社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2004－ＤＳＭ－33 (20)
2004／5／14

アドホックネットワークを利用したインターネット接続システムの管理方法に関する考察

島田 秀輝† 北須賀輝明†† 福田 晃†† 砂原 秀樹†

† 奈良先端科学技術大学院大学 情報科学センター
〒630-0101 奈良県生駒市高山町 8916-5
†† 九州大学大学院システム情報科学研究院
〒816-8580 福岡県春日市春日公園 6-1
E-mail: †hideki-s@is.naist.jp, suna@wide.ad.jp, ††{kitasuka, fukuda}@f.csce.kyushu-u.ac.jp

あらまし 無線 LAN のアクセスポイント近辺において，端末がアドホックネットワークを構成し，端末に対してインターネット接続性を提供するシステムの構築を目指している．このように端末が中継を行うことによって，一時的にアクセスポイントの利用エリアを拡大できると考えられる．本稿では，アクセスポイント近隣におけるアドホックネットワークの構成方法について述べる．また，その際に問題となる端末の成りすましを防ぐために，アドホックネットワークを構成する端末の管理方法について提案を行う．

キーワード モバイルコンピューティング，アドホックネットワーク，インターネット，無線ネットワーク

Consideration about the Management Method of the System that provides the Internet Connectivity by using Ad-hoc Network

Hideki SHIMADA†, Teruaki KITASUKA††, Akira FUKUDA††, and Hideki SUNAHARA†

† Information Technology Center, Nara Institute of Science and Technology
8916-5 Takayama,Ikoma, Nara, 630-0101, JAPAN
†† Faculty of Information Science and Electrical Engineering, Kyushu University
6-1 Kasuga-Koen, Kasuga, Fukuoka, 816-8580, JAPAN
E-mail: †hideki-s@is.naist.jp, suna@wide.ad.jp, ††{kitasuka, fukuda}@f.csce.kyushu-u.ac.jp

Abstract To configure the ad-hoc network in the neighborhood of the access point of wireless LAN, we aim at construction of the system that provides the internet connectivity to the terminals. Thus, when a terminal acts as intermediary, we think that the use area of an access point is temporarily expandable. In this paper, we describe the configuration of the ad-hoc network in the neighborhood of the access point. Moreover, we propose the management method of the terminals that configure the ad-hoc network, to prevent the spoofing of terminals.

Key words Mobile Computing, Ad-hoc Network, Internet, Wireless Network

1. はじめに

計算機の高性能化に加え，ネットワークのブロードバンド化や常時接続が普及し，インターネットから情報を収集することが一般的になっている．インターネットは，従来から存在するクライアント/サーバ型の情報配信システムであるが，各端末がクライアントとサーバそれぞれの役割を担うピア・ツー・ピア (Peer-to-Peer, P2P) 型のアプリケーションも一般的になりつつある [1].

また，ネットワークのブロードバンド化に伴い，無線ネットワークシステム (IEEE802.11b/a) は社内や家庭内への普及しており，IEEE802.11g など，より通信速度の速い製品も普及しつつある．一般的に利用されている基地局を利用したシングルホップの無線ネットワーク接続だけでなく，各端末が中継を行い，自律的にネットワークを構成しネットワーク接続を行うシステムも実現されている [2]. さらに，街中で利用できるホットスポットなどの公衆無線 LAN 網が提供されてきており，屋内だけ無く，屋外においても使用できる環境が整いつつある．これらを利用することにより，いつでも，どこでも高速なネットワークサービスを利用することができるようになる．

このような屋外において無線ネットワークシステムを利用例として，Mesh Networks 社(注1)による ITS(Inteligent Transport Systems) における情報提供などが挙げられる．

