

IEEE802.11u を用いた無線 LAN ローミングシステムの開発

山田雄輝[†] 加藤優一[†] 小林英子[†] 早乙女優[†] 松本大介[†] 八槇博史[†]東京電機大学[†]

1. はじめに

公衆無線 LAN のサービス増強が求められている。その一方、特に都市部ではアクセスポイント（以下 AP と記述する）の乱立により無線チャネルが埋まり、相互干渉による品質低下が顕著である。これ以上のサービス増強は、個別事業者が独自に AP を設置しているかぎりには困難である。これを解決するためには、一つの AP に複数の事業者のサービスが相乗りするローミングシステムが必要となる。

現在は、物理的には1台の AP が、仮想的に複数台の AP であるかのように振る舞う仮想 AP 方式が一般的に使われている。この方式の弱点は、一種の時分割方式によるため収容するサービス数の増加とともにパフォーマンスの低下が避けられないことである。このため商用製品でも二桁以上の仮想 AP を安定的に提供できるものは稀である。

本研究ではこの問題に対処するため、SSID によってサービスを識別する仮想 AP 方式ではなく、Hotspot 2.0 あるいは PassPoint の名称でも知られる IEEE 802.11u に基づいた複数サービス収容を行う方式を提案する。

2. IEEE802.11u

IEEE802.11u では、各 AP に対してネットワークアクセスを提供するサービスをローミングコンソーシアムと呼び、それが提供する外部接続を SSPN (subscription service provider network) と呼ぶ。それぞれのローミングコンソーシアムは 3 から 15 オクテットからなる OI (organization identifier) により識別される。端末が AP とアソシエーションを確立する前に、GAS (generic advertisement service) により、AP に登録された OI のリストを通知する。端末側にはそのユーザが予め契約したローミングコンソーシアムの OI が登録されており、通知された OI の中に既知のものがあれば、そのローミングコンソーシアムに対応した認証情報を用いて認証を行う。

従来の IEEE802.11 によって複数のネットワーク接続サービスを提供する場合は、SSID によるサービスの識別が一般に行われる。一つの AP に収容で

きる仮想 AP の数には限界があり、これが複数サービスを提供する際の制限となっている。IEEE802.11u の適用により、SSID によることなくサービスを識別することが可能となる。

その一方で、現行の規格には端末がどの OI を選択したかを AP に対して通知する仕組みを欠いており、IEEE802.21 などの別規格にもとづいて制御するものとされている。現在市販されている端末の多くにはその種の仕組みが実装されておらず、本研究で提案する機能の実現のためには、サービス選択機構を設計・実装する必要がある。

3. IEEE802.11u を用いた無線 LAN ローミングシステム

本研究では、複数の事業者のサービスを一つの AP にまとめるための IEEE802.11u を用いた無線 LAN ローミングシステムを開発した。図 1 にシステムの構成例を示す。これは、一つの AP に三つのインターネットアクセスサービスを収容する例である。

AP 管理者と事業者 1, 事業者 2, 事業者 3 は提携している。AP はサービス 1, サービス 2, サービス 3 を提供でき、サービス 1 の OI である 0A:0B:01, サービス 2 の OI である 0C:0D:02, サービス 3 の OI である 0E:0F:03 を OI のリストとして所持する。それぞれのサービスのトラフィックは別の VLAN に出力され、事業者の提供する SSPN へと転送される。

この例では、ユーザと事業者 2 は事前登録をしておきユーザは事業者 2 のサービスは利用可能である。よって、ユーザ端末にはサービス 2 の OI である 0C:0D:02 が登録されている。以下にこのシステムの流れを示す。

- ① IEEE802.11u の GAS を用いて AP がユーザにサービスを通知するための OI のリストを送信する。
- ② ユーザ端末は自身の登録してある OI と受け取った OI リストを照合する。この場合、ユーザ端末に登録してある 0C:0D:02 が OI のリスト内にあるのでサービス 2 に接続を行う。
- ③ AP はユーザ端末の認証情報を事業者 2 の認証サーバへ送信する。ユーザ端末と事業者 2 の間で EAP 認証による相互認証を行う。
- ④ 認証が成功した場合、A0C:0D:02 に基づいたサービス 2 の SSPN に VPN (virtual private network) 接続しユーザ端末のトラフィックを流す。

Development of Wireless LAN Roaming system using IEEE802.11u

Yamada Yuki[†] Kato Yuichi[†] Kobayashi Eiko[†]
Saotome Yu[†] Matsumoto Daisuke[†] Yamaki Hirofumi[†] Tokyo Denki University[†]

