Vol. 49 No. 6 情報処理学会論文誌 June 2008

無線メッシュネットワーク ”WAPL ”の提案とシミュレーション評価

伊藤将志[†] 鹿間敏弘[††] 渡邊晃[†]

無線メッシュネットワークは有線 LAN で接続していたアクセスポイント間をアドホックネットワークで接続することにより無線 LAN のバックボーンインフラを容易に構築することができる．しかし，従来の無線メッシュネットワークは，アドホックルーティングプロトコルを改造する方式が一般であり，用途が限定されるという課題があった．また，端末が移動したときにパケットロスが発生するという課題があった．本稿で提案する WAPL（Wireless Access Point Link）は，無線メッシュネットワークを実現するための機能を，アドホックルーティングプロトコルから完全に独立させた．その結果，ルーティングプロトコルを自由に選択し，様々な用途に応用できる．また，無線メッシュネットワークに必要なテーブルの生成をオンデマンドで実現するため，制御パケットが通信トラヒックに与える影響が少ない．さらに近隣の AP の通信状況を常時監視しておくことにより，端末が移動したときのハンドオーバ通知をユニキャストで実現できるようにした．これによりシームレスハンドオーバを確実に行うことができる．提案方式の有効性を評価するため，既存方式と WAPL を ns-2 のモジュールに組み込んで比較を行った．その結果，WAPL の特徴を定量的に示すことができた．

A Proposal of a Wireless Mesh Network ”WAPL” and Its Simulation Results

Masashi Ito,[†] Toshihiro Shikama[††] and Akira Watanabe[†]

Wireless Mesh networks have an advantage of building a backbone infrastructure easily, where access points, which have been conventionally connected by wired LANs, are connected by an ad-hoc network using Wireless LANs. However, the usage of existing Wireless Mesh networks is limited, because particular ad-hoc routing protocols are modified to realize Wireless Mesh networks. There is also a problem that packet loss occurs when a station moves during communication. In WAPL (Wireless Access Point Link), proposed in this paper, functions of a Wireless Mesh network are completely independent of an ad-hoc routing protocol. As a result, WAPL can select any ad-hoc routing protocols freely, and can be used to various applications. Also it does not give much influence on the traffic, because tables that are needed for a Wireless Mesh network are generated on-demand. Moreover, in order to realize a seamless handover, WAPL monitors all communication packets and acquires their routes, so that the message that reports its handover can be sent in unicast. By this method, WAPL can insure a success of a seamless handover process. In this paper, we have implemented WAPL in network simulator ns-2, and compared it with the existing methods. We show the features of WAPL quantitatively.

1. はじめに

無線 LAN の AP（Access Point）間をアドホックネットワークで接続し，バックボーンインフラを容易に構築する無線メッシュネットワークの研究に注目が集まっている．無線メッシュネットワークでは AP を適切に配置していくだけで無線 LAN の通信エリアを容易に広げていくことができ，増設や移設が簡単で柔軟性の高いシステムを構築できる．無線メッシュネットワークは様々な機関で研究・開発が進められてきたが[1)~4)]，いずれも独自の方式であることから互換性がなかった．このことを解決するため，IEEE802.11 委員会では 2004 年 6 月にタスクグループ s を発足させ，無線メッシュネットワークの標準化を進めている[5)]．無線メッシュネットワークと呼ぶものの中には通信端末も含めてすべての装置がアドホックモードに設定されていることを前提とする場合がある．しかし，IEEE802.11s では一般の通信端末が設定を変えることなくネットワークに接続できることを目的とし，AP と通信端末はインフラストラクチャモードで接続

† 名城大学大学院理工学研究科
Graduate School of Science and Technology, Meijo University
†† 福井工業大学電気電子工学科
Department of Electrical and Electronic Engineering, Fukui University of Technology

するものと定義している．本論文でも AP 同士はアドホックネットワークを構築し，AP と通信端末はインフラストラクチャモードで接続するものを無線メッシュネットワークと定義する．

無線メッシュネットワークを実現するには，AP が端末間の通信パケットを，アドホックネットワークを介して適切に中継できる必要がある．このためには，各 AP は通信相手の端末がどの AP と接続しているかを示すマッピング情報（以下，AP/端末マッピング情報）を何らかの方法であらかじめ知っている必要がある．AP/端末マッピング情報の生成/保持方法の違いにより様々な方式が存在し，それぞれに特徴や性能の違いがある．

従来の無線メッシュネットワークでは，AP/端末マッピング情報の生成方法として，アドホックルーティングプロトコルを改造する方法をとる．この方法は AP/端末マッピング情報を生成するための情報をルーティングプロトコルの制御パケットに含ませることができ，制御パケットが増加しないという特徴がある．しかし，特定のアドホックルーティングプロトコルに限定する必要があり，おのずと目的を絞ったシステムとなる．これまでの無線メッシュネットワークは，無線 LAN の公衆バックボーンを迅速に構築することが目的とされており，それに適したルーティングプロトコルが選定されていた．しかし，無線メッシュネットワークは，他にも様々な応用を考えることが可能であり，ルーティングプロトコルが限定されるのは好ましくない．ただし，これによって制御パケットが大きく増加しない方式であることが望ましい．

次に通信中に端末が移動した場合においてもパケットのロスがないまま通信の継続ができることが望ましい．本論文ではこのような機能をシームレスハンドオーバと呼ぶ．無線メッシュネットワーク内での移動は，AP が切り替わるだけであるため，端末の IP アドレスが変わることはない．しかし，AP に登録されている AP/端末マッピング情報を迅速に書き換えることができないとパケットロスが発生することになる．

既存技術の代表である IEEE802.11s では，各 AP がデータリンク層においてアドホックルーティングプロトコルと同様の動作を実行して MAC アドレスを用いたルーティングテーブルを生成し，その中で AP/端末マッピング情報も同時に生成する．ルーティングプロトコルにはハイブリッド方式を採用し，リアクティブ型とプロアクティブ型を環境によって切り替えることができるが，選択はその 2 通りに限られ，他のルーティング方式は利用できない．また，シームレスハンドオーバについての議論はなされていないため，移動のタイミングや通信の方向によってはしばらくの間通信が途絶する可能性がある．

シームレスハンドオーバを実現できることを特徴とした無線メッシュネットワークの研究として SMesh[6] と iMesh[7] がある．SMesh ではハンドオーバ時にパケットの経路を二重化することによりパケットロスを回避する．しかし，SMesh は端末もアドホックモードに設定されている必要があり，本論文が定義するメッシュネットワークとは異なる．iMesh ではハンドオーバが発生したときにそのことを検出した AP がフラッディングにより周辺の AP に通知し，さらに AP が必要なパケットをバッファリングしておくことによりパケットが消失しないように制御する．しかし，アドホックネットワークにおけるフラッディングは信頼性が低く，ハンドオーバに失敗する可能性があるという課題がある．

