

高密度無線LAN環境における 仮想化技術を用いたアクセスポイント集約機構

永井 隆博^{1,a)} 重野 寛²

受付日 2011年5月19日, 採録日 2011年11月7日

概要: 無線LANにおいてアクセスポイント(AP)の配置や使用チャネルを適切に決めることは、電波干渉を抑制して無線端末(MN)がAPと効率的に通信するために重要である。しかし実際にはAPは適切に配置・設定されていないことが少なくない。そのため、APの高密度な存在により電波干渉が生じ、スループットが低下する場合がある。解決策の1つは余分なAPの停止だが、それには停止するAPの機能の存続が必要となる。本論文ではAPの機能を集約するVAPアグリゲーションを提案する。1つのAPに複数のAPの機能を集約することで、使用するAP数を低減させることができる。集約には複数のAPの機能の実現と、MNの通信の維持が必要である。そこでAPの仕組みに仮想化技術を用いる。また、通信の維持のために仮想ネットワークを構築する。そして本提案のプロトタイプの実装を行い、VAPアグリゲーションが可能であり、またスループットの改善を期待できることを確認した。

キーワード: 無線LAN, アクセスポイント, 仮想ネットワーク

AP Aggregation Using Virtualization Techniques for High Density WLANs

TAKAHIRO NAGAI^{1,a)} HIROSHI SHIGENO²

Received: May 19, 2011, Accepted: November 7, 2011

Abstract: In Wireless LANs, It is important for mobile nodes (MNs) to decide the placement and channel of access points (APs) effectively. However, chaotic unplanned AP configurations become the norm rather than exceptions and cause interferences. One of solutions is to bring down extra APs, but maintenance of functions of the APs is necessary for it. In this paper, we propose VAP Aggregation which aggregates AP functions. By aggregating AP functions to one AP, we can reduce the number of APs. It is necessary for VAP Aggregation to run multiple AP functions and to connect between MN and the own domain. We use virtualization techniques for framework of AP. And we use virtual network for communication. In addition, we implemented a prototype system. We confirmed that VAP Aggregation is available and showed improvement of the throughput.

Keywords: Wireless LAN, access point, virtual network,

1. はじめに

無線LANにおいて、アクセスポイント(AP)の配置や使

用する無線チャネルを適切に決めることは無線端末(MN)が効率的な通信を行うために重要である。このため、APの配置場所や無線チャネルの割当てに関する研究が行われている [1], [2], [3], [4]。配置するAPの数は少ないほうが設置コストが少なく済み、また、接続するAPや無線チャネルを適切に決めれば電波干渉を低減させることができるため効率的な通信が期待できる。

しかし実際にAPを設置する場合、各ドメインの管理者

¹ 慶應義塾大学大学院理工学研究科
Graduate School of Science and Technology, Keio University,
Yokohama, Kanagawa 223-8522, Japan

² 慶應義塾大学理工学部
Faculty of Science and Technology, Keio University, Yokohama,
Kanagawa 223-8522, Japan

a) nagai@mos.ics.keio.ac.jp

で必ずしも連携がとれているわけではない。オフィスや大学のキャンパスのように地理的に狭い範囲に多くのドメインが密集する場所では、AP が高密度に存在することがあり AP 間で電波干渉が生じる。AP 間の電波干渉はパケットエラーレートを増加させるため、効率的な通信の観点から問題である [5]。

ドメイン間の連携により AP 数を低減させると、複数のドメインが1つの AP を使用する状況が生じるが、ドメインごとに AP に施したい設定は異なる。現在、物理的な AP の所有とその管理は不可分であり、1つの AP 内で同時に複数のドメインのネットワークが動作することは一般的ではない。そのため、一方を優先させるともう一方のドメインの AP の機能を維持できない。AP 数の低減には AP の機能を維持できるように、AP の所有と管理を分離し柔軟に AP を管理できる仕組みが必要である。

本論文では仮想化技術を用いて AP の機能を AP から分離して集約する Virtual Access Point アグリゲーション (VAP アグリゲーション) を提案する。Virtual Access Point (VAP) とは AP の機能であり、VAP を可能にする機器を Physical Access Point (PhyAP) と呼ぶ。そして、ある PhyAP 上で動作する VAP を他の PhyAP へ移動させ、複数の VAP を特定の PhyAP へ集めることを VAP アグリゲーションとする。VAP アグリゲーションにより、各ドメインの AP の機能を維持したまま、起動する PhyAP 数を低減させることができる。VAP アグリゲーションの実現には、複数の VAP が PhyAP で動作できること、VAP の移動後も MN の通信を維持できること、VAP を移動できることが必要である。そこで、これらを PhyAP アーキテクチャ、L2 フラットネットワーク、管理フラットネットワーク、VAP マイグレーションの4つの仕組みで実現する。また、VAP アグリゲーションのプロトタイプシステムの実装を行った。プロトタイプシステムにより MN の通信を維持しつつ VAP を集約できること、スループットを改善可能であることを確認した。

以下、2章で関連研究とその問題点を明らかにし、3章で VAP アグリゲーションを提案する。そして4章でプロトタイプシステムの実装と評価について述べ、5章に結論を示す。

2. 関連研究

2.1 AP の管理とネットワーク仮想化

大学のキャンパスのような場所では、各ドメインの管理者それぞれが AP を設置することが少なくない。図 1 に各管理者が AP を設置している様子を示す。各部屋に1つのドメインがあり、各ドメインが自身のドメイン内に AP を配置している。チャンネル数には限りがあるため、AP 数が増加すると使用するチャンネルの間隔が狭まりパケットの衝突頻度が高まる。本研究では、このようなチャンネル割

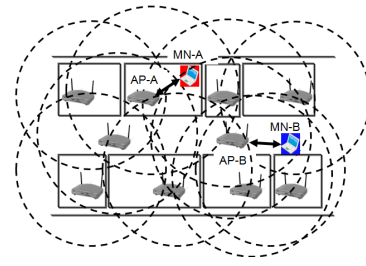


図 1 高密度な無線 LAN
Fig. 1 High-density WLANs.