このような無線ネットワークデバイスの普及に伴い，固定のネットワークシステムを利用しないワイヤレス P2P システムを利用した仕組みが数多く提案されている．中でも，代表的な研究としてアドホックネットワークが注目されている．アドホックネットワークとは，無線の特性を利用し，端末が集まり，その場その場で構成される動的なネットワークである．従って，固定のネットワークと異なり，インフラストラクチャを必要としないため，目的端末への経路を設定するためのルーティングが大きな問題となる．また，このルーティングによってスケーラビリティの問題も生じる [3]．アドホックネットワークの研究では，このルーティングの技術は，IETF(Internet Engineering Task Force)(注2)の Mobile Ad-hoc Networks Working Group(注3)を中心に，様々な提案，研究がなされており，標準化が進められている．しかし，アドホックネットワークの仕組みのみを利用するアプリケーションは，あまり一般的には普及していないのが現状である．アドホックネットワークの技術を利用し，セルラー電話などの固定のネットワークを併用した研究もなされている [4] [5] [6]．

このような背景のもと，無線ネットワークの利点を生かし，有線ネットワークを用い，無線ネットワークの欠点を補うことにより，アドホックネットワークの利用範囲が広がると考えられる．また，街中に数多く存在するホットスポットを共有し，協調しあうことができれば，既存のインフラを用いアドホックネットワークを利用して，日常的に利用することができる様々な応用を考えることが可能であると考えられる．

そこで，ワイヤレス P2P システムを利用した仕組みとして，アクセスポイントへのアドホックネットワークを利用し，インターネット接続を可能にするシステムを提案する．本システムを利用することにより，アクセスポイントからの電波が届かない端末もアドホックネットワークを形成し，各端末が中継を行うことにより，インターネットサービスを利用することが可能になる [7]．本稿では，アクセスポイント近辺でのアドホックネットワークの構成方法，また，構成する端末の管理方法について述べる．

2. 提案システム概要

2.1 システム構成

提案システムにおける各端末の構成を図 1 に示す．システム内では，無線ネットワークデバイスを装備した計算機，無線 LAN の基地局となるアクセスポイントのみで構成され，システム固有の機器は不必要である．

図 1 のようにアクセスポイントの電波到達エリア内 (図 1 中の破線の円で囲まれた内部) に存在する移動端末は，アクセスポイントと直接，接続を行いインターネットに接続することが可能である．さらに，提案システムでは，アクセスポイントの電波到達エリア外に存在する端末も，各端末が中継を行いマルチホップでアクセスポイントのエリア内に存在する端末と接続し，インターネット接続性を取得する．

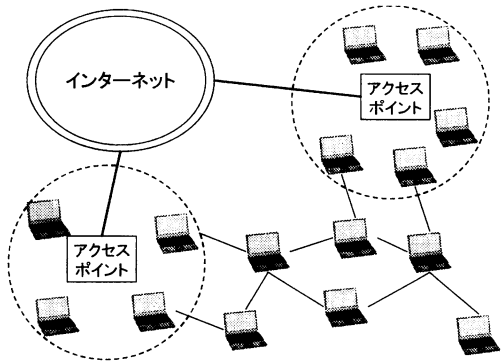

図 1 提案システム概要

一般的な無線 LAN システムとは異なり，提案システムでは，アクセスポイント近辺においてアドホックネットワークを構成する．このため，各端末は中継機能を持っており，他の端末が送信したリクエストを中継し，リクエストをアクセスポイント，インターネット上へと送信する．提案システムにおけるデータのやり取りを，以下に示す．

(1) 送信元端末は，近隣に存在するアクセスポイントを探索し，検出する．

(2) アクセスポイントの選択を行い，検出時に取得した中継端末情報を用い，アクセスポイントに対してリクエストを送信する．

(3) 中継端末は，送信元端末から送信されたリクエストの中継を行う．

(4) アクセスポイントにリクエストが到達すると，アクセスポイントはリクエストをインターネットに対して送信する．

(5) アクセスポイントにデータが届けられ，再び中継端末を経由し，送信元端末にデータが届けられる．

2.2 応 用 例

無線ネットワークデバイスを用い，このように他の端末によってパケットが中継されるためセキュリティの問題が考えられる．しかし，これにより，一時的にアクセスポイントを利用することができるエリアを拡大することができ，有効にアクセスポイントを利用することが可能になる．さらに，人口の密集地域などでは中継端末数が増加すると考えられるので，アクセスポイントの設置数を削減することも期待される．