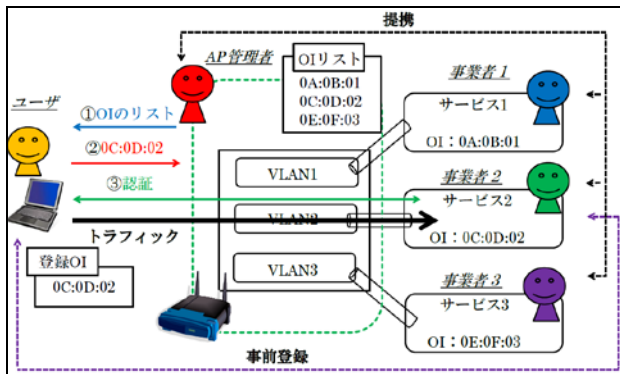


図1 想定する無線 LAN ローミングシステム

4. 認証連携

前節において、端末が選択した OI を②において通知することとなっているが、現行の IEEE802.11u 規格ではこの機能を欠いている。このため本研究においては、③の認証時に認証情報と合わせて選択した OI を通知する仕組みを採用する。

認証プロトコルとしては EAP-TLS, EAP-PEAP, EAP-TTLS といった、ユーザ ID を認証時に使用するものを前提とする。ユーザ ID に OI を付加することによって、どの事業者のサービスを使用するかを指定する。具体的には、各事業者が用いているユーザ名の先頭に OI を付加し、OI とユーザ ID の間にデリミタとして/(スラッシュ)をおく。たとえば、ユーザ ID が「個人識別番号@レルム名」の形式であるような事業者の場合、端末が AP に通知するユーザ ID は「OI/個人識別番号@レルム」の形式となる。

図2はこの方式に基づく認証連携機構の概要を示す。AP 管理者の管理下に AP と、OI に基づいて認証トラフィックの振り分けを行う認証プロキシサーバがある。認証成功後に端末のトラフィックを各事業者の SSPN に振り分けるのは無線 LAN ローミングシステム側の役割であり、その振り分け方針は AP 管理者によるものであるため、OI と VLAN の対応付けるデータベースは AP システム上に保持する。事業者がレルムによる振り分けを行うケースでは、事業者の管理下にも認証プロキシがおかれる。認証トラフィックは各事業者のもつ認証サーバで終端される。以下に図2の場合における認証手順を示す。

- ① 端末から送信された認証情報を AP は認証プロキシ 1 に送信する。認証プロキシ 1 がユーザ名の/より前に記述された OI に基づいて、事業者の管理下にある認証系である認証プロキシ 2 に対して振り分ける。
- ② 認証プロキシ 1 から送信された認証情報を受信した認証プロキシ 2 は@より後にあるレルムに基づいて振り分けを行う。
- ③ 認証プロキシ 2 から受け取った認証情報を用いて認証サーバはユーザ認証を行う。

- ④ 認証が成功した場合、認証サーバは認証成功通知を認証プロキシ 2 に送信する。この通知が認証プロキシ 1 を通じて AP に到達する。
- ⑤ 認証サーバから受信した認証成功通知内のユーザ ID 中の OI に対応した VLAN ID をデータベースから検索し、それをユーザ端末に割り当てる。

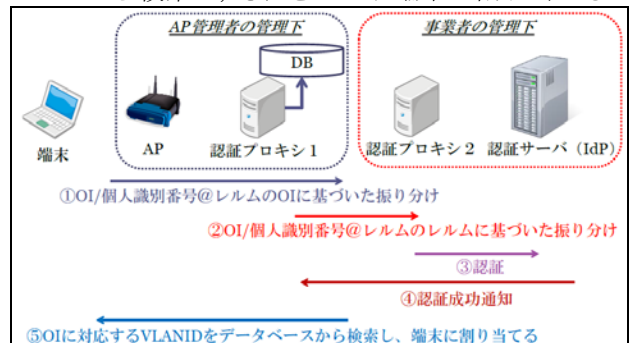


図2 認証連携機構の概要

5. 実装

本システムのプロトタイプを CentOS6.6 上に実装した。IEEE802.11u によるメッセージ交渉を行う AP プログラムとして hostapd-devel, 認証系に freeradius 2.1.12, VLAN と OI の対応関係や SSPN 構成を保持するためのデータベースとして MySQL5.1.73 を用いた。また、AP から各事業者の SSPN へトラフィックを誘導するための VPN システムとして、x12tpd による L2TP トンネルを使用した。

本システムの有用性の確認のため、1AP に収容するサービス数と、端末がアソシエーションを確立するまでの時間との関係を計測した。その結果、収容サービス数を 30 まで増加させてもアソシエーション時間 (約 0.6 秒) に変化はみられず、また通信を行う上での障害も発生しなかったことから、従来方式である仮想 AP 方式と比較してサービス収容数に関して優位性があると結論した。

6. おわりに

本稿では、IEEE802.11u 規格にもとづいて多数のネットワークアクセスサービスを 1 台の AP に統合する方式と、そのプロトタイプ実装による性能評価について報告した。今後は、同システムのオープンソース化による普及と、セキュリティに関する検討とを実施する予定である。

参考文献

[1] IEEE Standards Association. "802.11-2012-IEEE Standard for Information technology-Telecommunications and information exchange between systems Local and metropolitan area networks-Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications." (2012).