第 XXVIII 部

IEEE802.11 ワイヤレスネットワークの構築・運用とその検証

第 28 部
IEEE802.11 ワイヤレスネットワークの構築・運用とその検証

第 1 章　wlanops ワーキンググループ 2003 年度研究報告書

1.1 はじめに

wlanops ワーキンググループは、ワイヤレスネットワークを運用する上で必要な技術を確立するために設立された。

本報告書は、2003 年に行った研究結果をまとめたものである。各報告の概要は次の通りである。

- IEEE802.11 ワイヤレスネットワーク管理システムの構築と検証

  本報告は、IEEE802.11 プロトコルを用いたワイヤレスネットワーク上での不正ノードを遮断する機構の提案とその運用結果を述べている。

  国際会議などでのネットワーク提供用に運用されるワイヤレスネットワークは、不特定多数に利用される。したがって、ワーム等に感染したノードや RA・DHCP サーバが設定されたノード等の不正ノードが接続される場合がある。

  本報告では、不特定多数が利用するワイヤレスネットワークをこのような脅威から守るための手法を提案し、その実装と運用評価を行った。
- On operation of 802.11 wireless network services

  本報告は、IETF 横浜会議および、WIDE 研究会でのワイヤレスネットワークの運用結果から、ワイヤレスネットワークを運用する指針を述べたものである。

  その内容は、アクセスポイントの選定や、その設置方法、不特定多数が利用する環境において発生する問題、運用上での対処など、不特定多数を対象としたワイヤレスネットワークを運用する際に必要な情報が述べられている。

以下、第 2 章で「IEEE802.11 ワイヤレスネットワーク管理システムの構築と検証」を、第 3 章で「On operation of 802.11 wireless network services」を掲載する。

第 2 章　IEEE802.11 ワイヤレスネットワーク管理システムの構築と検証

概要

IEEE802.11 を利用したワイヤレスネットワークは、国際会議や研究会等におけるインターネットへの接続サービス提供の為に利用されている。このような不特定多数が利用するワイヤレスネットワークには、ワーム等に感染したノードや RA・DHCP サーバが設定されたノード等の不正ノードが接続される場合がある。その結果、他のノードに対して悪影響を与え、場合によっては、ネットワーク全体を麻痺させてしまう場合もある。従って、ワイヤレスネットワークにおいては、不正ノードを遮断することが重要である。また、これらのノードのネットワークの利用履歴や現在位置をデータベース化し把握することが、ノードへの対策を行うために必要不可欠である。本報告では、不特定多数が利用するワイヤレスネットワークをこのような脅威から守るための手法を提案し、その実装と運用評価を行った。提案手法は、既存のアクセスポイントの機能を利用し、各クライアントの情報を収集、データベース化する。また、ノード単位にアクセスポイントの利用制限や、ノード毎の移動記録の閲覧が可能となっている。そして、本実装を用いた実験を行い、その結果、不正ノードの遮断によりワイヤレスネットワークへの影響を最小限とすることが可能であった。

2.1 まえがき

IEEE802.11 を利用したワイヤレスネットワークの普及が進んでいる。この要因には、WiFi Alliance（旧 Wireless Ethernet Compatibility Alliance）による相互接続性の検証（Wireless Fidelity, WiFi）、ベンダー間競争による低価格化、様々なデバイスへの搭載等が考えられる [112, 113, 114, 115, 321, 322]。

また、Ethernet 等でのケーブルの煩わしさがなく、配線や情報コンセント設置に伴うコストも大幅に削

減することができる。

したがって、整備・管理コスト等のメリットから、IEEE802.11 は、企業内・家庭内 LAN はもとより、コーヒーショップ、駅構内、会議場や街中などの公共空間におけるインターネット接続サービスのメディアとしても、積極的に用いられている。

特に、ワイヤレスネットワークは、国際会議や研究会などの会議場において、参加者に対して、臨時のインターネットコネクティビティとして利用されている。この理由は、Ethernet の場合、多数のハブや配線、情報コンセントの設置コスト（時間・費用）が必要である。しかし、ワイヤレスの場合は、アクセスポイントの設置と配線のみであることから、柔軟なネットワーク利用形態を低コストで提供できるからである。

一方、ワイヤレスネットワークは、電波を利用した通信メディアであるため、電波帯域の資源制約、電波干渉、盗聴による情報漏洩やワイヤレスノード（クライアント）の位置特定が困難等の問題がある。従って、ケーブルを必要としない通信環境の提供は、便利である反面、ケーブルを利用したネットワークへの接続において、解決が容易であった事が困難となる場合がある。それは、ワイヤレスネットワークに接続する不正ノードへの対策である。

不正ノードとは、DHCP や RA サーバが設定されたノードや、ワームに感染したノード、不正アクセスを目的としたノードであり、これらがネットワークに接続することでワイヤレスネットワークが混乱する。

例えば、ネットワーク管理者が意図しない DHCP サーバ（不正 DHCP サーバ）がワイヤレスネットワークに接続された場合、正規 DHCP サーバからの情報と不正 DHCP サーバからの情報が一般のノードへ提供される。その結果、不正 DHCP サーバが提供する誤った IP アドレスの割り当てやデフォルト・ゲートウェイの設定によって、通信不能となったり、既存のセッションが切断されるなど様々な問題が発生する。