提案システムでは、屋内/屋外においてアクセスポイントを利用しインターネット接続が可能であるので，応用例として、ワイヤレス IP 電話などが考えられる．既に設置されているアクセスポイントを利用することができれば，新たに基地局や中継局を設置する必要がないので，低コストで携帯可能な電話システムを利用することができる．また，移動端末の特性として

(注1) : Mesh Networks : http://www.meshnetworks.com/
(注2) : IETF : http://www.ietf.org/
(注3) : MANET Working Group : http://www.ietf.org/html.charters/manet-charter.html

挙げられるモビリティの特性を考え，位置情報と連携することにより，歩行者/移動体のナビゲーションに利用可能であると考えられる[8].

3. アドホックネットワークの構成

提案システムでは，各端末間においてアドホックネットワークを構成し，データの送受信を行う．端末は，初期状態ではアクセスポイントの情報や近隣に存在する端末の情報を持っていない．このような端末が，近隣の端末と通信を行う場合は，アドホックネットワークのルーティングプロトコルを利用し，目的端末への経路情報を取得することができる．しかし，インターネット上のデータを要求するためには，アクセスポイントの情報を取得する必要がある．

そこで，データの送受信する前にアクセスポイントまでの経路を調べる「アクセスポイント探索フェーズ」，アクセスポイントの情報を取得後，通信を行うアクセスポイントを決定する「アクセスポイント選択フェーズ」，そして，データを実際に送受信する「通信フェーズ」のこれら3つに分けてデータのやり取りを行う．本節では，これら3つのフェーズについて，それぞれの処理の概要を述べる．

3.1 アクセスポイント探索フェーズ

インターネット上の端末とデータのやり取りを行う端末は，まず近隣に存在するアクセスポイントの所在を把握しなければならない．また，端末は，周囲に存在する端末の情報を持っていない．そこで，端末間でアドホックネットワークを構成し，近隣の端末よりアクセスポイントの情報を取得する．

アクセスポイントの電波到達エリア内に存在する端末は，アクセスポイントから定期的に送信されるビーコンを受信している．提案システムでは，電波到達エリア内に存在する端末は，このビーコンをアドホックネットワーク内の端末に対して転送を行う．このようにして，アドホックネットワークを構成する端末は，アクセスポイントの情報を取得する．Reactive 型のルーティングプロトコルを使用した際のアドホックネットワークの構成，アクセスポイントの情報取得の流れを図2と共に以下に示す．