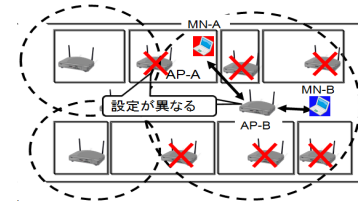


図 2 解決した状態
Fig. 2 One solution for High-density WLANs.

当てに余裕がない状況を想定している。問題の解決策として、必要最低限の AP のみを使用することが考えられる。文献 [6], [7], [8] では最適な AP 選択について、AP や MN のカバーエリアやトラフィック量を考慮し、使用すべき AP や最適な MN の接続先およびそのチャンネルの決定方法が示されている。図 2 に AP 選択の例を示す。適切な AP の選択により干渉を低減させることができる。それには MN の接続先の変更が必要となるが、通常、ドメインごとに提供されるサービスやポリシーは異なるため MN は接続を変更できない。サービスとはサーバから提供されるメールやウェブページなどである。ポリシーとは通信品質やセキュリティなど、ネットワークの運用規定である。必要最低限の AP のみを使用するには AP-B 上で AP-A, B の両方のサービス・ポリシーを実現する必要がある。

MN に合わせた通信設定を提供するために、LWAP (LightweightAP) と WLC (Wireless LAN Controller) を用いたシステムがある [9]。LWAP の設定はエントリとして WLC に格納され、MN の IP アドレス、セキュリティコンテキスト、QoS などが登録されている。MN が LWAP にアソシエーションする際、WLC から設定をダウンロードすることで MN に合わせた設定で通信できる。また、1つの AP で複数の SSID を保持でき、SSID ごとにキャプティブ・ポータルや任意の暗号化/認証タイプの組合せをサポートする製品がある [10], [11]。

また、ネットワークの管理に仮想化を用いる研究が行われている。VROOM [12] はルータを仮想化する研究である。仮想ルータを構築し物理的なルータ間の移動を可能にすることで新しいルータ管理の方法を提示している。文献 [13] はプログラマブルなネットワークの共存を可能にするアーキテクチャとしてのネットワーク仮想化を述べて

いる。また、文献 [14] では AP の仮想化が示されている。AP の仮想化により、物理的な AP と AP の機能を分離することで無線 LAN をより柔軟に管理するコンセプトを提案している。

2.2 関連研究の問題点

文献 [9], [10], [11] は LWAP や WLC, 複数の SSID の保持により 1 つの AP に複数の設定を行うことできる。しかし、それらは 1 人の管理者による AP の管理を想定しており、AP ごとに AP の管理者が異なる状況は想定されていない。そのため、1 つの AP・WLC 上で動作する OS は 1 つのみである。最低限の AP は無線と有線をブリッジ接続するが、実際には管理用アプリケーションや DHCP やルーティングの機能を持つなど AP は多様化しており、様々なアプリケーションが動作する。導入するアプリケーションは OS により制限されるため、各ドメインの管理者が扱えるアプリケーションはその OS がサポートする範囲までである。そのため、管理者が希望するサービス・ポリシーを実現できない可能性がある。

また、ルータにおける VROOM のような仮想化の仕組みは AP においてはまだ実現されていない。文献 [14] では AP をより柔軟に管理するための仮想 AP のコンセプトが示されているが、具体的な仕組みは実現されていない。AP を柔軟に管理し AP 数を必要最低限にするには、1 つの AP で各ドメインの AP が動作できる仕組みが必要である。

3. VAP アグリゲーション

3.1 VAP アグリゲーションの概要

本論文では、仮想化技術を用いて AP を仮想化しその仮想化した AP を集約する Virtual Access Point アグリゲーション (VAP アグリゲーション) を提案する。仮想化された AP を Virtual AP (VAP) と呼び、VAP が動作する環境を提供する計算機を Physical AP (PhyAP) と呼ぶ。VAP は仮想化技術による仮想マシンに加えて無線インタフェースの構成情報である無線インタフェースの IP アドレス, MAC アドレス, SSID を持つ。そして、VAP アグリゲーションとは複数の VAP を特定の PhyAP へ集めることである。VAP アグリゲーションにより、各 AP のサービス・ポリシーを維持したまま起動する AP 数を低減させることができる。

図 3 に VAP アグリゲーションの例を示す。図 3(a) で PhyAP-A, B, C それぞれにおいて VAP-A, B, C を作成する。次に図 3(b) で VAP-B, C を PhyAP-A に集約する。PhyAP-A は VAP-A に加えて VAP-B, C を実現し、ドメイン B, C への通信を可能にする。アグリゲーション後、VAP を持たない PhyAP-B, C は動作する必要がない。また、ドメイン B, C の MN はそれぞれ VAP-B, C に接続することでドメイン B, C と通信できる。したがって、

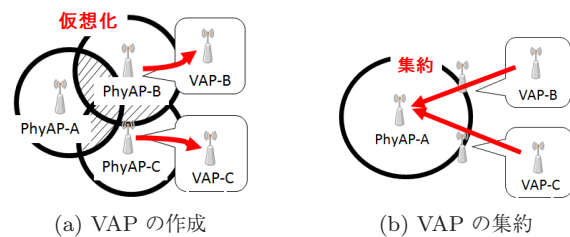


図 3 VAP アグリゲーション

Fig. 3 VAP aggregation.

