 種類を示す.

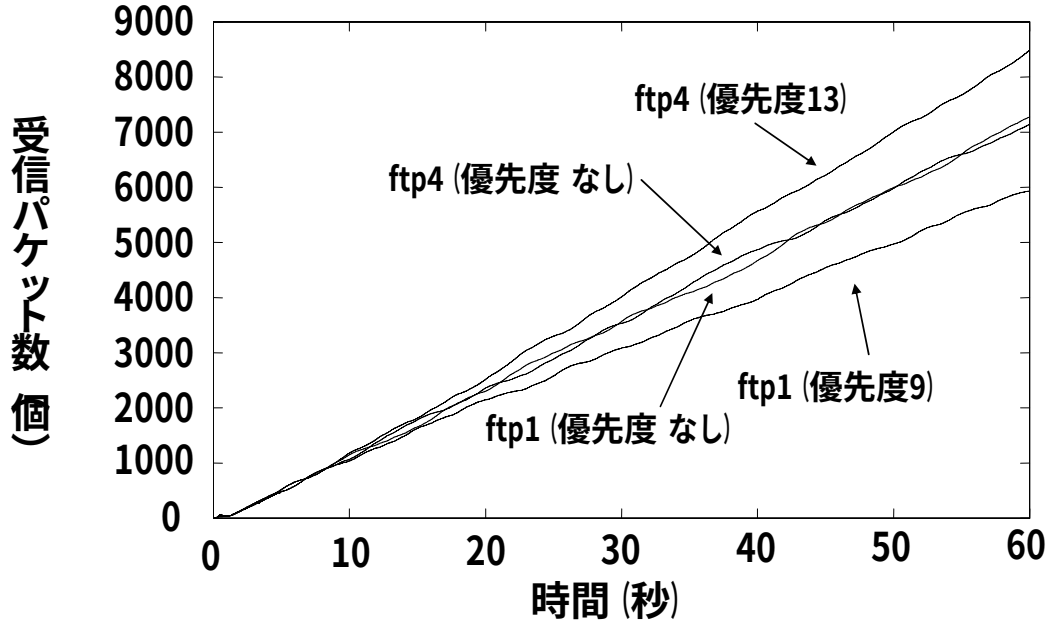


図3.7 受信パケット数の比較

図3.7において，ftp1 では，開始から 30 秒後，および 60 秒後に受信したパケット数は，優先制御なしの場合にそれぞれ 3565 個（1825K バイト），および 7280 個（3727K バイト）であるのに対し，優先度 9 では 3081 個（1577K バイト），および 5933 個（3038K バイト）となり，優先制御なしの場合の 86.4%，および 81.5%に低下している．また，ftp4 は，優先制御なしの場合の 3532 個（1808K バイト），および 7141 個（3656K バイト）から，優先度 13 では 4016 個（2056K バイト），および 8488 個（4346K バイト）となり，優先制御なしの場合の 113.7%，および 118.9%に上昇している．以上から，低優先分のスループットが高優先のそれに割り当てられていることが分かり，優先度を考慮した輻輳制御が行われていることが確認出来る．

3.3.2. 最小スレッショルドの変化による比較

ルータのバッファにおける $\min_{th}$ を 4096 バイト，5120 バイト，6144 バイト，7168 バイト，8192 バイトと変化させた場合のスループットを比較する．図3.8に優先度を考慮しない場合を，図3.9に優先度を考慮した場合のシミュレーション結果を示す．

図3.8から，優先制御なしの場合には 4 つのコネクションでそれぞれ 250Kbps のスループットが得られており，すべての $\min_{th}$ について等しい．これは，ボトルネックとなっている 1Mbps の帯域を 4 つのコネクションで均等に利用しているからである．

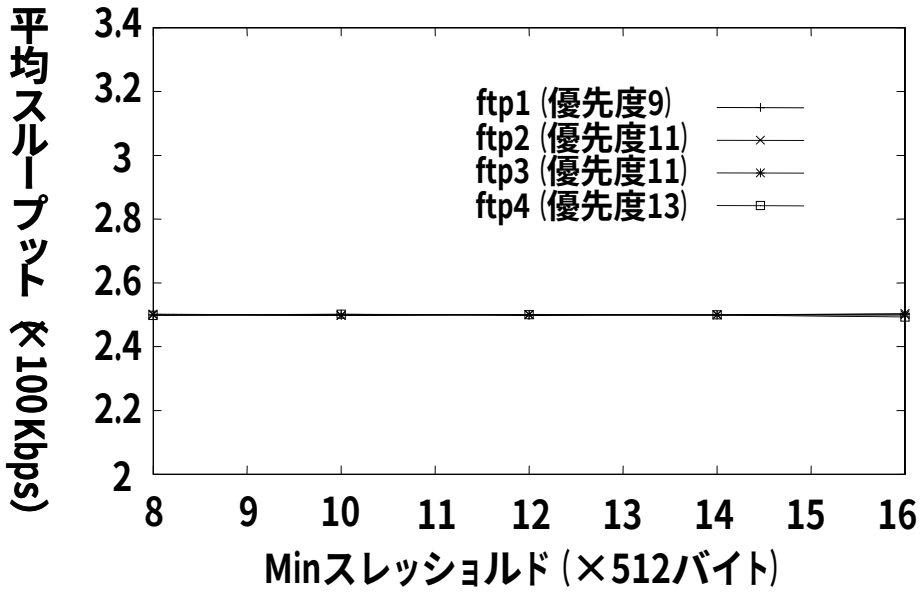


図3.8 $\min_{th}$ とスループットの比較 （優先度 なし）

図3.9より， $\min_{th}$ を大きくするに従い，高優先のスループットは減少するが，低優先のそれは増加し，高優先と低優先のスループットの差が小さくなる．例えば，$\min_{th} = 4096$ バイトのとき，ftp1 と ftp4 のスループットはそれぞれ 208Kbps，311Kbps であり，図3.8の結果（250Kbps）との比率はそれぞれ 83.2%，124.4%となるのに対し， $\min_{th} = 8192$ バイトでは 241Kbps，259Kbps にとどまり，比率もそれぞれ 96.4%，103.6%である．これは，$\min_{th}$ が大きくなると CE ビットをセットする確率が下がるためであり，非輻輳時には優先度の低い IP パケットの送信を制限しないことを示している．また，ftp2 と ftp3 のスループットは 240～250Kbps に収まり，図3.8とほぼ同じ結果となった．さらに，全 ftp の平均

スループットはすべての min_{th} で 250Kbps であり，図3.8の結果と同じ値である．従って，優先制御により全体のスループットは低下しないことが分かった.

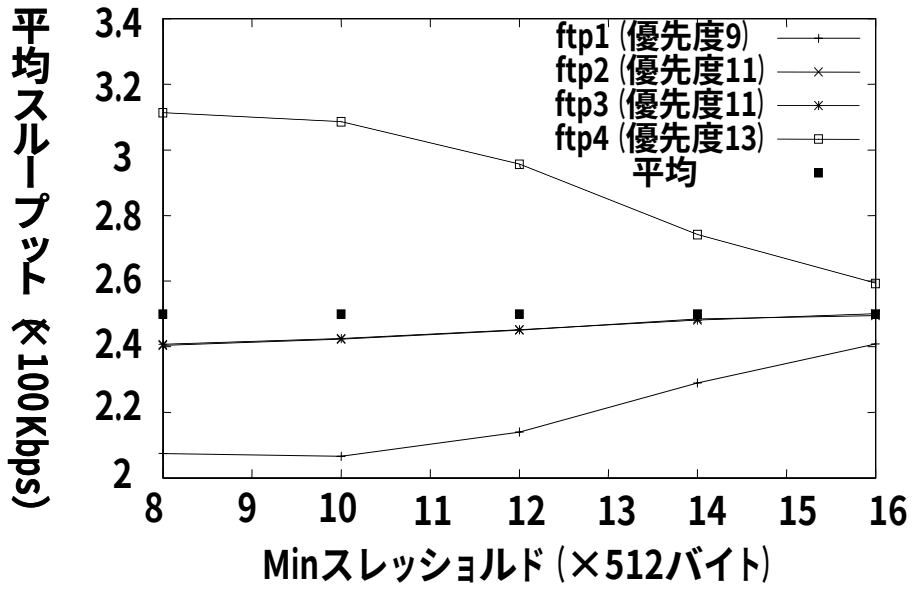


図3.9 min_{th} とスループットの比較 （優先度 あり）

3.3.3. IP パケットサイズの変化による比較

送信 IP パケットサイズを 512 バイト，1024 バイト，1536 バイト，2048 バイトと変化させた際のスループットの変化を比較する．図3.10に優先度を考慮しない場合を，図3.11に優先度を考慮した場合のシミュレーション結果を示す.

図3.10から, 優先度を考慮しない場合には各コネクションにスループットの違いは見られない．これは与えられた帯域を 4 つのコネクションで均等に利用しているからである．4 つの ftp の平均スループットは，IP パケットサイズが小さい順に 250Kbps，249Kbps，242Kbps，223Kbps となり，IP パケットサイズが大きくなるに従い徐々に低下していることが分かる．これは，IP パケットサイズが大きくなるほど，再送によるオーバヘッドが大きくなるためである.

しかし，文献[62]より多くの IP パケットサイズは 512 バイトであるため，ユーザは IP パケットサイズによる再送オーバヘッドの相違を意識せずに優先度を割り当て，それに伴ったスループットを得ることが出来る.

図3.11より，IP パケットサイズを大きくするに従い，高優先のスループットは減少するが，低優先のそれは IP パケットサイズが 1536 バイトまでは増加し，それ以降は減少している．ただし，IP パケットサイズが大きくなるに従い，全体的に徐々に低下している．たとえば，IP パケットサイズが 512 バイトのとき，ftp1 と ftp4 のスループットはそれぞれ 214Kbps，296Kbps であり，図3.10の結果（250Kbps）との比率はそれぞれ 85.6%，118.4% となるのに対し，IP パケットサイズが 2048 バイトでは 216Kbps，226Kbps にとどまり，図3.10の結果（223Kbps）との比率もそれぞれ 96.9%，101.3%である．この理由は，図3.10の結果と同様，再送オーバヘッドによるものである．また，図3.11での 4 つの ftp の平均値は，IP パケットサイズが小さい順に 250Kbps，250Kbps，240Kbps，222Kbps であり，図

3.10の各 IP パケットサイズにおけるスループットとほぼ同じ値である．従って，優先制御による全体のスループットの低下はほとんど見られないことが分かる．

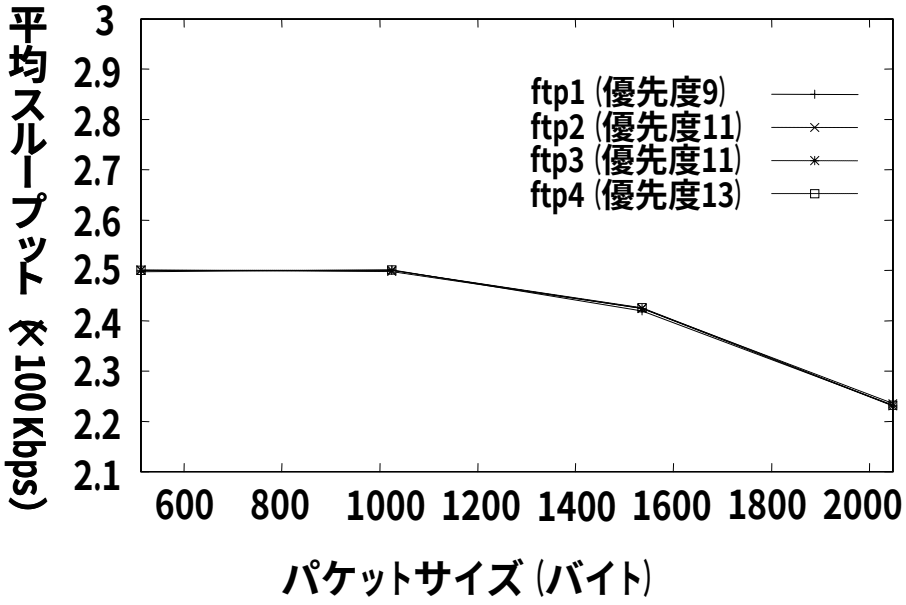


図3.10 IP パケットサイズとスループットの比較 （優先度 なし）

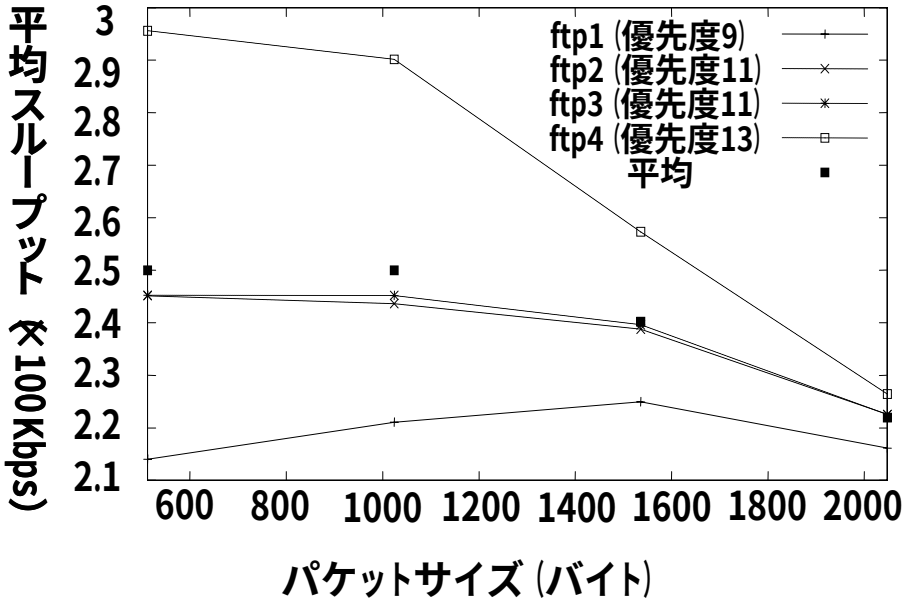


図3.11 IP パケットサイズとスループットの比較（優先度 あり）

3.3.4. 重みの変化による比較

図3.12は優先度の重み w を変化させたときの各優先度におけるスループットを示している．

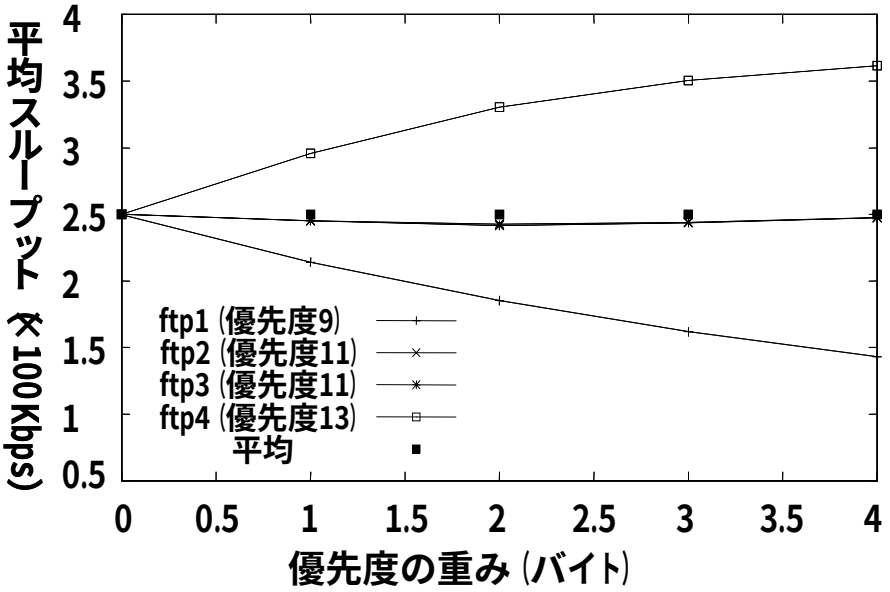


図3.12 優先度の重みによるスループットの比較

図3.12では優先度の重みwを高くすると，高優先と低優先 IP パケットのスループットの差が大きくなることが確認出来る．優先度の重みが$w=0$のときには優先制御を行わない場合であり，4 つの ftp で 250Kbps のスループットが得られている．ftp1 はwの値が大きくなるに従ってスループットが低下しているのに対し，ftp4 は上昇している．たとえば，$w=2$のときの ftp1，ftp4 の値はそれぞれ 185Kbps，330Kbps となり，$w=4$のときはそれぞれ 143Kbps，362Kbps となっている．さらに，ftp2 と ftp3 は 240～250Kbps であり，$w=0$のときとスループットがほぼ等しい．また，各 ftp の平均スループットは$w=0$の場合と同じく 250Kbps である．wによる CE ビットセット確率の影響については3.2.3節で考察したが，$w=4$において ftp1 のスループットは$w=0$のときの 42.8%の減少にとどまっており，表3.1での確率が約 5 倍となったことを考慮すると下降幅は十分抑えられていることが確認された．ftp4 のスループットについても 44.8%の増加であり，同様のことが言える．以上のことから，優先度の重みwの値を高く設定することにより，全体のスループットを低下させることなく，高いスループットを求めているユーザに対して適切なスループットを割り当て可能なことが分かった．

次に，図3.12で得られたスループットで 1M バイトと 80 バイトのファイル転送に何秒要するかを比較した結果を表3.3に示す．なお，表中の優先度 11 は ftp2 と ftp3 の平均スループットを用いている．また，各優先度の項目の左側(1)に 1M バイトの転送に要する時間（秒），右側(2)に 80 バイトのファイル 1000 個の転送に要する時間（秒）を表している．前者は通常のファイル転送を，後者はリアルタイム性の通信におけるファイル転送を想定出来る．前者では優先制御を行わない場合（$w=0$）は 32.0 秒であり，優先度 9 では$w=1$，$w=4$のとき，それぞれ 37.4 秒，56.0 秒となり，それぞれ 16.9%，75.0%の増加となる．後者の場合，w=0 のときは 2.56 秒であるのに対し，優先度 13 では$w=1$，$w=4$においてそれぞれ 2.16 秒，1.77 秒となり，一個あたり，0.40 ミリ秒，0.79 ミリ秒の減少となる．前者の増加は 2 倍以下にとどまることから，重要性の低いファイル転送を割り当てた場合では十分実用性に耐える．逆に後者の減少は体感的にはほとんど相違はないが，時間制約が厳しい場合はこの減少幅は大きく，その効果は前者の転送時間の増加を十分補うものである．

表3.3 データの転送にかかる時間（秒）

w	優先度 9		優先度 11		優先度 13	
	（1）	（2）	（1）	（2）	（1）	（2）
0	32.0	2.56	32.0	2.56	32.0	2.56
1	37.4	2.99	32.6	2.61	27.0	2.16
2	43.2	3.45	33.0	2.64	24.2	1.94
3	49.4	3.96	32.8	2.63	22.8	1.83
4	56.0	4.47	32.3	2.59	22.1	1.77

（1）：1M バイト×1 個
（2）：80 バイト×1000 個

3.3.5. 優先度の分布に偏りがある場合の比較

ここまでは，ユーザにより与えられた優先度に偏りがない場合について実験を行った．本節では，与えられた優先度に偏りがあった場合にどのように動作するかについて検証する．

以下の実験では，表3.4の 7 つの場合の優先度の偏りを持たせる．以下では，この表をもとにユーザが保持するデータの優先度にどのような偏りを持たせたかを説明する．case1 は偏りのない場合であり, case2 は全てのユーザが高優先データの転送を要求した場合, case3 は高優先データの転送要求が多いが，低優先データの転送要求もある場合，case4 は低優先データの転送要求が多いが，高優先データの転送要求もある場合，case5 は低優先データの転送要求が多い場合，case6 は高優先でも低優先でもないデータの転送要求が多いが，特に緊急度の高いデータの転送要求もある場合, case7 は特に緊急度の高いデータ転送の要求が多数あり，高優先でも低優先でもないデータの転送もある場合を想定している．

表3.4 各コネクションに与えた優先度

識別名	case1	case2	case3	case4	case5	case6	case7
ftp1	9	13	9	9	9	11	11
ftp 2	11	13	13	9	9	11	15
ftp 3	11	13	13	9	9	11	15
ftp 4	13	13	13	13	11	15	15

表3.4で与えた各場合において，各 FTP コネクションの平均スループットと，4 つの FTP コネクション全体の平均スループットを表3.5に示す．

表3.5 各コネクションの平均スループット（×Kbps）

識別名	case1	case2	case3	case4	case5	case6	case7
ftp 1	215	250	194	229	241	210	102
ftp 2	245	250	269	229	241	210	300
ftp 3	245	250	269	229	241	210	299
ftp 4	296	250	269	313	275	370	299
平均	250	250	250	250	250	250	250

case2 では，全てのコネクションが高優先である優先度 13 を要求しているため，本来高優先のデータとして扱われなければならないにもかかわらず，優先制御のない場合と同じ 250Kbps のスループットしか得られておらず，4 つのコネクションが均等にネットワークを利用している．また，case3 では，優先度 13 を要求しているコネクションでは平均値の 107.6%とスループットの上昇は得られているが，3 つのコネクションが優先度 13 を要求しているため，case1 の優先度 13 で得られた 118.4%には及ばない．また，case4 では，優先度 13 を要求しているコネクションでは 125.2%とスループットの上昇が得られており，case1 の 118.4%より高くなっているが，これは，他の 3 コネクションが優先度 9 を要求しているからである．また，case5 では，高優先でも低優先でもない優先度 11 を要求しているコネクションでは 110.4%とスループットの上昇が得られているが，これは，他の 3 コネクションが低優先である優先度 9 を要求しているためである．また，case6 では特に優先度の高いものに与える優先度 15 のスループットは 148.0%と大幅な上昇が得られているが，優先度 11 の 3 つのコネクションのスループットが低下している．さらに，case7 では 3 つのコネクションに優先度 15 を与えているので，約 120.0%の上昇にとどまっており，逆に優先度 11 のスループットが 40.8%と極端に低下している．

以上のように，各コネクションによって得られるスループットは，その時点において，他のコネクションの優先度がどのように与えられているかということに左右され，それは相対的なものであることが分かる．典型的な例をあげると，case2 と case5 を比較すると，case2 では優先度 13 が与えられているのにもかからず，case5 の優先度 11 で得られるスループットよりも低くなるという逆転現象が発生している．ただし，各優先度に偏りがある場合においても，優先度の高低に従ったスループットが得られること，さらに，全体のスループットの低下はなく平均スループットは各場合で等しいことが示された．

そもそも TCP は，各コネクションに対して提供されるスループットは保証されていない．従って，高い優先度のコネクションに対して，必ずしも高いスループットが割り当てられないのは妥当である．しかし，本結果は，全体のコネクションの平均スループットを保ちながら，本方式により各コネクションに与えるスループットを相対的に制御出来ることを示している．従って，各優先度の分布をあらかじめ規定することが出来れば，本方式により，各優先度のコネクションに対して割り当てられるスループットをある程度予測出来ることを示唆している．

3.4. 本章のまとめ

本章では，明示的輻輳通知を利用した TCP の優先制御方式の提案を行い，計算機シミュレーションにより提案方式の性能評価を行った．性能評価の結果，従来方式と同等な平均スループットを保ちながら提案方式による優先輻輳制御が可能であることが示された．また，バッファ長の閾値（$\min_{th}$）や IP パケットサイズ，優先度の重み w の変化に対する関係を，シミュレーションにより定量的に示したことは，優先制御方式の研究に対して重要な知見を与えることが出来た．

本提案方式の特徴をまとめると，以下の事項があげられる．

- いずれの条件下でも，平均スループットは，優先制御を行わない場合と，優先制御を行った場合に，ほぼ同じ値になっているという結果が得られた．すなわち，RED ルータを用いた ECN の CE ビットセット確率に変更を加えるだけで，平均スループットを落とすことなく，優先制御が実現可能である．

- 重み w を変化させることによって優先制御の度合を調整出来る．

- 従来の IPv6 の優先度フィールドを用いる優先制御において，優先度の低い IP パケットは輻輳の条件の下では廃棄されることを意図して設定されている[4]．しかし，廃棄したパケットは再送される必要があることから，この方式では再送オーバヘッドが生じることになる．これに対して，本方式では，輻輳通知に RED ルータを用いた ECN を用い，前もってウインドウサイズを下げるように通知する．これにより，優先制御のために廃棄される IP パケットは減少し，オーバヘッドを減らすという利点がある．

- 本方式の優先制御は，IP ヘッダから IP パケットの優先度を取り出すことと，RED ルータのアルゴリズムにより計算される CE ビットセット確率 P_a の変更のみであり，これに要する処理時間は十分に小さいので，優先度処理によるオーバヘッドは考察の対象とはしなかった．ただし，本提案方式は，RED アルゴリズムが実装されているルータを用いて実現する必要がある．もし，実装されていないルータが介在したとしても，このルータは IPv6 の輻輳通知拡張ヘッダを無視して通常の動作を行うことが出来るので，現存システムから RED ルータへの部分的な移行がスムーズに行える．

本研究と同様な優先度制御方式の導入に関する研究は現在に至るまで様々な提案が行われている．例えば，本提案と同様に IP ヘッダの優先度を利用し，IP レベルでの優先度制御の枠組みを提供する DiffServ が 1998 年に最初に提案され[57][58]，その後様々な拡張がされている．本研究などの提案により従来の通信方式の枠組みを維持しつつも全体の通信効率を低下させることなく優先度制御が可能なことを示したことは，マルチメディア通信において不可欠となる QoS（Quality of Service）保証の実現のための基礎を示したものであり，一定の成果を修めたといえる．なお，QoS 保証はその重要性が認識されつつも，一般に定着した方式が未だに存在しておらず，今後も更なる研究が必要とされる．

3.4.1. 今後の研究課題

今回の実験では，FTP を用いたデータの転送による実験を行ったが，優先度の低い FTP としては，時間的制約がないデータを転送する場合を想定することができ，anonymous FTP での転送や，データのミラーリングが例としてあげられる．また，優先度の高い FTP としては，時間的制約があるデータを転送する場合が考えられる．他のプロトコルについては，対話性のない SMTP や NNTP の転送は，高いスループットを必要としないので優先度を低く設定することができ，逆に対話性のある TELNET，HTTP などの転送は優先度を高く設定することが望まれる．

本方式では優先度や重みの設定はユーザが自由に行うことが出来るため，ユーザが与えた優先度に偏りがある場合には，低優先のデータのスループットが極端に下がる場合があった．この時には，一時的に低優先のデータのスループットを上げるための制御を加えることや，偏りがなくなるようユーザに報告するといった考慮が必要である．ユーザは自分のデータに対しては高いスループットを得たいという希望があるため，このような必要性が頻繁に発生する可能性がある．従って，ユーザは得られるスループットの特性を理解したうえで，優先度を与える際に偏りが生じないように考慮する必要があるが，適切な優先度の値の基準を与えることは難しい．この制御方法とその評価については研究の余地があるが，一つの解決法として，オペレーティングシステムのプロセスに優先度が与えられたときのタスクスケジューリングの方式を応用して，ユーザから指定された優先度をネットワークの状況に応じてシステムが変更する方策が考えられる．

第4章 W-CDMA 上の HTTP/TCP と WAP の性能評価

移動通信網は，当初，固定電話の代替手段としての音声通信のみが可能なアナログ通信であったが，加入者収容数の拡大とデータ通信の提供を実現するため，1993 年からデジタル通信による第二世代移動通信網のサービスが開始された．しかし，この世代の移動通信網では通信速度は 9.6Kbps までと低く，また，エラー発生率が高いといった無線通信特有の性質から，データ通信に TCP をそのまま適用することは問題があった．そこで，携帯電話等から Web ページなどを参照するための通信プロトコルとして 1998 年に WAP（Wireless Application Protocol）が提案された[6]．WAP は，GSM（Global Systems for Mobile Communications）等の第二世代移動通信網の利用を主に想定し，様々な移動通信網に適用出来るように設計されている[63]．この WAP の登場により，携帯端末からインターネット上のコンテンツを容易に利用することが可能となり，ユーザの利便性が大幅に向上した．

その結果，携帯端末の通信速度の大幅な向上がますます求められるようになり，2001 年には最大で 384Kbps の通信速度を提供する第三世代移動通信網が開発された[63]．これにより，従来のファイル転送のみならず，より高い伝送速度が必要な動画像などを含むマルチメディア通信を携帯端末上で利用することがより現実に近づいた．その一方で，この当時，低速度な第二世代移動通信網を前提とした WAP では，第三世代移動通信網における性能が十分に活用されない可能性があるという問題点が指摘されるとともに，そのための代替プロトコルの提供が重要な課題となっていた．

本章では，この課題を解決するため著者らが 2000 年代初めに行った研究成果について述べる．まず，WAP について概説する．次に，第三世代移動通信網の代表的な無線アクセス方式である W-CDMA（Wideband Code Division Multiple Access）を対象とし，WAP が持つバイナリエンコーディング等の無線通信向けの機能について評価を行い，第三世代移動通信網におけるこれらの機能の有効性を検証する．最後に，WAP と HTTP/TCP（TCP 上で動作した HTTP）の比較を行うとともに，その結果に基づき，第三世代移動通信網に適したプロトコルとそのネットワークアーキテクチャを提案する．

4.1. WAP 概要

WAP は，主に第二世代移動通信網等の低速な移動通信網を対象として，1997 年に設立された WAP フォーラムによって開発された通信プロトコルである．WAP は，移動通信網に接続する携帯電話や PDA 等の携帯端末からインターネットにアクセスし，WWW 等の各種アプリケーションを提供する他にも，テレフォニーアプリケーションと呼ばれる電話機能との連携，また，電子メールの着信通知等のプッシュ機能を提供することを特徴としている．

PC を利用した場合とは異なり，携帯端末には画面サイズや CPU 処理能力等の制約がある．また，無線ネットワークでは高遅延，高エラー率といった通信環境を考慮する必要があり，WAP は通信の中断と再開や，コンテンツや各種ヘッダのバイナリエンコーディング

による圧縮などの有線ネットワークでは利用されない各種機能を提供することで，これらの条件の元においても十分に性能が得られるように設計されている[6].