また、2003 年 8 月発生したブラスターワーム [129] は、このような不特定多数が利用するワイヤレスネットワーク上で大きな影響力がある。ワームに感染したノードが接続された場合、他ノードへの伝搬・感染や、それに伴うトラフィック増加によるネットワーク・パフォーマンス低下等の直接被害が発生する。また、感染したノードが企業内ネットワーク等に接続することによって、内部ネットワークでの感染を広げるという二次被害も発生する。この直接被害への対策には、不正ノードを一刻も早くワイヤレスネットワークから切りはずさなければならない。

不正ノードの特定は、その MAC アドレス情報を元に行うことができる。例えば、不正 DHCP サーバの場合は、被害を被ったノードで、不正なアドレスを割り当てた不正 DHCP サーバの MAC アドレス情報を取得する。そして、Ethernet 接続の場合は、その MAC アドレスを収容するレイヤ 2 ネットワーク機器（スイッチングハブなど）の FDB（forwarding database）を探索すれば容易に接続ポートおよび、不正 DHCP サーバの物理的位置の特定も可能である。これにより、被害を収束させることができる。

一方、ワイヤレスの場合は、ワイヤレスノードが接続しているアクセスポイントの特定は可能である。しかし、物理位置を特定するには、専用製品 [354] や指向性アンテナなどによって、電波の発信源を特定する事が必要である。また、移動に伴って不正ノードが利用するアクセスポイントは変化するため、全アクセスポイントに対して、MAC アドレスのフィルタリングなどの対策を行わなければならず、時間を要する。

このように、不特定多数に対してワイヤレスネットワークを提供する場合、不正ノードをワイヤレスネットワークから遮断し、また、事後追跡の為に各ワイヤレスノードの移動を記録し、追跡可能とすることが非常に重要である。

そこで、本報告では、この問題を解決する手法として、ワイヤレスノードの MAC アドレス（Media Access Control Address）をベースにしたワイヤレスネットワーク管理システムを提案する。本手法は、ワイヤレスノード（利用者）側において改変の必要がなく、不特定多数の利用者が利用するワイヤレスネットワークの運用において適した手法である。

そして、提案手法の実装を行い、ワイヤレスネットワーク上での運用を通して、提案手法の有効性を検証する。

本報告の構成は次の通りである。2.2 節では既存手法を利用した解決策とその問題点を述べ、問題解決に必要な条件を説明する。そして、2.3 節において、本提案手法の説明を行う。2.4 節では、提案手法の実装構成の説明と今回の実装の検証を行った実験につ

いて述べ、2.5 節にて、実験結果と考察結果を示す。最後に、2.6 節にてまとめと今後の課題を述べる。

2.2 既存手法とその問題点

ここでは、既存手法を利用した不正ノード対策について述べ、不特定多数が利用するワイヤレスネットワーク環境における問題点を示す。そして、問題点の解決に必要な条件を定める。

2.2.1 既存手法

ワイヤレスネットワークでの不正ノード対策手法としては、ワイヤレスノードを認証管理する方法がある。ここでは、レイヤ 2 における手法と、レイヤ 3 における手法に分けて述べる。

1. **レイヤ 2 認証**

   レイヤ 2 で認証する技術として、WPA や、PPPoE がある。

   WPA（WiFi Protection Access）は、WiFi アライアンスによって標準化が進められた、IEEE802.11 の通信路を暗号化するプロトコルである [323]。WPA は、暗号化に用いる共通鍵を一定時間毎に更新する。このため、単一の共通鍵を使い続ける WEP（Wired Equivalent Privacy）に対して、より安全なワイヤレスネットワークを構築することができる。

   また、WPA では、IEEE 802.1x[111] で定義される EAP（Extensible Authentication Protocol）により、レイヤ 2 のネットワーク上で、ユーザ認証も可能となっている。これによって、ワイヤレスネットワークを利用するユーザを管理することが可能である。

   WPA は、強固なセキュリティを実現し、WiFi による標準化と推進が行われているので、ワイヤレスネットワークにおける標準認証技術となると考えられるが、まだまだ普及の問題がある。そのため、現時点では、運用に多大なコストを伴う技術である。

   PPPoE（PPP over Ethernet）は、PPP セッションを Ethernet 上で利用することによってユーザ認証やネットワークの選択を行う技術である [168, 263]。本方式は、一般向けブロードバンドサービス（NTT 東西フレッツサービスなど）において標準認証技術となっているが、ノードでの設定や導入コストは WPA 同様に高いといえる。

2. **レイヤ 3 認証**

   レイヤ 3 認証とは、ワイヤレスネットワークへの接続と DHCP 等による IP アドレスの取得後、認証ゲートウェイ（レイヤ 3）において認証を行う方式である。認証後、ファイヤウォールやルータなどでのアクセス制限が解除されネットワークが利用可能となる。また、スイッチングハブ等のレイヤ 2 機器とレイヤ 3 認証が連携して、ポート単位にアクセス制限のコントロールを行う方法もある [333]。

