

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

大江 将史, 樫山 寛章, 山本 成一, 白畑 真

September 1, 2004

Abstract

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、各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おこない、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。

Keywords: IEEE802.11, ワイヤレス, セキュリティ, ワーム, インターネット

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 [1][2][3][4][5][6]。

また、イーサネット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、臨時的インターネット接続サービスとして利用されている。この理由は、イーサネットの場合、多数のバブや配線、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ワーム [7] 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った 2 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、イーサネット接続の場合は、その MAC アドレスを収容するレイヤー 2 ネットワーク機器 (スイッチングハブなど) の FDB(forwading 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 [8] 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ない、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) 側において変更の必要がなく、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。第 2 章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、第 3 章において、本提案手法の説明を行う。第 4 章では、提案手法の実装構成の説明と今回実装の検証を行った実験について述べ、第 5 章にて、実験結果と考察結果を示す。最後に、第 6 章にてまとめと今後の課題を述べる。

2 既存手法とその問題点

ここでは、既存手法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。

2.1 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、レイヤー 2 における手法と、レイヤー 3 における手法に分けて述べる。

1. レイヤー 2 認証

レイヤー 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 [9]。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[10] で定義される EAP(Extensible Authentication Protocol) を使用して、レイヤー 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 [11][12]。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. レイヤー 3 認証

レイヤー 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 (レイヤー 3) において、認証を行う方式である。認証後、ファイア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ー 2 機器とレイヤー 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 [13]。

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 問題点

前節で述べた手法は、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出来ない。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。

2.3 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、遮断解除が出来なければならない。

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。

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。

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、パツファロー社 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、各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、事後追跡も出来る。

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。

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 1 の (1))。

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 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 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 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 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 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 1 の (7)) .

以上が本提案における認証手順である .

4 実装と実験

本章では、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 .

4.1 実装構成

本提案手法に基づく実装の構成図を、図 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 .

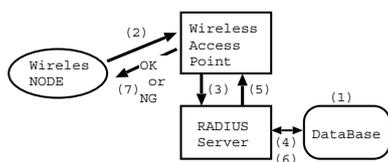


Figure 1: RADIUS サーバとアクセス・ポイントの関係

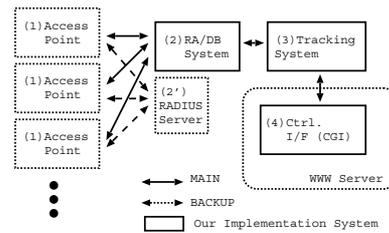


Figure 2: 実装構成図

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、Aironet1220B 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 [14] 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出来なくなるため、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 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 秒毎にアカウント情報を作成・更新する . アカウント情報は、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トリング情報を基に、ワイヤレスネットワークを利用するユーザ数、各ノード毎のアクセスポイントの利用履歴、利用時間、各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や、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。

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秋研究会において、本実装によるワイヤレスネットワークの運用を行なった。

設置構成は、図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。チャンネル設定は、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。

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。

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、802.11bが、36ノード(9日20時59分)、802.11a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ブ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。

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めやすとなり、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、0%～1%程度、140の場合、1%～5%、170の場合、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

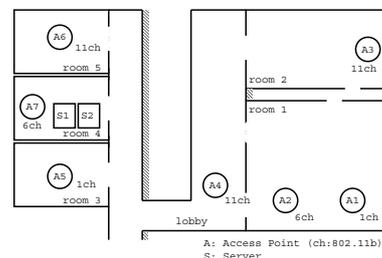


Figure 3: 実験ネットワーク

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 protocols 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 の同時に運用によって、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、2.4GHz (IEEE 802.11b/g) および 5GHz 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 国際会議クラス的环境に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。

ワイヤレスノードの位置情報・利用時間の出力を、図 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 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言える。