WAP 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 プロトコルは，WAP クライアントと WAP ゲートウェイ間で使用され，インターネットのプロトコル（HTTP，TCP）が WAP ゲートウェイとオリジンサーバ間で使用される（図4.1）．WAP では，移動通信網の各種要求条件を満たすために各種の最適化や拡張が行われる．

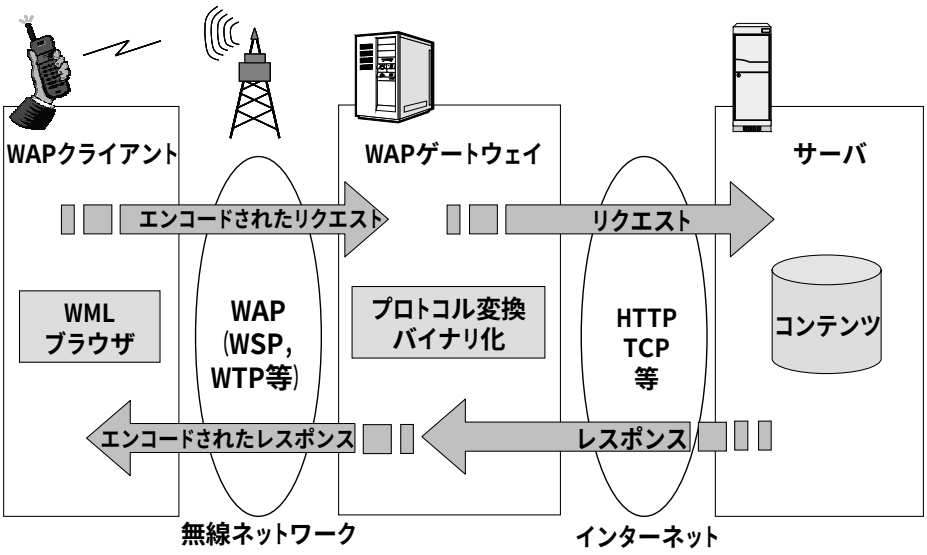


図4.1 WAP1.X アーキテクチャ

WAP プロトコルは，WDP（Wireless Datagram Protocol）[64]，WTLS（Wireless Transport Layer Security）[65]，WTP（Wireless Transaction Protocol）[66]，WSP（Wireless Session Protocol）[67]，WAE（Wireless Application Environment）[68]から構成される（図4.2）．

WDP は，ベアラアダプテーション機能を提供し，下位の移動通信網の違いによるプロトコル間インタフェースの違いを吸収する機能を持つ．下位のワイヤレスネットワークに IP が使われている場合には UDP がそのまま WDP として用いられる．つまり，WDP は UDP と同等の機能を提供する．WLTS は TLS（Transport Layer Security）をベースとし，データ秘匿，相互認証，メッセージ認証等のセキュリティ機能を提供する．WTP は，トランザクション型の通信手段を提供し，Class 0，Class 1，Class 2 の 3 種類のトランザクションタイプを提供する．Class 2 は，パケットの再送を伴う高信頼なデータ転送機能を提供する．WTP は分割再組み立て機能を提供するため，MTU（Maximum Transfer Unit）を超える大きなサイズのデータを転送することが可能である．WTP の動作については，4.4.1 節においても TCP と比較しながら述べる．WSP はセッションの開設と終了や，中断と再開等のセッション管理機能を持つ．WSP は，HTTP と同等機能を提供するが，ヘッダ圧縮やプッシュ機能等の追加機能を持っている．

WAE は，WAP アプリケーション環境の総称であり各種機能を持つ．WAP では，WML（Wireless Markup Language）を記述言語として規定している．図4.3は，WML で記述されたコンテンツとその画面表示例を示している．WML は，XML（Extensible Markup Language）を基にして各種のタグを定義しているが，HTML との互換性はない．さらに，WML にはバイナリエンコーディング（バイナリ圧縮）機能があり，WML コンテンツサイズを削減することで通信データ量を減少させる効果がある．なお，WML のバイナリ圧縮は

WAP ゲートウェイにおいて実行される．また，WAE では，WML Script と呼ばれるスクリプト言語により Java Script と同等の機能の提供が可能である他，携帯電話特有のアプリケーション，例えば，WTA（Wireless Telephony Application）と呼ばれる WWW アクセス中の画面から音声通話の発呼を行う機能などを提供可能である．

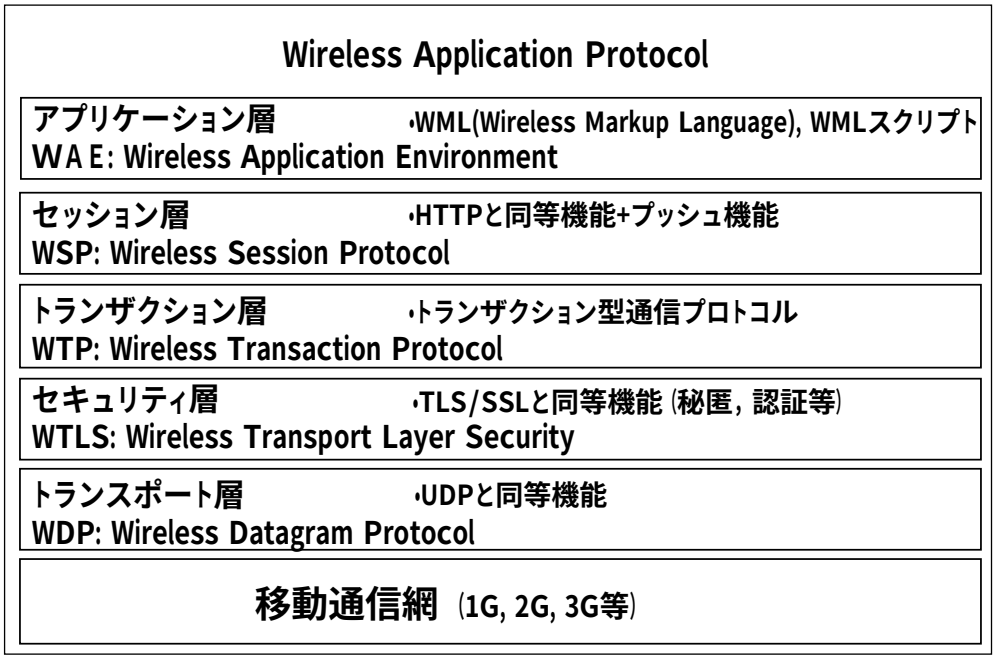


図4.2 WAP プロトコル階層構造

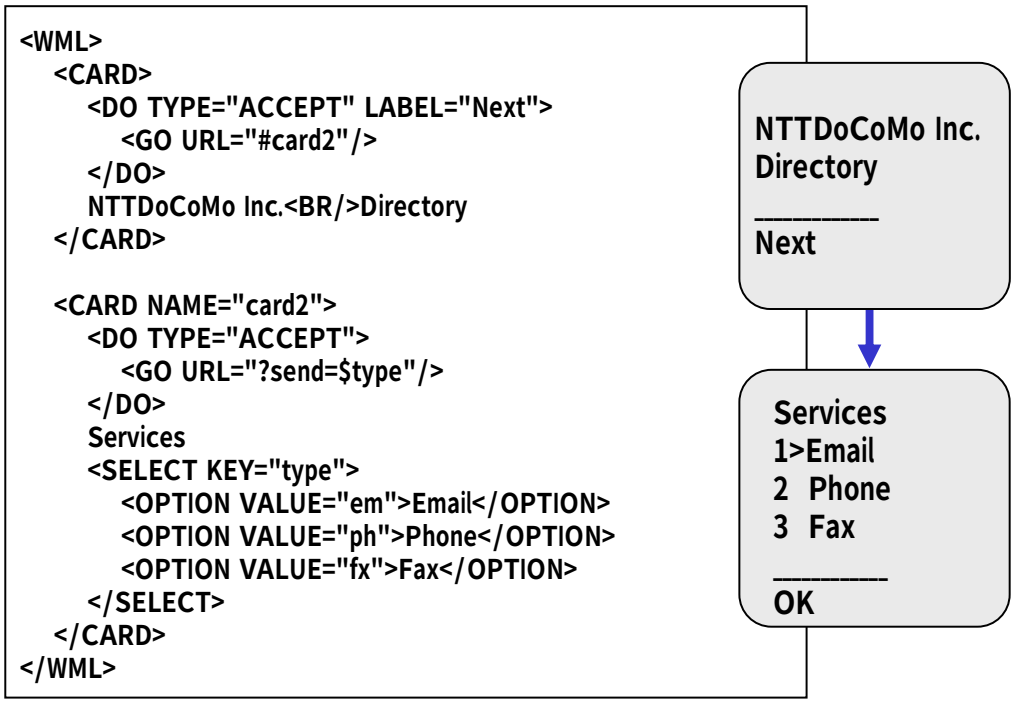


図4.3 WML コンテンツと画面表示例

さて，WAP バージョン 1.0（WAP1.0）が 1998 年に提案されて以来，WAP には幾つかの拡張が施されている．WAP バージョン 1.1（WAP1.1）では，WAP1.0 からプッシュ等の新機能が追加された．WAP1.2.1 では，WTP Class 2 の拡張を行うことで送信可能なデータ量の制限を取り除く等の拡張を行った．しかし，これら WAP1.X の基本的な機能は WAP1.0 と同等である．なお，後述するように WAP バージョン 2.0（WAP2.0）では大幅な変更が行われるが，以下では，特に明示しない限り WAP のバージョンは 1.X であるとする．

4.2. WAP テストベッド

WAP の性能を評価した関連研究として，文献[69]が挙げられる．この文献では，WAP プロトコルの実装システム上で WTP Class 2 の性能を評価し，WAP 仕様におけるいくつかの矛盾点等を指摘している．しかし，移動通信網上での WTP の評価は行っておらず，移動通信網上の WAP プロトコルの性能を明確にするという目的が達成されていない．また，この文献では第二世代移動通信網を対象に評価しており，第三世代移動通信網を対象とした評価は行っていない．

以上を踏まえ本節では，第三世代移動通信網を対象とした WAP の性能評価を行うために作成した WAP テストベッドについて述べる．本システムは W-CDMA シミュレータと，WAP1.1 に基づく WAP クライアントおよび WAP ゲートウェイで構成される．なお，前述のように WAP1.X には WAP1.1 以外のバージョンも存在するが，基本機能についてはいずれのバージョンも同等である．従って，本性能評価実験は基本機能にのみ依存しており，これらのバージョン間の違いは無いものと考えられる．

さて，実験で用いた W-CDMA シミュレータはハードウェアで作成しており，ネットワーク速度，エラー率，RLC（Radio Link Control）[70]の再送回数などの様々なパラメタを設定することで，W-CDMA の移動通信網の擬似環境を提供することが可能である．表4.1は，評価実験のために W-CDMA シミュレータで設定した主要な各種パラメタの要件を示す．エラー率は，W-CDMA を用いた商用サービスにおける典型的な値を示しており，フェージング等の無線特有の環境を再現することが出来る．なお，W-CDMA では，1 から 12 までの RLC フレームが PDU（Protocol Data Unit）を構成し，一つの FEC（Forward Error Correction）フレームを構成しており，表4.1のエラー率は FEC フレーム単位での割合を示している．

表4.1 W-CDMA シミュレータで設定した主要なパラメタ

パラメタ	値
下り通信速度	384Kbps，64Kbps
上り通信速度	64Kbps
レイヤ 2 プロトコル	RLC Protocol
ベアラ MTU	1500 バイト
エラー率	5%（FEC フレーム単位）

図4.4に WAP テストベッドの概観を示す．以下にそれぞれの装置の概要を示す．

- WAP クライアント

Windows98 を実装した PC 上に C++言語を用いて WAP クライアントを実装した．この WAP クライアントは，WML ブラウザや，WAP プロトコル等を実装している．WML ブラウザは携帯端末をエミュレート可能で，WML コンテンツの表示が可能である．

- WAP ゲートウェイ

Solaris2.6 上に C 言語を用いて WAP ゲートウェイを実装した．この WAP ゲートウェイは，WAP プロトコル，インターネットプロトコル，ゲートウェイアプリケーション等の各種モジュールを備えている．ゲートウェイアプリケーションモジュールは，WML コンテンツの構文解析と，そのバイナリ変換を行い，バイナリ化コンテンツを WAP クライアントに提供することが可能である．

- サーバ

Linux 上に，WWW サーバとして Apache1.3.9 を用意した．本サーバは，CGI（Common Gateway Interface）機能を備えており，ダイナミックな WML コンテンツを作成することが出来る．

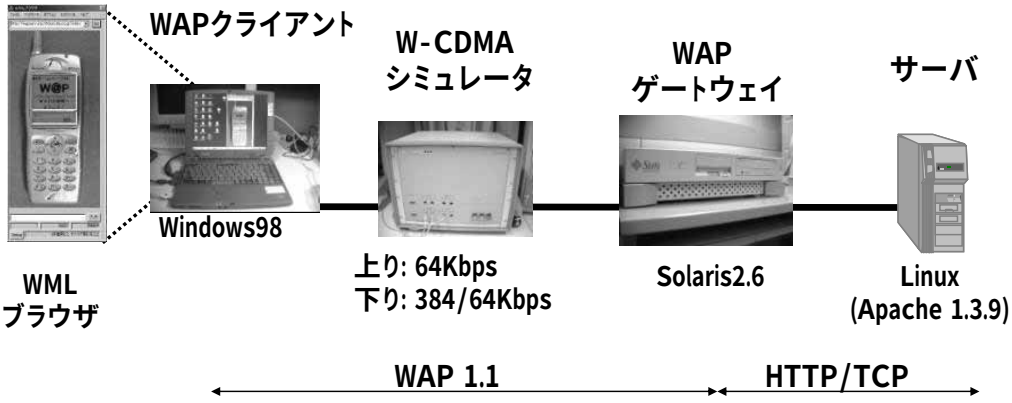


図4.4 WAP テストベッドの構成

表4.2は，WAP テストベッドに実装されたアプリケーションを示す．WSP GET と WSP POST メソッドは WWW ブラウジングに用いられる．プッシュアプリケーションについては，WAP ゲートウェイがプッシュサーバとなり，確認型プッシュメソッドもしくは非確認型プッシュメソッドを用いて WAP クライアントにコンテンツをプッシュすることが可能である．さらに WSP の POST やプッシュメソッドを応用し CGI を用いて電子メールが送受信出来るアプリケーションを実装している．

表4.2 WAP テストベッドに実装したアプリケーション

アプリケーション	データ	利用した WSP 機能
ブラウジング	WML	GET メソッド（受信時） POST メソッド（送信時）
プッシュ	GIF，テキスト	確認型プッシュメソッド 非確認型プッシュメソッド
電子メール	テキスト	POST メソッド（送信時） 確認型プッシュメソッド（受信時） 非確認型プッシュメソッド（受信時）

4.3. WAP バイナリエンコーディングの評価

WAP においてボトルネックとなる負荷が高い処理として，WAP で定義された二種類のバイナリエンコーディングが挙げられる．一つは，WSP ヘッダのヘッダ圧縮であり，もう一つは WML のバイナリエンコーディングである．本節では，これらの機能や性能について詳細に評価し, これらのエンコーディングを W-CDMA 等の第三世代移動通信網へ適用する可否について検討する．

4.3.1. WML バイナリエンコーディングの評価

WAP ゲートウェイは，WML コンテンツの XML 構文解析の後，WML タグや制御コードのバイナリエンコーディングを行う. WML のバイナリエンコーディングの効果はコンテンツごとに異なるため，本実験では図4.5に示す典型的な WML コンテンツをその評価に使用した．

使用したコンテンツは“ wml ”, “ card ”, “ p ”等の必須 WML タグのほかにテキストデータと改行を示す“ br ”タグ等を含んでいる．このようなコンテンツのサイズを 500 バイト，1000 バイト，1400 バイト，20K バイト，100K バイト，360K バイトに変化させ，以下の点について評価した結果を図4.6に示す．

- WML バイナリエンコーディングと gzip の圧縮率の比較
- WML バイナリエンコーディングに必要な処理時間とその時間中に含まれる XML 構文解析に要する時間

```
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.1//EN"
    "http://www.wapforum.org/DTD/wml_1.1.xml">
<wml>
 <card id="card2" ontimer="./auto500-2.wml#card1">
 <timer value="50"/>
  <p mode="wrap">
   *Test of 1400 Octet Contents*<br/>
   ***deck1***<br/>
   WAP is a protocol that is designed for wireless environment.<br/>
   WAP is a protocol to access to the Internet from cellular phones, PDAs and so
     on. <br/>
   (残りは省略) </p>
 </card>
</wml>
```

図4.5 実験に用いた WML コンテンツの例

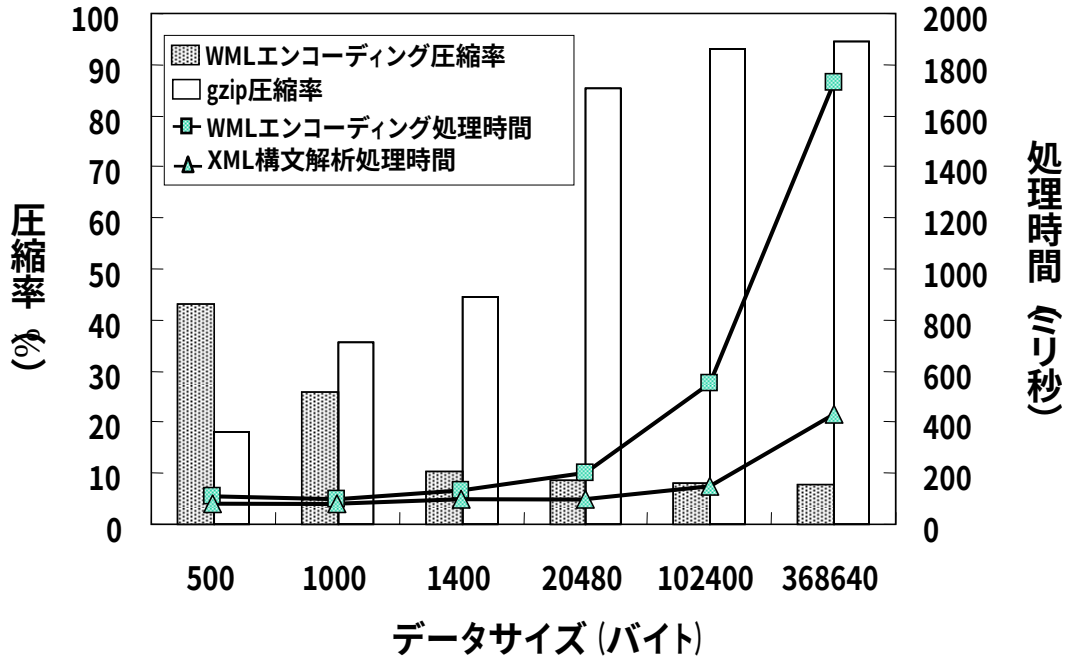


図4.6 WML バイナリエンコーディングの圧縮率と処理時間の比較

図4.6の結果から，WML バイナリエンコーディングの圧縮率は，コンテンツサイズが小さい場合に特に有効であることが分かった．その理由として WML が使用する XML の DOCTYPE 宣言部の圧縮率が要因となっていることが考えられる．DOCTYPE 宣言部は，図4.5の最初の 3 行の部分であり，この部分は全ての WML コンテンツに含まれる．DOCTYPE 宣言部は，バイナリエンコーディングにより，115 バイトから 3 バイトに圧縮されるなどその圧縮率が非常に高いため，コンテンツサイズが小さい場合には DOCTYPE 宣言部の圧縮率が全体のコンテンツ圧縮率を高めることとなった．逆にコンテンツサイズが大きい場合には，コンテンツ全体に占めるタグの比率が低くなることから，WML バイナリエンコーディングにおける全体のコンテンツ圧縮率を下げたのに対し，データ部分まで圧縮を行う gzip は高い圧縮率を達成することとなった．

WML バイナリエンコーディングの処理時間については，WML エンコーディングや XML の構文解析のいずれもコンテンツサイズに応じて増加することが分かった（例：360K バイトのコンテンツの場合に 1730 ミリ秒）．なお，500 バイトのコンテンツの場合，処理時間全体のうち 72.7%が XML の構文解析に必要な時間であり，残りは WML エンコーディングに実際に要する時間であった．360K バイトのコンテンツの場合には 24.9%が全体の WML エンコーディングに必要な時間のうち XML の構文解析に必要な時間であった．従って，コンテンツサイズが大きくなるに従い，WML コンテンツの実際の圧縮時間よりもその構文解析に要する時間が長くなるという特徴があることが分かった．

以上の結果を利用し，以下では WML バイナリエンコーディングの効果を考察する．1400 バイトの WML コンテンツは 1117 バイトに圧縮されるが，その減少した 283 バイト分の転送遅延は 384Kbps の通信速度の場合には 6 ミリ秒であり，9600bps の場合には 236 ミリ秒を要する．ここで，1400 バイトの WML コンテンツの圧縮には図4.6の実験結果から 130 ミリ秒の処理時間を要するため，無線ネットワークが高速の場合には WML エンコーディングを行わずにそのままデータを転送したほうがトータルの遅延は小さい．つまり WML バイナリエンコーディングは第二世代移動通信網以前の低速な移動通信網の場合には処理時間に見合う転送遅延の削減が期待できるのに対し，W-CDMA 等の第三世代移動通信網以後の高速な移動通信網では WML エンコーディングを行わずにそのままデータを転送した方が全体の遅延が小さくなることが分かる．

バイナリエンコーディングの処理時間はWMLがベースとしているXMLの構文解析の処理時間が大きく影響することから，データサイズが大きな場合においても同様な結論が導かれる．第三世代移動通信網以降においては，携帯端末に提供されるデータはその高速性を活かしてリッチ化され，そのサイズはますます大きくなる傾向にある．そのような状況下において，WML バイナリエンコーディングの必要性は低いと言える．

今後，CPU の処理能力の向上等により WML バイナリエンコーディングに要する時間が減少することも考えられるが，これらの技術的な進歩に伴い，ネットワークの通信速度も向上すると考えられ，データの転送遅延時間も同様に減少することが期待される．従って，本節での評価と同様に, WML バイナリエンコーディングの効果は今後とも飛躍的に改善されないと考えられる．

4.3.2. WSP ヘッダ圧縮の評価

WSP が提供するバイナリエンコーディングとして WSP のヘッダ圧縮がある．この機能は，HTTP ではテキスト表記される HTTP ヘッダに相当する WSP ヘッダをバイナリ化することによりデータ量を少なくするものである．WAP テストベッドにおいて WSP ヘッダの圧縮を行ったところ 10 ミリ秒の圧縮時間を要し，平均 185 バイトの WSP ヘッダを 50 バイトに圧縮する効果があることが観測された．

この結果から，WSP ヘッダ圧縮についても無線ネットワークの速度が高速の場合には効果的ではないことが分かる．例えば，ネットワーク速度が 384Kbps である場合には WSP のヘッダ圧縮により減少した 135 バイトのデータの転送遅延は 3 ミリ秒である．明らかに WSP ヘッダの圧縮による処理時間よりは，圧縮を行わない WSP ヘッダそのものを送信したほうが全体的な遅延は小さい．逆にネットワーク速度が 9600bps の場合は，135 バイトのデータの転送遅延は 112 ミリ秒であるため, これら低速のネットワークでは WSP ヘッダ圧縮は有効であったことが分かる. 以上のことから WSP ヘッダ圧縮についても第二世代移動通信網以前の低速な無線ネットワークには適するが, W-CDMA 等の第三世代移動通信網以後の高速な無線ネットワークには適していないことが分かった．

4.4. WAP とインターネットプロトコルの通信性能の比較

本節では，WAP とインターネットの通信プロトコル全体の通信性能を比較するために，その性能に大きな影響力を持つ WTP と TCP を中心にその通信性能を比較する．

4.4.1. WAP と HTTP/TCP の機能比較

TCP は信頼性のあるデータ転送を行うためのコネクション型のトランスポート層プロトコルを提供するのに対し，WAP は，トランザクション型のメッセージ転送プロトコルである WTP を使用することで TCP と同様な信頼性を確保することが可能である．TCP コネクションの開設には 3 ウェイハンドシェイクが必要であるが，WAP では WSP の Connect メソッドと Connect Reply メソッドを使用することでセッション開設を行う. WTP はオプションとして非同期トランザクション機能をサポートしている．非同期トランザクション機能とは，WTP イニシエータ（WTP データの送信元であり通常は WAP クライアント）が連続したメッセージを確認応答無しに一度にまとめて送る機能であり，これにより WAP のトータルの通信時間を短縮することが可能となる．

図4.7では，それぞれのプロトコルの通信シーケンスの例を示す．本例では，クライアントが単一パケットに収まるデータを受信した場合の例を示している．それぞれのプロトコルはいずれも以下の 3 つの大きなステップを踏まえ通信を行っている．

- WSP セッションもしくは TCP コネクションの接続手順
- データの取得手順
- WSP セッションもしくは TCP コネクションの切断手順

なお，HTTP ではパーシステントコネクション機能[13]が提供されており，これを利用することで TCP コネクションを維持したまま，開放および開設の手続きをすることなく次のデータ取得が可能である．WAP においても WSP のセッションで同様な機能を提供する．

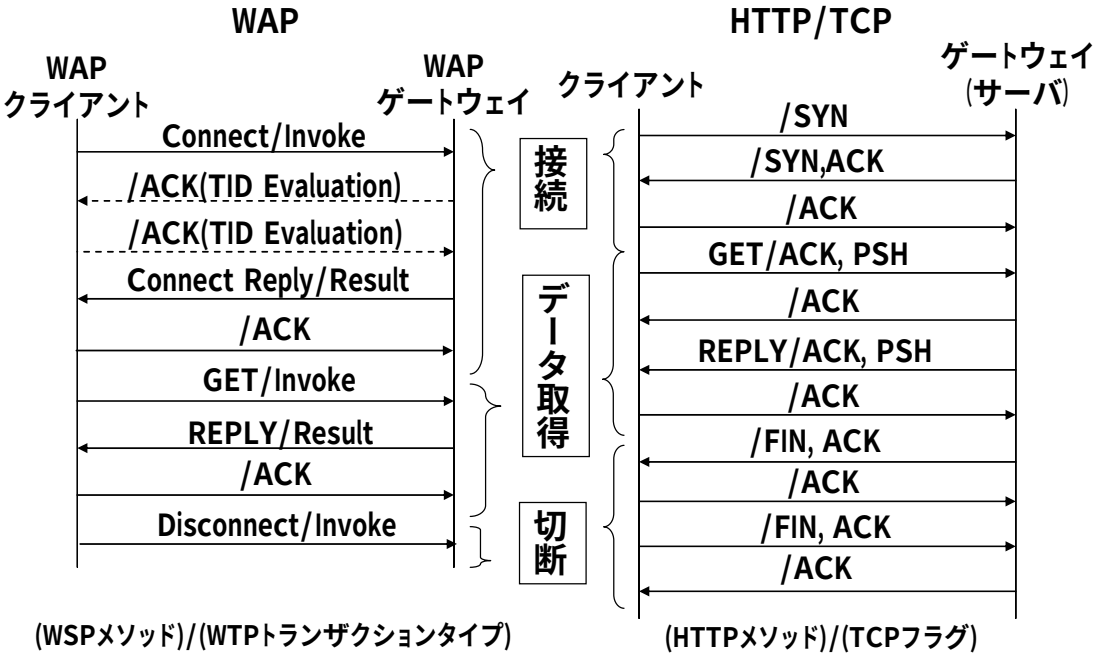


図4.7 WAP と HTTP/TCP の通信シーケンスの比較

4.4.2. 性能評価パラメタ

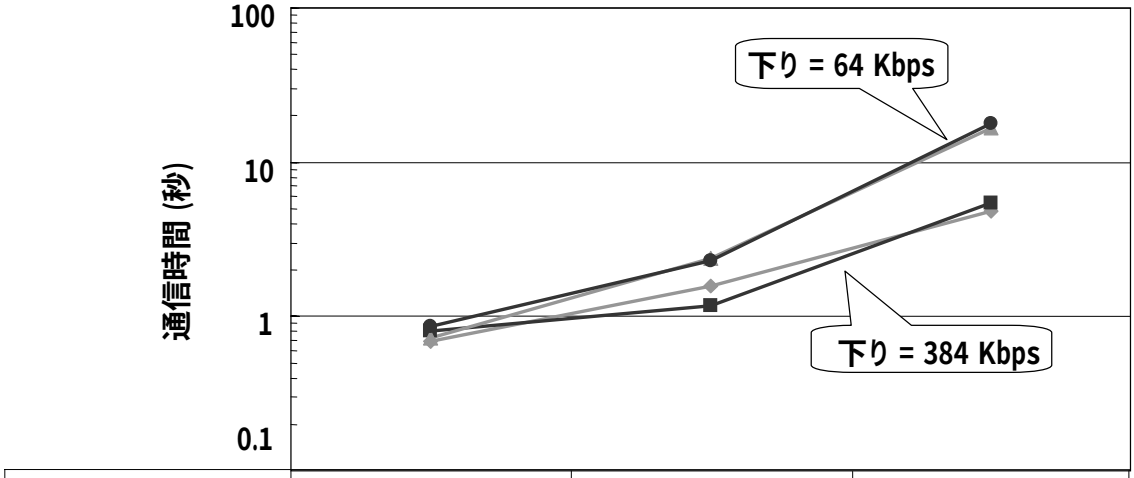
WAP と HTTP/TCP の性能評価を行うにあたり, 以下では 1K バイト, 10K バイト, 100K バイトの 3 種類のサイズのコンテンツを準備した．ここで，1K バイトのコンテンツは小さい画像やテキストデータを想定しており，MTU サイズが 1500 バイトである場合には 1 パケットに収まるデータ量である．携帯端末向けのコンテンツでは，このようにコンテンツサイズをなるべく小さくして通信時間が短くなるように工夫されることが一般的である．例えば，大きいサイズのテキストコンテンツを携帯端末に提供する場合は，Web ページ中にリンクを設けることで，ユーザにこのコンテンツを閲覧するか否かの選択を促す傾向がある．また，100K バイトのコンテンツは MPEG 等のファイル型の動画像や Java ゲームのような比較的容量の大きいデータを想定している．第三世代移動通信網の普及によって，このようなサイズのコンテンツがますます増加する傾向にあると考えられる．なお，WAP の場合に，転送するデータサイズが 1 MTU サイズを超える場合には WTP の分割再組み立て機能（SAR：Segmentation and Reassembly）が使用される．

なお，本節における性能測定では，WTP 仕様[66]により推奨された各種パラメタを採用している．また，W-CDMA シミュレータで使用するパラメタについては4.2節に述べたものと同じである．

TCP に関する条件としては，無線ネットワーク向け最適化について述べている文献[71]に基づき，本研究では，選択再送信（SACK：Selective Acknowledgement）[72]と，TCP 初期ウインドウサイズの増加[73]，最適なウインドウサイズの選択を採用した．最適なウインドウサイズの選択とは，エンドトゥエンドの帯域遅延積（BDP：Bandwidth Delay Product）に基づき最適なウインドウサイズの見積もりを行う方法である．最適な広告ウインドウ（rwnd）の選択は転送パフォーマンス全体を左右する重要なパラメタである．TCP 仕様[1]では，TCP の広告ウインドウを 64K バイトまでに制限しているため，もしも帯域遅延積が 64K バイトを超える場合には，ウィンドウスケールオプション[74]を使用することにより 64K バイトの制限を取り払うことが可能となる．なお，多くのオペレーティングシステムにおける TCP の広告ウインドウサイズはデフォルトで 16K バイトに設定されているため，帯域遅延積が 64K バイトよりも小さい場合において無線ネットワークを利用する場合にもそのパラメタを変更することで適切な性能を得ることが可能である．例えば，W-CDMA では最大 384Kbps のネットワーク速度を提供し，そのエンドトゥエンドのラウンドトリップタイム（RTT）は約 500 ミリ秒から 1 秒程度になることもあるため[71]，W-CDMA ネットワークの帯域遅延積はインターネット等と比較しても非常に大きい値になる．従って，受信広告ウインドウサイズがこの W-CDMA の特性に合ったウインドウサイズを持たない場合にはネットワークの通信性能に大きな影響がある．本実験における初期の評価では，広告ウインドウサイズを 32K バイトに設定することにより W-CDMA 上で 667 ミリ秒までの RTT に対応することが可能であることが分かっており，この値がメモリコストと得られるパフォーマンスの間の最適なサイズであると判断した．従って，4.4.3節以降の評価ではこの値を使用することとする．また，WTP についても最大グループサイズを任意の値に設定することが可能であり，TCP と同じ条件にするために 32K バイトの最大グループサイズを使用する．

4.4.3. WAP1.1 と HTTP/TCP の性能比較

まず，WAP クライアントからデータ取得のための要求（WTP Invoke）を送信してから WAP ゲートウェイからデータの応答があるまで（WTP Reply）の応答時間を測定した結果と TCP についても同様に応答時間を測定した結果を図4.8に示す．なお，HTTP のパーシステントコネクション機能や WSP の継続したセッションを使用してデータ転送をすることを考慮したため，コネクション開設と開放に要する応答時間は WAP1.1 と HTTP/TCP のいずれの測定結果にも含まれていない．



	1K	10K	100K
HTTP/TCP 384Kbps	0.691	1.57	4.79
WAP1.1 384Kbps	0.809	1.17	5.40
HTTP/TCP 64Kbps	0.719	2.36	16.8
WAP1.1 64Kbps	0.863	2.32	17.8

データサイズ (バイト)

図4.8 WAP1.1 と HTTP/TCP の応答時間の比較

図4.8から, WAP1.1 と HTTP/TCP のいずれも W-CDMA 上では同様な応答時間が得られることが分かった．しかし，サイズの大きいデータの場合には HTTP/TCP の応答時間が WAP1.1 の応答時間よりも短いことが分かった．また，その傾向は測定したベアラ速度の差異（384Kbps，64Kbps）の違いによっても変わらないことが分かった．しかし，それぞれのデータサイズにおける通信時間の差異に着目すると，各プロトコルの性質を明らかにすることが出来る．以下では，それぞれのコンテンツサイズにおけるそれぞれのプロトコルの違いにより得られる応答時間への差異について説明する．