   認証には、WEB や telnet を利用した ID パスワード認証、PPTP による認証、IPsec トンネルモード等がある。

   これらの方法は、認証に WWW ブラウザ、telnet クライアント、OS に付属する機能などの標準化され普及した機能を利用することによって、ノードでの利用コストを下げる工夫がされている。しかしながら、同一リンクレイヤー内での通信が可能であるなど、利用コストが低い分、セキュリティ対策が不十分な面がある。

2.2.2 問題点

2.2.1 項で述べた手法は、不特定多数が利用するワイヤレスネットワークにおいて、技術的には運用可能である。

しかし、1. を実現するには、WPA に対応したノードでなければならない。このため、国際会議などにおいては、ユーザへのサポート体制に多くのコストが必要であり、非現実的であることは明らかである。

2. の手法は、認証ゲートウェイを介した通信に関しては、遮断することが可能であるが、ワイヤレスネットワーク内における通信に対しては遮断ができない。したがって、ワームや不正 DHCP サーバなどによるリンクレイヤーへの攻撃から、ワイヤレスネットワークを防御することは不可能である。

以上より、本研究の対象とする不特定多数が利用するワイヤレスネットワーク環境において、既存手法による問題解決は困難であるといえる。

2.2.3 問題解決の前提条件

これらの問題点をふまえて、本研究では、不特定多数に対して提供するワイヤレスネットワークには不正ノードが存在せざるを得ない事を前提とした。筆

者らは、ワイヤレスネットワークを守るために、任意ノード（対象は不正ノード）をワイヤレスネットワークから遮断・遮断解除することに重点をおき、次の前提条件を設けた。

1. **任意ノードを遮断・遮断解除できる事**
   不正ノードの存在は、ワイヤレスネットワークに対する運用コストを増加させるため、即座に遮断しなければならない。また、対策後は、ノードがワイヤレスネットワークを利用可能となるように、遮断解除ができなければならない。
2. **ノード側への改変を行わない事**
   様々な環境のノードがワイヤレスネットワークを利用するため、ノードの改変には大きなコストを伴う。
3. **既存のアクセスポイント製品が改変なく使える事**
   ワイヤレス市場が成熟しつつあるため、アクセスポイントに新たな改変を伴う運用は現実的ではない。
4. **事後追跡が可能である事**
   不正ノードに対する事後追跡は、ノード特定の為に必要である。

本報告では、これらの条件を満たす「MAC アドレス・ベースによるノード管理システム」を提案する。

2.3 提案手法

ここでは、提案手法である「MAC アドレス・ベースによるノード管理システム」について述べ、その動作説明を行う。

2.3.1 MAC アドレス・ベースによるノード管理システム

本手法は、アクセスポイントの「ワイヤレスノードの MAC アドレスを RADIUS で認証する機能」を利用している。

本機能は、コンシューマ向け製品を除けば、多くのアクセスポイントに標準的に搭載されている。例えば、IEEE802.11 に対応したアクセスポイントにおいて、Avaya 社 AP シリーズ、Cisco 社 Aironet シリーズ、バッファロー社 AirStationPro シリーズなどが本機能に対応している。

本機能を使えば、次のようにして任意の MAC アドレスをワイヤレスネットワークから遮断できる。

ワイヤレスネットワークから遮断するワイヤレスノードの識別子（MAC アドレス）を RADIUS の非承認対象として RADIUS サーバ上で登録しておく。該当する MAC アドレスは、RADIUS から承認されないため、アクセスポイントは、アソシエーション（接続）を中止する。したがって、該当するノードは、ワイヤレスネットワークを利用できなくなる。

また、アクセスポイントからの RADIUS 経由によるワイヤレスノードの認証を基に、ワイヤレスノードが利用するアクセスポイント（位置情報）、利用時刻、ノード識別子（ワイヤレスノードの MAC アドレス）などの利用記録をデータベース化することで、アクセスポイント毎のワイヤレスノード数の状態や、移動状況、存在位置を把握することが可能である。

本提案手法は、既存製品であるアクセスポイントの RADIUS クライアント機能と、RADIUS サーバをベースとしたワイヤレスノードの管理システムを組み合わせたものである。よって、アクセスポイント側およびワイヤレスノード側共に、ワイヤレス通信の標準パラメータ（ESSID や WEP キーなど）を設定するのみで、それ以外の改変を必要とせず、不正ノードの遮断が可能である。また、各ワイヤレスノードの利用記録データベースから、事後追跡もできる。

したがって、本提案手法は、先に示した前提条件を満たし、かつ、既存の運用されているワイヤレスネットワークに対して、利用者の利便性を損なうことなく、より安全な運用体制を実現可能な手法となっている。

2.3.2 認証手順

ここでは、ノードのワイヤレスネットワークへの接続から、各アクセスポイントが行う認証要求とその応答の手順について述べる。

1. **データベースの管理**
   利用記録や不正ノード（ワイヤレスネットワークから遮断するワイヤレスノード）の MAC アドレスが管理されている。（図 2.1 の (1)）。