MN の通信を維持しながら PhyAP 数を低減させることができる。

また、VAP アグリゲーションにおける技術的課題として、1 つの AP 上での複数の AP の機能の動作, MN の通信の維持, リソース情報などの把握, AP の機能の移動, マイグレーションによるカバレッジの変化があげられる。カバレッジの変化については AP 選択の研究 [6], [7], [8] を利用可能である。AP 選択により求められた使用すべき PhyAP が使用中の PhyAP とは別の PhyAP であった場合に VAP を移動する。これらが VAP アグリゲーションにおいても最適である保証はないが、カバレッジやトラヒックを考慮した AP の選択が可能である。本論文では他者が管理する AP においても自身が管理する AP の機能を維持する仕組みの実現に主眼を置き、1 つの AP 上での複数の AP の機能の動作, MN の通信の維持, リソース情報などの把握, AP の機能の移動の実現方法について述べる。

3.2 VAP アグリゲーションの必要条件

VAP アグリゲーションの実現には 4 つの技術が必要である。

1 つ目は PhyAP アーキテクチャである。PhyAP アーキテクチャは無線インタフェースの構成情報を扱い、複数の VAP の動作を実現する。VAP の実現には仮想化技術による仮想マシンに加えて無線インタフェースの構成情報が必要である。しかし、仮想化技術では無線インタフェースの構成情報を扱っていない。また、VAP の集約により複数の VAP が 1 つの PhyAP 上で動作するため、PhyAP 上で同時に複数の VAP が動作できる必要がある。

2 つ目は L2 フラットネットワークである。L2 フラットネットワークにより自身のドメインとの通信および VAP ごとの通信の独立を行う。そもそも AP は MN を自身のドメインに接続する機能を提供するため、VAP が集約された場合でも自身のドメインと通信できる必要がある。また、PhyAP で複数の VAP が動作する際に、セキュリティの問題やポリシーの内容が相反するという問題があるため、VAP ごとに通信が独立である必要がある。

3 つ目は管理サーバと管理ネットワークである。管理サーバと管理ネットワークは、VAP アグリゲーションが可能かどうかを判断するために、リソースの情報を収集し指

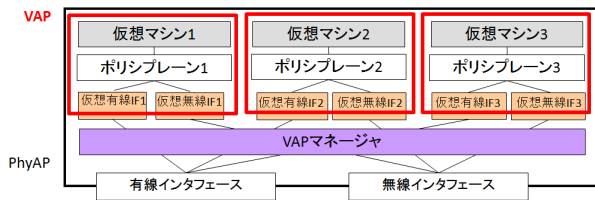


図 4 PhyAP アーキテクチャ
Fig. 4 PhyAP architecture.

示を出す仕組みである。PhyAP の持つリソース量や VAP が消費するリソース量などの情報を収集し、VAP アグリゲーションの指示を行う、

4つ目は VAP マイグレーションである。VAP の PhyAP 間の移動を実現するためには、仮想化技術による仮想マシンの移動に加えて無線インタフェースの構成情報の移動が必要である。VAP マイグレーションにより、VAP の移動を実現する。

以下の 3.3 節から 3.6 節でそれぞれの詳細を述べる。

3.3 PhyAP アーキテクチャ

PhyAP アーキテクチャは VAP を動作させる環境を提供する PhyAP の仕組みである。図 4 に PhyAP アーキテクチャを示す。PhyAP アーキテクチャは VAP マネージャ、有線インタフェース、無線インタフェース、VAP からなる。VAP マネージャは VAP を制御するプログラムであり、仮想マシンの作成、各 VAP のポリシープレーンの作成、仮想有線インタフェースと仮想無線インタフェースの作成を行う。

VAP は仮想マシン、ポリシープレーン、仮想有線インタフェース、仮想無線インタフェースからなる。仮想マシンでは OS とアプリケーションが動作し、サービスが実現される。また、ポリシープレーンによりポリシーを実現する。ポリシープレーンとは VAP のポリシーを実現する設定である。仮想有線インタフェースは MAC アドレス、IP アドレスを持ち、3.4 節で説明する L2 フラットネットワーク上のインタフェースとして使用される。仮想無線インタフェースは SSID、MAC アドレス、IP アドレスを持ち、マスターモードとして動作し MN との通信に使用される。文献 [15] で示されるように、仮想無線インタフェースの多重化は時分割多重が適している。そこで、仮想無線インタフェースは時分割多重により 1つの物理インタフェース上に多重化されるものとする。そのため、1つの PhyAP 内の VAP 同士ではパケット衝突は生じない。

AP の機能の実現のために仮想化技術による仮想マシンを用いることは、必要な計算機のリソース量や計算能力の観点からコストが高い可能性がある。しかし、仮想マシンにより VAP ごとに OS を持つことができ、VAP を管理する管理者がそれぞれ自由に必要とする OS を保持できる。また、ドメインごとの AP の機能は仮想マシンの OS 上で実

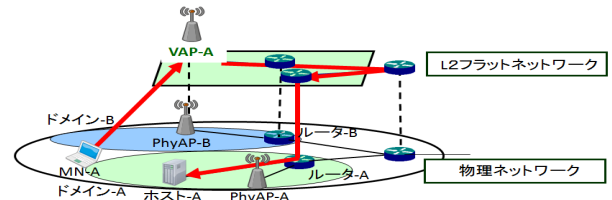


図 5 L2 フラットネットワーク
Fig. 5 L2 flat network.