国内における無線メッシュネットワークの研究として M-WLAN[1] がある．M-WLAN ではアドホックルーティングプロトコルとして OLSR を選定し，これを改造することにより AP/端末マッピング情報を生成する．このため，AP/端末マッピング情報は定期的に交換される．用途としては無線 LAN バックボーン向けである．また，ハンドオーバ時の動作は iMesh と同様な方式をとるが，バッファリングは行わないためパケットロスが発生する．

そこで本論文ではこれらの課題を解決する無線メッシュネットワーク WAPL（Wireless Access Point Link）を提案する．WAPL では AP/端末マッピング情報の生成機能をアドホックネットワークと完全に独立させ，ルーティングプロトコルを自由に選択可能とした．また，AP/端末マッピング情報の生成に係るトラヒックの増加を抑えるため，これらの情報は必要に応じてオンデマンドで生成させることとした．さらにシームレスハンドオーバを実現するため，AP が近隣 1 ホップの通信を常時監視し，通信ペアの端末と各端末が接続する AP との関係を把握する．この情報により端末のハンドオーバ発生時に，ユニキャストにより確実に AP/端末マッピング情報の更新を行い，ハンドオーバの失敗を防止する．

ns-2 によるシミュレーションの結果，従来のフラッディングを用いたハンドオーバ通知では最大 13% が不到達になっていたのに対し，WAPL では同じ条件下で不到達率をほとんど 0% に抑えることができシームレスハンドオーバを実現できることを示した．また，AP/端末マッピング情報の生成方式として，定期交換

方式とオンデマンド生成方式がトラヒックに与える影響を調査し，オンデマンド方式が有利であることを示した．さらに，アドホックルーティングプロトコルの違いがシステム性能にどのように影響するかを明らかにした．

以下，2 章で既存の無線メッシュネットワークの概要とその課題について，3 章で WAPL の概要を説明する．4 章ではシミュレーションの結果と考察を述べ，5 章でまとめる．

2. 既存技術

既存技術の代表として，IEEE802.11s をあげる．IEEE802.11s は様々な方式を公募し，日本のグループが提案した SEE-Mesh[8] が方式のベースとなった．しかし，IEEE802.11s はシームレスハンドオーバについては現時点では未検討の状態である．そこで，シームレスハンドオーバを実現する既存技術としては iMesh を取り上げ，その方式を説明する．また，iMesh で利用するフラッディングによる移動通知が信頼性の低い理由を説明する．なお，本論文では AP は移動しないことを前提とする．

2.1 IEEE802.11s

IEEE802.11s では無線接続された AP を MAP（Mesh Access Point）と呼ぶ．**図 1** に IEEE802.11s の構成と経路生成のシーケンスを示す．MAP 間はアドホックネットワーク，MAP/端末間はインフラストラクチャモードの無線 LAN である．IEEE802.11s では MAP 間のルーティングテーブル生成と MAP/端末マッピング情報の生成に HWMP（Hybrid Wireless Mesh Protocol）を利用する．HWMP は，IP アドレスのかわりに MAC アドレスを用いて，アドホックルーティングプロトコルと同様の動作を行う．HWMP は基本的には AODV（Adhoc On-Demand Distance Vector)[9] をベースとした RM-AODV（Radio Metric AODV）によるリアクティブ型のルーティングを行うが，固定的なネットワークを形成する場合は，ツリー型のパスを事前に形成し，プロアクティブ型のルーティングを行うこともできる．IEEE802.11s ではこのように MAC アドレスを用いてルーティングを行うが，これは IEEE802.11 の関与する範囲が MAC 層であるためである．

RM-AODV では，端末が通信を開始すると，図 1 に示すように，その端末が接続している MAP が端末の代理で経路要求メッセージを他の MAP に対してフラッディングする．宛先の端末と接続している MAP は送信元 MAP へユニキャストで経路要求応答メッセージを返信する．以上のやり取りでルーティングテーブルと MAP/端末マッピング情報が同時に生成され，端末から端末への経路が確立する．IEEE802.11s で用いられるフレームは WDS（Wireless Distribution System）をベースにしており，MAP/端末間，および MAP 間のすべての通信フレームは，宛先端末，送信元端末，宛先 MAP，送信元 MAP の 4 つの MAC アドレスを持つ．MAP はこの情報から自分がアドホックルーティングの先頭/終点であることを知り，インフラストラクチャモードに設定されている端末同士の通信を実現することができる．

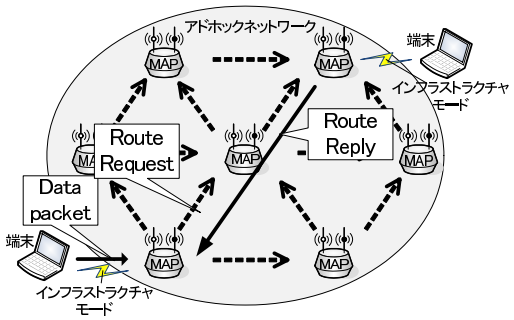

図 1 IEEE802.11s の構成と経路生成シーケンス
Fig. 1 A construction of IEEE802.11s and its route generation process

ハンドオーバの方式については IEEE802.11s では未検討の状態である．無線 LAN のハンドオーバについては，別途 IEEE802.11F，IEEE802.11r，および IEEE802.21[10] で検討されており，通信パケットを AP がバッファリングする方法や認証処理の高速化などが検討されている．しかし，これらの方式は AP 間の接続が有線であることを想定しており，無線メッシュネットワークには適していない．例えば，AP の切り替えを通知するために有線 LAN 上にブロードキャストパケットを送信するが，無線メッシュネットワークの場合はこれがフラッディングになる．フラッディングは 2.3 節で述べるように，有線のブロードキャストに比べて信頼性が低く，通知に失敗する場合がある．また，これらの機能を実現するには端末側に対応する機能の実装が必要となる．

2.2 iMesh

本論文では他の方式と区別するため iMesh における無線接続された AP を iAP（iMesh AP）と呼ぶことにする．iMesh は iAP/端末マッピング情報を生成する方法として OLSR[11] をベースに改造を施す方法をとっている．iMesh は既存のアドホックルーティングと同様に IP 層でルーティングを行う．端末が iAP に参入すると，iAP は HNA メッセージ（OLSR のオ

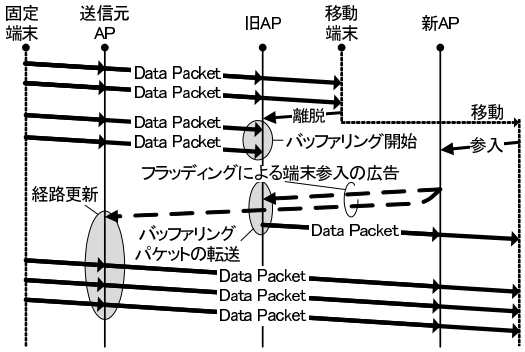

図 2 iMesh のハンドオーバシーケンス
Fig. 2 Sequence of a handover process in iMesh.

