

無線 LAN 統合認証方式における優先度制御の実装

阪口 敬司[†] 山下 真純^{††} 西村 俊和[‡] 小川 均[‡]立命館大学理工学部情報学科[†]立命館大学大学院理工学研究科^{††}立命館大学情報理工学部情報コミュニケーション学科[‡]

1. はじめに

従来の無線 LAN では、それぞれのサービス提供者がそれぞれのアクセスポイント(以下 AP)を登録されたユーザに開放している。すなわち AP は組織毎に複数存在するが、ほとんどの AP を利用する事ができない。これによって AP の乱立による電波干渉や周波数の枯渇等の問題が発生している。この理由として、不特定のユーザにも AP を開放し、そのユーザがそのネットワーク環境に障害や負荷を与えた場合、そのユーザを特定する事の困難さがある。そのため組織毎で AP を抱え、管理しているのが現状である。

そこで無線 LAN 統合認証方式が提案されている。本システムは、無線 LAN ルータで認証に失敗したパケットを破棄せずに、VPN(Virtual Private Network)を用いて、外部に存在する認証機構に送信する。それによって、登録者は遠隔地から容易に、認証登録している LAN に接続し、安全に利用できるという特徴を持つ。外部に認証機構を置き、分断されたセグメントをレイヤ 2-VPN でつなぐ事で、すべての AP を利用可能にしている。

しかしこの場合、1つの AP を複数の組織が共同で利用するので、多種多様なユーザ利用が予想される。また重要なパケットを伝送したい場合や、緊急時の場合に素早くパケットを伝送するために、この無線 LAN 統合認証方式に優先度の導入を検討する。本稿では、利用帯域を動的に確保する事で、重要なパケットを他の帯域を抑える事によって優先させて伝送する手法を提案する。

2. システム構成

2.1 動作概略

本システムは、AP に併設するパケット制御部、全体の優先度制御を管理する優先度管理局及び、複数の認証機構によって実現される。

以下の図 1 に全体構成図を示す。

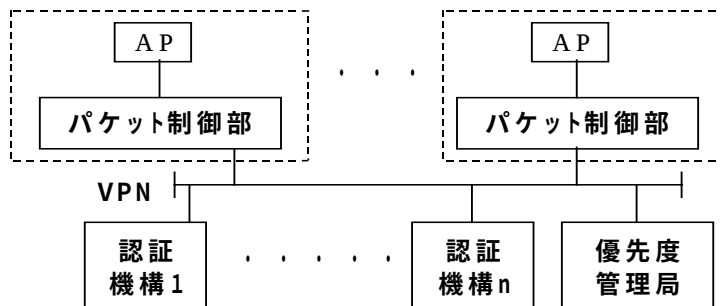


図 1 . 全体構成図

一般に優先度制御はネットワーク層のプロトコルである IP を用いて制御対象パケットの識別を行うが、本研究では MAC アドレスを用いて実装する。その理由として、レイヤ 2-VPN によって全体のネットワークを構築していることが挙げられる。以下に全体の流れを示す。

(1) ユーザの接続

ユーザは AP を経由し、PPPoE の認証手順に従い、ID、パスワードを利用して認証を試みる。

認証要求パケットを受けた認証機構は、ユーザに対して、IP アドレスの付与を行う。

同時にパケット制御部では、その認証パケットのヘッダチェックを行い、そこから得られた認証機構先に認証の可否を問う。認証に成功した場合、認証機構は、成功したユーザの MAC アドレスと自分の認証機構名をパケット制御部に通知する。認証に失敗した場合、パケットは破棄される。

(2) 優先度管理局への問い合わせ

認証済みパケットを受け取ったパケット制御部は、認証機構に対応する優先度ランクを優先度管理局に問い合わせる。優先度管理局は認証機構に応じた優先度ランクをパケット制御部に通知する。

(3) 優先度処理

パケット制御部は優先度管理局から通知された

「The implementing system unified Authentication for Wireless LANs and priority control」