行するため、機能を追加する場合 VAP の仮想マシンを変更すればよく、PhyAP の変更は必要ない。現在の現実的な AP のハードウェアでは 2, 3 台の VAP が 1つの PhyAP で動作できると考えられる。一方で、ドメインごとの AP の機能をアプリケーション単位で実現することも考えられる。必要な計算機のリソース量を低減させることができるが、VAP で提供されるサービスが PhyAP の持つアプリケーションに制限されるため、管理者が希望するサービス・ポリシーを実現できない可能性がある。また、管理やセキュリティの観点から、VAP とアプリケーションの数だけクォータの設定が必要となり管理が煩雑になることが想定される。

また、VAP ごとの QoS や firewall などのポリシーは VAP マネージャが VAP ごとに作成するポリシープレーンで実現する。VAP はそれぞれ固有のポリシーを持つことが考えられるが、PhyAP が許容する通信帯域幅など、リソースを超える場合はポリシーの調整が必要である。したがって VAP マネージャによる調整が可能となるように、VAP ごとのポリシーは仮想ホストの OS 上ではなく、仮想ホストの外部に設置した。

3.4 L2 フラットネットワーク

L2 フラットネットワークは MN が VAP に接続し自身のドメインと通信を行うための仮想ネットワークである。仮想ネットワークはネットワーク上のリソースを分割し、独立したネットワークを実現する技術である。図 5 に L2 フラットネットワークの例を示す。L2 フラットネットワークはルータ-A から PhyAP-B 間に構築され、データリンク層の仮想ネットワークと、データリンク層のトンネリングからなる。そのため、VAP が PhyAP-B に移動しても、MN は L2 フラットネットワークを通してドメイン-A に接続できる。また、L2 フラットネットワークにより VAP-A はマイグレーション後もドメイン A に接続しているように見えるため、VAP-A の位置によらず、設定を行う際は VAP-A の L2 フラットネットワーク上の IP アドレスを用いて接続する。一般的に、AP は設定のためにアクセス用の IP アドレスを保持する。同様に VAP もアクセスのための IP アドレスを保持する。VAP の IP アドレスは図 4 に示される仮想インタフェースが保持する。PhyAP-B 上の VAP-A の設定を行う場合は、VAP-A のための PhyAP-B 上の仮想イ

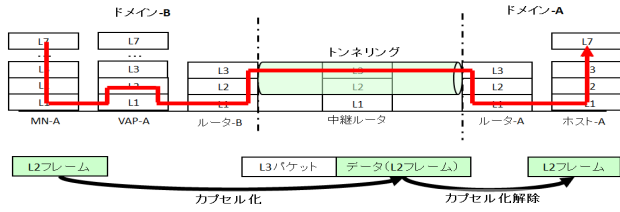


図 6 L2 トンネリング

Fig. 6 L2 tunneling.

インタフェースが保持するアドレスを用いて VAP-A へ接続し、設定を行う。

また、そもそも AP は L2 ブリッジとして使用されることが基本であるため、L2 のネットワークを提供することが必要である。そのため、L2 フレームをルータを通過させてドメイン-A に転送するためにトンネリングを行う。IP ルーティングによる転送も考えられるが、IP ルーティングでは中継の際に L2 フレームの書き換えが行われるため、ブリッジとしての機能を果たせない。L2 フラットネットワークにより他ドメイン内からでも自身のドメインへフレームを破壊せずに届けることができ、MN は VAP に接続することでドメイン-A に L2 レベルで接続できる。図 6 に L2 トンネリングの例を示す。図は MN-A が PhyAP-B 上の VAP-A に接続し、ドメイン-A のホストへ L2 フレームを送信の様子を示している。MN はホストへの宛先を持つフレームを送信する。それを受信した VAP は仮想有線インタフェースからフレームを転送する。フレームはルータにおいてカプセル化され、ドメイン-A へ転送される。ルータの管理は基本的にはそのルータを所有するドメインが行うが、管理サーバの依頼を受けてトンネルの作成、L2 フラットネットワーク用の仮想インタフェースの作成、仮想インタフェースとトンネルのインタフェースのブリッジングを行う。ルータ B の VAP 側のインタフェースには物理ネットワークのインタフェースのほかに L2 フラットネットワーク用の仮想インタフェースを用意する。ルータ B は仮想インタフェースとトンネルのインタフェースをブリッジングする。中継されるフレームは L3 まで上がるが、トンネル用の新たな L3 ヘッダを付与するために 1 度 L3 まで上げる必要があるためであり、L2 フラットネットワークのフレームに対してはブリッジングによりフレームが中継されるため経路制御は行われない。そして、ドメイン-A へ到着するとカプセル化が解除されホストへフレームが届けられる。また、VAP からトンネリングすることも考えられるが、ルータからトンネルを張ることで、VAP がドメイン内で移動した場合にトンネルの再構築の必要がない。

3.5 管理サーバと管理ネットワーク

管理サーバは PhyAP と VAP のリソースに関する情報の収集や停止する AP の選択、VAP マネージャへの指示を行

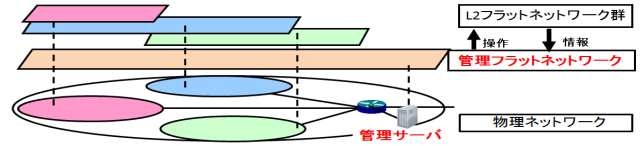


図 7 管理サーバと管理ネットワーク

Fig. 7 Administrative server and network.

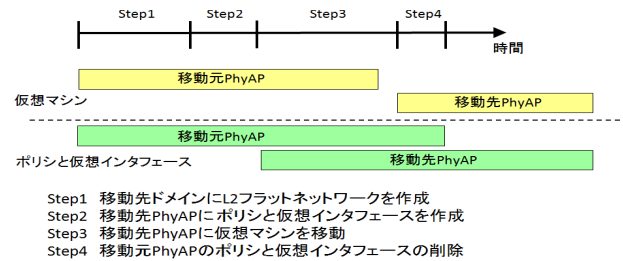


図 8 VAP マイグレーション

Fig. 8 VAP migration.