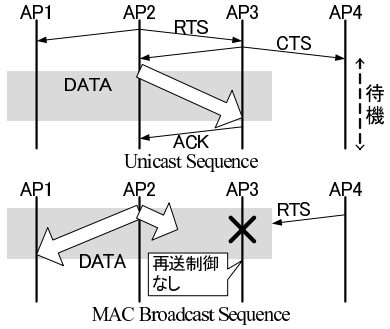

図 3 ユニキャストとブロードキャストのシーケンス
Fig. 3 Sequence of Unicast and Broadcast.

プション）を拡張したメッセージをフラッディングする．拡張 HNA メッセージには端末のアドレス情報が含まれており，このメッセージを受け取った iAP は iAP/端末マッピング情報を生成する．ハンドオーバ時にも同様の処理が実行される．**図 2** に iMesh のハンドオーバシーケンスを示す．図は固定端末から移動端末に向けたパケットが連続して送信されている状態を示している．ここで，移動端末が移動前に所属していた iAP を旧 iAP，移動後に所属する iAP を新 iAP，パケットの送信元の端末が所属している iAP を送信元 iAP と呼ぶ．移動端末は iAP を移動する際，離脱する旧 iAP に対し Deauthentication メッセージ，新 iAP に対し Reassociation Request メッセージを送信する．Reassociation Request メッセージを受信した新 AP は拡張 HNA メッセージをフラッディングする．各 AP に上記拡張 HNA メッセージが届くと移動端末に対する iAP/端末マッピング情報が新 iAP 宛に更新される．この間，固定端末から送信されたパケットは旧 iAP 内にバッファリングされ，拡張 HNA メッセージを受信したときに新 iAP へ転送される．この方式により全てのパケットは移動端末へロスが発生することなく届けることができる．なお，Deauthentication，Reassociation Request メッセージは無線 LAN で定義されているメッセージであり，端末に特殊な機能が必要となるものではない．しかし，フラッディングは次に述べるように信頼性の低い通信方式であり，内容の通知に失敗する場合があるという課題がある．

2.3 フラッディングの信頼性

フラッディングとは，メッセージがアドホックネットワーク全体に行き渡るように MAC ブロードキャストの転送を繰り返すものである．MAC ブロードキャストは宛先が特定できないので，RTS/CTS の制御や ACK による再送制御を行うことができない．**図 3** にユニキャストとブロードキャストのシーケンスの違いを示す．ユニキャストは，AP2 と AP3 間の RTS/CTS 制御により AP4 を待機状態にできる．また ACK により確実に衝突を検出して再送制御が行える．それに対してブロードキャストは，RTS/CTS 制御と ACK の制御は行われないため，AP4 は AP2 が送信中であることを知らずに RTS/CTS を開始してしまう．このようにブロードキャストパケットは破壊されやすい．また，AP では衝突によりパケットが破壊されたことを知ることができず再送制御が行われない．そのため，背景トラヒックのあるような状態ではブロードキャストの消滅率が高く，ハンドオーバの通知にフラッディングを用いると，その通知に失敗する可能性が高い．このような場合を救済するためには，フラッディングによる通知を一定時間ごとに繰り返す必要があるが，これによりシステム全体のトラヒックを圧迫する可能性がある．トラヒックへの影響を減らすためにはフラッディング間隔を大きくする方法があるが，通知に失敗した場合の回復に時間がかかるという課題がある．

3. WAPL の提案

3.1 WAPL の基本動作

WAPL では無線化した AP を WAP（Wireless Access Point）と呼ぶ．WAP 間の経路制御はアドホックルーティングプロトコルをそのまま採用し，WAP/端末マッピング情報は，ルーティングテーブルとは独立させ，LT（Link Table）と呼ぶ独自のテーブルとして保持する．また，WAPL では通信開始時に LT を生成するオンデマンドな方式を採用する．具体的には，端末が通信を開始する際の ARP 処理をトリガとして生成または更新する．LT の生成シーケンスを**図 4** に示す．WAP は端末からの ARP 要求を受信すると，他の WAP へ LT 生成要求メッセージをフラッディングにより広告する．上記フラッディングはアド

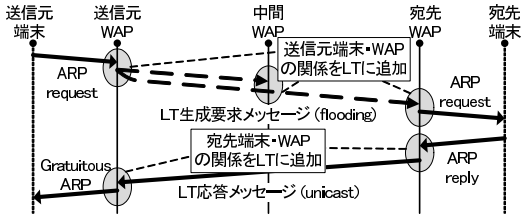

図 4 WAPL の LT 生成シーケンス
Fig. 4 Sequence of an LT generation process in WAPL.

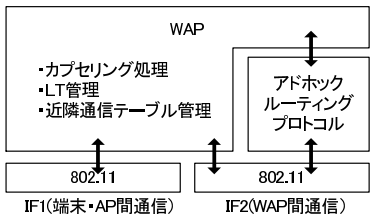

図 5 WAP の構成
Fig. 5 Construction of WAPL.

ホックルーティングプロトコルのフラッディングとは独立した WAPL 独自のものであり，これと区別するために以後 LT フラッディングと呼ぶ．LT フラッディングは，WAP を実現するアプリケーションがブロードキャストを繰り返すことで成り立つ．同一の LT フラッディングパケットを 2 度以上受信した WAP はそのパケットを中継せずに廃棄する．

LT 生成要求メッセージには探索端末の IP アドレス，送信元端末の IP アドレスと MAC アドレスが記載されている．LT 生成要求メッセージを受信した全ての WAP は自身の LT に送信元端末の IP アドレスと WAP の IP アドレスの対応関係を記述する．配下に ARP 要求を送信することにより目的の端末が存在することを検出した WAP は，ユニキャストで送信元 WAP に LT 応答メッセージを返す．LT 応答メッセージには探索端末と送信元端末それぞれの IP アドレスと MAC アドレスが記載されており，送信元 WAP は LT 応答メッセージを受信すると宛先端末の IP アドレスと WAP の IP アドレスの関係を LT に記述する．以上の動作により送信元 WAP と宛先 WAP に LT が生成される．送信元 WAP は LT 応答に含まれる宛先端末の MAC アドレスから ARP 応答を生成し，送信元端末へ返す．以後，端末が送信したデータパケットは，送信元 WAP が MAC ヘッダも含めて WAP の IP アドレスにより IP カプセリングし宛先 WAP まで中継する．MAC ヘッダを含めてカプセリングする理由は，3.3 節で述べるシームレスハンドオーバを実現するためにその情報を使用するためである．無通信状態が一定時間以上続くと，通信が終了したものとみなし LT を削除する．もし，端末に ARP キャッシュが残っていると、通信開始時であっても ARP は実行されずにデータパケットが送信されることもある．このとき，もし WAP 側に LT が存在しない場合は，データパケットを一時退避し，ARP の場合と同様に LT 生成要求から始まる LT の生成手順を実行する．

LT フラッディングを定義したことにより通常のアドホックネットワークよりも制御トラヒックが増加する．しかし，WAPL では LT の生成を必要に応じてオンデマンドで生成するため，他のトラヒックのスループットに与える影響は小さい．LT フラッディングは一般のフラッディングと同様の原理であるため，信頼性が高いものではない．そのため，LT の生成に失敗する可能性もあるが，通信開始時においては WAP の再送制御により確実に LT を生成することが可能である．ここで，再送制御とは，LT 応答メッセージが一定時間内に返ってこない場合に再度 LT フラッディングを行う機能である．