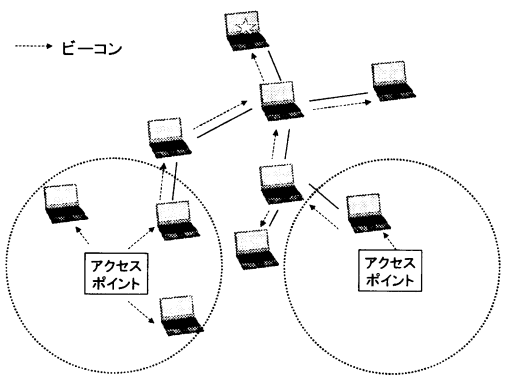

図2 アクセスポイント探索フェーズ

（1） 送信元端末は，近隣の端末に対して，アドホックモードで通信を開始し，パケットを送信し，近隣に存在する端末とアドホックネットワークを構成する．

（2） アドホックネットワークに参加し，パケットの中継を行うことにより，アドホックネットワークに属する端末情報を取得する．

（3） 参加する中で，アクセスポイントから送信されるビーコンが中継され，送信元端末が受信する．これによって，アクセスポイントの情報を取得する．

このようにして，端末はアドホックネットワークを構成し，近隣の端末からアクセスポイントの情報を取得する．

3.2 アクセスポイント選択フェーズ

アクセスポイント探索フェーズでは，送信元端末は近隣に存在するアクセスポイントの情報を取得し，要求を送信することが可能になる．しかし，図2のように複数のアクセスポイントが近隣に存在する場合が想定される．このような場合，複数のアクセスポイントを併用し，データの送受信を行う仕組みも考えられるが，複数のアクセスポイントを利用すると中継端末が増加する．従って，経路を維持するために端末間で送信される不用なパケット量が多くなると考えられる．さらに複数のアクセスポイントを併用すると，一つの無線ネットワークデバイスに対して複数の IP アドレスが割り当てられ，ネットワークのコネクションを保持することができなくなる．そこで本システムでは，各端末は一つのアクセスポイントを選択し，通信を行う．

このアクセスポイントの選択基準として，アクセスポイントへの経路のホップ数，電波強度，また，アクセスポイントの使用台数，設置場所などが挙げられる．設置場所を利用するためには，各端末が GPS などの位置情報取得デバイスを備える必要があり，また，使用台数を調べるためには，アクセスポイントの管理権限が必要になるため，難しいと考えられる．今後，ホップ数，電波強度を中心に選択基準の定式化を行う予定である．

3.3 通信フェーズ

今までの処理において，通信を行うアクセスポイントの情報を取得し，決定している．この通信フェーズでは，端末は実際にアクセスポイントへリクエストを送信し，インターネットからデータの取得を行う．その流れを図3と共に以下に示す．

（1） 送信元端末は，アクセスポイント選択フェーズにて決定したアクセスポイントに対して，アドレスを要求するために，アドレス要求パケットを送信する．このアドレス要求パケットの宛先は，アクセスポイントとなる．

（2） アドレス要求パケットを受信した端末は，中継を行い隣接端末に対して送信する．

（3） アドレス要求パケットがアクセスポイントに到着すると，送信元端末に対して IP アドレスを割り当て，確認応答パケットを送信元端末に対して送信する．

（4） 送信元端末は，IP アドレスを取得するとアクセスポイントに対してリクエストを送信する．

（5） アクセスポイントは，送信元端末からのリクエストをインターネット上へ送信する．インターネットからデータを受

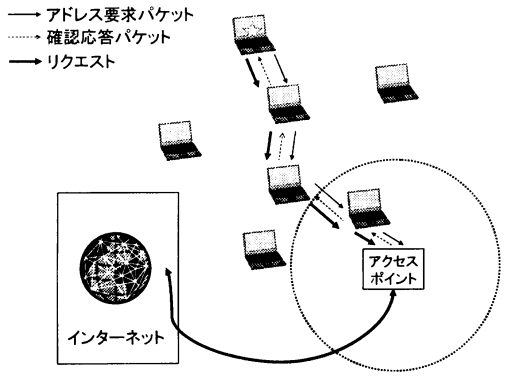

図 3　通信フェーズ

信し，アクセスポイントはリクエストの逆経路で送信元端末に対して，データの送信を行う．

4. アクセスポイントの探索

本章では，アクセスポイント探索フェーズの詳細について説明する．提案システムでは，各無線端末において，アドホックネットワークが構成されている状況を想定している．アクセスポイントの情報を伝播させるビーコンは，アドホックネットワーク上で使用されているルーティングプロトコルを用いて送信される．提案システムは，Proactive 型，Reactive 型など多様なプロトコルに対応することが可能である．Proactive(table driven) 型，Reactive(On-demand) 型それぞれの場合における動作を以下に述べる．

* Proactive 型

Proactive 型のルーティングプロトコルは，table-driven 型とも呼ばれるように，通信を行う前にあらかじめ他の端末とルート情報の交換を行い，経路表の作成を行う．常に他の端末との接続関係を管理しているため，近隣に存在するアクセスポイントをすぐに検出することが可能である．しかし，トポロジーの変化に対処するため，端末の移動に対して脆弱であり，端末数が多くなるとルーティングテーブルの管理が難しいという欠点がある．