うサーバである。リソース情報は過剰に VAP を集約することによるリソース不足の把握や AP の選択のために使用され、CPU、メモリ、帯域幅、各 PhyAP と各 MN 間の信号強度や各 MN の通信量などがあげられる。管理ネットワークは管理サーバの制御情報の送受信に使用する L2 フラットネットワークである。図 7 に管理サーバと管理ネットワークを示す。管理サーバは VAP アグリゲーションを行う上位のドメインに設置される。管理ネットワークは VAP アグリゲーションを行うすべてのドメインのネットワーク上に構築する。これにより、管理サーバは全ドメインの PhyAP の VAP マネージャに指示できる。また、上位ドメインに設置された管理サーバから各ドメイン内の PhyAP と制御情報を交換するには、NAT やファイアウォールを通過しなければならない。そのため、VAP アグリゲーションを使用するドメインはあらかじめ管理ネットワークに参加する必要がある。

3.6 VAP マイグレーション

VAP マイグレーションとは、ある PhyAP 上で動作している VAP を他の PhyAP へ移動することである。VAP マイグレーションでは MN に対して透過的なマイグレーションを実現する。また、VAP マイグレーションは通信途中でのマイグレーションを前提としているため、VAP マイグレーションによるダウンタイムは可能な限り短い方が望ましい。そこで、仮想ホストとポリシ・仮想インタフェースを分けて移動する。図 8 は仮想マシンとポリシ・仮想インタフェースがそれぞれどちらの PhyAP で動作しているかを表している。VAP マイグレーションでは Step1 において、管理サーバが移動先のドメイン上に移動元のドメインの L2 フラットネットワークを作成する。これによりフレームは L2 フラットネットワークに転送されるようになる。Step2 では、移動元の PhyAP から移動先の PhyAP

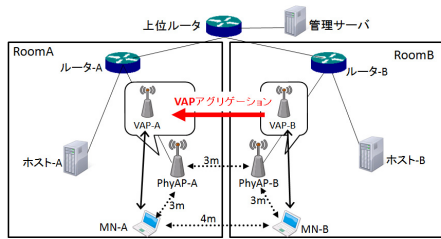


図 9 プロトタイプシステム的环境

Fig. 9 Prototype system environment.

へ VAP のポリシと仮想インタフェースの構成情報の情報を転送する。そして、移動先の PhyAP 上で VAP マネージャがポリシブレンと仮想インタフェースの作成を行う。これにより、VAP が移動先の PhyAP 上で動作しても移動元ドメインのネットワークを提供できる準備が整う。このとき、仮想インタフェースの移動では SSID や MAC アドレスなどが移動されるため、再アソシエーションを必要としない。Step3 では、仮想化技術による仮想マシンの移動を行う。移動先 PhyAP にはすでにポリシ・仮想インタフェースが存在するため、仮想マシンの移動後、パケットはただちに移動先 PhyAP 上の VAP を通過できる。また、Step3 終了直前のダウンタイムによりパケットロスが生じるが、ダウンタイムは十分に短いためセッションは維持される。Step4 では、移動元の PhyAP のポリシと仮想インタフェースの構成情報を削除し、VAP マイグレーションを終了する。

VAP のダウンタイムは仮想ホストの移動におけるメモリの移動にかかる時間のみである。VAP マイグレーションとして加えたポリシと仮想インタフェースの移動は一定時間移動元の PhyAP と移動先の PhyAP の両方に存在する。したがって、ポリシとインタフェースの移動にダウンタイムはなく、仮想化技術におけるマイグレーションのみにダウンタイムは影響される。また、VAP の SSID, MAC アドレス, IP アドレスも移動されるため、MN からは VAP マイグレーション前後で同一の AP を使用しているように見える。

4. プロトタイプシステムの実装と評価

4.1 プロトタイプシステム的环境

大学内の約 7.5m × 7.5m の隣接する 2 つの部屋にプロトタイプシステムを実装した。図 9 にプロトタイプシステムの実装環境を示す。各部屋を RoomA, RoomB とし、異なるドメインを構築した。実線部分のリンクは 100Base-T で結線されている。RoomA, B のドメインにはルータ, PhyAP, ホスト, MN が存在する。各 PhyAP と MN 間の距離は図 9 に示すとおりである。また、PhyAP-A, B 間の受信信号強度は互いに -45 dBm 程度、PhyAP-A と MN-A 間および PhyAP-B と MN-B 間は互いに -45 dBm 程度。MN-A, B 間は互いに -50 dBm 程度、MN-B と PhyAP-A

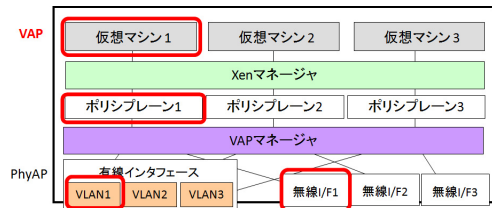


図 10 プロトタイプシステムにおける PhyAP アーキテクチャ

Fig. 10 PhyAP architecture for prototype system.