3.2 WAP の構成とその利点

WAP の構成を**図 5** に示す．WAP はインフラストラクチャモードとアドホックモードの IEEE802.11 インタフェースを持ち，アドホックモードのインタフェース側ではアドホックルーティングが動作する．WAP は LT を生成し，パケットを中継するための LT 管理，IP カプセリングや近隣通信テーブル管理のモジュールとアドホックルーティングのモジュールを完全に独立させる．これにより，LT の生成方法と WAP 間のルーティングテーブル生成方法を分けて考えることができ，利用環境に応じて効率の良いメッシュネットワークを構築することができる．また，収容する端末数が多いとネットワークに参加していても通信は行わない端末も多く存在する．そのため，AP/端末マッピング情報の生成には常時全端末に係る情報を保持しておく定期交換方式より，WAPL で実現するオンデマンド方式が適している．

一方，AP 間のルーティングテーブルの生成方法は利用環境によって有利となる方式が異なる．利用環境としては公共通信網に使用するような無線 LAN バックボーンインフラを構築する場合と，災害発生時や工事現場，イベント会場などに一時的に通信網を構築する場合が考えられる．バックボーンインフラでは AP の移動はなく，電源も供給できる．このような場合は，常時安定したルーティングテーブルを生成しておく OLSR が適していると考えられる．それに対し一時的な通信網では AP が移動する場合が考えられ，電源

供給もできるとは限らない．例えば，災害発生時に現地にネットワークインフラを迅速に構築するために利用する応用例が考えられる．この場合は電力を消費しないとされる AODV を採用できる方がよいと考えられる．

また，同一のルーティングプロトコルであってもプロトコル自体が技術的に進化していくことも考えられる．例えば，マルチチャネルや指向性アンテナを用いてアドホックネットワークの帯域幅を広げようとする試みが多岐にわたって行われている[12)~15)]．WAPL ではこれらの研究成果をそのまま利用できるという利点がある．さらに，同一プロトコルのバージョンアップが行われた場合にも，他の機能に手を加えることなく容易に追随することができる．

3.3 シームレスハンドオーバの実現

次に WAPL ではシームレスハンドオーバが実現できることが重要と考え，以下のような対策をとった．

3.3.1 近隣通信の把握

WAPL では端末移動時のハンドオーバ通知を確実に行うために，新 WAP から旧 WAP と送信元 WAP に対してフラッディングではなくユニキャストでハンドオーバを通知する．これを可能とするためには，新 WAP は端末が WAP 間をどのように移動したかを知っている必要がある．そこで，各 WAP では予め近隣で通信中の端末の IP アドレスおよび MAC アドレスと WAP の IP アドレスを関連付けるテーブルを作成しておく．このテーブルを近隣通信テーブルと呼ぶ．近隣通信の把握方法を**図 6** に示す．WAP はプロミスキャスモードで近隣の WAP が送信する通信パケットを常時モニタする．WAP は自身宛以外のパケットの IP ヘッダから宛先 WAP，送信元 WAP の IP アドレスを，カプセル化された MAC ヘッダと IP ヘッダから宛先端末，送信元端末の MAC アドレスと IP アドレスを取得し，それらを図 6 に示す近隣通信テーブルのフィールドである DstWAP，SrcWAP，DstSTA，SrcSTA に記録する．

また，WAPL では常時モニタを行うため，暗号化への対応を考慮する必要がある．WAP と端末間の暗号化には WEP（Wired Equivalent Privacy），WPA（Wi-Fi Protocol Access）等の技術があるが，WAP で一度平文に戻すため，WAP のモニタには影響しない． WAP 間の通信は WAPL の管理下であるため，暗号化を行うか否かを選択することができる．暗号化する場合は全 WAP があらかじめ共通の秘密鍵を共有し，WEP，WPA などを適用する方法が考えられる．また，IPsec のような IP 層以上の暗号化においては，IP アドレス部分は平文であるため，モニタ処理には影響ない．

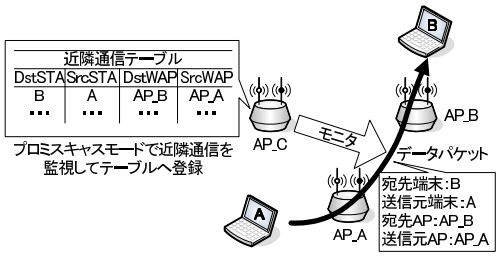

図 6 近隣通信の把握方法
Fig. 6 Acquisition method of neighbor communication.

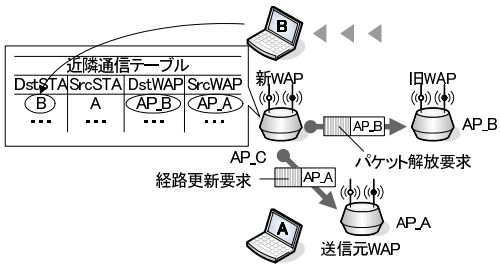

図 7 ハンドオーバ通知
Fig. 7 Handover notification.

3.3.2 ハンドオーバ通知

端末が移動した際のハンドオーバ通知の動作を**図 7** に示す．ハンドオーバ処理のトリガは iMesh 同様，Deauthentication/Reassociation Request メッセージとする．旧 WAP は端末から Deauthentication メッセージを受信するとパケットのバッファリングを開始する．新 WAP は端末から Reassociation Request メッセージを受信すると，端末の MAC アドレスから近隣通信テーブルを参照し，移動してきた端末の MAC アドレスを持つレコードが存在すれば通信中であると判断し，ハンドオーバを開始する．すなわち，近隣通信テーブルから端末の旧 WAP と送信元 WAP の IP アドレスを参照し，旧 WAP にはパケット解放要求メッセージ，送信元 WAP には経路更新要求メッセージをユニキャストで送信する．旧 WAP と送信元 WAP は受信したメッセージに対して応答メッセージを返す．新 WAP は一定時間の間に応答メッセージが返ってこない場合は再送処理を行う．旧 WAP はパケット解放メッセージを受け取るとバッファリングしていたパケットを新 WAP に転送する．送信元 WAP は経路更新要求メッセージを受け取ると LT を書き換えることによりパケットの経路を更新し，ハンドオーバが完了する．制御メッセージをユニキャストで通知するため，パケット到達の信頼性が高く，通信相手を特定してい

るため再送制御も可能である．なお，新 WAP における送信元端末に対する LT は移動端末が新 WAP へ移動した時点で近隣テーブルの内容から直ちに更新することができる．近隣通信テーブルの保持時間は ARP キャッシュと同程度の「2 分」程度が最適と考えられる．また，応答メッセージの待ち時間タイマは今回は 50 ミリ秒とした．