Proactive 型の代表的なアドホックネットワークルーティングプロトコルの一つである Optimized Link State Routing(OLSR) ルーティングプロトコル [9] を例にとり，説明する．OLSR 網がアクセスポイント近辺で構築されているものとする．

（1） ある端末 S が構築されている OLSR 網近辺に移動し，アドホックネットワークを構成する他の端末と OLSR を用いて経路情報の交換を開始する．

（2） 端末 S は，近隣の端末に対して HELLO メッセージの送信を行う．

（3） 近隣の端末は，定期的に周囲の端末と HELLO メッセージ，TC(Topology Control) メッセージなどを交換している．従って，各端末はアクセスポイントへの経路を持っていると考えられるので，端末 S からのメッセージを受け取った端末は，アクセスポイントへの経路を含むローカルリンク情報を端末 S に対して送信する．

（4） 端末 S は，ビーコンを隣接端末から受信し，アクセスポイントの情報を取得する．

（5） 端末 S は，ローカルリンク情報をもとに，アクセスポイントへの経路を設定し，リクエストを送信する．

* Reactive 型

Reactive 型のルーティングプロトコルは，on-demand 型とも呼ばれるように，通信要求が発生しない時には他の端末と通信を行わず，発生時に各端末がオンデマンドでルートの構築を行う．通信要求時のみ経路の構築を行うため，ルーティングテーブルを管理する必要がなく，端末の移動の影響が少なく，スケーラビリティの問題も Proactive 型と比べ有効である．しかし，通信要求が発生後に経路探索を行うので，リアルタイム性が必要な通信には不向きである．

Reactive 型のアドホックネットワークルーティングプロトコルの一つである Ad Hoc On-Demand Distance Vector(AODV) ルーティングプロトコル [10] を例にとり，説明する．AODV 網がアクセスポイント近辺で構築されているものとする．

（1） ある端末 S が構築されている AODV 網近辺に移動し，アドホックネットワークを構成する他の端末と AODV を用いて経路情報を交換を開始する．

（2） 端末 S は，ビーコンを隣接端末から受信し，アクセスポイントの情報を取得する．

（3） ある端末 S が通信要求を行う．端末 S は，Route Request(RREQ) パケットを近隣の端末に対してブロードキャストする．この RREQ の宛先アドレスはアクセスポイントである．

（4） RREQ パケットを受信した端末は，自身の経路表 (タイマ付) に端末 S の情報を加える．その後，受信した端末は，RREQ パケットの送信先端末であるアクセスポイントへのエントリを調べる．

経路表に存在した場合

Route Reply(RREP) パケットを作成し，送信元端末 S に対して送信を行う．このとき，この RREP パケットは各端末の経路表を元に送信される．アクセスポイントに RREQ パケットが到達した場合も同様の処理を行う．

経路表に存在しなかった場合

経路表にアクセスポイントのエントリを作成し，RREQ パケットの転送を行う．この動作が経路表にアクセスポイントへのエントリが見つかる，もしくは，アクセスポイントに到達するまで繰り返される．

このように Proactive 型のプロトコルでは，どのような端末が近隣に存在しているかを定期的に監視しているため，Reactive 型のプロトコルよりも簡単にアクセスポイントの検出を行うことが可能である．しかし，どちらのタイプのプロトコルも利点，欠点がある．提案システムでは，どちらのタイプが使用されていても上記のように対応できるため，その利用用途に応じて使い分けることができる．

5. 構成端末の管理方法，認証方法

アドホックネットワークを構成するため，各端末のリクエストは他の端末を経由して，インターネットへ送信される．そのため，セキュリティや認証の問題が発生すると考えられる．本章では，そのために必要なインターネットへの認証方法について述べる．

5.1 問 題 点

一般的なシングルホップの形態の場合，アクセスポイントの利用者を認証するための計算機(認証サーバ)を設置し，そこで端末の認証を行う．ホットスポットサービスのようなアクセスポイントを利用し，インターネット接続を行うシステムにおける認証方法は以下のような流れになる．