間は互いに -50 dBm 程度である。また、プロトタイプでは両ドメインを結ぶ上位のネットワークがあり、そこに管理サーバを構築した。なお、本環境では、実運用されている他の無線 LAN の AP が近隣に 30 台ほど存在したが、その影響をできる限り抑制するために実験以外のトラフィックが極力少ない休日に実験を行った。パケットをキャプチャした結果では、およそ 120 kbps 程度のトラフィックが検出された。

4.2 プロトタイプシステムの実装

4.2.1 PhyAP アーキテクチャ

プロトタイプシステムの PhyAP アーキテクチャを図 10 に示す。PhyAP アーキテクチャは Xen マネージャ, VAP マネージャ, 有線インタフェース (有線 I/F), 無線インタフェース (無線 I/F) からなる。VAP マネージャによって構築された VAP は仮想マシン, ポリシブレン, 仮想有線インタフェース (仮想有線 I/F), 無線 I/F からなる。

また、プロトタイプシステムでは Xen [16] を用いて仮想マシンを構築した。VAP マネージャは管理サーバからの指示により、Xen マネージャを用いた仮想マシンの構築, インタフェースの設定, ポリシブレンの生成を行う。プロトタイプシステムではポリシブレンの例としてトークンバケットフィルタによる帯域制限を行った。

仮想有線 I/F の作成には VLAN を用いた。各 VLAN が L2 フラットネットワークと接続するインタフェースとなり、VAP は自身のドメインとフレーム単位で通信できる。プロトタイプにおいては VAP が利用する有線の IP, MAC アドレスは仮想有線 I/F が保有する。

仮想無線 I/F の実現では、仮想化技術をサポートする WirelessNIC を調達できず、新たにインタフェースを設計・開発する必要があり困難であったため、仮想無線 I/F を作成する代わりに 1 つの VAP につき 1 つの実際の無線 I/F を使用した。Wifi の規格は 11g であり、マスタモードとして動作させた。また、この無線 I/F は VAP が利用する無線の SSID と MAC アドレスを持ち、MN とのネゴシエーションに利用される。VAP が無線の IP アドレスを持つ場合は仮想無線 I/F が持つ。

4.2.2 L2 フラットネットワーク

プロトタイプシステムにおいて L2 フラットネットワー

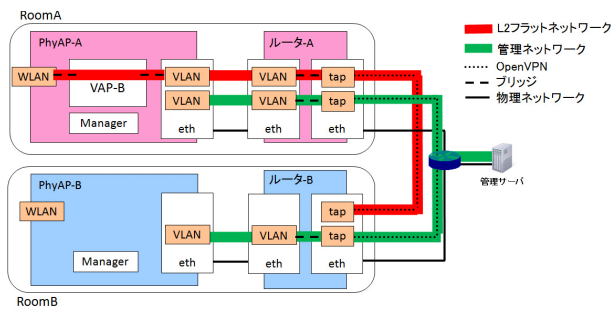


図 11 プロトタイプシステムにおける L2 フラットネットワーク
 Fig. 11 L2 flat network for prototype system.

は VLAN と VPN を用いて構築した。プロトタイプシステムでは VLAN は仮想ネットワークを構築するために PhyAP とルータ間で利用され、VPN はドメイン間でフレームを通すためにルータ間で利用される。

プロトタイプシステムの L2 フラットネットワークを図 11 に示す。図では VAP-B が PhyAP-A に VAP アグリゲーションした例を示している。図において L2 フラットネットワークはルータ-B の tap デバイスから PhyAP-A の WLAN インタフェースを接続したネットワークである。L2 フレームを通過させるため、ドメイン間はトンネリングで接続されている。プロトタイプシステムでは OpenVPN [17] を用いてドメイン間にデータリンク層のトンネルを作成した。また、両ルータにおいて OpenVPN が作成する仮想的なインタフェースである tap デバイスと VLAN インタフェースをブリッジした。ルータと PhyAP 間は VLAN の同じタグによって接続した。これらにより、Room-A のネットワークと Room-B のネットワークとのデータリンク層のレベルでの結合を実現した。

4.2.3 管理サーバと管理ネットワーク

本プロトタイプでは管理ネットワーク上の管理サーバでアプリケーションを動作させて VAP を管理した。図 11 に管理ネットワークを示す。管理ネットワークは PhyAP-B の VLAN インタフェースから PhyAP-A の VLAN インタフェースを接続したネットワークで、L2 フラットネットワークと同様に実現した。管理サーバは上位のドメインに構築し、管理ネットワークを用いて VAP マネージャと通信する。管理サーバでは管理アプリケーションが動作し、PhyAP や VAP のリソース情報を収集して VAP アグリゲーションを行う。

4.2.4 VAP マイグレーション

VAP マイグレーションは管理サーバからの指示により仮想マシンの移動、ポリシーの移動、インタフェースの移動を行う。仮想マシンは Xen の持つマイグレーション機能を利用して移動した。ポリシーの移動ではポリシーをファイル化して PhyAP-A へ送信し、PhyAP-A の VAP マネージャがそのファイルからポリシープレーンを作成する。インタフェースの移動は SSID と MAC アドレスと IP アドレスをファ

イル化して PhyAP-A へ送信する。PhyAP-A はそのファイルからインタフェースの SSID, MAC アドレス, IP アドレスの設定を行う。

4.3 プロトタイプシステムを用いた評価

4.3.1 スループット

プロトタイプシステムを用い、提案方式を用いない場合と VAP を構築し VAP アグリゲーションを用いた場合のそれぞれの状態における、AP と MN 間の最大スループットを測定した。図 9 に評価で用いたネットワークのトポロジを示す。図 9 のように 2 つのドメインがあり、各ドメインにホスト、ルータ、PhyAP、MN が 1 つずつ設置されている。VAP アグリゲーションを実行すると VAP-B が PhyAP-A に移動し、PhyAP-A 上で VAP-A と VAP-B の 2 つの VAP が動作し、VAP が無い PhyAP-B は電波を發しない。