4. 評　　価

WAPL の有効性を示すため，ネットワークシミュレータ ns-2（network simulator-2）[16] を利用して WAPL と既存技術の比較評価を行った．iMesh と WAPL において通信中にハンドオーバが発生したとき，ハンドオーバ通知の不到達率を比較して WAPL によるユニキャスト方式がシームレスハンドオーバにいかに有効であるかを 4.2 節に示した．次に，iMesh が iAP/端末マッピング情報を定期的に生成するのに対し，WAPL は WAP/端末マッピング情報をオンデマンドで生成するという違いがある．このことに起因する違いを評価するため，以下のようなシミュレーションを行った．まず，ネットワークに接続する端末の数が増加したとき，WAPL では制御メッセージによるトラヒックの増加は発生しないが，iMesh では制御メッセージが増加する．そこで 4.3 節では iMesh の制御メッセージがどの程度増加するかをシミュレーションした．次に，端末の通信開始頻度が増加したとき iMesh では制御メッセージによるトラヒックの増加はないが，WAPL では制御メッセージが増加する．そこで 4.4 節では WAPL の制御メッセージがどの程度増加するかをシミュレーションした．さらに，iMesh では通信開始遅延は発生しないが，WAPL では通信開始遅延が発生する．そこで 4.5 節では WAPL の通信開始遅延をシミュレーションにより測定した．

4.1 ns-2 の改造

ns-2 は研究機関でよく利用されているフリーソフトである．しかし，ns-2 はアドホックネットワークの機能は充実しているものの，現時点では無線 LAN インフラストラクチャモードの機能が備わっていない．従ってそのままではメッシュネットワークのシミュレーションも不可能である．そこで，ns-2 に以下のような改造を施し，シミュレーション環境を構築した．ns-2 の IEEE802.11 機能実行モジュールにビーコンの発信，電波強度による AP 離脱と次の AP への移動の判断，離脱・参加処理を追加した．無線メッシュネットワークは AP がインフラストラクチャモードとアドホックモードの 2 種類のインタフェースをもつ必要があるが，それぞれのインタフェースを持つノードの内部モジュール間のインタフェース同士をネットワークを介さず直接接続することにより WAP を実現した．今回のシミュレーションでは簡単のためインフラストラクチャモード側はアドホックモード側と干渉しない上で同一チャネルとした．

表 1 シミュレーションパラメータ（1）
Table 1 Simulation parameters (1).

ハンドオーバを行う端末	
台数	2 台（1 ペア）
通信タイプ	UDP，20ms 間隔，172bytes
ホップ数（AP 間）	1，2，3，4
ハンドオーバ回数	800
背景負荷を発生する端末	
台数	10 台
セッション数	10
送信トラヒック/端末	250, 500, 750, 1000, 1250kbps
設置位置	ランダム
メッシュネットワーク	
AP （WAP）台数	24 台
電波到達距離	100m
WAP(iAP) 間の距離	80m
MAC プロトコル	IEEE802.11g
メッシュネットワークプロトコル	iMesh, WAPL（OLSR）

4.2 ハンドオーバ通知の不到達率

端末が移動したとき，新 AP から旧 AP にハンドオーバを通知できなければ旧 AP でバッファリングしていたパケットは損失する．また，送信元 AP と新 AP 間の AP/端末マッピング情報を更新できなければ経路不整合となり，パケットの損失や通信の回復時間が大きくなる原因となる．本シミュレーションではハンドオーバ時に旧 AP と送信元 AP に送信される制御メッセージの不到達率を計算し，同時に制御メッセージが不到達になったときに経路が更新されるまでの回復時間を求めた．制御メッセージは，iMesh 方式はフラッディング，WAPL 方式はユニキャストである点が大きく異なる．シミュレーションのパラメータを**表 1** に，シミュレーションフィールドの構成を**図 8** に示す．シミュレーションフィールド上には WAP（iAP）を複数配置し，2 台の端末に VoIP を想定した双方向通信をさせながら，一方の端末は固定し，もう一方の端末は 2 つの WAP（iAP）間を繰り返し移動させる．図 8 で示すように，WAP（iAP）同士の距離はすべて等間隔の 80m で近隣の WAP（iAP）が六角形を作るように配置した．WAP（iAP）と端末の電波到達距離は 100m で WAP（iAP）は近隣の WAP（iAP）の無線セルと重なりあっている．背景負荷をかけるため，

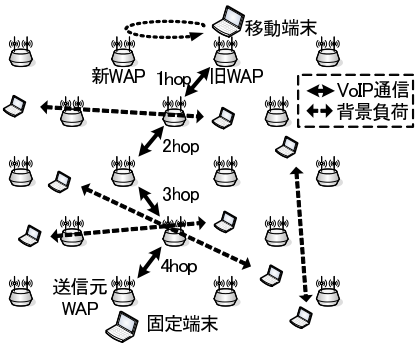

図 8 シミュレーションフィールドの構成
Fig. 8 Construction of a simulation field.

端末を複数台設置し，一定期間ごとにランダムにペアを変更しながら双方向の UDP 通信を行わせた．ホップ数ごとの違いを評価するために固定端末の位置をずらし WAP（iAP）間のホップ数を 1，2，3，4 と変化させた．端末側のチャネルはすべて同一とした．なお，ホップ数の値は新旧 WAP（iAP）と送信元 WAP（iAP）間の最短ホップ数であり，経路構築時にルーティングプロトコルによっては冗長経路を生成することもある．

旧 WAP（iAP）へのハンドオーバ通知の不到達率を**図 9**，送信元 WAP（iAP）への不到達率を**図 10** に示す．横軸の背景トラヒックは背景トラヒック生成用の端末 1 台が送信したトラヒック量を bps に変換して表している．iMesh 方式の旧 iAP への不到達率は背景トラヒックとともに上昇し，背景負荷用端末のトラヒックが 1.25Mbps の時には 10% 程度にまで達することがわかる．送信元 iAP への不到達率はホップ数によって差があり，4 ホップでは背景負荷が 1.25Mbps の時は不到達率が約 13% になる．背景トラヒックが 0 でも iMesh 方式の場合は不到達率が 0% にならない．これは移動端末自身が送受信している双方向の UDP 通信により，ブロードキャストパケットが破壊されるためである．また，ホップ数が多くなれば，送信元 iAP へ拡張 HNA メッセージが届くまでにパケットが衝突する可能性が高くなり，不到達率が高くなることがわかる．これに対して，WAPL ではユニキャストを用いることによる効果でパケット解放要求，経路更新要求とも不到達率がほぼ 0% になっていることがわかる．ユニキャストは RTS/CTS 制御が働くことと ACK による確認により確実に衝突の検出と再送が行えるためである．

WAPL では送信元 WAP への経路更新要求が不到達となると通信中のパケットは旧 WAP へ送信され続ける．このとき，旧 WAP へのパケット解放要求が正

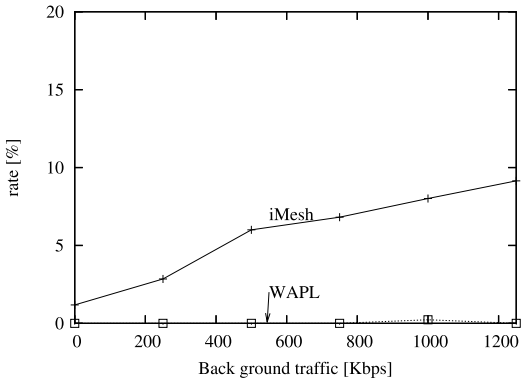

図 9 旧 AP への通知不到達率
Fig. 9 Unreachable rates to the old AP/WAP.