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。

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、

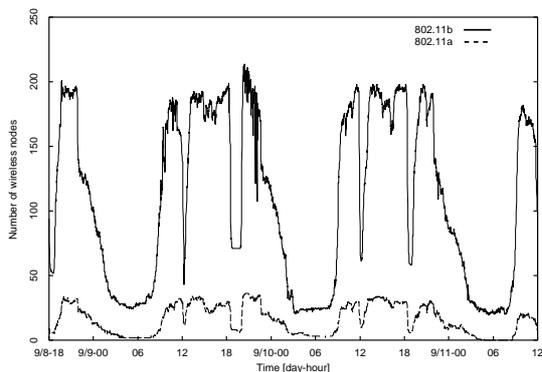


Figure 4: ワイヤレスノード数の変化

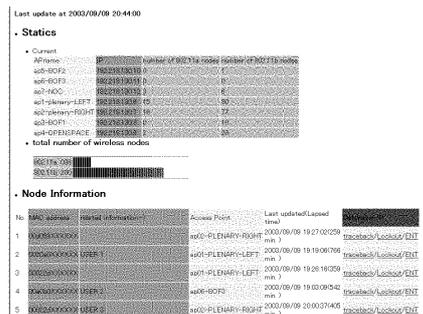


Figure 5: 位置情報・利用時間の出力

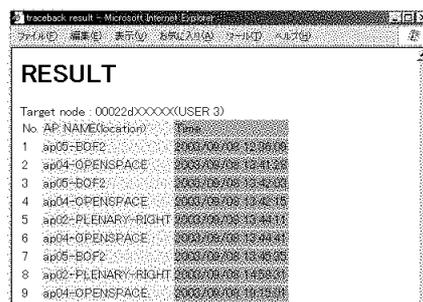


Figure 6: 移動履歴の出力

ワイヤレスネットワークからの即座に遮断が行われた (図 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、ワームへの対策をおこなった。その後、遮断を解除した。

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。



Figure 7: 遮断する MAC アドレスの登録

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出来た。

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、発見からの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、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、引き続き廊下の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出来ないため、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、プライバシー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があると言える。

References

- [1] WiFi Alliance, "What is WiFi?," <http://www.wifialliance.com/>.

- [2] WiFi Alliance, "Wi-Fi overview," http://www.wi-fi.org/OpenSection/why_Wi-Fi.asp
- [3] IEEE 802.11 Working Group, "IEEE 802.11-1999," IEEE 802 Standards, IEEE, 1999.
- [4] IEEE 802.11 Working Group, "IEEE 802.11b-1999 Supplement to 802.11-1999," IEEE 802 Standards, IEEE, 1999.
- [5] IEEE 802.11 Working Group, "IEEE 802.11a-1999," IEEE 802 Standards, IEEE, 1999.
- [6] IEEE 802.11 Working Group, "IEEE 802.11g-2003," IEEE 802 Standards, IEEE, 2003.
- [7] Internet Security Systems, "MSRPC DCOM ワーム「MS Blast」の蔓延," ISS Security Alert <http://www.isskk.co.jp/support/techinfo/general/MS.Blast.html>, Aug. 2003.
- [8] 日立製作所, 日立電線 "無線 LAN 位置検知システム「日立 AirLocation(TM)」," <http://www.hitachi.co.jp/airlocation/>, Nov. 2003.
- [9] WiFi alliance, "WiFi Alliance Protected Access," WECA White paper, <http://www.wifialliance.com/OpenSection/pdf/Wi-Fi.Protected.Access.White.Paper-Japanese.pdf>, Apr. 2003.
- [10] IEEE 802.1 Working Group, "IEEE 802.1x - Port Based Network Access Control," IEEE 802 Standards, IEEE, Oct. 2001.
- [11] L. Mamakos, K. Lidl, J. Evarts, D. Carrel, D. Simone, and R. Wheeler, "A Method for Transmitting PPP Over Ethernet (PPPoE)," RFC 2516 <http://www.ietf.org/rfc/rfc2516.txt>, Feb. 1999.
- [12] Simpson, W., Editor, "The Point-to-Point Protocol (PPP)," STD 51, RFC 1661, Jul. 1994.
- [13] 石橋, 山井, 安倍, 大西, 松浦, "IP アドレス/MAC アドレス偽造に対応した情報コンセント不正アクセス防止方式," 情報処理学会論文誌, Vol.40 No.12-025, Dec. 1999.
- [14] The FreeRADIUS Server Project, "FreeRADIUS 0.9.1," <http://www.freeradius.org/>, Sep. 2003.

Copyright Notice
Copyright (C) WIDE Project (2004). All Rights Reserved.
Full Copyright Statement
Copyright (C) IEICE, 2004. All Rights Reserved.