評価では、(a) 提案方式を用いない場合で 2 つの PhyAP が隣接チャネルを使用し電波干渉が発生している状態、(b) VAP アグリゲーション後、2 つの VAP が隣接チャネルを使用し電波干渉が発生している状態、(c) VAP アグリゲーション後、2 つの VAP が同一チャネルを使用し電波干渉が発生していない状態の 3 つのケースについて測定を行った。ケース (a) では PhyAP と MN 間、ケース (b), (c) では VAP と MN 間におけるスループットを測定した。測定には iperf を用い、無線インタフェースが許す最大のトラヒック量を発生させるために、コマンドによりトラヒック量を 54Mbps に指定した。プロトコルは UDP とし、100 秒間の測定を合計 24 時間にわたって繰り返し、その平均値を測定値とした。

表 1 に VAP アグリゲーション前後のスループットの測定結果を示す。VAP アグリゲーションを行った (b) は、VAP アグリゲーションを行わない (a) とほぼ同等のスループットを達成していることから、VAP アグリゲーションが実現できていることとともに、処理負荷や経路延長がスループットに及ぼす影響が少ないことが確認できる。また、(b) では同じ PhyAP-A に VAP-A, B が動作することから (a) と比較して、より近くに干渉要因が存在するが、各ノードの距離が近く、受信信号強度の値がほぼ同値であるため (a) と (b) では干渉状況はほぼ同等である。

仮想化技術をサポートする Wireless NIC を使用すれば、2 つの VAP からのフレームはスケジュールされて転送されることが期待できる。そのため、VAP アグリゲーション後は電波信号としての干渉は発生せず、スループットの改善を期待できる。ケース (c) は 2 つの VAP が同一のチャネルを使用することにより、擬似的に仮想無線インタフェースを実現している。インタフェースが互いにキャリアセンスするため、1 つの物理的なインタフェースを共有することと近い動作をすることが期待できる。表 2 に各ケースに

表 1 プロトタイプシステムの VAP アグリゲーションにおける最大スループットの評価

Table 1 Evaluation of maximal throughput in VAP aggregation of prototype system.

	PhyAP-A と MN-A 間	PhyAP-B と MN-B 間	VAP-A と MN-A 間	VAP-B と MN-B 間	合計
(a) アグリゲーションを用いない場合	8.56 Mbps (Ch1)	7.84 Mbps (Ch2)	NA	NA	16.4 Mbps
(b) アグリゲーション後隣接チャネルを使用	NA	NA	8.41 Mbps (Ch1)	8.21 Mbps (Ch2)	16.6 Mbps
(c) アグリゲーション後同一チャネルを使用	NA	NA	11.7 Mbps (Ch1)	11.5 Mbps (Ch1)	23.2 Mbps

表 2 プロトタイプシステムの VAP アグリゲーションにおけるパケット損失率の評価

Table 2 Evaluation of packet loss rate in VAP aggregation of prototype system.

	PhyAP-A と MN-A 間	PhyAP-B と MN-B 間	VAP-A と MN-A 間	VAP-B と MN-B 間
(a) アグリゲーションを用いない場合	2.1%	2.2%	NA	NA
(b) アグリゲーション後隣接チャネルを使用	NA	NA	1.9%	2.3%
(c) アグリゲーション後同一チャネルを使用	NA	NA	0.14%	0.22%

表 3 L2 フラットネットワークのオーバーヘッド

Table 3 Overhead of L2 flat network.

	スループット (Mbps)	遅延 (ms)
(A) 通常のネットワーク	94.58	0.417
(B) VAP アグリゲーション前	93.75	0.545
(C) VAP アグリゲーション後	83.32	1.377

におけるパケット損失率を示す。iperf では 54Mbps のトラフィック量を指定したが、iperf のパケット損失率は、実際に無線インタフェースから送信されたパケット数により計算される。そのため、パケット損失率は実際に送信されたパケットに対するものである。(a) に対し、疑似的に仮想無線インタフェースを実現した (c) ではパケット損失率の改善が確認できる。また、表 1 より (c) の合計スループットは 23.2Mbps であり、(a) と比較してスループットが改善されている。これらの結果より、VAP アグリゲーションがスループットを改善させることが期待できる。

4.3.2 L2 フラットネットワークのオーバーヘッド

L2 フラットネットワークのオーバーヘッドを計測した。(A) 提案方式を用いない場合の PhyAP-B からホスト-B までの経路、(B) PhyAP-B 上の VAP-B からホスト-B までの経路、(C) L2 フラットネットワークを用いた場合、PhyAP-A 上の VAP-B からホスト-B までの経路の 3 つの経路においてスループットと遅延を計測した。表 3 に結果を示す。(A) と比較し、(C) においてもスループットの低下は 10% 程度、遅延の増加は 1ms 程度に抑制されている。表 1 より各 MN-VAP 間のスループットは 10Mbps 程度であるため、L2 フラットネットワーク上でも十分な帯域を得られることが分かる。

4.3.3 VAP マイグレーション時間

linux の time コマンドを用いて、VAP マイグレーションに要する時間を測定した。測定は仮想マシンのメモリサイズが 32M、128M、256M バイトの 3 つの場合で行った。メモリサイズを変化させたのは、VAP マイグレーションの時間が主にメモリサイズに依存するからである。測定の結果、メモリサイズが 32M のときで約 15 秒、128M 時で 26 秒、256M 時で 38 秒の時間を要した。また、ダウンタイムはそれぞれ 1.7 秒、2.1 秒、2.4 秒であった。オフィスや研究室などで AP を使用する場合には状況の変化は十数分単位であると考えられるため、この時間は VAP アグリゲーションにとっては十分に短い時間であると考えられる。