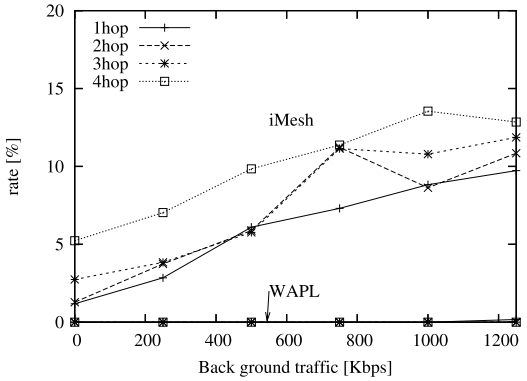

図 10 送信元 AP への通知不到達率
Fig. 10 Unreachable rates to the source AP/WAP.

しく到達していればパケットは旧 WAP から新 WAP に中継され，通信の継続は可能である．パケット解放要求も同時に不到達の場合のみハンドオーバは失敗となり，通信が継続できなくなる．

次に，ハンドオーバ開始から経路が更新されるまでの平均回復時間を求めた．ここで言う回復時間とは，端末が新 WAP（iAP）に移動してから送信元 WAP（iAP）の WAP（iAP）/端末マッピング情報の内容が新 WAP（iAP）に更新されるまでの時間である．**図 11** に背景負荷用端末のトラヒックを 750Kbps に固定した場合の平均回復時間を示す．横軸は新 WAP（iAP）と送信元 WAP（iAP）間のホップ数を示している．iMesh では拡張 HNA メッセージの送信間隔が大きくかつホップ数が増えるにつれて，平均回復時間は大きくなり，拡張 HNA メッセージ間隔が 5 秒，ホップ数が 4 のときは平均回復時間が 0.6 秒となる．WAPL においては 4 ホップの場合でもルーティングプロトコルに OLSR を利用した場合 0.02sec，AODV を利用した場合 0.04sec 程度で iMesh 方式に比べて十分小さい時間で回復していることがわかる． WAPL

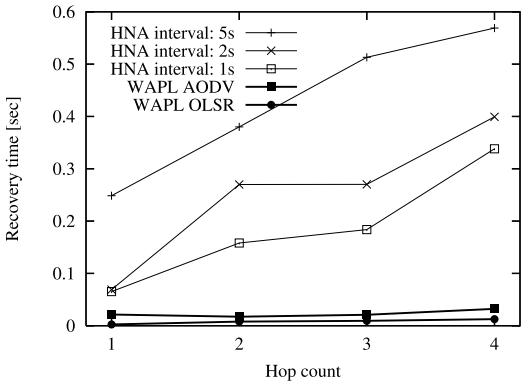

図 11 平均回復時間
Fig. 11 Average recovery time.

表 2 回復時間の分布
Table 2 Distribution of recovery time.

Delay（sec）	0-0.5	0.5-1	1-1.5	1.5-2	2-
WAPL（OLSR）	100	0	0	0	0
WAPL（AODV）	99.1	0.8	0	0.1	0
iMesh（HNA:1s）	85.0	4.0	4.5	4.5	2.0
iMesh（HNA:2s）	80.2	9.8	6.0	2.8	1.2
iMesh（HNA:5s）	65.0	24.6	4.1	1.0	5.3

単位 [%]

において AODV の方が OLSR に比べて平均回復時間が大きいのは，OLSR が常に最適な経路を確立維持しているのに対して，AODV ではハンドオーバごとに経路探索を実行するためである．**表 2** に 4 ホップのときの回復時間の分布を示す．iMesh ではハンドオーバ通知が失敗した際に，次の拡張 HNA メッセージの周期まで通知が遅れるため，大きな回復時間を要する場合がある．それに対し，WAPL では通知が正常に終了するまでその時点で再送処理を行うため，回復時間は極めて少ないことがわかる．また拡張 HNA メッセージは少し待機してから他のメッセージと相乗りして転送される．この待機時間も iMesh の平均回復時間を遅くする要因となっている．

4.3 定期生成方式がトラヒックに与える影響

iAP/端末マッピング情報を定期的なフラッディングにより生成する定期生成方式がトラヒックに与える影響を調べるために，iMesh のシミュレーションを行った．iMesh では拡張 HNA メッセージを定期的にフラッディングする．このフラッディングには全ての端末の情報を必要とするので，通信を行っていない端末の情報も含まれる．**表 3** にシミュレーションパラメータを示す．シミュレーションフィールド上には iAP を等間隔に配置し，通信を行わない端末をランダムに配置する．その上で，測定用に設置した 2 台の端末に FTP 通信を実行させ，スループットを計測した．拡張 HNA メッセージの間隔は，5 秒,2 秒,1 秒とした．ネットワーク規模による違いを示すため，iAP の台数は IEEE802.11s で想定するネットワーク規模と同程度の 38 台の場合と，さらに規模の大きい 52 台の 2 通りとした．ネットワーク規模が大きくなるとシミュレーション時間が膨大になるため今回は 52 台を最大とした．上記条件のもとで 4 回ずつシミュレーションを行い，平均値を算出した．

表 3 シミュレーションパラメータ（2）
Table 3 Simulation parameters (2).

スループット測定用端末	
台数	2 台（1 ペア）
通信タイプ	FTP（50 秒間）
ホップ数（AP 間）	1, 2, 3, 4
背景負荷を発生する端末	
端末密度（台数/AP）	0, 1, 2, 3, 4
通信	なし
拡張 HNA の間隔（秒）	1, 2, 5
設置位置	ランダム
メッシュネットワーク	
AP 台数	38, 52 台
電波到達距離	100m
WAP(iAP) 間の距離	80m
MAC プロトコル	IEEE802.11g
メッシュネットワークプロトコル	iMesh

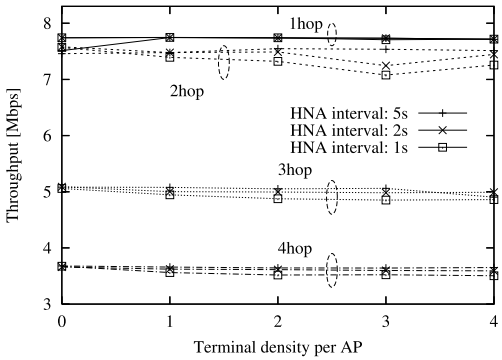

図 12 定期生成方式のスループット（AP38 台）
Fig. 12 Throughput of the periodical generation method (38APs).