- 1K バイトデータ：HTTP/TCP が WAP1.1 よりも優れる
  1K バイトのデータの場合には HTTP/TCP が WAP よりも通信時間が 0.118 秒短い（ベアラ速度 384Kbps の場合）．1K バイトのデータの場合には 1 パケットに収まるデータ量であり応答時間は元々短いが，WAP の場合には WAP ゲートウェイにおける WAP からインターネットのプロトコルへの変換の処理時間が影響している．しかし，元々データサイズが小さくその応答時間も短いため，1K バイトデータの応答時間の差異がユーザへのサービス性に影響するまでの深刻な差にはならない．

- 10K バイトデータ：WAP1.1 が HTTP/TCP よりも優れる
  10K バイトのデータの場合には WAP が HTTP/TCP よりも応答時間が 0.40 秒短い（ベアラ速度 384Kbps の場合）．この応答時間の性能の際は WAP で使用される WTP と TCP フロー制御アルゴリズムの差異が大きく影響している．WTP では，固定サイズのウインドウ制御方式を採用しており，ここで採用した 32K バイトのウインドウサイズにより 10K バイトのデータ全てを一度に送信することが可能である．TCP の場合にはスロースタートアルゴリズムにより，徐々にウインドウサイズを大きくするために，10K バイトのデータの送信の場合には TCP はその無線ネットワークの帯域幅を十分には使い切れないうちに通信が終了していることが分かる．

- 100K バイトデータ：HTTP/TCP が WAP1.1 よりも優れる

100K バイトのデータの場合には HTTP/TCP が WAP よりも通信時間が 0.61 秒短い（ベアラ速度 384Kbps の場合）．WAP の場合には，図4.9左に示すように，データサイズが 100K バイトになるとウインドウサイズである 32K バイトごと（ベアラ MTU が 1500 バイトの今回の例ではパケット 21 個分に相当）にデータの送信を停止し，その確認応答が届くまでデータの送信を止める．このため，全体の通信時間に影響が出る．特に無線ネットワークにおいてはインターネットと比較して高遅延であるためにこのような待ち時間はネットワーク全体の性能に影響する．これに対して TCP では，確認応答がピギーバックされるため，データの送受信と共に確認応答を行っている．従って，図4.9右に示すように，一度スロースタートアルゴルゴリズムによりウインドウサイズがネットワーク帯域幅に対して十分に拡大された後には，ネットワークの帯域幅が十分に使用されるという特徴があることが分かる．

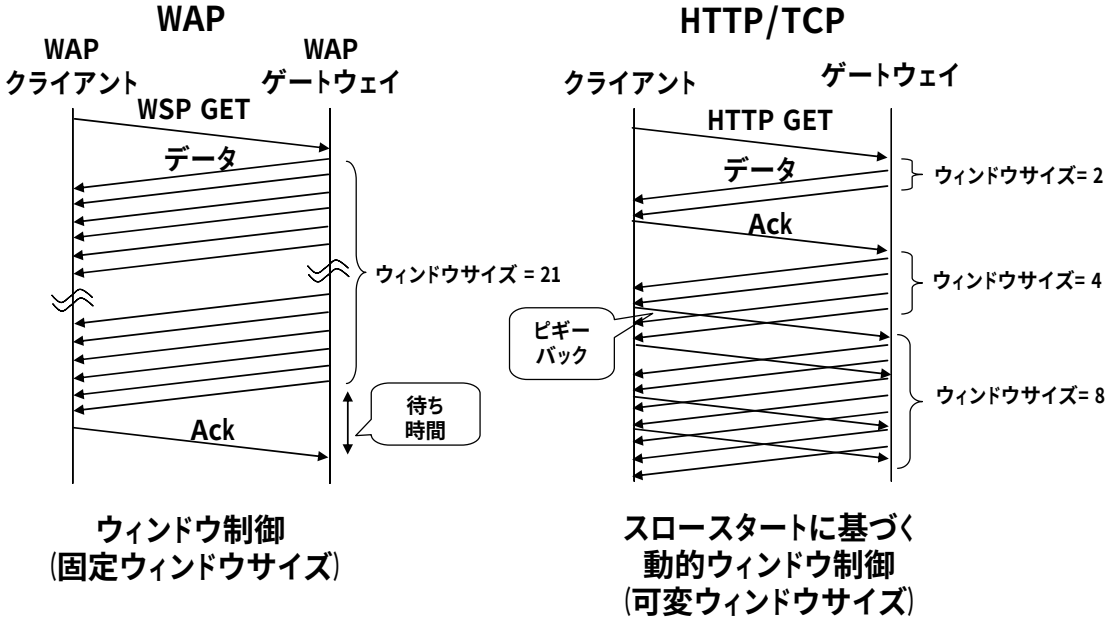


図4.9 データサイズが大きい場合の WAP と HTTP/TCP の比較

以上の WAP1.1 と HTTP/TCP の性能比較で示したように，TCP を無線ネットワーク向けに最適することで WAP1.1 以上の性能を得られるケースがあることが分かった. WAP1.1 は，第二世代移動通信網までの低速の無線ネットワークを想定して作成されたため，W-CDMA 等の第三世代移動通信網のような高速の移動通信網においては必ずしも適切とは言えず，さらに，インターネットで用いられている HTTP や TCP をそのまま第三世代移動通信網に適用しても性能に問題が無いことが確かめられた．特に TCP は，ネットワークの帯域幅に合わせてそのウインドウサイズを調整することにより柔軟にネットワークの特徴に対処出来ることから，高速な第三世代移動通信網には特に適しているといえる．さらに TCP には，ECN[54]等の各種最適化アルゴリズムが提案されている．これらの各種技術を組み合わせることによりさらに性能向上を図ることが可能となる．

4.5. W-CDMA 向け通信プロトコルの提案

前節の評価から，インターネットで用いられているプロトコルである HTTP/TCP を使用しても, 第三世代移動通信網以降の高速なネットワークにおいては WAP 以上の性能を得られるケースがあることが分かった．特に TCP は，ネットワークの帯域幅に合わせてそのウインドウサイズを調整することにより柔軟にネットワークの特徴に対処できることから，高速な第三世代移動通信網において適しているといえる. 従って, 本章の結論として, HTTP や TCP 等のインターネットで用いられているプロトコルを第三世代移動通信網以降の高速なネットワークで採用することを提案する（図4.10）．これにより，トランスポート層のセキュリティに TLS（Transport Layer Security）や SSL（Secure Socket Layer）を使うことが可能となり，WAP では不可能であったトランスポート層でのエンドトゥエンドセキュリティの実現も容易になるという利点がある．

また，3G 以降で提供するコンテンツの記述言語として無線向けに設計された WML ではなく，インターネットで一般的に用いられる HTML を採用することを提案する．その理由として, WML のバイナリエンコーディングの効果は第三世代移動通信網以降の高速なネットワークにおいては期待できないこと，および，WML は HTML と互換性が無くその普及には問題があることが挙げられる. また, HTML を採用した場合, これに合わせて XHTML（Extensible HTML）[75]を採用することが容易となり，将来にわたり充実したコンテンツの提供が可能となることが期待される．以上の議論に基づき，本章で提案する通信プロトコルとそのネットワークアーキテクチャを図4.10に示す. 本アーキテクチャは, 無線区間で利用する Wireless TCP（W-TCP）[71]とインターネットで利用する TCP を変換するためのゲートウェイを設置し，前述した各種通信プロトコルや記述言語を採用している．

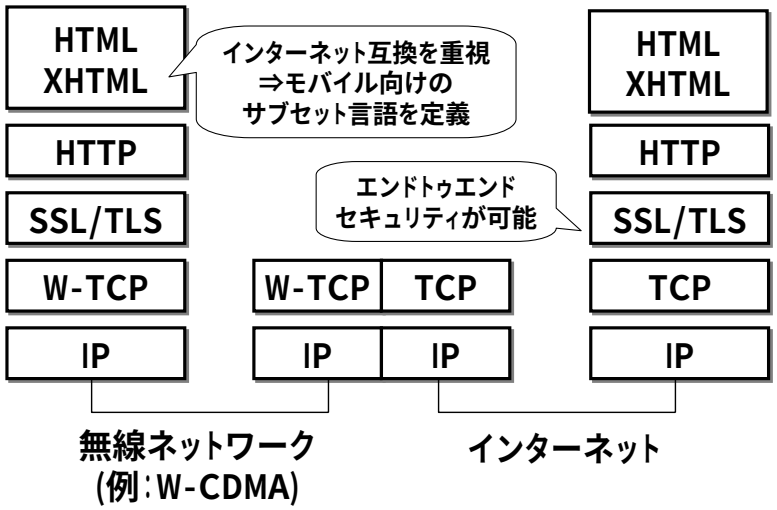


図4.10 提案する第三世代移動通信網向け通信プロトコルとアーキテクチャ

4.6. 本章のまとめ

本章では, 第三世代移動通信網向けに適する通信プロトコルを明らかにするために, WAP と HTTP/TCP を実装したテストベッドを実装し，W-CDMA のベアラシミュレータ上でこれらを実際に動作させることでその性能評価を行った．本章で得られた結論としては以下が挙げられる．

- 第三世代移動通信網等の高速のネットワークにおいては，HTTP/TCP を用いることにより WAP と比較しても十分な性能が得られる．特にデータサイズが大きい場合には HTTP/TCP の通信時間が WAP の性能を上回る．

- W-CDMA 等の第三世代移動通信網上で利用されるコンテンツは，第二世代移動通信網までに利用されたコンテンツよりもそのサイズが増加しており，そのような状況においては HTTP や無線向けに最適化された TCP を用いることでより良い性能が得られる．

- WML や WSP のバイナリエンコーディングは第一世代移動通信網や第二世代移動通信網においては効果が得られるが，W-CDMA 等の第三世代移動通信網等の高速のネットワークにおいてはその効果が得られないばかりか，バイナリエンコーディングの処理が遅延となってオーバヘッドを増加させる要因になる．

- W-CDMA 等の第三世代移動通信網以降の高速なネットワークにおいては，HTTP/TCP 等のインターネットで用いられているプロトコルを用いることによりトランスポート層でのエンドトゥエンドセキュリティが実現可能になるなど，WAP で未提供であった機能を提供することが可能である．また，HTML や XHTML のようにインターネットで用いられている記述言語を携帯電話においてもサポートすることにより充実したコンテンツをユーザに提供することが可能である．

- 以上の考察結果に基づき，第三世代移動通信網向け通信プロトコルとアーキテクチャを提案した．

なお，著者らは図4.10で示した第三世代移動通信網向け通信プロトコルとアーキテクチャを WAP フォーラムに対して提案した．その結果，同フォーラムでは 2001 年に本提案に基づいた WAP2.0 の仕様化を行っている[76]．この WAP2.0 では，通信プロトコルに HTTP と Wireless Profiled TCP[77]を採用し，記述言語として XHTML のモバイル向けサブセット（XHTML Mobile Profile[78]）を定義している．現在，WAP2.0 に基づいた携帯電話やサーバ製品は多数出荷されており，例えば，日本における提案方式を実装した端末の利用者数は約 4000 万台に登っており，本章の研究は高い成果を修めたと言える．

4.6.1. 今後の研究課題

2001 年に最初に第三世代移動通信網が商用化された後，利用可能なネットワークがさらに多様化している．例えば，無線 LAN の利用が近年になって爆発的に増加し，無線 LAN の通信機能を搭載した携帯電話が発売されるなど，その利用形態も多様化している．今後利用が進むと予想される他の通信ネットワークとして，WiMAX，Super3G，All IP Network，第四世代移動通信網など様々な無線を利用した通信ネットワークが登場することが予想される[79].

今後の研究課題として，これら新しい通信ネットワークにおける TCP の性能評価が挙げられる．この性能評価結果に基づき TCP の無線向け拡張機能を提案することも今後の研究課題の一つである．

第5章 マルチキャスト用受信者認証グループ鍵配布プロトコルの提案とその評価

放送型データ配信サービスでは，送信者から発せられるリアルタイム性が要求されるデータ（音声や動画像など）を特定のグループに属する受信者（メンバ）に対して高速かつ低遅延に伝送することが必要となる．これらの通信形態では，一対多の伝送が行われるが，これらのサービスの実現にユニキャスト通信を用いることは，通信コストや帯域利用率の面で問題がある．このことは，特にネットワークが大規模になりメンバ数が増加した場合により顕著になる．

この問題を解決するため，送信データの複製を送信者ではなくルータにおいて行い，同一データをメンバに効率良く配信するマルチキャスト通信が注目されている．特に，無線 LAN や移動通信網では，資源が限られた無線を通信に利用するために有線で構成されたネットワークと比べて通信コストが高く，共通チャネルの利用により多数のメンバに対してデータの同報配信が可能なマルチキャスト技術が重要視されている．また，第三世代移動通信網向けの各種仕様を作成する標準化団体 3GPP では，移動通信網上で放送型サービスを実現するための MBMS[50]の仕様を策定するなど実際にサービス開始に向けた動きが高まっている．

しかし，IP マルチキャストは，一対多のデータ配信を実現することから，ユニキャストで用いているセキュリティ方式がそのまま適用できないという問題点があり，2.5節で述べたように解決するべきセキュリティ上の課題が存在する．例えば，共通チャネルでマルチキャストを行う場合，ここでやりとりされるデータをグループに属しない第三者から秘匿する必要があるが，そのために使用する暗号化鍵（グループ鍵）をグループメンバで共有するため，IETF は，2005 年にグループ鍵管理アーキテクチャ（General Key Management Architecture）[80]を規定している．その他にも，受信者認証や送信者認証，権限認証などといった提供すべきセキュリティ機能は多数存在している．

そこで本章では，マルチキャマルチキャストを用いた放送型のデータ配信サービスを対象とした，受信者認証グループ鍵配布プロトコル AKDP（Authentication and Group Key Delivery Protocol）を提案する．また提案方式の評価によりその有効性について考察する．

5.1. 関連研究と解決すべき課題

本節では，最初にマルチキャストセキュリティの課題をまとめ，マルチキャストセキュリティの関連研究を整理した後，本研究で取り組むべき課題を明らかにする．

5.1.1. マルチキャストにおけるセキュリティの課題

マルチキャストにおけるセキュリティの課題は論文[52]にまとめられており，図5.1を用いてその概要を説明する．

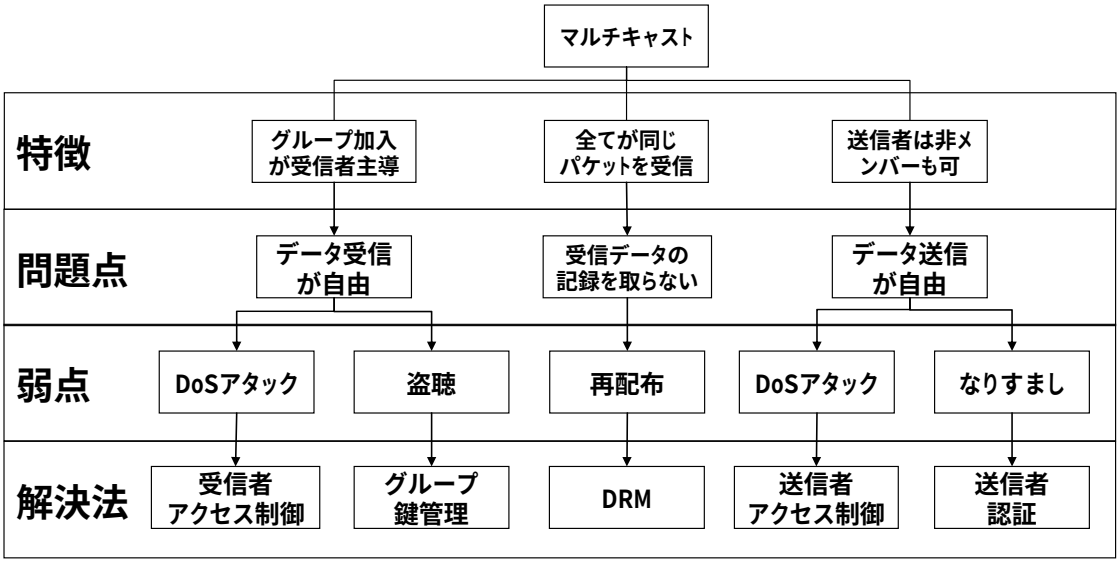


図5.1 マルチキャストセキュリティの課題と解決法

マルチキャストは，受信者の希望によりグループ加入と離脱が自由に行えるという特徴がある．また，データの受信を送信者には伝えない匿名モデルを採用している．以上のことから，匿名モデルの特徴に起因する数々の問題点がある．例えば，IGMP では，受信者を認証する機能がないため，悪意を持つ第三者によるグループへの不正な加入要求を防止する手段を持たない．そのため，偽りの加入要求によりマルチキャスト配信経路が不正構築されるマルチキャスト固有の DoS 攻撃が可能となる．なお，悪意のあるユーザによるグループへの不正な IGMP 離脱要求についても，サブネットワークの範囲に限り帯域やルータリソースの浪費につながるが，同じサブネットワークに他のメンバが存在する場合には，マルチキャストデータの配信を停止することにはならないためその影響はサブネットワーク内の帯域やリソースの浪費に限定される．しかし，IGMP 離脱要求についても IGMP 加入要求と同様にその DoS 攻撃に対する対処が重要となる．このマルチキャスト DoS の対処方法として，受信者認証を実行することによりアクセスルータにおいて不正な IGMP 加入要求を防止するための制御，つまりアクセス制御が必要である．アクセス制御は，IGMP 加入要求や離脱要求が正当な権限のある受信者より送信されたか否かを確認することで，不必要なマルチキャスト配信データの中継を防止することを目的とする．

また，IP マルチキャストでは，サブネットワーク上にマルチキャスト配信データが配信され，同一サブネットワークに存在する他の受信者もデータ受信が可能であることから，本来ではマルチキャスト配信データの配信対象でない受信者においてもデータ受信が可能となる．従って，データの受信権限のない受信者によるデータ盗聴の問題が存在する．しかし，IP マルチキャストでは，IPSec や SSL 等のユニキャストの技術がそのままでは適用不可能であり，IP マルチキャストに適したデータの秘匿と，データ秘匿に必要なグループ鍵（マルチキャストに用いられる暗号化鍵）の管理が必要である．

さらに，マルチキャストでは，複数の受信者が同じ配信データを受信することから，配信済みのデータを一意に特定することが不可能である．また，送信者において，受信者に対する送信済みデータをどの受信者に配信したかを管理していないため，悪意のある受信者によりデータの再配布が行われた場合にその受信者を特定する手段がない．例えば，配

信するデータが音楽の場合など，著作権保護を実現する必要があるデータである場合，受信者によってデータの再配布が行われてしまうと，著作者の権利が保護されない場合があるため問題となる．従って，データの再配布防止等を実現するデジタル著作権管理（DRM：Digital Rights Management）を実現する必要がある．

一方，データの送信者は必ずしもマルチキャストグループのメンバである必要が無いことから，悪意のあるユーザにより不正データが配信される懸念がある．また，送信元 IP アドレスの詐称によるなりすましが容易である．このため，受信者が不正なデータを受信したとしてもそのデータの送信者の特定が困難になり，マルチキャストの特徴を利用したウィルスの大量配信などが問題となる．これに対処するためには，送信者の認証が必要である．さらに，配信データが不正に改ざんされた場合にそれを検出出来るように，メッセージ認証機能（データ完全性検証）が必要である．

5.1.2. マルチキャストセキュリティの関連研究

図5.1に説明したマルチキャストセキュリティの課題を解決するために，これまでに数多くの関連研究が存在する．本節では各項目に分けてその関連研究について説明を行う．

- 受信者アクセス制御

受信者のアクセス制御については，IGMP の拡張方式を採用する文献[81]や，この文献の提案方式を改良した IGAP（Internet Group membership Authentication Protocol）[82]が存在する．IGAP は，IGMP の各メッセージを拡張してマルチキャストデータの受信開始時と終了時に受信者認証を実行することにより，受信者がデータ受信についての正当な権限を有しているか否かの判断を実現しており，受信者アクセス制御が可能となる他，マルチキャストにおける課金を実現出来るとしている．ただし，IGAP は ADSL や光ファイバ等のポイントトゥポイントネットワークでの利用を想定しており，傍受されやすい無線通信の利用を前提とした場合，本方式のデータ秘匿とその実現に必要なグループ鍵管理との連携についての考察が不十分である．

Gothic[83]は，ID ベースのアクセストークンと電子署名を適用する方法を提案している．この方式では，アクセスルータにおいて，受信者が取得済みのアクセストークンを検証することにより受信者認証を実現する．Gothic は，同様な機能を提供する他の提案[84][85]と比較してもスケーラビリティに優れている．さらに，アクセストークン取得時にグループ鍵を同時に取得することによって，受信者認証と共にグループ鍵管理を提供している点も文献[84]や文献[85]と比べて評価出来る．しかし，Gothic は，IGMP の各種メッセージを暗号化するため，受信者とアクセスルータ間に SA（Security Association）の構築と，受信者による各メッセージの暗号化と復号化処理が必要であり，特に携帯電話等の CPU 処理能力に制約がある端末には影響が大きいことが課題である．

- グループ鍵管理

データ秘匿とそのために必要なグループ鍵管理（グループ鍵配信，削除，更新等グループ鍵の扱いに関する各種処理に関することの総称）については，古くからマルチキャストセキュリティ上の最大の課題として認識されており，IETF においても活発に標準化が行われた分野である．例えば，データの盗聴を防止するため，データ秘匿に必要なグループ鍵の階層構造を定義した GKM（Group Key Management）アーキテクチャを策定した[80]（図5.2）．マルチキャスト配信に使われる各種暗号化鍵を階層構造にしてグループ鍵管理を実現する本方法は，衛星デジタルや地上波デジタル放送等のグループ鍵管理にも用いられている技術である[86].

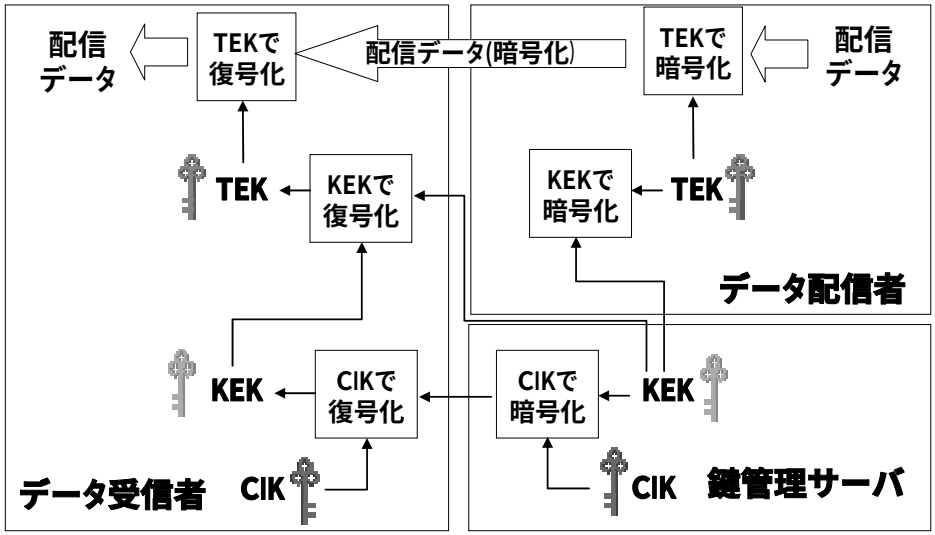


図5.2 グループ鍵管理

IETF のグループ鍵管理では，TEK（Traffic Encryption Key），KEK（Key Encryption Key），CIK（Client Individual Key）と呼ばれる 3 種類の鍵を用いる．TEK は，配信データの秘匿に用いられる鍵であり，KEK により暗号化されて受信者に配信される．KEK は，グループ鍵として受信者で共有される鍵であり，マルチキャストデータが有効な期間有効な鍵である．KEK は，各受信者個別の公開鍵である CIK（Client Individual Key）を用いて暗号化して配信される．なお，CIK には各受信者の公開鍵の他にも各受信者の共通鍵を用いることが可能である．

TEK は，暗号化や復号化の処理の高速性が求められるため，比較的ビット長の短い共通鍵を用い，解読されたときの対策として更新間隔は比較的短くする．KEK は，高速性は求められないものの解読される危険性を低くするためビット長を比較的長くする．なお，KEK の有効期間を定めることにより配信データの有効期限を定めることが可能である．例えば 1 ヶ月有効な KEK を用意することで 1 ヶ月間データの復号化が可能なデータ配信を行うことが可能である．また，配信期間と同じ有効期間を持つ KEK を複数用意することで，例えば番組毎に料金を支払う Pay-Per-View 型のサービス提供が可能となる．

IETF は，データ秘匿に関する以下の二つの技術分野についても標準化を行っている．

- グループ鍵配信プロトコル

  IETF では，グループ鍵である KEK を配信するためのプロトコルとして以下を規定している．GKMP（Group Key Management Protocol）[87]は，共通鍵を生成し受信者に対して配信するプロトコルを規定している．RFC1949[88]は，CBT（Core Based Tree）[89]等のマルチキャストルーティングプロトコルを用いてスケーラブルなグループ鍵配送方法を提供している．GDOI（Group Domain of Interpretation）[90]は，IPSec で用いられる鍵交換プロトコル IKE（Internet Key Exchange）を拡張し，マルチキャストのような複数受信者に対応可能としたグループ鍵配信プロトコルである．GSAKMP（Group Secure Association Key Management Protocol）[91]は，グループポリシを配信し，受信者を認証し，グループ鍵を生成し，グループ鍵が解読された場合にそれを無効化することが可能なプロトコルである．MIKEY（Multimedia Internet KEYing）[92]は，特に無線ネットワークに適用するために設計されたグループ鍵配信プロトコルであり，3GPP の MBMS の配信データのデータ秘匿プロトコルとして採用されるなど今後普及が期待されるグループ鍵配信プロトコルである．

➢ データ暗号化プロトコル

IETF では，マルチキャストデータの秘匿のためのプロトコルとして以下を規定している．MESP（Multicast Encapsulating Security Payload）[93]は，IPSec の ESP（Encapsulating Security Payload）を拡張し，マルチキャストデータの秘匿を実現するプロトコルである．また，MTLS（Multicast Transport Layer Security）[94]は，任意の UDP アプリケーションを暗号化するために設計されたマルチキャスト用のトランスポートセキュリティプロトコルである．これらの 2 つのプロトコルは，データの秘匿の他にもデータ完全性検証や送信者認証等を行うことが可能である．

なお，グループ鍵は，あるメンバがあるマルチキャストグループから離脱した場合に更新する必要がある．グループ鍵を更新しないとあるメンバがマルチキャストグループから離脱したとしても当該メンバによって引き続きマルチキャスト配信データの受信と復号化によるデータの盗聴が可能となってしまう．この問題に対処するため，グループ鍵を更新する技術である Logical Key Hierarchy（LKH）[95][96]が存在する．例えば，LKH の代表的な提案方式である Key Graph[95]では，鍵管理サーバの負荷を低減するために，共有鍵を暗号化するための鍵に階層構造をもたせている．Key Graph では，メンバ数n に対して$O(\log n)$ のオーバヘッドで鍵更新が可能であることが示されている．しかし，LKH を用いたとしてもメンバのマルチキャストグループの離脱毎にグループ鍵の更新を行っていては，メンバ数が増加した際のスケーラビリティの問題が無視できなくなる．例えば，マルチキャストグループメンバが大量になればなるほどグループ鍵の更新頻度が多くなり，この更新によってネットワークの利用効率が落ちる場合がある．従って，グループ鍵にある有効期間を設け，その有効期間中はこの鍵を利用可能とするという運用を適用する使い方が一般的である．例えば，グループ鍵の有効期間を一ヶ月間とした場合，そのグループ鍵の払い出しに際して課金を行う．ユーザは，その期間中に中途解約を行ったとしてもそのサービス利用料金の払い戻しは不可能とするという運用上の制約を設けることで，メンバ数増加時にも頻繁なグループ鍵の更新は不要となる．

- Digital Rights Management（DRM）

デジタル著作権管理（DRM）に関しては数多くの関連技術が存在する[97][98]．例えばモバイル向けアプリケーション要素技術の標準化団体である OMA（Open Mobile Alliance）では，ディジタルコンテンツの著作権管理を実現するための OMA DRM 仕様を策定した[99][100]．OMA DRM は，著作権法で保護されるコンテンツの複製を制限可能とするだけでなく，モバイル端末におけるコンテンツの利用に関する制限（使用回数，使用期限など）を指示することも出来る．OMA DRM では，コンテンツと権利情報を分離することにより，コンテンツの流通を図る超流通機能も備えるなど，コンテンツプロバイダの要求に応える様々な機能を備えている．DRM にはその他にも FairPlay や Windows Media DRM，また家電向けのコンテンツの利用に関する各種機能を実現する DTCP（Digital Transmission Content Protection）などの各種技術が存在する[97][98].