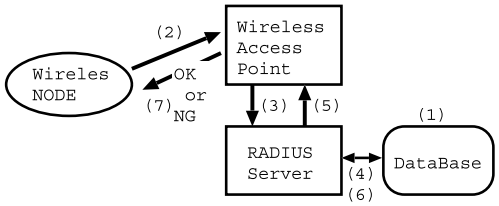

図 2.1.　RADIUS サーバとアクセスポイントの関係

2. **ワイヤレスノードからのアソシエーション要求**
   ワイヤレスネットワークの利用を開始するノードは、必要ならば、ESSID や WEP 等の各種通信パラメータを設定し、アクセスポイントへのアソシエーションを開始する（図 2.1 の (2)）。
3. **アクセスポイントでのアソシエーション要求**
   アクセスポイントは、ノードからのアソシエーション要求に従って、RADIUS サーバに対し、ノードの MAC アドレスの認証要求を行う（図 2.1 の (3)）。
4. **RADIUS サーバによる MAC アドレスの検証**
   RADIUS サーバは、アクセスポイント（RADIUS クライアント）からの MAC アドレスの認証要求を受け、遮断する MAC アドレスのリストを検索する（図 2.1 の (4)）。もし、検索結果が一致した場合は、不承認をアクセスポイントへ応答する。そうでない場合は、承認をアクセスポイントへ応答する（図 2.1 の (5)）。
5. **ワイヤレスノード情報の記録**
   認証後、認証結果、アクセスポイント、日時、ワイヤレスノードの MAC アドレスをデータベースに記録する（図 2.1 の (6)）。
6. **アソシエーション処理**
   アクセスポイントは、RADIUS サーバからの認証結果に従ってアソシエーションの継続もしくは終了をする（図 2.1 の (7)）。

以上が本提案における認証手順である。

2.4 実装と実験

本節では、提案手法の実装構成と、実装を用いた実験を行った結果について述べる。

2.4.1 実装構成

本提案手法に基づく実装の構成図を、図 2.2 に示す。構成は、(1) アクセスポイント部（AccessPoint）、(2) RA/DB システム部（RA/DA System）、(3) 遮断・追跡システム部（Tracking System）、(4) 制御インターフェース部（Ctrl. I/F）となる。

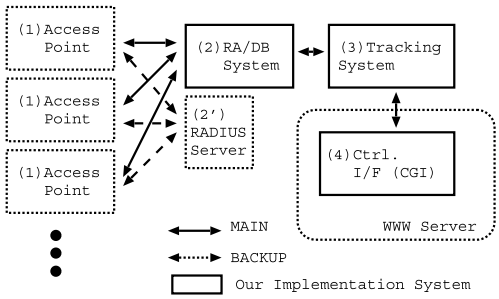

図 2.2. 実装構成図

次に、各構成部の機能を述べる。なお、本提案手法の実装は、FreeBSD（バージョンは 4-Stable を使用）上で行った。

1. **アクセスポイント部**
   アクセスポイントは、Cisco 社製 Aironet 1220B および Avaya 社製 AP-2/3 が利用可能である。これらの製品は、アソシエーション時に RADIUS サーバを利用した認証に対応している。本実装では、アクセスポイントから RADIUS サーバへの認証データの形式を解析し、この結果を基に、「遮断・追跡システム部」への実装を行った。従って、他社製品であっても、同様の解析作業で対応が可能である。
   本実験では数台から数十台のアクセスポイントを利用する。アクセスポイントに対する運用コストを低減するために、Aironet 1220B に対しては設定のひな形を作成し、これを基にした各アクセスポイントに対する設定ファイルの自動生成機能の実装を行った。
2. **RA/DB システム部**
   RA/DB システム部は、RADIUS サーバ部とデータベース処理部で構成されている。
   RADIUS サーバとして、FreeRADIUS[288] を利用した。アクセスポイントと RADIUS サーバとの通信が不調となった場合、アソシエーションができなくなるため、ワイヤレスネットワークの運用が困難になる。したがって、セカンダリの RADIUS サーバをバックアップシステムとして運用した（図 2.2 の (2′)）。
   データベース処理部は、FreeRADIUS の生成する認証ログを基に、60 秒毎にアカウンティング情報を生成・更新する。アカウンティング情報は、ワイヤレスノードが利用するアクセスポイント（位置情報）、利用時刻、ノード識別子（ワイヤレスノードの MAC アドレス）で構成されている。また、RADIUS サーバや遮断・追跡システム部が検索・登録・削除を行う、遮断する MAC アドレスのリストも保管する。
3. **遮断・追跡システム部**
   遮断・追跡システム部は、遮断システム部と追

跡システム部で構成されている。

追跡システム部は、制御インターフェース部からの要求に応じて、データベース処理部のアカウンティング情報を基に、ワイヤレスネットワークを利用するユーザ数、ノード毎のアクセスポイントの利用履歴、利用時間、アクセスポイント毎のワイヤレスノード数の推移等の統計を行う。