（1） 端末は，全端末に共通であるアクセスポイントのESS-ID，WEP-KEYを設定する．

（2） アクセスポイントを検知すると，端末は，アクセスポイントからIPアドレスを割り当てられる．

（3） ブラウザを起動するなどし，端末は認証サーバと通信を行い，IDとパスワードの入力を行う．

（4） IDとパスワードが一致するとコネクションが確立される．

このような形式でネットワーク接続する際，成りすましによるセキュリティの問題が生じる．成りすましには，以下のような二つの形式が挙げられる．

端末の成りすまし

端末Aとアクセスポイントの通信を傍受し，端末A'が端末AのIPアドレス，MACアドレスの情報を取得し，WEP-KEYの暗号を解読する．そして，端末A'が認証サーバと通信を行い，コネクションを確立する，その後は，認証サーバは，IPアドレスとMACアドレスでパケットを識別するため，端末A'がIPアドレス，MACアドレスを偽装することによって，成りすましが発生する．

アクセスポイントの成りすまし

設置されている正式なアクセスポイントAのWEP-KEYの暗号を複合化し，ESS-ID，周波数チャネルを把握する．これらの情報をもとに，同一のWEP-KEY，ESS-ID，周波数チャネルを持つアクセスポイントA'を設置する．そのアクセスポイントA'に，端末が接続し，その端末が利用したIDとパスワードが漏洩し，成りすましが生じる．

5.2 管 理 方 式

提案システムの特徴として，シングルホップではなく，マルチホップさせる点が挙げられる．提案システムのようなマルチホップ接続においても，同様の問題が想定される．マルチホップ接続では，各端末が中継を行うため，他の端末のIPアドレスやMACアドレスが，より多くの端末に伝播すると考えられる．より信頼性の高い通信を提供するためには，どの部分に対する信頼性を挙げるかが重要になる．その部分として，以下のような箇所が考えられる．

（1） 各端末間の全経路

（2） 端末と認証サーバ間

(1)の部分において信頼性を高めることを考えると，完全に端末間がセキュアになり，成りすましを防ぐことができる．しかし，アドホックネットワークのように端末が自律的に形成するネットワークでは，端末間の関係が複雑になり難しいと考えられる．一方，(2)の部分について考えると，端末間は自由に通信することが可能になり，インターネットに対しては，認証を行うことになるので，不正なインターネットに対するアクセスを軽減することができると考えられる．

そこで，今回は端末間と認証サーバ間に絞り，よりセキュアな通信環境を提供する仕組みの構築を目指す．具体的には，PKI(Public Key Infrastructure)の技術を用いて，個々の端末の証明に利用する．

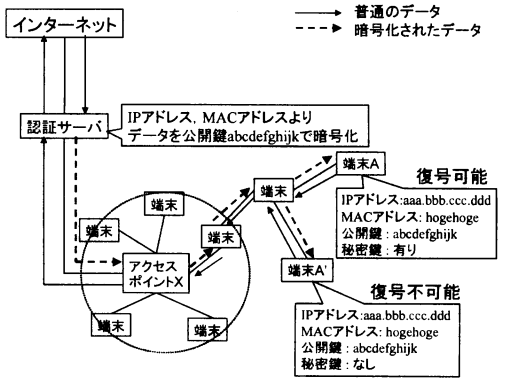

図4 認証方法

図4のように各端末は，認証サーバと通信を行う際，IDとパスワードに加え，公開鍵を登録する．インターネットに対してデータの送受信を行う場合，全てのパケットは認証サーバを経由して送信される．返答パケットを認証サーバにおいて，公開鍵を用いて暗号化し，アドホックネットワーク網に送信する．このようにすることによって，成りすまし端末(図4内の端末A')が返答パケットを受信しても，公開鍵に対応する秘密鍵を持っておらず，復号することができない．また，成りすまし端末がインターネットに対してデータを送信した場合においても，返答パケットは，成りすましたIPアドレス，MACアドレスに対応する公開鍵で暗号化されるため，データを解読することができない．