OMA DRM は，受信した装置等からコンテンツを外部に出せなくすることで一定の著作権保護を行うものである．しかし，PC などのオープンなプラットフォーム上のファイルシステムにおいては，コンテンツを機器の外部に出すことを制限すること自体が不可能な場合もある．そこで，画像や動画，音声などのマルチメディアデータに，画質や音質にはほとんど影響を与えずに特定の情報を埋め込む電子透かし技術が存在する．電子透かしでは，特定の電子透かし検出ソフトウェアにより，作者名やデータの識別 ID やコピー回数などの埋め込まれた情報を読み出すことが可能であり，これによって配信したデータの再配布等に対処可能である．ただし，マルチキャストでは，ユニキャストとは異なり複数の受信者が同一のデータを受信することになるため，電子透かし中に含める識別 ID を受信者に応じて異なるようにする[101][102]などの工夫が必要となる．

- 送信者アクセス制御

送信者アクセス制御の実現には，受信者アクセス制御と同様に送信者をネットワークにおいて認証する方法が存在する[81]．また，ルータにおいて転送データを受信する入力ポートを制限する Network Ingress Filtering[49]と組み合わせることで送信者の認証を行うことなく送信者のアクセス制御を実現することが可能である．特に IGMPv3 では，2.4.1節で説明した SSM（Source Specific Multicast）が実現されており，送信者の IP アドレスとマルチキャストアドレスを結び付けて管理することで，各ルータにおいて Network Ingress Filtering による送信者アクセス制御を容易に実現できる．

- 送信者認証

送信者の成りすましを防止するために，送信者を認証する方式として送信者の電子署名を各配信データに含める方法が考えられる．しかし，電子署名は RSA 等の公開鍵暗号方式を用いるため，その検証処理オーバヘッドが受信者にとって負担となる．特にストリーミング型のマルチキャスト配信データの場合においては，データの復号化処理がストリーミングデータの受信速度に追いつかない場合もあるため，電子署名の利用は適切ではない．送信者認証は，送信者アクセス制御の方式と共に，送信者をネットワークにおいて認証する方法が存在する[81]．また，送信者認証は，マルチキャスト配信データの改ざんを防止する完全性検証と深く関連する．このマルチキャスト向けのデータ完全性検証を実現する技術として TESLA（Timed Efficient Stream Loss-Tolerant Authentication）[103]が存在する．TESLA を用いてデータ完全性検証を実行することにより，間接的に送信者認証を実現することが可能である．

5.1.3. マルチキャストセキュリティに関する残存課題

5.1.2節にて説明したように，マルチキャストセキュリティに関する関連研究は数多く存在する．しかし，これまでのマルチキャストセキュリティに関する関連研究の特徴として，データ秘匿に必要なグループ鍵配信とその更新に注目した研究が多いことが挙げられる．また，それぞれの課題を解決する独立した各種提案は存在するが，複数のマルチキャストセキュリティの課題を解決する方式が存在しないということが特徴である．一部の提案方式では，例えば IGAP のようにポイントトゥポイント型ネットワークでの利用に制限される等，限定された状況のみ対応可能なものもあり，幅広い状況に対応可能な方式が強く求められる．

以下では，既存方式において改善の余地がある課題をいくつか説明する．

1. DoS 攻撃

IGAP[82]や Gothic[83]等の既存方式では，全ての受信者からの IGMP 加入要求と IGMP 離脱要求に対してユーザ認証を行うことにより正当なユーザであるか否かの確認を行い，マルチキャスト DoS の対処を行うことが出来る．しかし，IGAP や Gothic は，受信者がデータ受信についての正当な権限を有しているか否かの判断が可能ではあるものの，逆にその手順に必要な通信を発生させることを目的とし，IGMP 加入要求や IGMP 離脱要求毎に実行される受信者認証を手当たり次第に発生する DoS 攻撃手法に対処不可能であるなどの課題もある．

さらに，マルチキャスト DoS への対処法は，無線 LAN やイーサネット等の複数の受信者で通信路を共有する形態（シェアードネットワーク）に適用することを考慮すると今までの提案方式で着目していなかった点が存在する．既存方式では，サブネットワーク中のメンバのうち最初に IGMP 加入要求を行った 1 台目の受信者の受信者認証を行えば十分であるというマルチキャストの同報性の特徴を生かしたアクセス制御と

はなっていない．つまり，既存方式は，アクセスルータが 2 台目の受信者の認証を実行してもしなくても１台目の受信者宛ての配信データの中継はいずれにせよ必要であると言う点に着目していない．この点に着目すると，通信制御パケット数を減らすことが可能なマルチキャスト DoS への対処法を提案することが可能である．以上のことから，既存方式は，主にユーザ課金を実現するために提案された方式であるため，マルチキャスト DoS に対処するために十分な機能を提供しているとはいえない．

2. ユーザ課金

IP マルチキャストの匿名モデルは，送信者において受信者の特定を行わずにデータ配信を行うため，課金を伴うサービスの提供が困難である．IETF のグループ鍵配信プロトコルにより，グループ鍵を配信したユーザに対して課金を行うことは可能であるが，これは，マルチキャストグループへの在籍期間（IGMP 加入要求から IGMP 離脱要求まで）を正確に示したものではないため機能不足である．

IGAP 等の既存方式では，ユーザ認証を行うことによりユーザ課金が実現可能な方式となっている．しかし，IGAP では，データ秘匿は実現しないため，第三者によるデータの盗聴が可能であるなど機能的に不十分であり課題が残る．

以上のことからデータ秘匿を実現しつつメンバのマルチキャストグループへの在籍期間を反映したユーザ課金を実現する方法が求められている．

先述のように既存方式には，それぞれのマルチキャストセキュリティの課題を解決する独立した各種提案は存在するが，複数の課題を同時に解決することができない．そこで，本章では，複数のマルチキャストセキュリティの課題を同時に解決するために以下の 3 つの機能を実現する受信者認証グループ鍵配布プロトコル AKDP（Authentication and Group Key Delivery Protocol）を提案する．

- データ秘匿のためのグループ鍵の配信
- マルチキャスト DoS 対策のための受信者アクセス制御
- マルチキャストグループへの在籍期間に同期した課金を実現

次節では，AKDP に求められる要求条件とその解決法について整理する．

5.1.4. AKDP に求められる要求条件とその解決方法

AKDP は，5.1.3節に述べた機能を提供することを目的とする．本節では，AKDP に求められる要求条件を整理し，各要求条件を満たすための解決法について説明を行う．

① グループ鍵配信（要求条件１）

IETF のグループ鍵配信プロトコルで既に実現されるグループ鍵配信は，データ盗聴の対処のために AKDP においても重要な要求条件である．

② 受信者アクセス制御（要求条件２）

先述したマルチキャスト DoS に対処するために，IGMP 加入要求と IGMP 離脱要求のそれぞれについて受信者認証を実行し，その受信者の正当性を検証することが重要である．またこの受信者アクセス制御は，マルチキャストの性質を考慮して必要最低限の処理で実現されるべきである．

③ メンバシップに同期した課金（要求条件３）

メンバのマルチキャストグループに在籍した期間に同期した課金を実現するために，IGMP 加入要求と IGMP 離脱要求のそれぞれについて受信者認証を実行することが必要である．以後ではメンバの在籍期間に同期した課金をメンバシップ同期課金と呼び，グループ鍵の配信に同期した課金をグループ鍵同期課金と呼ぶことにする．

ただし，多くのケースでは，以上に述べたすべての要求条件を満たす必要は無い．たとえば，アプリケーションによっては，データ秘匿は重要であるが，メンバシップ同期課金は必要ない場合が考えられる．その他にも，あるメンバが既にグループ鍵の受信を行った状況で単にサブネットワークを移動した場合など，既にグループ鍵を保持している状態で他のサブネットワークにおいてマルチキャストグループに加入する際にはグループ鍵配信は必要で無い．以上のことから，AKDP では，状況に応じて必要な機能のみを選択して実行するように柔軟性を持つべきである．

その他にも，マルチキャストに関連するプロトコルの一般的な要求条件として，受信者数が増加した場合のスケーラビリティとネットワークの利用効率の向上が挙げられる．特に第三世代移動通信網においては，そのラウンドトリップ時間（RTT）が数百ミリ秒から 1 秒程度までと，有線ネットワークと比較して非常に大きい値であるため，ネットワークの利用効率の向上，特に通信ステップ数の減少は無線ネットワークにおいて重要な要求条件である[71].

5.2. AKDP の提案

本節では，5.1.4節に説明した各種要求条件を満たす AKDP を提案する．まず，AKDP が動作するマルチキャストセキュリティアーキテクチャについて説明した後，AKDP の詳細について説明する．

5.2.1. マルチキャストセキュリティアーキテクチャ

提案するマルチキャストセキュリティアーキテクチャ（図5.3）は，IETF のマルチキャストセキュリティアーキテクチャに基づき[104]，送信者，認証＆鍵管理サーバ，受信者で構成され，新規ノードとして AKDP ルータを定義する．

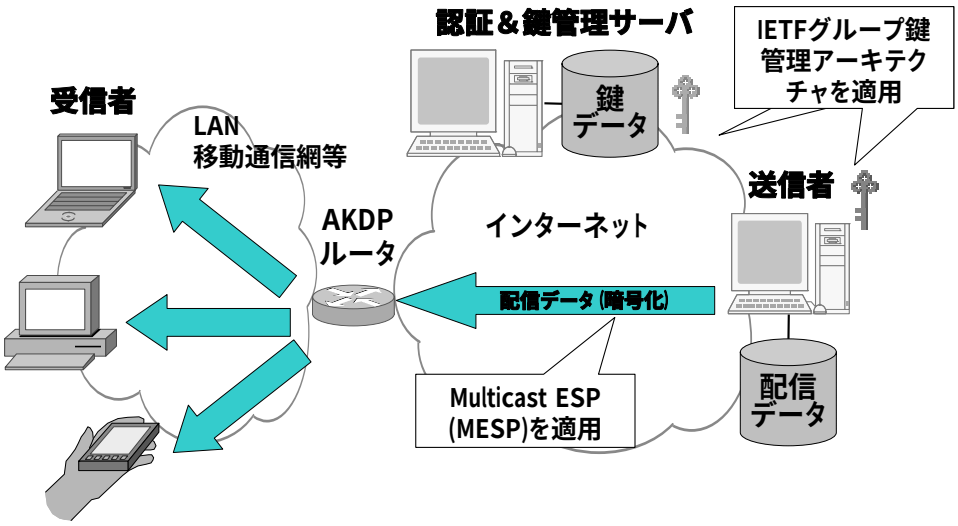


図5.3 AKDP によるマルチキャストセキュリティアーキテクチャ

AKDP ルータは，IGMP 加入要求や IGMP 離脱要求を受信した際に受信者認証を起動するため（要求条件 2 と 3），IGMP ルータの代わりに用いられるものである．受信者認証の

結果は，グループ鍵を受信者に対して配信するか否かを判断するためにも用いられる．そして，グループ鍵を配信するために（要求条件 1），AKDP ルータは認証＆鍵管理サーバと連携して動作する．また，認証＆鍵管理サーバは重要なノードであるために，一般的な DoS 攻撃の標的になりやすい．このことから，AKDP ルータによって認証＆鍵管理サーバへの直接通信を防止することは重要である．認証＆鍵管理サーバは，CIK と各受信者の権限情報を保持しており，送信者と連携してグループ鍵の共有を行う．CIK には，PKI（Public Key Infrastructure）によって運用された各種鍵を用いることが出来る．なお，図中にある配信データの暗号化については IETF で提案された MESP[93]や MTLS[94]を使用できるようなアーキテクチャになっており，AKDP の設計においては，これら MESP や MTLS との連携に矛盾が無いように考慮する必要がある．

5.2.2. AKDP 概要

AKDP は，通信開始時にネゴシーション機能が実行される．この機能は，必要の無い機能を選定してその実行を省略するために設けている．具体的には，ネゴシエーション機能は，受信者認証やグループ鍵の配信が必要か否かを判断するために用いられる．

まず，受信者認証が不必要な状況を以下に説明する．

- 共有メディアネットワーク上で 2 番目以降のメンバの場合

  イーサネットや無線 LAN 等の共有メディアを使用したネットワークでは，マルチキャストデータはサブネットワーク上にすでに同報配信されていることから，この状況下では 2 番目以降の受信者加入時の受信者認証によるアクセス制御は無意味となる．従って，受信者認証は，アクセス制御を実現する手段としては，ある受信者が最初のメンバとしてマルチキャストグループに加入しようとするときのみ実行されるべき機能である．

  なお，ある受信者によるマルチキャストグループへの加入要求が二台目か否かは，AKDP ルータが当該グループへの配信データの中継を既に行っているか否かにより判断可能である．そこで，受信者認証を実行すべきか否かは AKDP ルータから受信者に対して伝えられ，それを伝えられた受信者は，AKDP ルータから伝えられた受信者認証の実行要求に応答して受信者認証に必要な手順を開始することが可能である．

- メンバシップ同期課金が不必要のとき

  例えば，ある TV 番組が IP ネットワーク上にストリーミング配信されるようなアプリケーションを想定した場合に，当該番組の一ヶ月の視聴料が一律に固定額というケースが存在する．このような月額課金（サブスクリプション型課金）の実現のためには，メンバシップ同期課金は不要である．サブスクリプション型課金の実現の場合には，グループ鍵同期課金を用いることにより配信データ毎の課金が可能である．

  なお，送信者等のコンテンツ提供者は，メンバシップ同期課金を必要とするのか，グループ鍵同期課金を必要とするのかを決定する権限がある．従って，AKDP ルータは，送信者やコンテンツ提供者に問い合わせることで，あるマルチキャストグループの中継に際して受信者認証が必要か否かを判断することが可能である．さらに AKDP ルータは，受信者認証を必要とするか否かを受信者に伝えることにより，受信者は，受信者認証に必要な手順を開始することが可能である．

一方，グループ鍵配信を必要としないケースについては以下がある．

- 受信者が既に有効なグループ鍵を保持する場合

  サブスクリプション型課金を実現するケースで，グループ鍵が一定期間（一ヶ月等）有効で，受信者がその有効期間中にマルチキャストグループへの加入と離脱を繰り返し行う場合がある．このような場合には，一度取得したグループ鍵はその有効期間中であ

れば再使用できるため，マルチキャストグループ加入時にグループ鍵の配信が不必要な場合がある．

また，受信者がデータ受信を行いながら移動をすることによってサブネットワークを変更する場合も考えられる．このような場合，受信者は既にグループ鍵を受信済みであるため，移動先のサブネットワークにおいてマルチキャストグループ加入の際に，グループ鍵の入手は不要である．

なお，グループ鍵の配信が必要か否かは，受信者のみが知っているため，受信者から AKDP ルータに対して伝えられる必要がある．グループ鍵配信の必要性の通知を受けた AKDP ルータは，認証＆鍵管理サーバと連携することによって受信者に対してグループ鍵の配信が可能となる．

AKDP では，以上に説明した情報を受信者と AKDP ルータ間でやり取りを行うためにネゴシエーション機能を持つ．ネゴシエーション機能は，受信者認証，およびグループ鍵の配信機能を実行するか否かを決定するために用いられるものである．図5.4は，AKDP の基本的な通信手順を示したものである．

a) ネゴシエーション機能

AKDP ルータは，受信者から送信された IGMP 加入要求（IGMP Membership Report）を受信すると AKDP の実行を開始する．AKDP ルータは，受信者認証が必要か否かを示す認証情報を受信者に対して送信する（a-i）．それに対して受信者は，グループ鍵を取得するか否かを示すグループ鍵情報を AKDP ルータに対して送信する（a-ii）．以上の手順により，データ受信装置と AKDP ルータの双方が，お互いにどの機能を必要とするか否かを知ることが出来る．この手順により表5.1に示すような 4 つのケースに分けられ, 以後の手順は各ケースによって実行される機能が異なる．

b) 受信者認証機能

ネゴシエーション機能により受信者認証が必要だと判断されると（ケース 1 とケース 3 の場合）受信者認証機能が実行される（b-i から b-iii）．受信者認証は，パスワードを用いたチャレンジレスポンスによる認証や，受信者のデジタル証明書を用いた認証のいずれかの方式を用いることが出来る．具体的な受信者認証の実現方式については5.3節で述べる．

c) グループ鍵配信機能

ネゴシエーション機能によりグループ鍵配信が必要だと判断されると（ケース 1 とケース 2 の場合）グループ鍵配信機能が実行される（c-i から c-iv）．受信者の認証の結果をグループ鍵配信の可否の判断に用いるため，グループ鍵配信機能は受信者認証の後に実行される．グループ鍵配信については，IETF で標準化された各種グループ鍵配信プロトコル（MIKEY[92], GDOI[90], GKMP[87], GSAKMP[91]）の任意のものが使用出来るようにする．図5.4ではグループ鍵配信プロトコルとして MIKEY を使った場合の例を示している．AKDP では，任意のグループ鍵配信プロトコルを利用可能としたところが特徴的な機能のひとつである．具体的なグループ鍵配信の実現方式については5.3節で述べる．

AKDP では，以上に説明した 3 つの手順を完了すると，その有効期間を含めた認証成功を示すメッセージ（Success）が認証＆鍵管理サーバから AKDP ルータを経由しデータ受信装置に対して送信される．その後 AKDP ルータはその有効期間中，PIM-SM（Protocol Independent Multicast - Sparse Mode）[43]等を用いてマルチキャスト配信木等の構築を

行った後，マルチキャストデータの中継を実行する．以上の手順により受信者はマルチキャストデータの受信を開始することが可能となる．

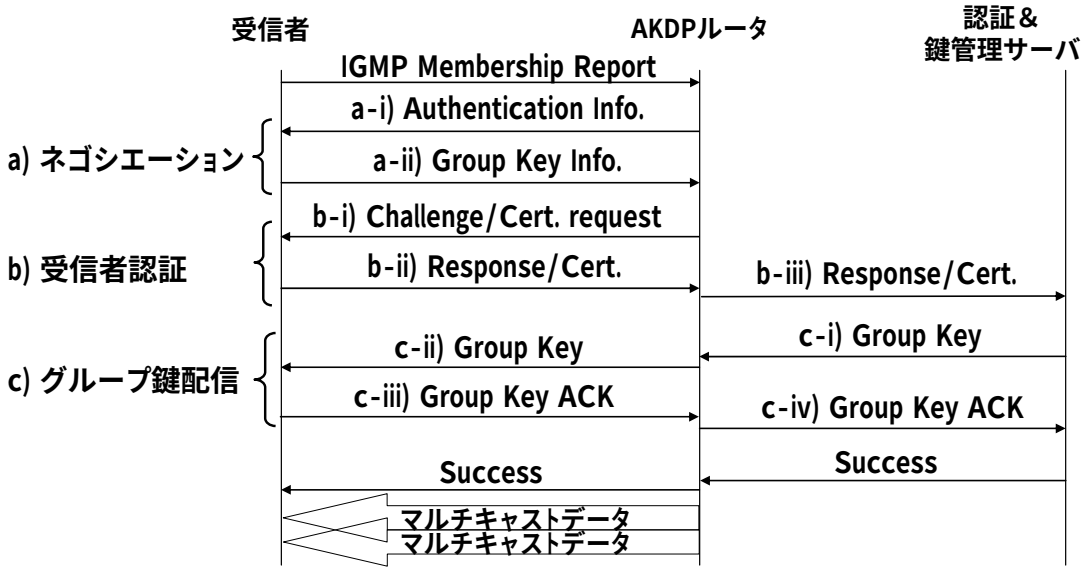


図5.4 AKDP の基本的な通信手順

表5.1 各ケースにおける必要な機能と省略可能な機能

	グループ鍵配信の必要性	受信者認証の必要性	省略可能な機能
Case1	必要	必要	無し
Case2	必要	不必要	受信者認証
Case3	不必要	必要	グループ鍵の配信
Case4	不必要	不必要	グループ鍵の配信，受信者認証

受信者が IGMP 離脱要求を送信する時の AKDP の手順は，IGMP 加入要求送信時と同様であるが，ネゴシエーション機能とグループ鍵配信機能は不要となる．受信者認証については，ネットワーク運用者であるオペレータによってメンバシップ同期アカウンティングやマルチキャスト DoS 対策が必要とされた場合に限り，図5.4の b-i)を送信することでその処理が開始される．受信者認証が必要でない場合には，通常の IGMP 離脱要求を受信したものとして IGMP の手順を継続する．なお，受信者の離脱に伴う他メンバのグループ鍵を更新する場合，AKDP ルータや認証＆鍵管理サーバはグループ鍵の更新手順を行う．グループ鍵の更新手順については Key Graph[95]等の効率の良いグループ鍵更新手順と組み合わせることが可能となる．

5.3. AKDP の詳細

IGMP はマルチキャストグループ管理プロトコルとして既に広く使われているため，AKDP は IGMP のすべてのバージョンと連携して動作する必要がある．従って，AKDP は，受信者からの全てのバージョンの IGMP 加入要求と IGMP 離脱要求により起動されるよう

に設計されている．このため，ルータが AKDP ルータでなく通常の IGMP ルータであった場合でも，ルータおよび受信者は通常の IGMP 手順を継続することが可能である．

図5.5に AKDP のプロトコルスタックを示す．この図に示すように，AKDP は，EAP（Extensible Authentication Protocol）[105]と RADUIS（Remote Authentication Dial In User Service）[106]を拡張したプロトコル（同図の EAP+や RADIUS+）で構成される．なお，EAP の動作に関しては，IP 上では EAP over UDP（EAPoUDP）[107]や無線 LAN 上では EAP over LAN（EAPOL）[108]等の各種プロトコルを使うことが出来る．また，MIKEY[92]や GDOI[90]等の IETF の任意のグループ鍵配信プロトコルを使用出来るようにするために，AKDP では，EAP や RADIUS に対してこれらのプロトコルを運搬することを可能にするための属性の追加を行っている．

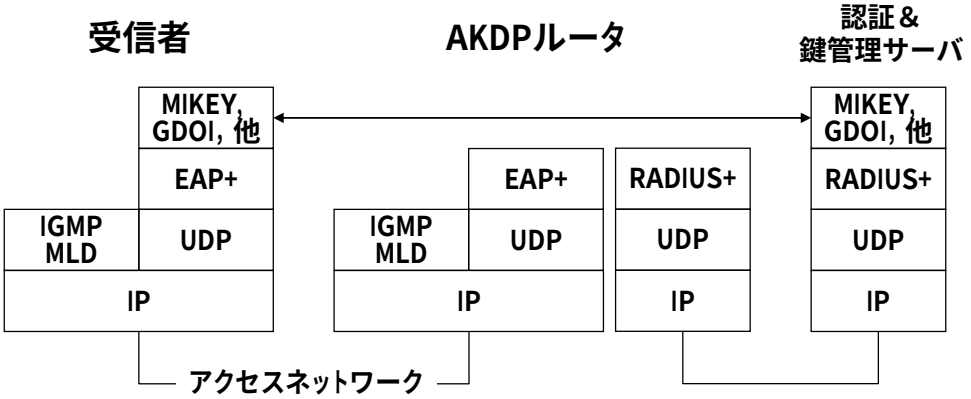


図5.5 AKDP のプロトコルスタック

5.3.1. AKDP の通信手順詳細

以下では，図5.6に示すケース１の通信手順例を用いて提案方式の動作を説明する．

受信者が，IGMP 加入要求を送信すると（①），EAP によるネゴシエーション手順が実行される（②，③）．MSecInfo は提案方式において新しく定義した EAP のタイプであり，ネゴシエーション機能で用いる様々な情報要素が含まれる．”Auth=Yes”は，AKDP ルータが受信者認証の実行を必要としていることを示す．また，”KEK=Yes”は，受信者がグループ鍵配信を必要としていることを示している．MSecInfo は，Receiver ID 属性により，IP アドレス，ユーザ名，電話番号等の受信者を一意に識別するための ID を含めることが可能である（③）．その後 AKDP ルータは，受信者の認証手順を実行する（④，⑤）．この例では，SHA-1（Secure Hash Algorithm - 1）に基づくチャレンジレスポンスにより受信者の認証を実行しているが，PKI に基づくデジタル証明書を用いた認証を行うことも可能である．次に，AKDP ルータは⑥により認証＆鍵管理サーバ対して必要な情報を送信し，この時点で認証＆鍵管理サーバは受信者の認証を行う．以上の④～⑥の手順が受信者認証手順である．その後，認証＆鍵管理サーバは任意のグループ鍵配信プロトコルを用いてグループ鍵の配信を行う．図の例では MIKEY を用いてグループ鍵を配信している様子を示している（⑦～⑩）．MIKEY は，各クライアントの CIK で暗号化した KEK を I_Message 中に含んでいるため，I_Message を受信したクライアントは，KEK の取得が完了し（⑧），その後 MIKEY の R_Message による確認応答を送る（⑨, ⑩）. なお, 提案方式ではこれらの MIKEY データを透過的に運搬するための新しいタイプを EAP と RADIUS に定義している．そして最後に，EAP の終了手順（⑪，⑫）が行われる．なお，図5.6の⑪を受信した AKDP ルータは，この時点で受信者認証が成功したことが分かるので，PIM-SM 等を用いて当該グループのマルチキャストツリー構築のための手続きを行い，Validity-Period で指定されるアクセス制御の有効期限まで配信データの中継を行う（⑫）．

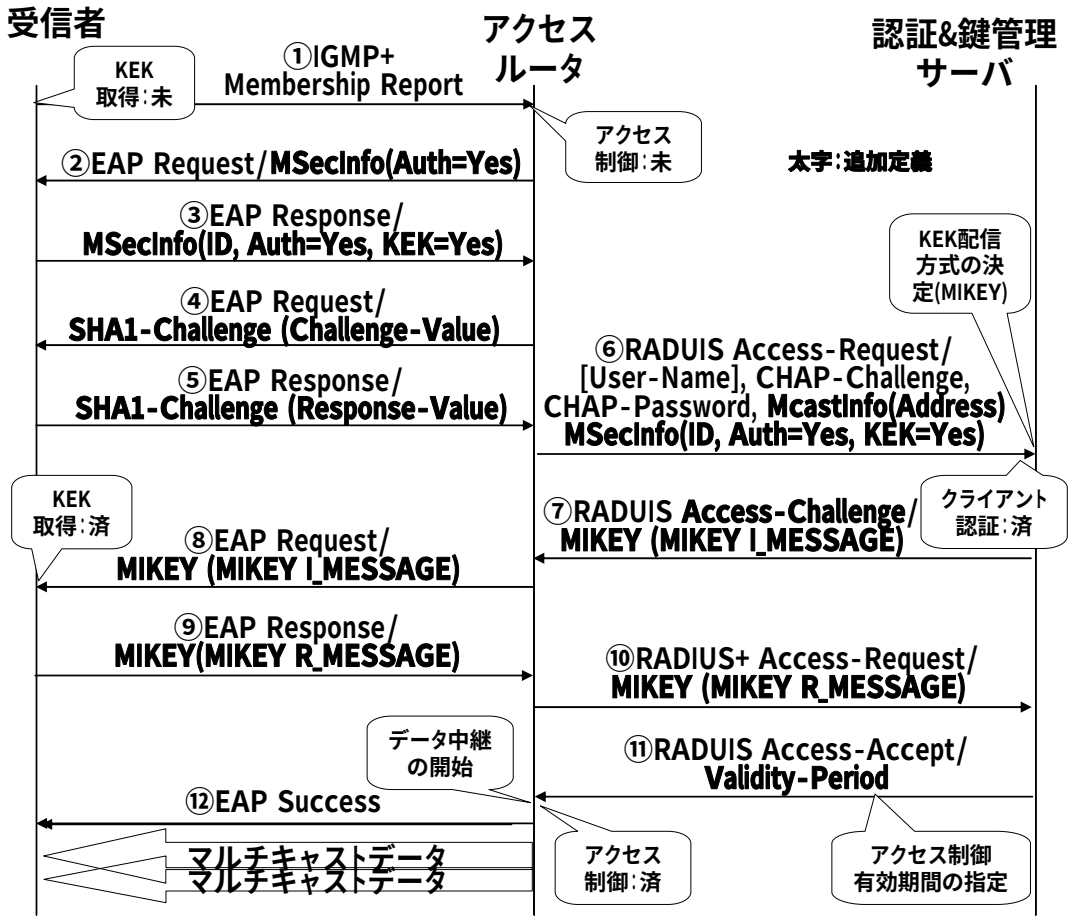


図5.6 ケース 1 のシーケンス

図5.7は，ケース２の通信手順例を示している．ケース 2 では，他の受信者によりアクセス制御が完了しているため，受信者は，IGMP 加入要求を AKDP ルータに送信後（①）すぐにマルチキャスト配信データの受信が可能である．AKDP ルータは，受信者認証が必要ないため”Auth=No”を示す MSecInfo を受信者に送信する．以上の動作により AKDP ルータは，データ受信装置の認証手順を省略する．

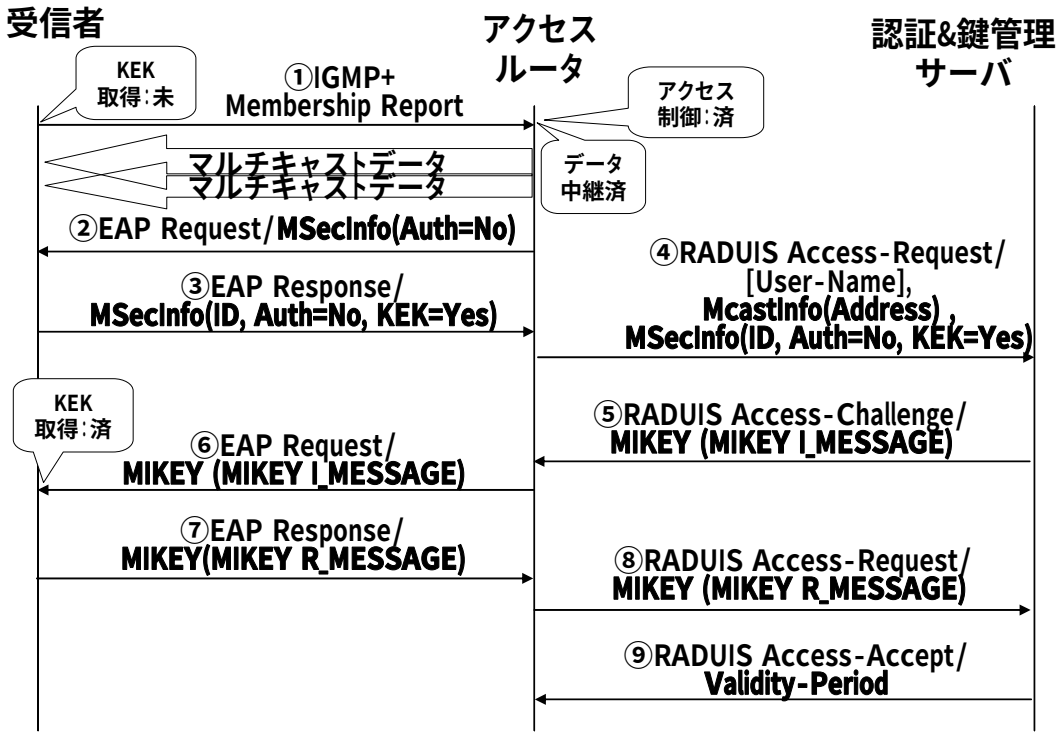


図5.7 ケース 2 のシーケンス

図5.8は，ケース 3 の通信手順例を示している．ケース 3 では，グループ鍵の配信が不要であるため受信者は”KEK=No”と記載された MSecInfo を AKDP ルータに対して送信する．受信者は，KEK の ID を MSecInfo に含めることにより，保持している KEK の情報を認証&鍵管理サーバに対して伝えることが可能である．認証&鍵管理サーバは，”KEK=No”を含む MSecInfo の受信によりグループ鍵配信の手順を省略することになる．

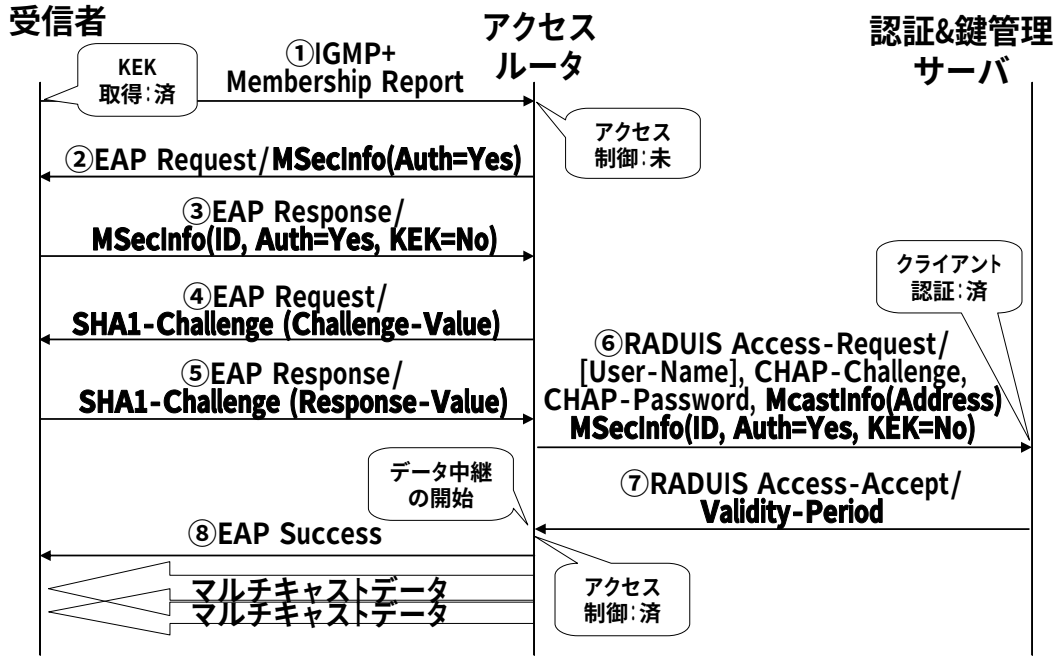


図5.8 ケース 3 のシーケンス

図5.9は，ケース 4 の通信手順例を示している．ケース 4 では，受信者認証，およびグループ鍵の配信が不要であるため，”Auth=No”，”KEK=No”を含む MSecInfo をやり取りすることにより，両機能は省略される．なおケース 4 では，アクセス制御が完了しているため，受信者は，IGMP 加入要求を AKDP ルータに送信後（①）すぐにマルチキャスト配信データの受信が可能である．

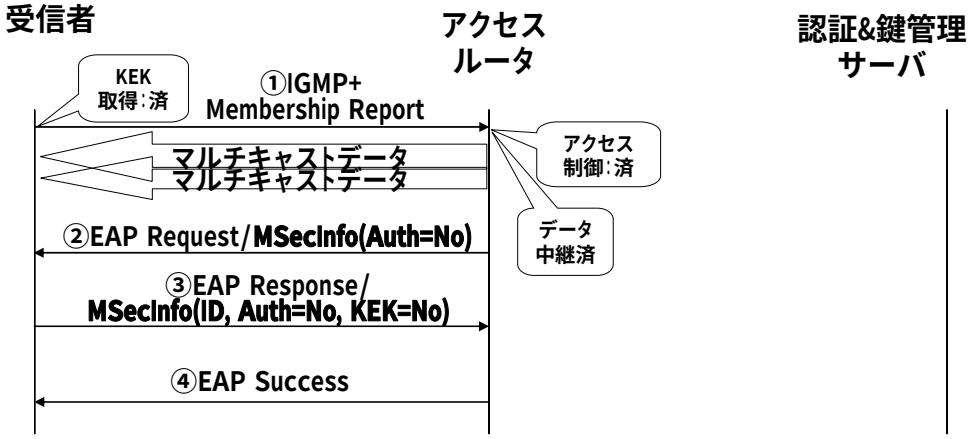


図5.9 ケース 4 のシーケンス

AKDP の受信者アクセス制御機能は，無線ネットワーク等の共有メディアでの利用を前提に設計されている．しかし，ADSL や光ファイバで構成されたポイントトゥポイントネットワークについても AKDP の適用は可能である．このようなネットワークでは，AKDP ルータは，IGMP 加入要求をすべてのメンバから受信することになるが，受信者認証については最初の受信者からの要求のみについて受信者認証をすれば受信者のアクセス制御は完了する．