遮断システム部は、制御インターフェース部からの要求に応じて、データベース処理部の遮断する MAC アドレスのリストに対して、MAC アドレスの登録・削除を行う。

4. **制御インターフェース部**

制御インターフェース部は、WEB ベースの CGI で提供されており、遮断・追跡システム部から得られる統計結果や、遮断中の MAC アドレスの情報表示、遮断登録・解除を行うユーザーインターフェースを提供する。また、各作業・閲覧は、利用者の認証（レベルは、管理者または、ユーザの 2 段階）を提供し、安全な情報提供・管理が可能となっている。

以上が、本提案手法の実装構成である。

2.4.2 実験ネットワークの構成

本実装を用いてワイヤレスネットワークの運用を行い、提案手法の評価を行った。

2003 年 9 月 8 日〜11 日に開催された WIDE プロジェクト主催による WIDE 秋合宿において、本実装によるワイヤレスネットワークの運用を行った。

設置構成は、図 2.3 に示す構成となっており、アクセスポイント 7 台（A1〜A7、Cisco Aironet 1220B）、2 台のサーバ（S1 と S2、x86 PC 上で FreeBSD 4.9 を利用）を運用した。

サーバ 1 上で RA/DB システム部、遮断・追跡システム部、そして、制御インターフェース部と WWW サーバの運用を行い、サーバ 2 上で、サーバ 1 トラブルに伴うアソシエーションの中断を回避することを目的としたバックアップ用 RADIUS サーバを運用した。

アクセスポイントは、802.11a および、802.11b のデュアルバンドで運用を行った。チャネル設定は、802.11b において、1-6-11ch、802.11a において、34-38-42ch を組み合わせて電波干渉の少ないアクセスポイントの配置を行った。

2.5 実験とその結果

ここでは、本提案システムの運用を行い、実際に発生した不正ノードに対する対策結果や利用記録の集計結果を検証し、本提案の有効性について述べる。

2.5.1 運用結果

本システムを 9 月 8 日 18:00〜9 月 11 日 12:00 の間運用を行った。その結果、本提案システムに関する運用障害は発生しなかった。

本システムの運用期間中の全アクセスポイントにおける 802.11b および 802.11a ワイヤレスノード数の変化は、図 2.4 に示す結果となった。

これらの結果より、本ネットワークを利用したワイヤレスノード数は 372 ノード、ワイヤレスノードの瞬間最大利用ワイヤレスノード数は、802.11a が 36 ノード（9 日 20 時 59 分）、802.11b が 214 ノード（9 日 20 時 26 分）、双方の場合 249 ノード（9 日 20 時 26 分）であった。これらの時間帯は、ほとんどの利用者が参加したプレナリセッションが開催されており、多くのワイヤレスノードが部屋 1 に集中する結果となった。したがって、部屋 1 を管轄するアクセスポイント 1 および 2 は、負荷が高い状態であった。

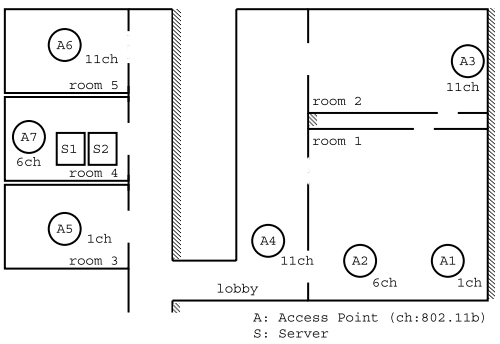

図 2.3. 実験ネットワーク

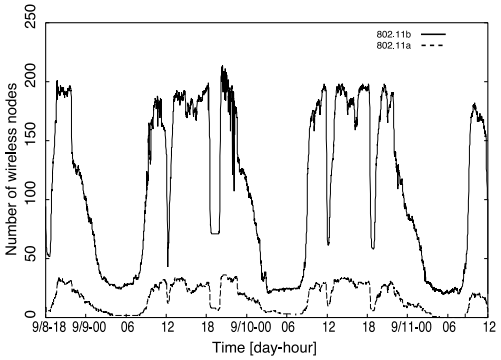

図 2.4. ワイヤレスノード数の変化

これより、ワイヤレスネットワークの設計は、会議のスケジュールなどから利用者が集中する時間帯を予測し、アクセスポイント増設や監視体制の強化を行わなければならないといえる。

次に、今回使用した Cisco Aironet 1220B における、パケットロスなく安定して利用可能であるノード数を調査した。

この値は、アクセスポイントあたりの実用上最大のノード数の目安となり、大多数が利用するワイヤレスネットワークのインフラ設計には欠かせない情報である。

実験は、9 月 9 日 22:00 からアクセスポイント 2 上で行った。アクセスポイント 2 上のワイヤレスノード数を、50、80、110、140、170 と変化させ、ワイヤレスノード数に対するパケットロス率を計測した。なお、パケットロス率の計測方法は、ワイヤレスネットワーク内から任意のノードを選択し、ping を 100 回行う計測を 5 回実施とした。

計測の結果、ワイヤレスノード数が、110 の場合で 0%〜1%程度、140 の場合で 1%〜5%、170 の場合で 1%〜27%のパケットロスが観測された。

したがって、本アクセスポイント 1 台あたりの実用上最大のノード数は、約 110 ノードである。802.11b では、一般に、独立した 3 つのチャンネルが利用可能であるため、閉域な空間においては、最大 330 ノード程度が上限といえる。