図 12 に iAP38 台時，**図 13** に iAP52 台時の端末密度の違いによるスループットの違いを示す．また**表 4** には HNA 拡張メッセージ送信間隔が 1 秒の場合のスループットの低下率を示す．iAP38 台ではスループットへの影響は少ないものの，拡張 HNA メッセージの間隔が 1 秒のときは端末密度が 0 台と 4 台のときを比較すると，最大約 4.3% の劣化がみられる．iAP52 台のときは拡張 HNA メッセージの間隔が 5 秒であればスループットへの影響は少ないが，1 秒のときは，端末密度が 0 台と 4 台のときを比較すると最大約 9.3%

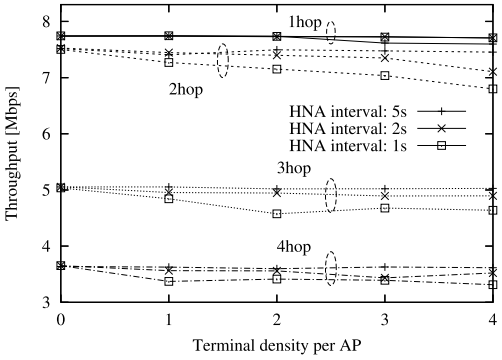

図 13 定期生成方式のスループット（AP52 台）
Fig. 13 Throughput of the periodical generation method (52APs).

表 4 HNA 拡張メッセージ送信間隔が 1 秒の場合のスループット低下率
Table 4 Throughput decreasing rate where the interval of HNA message is 1 second.

	1hop	2hop	3hop	4hop
AP38 台	0.3	4.1	3.9	4.3
AP52 台	0.4	9.4	7.9	9.3

単位 [%]

劣化していることがわかる．このように，ネットワーク規模が大きく，拡張 HNA メッセージの間隔が短いと，端末の密度が大きいときにスループットに影響が出ることがわかる．端末密度が高くなれば，拡張 HNA メッセージのデータサイズは長くなり，拡張 HNA メッセージの送信間隔が短くなればパケット数は増加する．また，ネットワークの規模により iAP の数が多くなれば拡張 HNA メッセージの発生源が多くなるため，ネットワーク全体の HNA メッセージ数が多くなる．上記結果から定期生成方式では端末移動時の経路の復旧を迅速に実現するために定期フラッディングの間隔を短くするか，ネットワークの規模，接続する端末の数を制限するかの選択が必要になる．これに対して，WAPL のようなオンデマンド型の方式では定期的メッセージは発生しないため，このようなトラヒックは発生しない．

4.4 オンデマンド方式がトラヒックに与える影響

WAP/端末マッピング情報を必要に応じて生成するオンデマンド方式がトラヒックに与える影響を調べるために，WAPL のシミュレーションを実施した．なお，IEEE802.11s もオンデマンド方式の 1 種である．WAPL では端末間の通信開始時に LT 生成のための LT フラッディングが実行されるため，通信開始頻度が高いと制御メッセージがネットワークの負荷となる可能性がある．これに対して iMesh のような定期生成方式では通信開始時に制御メッセージは発生しないため，通信開始頻度が変わってもトラヒックの増加はない．そこで，ネットワーク上の通信開始頻度を変化させ，WAPL の方式が一般通信のスループットにどれだけ影響を与えるかを評価した．シミュレーションのパラメータを**表 5** に示す．シミュレーションフィールド上に WAP を等間隔に設置し，背景負荷用端末に一定時間ごとにランダムにセッションを確立させ，通信開始を繰り返させることにより LT フラッディングによるトラヒックを発生させた．その背景負荷のもとで，1 ペアの端末に FTP による通信を行わせ，スループットの変化を測定した．WAP の台数と端末の密度は 4.3 節における最も厳しい条件と同様の 4 端末/WAP とした．通信開始に係わるトラヒックの影響のみを純粋に測定するため，通信開始後のデータパケットは WAP で遮断し，アドホックネットワーク側に出さないようにした．各端末が 60 秒おきに異なる相手に対して通信を開始する場合と，通信開始が全く発生しない場合を比較した．実際の通信では通信相手が特定のサーバやゲートウェイなど決まった相手に集中することもあるが，この場合は LT が一定時間保持されるため，LT フラッディングは発生しない．上記シミュレーション条件は，より過酷な条件として端末がネットワーク内で IP 電話のような P2P 通信を頻繁に行うというシナリオを想定した．即ち，IP 電話の 1 回の通話時間を 60 秒として，通話終了後にすぐに別の相手に掛け直すという動作をネットワーク上の全ての端末が繰り返し続けるものとする．これは実ネットワークで発生する通信に比べて十分過酷な条件設定であると考えられる．また，WAPL ではルーティングプロトコルを自由に選択できるのでアドホックルーティングプロトコルが OLSR と AODV の 2 通りの場合について比

表 5 シミュレーションパラメータ（3）
Table 5 Simulation parameters (3).

TCP スループット測定用端末	
台数	2 台（1 ペア）
通信タイプ	FTP（50 秒間）
ホップ数（AP 間）	1，2，3，4
背景負荷を発生する端末	
端末密度（台数/WAP）	4
1 端末の通信開始間隔（秒）	60
メッシュネットワーク	
WAP 台数	52 台
電波到達距離	100m
WAP（iAP）間の距離	80m
MAC プロトコル	IEEE802.11g
メッシュネットワークプロトコル	WAPL（OLSR，AODV）

表 6 スループットの低下率（OLSR）
Table 6 Degradation rate of throughput(OLSR).

WAP 間距離	スループット		低下率
	通信開始なし	全端末が 60 秒に 1 回通信開始	
1hop	7.65Mbps	7.61Mbps	0.54%
2hop	7.48	7.40	1.11
3hop	5.05	5.00	0.97
4hop	3.65	3.62	0.82

表 7 スループットの低下率（AODV）
Table 7 Degradation rate of throughput(AODV).

WAP 間距離	スループット		低下率
	通信開始なし	全端末が 60 秒に 1 回通信開始	
1hop	7.67Mbps	7.56Mbps	1.40%
2hop	7.55	7.39	2.17
3hop	5.12	4.96	3.18
4hop	3.70	3.57	3.28

較した．

表 6，**表 7** にルーティングプロトコルがそれぞれ OLSR の場合，AODV の場合のスループット低下率を示す．LT フラッディングが全く発生しない場合に比べて、通信開始による LT フラッディングの背景負荷がある場合は、FTP のスループットは OLSR の場合で約 0.5〜1.2% ，AODV では 0.9〜3.2% の低下となった．このようにオンデマンド生成方式はかなり厳しい条件を与えても一般通信にはほとんど影響を与えることがないことがわかる．

ルーティングプロトコルが AODV の場合と OLSR の場合を比べると，通信開始なしの場合は若干 AODV の方が平均スループットが高いが，これは OLSR では TC，Hello などの定期メッセージによる背景負荷があるためである．TC，Hello などの定期メッセージは OLSR のルーティングテーブルを生成するための OLSR 独自の制御メッセージである．OLSR の定期メッセージは通信開始がなくても発生するが，AODV は通信開始時にしか制御メッセージが発生しない．そのため通信開始なしの場合には AODV の平均スループットが若干高くなる．また，通信開始頻度によって OLSR の制御メッセージ量が変化しないのに対して，AODV の場合は LT 生成時に LT フラッディングとは別に AODV の経路探索のフラッディングが余分に発生するため，通信開始頻度が上がると AODV の制御メッセージ量は増加する．このため，60 秒に 1 回の通信開始の場合は OLSR のスループットの方が若干高くなる．