5.3.2. AKDP プロトコルフォーマット

先述したように本提案では EAP に新しいタイプを定義している（表5.2）．RADIUS についても EAP と同様な新しい属性を追加している．MSecInfo タイプの構造は，図5.10に示すようになっており，複数の属性を含められるようになっている．同図で，KEK&Auth 属性は5.2.2節で説明したネゴシエーション機能を提供するための情報を含める属性である．KEKInfo 属性は，受信者が保持する KEK の ID を含める属性であり，認証＆鍵管理サーバによりその KEK が有効であるか否かの判断のために用いる．また McastInfo 属性は，受信者が加入をしようとするマルチキャストグループを一意に識別する情報を含めることが可能であり，マルチキャストアドレスがその例にあたる．なお，図5.10に示す数字は各フィールドの長さをビット長で示している．

表5.2 AKDP 用に定義した EAP の新タイプ

タイプ名	概要
MSecInfo	KEK&Auth 属性（図5.10参照）
SHA1-Challenge	SHA-1 を用いた受信者認証
Certificate	電子証明書を用いた受信者認証
KEKInitRequest	受信者起動型鍵配信プロトコル起動要求
EAP-MIKEY	MIKEY over EAP
EAP-GDOI	GDOI over EAP
EAP-GSAKMP	GSAKMP over EAP
EAP-GKMP	GKMP over EAP

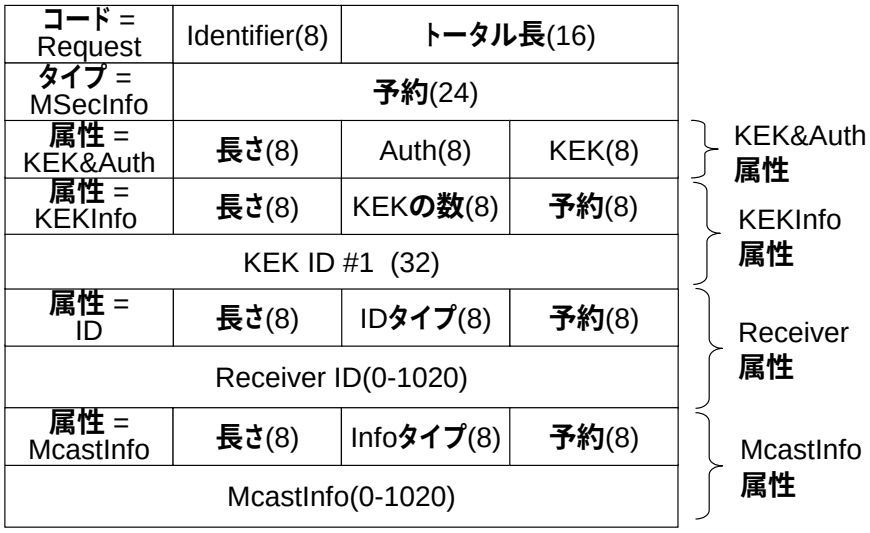


図5.10 EAP の MSecInfo タイプの構造

5.4. 実装

本節では，AKDP の効果と性能について評価するために実装したプロトタイプについて説明する．図5.11に示すように，本プロトタイプは，2 台の AKDP ルータと認証サーバ，および無線 LAN で構成したアクセスネットワーク上に設置した複数の PC と PDA で構成される．AKDP では，MIKEY に含まれる情報要素のうち KEK 配信に最低限必要な機能のみを実現した．CIK, KEK, TEK には，それぞれ 256, 192, 128 ビット長の Camellia[109]を用いた．本プロトタイプでは，MTLS[94]の実装も行っており，データの秘匿と HMAC（Hash Message Authentication Code)-SHA1 を利用したメッセージ認証機能の提供があわせて可能である．以後説明する性能評価は図5.11に示した PC を用いて行っている．

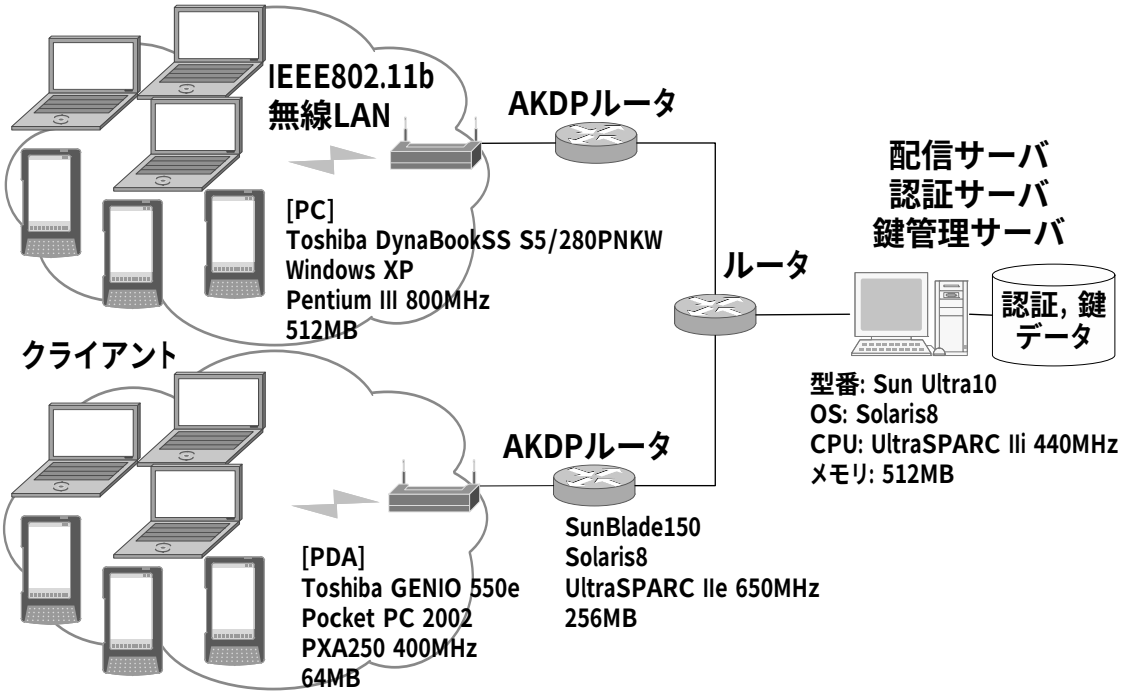


図5.11 実装システム

5.4.1. AKDP 手順に要する処理時間

最初に，AKDP の実行に必要な通信時間を測定する．図5.12は IGMP 加入要求（IGMP Message Report）を送信してから EAP Success を受信するまで，つまり AKDP の処理が開始されてから完了するまでの時間を示している．なお，同図では AKDP ルータにおいて測定した各制御パケット送受信の時間間隔を順に積み上げ棒グラフで表現している．

この図より，処理手順が最も複雑なケース 1 の通信時間に 406 ミリ秒を要することが分かる．文献[110]によると，データの取得要求から表示までにユーザが許容する時間は 8 秒以内という指標が示されている．この 406 ミリ秒にデータ取得までに要する時間を追加しても，8 秒以内という許容時間内に十分収まるものと考えられる．従って，最も処理時間がかかるケース１の場合においても，提案方式は十分使用に耐えうることが分かった．

また，認証＆鍵管理サーバにおいて受信者認証とグループ鍵の生成に要する時間が総時間を占める割合は，ケース１では 76%，ケース 2 では 57%であり，この処理時間がボトルネックになりうることが分かった．ただし，図5.3に示したマルチキャストセキュリティアーキテクチャでは，認証＆鍵管理サーバを複数用意することで，受信者認証とグループ鍵の生成を分散して処理できるようになっており，このようなボトルネックにも対処可能である．ケース 3 とケース 4 においては，KEK の生成が必要でないため，全体の応答時間についてもケース 1 とケース 2 と比較して短いことが分かった．

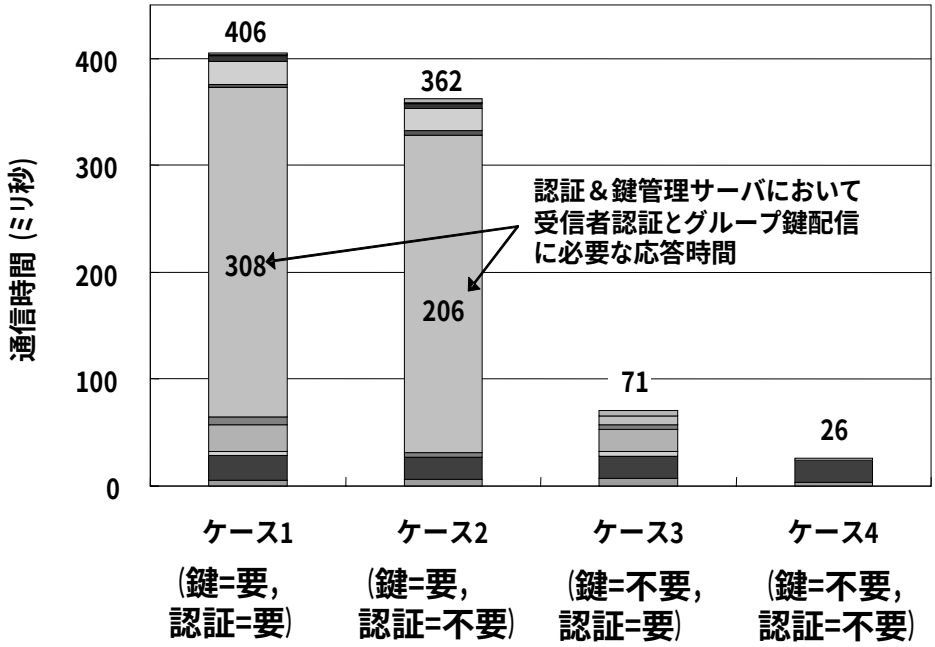


図5.12 各ケースの通信時間の比較

5.4.2. 認証＆鍵管理サーバにおける処理時間

次に，認証＆鍵管理サーバにおける受信者認証と KEK 生成に要する時間について受信者数を増加させた環境で測定した結果を図5.13に示す．その結果，複数の受信者が同時に認証＆鍵管理サーバにアクセスした場合にはその応答時間が無視できないことが分かった．特に 10000 台の受信者が存在する場合，CIK の検索と KEK の暗号化に要する KEK 生成のための処理時間は，全体の処理時間の 95%を占めることが分かった．

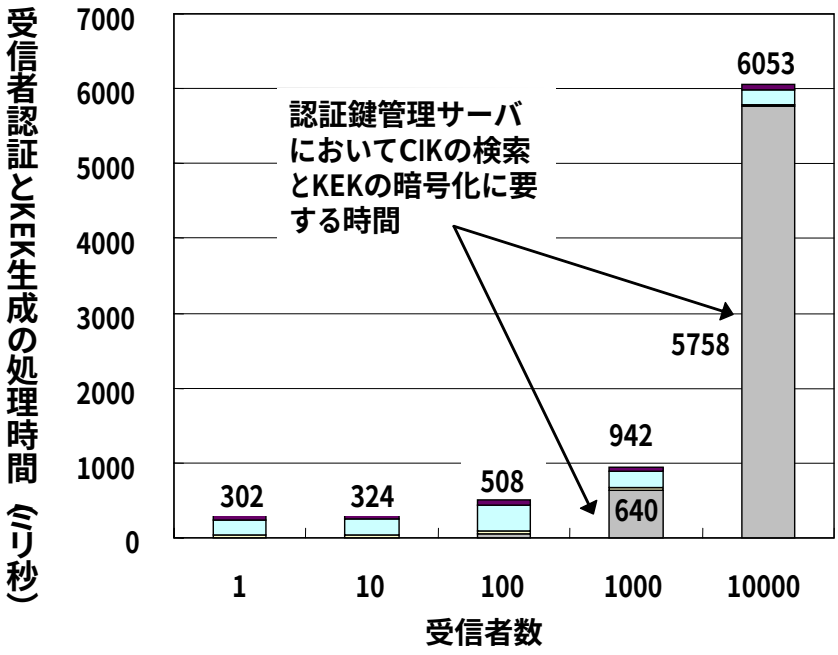


図5.13 認証＆鍵管理サーバにおける処理時間

5.4.3. AKDP ルータにおける処理時間

最後に，AKDP ルータの処理時間の評価を行うため，同ルータにケース 1 の IGMP 加入要求を 1 ミリ秒の間に 100 個受信させた．そして，その際に同ルータでやりとりされるメッセージの処理時間を測定し，そのうちから 7 個の加入要求に対するメッセージの処理時間を取り出したものを図5.14に示す．図の横軸にあるシーケンス番号は，図5.6において AKDP ルータで送受信される①～⑫のメッセージに対応する．縦軸は AKDP ルータで最初の加入要求を受信してから①～⑫の各メッセージを処理し終わるまでの累積時間を表す．

図5.14の結果から処理時間の増加が顕著なメッセージとして⑦と⑪がある．これらは認証＆鍵管理サーバにおける受信者認証のための処理と MIKEY の R_Message の処理に要する時間に相当し，AKDP ルータにおけるボトルネックではない．これらの値が大きいことは，図5.12で示した通りである．AKDP ルータにおいて一番大きなボトルネックとなったのは AKDP ルータにおける IGMP 加入要求の処理（①）や受信者認証のためにチャレンジ値を生成する処理（④）であったが，これらの値は認証＆鍵管理サーバにおけるボトルネックと比較すると小さく，この点が全体の応答時間に大きく影響しているとはいえないことが分かった．

なお，最初の IGMP 加入要求に対する処理が 616 ミリ秒を要しており，図5.12で示した処理時間よりも 1.5 倍の時間がかかっていることが分かった．この理由として，本プロトタイプではすべてのデータが単一のキューにバッファリングされ，FIFO（First in First Out）ベースで実装されたことが理由である．つまり，100 個の IGMP 加入要求がいち早くキューにたまったため，その処理が完了するまでに最初の IGMP 加入要求に対する MIKEY I_Message の処理（⑦）が完了しなかったことがこの原因である．この点に関しては実装を改善するなどの余地もあるが，100 個の IGMP 加入要求の同時処理全体でも 1371 ミリ秒程度の処理時間で済むことから，8 秒ルール[110]に影響があるような著しい処理性能の低下につながることが無いことが分かった．また，100 個の IGMP 加入要求が一度に AKDP ルータに集中すると，AKDP ルータにおける処理待ちが発生し，図5.14のシーケンス番号 2 で示すように特に 100 個目の IGMP 加入要求における処理時間が増加するが，この処理時間の増加についても 8 秒ルールに影響があるような著しい処理性能の低下とはならないことが分かった．さらに本測定は 1 ミリ秒に 100 個の IGMP 加入要求が集中する現実よりも厳しい環境で測定しているために，実環境ではより全体の処理時間が短くなることが予想出来る．

AKDP の処理の限界についてあわせて評価したところ，AKDP ルータは 256 個までの同時の IGMP 加入要求は受け付けることが出来たが，その後受信した 257 個目以降の IGMP 加入要求に関しては，破棄していることが分かった．ただし，IGMP は，連送機能により複数回送信されるため破棄されたとしても後に再送された加入要求が処理される可能性もある．

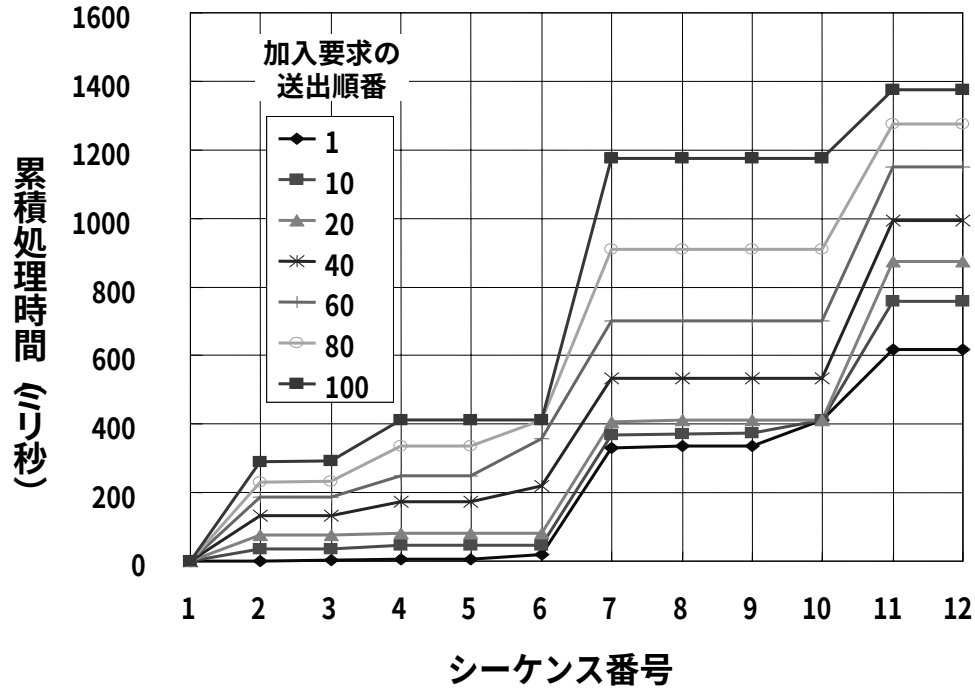


図5.14 AKDP ルータにおける処理時間

5.5. 考察

AKDP は，ネゴシエーション機能を持っており，グループ鍵配信機能や受信者認証機能を必要に応じて選択的に提供する特徴を持つ．最初にこのネゴシエーション機能の効果について述べたあと，AKDP の各機能について考察する．

- ネゴシエーション機能の効果

まず，図5.12で示した性能評価結果を踏まえ，アクセスルータ配下に存在する受信者数に着目した理論解析を行い，提案方式の有効性について考察する．本検討では，受信者アクセス制御の効果を検証するためにメンバシップ同期アカウンティングは必要としない状況を想定する．さらに，アクセスルータの変更を伴う受信者の移動についても考慮しない．なお，これらの状況を考慮した場合の考察は後述する．

以下では，ある AKDP ルータ配下に存在するメンバ数を n とした時の AKDP の各ケースが実行される回数を比較する．

①ケース１

AKDP は最初にグループに加入する 1 台のみが，受信者認証機能とグループ鍵取得機能の両方の機能を必要とする．

② ケース２

最初のメンバ以外のメンバ $(n-1)$ 台がグループ鍵取得のためそれぞれ一回ずつ実行する．

③ ケース 3

ここでは受信者が移動しない単純な環境を想定するためここでは相当する受信者は存在しない.

④ ケース 4

ケース 4 は，IGMP によるメンバ管理，つまり IGMP 問い合わせ後の IGMP 加入要求による通信が発生する．ここで IGMP の一般問い合わせの間隔をT_gとし，IGMP によるグループ管理をT_d間隔実行した場合には，AKDP は IGMP の一般問い合わせの結果としてT_d/T_g回実行される．さらに，最後にグループから離脱する受信者以外の$(n-1)$台のメンバがグループからの離脱処理を行った際に，その後の IGMP グループ特定問い合わせで$(n-1)$回の通信が発生する．従って，ケース 4 では，合計$(T_d/T_g+(n-1))$回の AKDP が実行される.

次に，AKDP のネゴシエーション機能を用いなかった場合に AKDP が実行される回数を計算する．この条件の下では，受信者認証やグループ鍵の配布が常に実行されるため，合計$(T_d/T_g+(2n-1))$回の AKDP のケース 1 相当の機能が提供される.

以上の計算結果をまとめたものを表5.3に示す．AKDP のネゴシエーション機能がある場合も無い場合も全体の 4 ケースの実行回数の合計はいずれも(T_d/T_g+2n-1)回となる.

表5.3 各ケースが実行される回数の比較

		ネゴシエーション機能あり	ネゴシエーション機能無し
実行回数	ケース 1	1	T_d/T_g+2n-1
	ケース 2	$n-1$	0
	ケース 3	0	0
	ケース 4	T_d/T_g+n-1	0

n：AKDP ルータ配下に存在するメンバ数
T_g：IGMP General Query（一般問い合わせ）の間隔
T_d：グループ管理が実行される時間

以上で比較した各ケースの実行回数を元に AKDP のネゴシエーション機能による効果を示すために代表的な数値例を用いて計算する．ここでは，AKDP 配下の各アクセスルータに 100 台の受信者が存在し（$n=100$），配信データが 30 分間配信される（$T_d=1800$）と想定する．なお，ここで想定したこれらの値は，日本における基地局の数と携帯電話の加入者数を元に計算された十分に実績のある値である．ここでは AKDP ルータは，基地局と併設される形で設置される状況を想定し，携帯電話全体の加入者のうち，2.5%のユーザが本サービスの提供を受ける状況を想定している．30 分間配信されるデータは IPTV 等によるストリーミングデータの配信を想定しているが，携帯電話等を考慮した場合には十分長い値である．なお，IGMP の一般問い合わせは 125 秒間隔で配信される（$T_g=125$）ことがデフォルト値で決められている．以上のことから，図5.12の各ケースにおける応答時間と表5.3に示す各ケースが実行される回数から全体の通信時間の平均値を求めることが可能である．表5.4に示すように AKDP は，ネゴシエーション機能を用いない方式と比較して平均処理時間が 52%減少することが分かる．受信者とアクセスルータ間の制御パケット数についても同様な計算を行うと，32%の減少が得られる．以上のことから移動通信網等の無線通信のコストが高く遅延が大きいネットワークにおいては，提案方式のネゴシエーション機能が有効であることを確認した.

表5.4 AKDP のネゴシエーション機能による効果

	ネゴシエーション機能有り	ネゴシエーション機能無し
全体通信時間（秒）	39.218 （52%減少）	82.115
全体制御パケット数（回）	1460 （32%減少）	2144

以下では AKDP に関するその他の点について考察する．

- メンバシップ同期課金

以上で説明した評価はメンバシップ同期課金を必要としない状況を想定していた．もしメンバシップ同期アカウンティングが必要な場合は，ケース 1 やケース 3 が常に実行されることになる．このようなケースでは，AKDP のネゴシエーション機能の効果は低下するが，グループのメンバの在籍状況に応じた正確なユーザ課金を行うことが出来る．この課金の方式は，ネットワークオペレータのポリシやアプリケーション毎に柔軟に変更可能とする必要があるため，AKDP はこれら要求に柔軟に対応出来る点で有効である．

- AKDP における通信時間への影響

AKDP は，受信者認証により受信者のアクセス制御や，メンバシップ同期課金を実現することが可能である．しかし，IETF の鍵管理アーキテクチャやプロトコルではこれらの機能をサポートしていない．従って，AKDP では，IETF の鍵管理アーキテクチャと比較して全体の通信時間が増加することが懸念される．しかし，図5.12に示した測定結果によると，AKDP のケース 1 のネゴシエーション機能と受信者認証による通信時間は 57 ミリ秒（全体の通信時間の 14%）であり，受信者認証機能はネットワーク全体における通信性能低下の最大の原因とはならないことを確認した．

また，IETF の GKM アーキテクチャと比較すると，提案方式には受信者と認証＆鍵管理サーバ間の通信を中継する AKDP ルータが存在するため，同ルータによる処理時間の増加が懸念される．これについても同様に，図5.12における AKDP ルータにおける処理待ち受け時間を測定したところ，その処理時間は 9 ミリ秒（全体通信時間の 2%）であった．従って，AKDP ルータを追加したことによる遅延時間の増加は，全体の処理性能の低下にはつながらないことが分かった．

- 認証＆鍵管理サーバのスケーラビリティ

複数の受信者が認証＆鍵管理サーバに同時にアクセスし，グループ鍵の生成の要求を同時に行った場合の処理時間の影響については，5.4.2節において課題があることを説明した．従って，認証＆鍵管理サーバのスケーラビリティを確保することが AKDP アーキテクチャの最大の課題である．しかし，提案した AKDP のアーキテクチャでは，認証＆鍵管理サーバの複数設置を可能とする構成を取ることが出来るため，AKDP がロードバランス装置としてユーザ毎に認証＆鍵管理サーバを振り分けることによって認証＆鍵管理サーバのスケーラビリティを確保することが可能である．

- ケース 2 とケース 4 における DoS 攻撃

AKDP は，ケース 1 が実行されることで不必要なマルチキャスト配信木の構築を防止することが可能であるため，結果的にルータやネットワークのリソースの浪費につながる DoS 攻撃に対処することが可能である．しかし，ケース 2 では，受信者認証を実行しないため，悪意のあるユーザが，受信者の識別子（Receiver ID 等）の詐称を伴ったグループ鍵の生成要求メッセージを送信することが可能である．その悪意のあるユーザは，

CIK で暗号化されたグループ鍵（KEK）を入手したとしても正当な CIK を持ち合わせていないため KEK の復号化は不可能であり, 結果として配信データを利用することは不可能である．しかし，悪意のあるユーザがケース 2 を多数連続して実行する攻撃手法が現実に考えられないわけではなくこの対処が重要である．ケース 4 についても同様に受信者認証を実行しないことを突いた攻撃手法への懸念が存在する．

ケース 2 やケース 4 を手当たり次第に発生させる DoS 攻撃手法については，例えば，AKDP ルータにおいてトラヒックモニタリングを行うことによってこの DoS アタックを検出する手法が提案されている[111]．この手法を用いることにより，監視状況に応じて，AKDP ルータが全体の応答時間の小さいケース 2 やケース 4 を用いるか，または受信者の認証を常に必要とするケース 1 やケース 3 を用いるかを動的に切り替えることが可能となる．このことは向上させるセキュリティの信頼性とその対処に必要な処理時間のトレードオフになるため，状況に応じて柔軟に対処可能とする必要がある．本研究では，各構成要素の処理時間に関する性能評価を与えており，このトレードオフを解析するための基礎的な指標を与えたと考えられる．

- 無線ネットワークにおける受信者の移動

受信者がアクセスネットワークの変更を伴う移動を行い，移動先アクセスネットワークにおいて IGMP 加入要求を送信することがある．この場合，受信者は，KEK を既に保持しているため，AKDP のケース 3 もしくはケース 4 のいずれかが実行されることになる．AKDP によるネゴシエーション機能が存在しない場合には, 不必要な KEK の配信を常に実行することになるため, 受信者の移動による AKDP の利用は極めて有意義である．

- 匿名モデルと非匿名モデルの共存

ユーザ課金を必要とするサービスがある一方で，無料のデータ配信をする場合など，従来の IP マルチキャストによる匿名モデルで十分なサービスも存在する．AKDP ルータは，受信者が受信を所望するサービスが匿名モデルか非匿名モデルかの区別がつけば，それに応じて AKDP による受信者認証を利用するか否かを切り替えることが可能である．匿名モデルと非匿名モデルを区別する方法として，例えば，マルチキャストアドレスの A から B は非匿名モデル用に使用されるアドレス帯域とし，B＋1 から C までは匿名モデルに使用されるアドレス帯域とするなど，マルチキャストアドレスによりどちらのモデルを利用するかを定める方法が考えられる．このように，本章で提案した AKDP のアーキテクチャは匿名モデルと非匿名モデルの双方を収容出来るものとなっており，柔軟性があるシステムであるといえる．

5.6. 本章のまとめ

本章では, データ秘匿や受信者認証等のセキュリティを確保したマルチキャストのアプリケーションやサービスを提供するため，受信者認証グループ鍵配布プロトコル AKDP を提案した．また本章では，AKDP を用いるためのマルチキャストセキュリティアーキテクチャを提案した．AKDP は，これまでに解決されていなかった IP マルチキャストの課題を解決するために，１）データ秘匿のためのグループ鍵の配信，２）マルチキャスト DoS 対策のための受信者アクセス制御，３）マルチキャストグループへの在籍期間に同期した課金の 3 種類の機能を単一方式で実現することが可能である．AKDP ではこれら 3 つの機能のうち必要なものを選択して実行するネゴシエーション機能を提供し，状況に応じて必要な機能のみを提供する柔軟性の高い方式となっている．また，AKDP を実装し，その性能評価を行うことによって以下の結果が得られた．

- AKDP の処理時間は一番処理時間が長い場合においても 406 ミリ秒であり，マルチキャストのアプリケーションやサービスの提供に影響の無い程度に抑えることが可能である．

- AKDP の性能評価結果を用いた理論解析から，AKDP は，ネゴシエーション機能を用いない方式と比較して平均処理時間を 52%減らすことが可能である．また，受信者とアクセスルータ間の制御パケット数を 32%減らすことが可能である．従って，AKDP は，移動通信網等の無線通信のコストが高く遅延が大きいネットワークに有効である．

- AKDP の処理のうちボトルネックになる可能性が高いのは，認証＆鍵管理サーバの処理である．ただし，提案したマルチキャストセキュリティアーキテクチャは，複数の認証＆鍵管理サーバを収容することが可能であり，ユーザによって認証＆鍵管理サーバを切り替えることによりボトルネックの問題を解決することが可能である．

- AKDP ルータの処理時間は，認証＆鍵管理サーバの処理時間と比較すると小さくボトルネックにはならない．

- AKDP によりマルチキャストのセキュリティ機能を高めることが可能となったが，AKDP を手当たり次第に実行させることによりネットワークリソースに影響を与えることを目的とした DoS 攻撃手法への対処が依然として課題として残る．本課題に対処するためには，AKDP におけるトラヒックモニタリングによって DoS 攻撃を検出するなどの手法と組み合わせる必要がある．

なお，IP マルチキャストは古くから存在する技術であり，ネットワーク利用効率を飛躍的に向上させるものとして長い間注目されてきていたが，ビジネスモデルの構築方法に課題がありこれまで爆発的な普及には至らなかった．しかし近年になって，ネットワークの高速化とインフラの整備によりビジネス上の課題は徐々に改善されつつある．このように IP マルチキャストへの需要が高まる中，本章においてマルチキャストの技術的な課題の一つであるマルチキャストセキュリティの課題を整理してその解決方法を提示するとともに，実装システムを用いてその性能評価を行ったことは，今後の IP マルチキャストの実用化に向けた基礎技術を確立したものと位置付けられる．

5.6.1. 今後の検討課題

マルチキャストセキュリティに関する研究対象は非常に幅広く，例えば，DRM との連携が課題の一つとして考えられる．また，マルチキャストセキュリティについてはその適用するサービスやアプリケーション毎に求める要求条件が異なるものであり，その要求条件を満たすために必要な機能を提供するためのセキュリティポリシ制御等の課題がある．さらに，本章で取り上げなかったマルチキャストを用いたサービスのビジネスモデルの構築方法についても検討を行い，提案方式を実用化に結び付けることにより，マルチキャストの利用を高めることが本研究における最大の課題である．

第6章 モバイルマルチキャスト向けグループ管理プロトコルの提案とその性能評価

これまでに述べたように，公衆無線 LAN や移動通信網では，資源が限られた無線を利用するために有線ネットワークと比べて通信コストが高い．従って，無線共通チャネルを利用することにより多数の受信者に対してデータの同報配信が可能なマルチキャストを適用する例が近年になって増加している．例えば，3GPP では，移動通信網上の放送型データ配信技術である MBMS の標準化を行っている[50]．その他にも，IP マルチキャストを用いた動画像のストリーミング配信を公衆無線 LAN 上で実現したみあこキャスト[112]－[114]のような実用化例が存在する．以上のような放送型データ配信サービス実現への需要の高まりから，マルチキャスト技術を無線ネットワークに適用するためのモバイルマルチキャスト技術への要求が高まっている．

これに対して，マルチキャスト技術のモバイル環境への適用に関する多数の検討が行われてきた．これらの研究の多くは，グループメンバがアクセスネットワークの変更を伴って移動した際に生じる受信データの欠落を防止するためのルーティング方式を重点に検討が行われており，移動通信網や無線 LAN に適用可能なマルチキャストグループ管理プロトコルはあらかじめ与えられていることが暗黙の前提となっている．

しかし，IGMP 等の既存のマルチキャストグループ管理プロトコルを単純に移動通信網や無線 LAN に適用すると弊害が生じる．例えば，前章で指摘したように IGMP にはマルチキャスト DoS 攻撃が可能であるというセキュリティ上の問題があるため，前章で提案した AKDP のように受信者認証機能を提供する必要がある．また，IGMP を適用した場合，その制御パケットが通信コストの高い無線区間を流れることから，その通信量を低減する必要があるほか，電源断や移動によりメンバとの接続が突然途絶えた場合の対策も必要である．以上を踏まえ，本章ではモバイルマルチキャスト向けグループ管理プロトコル MMGP（Mobile Multicast Group Management Protocol）を提案する．

6.1. MMGP で解決すべき課題

マルチキャストのモバイル環境への適用に関しては，これまでに多数の研究が存在する．これまでの研究の多くは，受信者がアクセスネットワークの変更を伴って移動した際にも受信データの欠落を防止するモバイル向けマルチキャストルーティングに関するものである[115][116]．マルチキャストルーティングの実現方法は双方向トンネリングおよびリモートサブスクリプションの二種類が基本になっており，これらに対する様々な拡張方式が存在する[117] - [119].