しかしながら、インターネットのプロトコル標準化を行う IETF 国際会議では、1 閉域空間（部屋）に、500 名を超えるワイヤレスノードが存在する。このような大多数が一度に使う環境では、周波数の異なる 802.11a や、日本においては、802.11b において、11ch と干渉のない 14ch の同時運用によって、さらなる利用可能なノード数の上積みが必要である。

今回の実験では、802.11b ノードと 802.11a ノードの存在比率は約 9 : 1 であったので、37 ノード程度が 802.11a を利用可能で、さらに 802.11b の 14ch 分の 110 ノードを追加し、閉域空間内の約 477 ノードへのワイヤレスネットワーク提供が可能であるといえる。

また、各ベンダーから、2.4 Ghz（IEEE 802.11b/g）および 5 Ghz 帯（IEEE 802.11a）に対応したネットワークカードが販売・導入されていることから、今後 802.11a の存在比率は増加し、IETF 国際会議クラスの環境おいても十分安定したワイヤレスネットワークが運用可能であるといえる。

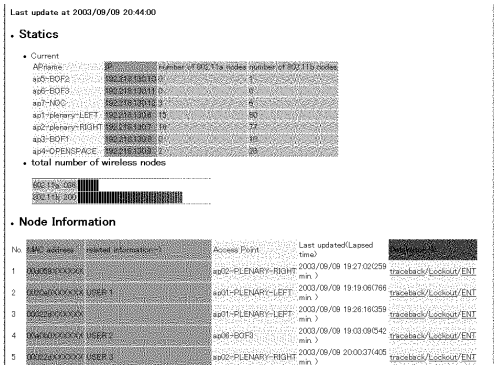

図 2.5. 位置情報・利用時間の出力

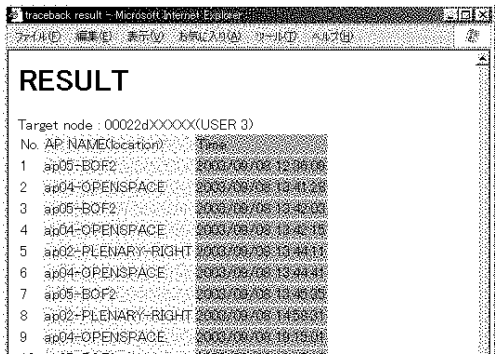

図 2.6. 移動履歴の出力

ワイヤレスノードの位置情報・利用時間の出力を、図 2.5 に示す。また、位置情報を基に、ワイヤレスノードの移動履歴の出力を、図 2.6 に示す。

このように、各ワイヤレスノード毎の現在位置や移動履歴が閲覧可能である。したがって、これらの情報は、不正ノードの事後対策に役立つといえる。

以上の実験結果より、提案手法の実装は、設計通り動作し、運用上問題ない事が証明された。

2.5.2 ワーム感染ノードを遮断

ブラスターワームに感染したノードからの不正トラフィックによって、会場から外部へのネットワーク回線が圧迫される事態となった。

このとき、ブラスターワームが生成するトラフィックの発信元 IP アドレスを基に 4 ノードの MAC アドレスを ARP テーブルを基に 5 分程度で調べ、本実装により、ワイヤレスネットワークから即座に遮断が行われた（図 2.7）。

そして、該当ノードの位置情報を基に、アナウンスを行いノードを特定し、ワームへの対策を行った。その後、遮断を解除した。

図 2.7. 遮断する MAC アドレスの登録

以上の結果、ワームによるネットワーク障害を回避し、ワイヤレスネットワークを安定化することが可能であった。

この結果は、本システムが、現在問題となっているワームなどの不正ノードに対する有効な対策であることを証明した。

2.6 まとめ

本報告は、不特定多数が利用するワイヤレスネットワークにおける不正ノードが与える影響を示し、それに対する既存手法に基づく解決策の提示と問題点を述べた。そして、問題解決の前提条件を定め、これを満たす、MAC アドレスに基づくノード管理システムを提案し、その手法の既存手法に対する優位性を示した。

次に、提案手法の実装構成についての説明を行い、開発した実装を用いて、約 372 ノードが利用するワイヤレスネットワーク上で運用を行った。

その結果から、ワイヤレスネットワークの状況、ノードの移動履歴や位置の把握、ワームなどの不正ノードの遮断が可能であることを証明し、本手法の有効性を示すことができた。

また、本実装を用いて、アクセスポイントあたりの利用可能なノード数を計測し、ワイヤレスネットワークの設計における参考値を明らかにすることができた。

今後の課題として、次のことが挙げられる。

ワームは、他ノードに対して急速に感染を広げるため、発見から遮断までの時間間隔を小さくしなければならない。今回は、ワームの発見に 30 分〜1 時間程度の時間を要し、その後に、MAC アドレスの特定を手動で行ったため時間を要した。その結果、ワイヤレスネットワークに対して影響を与える結果となった。