4.5 オンデマンド方式が通信開始遅延に与える影響

WAPL では通信開始時に LT を生成するために遅延が発生する．これはルーティングプロトコルからの独立性を実現した事に対する見返りの短所と言える．そこで WAPL において，LT を生成するまでにかかる時間を示すシミュレーションを行った．LT の生成に要する時間を純粋に測定するため，アドホックルーティングでは通信開始遅延の発生しない OLSR を利用した．送信元 WAP がインフラストラクチャモード側の端末からパケットを受け取り，LT フラッディングにより LT が生成され，パケットが送信される瞬間までの遅延を異なる背景負荷ごとに測定した．本シミュレーションのパラメータは 4.2 節と同一の条件とした．また，サンプルの分散を示すため，95% 信頼区間を算出した．これはサンプルの母集団の値が 95% の確率でその信頼区間の範囲内にあてはまることを示す．

表 8 LT の生成に要する時間
Table 8 Time for generation of LT.

背景負荷端末 1 台あたりの背景負荷 [Kbps]		0	500	1000	1250
1hop	平均	8	4	29	30
	95%信頼区間	± 5	± 2	± 11	± 10
4hop	平均	6	13	92	155
	95%信頼区間	± 4	± 6	± 42	± 64

単位 [ms]

シミュレーション結果を**表 8** に示す．1hop であれば背景負荷が最大時平均が 30ms，信頼区間は± 10ms となった．4hop では背景負荷が最大のとき平均が 155ms，信頼区間は± 64ms となった．これに対して，iMesh では定期交換方式であるため通信開始遅延はない．通信開始遅延に関しては iMesh が有利であるが，WAPL の遅延は実用上許容範囲と考えられる．

5. ま と め

無線メッシュネットワークの一方式として以下のような特徴を持つ WAPL を提案した．まず，アドホックルーティングプロトコルと WAP/端末マッピング生成機能を完全に独立させた．そのため，利用条件に適したルーティングプロトコルの選択ができる上，ルーティングプロトコルのバージョンアップにも容易に追随できる．また，WAP/端末マッピング情報を必要に応じてオンデマンドで生成することにより，一般通信のトラヒックに与える影響をなくした．さらに，各 WAP が近隣通信 WAP の状況を常に把握しておくことにより，ハンドオーバ通知メッセージをユニキャストで実現することとした．これにより，ハンドオーバ通知の信頼性を向上させた．シミュレーションにより，WAPL がシームレスハンドオーバを実現できることを示した．WAPL はアドホックルーティングプロトコ

ルを独立させたことにより，通信開始時のシーケンスが追加される．このため通信開始遅延が発生し，通信開始頻度が高くなると制御メッセージによるトラヒックが増加するという課題がある．ただし，このことによる影響は実用上ほとんどないことをシミュレーションにより示した．今後は WAPL を災害通信への応用など様々な条件下でのシミュレーションを行い，条件に応じたルーティングプロトコルの選定などを行っていく．また，WAP が移動するような応用例についても検討を行う．さらに，実機によるテストベッドを構築・運用し，評価を実施する予定である．

参 考 文 献

1) 大和田泰伯，照井宏康，間瀬憲一，今井博英：マルチホップ無線 LAN の提案と実装，電子情報通信学会論文誌 B， Vol.J89-B, No.11, pp.2092–2102 (2006).
2) MetroMesh: http://www.tropos.com/.
3) MeshCruzer: http://www.thinktube.com/.
4) Packethop: http://www.packethop.com/.
5) IEEE802.11: http://grouper.ieee.org/groups/802/11/.
6) Amir, Y., Danilov, C., Hilsdale, M. et al.: Fast Handoff for Seamless Wireless Mesh Networks, *ACM MobiSys* (2006).
7) Navda, V., Kashyap, A. and Das, S.R.: Design and evaluation of iMesh: an infrastructure-mode wireless mesh network, *World of Wireless Mobile and Multimedia Networks*, pp.164–170 (2005).
8) Aoki, H., Chari, N., Chu, L. et al.: 802.11 TGs Simple Efficient Extensible Mesh (SEE-Mesh) Proposal (2005).
9) Perkins, C.E., Belding-Royer, E.M. and Das, S. R.: Ad hoc On-Demand Distance Vector (AODV) Routing, *RFC 3561* (2003).
10) IEEE802.21: http://grouper.ieee.org/groups/802/21/.
11) Clausen, T. and Jacquet, P.: Optimized Link State Routing Protocol(OLSR), *RFC 3626* (2003).
12) 長島勝城，高田昌忠， 渡邊尚：スマートアンテナを用いた 2 種アクセス併用指向性メディアアクセス制御プロトコル，電子情報通信学会論文誌 B， Vol.J87-B, No.12, pp.2006–2019 (2004).
13) Nasipuri, A., Ye, S., You, S. et al.: A MAC protocol for mobile ad hoc networks using directional antennas, *IEEE Wireless Communications and Networking Conference*, pp.1214–1219 (2000).
14) Chen, J. and Chen, Y.-D.: AMNP: Ad Hoc Multichannel Negotiation Protocol for Multihop Mobile Wireless Networks, *IEEE International Conference on Communication* (2004).
15) Jain, N., Das, S.R. and Nasipuri, A.: A Multichannel CSMA MAC Protocol with Receiver-based Channel Selection for Multihop Wireless Networks, *IEEE ICCCN*, pp.432–439 (2001).
16) ns2: http://www.isi.edu/nsnam/ns/.

(平成？年？月？日受付)
(平成？年？月？日採録)

伊藤 将志（学生会員）

2004 年名城大学理工学部情報科学科卒業．2006 年同大学大学院理工学研究科情報科学専攻修了．現在，同大学院理工学研究科電気電子・情報・材料工学専攻博士後期過程に在学中．VoIP，無線ネットワーク等の研究に従事．修士（工学）．2007 年 DICOMO ヤングリサーチャー賞受賞．

鹿間 敏弘（正会員）

1976 年東工大・総合理工学研究科・電子システム専攻修了．同年三菱電機（株）入社．衛星利用コンピュータネットワーク，高速リング型 LAN，ATM 関連装置，ネットワークセキュリティ，高速 PLC 等に関する研究開発に従事．2007 年 4 月より福井工業大学電気電子工学科．電子情報通信学会，IEEE 各会員．情報学博士．

渡邊 晃（正会員）

1974 年慶応義塾大学工学部電気工科学科卒業．1976 年同大学大学院工学研究科修士課程修了．同年三菱電機株式会社入社後，LAN システムの開発・設計に従事．1991 年同社情報技術総合研究所に移籍し，ルータ，ネットワークセキュリティ等の研究に従事．2002 年名城大学理工学部教授，現在に至る．博士（工学）．電子情報通信学会，IEEE 各会員．