しかし，モバイルマルチキャストに関するこれらの研究では，IGMP[10][11]等のマルチキャストグループ管理プロトコルをモバイル環境へ適用した場合について検討した研究例は少ない．例えば，文献[120]は，受信者が移動した際に移動先ネットワークにおいて送信する IGMP 加入要求や移動元ネットワークにおいて送信する IGMP 離脱要求を一つのメッ

セージにまとめることによりそのデータ量の削減を図る方法を提案している．しかしこの論文は，IGMP 問い合わせによる通信量増大の問題やセキュリティ機能についての考察がされておらずモバイル環境に適用するための検討が不十分である．この研究以外にはモバイル環境にマルチキャストグループ管理を適用することに着目した研究例は存在せず，本分野に関する研究は十分でないといえる．

以上のことから本章では，IGMP 等のマルチキャストグループ管理プロトコルをモバイル環境に適用した場合の課題を解決する新しいモバイルマルチキャスト向けグループ管理プロトコル（MMGP: Mobile Multicast Group Management Protocol）を提案する．以下では，IGMP をモバイル環境に適用した場合の課題を整理し，MMGP の要求条件を明らかにする．まず以下では，無線を利用した通信において考慮すべき課題について整理する．

- 無線区間の通信コスト

無線通信に利用可能な周波数は限られているため一般的に無線通信は有線通信と比較してコスト高である．従って，無線区間の通信量を低減することが重要である．さらに，携帯電話を受信者として利用する場合には，その処理能力（CPU，電源容量）に制限があるため，受信者におけるデータ送受信量を低減する必要がある．データ送受信量を低減することにより，受信者における通信処理を低減することが可能になるため，例えば携帯電話の待ち受け時間の延長を図ることが可能となる．

- 受信者の移動等

移動通信においては，突然の電源断や移動に伴う受信者の圏外流出が発生する可能性がある．このことにより，例えば IGMPv3 のようにアクセスルータが受信者の状態（アクセスネットワークの在籍状況等）を管理する場合には，そのアクセスルータと受信者のそれぞれが保持する状態情報の不一致が発生する可能性がある．また，発生した状態不一致の状態（準正常系）を検出し，準正常系から正常系に復帰するまでに本来不必要な通信が発生する可能性がある．

以上の特徴を考慮すると，IGMP をモバイル環境に適用した場合にいくつかの課題が明らかになる．以下では，これらの課題について整理し，MMGP に求められる要求条件について述べる．

① メッセージの連送による不要な通信を削減

IGMP では，加入要求等の各種メッセージに対する確認応答が存在しないため，メッセージの欠落による未到達が検出不可能となる場合がある．そこで，同じメッセージを複数回連送する（IGMP の Robustness-Variable では 2 回がデフォルト）ことでメッセージ未到達の確率を抑制している．しかし，この対処により無線区間の通信量を不要に増大させる要因となるため，MMGP ではメッセージの連送を必要としないグループ管理方式を検討する必要がある．

② IGMP 問い合わせによる受信者処理量の削減

IGMP では，IGMP 問い合わせにより定期的にメンバの存在確認を行う．IGMP 問い合わせには，グループ特定問い合わせと全ての受信者を対象とする一般問い合わせが存在し，いずれも多数の受信者がこれを処理する必要があるため，受信者が電源容量に制限のある携帯電話である場合は待ち受け時間低下の要因となる．従って MMGP では，問い合わせによる通信の影響を最低限のメンバのみに抑えることで受信者全体の処理量を低減する必要がある．

③ メンバの移動による通信発生を低減

IGMPv3 では，アクセスルータが全てのメンバの加入状況を管理する．従ってアクセスルータは，メンバからの離脱要求受信時にグループ指定問い合わせを送信せずに当該メンバの状態情報を削除する機能（Fast Leave）が利用可能である．しかし，モバイル環境では，メンバが離脱要求を送信せずに他のアクセスネットワークに移動してしまう可能性がある．このため，この Fast Leave 機能が有効に働かず，状態不一致を解消するための通信がさらに必要となる懸念がある．従って，MMGP では，メンバの移動が頻繁に発生するモバイル環境においても柔軟に対処できる必要がある．

④　マルチキャスト DoS への対処

IGMP では，第 5 章で述べたように，任意の受信者がデータ受信の開始を要求出来るため，手当たり次第にグループに加入し，マルチキャスト配信経路を不必要に構築するマルチキャスト DoS の問題が存在する．マルチキャストグループからの離脱に際しても不必要な通信処理を発生する同様な問題が存在する．特にモバイル環境においては，受信者が直接ケーブル等で接続されておらず，問題を発生させた受信者を特定することが難しいため，マルチキャスト DoS への対処は特に重要である．MMGP では，文献[111]に紹介されるマルチキャスト DoS 対策と同様に，マルチキャストグループに加入する最初のメンバと，マルチキャストグループから離脱する最後のメンバについて受信者認証を行い，その正当性を判断する必要がある．

MMGP では，以上に説明した各種要求条件を満たす必要がある．次節では，MMGP の詳細について説明する．

6.2.　MMGP の提案

本節では，6.1節に説明した要求条件を満たす新しいモバイルマルチキャスト向けグループ管理プロトコル MMGP の詳細を説明する．

マルチキャストでは，配信を希望するメンバが配下に存在すれば，その数が何台であったとしても，アクセスルータは配信データの中継を行う必要がある．このため，マルチキャストグループ管理プロトコルの本来の目的は，このようなメンバがアクセスルータ配下に存在するか否かを把握できる機能を提供することだと言える．

MMGP ではこの点に着目し，メンバの中から選択した 1 台以上のメンバのグループ在籍状況をアクセスルータにおいて集中的に管理する．そして，選択したメンバを識別するためにトークンを用いる方法を提供する．MMGP の動作の概要は以下のとおり．

- MMGP ルータ（MMGP をサポートしたアクセスルータ）は選択した 1 台以上のメンバに対してトークンを与え，これらのメンバ（トークンメンバと呼ぶ）のグループ在籍を定期的に確認するなどの厳密な管理を行う．つまり MMGP ルータは，確認応答を伴うユニキャストによりトークンメンバの在籍確認を行うことで，IGMP で問題であったメッセージの連送や問い合わせ処理の問題を解決する（要求条件①②の対処）．

- MMGP では，最低 1 台のメンバにトークンを与える．これにより，最初にマルチキャストグループに加入するメンバ，およびマルチキャストグループから最後に離脱する（可能性がある）メンバ（マルチキャストグループに他のメンバがいない状態のメンバ）は必然的にトークンメンバとなる．

- トークンを与えられないメンバ（非トークンメンバと呼ぶ）の状態管理は重要ではないため，MMGP ルータは，非トークンメンバのグループへの加入や離脱を把握する必

要がなく，例えば非トークンメンバが移動により他のサブネットワークに移動した場合や，電源断等により突然通信ができなくなった場合でも特に処理は行わない．以上により，非トークンメンバの移動に伴う通信を削減する（要求条件③の対処）．

- 全てのトークンメンバが離脱した場合には，非トークンメンバを選択して，これにトークンを再割り当てする．

- MMGP ルータは，トークンメンバが配下に存在する限りマルチキャスト配信データの中継を行う．トークンメンバが存在するということは当該マルチキャストアドレスの配信データを受信するメンバが最低 1 台存在することを意味するためである．

- MMGP では，トークンメンバの加入時および離脱時に受信者認証を実行する．これは，最初にグループに加入するメンバ，および最後にグループから離脱するメンバは必ずトークンメンバになるという点に着目したものである．これによってマルチキャスト DoS 対策が可能となる．（要求条件④の対処）．

次節以降では，以上で説明した MMGP の基本動作の詳細について説明する．

6.2.1. MMGP 詳細

本節では，MMGP の詳細について通信シーケンスを用いた具体例を用いて説明する．

1. トークンメンバの加入（MMGP Join）

受信者が最初にマルチキャストグループに加入する際には，以下に示すトークンメンバの加入手続きが実行される（図6.1）．①受信者が MMGP Join Request を送信すると，MMGA ルータは，当該マルチキャストグループに加入しようとする最初のメンバであることが分かる．ここで，MMGP ルータがマルチキャスト DoS 対策を必要とする場合には，②③に示す受信者認証手続きを実行しても良い．なお，本図中の点線はその実行がオプションであることを示している．受信者認証ではチャレンジ認証もしくは電子証明書による認証を選択し，MMGP ルータが受信者に対して要求する（②Authentication Request）．これに対して，受信者は MMGP ルータからのチャレンジ値に対するレスポンス値，もしくは電子証明書を返す（③Authentication Response）．以上の動作により，MMGP ルータは，受信者認証が可能となる．受信者認証が必要か否かは MMGP ルータが判断し，必要な場合に②Authentication Request を送信することで受信者は受信者認証が必要であることを認識することが出来る．

次に，④受信者に対してトークンを付与する．トークンに対して電子証明書を付加することにより，受信者は，MMGP ルータが発行したトークンであることの検証が可能となる．その後，トークンが到達したことを MMGP ルータに伝えるため，受信者は⑤送達確認（ACK）を送信する．

なお，MMGP ルータは，①の MMGP Join Request の受信，もしくは③の受信者認証完了後，必要に応じてマルチキャストツリーの構築を行い，マルチキャストデータの中継を開始する．以上に説明したトークンメンバの加入に関する一連の通信は全てユニキャストで実行される．

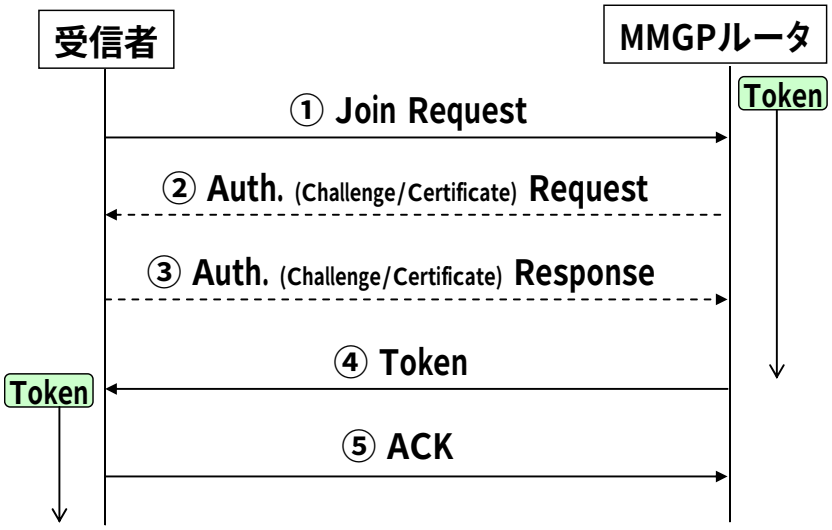


図6.1 トークンメンバの加入（MMGP Join）手続き

2. 非トークンメンバの加入（MMGP Join）

他のメンバが既に存在するマルチキャストグループに受信者が加入する場合には，非トークンメンバの加入手続きが実行される（図6.2）．①受信者は，図6.1における加入手続きと同様に MMGP Join Request を送信する．MMGP ルータは，本メッセージを受信した時点で 2 番目以降のメンバ（つまり非トークンメンバ）の加入要求であることが判断可能なため，この時点で処理は終了する．なお，受信者は，既に当該マルチキャストグループ宛のデータの受信を検出するなど，何らかの方法で既にマルチキャストグループに加入しているメンバが他に存在するということが検出可能であれば, MMGP Join Request の送信を省略出来る．つまり非トークンメンバに関しては MMGP Join Request の送信は必ずしも必要ではない．ただし，他のメンバがマルチキャストグループに加入しているか否かは，当該マルチキャスト配信データの受信で検知するのが典型であるため，基本的に MMGP Join Request の送信は全ての受信者で必要とされる機能である．なお，以上に説明した非トークンメンバの加入に関する一連の通信は全てユニキャストで実行される．

図6.2 非トークンメンバの加入（MMGP Join）手続き

3. 非トークンメンバの離脱（MMGP Leave）

非トークンメンバである受信者は，①MMGP Leave Request をユニキャストで送信することでマルチキャストグループから離脱する（図6.3）．MMGP ルータは，非トークンメンバの離脱の把握が必ずしも必要無いため，本メッセージは省略することも可能である．

図6.3 非トークンメンバの離脱（MMGP Leave）手続き

4. トークンメンバの離脱（MMGP Leave）

トークンメンバがマルチキャストグループから離脱する際には，以下に示すトークンメンバの離脱手続きが実行される（図6.4）．①受信者は，先に受信していたトークンを MMGP Leave Request メッセージ中に付加して MMGP ルータに送信する．MMGP ルータは受信したトークンを確認し，自分で発行したものかどうかの検証を行う．ここで，マルチキャスト DoS 対策の必要性に応じ，②③受信者認証手続きを実行しても良い．なお，離脱時のトークンメンバ認証は，トークンメンバの加入時の認証よりも重要性が低い．MMGP ルータは，トークンに対して電子署名を付加することにより，自身が配布したトークンであるか否かの検証が可能であるため，受信者を認証せずともかつて自身がトークンメンバ加入手続きに認証したことを判定可能であることがその原因である．

最後に，④トークンを受信したことを示す OK メッセージを返信する．なお，以上に説明したトークンメンバの離脱に関する一連の通信は全てユニキャストで実行される．

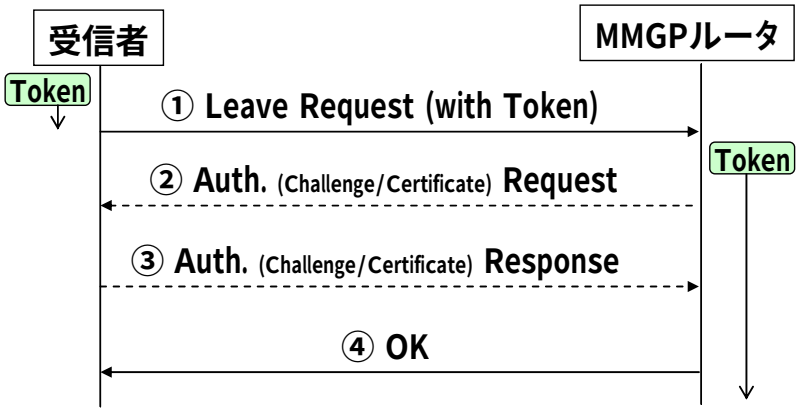


図6.4 トークンメンバの離脱（MMGP Leave）手続き

5. トークン再割り当て

MMGP では，最低 1 台のメンバに対してトークンを付与することが原則であるため，トークンメンバの離脱が発生した場合には，トークンを他のメンバに再割り当てする必要がある（図6.5）．MMGP ルータは，トークン再割り当てが必要だと判断すると，①メンバが加入しているマルチキャストグループに対して MMGP Query メッセージを送信する．②それを受信した各メンバは MMGP Join Request を送信することでメンバとして在籍していることを MMGP ルータに対して伝える．MMGP ルータは，MMGP Join Request を受信したメンバの中から 1 台をトークンメンバとして決定するが，③④この際マルチキャスト DoS 対策が必要な場合には，受信者認証処理を実行しても良い．⑤⑥そして，決定したメンバに対して図6.1と同様にトークン付与のための手続きを行う．なお，残存メンバが存在しない場合には，MMGP Join Request を送信する受信者が存在しないため，MMGP ルータは MMGP Join Request 待ちタイマの満了を待ってマルチキャスト配信の中継を停止す

る．なお，以上に説明したトークン再割り当てに関連する一連の通信は，MMGP Query のみがマルチキャストで実行され，それ以外の一連の通信は全てユニキャストで実行される．

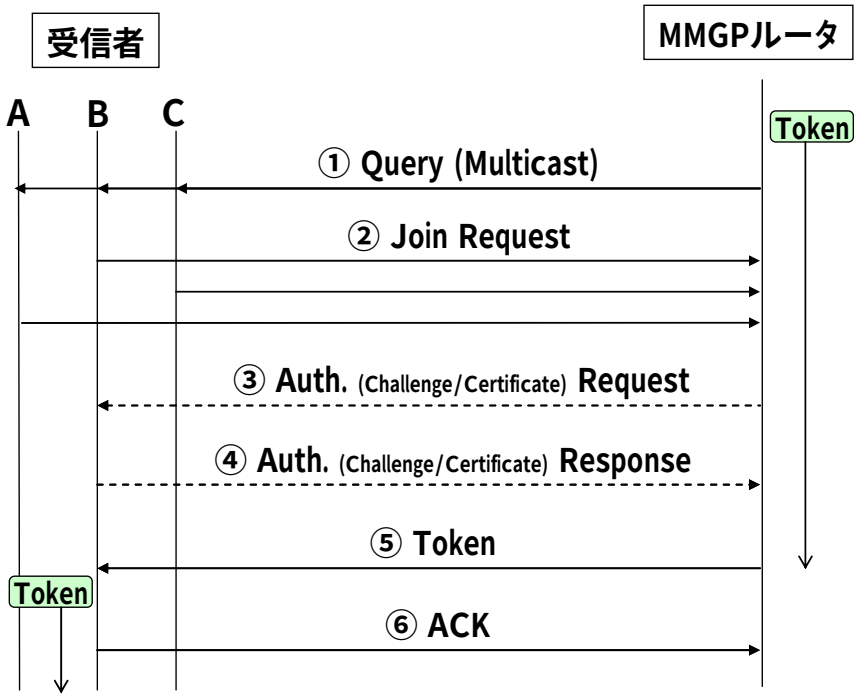


図6.5 トークン再割り当て手続き

6. トークンメンバの在籍確認（Hello）

MMGP では，トークンメンバのグループ在籍状況を把握するために定期的にトークンメンバの在籍確認を行う（図6.6）．①MMGP ルータは，定期的に MMGP Hello メッセージをトークンメンバに対して送信する．②それに対して受信者は，MMGP Hello ACK によって在籍していることを MMGP ルータに伝える．以上の MMGP Hello と MMGP Hello ACK はユニキャストを用いて通信される．MMGP ルータは，MMGP Hello メッセージ待ちタイマの満了を持ってトークンメンバの不在を検知することが可能であり，その後，図6.5に示すトークン再割り当て手続きを実行する．

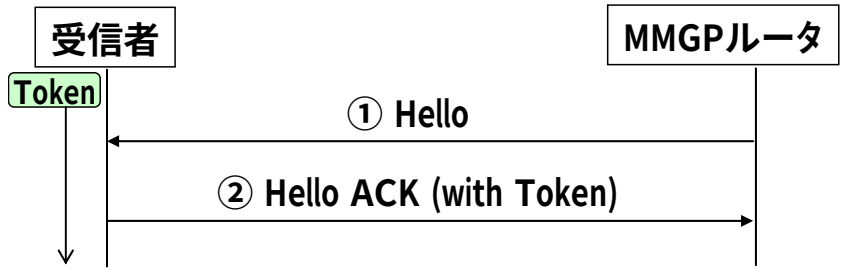


図6.6 トークンメンバの在籍確認（Hello）

6.3. MMGP の評価

本節では，ns[61]を用いたネットワークシミュレーションにより MMGP と，IGMP の二種類のバージョン（IGMPv2 と IGMPv3）を比較し，提案方式の有効性を評価する．このとき，評価する項目は以下の二項目である．

- 通信に必要な制御パケット数
  MMGP/IGMP の通信に要する制御パケット数を測定することにより MMGP/IGMP の処理に必要な通信量の評価を行う．特に無線を用いたネットワークにおいて MMGP/IGMP を適用する場合には，制御パケット数とその方式に必要となる通信コストが比例するため，制御パケット数がより少ない方式がモバイル向けマルチキャストグループ管理プロトコルとして優れていると考えることができる．

- 受信者の送受信パケット数
  受信者における MMGP/IGMP の送受信パケット数を比較する．受信者におけるパケットの送受信には CPU による処理やメモリの利用が伴うため，これにより受信者が利用する端末の電力を消費する．消費電力を低くすることは，例えば，受信者に携帯電話を用いる場合の待ち受け時間の改善につながることから，送受信パケット数が少ないほうがモバイル向けマルチキャストグループ管理プロトコルとして優れている方式と考えることができる．

以上の二項目の評価をするに当たり，利用するネットワークとして以下の二種類を想定する．

- 有線ネットワーク
  IGMP は，当初有線ネットワーク（以下では，イーサネット等のケーブルを用いて通信を実現するネットワークで構成する LAN を想定する）を対象に設計されており，逆に MMGP が有線ネットワークに適用すると障害が発生するのかどうかを確認する必要がある．そこで，評価に用いるネットワークの一つとして，有線ネットワークを採用する．この有線ネットワークにおいては，マルチキャストデータはサブネットワーク上の全ての受信者において受信可能であり，例えば，ある受信者が送信した IGMP 加入要求や IGMP 離脱要求は，サブネットワーク上の他の受信者が受信可能であると仮定する．

- 無線ネットワーク（移動通信網，無線 LAN 等）
  MMGP はモバイルマルチキャスト向けに設計されていることから，評価に用いるネットワークのもう一つとして，無線ネットワーク（以下では，移動通信網や無線 LAN 等の無線のネットワークで構成する LAN を想定する）を採用する．例えば，移動通信網の場合には，アクセスルータから送信されたマルチキャストデータは，無線共通チャネルを用いることによりサブネットワーク上の全ての受信者で受信可能である．逆に受信者が送信したマルチキャストデータは，無線基地局が最初に受信し，無線基地局は受信したデータを単にアクセスルータに中継するのみであるため，受信者が送信したマルチキャストデータを他の受信者が受信することは無い．つまり，無線ネットワークでは，受信者が送信した IGMP 加入要求や IGMP 離脱要求は他の受信者が受信することは不可能である．なお，無線 LAN の場合には受信者が送信したマルチキャストデータは，受信者が発した電波を他の受信者が直接受信することもある．しかし，無線 LAN における隠れ端末問題の要因と同様に，送信者から距離の離れた受信者においては当該データの受信ができない場合も存在する．従って，本節では，無線 LAN の例の場合にも移動通信網と同

様に考え，ある受信者が送信したマルチキャストデータが他の受信者によって受信できない状況を想定することにする．

そして，受信者の移動状況を考慮し，以下の二点について評価を行う．

- 受信者が移動しない状況
  有線ネットワークにおいては，受信者はケーブルを通じて接続されるため，受信者の移動を考慮する必要性は少ない．また，無線ネットワークにおいても，無線基地局を受信者が集まるような場所（喫茶店等）に設置するようなスポット的な利用においては，受信者が移動することにより単に圏外になってしまうため，サブネットワークの変更を伴わない場合も考えられる．そこで本節では，受信者が移動しない状況を考慮し，その場合の MMGP と IGMP の評価を行う．

- 受信者が移動する状況
  無線ネットワークにおいては，受信者はケーブルを通じて接続されていないため，通信を行ったままサブネットワークの変更を伴う移動を考慮する必要性がある．従って，本節では, 無線ネットワークに限り, 受信者が移動した状況を考慮し, その場合の MMGP と IGMP の評価を行う．

  なお，性能評価実験における条件は以下のとおりである．

- 1 台の MMGP ルータで構成するサブネットワーク中に複数の受信者が存在する状況を想定し，受信者数は 1 台から 200 台の範囲で変化させて測定を行う．MMGP ルータと受信者間は IGMP や MMGP によるマルチキャストグループ管理プロトコルを動作させる．

- 評価実験では，送信者は 30 分間のデータ配信を行う．受信者は，配信開始前の 5 分間にマルチキャストグループに加入し，データ配信完了後の 5 分間で当該マルチキャストグループから離脱する．5 分間のマルチキャストグループへの加入と，5 分間のマルチキャストグループからの離脱は偏ることなく一様な間隔で行う．

- 受信者が各サブネットワークに滞在する時間は平均 10 分または平均 1 分の指数分布に従う．滞在時間後，サブネットワークの変更が生じる．仮に 1Km のセル半径で構成される円形のエリアを想定した場合に，10 分でこのセルに流入してから流出するには時速約 9Km，1 分の場合には時速約 94Km で移動する必要がある．実際には郊外でのセル半径は数 Km になるため，本条件は移動通信網における移動環境の想定として十分な速度であると言える．

- 制御パケット数の比較において，ユニキャストおよびマルチキャストのいずれで送受信された場合でも，制御パケットは一つにつき一個と数える．これは，無線ネットワークでは共通チャネルを利用することから，マルチキャストはユニキャストと同じ電波リソースを占有するためである．また，以下で示す測定結果では，アクセスルータと受信者で送信した全ての制御パケット数の合計のみを示す．

- 送受信パケット数についても，ユニキャストおよびマルチキャストのいずれで送られた場合でもパケットは一つにつき一個として数える．例えば，n 台の受信者を対象にマルチキャストでのデータ配信を行った場合には, 受信者の受信パケット数は合計 n 個となる．また，以下で示す測定結果では，受信者全ての送受信パケット数の合計数のみを示す．

- 受信者が移動する際には移動元のサブネットワークに対してIGMP離脱要求やMMGP Leave 等のメッセージを送信しないものとする．また，移動先のサブネットワークにおいては，他のメンバが必ず存在するものと仮定し，IGMP 加入要求や MMGP Join Request を送信せずともデータ受信を再開することが可能である状況を想定する．

- 受信者が移動する際にはサブネットワークから受信者が隣接するサブネットワークへ移動するのと共に隣接するサブネットワークから当該サブネットワークに流入する受信者も存在するものとして想定する．従って，一時的に受信者数の変化はあるもののトータルで考えた場合のサブネットワーク内に在籍する受信者数は一定である．

MMGP では，さらに以下の条件を仮定している．

- 非トークンメンバの MMGP Leave Request は実行されないものとする．6.2.1節に説明したように MMGP Leave Request については省略可能である．

- MMGP と IGMP の同等機能提供時の評価を行うため, IGMP が提供していない受信者認証手順を MMGP でも使用しない．

- MMGP における受信者へのトークンの割り当てはランダムに行う．

- MMGP Hello は IGMP における一般問い合わせと同等機能を提供するため，MMGP Hello 間隔を IGMP の一般問い合わせ間隔のデフォルト値と同じ 125 秒とする．

6.3.1. 制御パケット数の比較

まず，通信に必要な制御パケット数の比較を行う．

- 有線ネットワークにおける制御パケット数の比較
  図6.7に，有線ネットワークにおける各グループ管理プロトコルで送られた制御パケット数を示す．有線ネットワークにおいては IGMPv2 の制御パケット数が一番少なく，IGMPv3 の制御パケット数が一番多い．IGMPv3 では，全ての受信者が IGMP 加入要求と IGMP 離脱要求を送信し, さらに IGMP 加入要求は IGMP 問い合わせ発生毎に必要とするため，制御パケット数が受信者数に比例して増加する．それと比較して，IGMPv2 では Suppress 機能により IGMP 問い合わせ後の IGMP 加入要求は最低一台のメンバが送信すればよく，また，IGMP 離脱要求を全ての受信者が送信する必要がないため制御パケット数が IGMPv3 と比較して少ない．MMGP においても，最初の MMGP Join Request はトークンメンバ, 非トークンメンバのいずれも送信するが, ユニキャストを用いる MMGP Hello を用いてトークンメンバに対してのみ在籍確認を行っているため IGMPv3 ほど制御パケット数は必要としない．MMGP が IGMPv2 と比較して制御パケット数が僅かに上回っている理由は，MMGP ではトークン再割り当てに MMGP Query とその後の MMGP Join Request が必要となり，これらの分の制御パケット数が増加するためである．

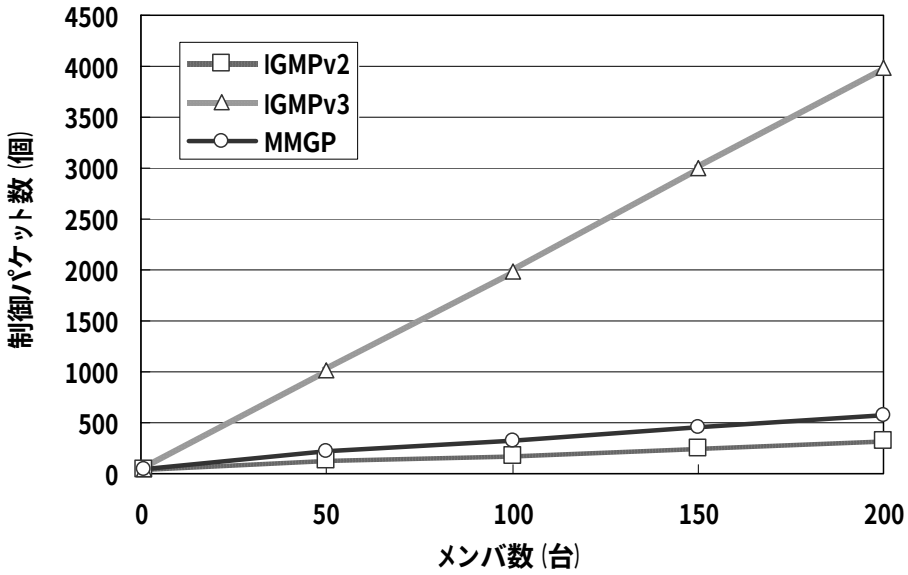


図6.7 有線ネットワークにおける制御パケット数の比較

- 無線ネットワークにおける制御パケット数の比較（移動無し）

  図6.8に，受信者の移動を考慮しない場合における無線ネットワークにおける制御パケット数を示す．無線ネットワークにおいては，MMGP の制御パケット数が一番少なく，IGMPv2 の制御パケット数が一番多い．無線ネットワークにおいては，IGMP 加入要求が他の受信者によって受信されないため，結果的に IGMP 加入要求と IGMP 離脱要求が全ての受信者によって送信されることがその原因である．これは IGMPv2，IGMPv3 のいずれにおいても共通である．ただし IGMPv2 の場合には Fast Leave 機能を持たないため, IGMP 離脱要求後に IGMP グループ特定問い合わせが発生し, それがさらに IGMP 加入要求を発生させる要因になっている．従って，IGMPv2 は，IGMPv3 と比較しても制御パケット数が多くなっている．これに対して MMGP では，MMGP Hello を用いてトークンメンバに対してのみ在籍確認を行っているため制御パケット数の増加を抑えることが可能である．