また，端末間でアドホック通信を行う場合も，この公開鍵を他の端末に伝播させることによって，端末間でセキュアな通信環境を構築することができると考えられる．

6. ま と め

本稿において，端末がアクセスポイント近辺で，アドホックネットワークを構成し，アクセスポイントを利用して通信を行うシステムの提案を行った．これにより，アクセスポイントの電波到達エリアを一時的に拡大することが期待できる．さらに，PKIを用いたインターネット接続する際の問題点となる端末の成りすましを解決する仕組みの提案を行った．

今後の課題としては，近隣に複数のアクセスポイントを検出した際に，最適なアクセスポイントへのルートを選択する仕組みについてシミュレーションを通し評価を行うことが挙げられる．ホップ数を対象とした評価を現在進めており[11]，電波強度に関してもシミュレーションを行う予定である．また，認証機構を想定し，通信負荷がどのようになるかシミュレーションを行う予定である．

文　献

[1] H. Shimada, S. Tagashira, T. Nakanishi, A. Fukuda : "Evaluation of a Location Management System for Wireless Communicating Mobile Computers", Proc. of the 16th Int. Conf. on Information Networking (ICOIN), Vol.I, pp. 3C-5.1–5.11 (2002).

[2] MOTERAN(Mobile Telecommunication Radio and Relay Network) : http://www.mitsubishi.co.jp/ndesk/newsr/020702.html

[3] X. Hong, K. Xu, M. Gerla : "Scalable Routing Protocols for Mobile Ad Hoc Networks", IEEE NETWORK, July/August 2002, Vol.16, No. 4, pp. 11–21 (2002).

[4] Y. Shimotsuma, T. Sakakura, K. Yoshida, M. Kuroda, T. Mizuno : "Percolating Data Delivery on Cellular-Ad Hoc Integrated Network", IEICE transactions on communications, Vol.84E-B, No.4, pp. 771–778 (2001).

[5] R. Wakikawa, J. T. Malinen, C. E. Perkins, A. Nilsson, A. J. Tuominen : "Global connectivity for IPv6 Mobile Ad Hoc Networks", IETF Internet draft, http://www.wakikawa.net/Research/drafts/draft-wakikawa-manet-globalv6-02.txt (2002)

[6] 島田 秀輝, 田頭 茂明, 中西 恒夫, 福田 晃 : "複数のアドホックネットワークを結合した環境における通信制御システムの提案", マルチメディア, 分散, 協調とモバイル (DICOMO2002) シンポジウム論文集, pp. 93–96 (2002).

[7] H. Shimada, S. Tagashira, T. Kitasuka, T. Nakanishi, A. Fukuda : "Proposal of Wireless Peer-to-Peer System using the Wireless Multi-Hop Network to access Wireless Hot Spot", Proc. 2003 Int. Conf. on Parallel and Distributed Processing Techniques and Applications(PDPTA2003), Vol.II, pp. 977–881 (2003).

[8] Y.-C. Tseng, S.-L. W. W.-H. Liao, C.-M. Chao : "Location Awareness in Ad Hoc Wireless Mobile Networks", IEEE COMPUTER, June 2001, pp. 46–52, (2001).

[9] T. Clausen, P. Jacquet : "Optimized Link State Routing Protocol (OLSR)", RFC 3626, http://www.ietf.org/rfc/rfc3626.txt (2003).

[10] C. Perkins, E. Belding-Royer, S. Das : "Ad Hoc On Demand Distance Vector (AODV) Routing", RFC 3561, http://www.ietf.org/rfc/rfc3561.txt (2003).

[11] 島田 秀輝, 田頭 茂明, 北須賀 輝明, 中西 恒夫, 福田 晃 : "無線マルチホップネットワークを利用したインターネット接続システムの提案", マルチメディア, 分散, 協調とモバイル (DICOMO2003) シンポジウム論文集, pp. 405–408 (2003).