[†] 「Keiji Sakaguchi・Ritsumeikan University」

^{††} 「Masumi Yamashita・Ritsumeikan University」

[‡] 「Toshikazu Nishimura・Ritsumeikan University」

[‡] 「Hitoshi Ogawa・Ritsumeikan University」

優先度ランクを持つ MAC アドレスを使っている通信に対し、優先度ランクに基づいた帯域をユーザに割り当てる。

以下の図 2 に優先度処理全体の流れを示す。

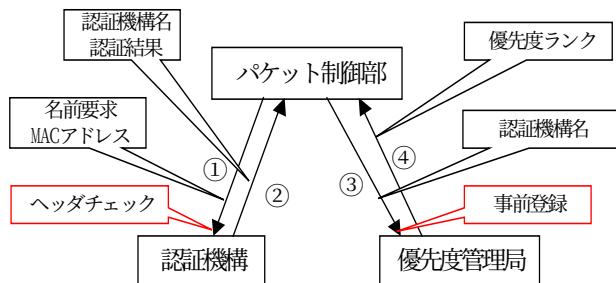


図 2. パケットの流れ

2.2 各部詳細

2.2.1 認証機構

本研究によって構築されるネットワークを利用する場合、1 つ以上の認証機構でユーザ登録を行う必要がある。各認証機構では、登録されたユーザの ID、パスワードを管理している。

認証機構は、ユーザの認証が成功すると、そのユーザに IP を付与する。同時に、パケット制御局からの要求に対して、自分の認証機構名と認証の可否を返す。また、ユーザがインターネットや社内 LAN を利用する場合は各認証機構のセキュリティポリシーが適用される。

2.2.2 優先度管理局

優先度管理局では全ての認証機構とその優先度ランクのリストを一元管理する。そのリストを参照し、認証機構から通知されたパケット制御部に MAC アドレスとそのランクを通知する。

将来、ネットワーク規模が拡大した場合は、DNS のような構造を持つ、優先度管理局のツリーによって大規模管理も可能と考える。

2.2.3 パケット制御部

パケット制御部はすべてのパケットのヘッダをチェックし、優先度管理局によって通知された MAC アドレスに対して処理を行う。そのため認証を受けたユーザの MAC アドレスと優先度ランクを組として保持する。

優先度管理局によって通知された MAC アドレスが未登録であれば、認証に成功するまでその MAC アドレスを持つ認証要求以外の全てのパケットを破棄する。

3. 優先度制御

3.1 優先度の概念

Diffserv 等の優先度機構はその背景として

VoIP やビデオストリーミングといったリアルタイムアプリケーションの普及に伴い、QoS 制御技術の必要性が高まり開発されたシステムである。そのため、優先度はアプリケーション又はパケットの種類に対し適用される。

しかし、本研究の優先度は認証団体毎に設定され、その団体に所属する全てのユーザが同一の優先度を得る。また、Diffserv では経路中の全てのルータにおいて優先度制御を行うが、本研究では、インターネット VPN によって構築されるため Diffserv を導入する事は不可能である。そのため、ネットワークの入り口で優先度を用いた帯域制御を行う。

3.2 優先度の順位

優先度の選定は認証機構毎の公私関係において、社会的意義が高位なほど利用帯域を保証する。つまり災害現場に置いて優先度の高いユーザとは、警察や消防といった状況改善ないしは緊急性の高い通信を行う団体に所属するユーザを指す。現時点で実装される順位はそのようなユーザとそれ以外のユーザに区別される。

3.3 優先度の適用

優先度はパケット制御部で制御する。パケット制御部に設置したキューには、AP を経由して VPN に流れるパケットを一旦全て入れる。その後、優先度ランクの高いキューに振り分けられたパケットから順に伝送する。ただし、認証要求パケットに関しては、常に最上位キューに貯められ優先的に伝送する。

現状では、前述の Priority Queuing を用いた優先度制御であるが、緊急時以外の状況に対して拡張性を持たすため、WFQ(Weighted Fair Queuing)を用いた優先度制御を考えている。

4. 終わりに

本稿では、無線 LAN 統合認証方式に優先度制御を導入した実装方法について提案した。現在、上記の実装環境を構築している。今後、優先度の適用が正しく行っているか実験を通して確認する。

文 献

- [1] 西村 俊和, 前田 忠彦, 小川 均, アンテナ 指向性制御を組み合わせた無線 LAN 統合認証方式, 情処研究報告 2004-MBL, Mar. 2004.
- [2] 戸田 巖, ネットワーク QoS 技術, オーム社, 2001.