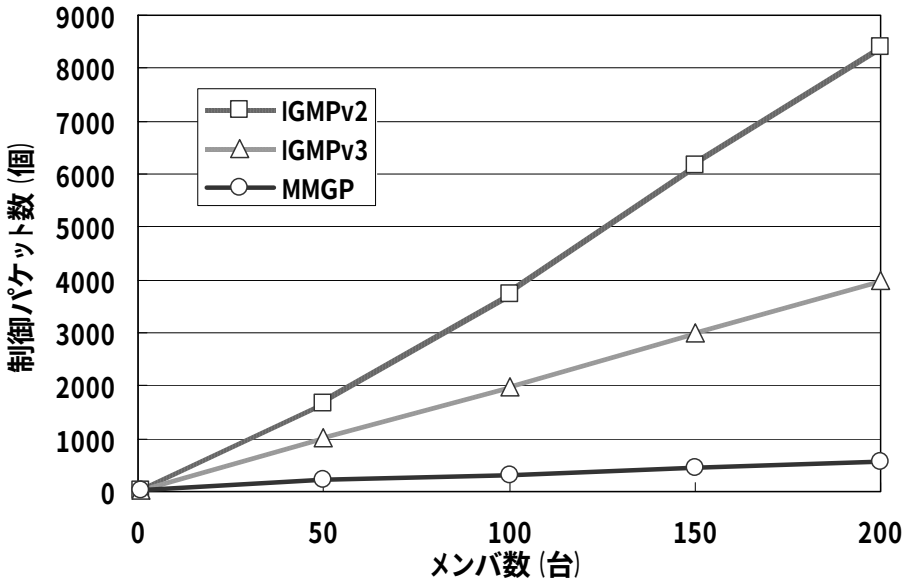


図6.8 無線ネットワークにおける制御パケット数の比較（移動無し）

- 無線ネットワークにおける制御パケット数の比較（移動有り）

図6.9に，受信者が平均滞在時間 10 分でセルを移動する無線ネットワークでの制御パケット数を示す. IGMP では, いずれのバージョンにおいても, 受信者が移動しない図6.8と比較して，制御パケット数の変化は少ないことが分かる．これは，受信者が他のサブネットワークに移動するのと同時に，他のサブネットワークからも移動する状況を考慮していることがその要因である．つまり，IGMP の制御パケット数は受信者の移動には関係なく，単にアクセスルータ配下の受信者数に依存することが原因となっている．これに対して MMGP では, トークンメンバが移動することに発生するトークン再割り当てに通信が必要であるため，受信者が移動しない状況と比較した場合に，制御パケット数が増加している．ただし，トークンメンバはメンバの中の代表者 1 台のみが指定されるため，トークンメンバの移動によるトークン再割り当ての影響は少ない．評価結果から見ても，MMGP は，IGMPv2 や IGMPv3 と比較して制御パケット数は少ないことが分かる．

図6.10に，受信者が平均滞在時間 1 分でセルを移動する無線ネットワークでの制御パケット数を示す. IGMP では, いずれのバージョンにおいても, 受信者が移動しない図6.8と比較して，制御パケット数の変化は少ないことが分かる．MMGP においては受信者の移動傾向が強まるとそれに合わせてトークン再割り当てにより制御パケット数が増加するが, このように受信者が頻繁に移動する状況においても IGMPv2 や IGMPv3 と比較して制御パケット数は少ないことが分かる．

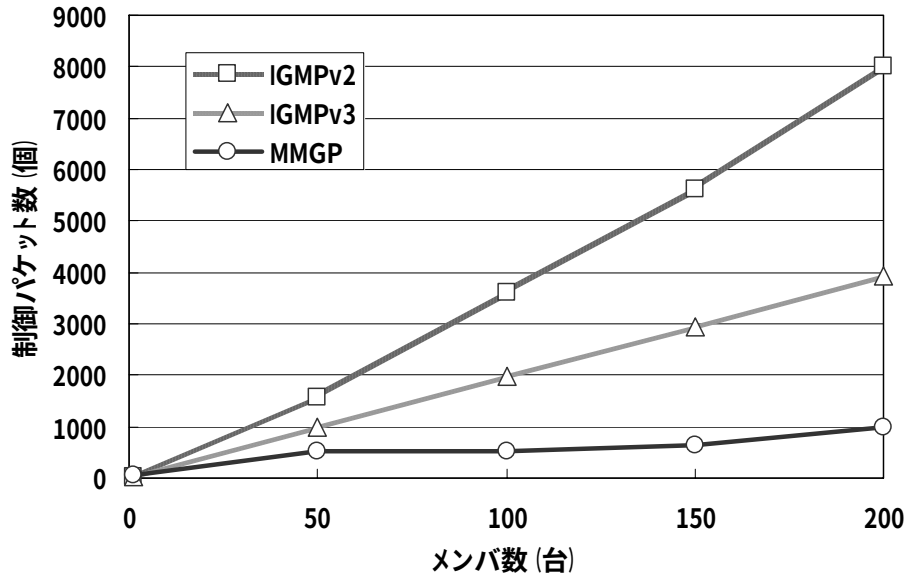


図6.9 無線ネットワークにおける制御パケット数の比較（移動有り：平均滞在時間 10 分）

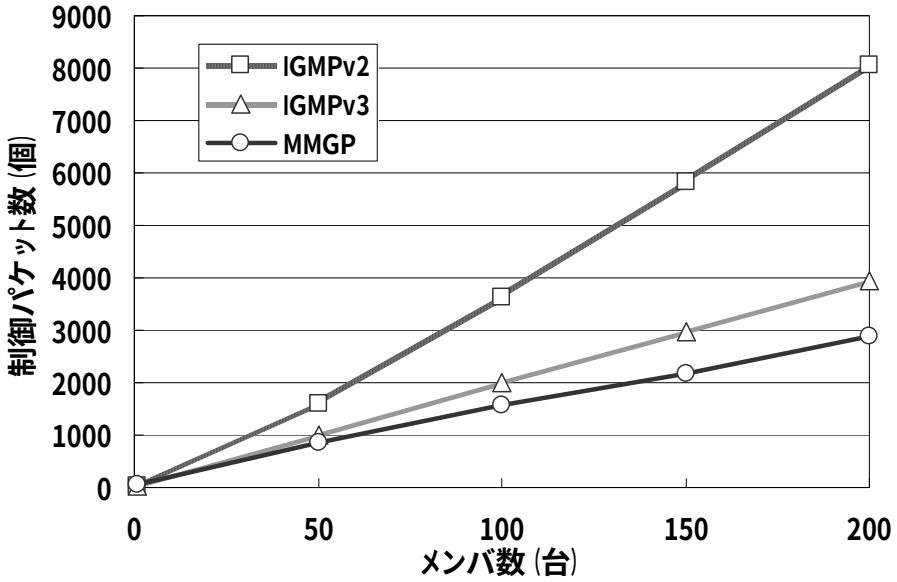


図6.10 無線ネットワークにおける制御パケット数の比較（移動有り：平均滞在時間 1 分）

6.3.2. 受信者の送受信パケット数の比較

次に，受信者における送受信パケット数を比較することにより，MMGP と IGMP における消費電力への影響の評価を行う．

- 有線ネットワークにおける受信者の送受信パケット数

  図6.11に，有線ネットワークにおける受信者の送受信パケット数を示す．有線ネットワークにおいては，IGMPv2 と IGMPv3 の送受信パケット数が多く，MMGP の送受信パケット数は少ない．また，受信者数が少ない状況では IGMPv2 の送受信パケット数は

IGMPv3 と比較して少ないが，受信者数が増加すると IGMPv2 の送受信パケット数が IGMPv3 よりも多い．この理由は，IGMPv2 では，受信者数が増加するにつれて受信者のグループ離脱時に発生するグループ特定問い合わせによる受信パケット数の増加傾向が強まるからである．これに対し IGMPv3 ではグループ特定問い合わせが存在しないため，受信者数増加による影響は IGMPv2 ほど大きくない．IGMP の送受信パケット数に対し MMGP の送受信パケット数が少ない理由は，MMGP では，トークン再割り当て時以外にはユニキャストを用いて基本的に通信を行うため，通信を必要とするのは通信対象となる受信者のみであることが影響している．以上のことから，MMGP により受信者の送受信パケット数を減らす効果があることが分かる．

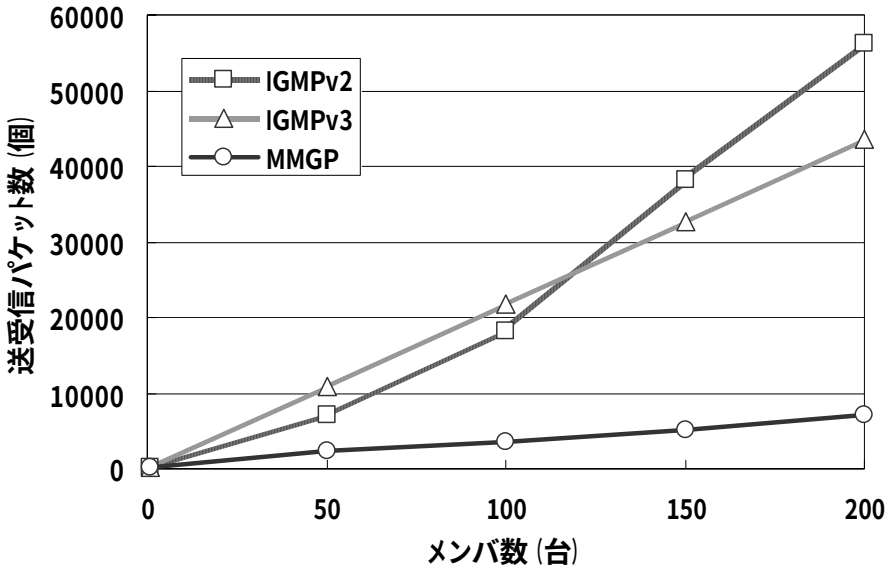


図6.11 有線ネットワークにおける受信者の送受信パケット数の比較

- 無線ネットワークにおける受信者の送受信パケット数（移動無し）

図6.12に，無線ネットワークにおける受信者の送受信パケット数を示す．無線ネットワークにおいても，IGMPv2 と IGMPv3 の送受信パケット数は多く，MMGP の送受信パケット数は少ないという傾向は図6.11と同様である．IGMPv2 の送受信パケット数が IGMPv3 の送受信パケット数と比較して多いのは，IGMPv2 には IGMPv3 で提供されている Fast Leave 機能が無いためである．Fast Leave 機能の有無が無線ネットワークにおける送受信パケット数の差に大きく表れることが分かる．

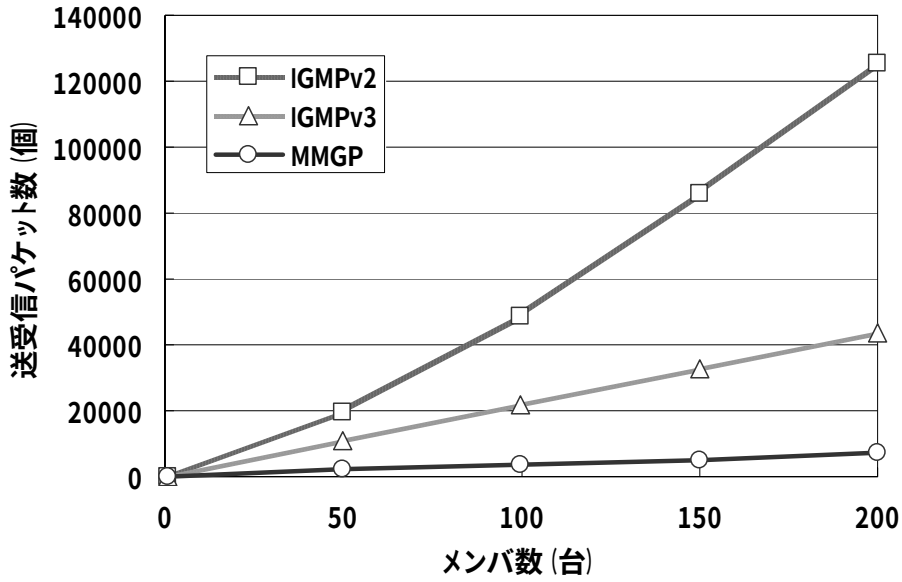


図6.12 無線ネットワークにおける受信者の送受信パケット数の比較（移動無し）

- 無線ネットワークにおける受信者の送受信パケット数（移動有り）

図6.13に，受信者が平均滞在時間 10 分でセルを移動する無線ネットワークにおける受信者の送受信パケット数を示す．IGMP では，いずれのバージョンにおいても，受信者が移動しない図6.12と比較して，受信者の送受信パケット数の変化は少ないことが分かる．これは，受信者が他のサブネットワークに移動するのと同時に，他のサブネットワークから移動する状況を考慮していることがその要因である．つまり，IGMP パケットの送受信数は受信者の移動には関係なく，単にアクセスルータ配下の受信者数に依存することが原因となっている．これに対して，MMGP では，トークンメンバが移動することにより発生するトークン再割り当てに通信が必要であるため，受信者が移動しない状況と比較した場合に，送受信パケット数が増加している．なお，このような状況においても IGMPv2 や IGMPv3 と比較して送受信パケット数は少ないことが分かる．

図6.14に，受信者が平均滞在時間 1 分でセルを移動する無線ネットワークにおける受信者の送受信パケット数を示す．IGMP では，いずれのバージョンにおいても，受信者が移動しない図6.12と比較して, 送受信パケット数の変化は少ないことが分かる. MMGP においては受信者の移動傾向が強まるとトークン再割り当てにより送受信パケット数が増加するが, 受信者が頻繁に移動する状況においても IGMPv2 や IGMPv3 と比較して送受信パケット数は少ないことが分かる．

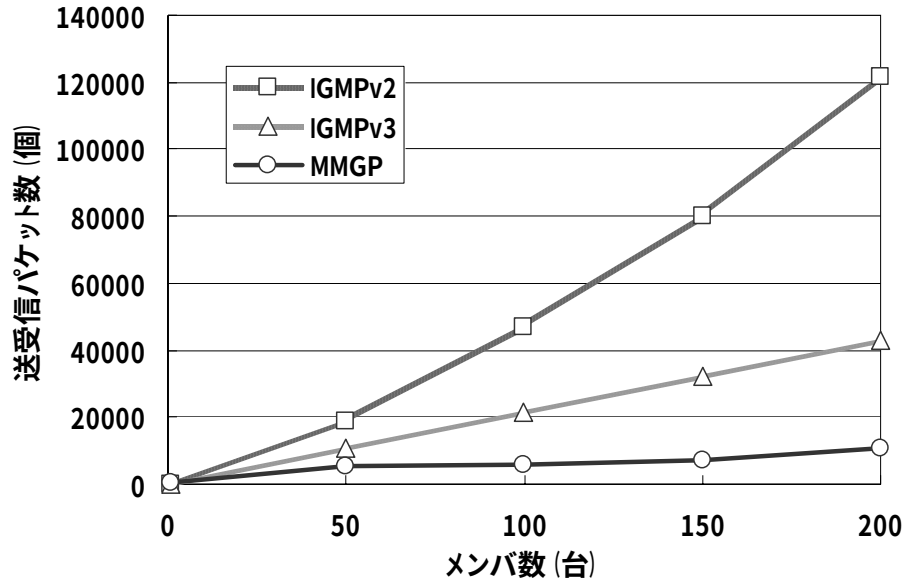


図6.13 無線ネットワークにおける受信者の送受信パケット数の比較（移動有り：平均滞在時間 10 分）

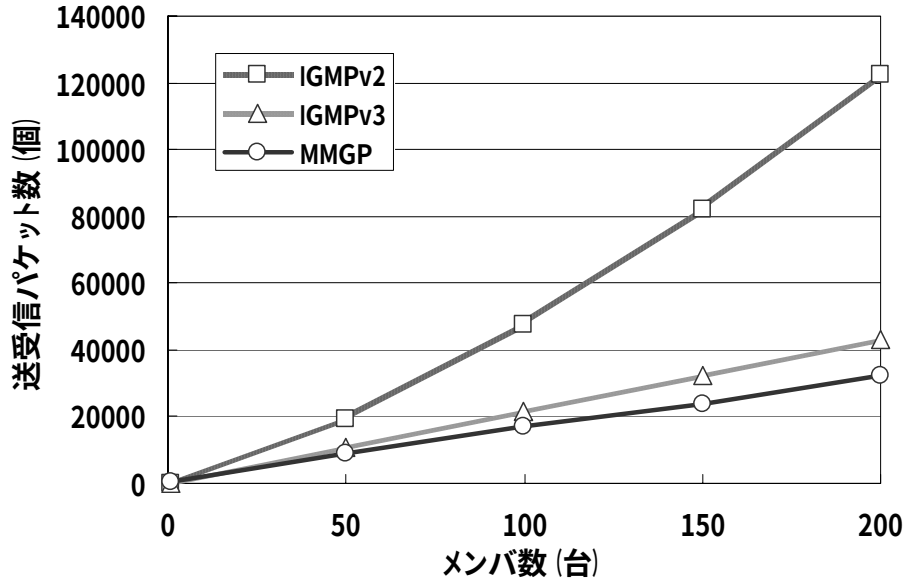


図6.14 無線ネットワークにおける受信者の送受信パケット数の比較（移動有り：平均滞在時間 1 分）

6.4. MMGP の考察

以下では，6.3節の評価結果を踏まえ，MMGP に関して考察する．

- MMGP の制御パケット数（通信量）に関する考察

MMGP は，アクセスルータ配下に最低 1 台のメンバが存在するか否かを把握するという本来のマルチキャストグループ管理の目的に沿って設計されたプロトコルであり，トークンを利用して 1 台のメンバの管理を厳密に行うことで効果的なグループ管理を実現している．そのため MMGP は，有線ネットワークにおいては IGMPv2 より制御パケット数が多いものの，無線ネットワークにおいては IGMP のいずれのバージョンよりも少ないパケット数でグループ管理が可能であることを示した（6.1節の要求条件①）．

IGMPv2 は，LAN 等の有線のネットワークにおいては，MMGP よりも少ない制御パケット数でグループ管理が可能であることを確認したが，無線ネットワークにおいては，制御パケット数が著しく増加する傾向にあることが確認できた．これは，無線ネットワークでは，アクセスルータから受信者への下り通信のみマルチキャスト配信データが全ての受信者において受信可能であるが，受信者からアクセスルータへの上り通信ではマルチキャストデータは他の受信者で受信できないということが要因になっており，IGMPv2 を無線ネットワークに適用するには課題があることを確認した．

IGMPv3 は，有線ネットワーク，無線ネットワークのいずれに適用してもその制御パケット数の変化は無いことを確認した．また，IGMPv3 は，MMGP と比較して全ての場合において制御パケット数が多いことを確認した．ただし，IGMPv3 はアクセスルータにおいて全ての受信者を管理する機能を持っており，それについては MMGP では保持していない機能である．従って，アクセスルータにおいて全ての受信者の管理が必要な場合においては MMGP の代わりに IGMPv3 を適用する必要があるが，そのことによる制御パケット数の増加を考慮する必要がある．

- 受信者の送受信パケット数（消費電力）に関する考察

MMGP では，トークンメンバの離脱を原因とするトークン再割り当てに用いる MMGP Query にのみマルチキャストを用いるが，その他の全ての制御メッセージはユニキャストを用いて通信を行う．従って，MMGP は有線ネットワーク，無線ネットワークの全てのケースにおいて IGMP と比較して少ない送受信パケット数でグループ管理の実現が可能である．つまり，MMGP は，受信者全体を考慮した際の送受信パケット数の低減を図ることが可能であり，受信者が使用する端末の消費電力を低減することが可能である（6.1節の要求条件②）．

IGMPv2 と IGMPv3 のいずれも，全ての制御メッセージはマルチキャストアドレスを宛先としてやり取りされる．特に IGMP 一般問い合わせは，サブネットワーク中の受信者全てがその受信対象であるために，受信者全体の送受信パケット数が増加する原因となっており，受信者が使用する端末の消費電力に影響があることが課題である．特に電源容量の制限が厳しい携帯電話を受信者として用いた場合には，その待ち受け時間への影響が無視できなくなる．

- 受信者の移動に関する考察

MMGP では，受信者の移動によりトークンの再割り当てに必要な手順を原因とする制御パケット数の増加が確認できた．しかし，受信者の一般的な移動速度を考慮した測定結果によると，そのような制御パケットの増加傾向を考慮しても，IGMP よりも少ない制御パケット数でグループ管理を実現可能であることを示した（6.1節の要求条件③）．

IGMP では，受信者の移動が発生した状況においてもそれが要因となって制御パケット数が増減する要因にはならないことが分かった．ただし IGMPv3 においては，アクセスルータにおいて受信者のグループ加入状況を全て管理しているため，受信者の移動によりその状態情報の不一致の要因になる．IGMPv3 では，一般問い合わせ（デフォルトで 125 秒間隔）により一定間隔で受信者の在籍情報を確認することによりこの状態不一致を解消することが可能であるが，受信者が頻繁に移動する環境においては，最大一般問い合わせの間隔時間だけ状態不一致が発生する可能性があることを考慮する必要がある．以上のことから，受信者が移動する無線ネットワークにおいては，受信者のグループ加入状況を全て

管理する IGMPv3 の設計思想は適さないため, MMGP のように受信者の状態管理を行わないグループ管理方式の採用を検討する方が合理的である.

次に，MMGP の機能に着目し，各項目に分けて考察する.

- MMGP のトークン再割り当ての課題

トークンメンバの離脱や移動に伴うトークン再割り当ての発生は，その後のトークン再割り当ての処理を必要とするため，MMGP における制御パケット数の増加の要因になる．従って MMGP では, 移動する確率が低い受信者や最後にグループから離脱する受信者にトークンを割り当てることにより制御パケット数の更なる減少を図ることが可能となる.

例えば，グループ在籍時間が一番長いメンバにトークンの再割り当てを行うことにより，移動や圏外流出等の可能性が低いメンバにトークンを割り当てることにつながるため，結果的にトークン再割り当てが発生する回数を低減することが期待出来る．以上を実現するための一つの実現例として，受信者のグループ在籍時間に応じて MMGP Query 受信後の MMGP Join Request の送信タイミングを変化させる方法を検討している．これは，受信者のグループ在籍時間が長い場合には MMGP Join Request 送信を早く行い，逆にグループ在籍時間が短い場合には MMGP Join Request 送信を遅らせ，MMGP ルータが一番早く MMGP Join Request を受信したメンバをトークンの再割当先メンバとして選択する方法である．上記の方法以外にも，受信者の移動速度を検出して静止している受信者にトークンを割り当てる方法など，様々な工夫が考えられる．トークン再割り当てに関する更なる考察と性能評価は今後の課題として継続して検討を続ける予定である.

- MMGP のセキュリティに関する考察

MMGP では，必要に応じてトークンメンバの加入や離脱に対して受信者認証を実行し，マルチキャスト DoS の対策が可能である（6.1節の要求条件④）．ただし，配信データの第三者による盗聴を防止するためには，受信者認証だけでは不十分であり，マルチキャスト配信データの暗号化を組み合わせる必要がある．MMGP は，各種マルチキャスト用暗号化プロトコルと併用して利用可能であり，必要に応じてデータ暗号化プロトコルと組み合わせることが出来る．その一例として第 5 章で説明した AKDP との併用がその一例として考えられる．AKDP は，全ての IGMP バージョンに対応できるように設計されている．つまり，AKDP は，IGMP の加入要求により起動され，ネゴシエーション機能を実行することにより以後の受信者認証やグループ鍵の配信の必要性を判断している．AKDP は，IGMP と同様に MMGP Join Request や MMGP Leave Request によって起動することも可能である．MMGP/AKDP ルータ（MMGP と AKDP の両方を実装したルータ）は，MMGP Join Request を受信すると当該マルチキャストグループの最初のメンバであるか否か, つまり最初の MMGP Join Request であるか否かを判断する．前記判断の結果，当該マルチキャストグループの最初のメンバであることを判断すると，AKDP のネゴシエーション機能を実行し, その後, 必要に応じて受信者認証とグループ鍵配信を実行する. その後 MMGP/AKDP ルータは，MMGP Success と共に当該受信者に対してトークンを発行することで，MMGP と AKDP の実行が可能である.

- トークンメンバと非トークンメンバの公平性

MMGP は，トークンメンバの状態管理のための通信量が非トークンメンバと比較して多い．使用するネットワークが従量制課金である場合には，受信者間で通信料金の不公平が生ずる可能性がある．トークンを受信者で公平に割り当てるための仕組みについては，受信者における過去のトークン受領回数に応じて MMGP Query 受信後の MMGP Join Request の送信タイミングを変化させる方法が考えられる．これは，受信者における過去のトークン受領回数が少ない場合には MMGP Join Request 送信を早く行い，逆に受領回数が

多い場合は MMGP Join Request 送信を遅らせ，MMGP ルータが一番早く MMGP Join Request を受信したメンバをトークンの再割当先メンバとして選択する方法である．

ただし，トークンメンバと非トークンメンバの通信量の差異は 1 度のグループ管理開始から終了までの短い期間のみを考えた場合であり，長期間にグループ管理が繰り返し実行される状況を考慮した場合には，トークンは元々ランダムに与えるものであるため，上記方法によらずともトークンメンバになる確率は全ての受信者で等しいため結果的に通信量の差異は問題にならないと考えられる．また，携帯電話における通信料金定額制等の制度面の整備により通信料金の不公平が改善されることも期待出来る．

6.5. 本章のまとめ

本章では，既存のグループ管理プロトコルを移動通信網や無線 LAN で適用した場合，通信コストが高くなるほか，電源断や移動によりクライアントとの接続が突然途絶えた場合の対策が行われていない問題を指摘し，これを解決するため，モバイルマルチキャスト向けのグループ管理プロトコル MMGP を提案した．そして，シミュレーション実験により MMGP と IGMP の比較を行い，MMGP の性能とその特徴を明らかにした．性能評価や考察の結果得られた結論は以下のとおりである．

- MMGP は，有線 LAN で構成されるネットワークや移動通信網，無線 LAN で構成されるネットワークにおいて利用可能である．特に無線を利用したネットワークにおいては，IGMP と比較して少ない制御パケット数でグループ管理の実現が可能である．

- MMGP は，無線を利用したネットワークにおいて受信者が移動する環境を考慮した場合において，IGMP と比較して少ない制御パケット数でグループ管理の実現が可能であり，IGMP と比較して通信コストを低く抑えることが可能である．

- MMGP は，受信者において，IGMP と比較して少ない消費電力でグループ管理が可能である．特に携帯電話など電源容量の制約が大きい端末を受信者として用いる場合には MMGP は有効である．

- MMGP は，グループ管理のみでなく，マルチキャスト DoS への対策が可能である．また，AKDP と MMGP の併用によりデータの暗号化など更なる機能追加も可能であるなど拡張性を持つ．

なお，これまでにマルチキャストグループ管理プロトコルのモバイル環境への適用について十分に検討が行われた研究例は存在せず本研究の新規性は高い．従って，本研究は今後のモバイル向けマルチキャストグループ管理プロトコルの検討における重要な位置付けとなることが期待できる．

6.5.1. 今後の検討課題

今後は，MMGP の残存課題として挙げたトークンメンバと非トークンメンバの公平性に関して検討を継続する予定である．また，本研究では，ネットワークシミュレーションによって MMGP の比較検討を行うにとどまった．今後は，MMGP を実装することにより，実装システム上での課題を整理するなど実用化に向けた取り組みも行う予定である．その後，MMGP の国際標準化を実現することによって MMGP が実装された製品の普及促進を図ることがもう一つの課題である．

第7章 本論文のまとめ

本論文では，コンピュータの高性能化や携帯端末の小型化等による進展と各種通信方式の出現によるネットワークの普及に伴い，多様化するアプリケーションやサービスを提供するマルチメディア通信を対象に，その通信性能を改善するためのプロトコルの提案とその評価を行った．

図7.1は，本論文で研究対象としたマルチキャスト通信プロトコルと他のプロトコルとの関連を示す．

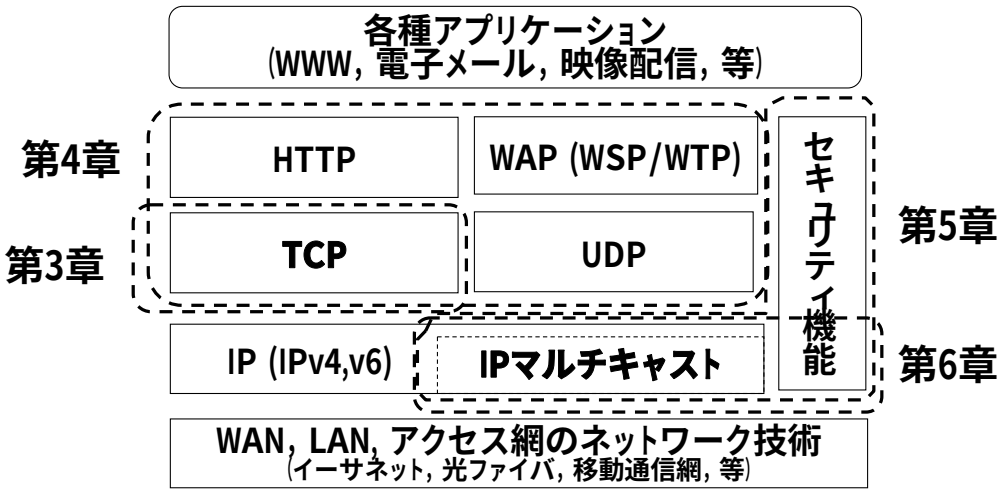


図7.1 本論文で検討対象としたマルチメディア通信プロトコル

第 3 章と第 4 章では，インターネット上の 98%以上の通信で利用されている TCP に着目し，その性能改善を試みた．これらの研究の成果は，TCP を利用するマルチメディア通信の性能改善につなげることが可能である．

最初に第 3 章では，TCP が要求通信品質の異なるコネクションを公平に扱う問題を解決するため，明示的輻輳通知を利用した TCP の優先制御方式の提案を行った．計算機シミュレーションにより提案方式の性能評価を行った結果，従来方式と同等な平均スループットを保ちながら提案方式による優先輻輳制御が可能であることを示した．

次に第 4 章では，第三世代移動通信網を利用したサービスの開始に際し，第三世代移動通信網におけるデータ通信に適する通信プロトコルを明らかにするために，WAP と HTTP/TCP を実装したテストベッドを実装し，W-CDMA のベアラシミュレータ上で実際に動作させることでその性能評価を行った．そして，第三世代移動通信網以降の高速な移動通信網においては WAP よりも HTTP/TCP を利用した方が効果的であることを示した．また，第三世代移動通信網向け通信プロトコルとアーキテクチャを提案し，関連した標準化活動を行った結果，本提案方式が実用化に結びついたことを説明した．

第 5 章と第 6 章では，音声や動画像などのリアルタイム性が要求されるデータを多数のグループメンバに対して同報配信することが可能なマルチキャストを対象とし，本通信方式に残存する課題を解決するための新たな通信プロトコルの提案を行った．マルチキャストは，ネットワークの利用効率を飛躍的に向上することが可能であるため，その残存課題

の解決によりマルチキャストの利用を普及させることが出来れば，マルチメディア通信全体の性能改善につなげることが可能になる．

まず第 5 章では，マルチキャストをより安全に利用するためのマルチキャスト用受信者認証グループ鍵配布プロトコル AKDP を提案し，その実装を行うことにより性能評価を行った．その結果，マルチキャストを利用したサービスを提供するに当たり，AKDP はサービス性に影響を与えない範囲内でセキュリティ機能の提供が可能であることを示した．

次に第 6 章では，IP マルチキャストをモバイル環境に適用するモバイルマルチキャスト向けグループ管理プロトコル MMGP を提案した．また，シミュレーション実験により MMGP と IGMP の比較を行い，MMGP の性能とその特徴を明らかにした．その結果，MMGP は, 無線を利用したネットワークにおいて受信者が移動する環境を考慮した場合に, IGMP と比較して少ない制御パケット数でグループ管理の実現が可能であることを示した．さらに，MMGP は，受信者において，IGMP と比較して少ない消費電力でグループ管理が可能であることを示した．

なお，第 5 章で提案した AKDP と，第 6 章で提案した MMGP は，組み合わせて利用することで，お互いに不足した機能を補完することが可能である．つまり，MMGP によるマルチキャストグループの加入時と離脱時に AKDP を実行することにより，IGMP をモバイルマルチキャスト向けに拡張すると共にセキュリティ機能を高めることが可能である．

第 3 章と第 4 章で取り組んだ TCP に関連する研究成果は，一部実用化に結びつくなど，高い成果を上げることが出来たため，一定の成果が既に得られたということが出来る．また，第 5 章と第 6 章で取り組んだ IP マルチキャストは，今後本格的な実用化が期待される技術であり，今後も更なる研究への取り組みが重要である．従って，本研究結果は，今後の更なる IP マルチキャストの研究において重要な指標とされることが期待できる．

今後の課題としては，本研究で取り上げた TCP が主に使用されるユニキャストと IP マルチキャストの混在環境におけるマルチメディア通信の課題とその解決法を明らかにすること等が挙げられる．さらに，今後爆発的に普及することが期待される IP マルチキャストの残存課題を明らかにし，これらの課題に取り組むことでネットワークの利用効率を高め，マルチメディア通信の性能向上を目指す．

謝辞

本論文を執筆するに当たり，研究開始から絶えずご指導頂きました筑波大学大学院システム情報工学研究科の海老原義彦教授と木村成伴助教授に深い感謝の意を表します．また，本論文の副査をご担当いただきました，筑波大学大学院システム情報工学研究科の大保信夫教授，西原清一教授，田中二郎教授には様々なご助言をいただきましたことを感謝いたします．さらに，株式会社 NTT ドコモに入社以来絶えずご指導をいただきました公立はこだて未来大学システム情報科学部の高橋修教授に深く感謝いたします．さらに，株式会社 NTT ドコモの石川憲洋氏，鈴木偉元氏，角野宏光氏にも研究を進めるに当たり絶えずご助言をいただきましたことを深く感謝いたします．さらに，研究を進めるにあたり切磋琢磨した筑波大学コンピュータネットワーク研究室の諸氏，株式会社 NTT ドコモの諸氏には絶えず励ましを頂きました．本論文を完成させることが出来たのも，ここに述べさせていただいた諸氏のご協力の賜物であり，ここに深い感謝の念を表します．

参考文献

[1] J. Postel, “Transmission Control Protocol,” IETF RFC793, 1981.