よって、IDS（Intrusion Detection system）との連携などによる発見から遮断までの過程の自動化によって、より少ない影響ですむことが予想される。しかし、この場合は、誤検知に対する対策を考慮する必要があるといえる。

運用において、室内においても室外（廊下）のアクセスポイントを利用するという現象が確認された。これは、部屋間などのノードの移動の際、室外のアクセスポイントとアソシエーションし、新たな部屋においても、電波の拡散性によって、引き続き室外のアクセスポイントを使えた為発生した。この場合、本提案手法のみではワイヤレスノードの位置を十分把握できないため、事後追跡が困難となる。

したがって、アクセスポイントの配置の調整、たとえば、アンテナ方向・種類の変更や送信出力の修正などや、他アクセスポイントでの該当ノードの電波強度観測などの対策が必要と考えられる。

また、本システムは、結果的に各個人の移動記録を行うため、プライバシの扱いが問題となる。これには、MAC アドレスと鍵のハッシュ化などによって、ノードから移動情報への関係を隠蔽化する仕組みが必要であるといえる。

第 3 章　On operation of 802.11 wireless network services — lessons from IETF54 Yokohama and WIDE meeting —

3.1 Introduction

This document describes several techniques to provide a wireless network environment based on 802.11 families in conferences where a large number (order of 1,000) of participants get together. It is possible that various types of problems could rise in the operation of such an environment.

To prevent the problems, there are three key elements in the wireless infrastructure with high performance access points (wireless base stations), monitoring statistics of access points, and operating a wireless node tracking system.

The rest of this document is organized as follows. Section 3.2 describes the problems observed in the past wireless environments. Section 3.3 describes the solutions for the problems.

Section 3.4 shows about past wireless operations, Section 3.5 gives conclusions.

3.2 Problems in wireless network operation

This section describes the problems observed in the operation of wireless networking environment in a couple of meeting, IETF Yokohama meeting and 2003 WIDE Project autumn meeting.

3.2.1 Access points overloaded

An access point can be overloaded when too many nodes connect (associate) with it. Under the overloaded state, the access point does not work correctly. Some access points at IETF Yokohama lost packets and halted. In this case, it is necessary to perform power cycle them. The maximum capacity of association nodes depends on each product, and vender usually provides no information about it.

We measured packet loss ratio regarding to the number of associated nodes with Cisco Aironet 1220B (IOS version) in Sep. 2003. About 3% of packet drop was observed when the number of association nodes reached about 140 nodes. The packet loss rate depends on the traffic volume and the performance of access point.

Thus, on planning a wireless network environment, it is necessary to provide a single access point for 140 nodes or less based on Cisco Aironet 1220B. In most countries, there are three independent channels (interference-free channels) on open space for 802.11 environment. Thus, about 420 nodes in a space can be considered as the upper bound.

The most serious case was halt (or self-reset) of an access point according to overload. In this case, all nodes associated with the halted access point re-associate other available access points. This likely cause is the access points around the halted access point overloaded as well. More badly the sequence of such events could cause avalanche of the crash of access points and this phenomenon happens repeatedly.

3.2.2 Countermeasures for troublesome nodes

When an unofficial DHCP server or an RA server that has bogus configurations connects to a wireless network, the wireless network may have connectivity trouble. If it is the wired connection, we are easy to find the topology of the troublesome node by tracking the switches and the cables. After disabling a switch port or pulling out the cable, we can warn the owner of the node.

On the other hand, in a wireless environment, we are able to locate the access point associated with the troublesome node. But it is difficult to detect its location. Thus, we should operate a node authentication system for shutting out such troublesome nodes. Section 3.3 describes the system developed and operated on IETF Yokohama and WIDE meeting.

3.2.3 Radio resource issue

It is possible that radio signals from different access points interfere together according to the position of the access point and the structure of the building. The coverage of an access point varies according to the structure of the building, the type of antenna, the type of frequency band, and other factors. Therefore, adjusting the position of each access point might be necessary after the logical design is defined.

In the next section, the solution of these problems for operating a stable wireless network is described.

3.3 Solution

3.3.1 Access point requirements

It is important to select high performance access points that have capability for SNMP management and RADIUS authentication to manage. You should not use a cheap consumer-class wireless access points because they do not work well under a heavy load condition in most cases. Most of the consumer-class products assume that the number of the wireless clients is about 40 or less. Following access points works well under the

heavy load condition with a good performance.

- Cisco Aironet 1200 series
  - Capable for 802.11a and 11b, dual band operation.
  - Performance is nice
  - Works stably under a heavy load condition
  - It is possible to map the traffic to 802.1Q VLAN based on ESSID
  - Number of association nodes can be limited
  - SNMP Management/ RADIUS Client capable
  - 802.11g support
- AVAYA (Lucent) AP-2 (AP-2000) series
  - Capable for 802.11a and 11b (dual band)
  - SNMP Management/ RADIUS Client capable

Best choice is Cisco Aironet1200 dual band model (Aironet 1220B) at this moment. It is possible to define a maximum number of association nodes. This function is useful for preventing from the overloaded condition. AP-2 and AP-1000 were used on the IETF Yokohama meeting, but not flagship products now. AP-2 and AP-1000 have no functionality to limit the number of associated station. It was rather unstable, sometime rebooted or halted under such a condition where more than 100 nodes associate with it. It was difficult to prevent from the overload state with AP-2 and AP-1000.