5. おわりに

本論文では仮想化技術を用いて AP の機能を集約する VAP アグリゲーションを提案した。VAP アグリゲーションは PhyAP アーキテクチャ、L2 フラットネットワーク、VAP マイグレーション、管理サーバと管理ネットワークからなり、各 AP の機能を維持したまま、起動する PhyAP 数を低減させることができる。PhyAP アーキテクチャは各インタフェース、VAP マネージャなどからなり、複数の VAP の動作を可能にする。L2 フラットネットワークにより VAP アグリゲーション後も VAP は同じドメインに所属できる。VAP マイグレーションでは、マイグレーションによるダウンタイムの増加を抑制するため仮想ホストとポリシー・仮想インタフェースを分けて移動する。管理サーバはリソース情報の収集や VAP マネージャへの指示を行う。そして、VAP アグリゲーションのプロトタイプシステムの実装・評価を行い、VAP アグリゲーションが可能であり、

スループットを改善可能であることを確認した。

参考文献

[1] Rodrigues, R., Mateus, G. and Loureiro, A.: On the design and capacity planning of a wireless local area network, *Network Operations and Management Symposium, NOMS 2000*, IEEE/IFIP, pp.335-348 (2000).

[2] Huang, J.-H., Wang, L.-C. and Chang, C.-J.: Deployment strategies of access points for outdoor wireless local area networks, *IEEE 61st Vehicular Technology Conference, VTC 2005-Spring*, Vol.5, pp.2949-2953 (2005).

[3] Han, J.K., Park, B.S., Choi, Y.S. and Park, H.K.: Genetic approach with a new representation for base station placement in mobile communications, *IEEE 54th Vehicular Technology Conference, VTC 2001-Fall*, Vol.4, pp.2703-2707 (2001).

[4] Eisenblatter, A., Geerdes, H.-F. and Siomina, I.: Integrated Access Point Placement and Channel Assignment for Wireless LANs in an Indoor Office Environment, *World of Wireless, Mobile and Multimedia Networks, WoWMoM 2007, IEEE International Symposium*, pp.1-10 (2007).

[5] Ergin, M.A., Ramachandran, K. and Gruteser, M.: Understanding the effect of access point density on wireless LAN performance, *MobiCom '07: Proc. 13th Annual ACM International Conference on Mobile Computing and Networking*, pp.350-353, ACM, New York, NY, USA (2007).

[6] Jardosh, A.P., Papagiannaki, K., Belding, E.M., Almeroth, K.C., Iannaccone, G. and Vinnakota, B.: Green WLANs: On-Demand WLAN Infrastructures, *Mob. Netw. Appl.*, Vol.14, pp.798-814 (2009).

[7] Lee, Y., Kim, K. and Choi, Y.: Optimization of AP placement and channel assignment in wireless LANs, *Proc. 27th Annual IEEE Conference Local Computer Networks, LCN 2002*, pp.831-836 (2002).

[8] Abusubaih, M., Gross, J., Wiethoelter, S. and Wolisz, A.: On Access Point Selection in IEEE 802.11 Wireless Local Area Networks, *Proc. 31st IEEE Conference on Local Computer Networks*, pp.879-886 (2006).

[9] Cisco, 入手先 (<http://www.cisco.com/>) (参照 2011-02-04).

[10] ARUBA, 入手先 (<http://www.arubanetworks.com/>) (参照 2011-02-04).

[11] MERU, 入手先 (<http://www.merunetworks.com/>) (参照 2011-02-04).

[12] Wang, Y., Keller, E., Biskeborn, B., van der Merwe, J. and Rexford, J.: Virtual routers on the move: live router migration as a network-management primitive, *SIGCOMM '08: Proc. ACM SIGCOMM 2008 Conference on Data Communication*, pp.231-242, ACM, New York, NY, USA (2008).

[13] Nakao, A.: Network Virtualization as Foundation for Enabling New Network Architecture and Applications, *IEICE Trans. Commun.*, Vol.E93-B, No.3, pp.454-457, IEICE (2010).

[14] Hamaguchi, T., Komata, T., Nagai, T. and Shigeno, H.: A Framework of Better Deployment for WLAN Access Point using Virtualization Technique, *3rd International Workshop on Data Management for Wireless and Pervasive Communications, DMWPC 2010*, pp.968-973 (2010).

[15] Smith, G., Chaturvedi, A., Mishra, A. and Banerjee, S.: Wireless virtualization on commodity 802.11 hardware,

WinTECH '07: Proc. 2nd ACM International Workshop on Wireless Network Testbeds, Experimental Evaluation and Characterization, pp.75-82, ACM, New York, NY, USA (2007).

[16] Xen, 入手先 (<http://www.xen.org/>) (参照 2010-01-09).

[17] OpenVPN, 入手先 (<http://openvpn.net/>) (参照 2010-01-09).



永井 隆博 (学生会員)

2010年慶應義塾大学理工学部情報工学科卒業。現在、同大学大学院理工学研究科在学中。仮想ネットワークの研究に従事。



重野 寛 (正会員)

1990年慶應義塾大学理工学部計測工学科卒業。1997年同大学大学院理工学研究科博士課程修了。現在、同大学理工学部准教授。博士(工学)。情報処理学会学会誌編集委員、同論文誌編集委員、同マルチメディアと分散処理研究会幹事、同モバイルコンピューティングとワイアレス通信研究会運営委員等を歴任。ネットワーク・プロトコル、モバイルコンピューティング、ITS等の研究に従事。著書『コンピュータネットワーク』(オーム社)、『ユビキタスコンピューティング』(オーム社)等。電子情報通信学会、IEEE、ACM各会員。