[2] S. Deering, “Multicast Routing in a Datagram Internetwork,” Ph.D. thesis, Stanford University, 1991.

[3] S. Deering, “Host Extensions for IP Multicasting,” IETF RFC1112, 1989.

[4] S. Deering and R. Hinden, “Internet Protocol, Version 6 (IPv6) Specification,” IETF RFC1883, 1995.

[5] 上野英俊, 木村成伴, 海老原義彦, “明示的輻輳通知を用いたTCPの優先輻輳制御方式,” 情報処理学会論文誌, Vol.40, No.1, pp.57–65, 1999.

[6] V. Kumar, S. Parimi, and P. Agrawal, “WAP: Present and Future,” Pervasive Computing IEEE, Vol.2, No.1, pp.79–83, 2003.

[7] H. Ueno, N. Ishikawa, H. Suzuki, H. Sumino, and O. Takahashi, “Performance Evaluation of WAP and Internet Protocols over W-CDMA Networks,” Cluster Computing, Vol.8, No.1, pp.27–34, 2005.

[8] H. Ueno, H. Suzuki, N. Ishikawa, and O. Takahashi, “A Receiver Authentication and Group Key Delivery Protocol for Secure Multicast,” IEICE Transactions on Communications, Vol.E88-B, No.3, pp.1139–1148, 2005.

[9] H. Ueno, H. Suzuki, and N. Ishikawa, “A Group Management Protocol for Mobile Multicast,” 4th International Conference on Networking (ICN’ 05), LNCS 3421, pp.892–903, 2005.

[10] W. Fenner, “Internet Group Management Protocol, Version 2,” IETF RFC2236, 1997.

[11] B. Cain, S. Deering, I. Kouvelas, B. Fenner, and A. Thyagarajan, “Internet Group Management Protocol, Version 3,” IETF RFC3376, 2002.

[12] International Organization for Standardization, “Information Processing Systems – Open Systems Interconnection – Basic Reference Model”, ISO 7498-1, 1984.

[13] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, and T. Berners-Lee, “Hypertext Transfer Protocol – HTTP/1.1,” IETF RFC2616, 1999.

[14] T. Kushida, “The Traffic Measurement and the Empirical Studies for the Internet,” Global Telecommunications Conference, 1998 （GLOBECOM 98）, The Bridge to Global Integration. IEEE Volume 2, pp.1142–1147, 1998.

[15] J. Postel, “Internet Protocol,” IETF RFC791, 1981.

[16] Multicast Technologies, Inc., “Multicast Status web pages,” http://www.multicasttech.com/status/

[17] K. Almeroth, “The Evolution of Multicast: From the MBone to Inter-Domain Multicast to Internet2 Deployment,” IEEE Network, pp.10–20, 2000.

[18] Stardust.com, Inc., “A Survey of the History of Internet Multicast,” Mcast 2000 White Paper – A Survey of the History of Internet Multicast, 2000.

[19] M. Allman, V. Paxson, and R. Stevens, “TCP Congestion Control,” IETF RFC2581, 1999.

[20] V. Jacobson, “Congestion Avoidance and Control,” ACM SIGCOMM ’88, August 1988.

[21] S. Floyd, “Congestion Control Principles,” IETF RFC2914, 2000.

[22] R. Jain, “Congestion Control in Computer Networks: Issues and Trends,” IEEE Network Magazine, pp.24–30, 1990.

[23] S. Floyd and K. Fall, “Promoting the Use of End-to-End Congestion Control in the Internet,” IEEE/ACM Transactions on Networking, 1999.

[24] S. Floyd, “Random Early Detection Gateways for Congestion Avoidance,” IEEE/ACM Transactions on Networking, Vol.1, No.4, pp.397–413, 1993.

[25] S. Schneyer, “Survey Paper on TCP,” 1998.

[26] C. Barakat, E. Altman, and W. Dabbous, “On TCP Performance in a Heterogeneous Network: a Survey,” IEEE Wireless Communications Magazine, Vol.38, No.1, pp.40–46. 2000.

[27] 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.

[28] G.; Polyzos, G. Mahonen, P. Saaranen, and M. Xylomenos, “TCP Performance Issues over Wireless Links,” IEEE Communications Magazine, Vol.39, No.4, pp.52–58, 2001.

[29] H. Balakrishnan, V. Padmanabhan, S. Seshan, and R. Katz, “A Comparison of Mechanisms for Improving TCP Performance over Wireless Links,” IEEE/ACM Transactions on Networking, Vol.5, No.6, pp756–769, 1997.

[30] 上野英俊, 鈴木偉元, 田中希世子, 石川憲洋, “放送型データ配信サービスのためのマルチキャスト技術,” NTT ドコモ テクニカルジャーナル, Vol.12, No.2, 2005.

[31] 上野英俊, 鈴木偉元, 田中希世子, 石川憲洋, “放送型データ配信サービスのためのマルチキャスト技術,” NTT 技術ジャーナル, Vol.17, No.9, 2005.

[32] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson, “RTP: A Transport Protocol for Real-Time Applications,” IETF RFC3550, 2003.

[33] 木下真吾, “リライアブルマルチキャスト技術の最新動向,” 電子情報通信学会論文誌, Vol.J85-B, No.11, 2002.

[34] B. Adamson, C. Bormann, M. Handley, and J. Macker, “Negative-acknowledgment (NACK)-Oriented Reliable Multicast (NORM) Protocol,” IETF RFC3940, 2004.

[35] T. Paila, M. Luby, R. Lehtonen, V. Roca, and R. Walsh, “FLUTE – File Delivery over Unidirectional Transport,” IETF RFC3926, 2004.

[36] 山内長承, 城下輝治, 佐野哲夫, 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, 1998.

[37] M. Handley, S. Floyd, B. Whetten, R. Kermode, L. Vicisano, and M. Luby, “The Reliable Multicast Design Space for Bulk Data Transfer,” IETF RFC2887, 2000.

[38] B. Whetten, L. Vicisano, R. Kermode, M. Handley, S. Floyd, and M. Luby, “Reliable Multicast Transport Building Blocks for One-to-Many Bulk-Data Transfer,” IETF RFC3048, 2001.

[39] M. Luby, J. Gemmell, L. Vicisano, L. Rizzo, and J. Crowcroft, “Asynchronous Layered Coding (ALC) Protocol Instantiation,” IETF RFC3450, 2002.

[40] M. Luby, J. Gemmell, L. Vicisano, L. Rizzo, M. Handley, and J. Crowcroft, “Layered Coding Transport (LCT) Building Block,” IETF RFC3451, 2002.

[41] M. Luby, L. Vicisano, J. Gemmell, L. Rizzo, M. Handley, and J. Crowcroft, “The Use of Forward Error Correction (FEC) in Reliable Multicast,” IETF RFC3453, 2002.

[42] M. Luby and L. Vicisano, “Compact Forward Error Correction (FEC) Schemes,” IETF RFC3695, 2004.

[43] D. Estrin, D. Farinacci, A. Helmy, D. Thaler, S. Deering, M. Handley, V. Jacobson, C. Liu, P.

Sharma, and L. Wei , “Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification, “IETF RFC2362, 1998.

[44] D. Waitzman, C. Partridge, and S. Deering, “Distance Vector Multicast Routing Protocol,” IETF RFC1075, 1988.

[45] D. Thaler, “Border Gateway Multicast Protocol (BGMP): Protocol Specification,” IETF RFC3913, 2004.

[46] B. Fenner and D. Meyer, “Multicast Source Discovery Protocol (MSDP),” IETF RFC3618, 2003.

[47] S. Deering, W. Fenner, and B. Haberman, “Multicast Listener Discovery (MLD) for IPv6,” IETF RFC2710, 1999.

[48] R. Vida and L. Costa, “Multicast Listener Discovery Version 2 (MLDv2) for IPv6,” IETF RFC3810, 2004.

[49] P. Ferguson and D. Senie, “Network Ingress Filtering: Defeating Denial of Service Attacks which Employ IP Source Address Spoofing,” IETF RFC2827, 2000.

[50] 3rd Generation Partnership Project, “Multimedia Broadcast Multicast Service (MBMS); Architecture and Functional Description,” 3GPP TS 23.246, 2004.

[51] C. Diot, B. Levine, B. Lyles, H. Kassem, and D. Balensiefen, “Deployment Issues for the IP Multicast Service and Architecture,” IEEE Network Magazine, Special Issue on Multicasting, 2000.

[52] P. Judge and M. Ammar, “Security Issues and Solutions in Multicast Content Distribution: A Survey,” IEEE Network Magazine, Vol.17, No.1, pp.30–36, 2003.

[53] D. Matthew J. Moyer, Josyula R. Rao, and P. Rohatgi, “A Survey of Security Issues in Multicast Communications”, IEEE Network Magazine, Vol.13, No.6, pp12–23, 1999.

[54] K. Ramakrishnan and S. Floyd, “A Proposal to Add Explicit Congestion Notification (ECN) to IP,” IETF RFC2481, 1999.

[55] B. Braden, D. Clark, J. Crowcroft, B. Davie, S. Deering, D. Estrin, S. Floyd, V. Jacobson, G. Minshall, C. Partridge, L. Peterson, K. Ramakrishnan, S. Shenker, J. Wroclawski, and L. Zhang , “Recommendations on Queue Management and Congestion Avoidance in the Internet,” IETF RFC2309, 1998.

[56] S. Floyd, “TCP and Explicit Congestion Notification,” ACM Computer Communication Review, Vol.24, No.5, pp.10–23, 1994.

[57] K. Nichols, S. Blake, F. Baker, and D. Black, “Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers,” IETF RFC2474, 2004.

[58] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss, “An Architecture for Differentiated Service,” IETF RFC2475, 1998.

[59] S. Deering and R. Hinden, “Internet Protocol, Version 6 (IPv6) Specification,” IETF RFC2460, 1998.

[60] C. Chen, H. Krishnan, S. Leung, N. Tang, and L. Zhang, “Implementing Explicit Congestion Notification (ECN) in TCP over IPv6,” UCLA Technical Report, 1997.

[61] Network Simulator (NS), http://www.isi.edu/nsnam/ns/

[62] 串田高幸, “インターネットの TCP のトラヒックの解析,” 情報処理学会研究報告, マルチメディアと分散処理, Vol.84, No.4, pp.19–24, 1997.

[63] P. Chaudhury, W. Mohret, and S. Onoe, “The 3GPP Proposal for IMT-2000,” IEEE Communications Magazine, Vol.37, No.12, December 1999.

[64] Wireless Application Protocol Forum, “Wireless Datagram Protocol Specification,”

WAP-259-WDP-20010614-a, 2001.

[65] Wireless Application Protocol Forum, “Wireless Transport Layer Security Specification,” WAP-261-WTLS-20010406-a, 2001.

[66] Wireless Application Protocol Forum, “Wireless Transaction Protocol Specification,” WAP-224-WTP-20010710-a, 2001.

[67] Wireless Application Protocol Forum, “Wireless Session Protocol Specification,” WAP-230-WSP-20010705-a, 2001.

[68] Wireless Application Protocol Forum, “Wireless Application Environment Specification,” WAP-236-WAESpec-20020207-a, 2001.

[69] S. Gordon and J. Billington, “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, 1999.

[70] 3rd Generation Partnership Project, “RLC Protocol Specification,” 3GPP TS 25.322, 2001.

[71] H. Inamura, G. Montenegro, R. Ludwig, A. Gurtov, and F. Khafizov, “TCP over Second (2.5G) and Third (3G) Generation Wireless Networks,” IETF RFC3481, 2003.

[72] M. Mathis, J. Mahdavi, S. Floyd, and A. Romanow, “TCP Selective Acknowledgment Options,” IETF RFC2018, 1996.

[73] M. Allman, S. Floyd, and C. Partridge, “Increased TCP’s Initial Window,” IETF RFC2414, 1998.

[74] V. Jacobson, R. Braden, and D. Borman, “TCP Extensions for High Performance,” IETF RFC1323, 1992.

[75] World Wide Web Consortium, “XHTML 1.0: The Extensible Hypertext Markup Language (Second Edition),” W3C Recommendation, 2000.

[76] Wireless Application Protocol Forum, “Wireless Application Protocol Architecture Specification,” WAP-210-WAPArch-20010712-a, 2001.

[77] Wireless Application Protocol Forum, “Wireless Profiled TCP Specification,” WAP-225-TCP-20010331-a, 2001.

[78] Wireless Application Protocol Forum, “XHTML Mobile Profile Specification,” WAP-277-XHTMLMP-20011029-a, 2001.

[79] 総務省, “情報通信白書 平成 17 年版,” 2005 年

[80] M. Baugher, R. Canetti, L. Dondeti, and F. Lindholm, “Group Key Management Architecture,” draft-ietf-msec-gkmarch-03.txt, June 2004.

[81] N. Ishikawa, N. Yamanouchi, and O. Takahashi, “An Architecture for User Authentication of IP Multicast and Its Implementation,” Internet Workshop ’99, 1999.

[82] T. Hayashi, D. Andou, H. He, W. Tawbi, and T. Niki, “Internet Group membership Authentication Protocol (IGAP),” draft-hayashi-igap-02.txt, 2003.

[83] P. Judge and M. Ammar, “Gothic: Group Access Control Architecture for Secure Multicast and Anycast,” The 21st Conference on Computer Communications (INFOCOM) 2002, pp.30–36, 2002.

[84] A. Ballardie and J. Crowcroft, “Multicast-specific Security Threats and Counter-measures,” ISOC Symposium on Network and Distributed System Security, pp.2–16, February 1995.

[85] T. Hardjono and B. Cain, “A Secure Group Membership Verification Protocol over IP Multicast,” IEEE International Symposium on Computers and Communications, pp.9–15, 1999.

[86] Association Radio Industries and Business, “The Conditional Access System Specifications for

Digital Broadcasting Standard Version 3.0,” ARIB-STD-B25, 2001.

[87] H. Harney and C. Muchenhirn, “Group Key Management Protocol (GKMP) Specification,” IETF RFC2093, 1997.

[88] A. Ballardie, “Scalable Multicast Key Distribution,” IETF RFC1949, 1996.

[89] A. Ballardie, “Core Based Trees (CBT version 2) Multicast Routing,” IETF RFC2189, 1997.

[90] M. Baugher, T. Hardjono, H. Harney, and B. Weis, “GDOI: The Group Domain of Interpretation,” IETF RFC3547, 2003.

[91] H. Harney, A. Schuett, U. Meth, and A. Colegrove, “GSAKMP: Group Secure Association Group Management Protocol,” draft-ietf-msec-gsakmp-sec-10.txt, 2005.

[92] J. Arkko, E. Carrara, F. Lindholm, M. Naslund, and K. Norrman, “MIKEY: Multimedia Internet KEYing,” IETF RFC3830, 2004.

[93] M. Baugher, R. Canetti, P. Cheng, and P. Rohatgi, “MESP: A Multicast Framework for the IPSec ESP,” draft-ietf-msec-mesp-01.txt, 2003.

[94] 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トランスポート層データ暗号化プロトコルの提案と実装,” 電子情報通信学会 技術研究報告, Vol.103, No.122, pp.25–28, June 2003.

[95] C. K. Wong, M. Gouda, and S. Lam, “Secure Group Communications Using Key Graphs,” IEEE/ACM Transactions on Networking, Vol.8, No.1, pp.16–30, 2000.

[96] D. Naor, M. Naor, and J. Lotspiech, “Revocation and Tracing Schemes for Stateless Receivers,” Advances in Cryptology – CRYPTO 2001, 21st Annual International Cryptology Conference, Lecture Notes in Computer Science (LNCS), Vol.2139, pp.41–62, 2001.

[97] F. Petitcolas, R. Anderson, and M. Kuhn, “Information Hiding – A Survey,” IEEE Special Issue on Protection of Multimedia Content, Vol. 87, No.7, pp.1062–1078, 1999.

[98] W. Jonker and J. P. Linnartz, “Digital Rights Management in Consumer Electronics Products,” IEEE Signal Processing Magazine, Vol. 21, No.2, pp.82–91, 2004.

[99] Open Mobile Alliance, “OMA Digital Rights Management v1.0 Approved Enabler,” OMA-DRM-V1_0-20040625-A, 2004.

[100] Open Mobile Alliance, “OMA Digital Rights Management v2.0 Candidate Enabler,” OMA-ERP-DRM-V2_0-20050915-C, 2005.

[101] M. Barni and F. Bartolini, “Data Hiding for Fighting Piracy,” IEEE Signal Processing Magazine, Vol.21, No.2, pp.28–39, 2004.

[102] Y. Takahashi, T. Aoki, and H. Yasuda, “A Study of Content Fingerprinting for Multicast Networks,” Proceeding of International Conference on Law and Technology, 2002.

[103] A. Perrig, R. Canetti, D. Song, and J. Tyger, “Efficient and Secure Source Authentication for Multicast,” Network and Distributed System Security Symposium (NDSS 2001), pp.35–46, 2001.

[104] T. Hardjono and B Weis, “The Multicast Group Security Architecture,” IETF RFC3740, 2004.

[105] L. Blunk and J. Vollbrecht, “PPP Extensible Authentication Protocol (EAP),” IETF RFC2284, 1998.

[106] C. Rigney, S. Williams, A. Rubens, and W. Simpson, “Remote Authentication Dial in User Service,” IETF RFC2865, 2000.

[107] P. Engelstad, “EAP over UDP (EAPoUDP),” draft-engelstad-pana-eap-over-udp-00.txt, IETF, 2002.

[108] IEEE, “IEEE Standards for Local and Metropolitan Area Networks: Port-Based Network Access Control,” IEEE 802.1X, 2004.

[109] K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajima, and T. Tokita, “Camellia: A 128-Bit Block Cipher Suitable for Multiple Platforms – Design and Analysis –,” Selected Areas in Cryptography, 7th Annual International Workshop, SAC 2000, Lecture Notes in Computer Science (LNCS), Vol.2012, pp.39–56, 2000.

[110] Zona Research, “The Economic Impacts of Unacceptable Web Site Download Speeds,” White Paper, 1999.

[111] 上野英俊, 鈴木偉元, 三浦史光, 石川憲洋, “マルチキャストにおける DoS アタック対策に関する考察, ” 第 2 回 情報科学技術フォーラム (FIT2003), 2003.

[112] 隅岡敦史, 古村隆明, 藤川賢治, 上野英俊, 高木治夫, “IP マルチキャスト/無線 LAN を用いた球場内マルチカメラ放送,” 電子情報通信学会研究報告, Vol.104, No.689, pp.95–100, 2005.

[113] 北原亮, 上野英俊, 鈴木偉元, 石川憲洋, 古村隆明, 藤川賢治, 高木治夫, “公衆無線 LAN「みあこネット」でのマルチキャストルーティング方式の提案, ” 電子情報通信学会研究報告, Vol.104, No.689, pp.107–112, 2005.

[114] 古村隆明, 北原亮, 藤川賢治, 上原哲太郎, 岡部寿男, “みあこネットでの実時間動画像マルチキャスト実験,” 電子情報通信学会研究報告, Vol.104, No.689, pp.101–106, 2005.

[115] I. Romdhani, M. Kellil, and H. Lach, “IP Mobile Multicast: Challenges and Solutions,” IEEE Communications Surveys and Tutorials, Vol.6, No.1, 2004.

[116] U. Varshney, “Multicast over Wireless Networks,” Communications of the ACM, Vol.45, No.12, pp.31–37, 2002.

[117] T. Harrison, C. Williamson, W. Mackrell, and R. Bunt, “Mobile Multicast (MoM) Protocol: Multicast Support for Mobile Hosts,” ACM International Conference on Mobile Computing and Networking (MOBICOM) 1997, pp.151–160, 1997.

[118] V. Chikarmane, C. Williamson, R. Bunt, and W. Mackrell, “Multicast Support for Mobile Hosts Using Mobile IP: Design Issues and Proposed Architecture,” ACM/Baltzer Mobile Networks and Applications, Vol.3, No4, pp.365–379, 1999.

[119] Y. Moritani and Y. Atsumi, “Seamless Hand-off Method for Multicast Receivers Based on Wireless Link Connection Intensity,” IEEE Wireless Communications and Networking Conference (WCNC), 2003.

[120] S. Kaur, B. Madan, and S. Ganesan, “Multicast Support for Mobile IP Using a Modified IGMP,” IEEE Wireless Communications and Networking Conference (WCNC), 1999.

論文リスト

学術論文 (査読あり)

(1) H. Ueno, H. Suzuki, N. Ishikawa, and O. Takahashi, "A Receiver Authentication and Group Key Delivery Protocol for Secure Multicast," IEICE Transactions on Communications, Vol.E88-B, No.3, pp.1139–1148, 2005.

(2) H. Ueno, N. Ishikawa, H. Suzuki, H. Sumino, and O. Takahashi, "Performance Evaluation of WAP and Internet Protocols over W-CDMA Networks," Cluster Computing, Vol.8, No.1, pp.27–34, 2005.

(3) 鈴木偉元, 上野英俊, 石川憲洋, 高橋修, 佐藤文明, 水野忠則, "無線網における高信頼マルチキャストのハイブリッド誤り回復方式の性能解析," 情報処理学会論文誌, Vol.45, No.11, pp.2497–2508, 2004.

(4) N. Ishikawa, H. Fujiwara, H. Ueno, H. Suzuki, and O. Takahashi, "Domain Constrained Multicast: A New Approach for IP Multicast Routing," Kluwer Journal on Telecommunication Systems, Vol.27, No.2-4, pp.207–227, 2004.

(5) 高橋修, 上野英俊, 石川憲洋, 角野宏光, 鈴木偉元, "移動機向けプッシュ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.

(6) 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.

(7) 上野英俊, 木村成伴, 海老原義彦, "明示的輻輳通知を用いた TCP の優先輻輳制御方式," 情報処理学会論文誌, Vol.40, No.1, pp.57–65, 1999.

国際学会 (査読あり)

(8) T. Kato, H. Ueno, and N. Ishikawa, "An Automatic Generation Method of Differential XSLT Stylesheet from Two XML Documents," 1st International Conference on Web Information Systems and Technologies (webist2005), pp.5–12, 2005.

(9) H. Ueno, H. Suzuki, and N. Ishikawa, "A Group Management Protocol for Mobile Multicast," 4th International Conference on Networking (ICN'05), LNCS 3421, pp.892–903, 2005.

(10) N. Ishikawa, H. Ueno, H. Suzuki, O. Takahashi, and H. Fujiwara, "Domain Constrained Multicast and its Application to IPv6," 3rd International Conference on Networking (ICN'04), 2004.

(11) N. Ishikawa, H. Fujiwara, H. Suzuki, H. Ueno, and O. Takahashi, "Domain Constrained Multicast: A New Approach for IP Multicast Routing," Internetworking 2003 International Conference, 2003.

(12) H. Suzuki, N. Ishikawa, H. Ueno, and T. Gotoh, “Mobile Content Transformation using XSLT and its Evaluation,” World Wide Web 2003 Conference, 2003.

(13) H. Ueno, N. Ishikawa, H. Suzuki, H. Sumino, and O. Takahashi, “Performance Evaluation on WAP and Internet Protocol over 3G Wireless Networks,” IFIP TC6 Networking Conference (Networking 2002), pp.527–538, 2002.

(14) N. Ishikawa, Takeshi Kato, H. Ueno, and H. Sumino, “Automatic Generation of a Differential XSL Stylesheet from Two XML Documents,” WWW 2002 Conference, 2002.

(15) N. Ishikawa, H. Suzuki, H. Ueno, H. Sumino, and O. Takahashi, “Considerations on the Mobile Internet Architecture for High-Speed Wireless Networks,” INET 2001, 2001.

研究会，シンポジウム

(16) 内田良隆，三瓶史彦，上野英俊，石川憲洋, “仮想 IP 層: IP コネクティビティを仮想的に拡張するアーキテクチャ,” 情報処理学会マルチメディア，分散，協調とモバイルシンポジウム（DICOMO2005）,Vol.2005, No.6, pp.365–368, 2005.

(17) 北原亮，上野英俊，鈴木偉元，石川憲洋，古村隆明，藤川賢治，高木治夫, “公衆無線 LAN「みあこネット」でのマルチキャストルーティング方式の提案,” 電子情報通信学会研究報告, Vol.104, No.689, pp.107–112, 2005.

(18) 隅岡敦史，古村隆明，藤川賢治，上野英俊，高木治夫, “IP マルチキャスト/無線 LAN を用いた球場内マルチカメラ放送,” 電子情報通信学会研究報告, Vol.104, No.689, pp.95–100, 2005.

(19) 上野英俊，鈴木偉元，石川憲洋, “モバイルマルチキャスト向けグループ管理プロトコルの提案,” 電子情報通信学会研究報告, Vol.104, No.279, (MoMuC2004-55-64), pp.47–52, 2004.

(20) 田中希世子，上野英俊，鈴木偉元，石川憲洋, “クラスタリングを用いたマルチキャストグループ構成方法の検討,” 情報処理学会マルチメディア，分散，協調とモバイルシンポジウム（DICOMO2004）,Vol.2004, No.7, pp.289–292, 2004.

(21) 北原亮，上野英俊，石川憲洋，鈴木偉元，“ドメイン限定マルチキャストの IPv4 への適用,” 電子情報通信学会 2004 年総合大会, B-6-24, 2004.

(22) 加藤剛志，上野英俊，石川憲洋，高橋修, “差分 XSLT スタイルシート生成法の提案と実装,” 電子情報通信学会第 15 回データ工学ワークショップ論文集, 2004.

(23) 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,” 第 2 回 情報科学技術フォーラム (FIT2003), 2003.

(24) 上野英俊，鈴木偉元，三浦史光，石川憲洋, “マルチキャストにおける DoS アタック対策に関する考察,” 第 2 回 情報科学技術フォーラム (FIT2003), 2003.

(25) 田中希世子，鈴木偉元，上野英俊，石川憲洋, “ユーザ適応型マルチキャスト配信グループ構成方法の一考察,” 電子情報通信学会 ソサイエティ大会論文集, 2003.

(26) 上野英俊, 田中希世子, 原下貴志, 鈴木偉元, 石川憲洋, 高橋修, “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,” 情報処理学会マルチメディア, 分散, 協調とモバイルシンポジウム(DICOMO2003),V ol.2003, No.9, pp.113–116, 2003.

(27) 田中希世子, 上野英俊, 鈴木偉元, 石川憲洋, 原下貴志, 高橋修, “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,” 情報処理学会マルチメディア, 分散, 協調とモバイルシンポジウム(DICOMO2003),Vol.2003, No.9, pp.117–120, 2003.

(28) 鈴木偉元, 原下貴志, 田中希世子, 上野英俊, 石川憲洋, 高橋修, “無線 LAN でのマルチキャスト誤り回復方式の比較評価,” 情報処理学会マルチメディア, 分散, 協調とモバイルシンポジウム(DICOMO2003), Vol.2003, No.9, pp.229–232, 2003.

(29) 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トランスポート層データ暗号化プロトコルの提案と実装,” 電子情報通信学会 技術研究報告, Vol.103, No.122, pp.25–28, 2003.

(30) 原下貴志, 鈴木偉元, 田中希世子, 上野英俊, 石川憲洋, “無線 LAN 環境における IP マルチキャストへの FEC,ARQ 適用に関する一考察,” 電子情報通信学会 2003 年総合大会, B-6-195, pp.195, 2003.

(31) 田中希世子, 原下貴志, 鈴木偉元, 上野英俊, 石川憲洋, “無線 LAN におけるマルチキャストパケットロスのモデル化に関する検討,” 電子情報通信学会 2003 年総合大会, B-6-196, pp.196, 2003.

(32) 石川憲洋, 藤原廣則, 上野英俊, 鈴木偉元, 高橋修, “ドメイン限定マルチキャストのドメイン間マルチキャスト経路制御への適用とその評価,” 情報処理学会マルチメディア通信と分散処理ワークショップ, Vol.2002, No.15, pp.233–238, 2002.

(33) 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,” 情報処理学会マルチメディア, 分散, 協調とモバイルシンポジウム(DICOMO2002),Vol.2002, No.9, pp.25–28, 2002.

(34) 上野英俊, 鈴木偉元, 石川憲洋, 高橋修, “プレゼンス情報を利用したモバイル向けマルチキャスト配信アーキテクチャの提案,” 電子情報通信学会研究報告, Vol.102, No.251, (MoMuC2002-19-24), pp.25–30, 2002.

(35) 鈴木偉元, 石川憲洋, 上野英俊, 後藤哲也, 矢野令, 田原歩, “i-mode コンテンツを用いたモバイルコンテンツの変換実験とその評価,” 情報処理学会マルチメディア, 分散, 協調とモバイルシンポジウム(DICOMO2002), Vol.2002, No.9, pp.479–482, 2002.

(36) 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 ハイブリッド制御方式の検討,” 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.75–82, 2002.

(37) 角野宏光, 鈴木偉元, 加藤剛志, 上野英俊, 石川憲洋 “携帯電話用 JAVA コンテンツ検索に向けたメタデータ構成方法に関する検討,” 情報処理学会研究会 マルチメディア通信と分散処理, No.106, 2002.

(38) 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.

(39) 石川憲洋, 藤原廣則, 上野英俊, 鈴木偉元, 高橋修, “ドメイン限定マルチキャストの提案,” 情報処理学会マルチメディア，分散，協調とモバイルシンポジウム（DICOMO2001）,Vol.2001, No.7, pp.313–318, 2001.

(40) 上野英俊, 石川憲洋, 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,” 情報処理学会マルチメディア，分散，協調とモバイルシンポジウム(DICOMO2001),Vol. 2001, No.7, pp.217–222, 2001.

(41) 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,” 電子情報通信学会技術研究報告, Vol.101, No.71 (MoMuC2001 12-24), pp.87–94, 2001.

(42) 上野英俊, 鈴木偉元, 角野宏光, 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,” 情報処理学会マルチメディア，分散，協調とモバイルシンポジウム(DICOMO2000),Vol. 2000, No.7, pp.289–294, 2000.

(43) 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,” 情報処理学会マルチメディア，分散，協調とモバイルシンポジウム(DICOMO2000),Vol. 2000, No.7, pp.283–288, 2000.

(44) 上野英俊, 木村成伴, 海老原義彦, “優先度を考慮にいれた輻輳通知によるフロー制御に関する研究,” 情報処理学会研究会，マルチメディア通信と分散処理, No.86, No.10, pp.55–60, 1998.