It is also worth to note that an Aironet1200 access point with older firmware could halt or self-reset in the plenary session at IETF Yokohama.

It is effective to operate both of 802.11a and 11b in an access point to increase the wireless capacity in a limited space. They use different radio frequency and are not interfere together. Recently some models of laptop computers are equipped with 802.11a and 802.11b combo (Dual-Band) wireless interfaces.

In the experience of WIDE 2003 autumn meeting, the number of 802.11a nodes were only about 10% of entire access nodes. It should also be kept in mind that the frequency ranges for 802.11a vary country by country and might have interoperability problem in an internal network workshop.

3.3.2 Position designing

11 channels are defined for 802.11b by FCC. Neighboring channels overlaps the bandwidth and can not be used in the same service area. Suggested channel allocation is to use only channel 1, 6, and 11 only. We must design position of access points regarding to these three channels. On the other hand, 802.11a has four independent channels, such as 34, 38, 42, and 46.

A design point is number of stations in a room is fixed by capacity of room (You assign one access point per 140 persons.). Access point conferring outside a conference room (lobby and restaurant, etc.) can be installed in sparsely. The coverage area of public space is wide due to reflection of radio wave and leaking radio wave from conference rooms.

It is difficult to fix positions of each access points theoretically. You should check radio wave statistics, such as interferences between same channels, coverage area, connectivity and so on, and add, remove or modify position of its on the site.

The base station is set up at the height of about 2 meter or more to prevent radio wave from obstructions. Power of the radio wave from an access point weakens by obstructions (for example, persons and chairs and partitions, etc.). Especially, if you operate 802.11a access points, it is highly recommended. 5.2 GHz in 802.11a is weaker for obstructions than 2.4 GHz in 802.11b.

3.4 Configuration and Operation

You should separate wireless network segment and wired network segment to protect multicast/broadcast storm and worm traffic coming from wired network with a high bandwidth. Also, you allocate same network address for a wireless network to enable seamless handover between access points. (At IETF Yokohama, we assigned /22 network address as IPv4 for wireless segment. Participants could use same IP address in any area

including the hotel.)

Also, it is better to operate monitoring system for the number of association nodes on each base station from SNMP management function. An access point provides association statistics via SNMP private MIB function. The private MIB information is provided by vender.

An access point has MAC authentication function. It is association node's MAC Address authenticates with RADIUS server. This function can work to shut out troublesome nodes from a wireless network. Also, you can track paths of the node from the RADIUS authentication log. You add a troublesome node's MAC address to deny list on RADIUS. Then all access points shut it out from wireless network.

You should download the access point configuration and prepare stand-by access points for avoiding down time. Also you prepare a laptop PC with "Network Stumbler" which is useful to track a wireless node for trouble shooting (Network Stumbler is free-ware and a powerful wireless network analyzer.).

We are releasing a wireless operation tool. This tool is a full functionality with Cisco Aironet 1220B and can solve the issues. Supporting function is as follows.

- Shut out and tracking wireless nodes.
- Counting and collection nodes' MAC address
- Visualization of association nodes at each access point.

3.5 Examples

3.5.1 IETF Yokohama meeting

Maximum number of unique MAC nodes was more than a thousand nodes. Also, maximum number of nodes per room was about 450 nodes at the plenary session.

We used two Pentium III PCs with FreeBSD 4 to run our wireless tool that is support RADIUS and SNMP operation. We operated AVAYA AP-3, Lucent AP-1000 and Cisco Aironet 1200 (VxWorks Version) as access point. Three or two 802.11b access points were operated at each conference room. In the plenary session we operated three access points and one extra access point with 14ch that is authorized in Japan only.

We used a circuit switching infrastructure in the hotel with xDSL technology as getting last one mile connectivity. We installed two wireless access points to each floor's EPS and loft via xDSL over telephone line to provide wireless connectivity for hotel visitors.

3.5.2 WIDE 2003 Autumn meeting

Maximum number of unique MAC nodes was about 320 nodes. We operated a dual band access point with Cisco 1220B (IOS version). We used two Pentium 4 PCs with FreeBSD to run our wireless tool. One or two access points were mounted each conference room. When a Coverage area of 11a and 11b was same area under dual band access point mounted at high position (over 2M).

We tested 802.11g and 11b dual band access point. As result, 802.11g was bad effect to wireless performance of 802.11b. You should not operate 802.11g to provide a wireless network environment in conferences where a large number (order of 1,000) of participants get together.

All of the MS blaster nodes were shut out by RADIUS function. Cisco 1220 did not drop packets until association of nodes was more than 120 nodes.

3.6 Conclusion

Wireless media is a best choice to reducing both developing cost of infrastructure and connectivity cost at a client. But it is difficult to clear the problems with wireless operation before starting. It will be clear after a large number (order of 1,000) of participants use together. Therefore, preparing high performance access points, monitoring static of wireless network and readiness for the emergency response to any troubles are very important.